10.17625/NKE.2022.027

NEMZETI KÖZSZOLGÁLATI EGYETEM

KATONAI MŰSZAKI DOKTORI ISKOLA

PARÁDA ISTVÁN

A kiberműveletekben alkalmazható penetrációs teszt módszertana

Doktori (PhD) értekezés

Témavezető:

Dr. Kovács László

egyetemi tanár

Budapest, 2022

Tartalomjegyzék

BEVEZETÉS

„A számítógépes támadások ugyanolyan károsak lehetnek, mint a hagyományos támadások. Egyetlen támadás dollármilliárdos értékű kárt okozhat gazdaságunkban, leállíthatja a globális vállalatokat, megbéníthatja kritikus infrastruktúránkat, alááshatja demokráciánkat és bénító hatást gyakorolhat a katonai képességekre.”

- *Jens Stoltenberg a NATO Főtitkára* [1]

Bár a NATO mindig is védte kommunikációs és információs rendszereit, a 2002-es prágai csúcstalálkozón vette először napirendre a kibervédelmet. [2] A szövetséges vezetők 2006-ban a rigai csúcstalálkozón felismerték, hogy további védelmet kell biztosítani ezeknek az információs rendszereknek. [3] Az Észtország állami és magánintézményei ellen 2007-ben végrehajtott kibertámadások nyomán a szövetséges védelmi miniszterek ugyanennek az évnek júniusában megállapodtak abban, hogy e területen jelentős munkára van szükség. [4] Mindezekből egyértelműen látszik, hogy a NATO felismerte az új biztonsági kihívásokat, és lépéseivel reagálni kíván a bekövetkezett eseményekre és a folyamatosan változó helyzetre. Ezen túlmenően fejleszteni akarja az eddig elért és alkalmazott képességeit a kérdéskörrel kapcsolatban, illetve támogatni kívánja az oktatási, gyakorlat orientált ismeretterjesztési, a tudományos és a kutatási irányvonalakat. Továbbra is alapvető a NATO védelmi jellege, és elismerték a kiberteret a műveletek egyik dimenziójaként, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren. A NATO megerősíti a kiberoktatásra, képzésre és gyakorlatokra vonatkozó képességeit. Ezek a törekvések és vállalások egyértelműen kivehetők a 2016-os varsói csúcstalálkozóhoz köthető zárónyilatkozatból: *„A számítógépes támadások egyértelműen kihívást jelentenek a szövetség biztonsága szempontjából, és ugyanolyan Kiberstratégia szövetségben károsak lehetnek a modern társadalmak számára, mint a hagyományos támadások. Walesben megállapodtunk abban, hogy a számítógépes védelem része a NATO kollektív védelmi feladatainak. Most Varsóban megerősítjük a NATO védelmi mandátumát, és elismerjük a kiberteret olyan műveleti területnek, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren.”* [5]

A nemzeti biztonsági és nemzeti katonai stratégiák szemszögéből hazánk és a Magyar Honvédség is jelentős kihívásokkal áll szemben a kiberhadviselés és a kiberműveleti képességek fejlesztése terén. Az ezzel kapcsolatos munkának rengeteg eredményét látni, mint például a Magyar Honvédség Kibervédelmi Akadémia [6] létrehozása Szentendrén. Emellett számos folyamatban lévő tevékenység kíván eleget tenni mind állami, nemzeti, mind katonai oldalról, összhangban hazánk jelenlegi Nemzeti Biztonsági Stratégiájával [7] [8], Nemzeti Katonai Stratégiájával [9], valamint a Nemzeti Kiberbiztonsági Stratégiájával [10].

Az új Nemzeti Biztonsági Stratégia egyértelmű célokat és irányokat határoz meg a kibertér katonai védelmével és műveleteivel kapcsolatosan. Ilyen például az offenzív képességek megteremtésének szükségessége a Magyar Honvédségen belül. Az előző Nemzeti Biztonsági Stratégiához képest, ezek a kibertérhez kapcsolódó elvárások, tényleges biztonság- és védelempolitikai elmozdulást mutatnak.

Ezen felül meghatározható, hogy Magyarországon a biztonságpolitikai és katonai kiberműveleti törekvések a 2013. évi L. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvénnyel [11] való konszenzus mentén valósulnak meg.

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A folyamatos technológiafejlődésnek köszönhetően, az újabb biztonsági kihívások és fenyegetések megjelenésével az információs műveletek, valamint a kiberműveletek a katonai tevékenységek mindennapi részévé váltak. Ezen képesség létjogosultságát és folyamatosan növekvő tendenciáit az Európai Unió (a továbbiakban: EU), az Észak-atlanti Szerződés Szervezete (továbbiakban NATO), az Amerikai Egyesült Államok (továbbiakban USA), valamint Magyarország is felismerte. Egyértelműen látszik, hogy szinte valamennyi ország biztonságpolitikai szempontból nemzeti szinten törekszik a kibertérrel kapcsolatos biztonsági kérdésekre megoldásokat találni. Tehát, ami a katonai kiberműveleteket szorosan összeköti a biztonságpolitikával az maga a biztonság. Amennyiben a biztonság vagy a kiberműveletek nemzeti léptékű kezeléséről beszélünk, az azt jelenti, hogy hadászati szinten kell annak értelmezését végrehajtani. Alapvető kérdésként tehető fel, hogy a nemzeti stratégiák milyen módon kezelik az informatikai forradalmat és a vele járó lendületes ütemű információs, technológiai fejlődést. Figyelmen kívül hagyják őket, beépítődnek a folyamatokba, esetleg kihasználják a bennük rejlő lehetőségeket?

A kiberhadviselés, illetve a kiberműveletek módozatai és eljárásai számos nézőpontból vizsgálhatók. A kiberképességek között az egyik ilyen fontos kutatható elem a behatolás

tesztelés (a továbbiakban penetrációs teszt), mellyel kibertámadásokat modellezve, hasonló eljárásokkal tárjuk fel a saját informatikai rendszereink hiányosságait.

Mindezek alapján tehát a kutatásaimat meghatározó tudományos problémának azt tekintem, hogy mivel a nemzetközi példák nem ültethetők át teljesen a hazai eljárásrendekbe (hiszen azok általában nem katonai jellegű felhasználásra készültek), hazánknak önállóan kell meghatározni és kifejleszteni egy olyan módszert, mely megfelelő alapot biztosít az informatikai hálózat tesztelése során, valamint részletes bizonyításokkal alátámasztva egy eljárásrendhez köthető és követhető keretet alkot.

Témaválasztásomat alapvetően meghatározta a Magyar Honvédség vitéz Szurmay Sándor Budapest Helyőrség Dandár, Híradó és Informatikai Rendszerfőközpont, Informatikai Főközpont (továbbiakban MH BHD MH HIRFK IFK) hálózati rendszermérnök beosztásban töltött évek során szerzett tapasztalat, valamint a NATO Kooperatív Kibervédelmi Kiválósági Központ (továbbiakban CCDCOE[1]) által tartott BOTNET[2] csökkentő, illetve Kibervédelem operatív szinten című[3] tanfolyamon való részvétel. Ezen felül a Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Híradó Tanszék oktatói beosztásban eltöltött idő tapasztalata, mely során arra a megállapításra jutottam, hogy szükséges az etikus hack-elési eljárások alapmódszereinek beépítése az oktatásba.

A tudományos kutatómunkám során végrehajtom a saját tesztelési módszertanom, illetve az alkalmazható tevékenységi folyamatok tudományos kidolgozását és továbbfejlesztését.

Szakmai meggyőződésem, hogy a Magyar Honvédség informatikai és információvédelmi szakemberei a lehető legnagyobb szakértelemmel látják el üzemeltetési feladataikat. Azonban az informatikai rendszer biztonságának növelése és szinten tartása érdekében alapvető és jogszabályban is lefektetett feltétel a tesztelés. Egyik legfontosabb ilyen biztonsági teszt a penetrációs teszt, amelynek első szintje a hálózati felderítés.

Ezen felül egy szakmailag modern, a jelenkor kihívásainak eleget tevő szakanyag fejlesztése, amely hozzájárulhatna a Nemzeti Közszolgálati Egyetem (a továbbiakban NKE)

---

[1] Cooperative Cyber Defence Centre of Excellence - Kooperatív Kibervédelmi Kiválósági Központ. a NATO Kiválósági Központjainak egyike. Központja Észtországban, Tallinnban, a Filtri u. 12. szám alatt lévő híradós laktanya területén található. A szervezet 2008. május 14-én jött létre. Oktatási, kutatási és fejlesztési feladatokat lát el. A NATO teljes jogú szervezete. Célja az elsajátított tapasztalatok és a konzultáció révén javítani a kibervédelem hatékonyságát, az együttműködést és az információ megosztását a NATO, annak tagjai és a kibervédelemben részt vevő partnerei között.

[2] A botnet olyan hálózatra kapcsolt gépek összessége, amelyek felett átvették az irányítást. Ezeket egész egyszerűen csak "botoknak", vagy zombi gépeknek hívjuk. A ilyen számítógépeket többnyire valamilyen malware-rel fertőzik meg azért, hogy a távolból is irányítani lehessen őket. Vannak olyan botnetek is, amelyek több százezer – esetenként több millió – számítógépből (vagy újabban okostelefonokból) állnak.

[3] https://ccdcoe.org/training/cyber-planning-at-operational-level-course-cpolc-oct-2019/

kiberspecifikus képzései vonatkozásában egy, a kiberműveletek során alkalmazható gyakorlati megvalósításokon, valamint az etikus hack-elési eljárásokon alapuló tananyag kialakításához, továbbá a hallgatók gyakorlati képzési szintjének emeléséhez. A jövőben a disszertációt tovább fejlesztve egy olyan szakmai útmutató kerül elkészítésre, melyet követve, a tesztelési folyamatot az arra jogosult alakulatok sikeresen végrehajthatják, természetesen az évenkénti felülvizsgálat melletti követelmény teljesülése esetén.

Mivel az értekezés összeállításnak időszakában bár léteznek általánosított tevékenység leírások, ezek elavultsága, valamint általános jellege lehetővé teszi, hogy specifikus műszaki megoldásokra tegyek javaslatokat, melyeket valós alternatívákkal kívánok alátámasztani.

KUTATÁSI HIPOTÉZISEK

1. A Magyar Honvédség egy megfelelő informatikai tesztelési módszertan birtokában hatékonyan tud reagálni a kor új típusú kihívásaira és fenyegetéseire, és kiaknázni a negyedik generációs hadviselésben, az információs műveletekben, a számítógép - hálózati, a hálózatközpontú hadviselésben, a hálózat nyújtotta képességben rejlő lehetőségeket. Egyik ilyen, a kiberműveleti képességekben rejlő lehetőség a saját hálózat és infrastruktúra tesztelése.
2. Egy fejlett, korszerű, technikai alapokon nyugvó penetrációs teszt keretrendszer megalkotása biztosítja a Magyar Honvédség infokommunikációs rendszerei alapvető biztonságának vizsgálatát, valamint annak elérését. A kiberműveletekben alkalmazott, főként technikai jellemzőkkel bíró felderítési megoldások, folyamatok megadják a keretet a saját infokommunikációs rendszerek, hálózatok tesztelésére és kiértékelésére.
3. A kiberműveleti penetrációs módszertannak költséghatékonynak, a doktrinális feladatrendszert támogató megoldásnak kell lennie. Ez megvalósítható a jelenlegi infokommunikációs eszközpark bázisán, előtérbe helyezve a nyílt forráskódú szoftvereket.
4. Végrehajtói szinten a kiberműveleti penetrációs módszertan képességelemek összpontosítására van szükség a rendelkezésre álló erőforrások optimális felhasználása érdekében. Ez a jelenlegi kiberműveleti alegység fejlesztésével, a képességmodulok egy egységbe rendezésével, egy már meglévő katonai szervezet vezetésével és irányításával valósítható meg a leghatékonyabban. Ennek struktúráját úgy kell meghatározni, hogy az illeszkedjen a nemzeti feladatrendszerhez, valamint a nemzetközi felajánlások rendszeréhez és jellegéhez egyaránt.

Kutatásaimban alapvetően támaszkodom a jelenlegi hazai, a Magyar Honvédség által használt, illetve a NATO és az amerikai stratégiákban, doktrínákban, valamint alapdokumentumokban rögzített elvek és eljárások feldolgozása során megismert információkra, javaslataimat ezen alapokon nyugvó tudományos eredmények tükrében fogalmazom meg.

KUTATÁSI CÉLKITŰZÉSEK

Kiterjedt elméleti kutatásaim és gyakorlati tapasztalataim alapján a következő célkitűzéseket fogalmazom meg.

1. **Megvizsgálni** a kibertér, kibervédelem, kiberművelet definícióit, valamint **elemezni** a NATO és az USA kibervédelmének fejlődését.
2. A nemzetközi penetrációs teszt modellek és módszerek példáinak **vizsgálatával,** a rendelkezésre álló nyílt forrású hazai, NATO, amerikai jogszabályokon keresztül **meghatározni** az alapdefiníciókat, a teszt kulcsfontosságú tulajdonságait, valamint a főbb nemzetközi infokommunikációs biztonsági tesztelések felépítését. Mindezek alapján **létrehozni a penetrációs tesztek saját megközelítésű osztályozását.**
3. **Megvizsgálni és értékelni** a Magyar Honvédségre vonatkoztatott jogszabályi háttér előírásait, valamint kapcsolódási pontjait egy penetrációs teszttel, és ezek alapján megalkotni **a penetrációs teszt Magyar Honvédségben alkalmazható modelljét.**
4. Nemzetközi, NATO, USA és hazai szabályzatok, szabványok, okmányok és releváns tudományos szakirodalmak elemzéseinek eredményei alapján **meghatározni a kiberhadviseléshez kapcsolható penetrációs teszt kiberműveleti hálózati technikai felderítés fejlesztésének lépéseit.** Meghatározott demonstrációk segítségével **bemutatni** egyes technikai tevékenységek lépéseit, bizonyításait, következtetésit, koncentrálva a közzétett adatok elemzésére és a portszkennelésre.

A KUTATÁS LEHATÁROLÁSA

Kutatómunkám során nem tekintettem a közvetlen kutatásaim tárgyának:

- A különböző analóg és digitális technológiák és technikák fejlődéstörténetének ismertetését, azok mélyreható vizsgálatát.
- A Magyar Honvédség analóg és digitális összetevőkkel egyaránt átszőtt stacioner és tábori hírrendszerének, a Kormányzati Célú Elkülönült Hírközlő Hálózatának a

részletes, rendszerszemléletű, technológiai, technikai, mérnöki jellegű bemutatását, jelenlegi állapotának vizsgálatát, mivel azt korábban már számos publikációban, szakcikkben, értekezésben és tudományos műben más szakemberek megtették.

- Az IoE[4] és IoT[5] kérdéskörét, mely témakör megítélésem szerint egy önálló PhD értekezés kutatási tárgyát is képezhetné egy különálló kutatási témaként, területként.
- A negyedik generációs hadviselésnek, az információs műveleteknek, a hálózatközpontú hadviselésnek, a hálózat nyújtotta képességnek, a digitális vagy másnéven információs hadszíntéren lezajló szembenállásnak, az információs fölény kivívásának, elérésének mélyreható, mindenre kiterjedő vizsgálatát, kutatását. Ezekre tanulmányok és tudományos szakcikkek formájában hivatkozok, és csak a szükséges mértékben, a fogalmak definiálása által térek ki.
- A sérülékenységelemzésnek, a social engineering-nek[6], a forensics-nek[7], a jelszó feltörésnek, a webes sérülékenységek exploit-jainak[8], a vezeték nélküli támadásoknak, a mobiltelefon támadásoknak és a stack alapú buffer overflow[9] támadások rendszerének részletes, mindenre kiterjedő bemutatását, ismertetését, mivel egyrészt ezeket korábban már számos publikációban, szakcikkben, értekezésben és tudományos műben más szakemberek megtették. Másrészt nem ebből a szemszögből közelítem meg a kiberműveleti penetrációs teszt módszertanának a Magyar Honvédség infokommunikációs rendszerére, hálózatára gyakorolt hatását, használhatóságát.
- A penetrációs teszt kiberműveleti technikai felderítési módszertan beintegrálhatóságának lehetőségének vizsgálatát.

---

[4] Internet of Everything Az internet mindennek (IoE) egy tág kifejezés, amely az internetre kapcsolt és kibővített digitális funkciókkal ellátott eszközökre és fogyasztói termékekre utal. Ez egy olyan filozófia, amelyben a technológia jövője számos különböző típusú készülékből, eszközből és tárgyból áll, amelyek kapcsolódnak a globális internethez.

[5] Internet of Things lényegében az a "platform", amelyen keresztül ez a sok-sok apró, kommunikációra képes okos eszköz elvégezheti az adatcserét.

[6] A Social Engineering (magyarul: pszichológiai befolyásolás) az a fajta támadás, mikor a támadó nem a technológiai sebezhetőséget használja ki egy-egy támadás során, hanem az emberi befolyásolhatóság a fő fegyvere. Rendszerint ezeknél a támadásoknál a támadó bizalmi kapcsolatot alakít ki az áldozattal, bizalmába férkőzik, hogy később ezt a bizalmat kihasználva az áldozat maga "kotyogja ki" az információt.

[7] A forensics célja, hogy egy informatikai rendszerben, egy számítógépen vagy egy mobil eszközön bekövetkezett eseményeket hiteles módon, az időrendiség betartása mellett rekonstruálja, felderítse.

[8] Az exploit (kihasználás, kiaknázás) informatikai biztonsági fogalom: olyan forráskódban terjesztett vagy bináris program, adathalmaz vagy parancssorozat, amely alkalmas egy szoftver vagy hardver biztonsági résének, illetve hibájának kihasználására, így érve el a rendszer tervezője által nem várt viselkedést.

[9] A puffertúlcsordulás (ang.: buffer overflow vagy buffer overrun) olyan szoftverhiba, sokszor biztonsági rés, melynél egy processz a fix hosszúságú tömbbe (puffer) történő íráskor nem ellenőrzi annak határait, így azt (például túl hosszú bemeneti adatok miatt) túlírva a szomszédos memóriaterületet írja felül. A felülírt memóriaterületen más adatok, a program változói, a program futását vezérlő adatok (programkód) is lehet. Ez a program hibás működéséhez, futásának befejeződéséhez (lefagyás) vagy a rendszer biztonságának sérüléséhez is vezethet.

KUTATÁSI MÓDSZEREK

Kutatásaim során primer és szekunder módszerek egyaránt felhasználásra kerülnek.

Deduktív kutatási stratégia alapján:

1. Szakirodalom kutatást, tanulmányozást, feldolgozást hajtok végre a releváns szakirodalmak vonatkozásában. Felkutatom, összegyűjtöm, áttekintem, elemzem, feldolgozom az értekezésem, vizsgálódásaim, kutatásaim által érintett részterületekhez kapcsolódó, releváns szabályozói hátteret, törvényeket, rendeleteket, utasításokat, határozatokat, intézkedéseket;
2. Összegyűjtöm, rendszerezem, elemzem, kifejtem a megítélésem szerint a kutatási témámhoz kapcsolódó releváns fogalmakat;
3. A rendelkezésre álló NATO és nemzetiközi szabályzók alapján megvizsgálom a hasonló tesztelésekre használt lehetséges modelleket, irányokat;
4. Kutatások másodelemzését hajtom végre úgymint, a NATO CCDCOE (a továbbiakban: NATO Kooperatív Kibervédelmi Kiválósági Központ) és az U.S. kiberműveleti képességek, kutatások, megvizsgálása. Következtetéseket vonok le, az ezzel kapcsolatos hatékonyságról és az adaptálási lehetőségek mértékéről. Megvizsgálom a hazai Kibervédelmi Stratégia témába illeszkedő elvárásait, előírásait. Következtetéseket vonok le a modell, illetve módszertan kidolgozásához;
5. A fenti vizsgálatok eredményeire, illetve szakmai tapasztalataimra alapozva meghatározom a penterációs teszt modelljének, illetve módszertanának elemeit. A rendszer tanulmányozása során elvégzem a módszertan eljárásainak vizsgálatát. Elemzem az ezekből felépülő metódusok tulajdonságait. Kidolgozom a módszertan eljárásrendjét, valamint üzemeltetésének műszaki megoldásit.

Induktív kutatási stratégia alapján:

6. Feldolgozom a rendelkezésre álló műszaki szakirodalmat, ezek reprodukálásával mérem a szoftveres végrehajtások létjogosultságát;
7. Végrehajtom a megvalósítható tesztelési mechanizmusok tapasztalati méréseit, és értékelem a kísérletek által szerzett adatokat, ezeket a Kali Linux[10] operációs rendszerrel hajtom végre;

[10] A Kali Linux egy nyílt forráskódú operációs rendszer, amelyet az alapokból fejlesztettek ki, mint a jól ismert BackTrack penetrációt tesztelő Linux-terjesztés. Több mint 300 behatolási tesztelési eszközt is tartalmaz, FHS-kompatibilis, széles körű vezeték nélküli eszközöket támogat, egyedi beágyazott rendszermaggal, több nyelven is támogatható, és teljesen testreszabható.

8. A kísérleti méréseken alapuló adatok értékeléséből következtetéseket vonok le, és állapítok meg.

AZ ÉRTEKEZÉS TERVEZETT FELÉPÍTÉSE

Értekezésem, felépítését tekintve négy fejezetet tartalmaz, melyek mindegyikét egy konklúzió formájában megfogalmazott, részkövetkeztetéseket, megállapításokat, részösszegzéseket tartalmazó résszel zárok le. A négy fő fejezetet megelőzendően, a bevezető részben vezetem fel, és fogalmazom meg a tudományos problémát. Ezt követően vázolom fel kutatási célkitűzéseimet, fogalmazom meg kutatási hipotéziseimet, határozom meg azt, hogy mi képezte és mi nem képezte kutatásom tárgyát, írom le kutatási módszereimet, adom meg azt, hogy mi képezte kutatásom bázisát, és határozom meg az alaki és formai megfontolásokat.

Disszertációm első fejezete a „Kibertér és kiberművelet". Ennek keretében, a tudományos eredményeim megfogalmazása érdekében, aprólékosan bemutatom a kiberteret és kiberműveleteket. Többek között részletezem a kibertér rétegeit, a kiberfölényt, a kiberműveletek jellemzőit, elveit és típusait. Ezen felül részletezem a kihívásokat és a penetrációs teszt szükségességét. Ezt követően bemutatom a NATO és az USA kibervédelmi irányelveinek kifejlődését.

Disszertációm második fejezetének a „Kiberműveleti penetrációs teszt alapjai és osztályozása" elnevezést adtam, mely az egyik legfontosabb pillére tudományos kutatásimnak, vizsgálódásaimnak. Ezért bemutatom a kiberműveleti penetrációs teszt alapjait. Többek között részletezem mi a különbség a penetrációs teszt és a sérülékenységelemzés között, kifejtem mi lehet a célja egy ilyen tesztnek, melyek a tulajdonságai, illetve korlátai. Ezen felül részletezem a kihívásokat és a teszt szükségességét. Ezt követően bemutatom magát a penetrációs tesztek osztályozást és azok jellemzőit. Általánosságban ismertetek minden olyan fogalmat, amelyek megítélésem szerint szükségesek, és elvezetnek a tudományos eredményeim megfogalmazásához és igazolásához.

A harmadik fejezetben, a „Kiberműveleti penetrációs teszt és annak munkafolyamata" kérdéskörére teszek javaslatokat, és fogalmazom meg tudományos eredményeimet. Ennek érdekében felvezetésként megvizsgálom, és bemutatom a módszertan lehetséges munkafolyamatát és ennek a Magyar Honvédséggel való kapcsolatát. Majd ezt követően a tervezés és előkészítés fázisban ismertetem magát a tervet és annak ismérveit, a hatókör meghatározását és a kötelezettségvállalást. Feldolgozom a dokumentáció és jelentés kérdéskörét.

A negyedik és egyben utolsó fejezetben bemutatom a kiberműveleti penetrációs tesztet, különös tekintettel a hálózati technikai felderítésen belül az információgyűjtés a közzétett adatokon keresztül, illetve a hálózatfeltérképezést demonstrálva. Tudományos módszerrel, ismételhetővé teszek egyes technikai lépéseket, melyek a végrehajtás és annak leírása után az általam megtervezett keretrendszerben módszertanná válnak. Alaposan kategorizálom, illetve csoportosítom e vizsgálatokat, és elméleti leírással segítem megértésüket.

Értekezésem ezen utolsó fejezetét pedig a tudományos eredményeim megfogalmazásával zárom, javaslatokat téve, ajánlásokat megfogalmazva.

1 KIBERTÉR ÉS KIBERMŰVELET

1.1 A KIBERTÉR

Napjainkban a háborús események műveleti környezete jelentősen eltérhet a hagyományos állam-állam elleni, reguláris erőkkel lebonyolított fegyveres konfliktusoktól. Az ilyen új típusú katonai műveletek egyik fontos jellemzője, hogy azok sokkal átfogóbbak és dinamikusabbak, illetve azokban az aszimmetrikus hadviselés elveit követve sok esetben irreguláris erők állnak szemben reguláris erőkkel. [12] A hibrid hadviselés másik jellemzője, hogy a béke és a háború közötti időhatár nem meghatározható, az állami és nem állami szereplők között általában nincs hadüzenet és nincs definiálható harctér sem. A műveletek egymástól elszigetelt helyszíneken, városokban vagy fizikailag nehezen behatárolhatóan a kibertérben kerülnek végrehajtásra.

Kiinduló értelmezés szerint a kibertér a számítógép-hálózatok és a rajtuk található szolgáltatások és információk alkotta virtuális világ összefoglaló neve. Az infokommunikációs technológia szakértői és a felhasználók szerint a kibertér egy számítógépekkel és kommunikációs kapcsolatokkal kialakított, globális hálózatra alapozott, többdimenziós, mesterségesen létrehozott virtuális valóság. Bármennyire is információtechnológia jellegű, mára az emberek közötti kapcsolatok kialakítására és fenntartására is szolgál. Kiemelendő a kibertér ember által létrehozott mesterséges tulajdonsága és az emberi kapcsolat hangsúlyozása. A kibertér térbeli tulajdonságának egyik alapja, hogy azt minden esetben mesterségesen hozzák létre, valamint több térformában van jelen. Ezt bizonyítja a Nemzetközi Távközlési Egyesület (a továbbiakban ITU[11]) kiberkörnyezet definíciója: „*közvetlenül vagy közvetett módon hálózatba kötött felhasználók, hálózatok, eszközök, szoftverek, folyamatok, tárolt vagy továbbított információk, alkalmazások, szolgáltatások és rendszerek összessége*”. [13] Ennek a környezetnek részét képezi minden olyan eszköz, rendszer, folyamat, információ és felhasználó, aki és amely hálózatos kapcsolattal rendelkezik. Nem tesz különbséget a kommunikáció módja és a hálózatba kapcsolt eszközök fajtája között.

[11] International Telecommunication Union- Nemzetközi Távközlési Egyesület az ENSZ mellett működő szervezet, melynek feladata a nemzetközi távközlési együttműködés segítése. Az ITU különböző bizottságai ajánlásokat adnak ki, amelyek figyelembe vételével dolgozzák ki az egyes országok kormányai a távközléssel kapcsolatos jogszabályokat.

A kibertér ilyen kiterjesztett értelmezését a hadtudomány az elsők között ismerte fel, és deklarálta, hogy azt a katonai műveleti környezet és így az információs hadszíntér egyik fontos tartományának tekinti. A kibertér katonai meghatározását elsőként az USA 2006-ban kiadott Kibertéri Műveletek Nemzeti Katonai Stratégiája tartalmazta: „*a kibertér egy olyan tartomány, ahol hálózatos rendszerekben és fizikai infrastruktúrákban működő elektronikai eszközöket és az elektromágneses spektrumot használják fel az adatok tárolására, cseréjére és módosítására*". [14] Az USA védelmi minisztériuma 2017-ben kiadott katonai terminológiai szótára módosította az előbbi meghatározást. Eszerint a kibertér „az információs környezetben, az egymással kölcsönös függőségben lévő információs infrastruktúrák hálózata és a bennük lévő adatok által létrehozott globális tartomány, amely magában foglalja az internetet, a távközlési hálózatokat, a számítógépes rendszereket, valamint a beépített feldolgozó és vezérlő elemeket". [15] A NATO Standard AJP-3.20 Allied Joint Doctrine For Cyberspace Operations doktrína meghatározza az ehhez tartozó alapfogalmakat: *Kibertér: „Az összes összekapcsolt kommunikációs, informatikai és egyéb elektronikus rendszerből, hálózatból és azok adataiból álló globális tartomány, beleértve az elkülönített vagy független, tartományokat is, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak."* [16] A kibertér nem korlátozódik egy mesterségesen felépített és folyamatosan fejlesztés alatt álló számítógépes környezetre. A kibertér infrastruktúra egy globálisan összekötött; azonban a földrajzi határoknak megfelelően a joghatósággal összefüggésben, nemzeti felelősséget vállaló hálózat. Ezért a klasszikus működési határok kiosztása a kibertérben különösen nehéz. A kibertér nem csak folyamatosan változik, de még ennél is fontosabb, hogy bárki szinte bármilyen célra használhatja. A kibertér abban is megkülönböztethető, hogy alapvető fizikai elemei teljesen ember alkotta, ami eltér a szárazföldtől, a levegőtől és az űrtől, valamint a tengertől.

A hazai kibertér definíciók közül az egyik a Magyarország Nemzeti Kiberbiztonsági Stratégiája, amely szerint: „*A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.*" [10] A Magyar Honvédség Kibervédelmi Szakmai Koncepciója szintén definiálja a kiberteret, amely szerint a „*kibertér az elektromágneses spektrum használatával meghatározható, dinamikusan változó tartomány, mely az összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál*". [17] Ezek hangsúlyozzák a kibertér hálózatos jellegét, és nem tesznek különbséget a hálózatok típusa és mérete között.

A kibertérnek a fent taglalt meghatározások analízis és szintézis útján kapott összefoglaló definíciója a következő: *A kibertér az ember által mesterségesen létrehozott,*

dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot. [18]

A katonai műveletekben a mobilitási követelmény kiütközőbb és kiugróbb. Harcászati-hadműveleti szinten a manőverező erők híradása, illetve a számítógép-hálózatok kialakítása az elektromágneses spektrumban főként rádiófrekvenciás megoldásokkal biztosítható. A harctéri infokommunikációs eszközök között többnyire rádiókapcsolaton keresztül valósul meg az adatátvitel. A harctéren az elektronikai eszközökből és számítógépekből napjainkban olyan összetett hálózatokat alakítanak ki, amelyeknek műveleti környezetüket a kibertér képezi. Ezek a hálózatok kevésbé használnak vezetékes kapcsolatot (akkor is főként stacioner pontok esetében), döntően vezeték nélküli eszközökkel valósítják meg a hálózati kommunikációt. [19] Természetesen a katonai műveletekben sem történt meg a teljes hálózatosítás, tehát nem minden elektromágneses spektrumban üzemelő eszköz bír hálózatos jelleggel. Vannak elektronikai berendezések, melyek önállóan működnek a harctéren. [20]

1.1.1 A kibertér rétegei

A kibertér az információs környezet mindhárom dimenziójában, vagyis a fizikai, az információs és a kognitív tartományban egyaránt értelmezhető. A kibertér rendelkezik fizikai eszközök hálózatos, a felhasználók, emberek közösségi hálózati kapcsolatos, valamint a vezeték nélküli kommunikáció hangsúlyos tulajdonságaival is. Az egyes eszközök, berendezések a fizikai térben definiálhatók, földrajzi elhelyezkedésük meghatározható. Az adatok gyűjtése, tárolása, feldolgozása és továbbítása az információs dimenzióban történik. A kibertér ugyanakkor az emberek társadalmi viszonyaira és a kapcsolataik alakulására is jelentős hatást gyakorol. Ezért létezik egy kognitív dimenzióban felfogható tartománya is, ahol az emberek egymással interakcióba kerülnek, valamint a hálózatban használt információt értelmezik. [21]

A kibertér rétegeit a 20. ábra mutatja be. E szerint a kibertér három rétegét különböztetjük meg:

- fizikai réteg;
- logikai réteg;
- kiberszemélyiség réteg.

A fizikai rétegben lévő entitások, például hardver alkatrészek, földrajzi helyhez vannak kötve. Ennek a rétegnek a kézzelfogható összetevői közé tartoznak a számítógépek, szerverek, útválasztók, hubok, kapcsolók, vezetékek és egyéb, az adattárolás, az adatfeldolgozás és az

adatátvitel szempontjából kulcsfontosságú berendezések. Tartalmazza más berendezések vagy rendszerek, például digitális érzékelők, fegyverrendszerek, C2 rendszerek és kritikus infrastruktúra integrált információs és kommunikációs technológiai összetevőit is. Bár a logikai rétegnek és a kiber-személyi rétegnek nincsenek tényleges határai, az államhatárok jogi szempontból relevánsak a hardverkomponensek földrajzi helyzetével kapcsolatban.

A logikai réteg kódokban vagy adatokban megnyilvánuló elemek, például firmware, operációs rendszerek, protokollok, alkalmazások és egyéb szoftverek és adatkomponensek. A logikai réteg nem tud működni a fizikai réteg és az információ vezetékes hálózatokon vagy az elektromágneses spektrumon keresztül történő áramlása nélkül. A logikai réteg a fizikai réteggel együtt lehetővé teszi a kiber-személy számára, hogy kommunikáljon és cselekedjen.

A számítógépes személyiségi réteg nem valós személyekből vagy szervezetekből áll, hanem virtuális identitásuk reprezentációjából. A virtuális személyazonosság lehet e-mail cím, felhasználói azonosító, közösségi média fiók vagy alias. Következésképpen egy személynek vagy szervezetnek több kiber-személye is lehet. Ezzel szemben több ember vagy szervezet is létrehozhat egyetlen közös, kiber-személyt. [16]

A kiberképességek kialakítása és alkalmazása során, az egyik nagy problémakör a hatásvizsgálat. Mivel a kibertér nem tisztán polgári vagy nem tisztán katonai tér, egy-egy rendszer elleni, az azok működését befolyásoló akciók számos más, esetenként nem is abban a dimenzióban működő rendszerre lehetnek hatással. Ezek felmérése a rendszerek összetettsége és komplexitása miatt szintén nehéz és bonyolult feladat. Mindezeken túl a kibertér megvalósításában és kialakításában nemcsak állami szereplők, hanem kis- és közepes vállalkozások, ipari szereplők, de még maguk az állampolgárok, azaz a felhasználók is részt vesznek. Ezért egy rendszer elleni kibertámadás nemcsak az adott rendszert létrehozó, az azt működtető, hanem az azzal kapcsolatban lévő többi rendszerre és alrendszerre is kihatással lehet. [23]

Összességében kijelenthető, hogy napjainkban a hálózatok fogalma nem csak infokommunikációs eszközök rendszerek összekapcsolását jelenti, hanem egy komplex, mindennapi életre is kiterjedő logikai és kognitív tartományokkal tűzdelt kibertéri jelenség. Ezen felül a hálózatos lehetőségek okán, az információs műveleti képességek és hatások a katonai műveletekben is megmutatkoznak.

1.2 KIBERMŰVELET

1.2.1 A kiberfölény és a kibertér műveletek értelmezése

Az amerikai szárazföldi haderő FM 3-12 Kibertéri és elektronikai hadviselési műveletek doktrínájának alapján a kiberfölény egy katonai erő kibertér-dominanciájának azon foka, amely lehetővé teszi e katonai erő számára, hogy adott időben és helyen biztonságos és megbízható műveleteket folytasson anélkül, hogy az ellenség vagy a szemben álló fél akadályozná abban. A kiberfölény lehetővé teszi, támogatja, biztosítja és megkönnyíti mindazon harci képességek kihasználását, amelyek befolyásolják, támogatják és lehetővé teszik mindenfajta harcfeladat végrehajtását és a mindennapi tevékenységet. [24] A kiberfölény hálózatos infokommunikációs technológiával valósítható meg, melynek következtében a saját képességek jelentősen megnőnek. A kiberfölény elérésének és megtartásának elemei közé tartozik az elektronikai és informatikai adatgyűjtő eszközökkel, illetve kommunikációs eszközökkel az információ biztosítása a másik fél képességeiről, a saját lehetőségekről és a környezetről, továbbá a másik fél hálózatos infokommunikációs rendszerei működésének hátráltatása, az információ feldolgozásának, továbbításának nehezítése, és a döntéshozók, a személyi állomány infokommunikációs hálózatokon keresztüli befolyásolása. Mindezek mellett a saját hálózatos információs képességek, a saját döntéshozók és a személyi állomány védelme a másik fél hálózaton keresztül végrehajtott logikai és fizikai (elektronikai) támadásaival és befolyásolási kísérleteivel szemben. Ahogy azt Haig Zsolt és Várhegyi István A cybertér és a cyberhadviselés értelmezése című művükben is megfogalmazzák: *„Az információ biztosítása egyrészt a másik fél elektronikai rendszereinek, számítógép-hálózatainak felderítését, másrészt a saját helyzetről szóló információk elektronikus feldolgozását, tárolását és továbbítását, harmadrészt pedig a környezetről szóló adatok elektronikai rendszerekkel, eszközökkel való megszerzését, feldolgozását, továbbítását jelenti. A másik fél hálózatos infokommunikációs rendszerei működésének korlátozása, akadályozása egyrészt a számítógép-hálózatokba való behatolással és ennek következtében például adatbázisok tönkretételével, módosításával, a hozzáférés akadályozásával, szoftveres és hardveres hibák előidézésével valósítható meg, másrészt az elektromágneses tartományban különböző támadási módszerek alkalmazásával is korlátozható e rendszerek működése. A döntéshozók és a személyi állomány befolyásolása a hálózaton keresztül továbbított valós és hamis üzenetekkel érhető el. A saját hálózatos információs képességeknek a másik fél logikai és fizikai (elektronikai) úton végrehajtott különböző támadásaival szembeni védelme magában foglalja a saját hálózatos infokommunikációs*

rendszereinkben rejlő lehetőségek maximális kihasználását, illetve e rendszereink elektronikai és számítógép-hálózati védelmét." [19]

Az információs műveletek meghatározásából kiindulva a kibertér műveleteket az alábbiak szerint definiálhatjuk: „*A kibertéri műveletek a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva, a kognitív képességekkel közvetlenül, illetve a technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire."*

Az Allied Joint Publication-3.20 dokumentum értelemzése szerint a kibertér művelet: „*A kibertérben vagy azon keresztül történő cselekvések, amelyek célja a barátságos cselekvési szabadság megőrzése a kibertérben és/vagy hatások létrehozása a parancsnokok céljainak elérése érdekében."[16]*

Figyelembe véve a kibertér kibővített meghatározását, a technikai képességekkel kapcsolatos tevékenységek közé sorolható:

- *„a számítógép-hálózatokba való bejutást, azok felderítését;*
- *az adatbázisokhoz való hozzáférést, azok módosítását, tönkretételét;*
- *a szerverek túlterhelésével a hozzáférés akadályozását;*
- *a távközlési hálózatok lehallgatását;*
- *az adatszerző és kommunikációs eszközök, rendszerek zavarását;*
- *a navigációs rendszerek elleni elektronikai támadás különböző formáit;*
- *valamint a szemben álló fél fentiekben részletezett hasonló tevékenységeivel szembeni védelmet."[18]*

Manapság számos esetben hallani különféle hackercsoportok által elkövetett kibertámadásról, amelyeket politikai célok vagy gazdasági haszon reményében kormányzati szervek, intézmények, gazdasági szervezetek stb. ellen követnek el. Ezek a támadások a megtámadott szervezet hálózatos infrastruktúrájában idéznek elő szolgáltatáskiesést, adatbázismódosítást, adatlopást. A hatásaik pedig a kibertér fizikai és logikai rétegében is jelentkeznek. Ezenfelül sűrűbben találhatók olyan kibertéri hatások is, amikor a cél nem valamilyen információs infrastruktúra működésképtelenségének előidézése, hanem a hálózatot használók és a tágabb közvélemény manipulálása. A hálózat által biztosított technológiai lehetőségek kamatoztatásával politikai és ideológiai üzenetek propagálásával olyan befolyásoló hatásokat elérni, amelyek az üzenetek követítőinek az érdekeit segítik. Ezek alátámasztják a

tényt, hogy a kibertérben végrehajtott műveletek felszámolják a markáns határokat a háborús és a békeidős tevékenységek között. Ez pedig a kibertérben zajló ellentevékenységek, védelmi és befolyásoló tevékenységek kulcsfontosságú tulajdonsága. [18]

Mindegyik képesség efefktív használatához nélkülözhetetlen a pontos, valós idejű és releváns felderítési információ. A technikai információs képességek lényegében a kibertér fizikai és logikai rétegeiben kerülnek végrejatásra, hatásuk is ott érzékelhető. Viszont a kognitív információs képességek a humánumra öszpontosítanak, az emberek és a társadalmi csoportok, véleményét, gondolkodását, viselkedését alakítják. Ezért a célpontjai, az emberek, közösségek. Csakhogy a befolyásoló, tájékoztató hatások kinyerése manapság már nem csak kizárólag a kognitív technikákkal vitelezhető ki. A modern hálózatos technológiák révén az internet, a közösségi hálózatok és az infokommunikációs eszközökön továbított célzott üzenetek alkalmazása mindennapossá vált. Tehát a kognitív befolyásoló hatások elérhetők hagyományos úton, mint például személyközi kommunikáció, illetve az infokommunikációs eszközöket alkalmazva, technikai eljárásokkal a kibertérben. Így a kognitív információs képességek felhasználásának területe lehet a kibertér fizikai és logikai rétege is, az itt továbított üzenetek pedig a kiberszemélyiség rétegben fejtik ki hatásukat. A fizikai megsemmisítés képesség szintén részét képezi a kibertéri információs műveleteknek. „*A tevékenység jellegét tekintve a fizikai megsemmisítés alapvetően a fizikai rétegben lévő hardverelemek, eszközök ellen alkalmazható különböző kinetikus hatású fegyverek, eszközök, valamint a megsemmisítést, rongálást végrehajtó erők, csoportok alkalmazását jelenti. Célpontjai a hálózatos infrastruktúra hardvereszközei (például szerverközpontok, optikai kábelek, mobilkommunikációs bázisállomások stb.), ezért a hatását is a kibertér fizikai rétegében fejti ki.”* [18]

1.2.2 Kiberműveletek jellemzői, elvei, típusai

A kibertér azért különbözik a többi tartománytól, mert ember alkotta, részben nem fizikai jellegű, és előfordulhat, hogy nem felel meg a földrajzi határoknak. A kiberműveletek számos környezetet érintenek, például az elektromágneses és információs környezeteket. A kibertér fizikai összetevői révén létezik a szárazföldön, a tengeren, a levegőben és az űrben. Ezzel szemben a fizikai területeken végzett műveletek hatékonyan működnek a kibertér révén. Következésképpen a négy tartomány dinamikusan kapcsolódik egymáshoz, az egyik tartomány változása hatással lehet a többi domain helyzetére. [16]

Elérés: Bár a kibertér tartomány más rendszerekben, például számítógépekben, hálózatokban vagy szervereken található fizikai elemeket tartalmaz, a hatások elérését a

kibertérben vagy azon keresztül nagymértékben nem befolyásolják azok a határok és korlátozások, amelyek általában más területekre vonatkoznak. Mivel a kibertér átfogó globális hatókörrel és összefüggésekkel rendelkezik, a kibertér szereplői szinte azonnal hatásokat hozhatnak létre a világ más részein. A kiberműveletek átfogó és határtalan jellege jelentősen növeli a célok kiválasztásának lehetőségeit. A kibertér alapvető összekapcsolhatósága miatt, ha csak egy elemet érint, legyen az egy weboldal, egy router vagy egy eszköz, a hatás lépcsőzetes lehet, lehetővé téve az effektek kihatását globális szinten több ponton. A kibertérben végzett műveletek területe tehát nem korlátozódik a műveletek szokásos földrajzi területére. [16]

Aszimmetrikus hatás: A kibertér könnyű, gazdaságos és globális hozzáférést kínál. Egy egyéni vagy viszonylag kicsi szervezet, megfelelő motivációval, erőforrásokkal és technikai képességekkel rendelkezve olyan támadást hajthat végre a kibertérben vagy azon keresztül, amely aránytalan az ellenfél méretéhez és viszonylagos erejéhez képest. A kibertérben vagy azon keresztül végzett tevékenységek kezdetben a digitális rendszerek, hálózatok vagy eszközök ellen irányulnak, bár a hatások a kibertér három rétegének bármelyikében megvalósulhatnak. [16]

Névtelenség: A kibertér alapos megértése és helyzetfelismerése elengedhetetlen. A számítógépes személyiségi rétegben található virtuális identitások gyakran lehetővé teszik a résztvevők számára, hogy névtelenek maradjanak, és elfedjék szándékukat, lehetővé téve mások számára, hogy a nevükben cselekedjenek. Ezenkívül a névtelenség megtévesztést tesz lehetővé. A kiberműveletek nyomon követése nehéz lehet, és a technológiai fejlődés ellenére sok incidens valószínűleg tagadható, néhány pedig követhetetlen. A tevékenységek hozzárendelése a kibertérben vagy azon keresztül elengedhetetlen, de nem függ kizárólag a digitális információktól. A több forrásból származó intelligencia, a rendszeres kriminalisztika és más módszerek kombinációja mind hozzájárul a résztvevő személyazonosságának feltárásához. [16]

Idő és sebesség: A kibertérben használt képességek a viszonylag egyszerű, gyorsan fejleszthető technológiai eszközöktől a kifinomult, hosszú fejlesztési időszakot igénylő eszközökig terjednek. Az ilyen képességek taktikai hatásokat fejthetnek ki, vagy stratégiai hatásokat érhetnek el. A technológia összetettsége és szintje elsősorban az elérendő hatásoktól, valamint a célzott rendszer összetettségétől függ. Ezért három időt és sebességet érintő szempontot kell figyelembe venni:

- Ezredmásodpercen belül az egyik országban a kibertérben vagy azon keresztül végrehajtott cselekvéseknek számos más országban is lehetnek távoli digitális hatásai, de a fizikai világban a bekövetkező hatások később következhetnek;

- A felkészülési idő hosszabb lesz, ha fontos a cél összetettsége, a hírszerzés, a specifikus hatások, a járulékos károk, a hozzáférés és/vagy az anonimitás. Következésképpen a hatás létrehozásáról szóló döntés, valamint a hasznos teher előkészítése és leszállítása közötti időszak jelentősen hosszabb lehet, mint a hagyományos fegyverek használata esetében. Hasonlóképpen az idő rövid lehet, ha ezek a megfontolások nem hangsúlyosak.
- A hasznos terhelés hatása azonnali, vagy szándékosan késleltethető.

A kibertér sajátosságai miatt a kiberműveletek hatásai megfoghatatlannak tűnhetnek a közvetlenül nem érintettek számára. Ez megnehezítheti a kibertér egyes hatásainak katonai értékű számszerűsítését.

Biztonság: A kibertérben a biztonság elengedhetetlen a cselekvési szabadsághoz azáltal, hogy megfelelő intézkedésekkel korlátozza a sebezhetőséget az ellenséges tevékenységekre és fenyegetésekre. A kiberbiztonság túlmutat a rendszerekre és hálózatokra irányuló rosszindulatú tevékenységek kezelésén. Ez magában foglalja a belső rendszerhibák és a külső hatások által nem okozott meghibásodások elleni védelmet is, amelyek hasonló romboló hatásúak lehetnek. Az ismert ellenfelek sebezhetőségének, kiaknázásának, módszereinek, technikáinak és rendelkezésre álló képességeinek nem kívánt nyilvánosságra hozatala veszélyeztetheti a jövőbeli kibertér műveletek hatékonyságát. [16]

Meglepetés: Az idő és a sebesség, az elérés és az anonimitás velejáró tulajdonságai alapján a kiberműveletek gyakran kihasználhatják a meglepetés elemét. A kiberműveletek hatásait nehéz lehet előre látni, észlelni és nyomon követni, ezért a figyelmeztetési idők jelentősen lecsökkenhetnek, vagy egyáltalán nem jelentkeznek. Ezenkívül a kiberműveletek lehetővé teszik a megtévesztést, ami hozzájárulhat a meglepetéshez. A kibertér műveletek ezért olyan ütemben futhatnak, amely eltér a többi katonai tevékenységtől. A kiberműveletek hatásai olyan időben, helyen és módon jelenhetnek meg, amelyre a megcélzott fél nincs felkészülve, és nagyobb eredményeket érhet el, mint az erőfeszítés. [16]

Az erő koncentrációja: A kiberműveletek egyedi jellemzői, különösen az elérés, valamint az idő és a sebesség alapján katonai hatások hozhatók létre egyszerre különböző helyeken. Ez kiterjeszti az erőkoncentráció hagyományos koncepcióját, és ezáltal már tartalmazza az egymást támogató, különböző helyszínű egyidejű hatásokat. [16]

A morál fenntartása: A kiberműveletek felhasználhatók a rendszerek vagy információk manipulálására. Ennek eredményeként csökkenhet a bizalom a katonai infokommunikációs rendszerekben és a katonai szervezetek vezetésében.

A cselekvés szabadsága: A cselekvési szabadság fenntartása a kibertérben előnyös a katonai, kormányzati és civil szervezetek számára. A cselekvési szabadság a kibertérben közvetlen hatással van minden katonai műveletre, de különösen a kibertér műveletekre, az információs műveletekre, a hírszerzésre, a megtévesztésre és a stratégiai kommunikációra. [16]

A jól meghatározott és jól kivitelezett kiberműveletek kiemelkedő fontosságúak a haderő harci hatékonysága szempontjából. Általában kétféle kiberművelet kerülhet végrehajtásra, a parancsnok szándékától és célkitűzéseitől függően. Fontos megjegyezni, hogy az ilyen típusú kiberműveleteket a szövetségesek és az ellenfelek is végrehajthatják:

- védekező kiberműveletek;
- támadó kiberműveletek.

1.2.2.1 Védelmi kiberműveletek

A védekező kiberműveletek olyan intézkedéseket tartalmaznak, amelyek célja a kibertér használatának megőrzése annak érdekében, hogy lehetővé tegye saját cselekvési szabadságát és erőinek védelmét. Ez magában foglalhatja a sebezhetőség értékelését és a kockázatkezelést, valamint a lehetséges reagáló intézkedések mérlegelését a működési igényeknek megfelelően. A védekező kiberműveletek általában a kibertérben zajló rosszindulatú tevékenységek megelőzésére és/vagy megszüntetésére és enyhítésére, valamint azok hatásaiból való helyreállításra irányulnak, ezáltal megőrizve a küldetésbiztosítást. A védekező kiberműveletek védik a hálózatokat és rendszereket, valamint az azokban található információkat. Az ellenséges kiberműveletek reagáló intézkedéseket követelhetnek meg, amelyek szükségesek a küldetés biztosításához és a parancsnok célkitűzéseinek eléréséhez. [16]

1.2.2.2 Támadó kiberműveletek

A támadó kiberműveletek végrehajthatók önálló műveletekként vagy más műveletekkel együtt. A kibertámadó képességek alkalmazásának célja főként az, hogy a lehető legmesszebb tartsuk a potenciális ellenérdekelt felet a saját rendszereinktől. Továbbá csökkenteni a lehetőségét a saját rendszereink felderítésére és támadására azáltal, hogy elérjük, hogy kiberkapacitásait a védekezésre fordítsa. A kibertérműveleteknek döntő többségben proaktív hozzáállást kell mutatniuk. Amennyiben a kibertérműveleteink csak a védelemre épülnek, úgy nagy eshetőséggel a szemben álló fél kezdeményezőképességeinek a dominanciája érvényesül. [16]

1.2.3 Kiberműveleti felderítés, adatgyűjtés

A kiberműveletek, a kibertámadás általában megelőző tevékenységet követel, ami nem más, mint a felderítés és adatgyűjtés. Ez az egyik legtöbb időt és teljes körű munkát igénylő előkészületi folyamat. Ezeknek a tevékenységeknek az összességére megfelelő képességeket kell kialakítani. A kibertérben alkalmazott műveletek információs (felderítő) támogatása megköveteli az összes elérhető, releváns, hiteles információ összegyűjtését. Ez lehet általános információgyűjtés és célzott felderítés eredményeként létrejövő információk együttese. Ennek az információgyűjtési- és elemzési képességnek tartalmaznia kell azokat a támadási lehetőségeknek az azonosítását, amelyeken keresztül az adott kiberművelet eredményesen kivitelezhető. Az információszerző- és feldolgozó képesség feltételezi a nemzetbiztonsági szolgálatok kiberhírszerzéssel foglalkozó szervezeti elemeivel fenntartott folyamatos és kétirányú kapcsolatot, de ezenfelül jelöli a nyílt forrásokból rendelkezésre álló információk gyűjtését. Természetesen a nyílt forrású információgyűjtésnek is vannak jogszabályi feltételei. Az információszerzés- és értékelés képesség azonban nem elegendő a kibertámadások célravezető megvalósításához. Ezenkívül a célpontok azonosítása, priorizálása és elosztása nélkülözhetetlen. [23]

A célpont-azonosításhoz, a műveletтervezéshez szükséges egy hiánytalan és hiteles kiberhelyzetkép létrehozása. Ennek a helyzetképnek a magját az információszerző- és elemző munkálat biztosítja, így lehetőséget nyújt a saját, a semleges, illetve a szemben álló fél erőforrásainak feltérképezésére. A kiberhelyzetkép ismeretében adódik mód a célok azonosítására, kijelölésére és priorizálására. Az ilyen típusú tevékenységek esetében kulcsfontosságú feladat a szemben álló fél hálózatai technikai kialakításának, valamint védelmi mechanizmusainak a meghatározása. Innentől kezdve a célok ismeretében a műveletek fő irányai definiálhatók. Attól függően, hogy önálló kiberművelet végrehajtása a cél vagy egy más domain-ben történő művelet kibertéri támogatása, úgy a célok változhatnak.Ezek tudatában kijelölhető a felhasználható humán és technikai erőforrás, az erők elosztása, és végrehajtható a kiberműveletek hatásainak vizsgálata. [23]

Amikor a kiberfelderítés elér egy bizonyos határvonalat, akkor az ellenérdekelt fél azt a kibertámadás megalapozásának tekintheti, és kibertámadás képében válaszreakciót válthat ki. Ezek szimulációs képességek végrehajtása esetében kirajzolódhatnak, megfelelően beállított jelzésértékek használatával. A szimuláció alkalmat ad a tervezett kibertámadások szisztémájának és eszközeinek a finomhangolására, valamint azok hatásainak előzetes felmérésére. [23]

1.2.4 Kibervédelem fejlődése az USA-ban és a NATO-ban

1.2.4.1 A NATO kibervédelmi irányelveinek fejlődése

Napjainkban az információs és az infokommunikációs technológiák használata alapszolgáltatásnak minősül. Életünk szinte valamennyi szegmensére hatást gyakorolnak a pénzügyi ügyletektől kezdődően a munkahelyi kötelezettségeinken keresztül az egyszerű tevékenységeinkkel bezárólag. Amennyiben a katonai oldalról vizsgáljuk meg a kérdéskört, akkor egyértelművé válik, hogy az informatikai, távközlési és elektronikai technológiák rohamos fejlődése kikerülhetetlenül elérte a biztonságpolitika területét is. E fejlődés és ennek nyomán a kiberműveletek megjelenése kihatással van a politikai és a gazdasági szektorra, valamint a fegyveres erőkre is. [25] Magyarország NATO-tagállamként betartja és teljesíti a Szövetség alapokmányában foglaltakat.

A kiberirányelvekkel kapcsolatos folyamatok bemutatása előtt fontos rögzíteni a kiberbiztonság meghatározását. A kiberbiztonság meghatározása – hivatkozva az ITU-T X.1205 jelzésű dokumentumára – a következő: *„A kiberbiztonság az eszközök, a politikák, a biztonsági koncepciók, a biztonsági garanciák, az iránymutatások, a kockázatkezelési megközelítések, a cselekvések, a képzés, a legjobb gyakorlatok, a biztosítékok és a technológiák gyűjteményét jelenti, amelyek a kiberkörnyezet, a szervezet és a felhasználói eszközök védelmére használhatók. A szervezet és a felhasználói eszközök közé tartoznak a számítástechnikai eszközök, a személyzet, az infrastruktúra, az alkalmazások, a szolgáltatások, a telekommunikációs rendszerek, valamint a továbbított és/vagy tárolt információk összessége a kiberkörnyezetben. A kiberbiztonság célja a szervezet és a felhasználók eszközei biztonsági tulajdonságainak elérése és fenntartása a kiberkörnyezetben meglévő biztonsági kockázatokkal szemben.” [26]*

A NATO 2007 óta kiemelten kezeli a kibervédelem és kiberhadviselés kérdéskörét. Számos adat van a 2007-ben Észtország ellen indított kiberműveletekről, amikor meghatározó jelentőségű szolgáltatásmegtagadást kiváltó támadássorozat történt. 2007 áprilisában Tallinnban egy második világháborús szovjet emlékmű eltávolítását az észtországi orosz lakosság nagy felháborodással fogadta. Ezzel egy időben internetes támadások érték az észt informatikai és távközlési infrastruktúrát, főként az országon kívülről. A valószínűsíthető orosz támadások az Észtország és Oroszország közötti nézeteltéréseknek tulajdoníthatók. Az incidens a hadviselés teljesen új formáira irányította a figyelmet. Az esemény jelzésértékű példa arra, hogy az infokommunikáció milyen fontos szerepet játszik a társadalomban. Az eseménysorozat egyértelművé tette, hogy a NATO-nak az új kihívásokra reagálnia kell, és fel kell ismernie a

megfelelő képességek fejlesztésének szükségességét. Különösképpen azért is, mert – az Észak-atlanti Szerződés Szervezete megalakulásakor Washingtonban 1949. április 4-én aláírt Alapokmány 5. cikke, azaz a kollektív védelem értelmében – egy NATO-tagországot ért támadás a szervezet elleni támadásnak tekintendő. A NATO Alapokmány 5. cikkelye így szól: *„A Felek megegyeznek abban, hogy egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek, és ennélfogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert jogos egyéni vagy kollektív védelem jogát gyakorolva támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Féllel egyetértésben azonnal megteszi azokat az intézkedéseket – ideértve a fegyveres erő alkalmazását is – amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart."* [27] Az észt informatikai és távközlési infrastruktúra megbénítását eredményező támadást felismerve a NATO szükségszerűnek látta kiberbiztonsággal és kiberműveletekkel kapcsolatos intézkedések bevezetését.

A Szövetség 2008-ban megalapította a Kooperatív Kibervédelmi Kiválósági Központot a CCDCOE-t. Az intézmény a kiberműveletek és a kiberbiztonság oktatásával, kutatásával és fejlesztésével foglalkozik, és a műszaki-technológiai nézőpontokon kívül vizsgálja az erkölcsi és a jogi kérdésköröket is. A CCDCOE alapításának elgondolását a szövetséges erők transzformációs főparancsnoka 2006-ban hagyta jóvá. A támogatónemzetek tárgyalásai 2007-ben kezdődtek, az egyetértési megállapodást 2008-ban írták alá. Az alapító tagokon kívül folyamatosan csatlakoznak a NATO-tagállamok közül a támogatónemzetek, köztük Magyarország is, aki 2010-ben csatlakozott. [28] A 2007-es események következményeként a nyilatkozatokban is egyre nagyobb hangsúlyt kaptak a kiberbiztonságról, kiberműveletekről alkotott elképzelések. Ahogy az látszik a 2008-as bukaresti csúcstalálkozó nyilatkozatán is. [29]

A lisszaboni csúcstalálkozón 2010-ben elfogadtak egy új stratégiai tervezetet, amelyben az Észak-atlanti Tanácsnak[12] feladata volt egy alapos, új NATO kibervédelmi politika kidolgozása és egy végrehajtási terv elkészítése. Az Alapokmány 5. cikke értelmében a fegyveres támadások kibővítésre kerülnek a kollektív védelem vonatkozásában. [30] A lisszaboni csúcstalálkozó nyilatkozata az előzőekhez képest részletesebb információkat

[12] North Atlantic Council – NAC - Észak-atlanti Tanács a NATO legfőbb politikai döntéshozó testülete. Mindegyik tagországnak van képviselője a NAC-ban. E testület legalább hetente ülésezik, vagy szükség esetén bármikor, különféle szinteken. Az üléseken a főtitkár elnököl, aki segíti a tagokat abban, hogy a fő kérdésekben megállapodásra jussanak.

tartalmazott a kiberbiztonság kérdéskörével kapcsolatban. Megjelent a kibertér fogalma, és fontossá vált a kibervédelem az ellentétek kezelésében. Jelentős szerepet kapott a képességek elérésének felgyorsítása, valamint a tervezési folyamatok szükségessége a szövetségesek segítésére. [31]

A 2012 májusi chicagói csúcstalálkozón a szövetségesek vezetői megerősítették elkötelezettségüket, hogy javítsák a Szövetség kibervédelmét oly módon, hogy valamennyi NATO-hálózatot központi védelem alá helyezték, és jelentős fejlesztéseket hajtottak végre a számítógépes incidenskezelő képesség (továbbiakban NCIRC[13]) területén. A Lisszabon utáni kibervédelmi elgondolás, politika és cselekvési terv elfogadásával elkezdődött annak megvalósítása is. Integrálták az újabb kibervédelmi intézkedéseket a Szövetség rendszereibe és eljárásaiba.

2014 májusában a NCIRC elérte teljes működőképességét, ami fokozott védelmet biztosított a NATO-hálózatok- és felhasználók számára. A szeptemberi walesi csúcstalálkozón a szövetségesek támogatták az új kibervédelmi politikát, és jóváhagytak egy új cselekvési tervet, amely a politikával együtt hozzájárul a Szövetség alapvető feladatainak teljesítéséhez. A politikát és végrehajtását a Szövetségen belül mind politikai, mind technikai szinten szoros felülvizsgálat alatt tartották, és a kiberfenyegetésnek megfelelően frissítették. A NATO és az Európai Unió 2016. február 10-én megkötötte a kibervédelemről szóló technikai megállapodást, miszerint mindkét szervezet megfelelő segítséget nyújt a kibertámadások megelőzéséhez és a reagáláshoz. Ez a technikai megállapodás az NCIRC és az EU számítógépes vészhelyzeti reagáló csoport (CERT-EU[14]) között keretet biztosít az információcseréhez és a legjobb gyakorlatok megosztásához a válságkezelő csoportok között.

2016. június 14-én a védelmi miniszterek megállapodtak abban, hogy a varsói csúcstalálkozón dimenzióként ismerik el a kiberteret. Ez a Szövetség jelenlegi működési területeinek – levegő, víz, szárazföld és világűr – a kiegészítése egy újabbal. A kiberteret illetően számos meghatározással találkozhatunk, a sok közül egyet emelnék ki. Az Amerikai Egyesült Államok Védelmi Minisztériumának hivatalos szótára alapján a kibertér *„az információs környezetben az egymással kölcsönös függőségben lévő információs infrastruktúrák hálózata és a bennük lévő adatok által létrehozott globális tartomány, amely magában foglalja az internetet, a távközlési hálózatokat, a számítógépes rendszereket, valamint a beépített feldolgozó és vezérlő elemeket”.* [32] Ez a felismerés nem változtatja meg a NATO küldetését vagy megbízását, amely védekező. Akárcsak a cselekvés minden területén, a NATO

[13] NATO Computer Incident Response Capability – számítógépes incidenskezelő képesség
[14] Computer Emergency Response Team European Union – EU számítógépes vészhelyzeti reagáló csoport

a nemzetközi joggal összhangban jár el. A Szövetség elismerte az egyéb nemzetközi fórumokon tett erőfeszítéseket is, melyek arra irányultak, hogy kidolgozzák a felelősségteljes állami magatartás normáit és a bizalomépítő intézkedéseket, és elősegítsék a nemzetközi közösség átláthatóbb és stabilabb kiberterének a létrehozását. A 2016 júliusban rendezett varsói csúcstalálkozón a szövetséges állam- és kormányfők ismét megerősítették a NATO védekező megbízatását és a már elismert kiberteret a műveletek egyik területeként, amelyben a NATO-nak hatékonyan meg kell védenie magát, mint ahogyan azt teszi a többi négy dimenzióban. A szövetségesek is kötelezettséget vállaltak arra, hogy nemzeti hálózataik és infrastruktúráik kibervédelmét előtérbe helyezzék. A NATO és az EU 2016. december 6-án több mint 40 olyan intézkedést fogadott el, amelyek elősegítik a két szervezet együttműködését, beleértve a hibrid fenyegetések[15] [33] elleni küzdelmet, a kibervédekezést és a közös szomszédságuk stabilabbá és biztonságosabbá tételét. A kibervédelem területén a NATO és az EU közös gyakorlatokat tart, elősegítik a kutatást, a képzést és az információk megosztását. *„(70.) A kibertámadások egyértelműen kihívást jelentenek a Szövetség biztonsága szempontjából, és ugyanolyan károsak lehetnek a modern társadalmak számára, mint a hagyományos támadások. Walesben megállapodtunk abban, hogy a kibervédelem része a NATO kollektív védelmi feladatainak. Most Varsóban megerősítjük a NATO védelmi mandátumát, és elismerjük a kiberteret olyan műveleti területnek, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren. Ez javítani fogja a NATO azon képességét, hogy ezeken a területeken védje és végezze műveleteit, és minden körülmények között megőrizze cselekvési és döntéshozatali szabadságát. Továbbá támogatja a NATO szélesebb körű elrettentését és védelmét: a kibervédelem továbbra is beépül a működési tervezésbe és a Szövetség műveleteibe és küldetéseibe, és együtt fogunk dolgozni, hogy hozzájáruljanak a sikerhez. Ezenkívül biztosítja a NATO-kibervédelem hatékonyabb megszervezését és az erőforrások, készségek és képességek jobb kezelését. Ez a NATO hosszú távú alkalmazkodásának része. Továbbra is végrehajtjuk a NATO-nak a kibervédelemre vonatkozó továbbfejlesztett politikáját, és megerősítjük a NATO kibervédelmi képességeit, kihasználva a legújabb élvonalbeli technológiákat. (71.) Biztosítjuk, hogy a szövetségesek megfeleljenek a 21. századra szabott követelményeknek. Napjainkban a Kibervédelmi Vállaláson (Cyber Defence Pledge) keresztül elköteleztük magunkat nemzeti hálózataink és infrastruktúráink kibervédelmének növelése mellett. Támogatjuk a NATO kibervédelmi gyakorlat (Cyber Range)*

[15] Hibrid fenyegetéseknek azon képességeket nevezzük, amelyek révén az ellenfelek hagyományos és nem hagyományos eszközöket egyidejűleg, adaptívan tudnak alkalmazni saját céljaik elérése érekében.

képességét és hatókörét, ahol a szövetségesek készségeket építhetnek, növelhetik a szakértelmet és megismerhetik a legjobb gyakorlatokat." [34]

A védelmi miniszterek egy frissített kibervédelmi és egy cselekvési tervet fogadtak el 2017. február 16-án a kibertér műveleti területként történő végrehajtására. Ez növeli a szövetségesek együttműködési képességét, képességeinek fejlesztését és az információk megosztását. A védelmi miniszterek 2017. november 8-án elvben egyetértésüket fejezték ki egy új Kiberműveleti Központ létrehozásáról az adaptált NATO parancsnoki struktúra körvonalazásának részeként. Ez erősíti a NATO kibervédelmét, és segít a kiberintegrációs tervezésben és működésben. A miniszterek megállapodtak abban is, hogy integrálják a szövetségesek nemzeti kiberképességeit a NATO-missziókba- és műveletekbe.

1.2.4.2 Az Amerikai Egyesült Államok kibervédelmi irányelveinek fejlődése

Az Amerikai Egyesült Államok globálisan élvonalban áll a kiberbiztonsági politikák és stratégiák megvalósításában. A kormány már 2003-ban kiadta az első nemzeti számítógépes biztonsági stratégiát. [35] A 2003. évi nemzeti kiberbiztonsági stratégia három stratégiai célkitűzést fogalmazott meg:

- a kritikus infrastruktúrák elleni kibertámadások megelőzését;
- az internetes támadásokkal szembeni sebezhetőségek minimalizálását;
- az internetes támadások által okozott károk és a helyreállítási idő csökkentését.

E célok elérése érdekében öt nemzeti prioritást határoztak meg:

- szövetségi számítógépes rendszerek és hálózatok biztosítása;
- a reakcióképesség fejlesztése;
- a fenyegetések és a sebezhetőség csökkentése programjának létrehozása;
- tudatosságnövelő és képzési program a kiberbiztonságról;
- a nemzetközi együttműködés rendszere.

A következő szakasz időrendben áttekinti a legfontosabb stratégiai okmányokat és a szövetségi törvényeket, beleértve az amerikai elnökök végrehajtható végzéseit a kiberbiztonságról. Ezek a dokumentumok magukban foglalják:

- a nemzeti kritikus infrastruktúrák védelmét, valamint a szövetségi számítógépes rendszerek és hálózatok biztonságát;
- a szövetségi, állami, helyi, területi és magánpartnerek szerepének és felelősségének meghatározását;

- valamint a nemzetközi és a nemzetbiztonsági, a védelemi és a kémelhárítási kiberbiztonságnak a szempontjait.

A kilencvenes évek eleji kiberbiztonság kellemetlen problémává vált a létfontosságú nemzeti biztonság szempontjából. Az amerikai kiberbiztonsági irányelv a kritikus infrastrukturális védelmi erőfeszítésekben gyökerezik. 1996-ban Bill Clinton elnök kiadta a „Kritikus infrastruktúra védelme" című 13010 végrehajtási rendeletet. [36] A határozat létrehozta a Kritikus Infrastruktúra Elnökségi Bizottságát, amely felhívta a figyelmet az internetes támadásokra és a nemzetbiztonsági fenyegetésekre. Az 1998. évi 63. elnöki határozati irányelv [37] (továbbiakban PDD[16]) létrehozott egy struktúrát a Fehér Ház vezetése alatt a szövetségi kormány tevékenységének összehangolására a kritikus infrastruktúrák védelme érdekében az internetes támadásokkal szemben. A PDD 63 a kormányon belül számos kiberbiztonsággal kapcsolatos szervezetet hozott létre, köztük a Nemzeti Biztonsági, Infrastruktúravédelmi és Terrorizmusellenes Koordinátort, a Kritikus Infrastruktúra Hivatalt, ami támogatja a koordinátort és a Nemzeti Infrastruktúravédelmi Központot. [38]

A szövetségi információbiztonsági gazdálkodási törvény [39] (továbbiakban FISMA[17]), a 2002. évi e-kormányzati törvény részeként a Nemzeti Szabványügyi és Technológiai Intézet által kidolgozott kockázatkezelési keretet alkalmazta (továbbiakban NIST[18]) a kiber-biztonsági folyamatok szabványosítása érdekében az amerikai kormányzati szervezetek között. Ezen esemény eredményeként, a szövetségi információs vezérigazgató-helyettes (továbbiakban FCIO[19]) felelős a kormány technológiai alkalmazásának felügyeletéért, mind a kiadások, mind a stratégia szempontjából. Ez tisztázta és megerősítette a NIST felelősségét a szövetségi számítógépes rendszerek (a védelmi és hírszerzési rendszerek kivételével) biztonsági szabványainak kidolgozásáért, létrehozott egy központi szövetségi incidens központot és az Igazgatási és Költségvetési Irodát (továbbiakban OMB[20]) tette felelőssé a szövetségi kiberbiztonsági szabványok közzétételéért.

A belbiztonsági törvény [40] 2002-ben létrehozta a belbiztonsági osztályt (továbbiakban DHS[21]), többek között azáltal, hogy összehangolja a kritikus infrastruktúra védelmének nemzeti infrastruktúráját az informatikai és kommunikációs ágazatokban.

[16] Presidential Decision Directive - Elnöki határozati irányelv
[17] Federal Information Security Management Act - Szövetségi információbiztonsági törvény
[18] National Institute of Standards and Technology - Nemzeti Szabványügyi és Techológiai Intézet
[19] Federal Chief Information Officer
[20] Office of Management and Budget - Gazdálkodási és Költségvetési Hivatal
[21] Department of Homeland Security - Belbiztonsági Minisztérium

A szárazföldi biztonságról szóló, 2003. évi 7. elnöki irányelv [41] meghatározta a kritikus infrastruktúrák azonosítását és rangsorolását a fizikai világban és a kibertérben, a terroristatámadásokkal szembeni védelem érdekében. Az irányelv naprakésszé tette a különféle ügynökségek szerepét és felelősségét a 2002. évi belbiztonsági törvényben és más okmányokban. Megerősítette a DHS felelősségét a teljes kritikus infrastruktúra védelmére irányuló erőfeszítések irányításában, és kinevezte az osztályt az informatikai és kommunikációs iparág vezető ügynökségének, amely megosztja a fenyegetéssel kapcsolatos információkat, értékeli a sebezhetőségeket, és elkészíti a megfelelő biztonsági és vészhelyzeti intézkedéseket, terveket. Ezen kívül arra utasította a DHS-t, hogy hozzon létre egy nemzeti infrastruktúravédelmi tervet (továbbiakban NIPP[22]), ezért 2006-ban közzétették a Nemzeti Infrastruktúra védelmi Tervet. [42]

A Bush-kormányzat alatt a kiberbiztonság bonyolult volt, korlátozott vezetéssel és felelősségmegosztással a Fehér Ház, illetve a védelmi minisztérium között (a továbbiakban: DoD[23]). A belbiztonság átfogó koordinációs szerepet kapott, de a felelősség továbbra is az egyes ügynökségekre hárult. 2006-ban a Legfelsőbb Parancsnokság által kiadott, a kibertér-műveletekre vonatkozó nemzeti katonai stratégia az első átfogó okmány [43], amely leírja az amerikai katonaság megközelítését a kibertér-műveletekben. A dokumentum felvázolta az amerikai fegyveres erők szerepét az amerikai érdekek védelme szempontjából a kibertérben végrehajtott katonai műveletek végrehajtásában. A DoD stratégia szerint a katonai, hírszerzési és üzleti műveletek a kibertérből támaszkodnak a nemzeti katonai célok elérésére.

George W. Bush elnök 2008 januárjában aláírta a nemzetbiztonsági elnöki irányelvet és a 23-as belbiztonsági elnöki irányelvet [44] a DHS-re és az OMB-re, hogy minimális működési szabványokat állítson fel a szövetségi kormány polgári hálózatainak. Mindkét irányelv hangsúlyozta a teljes irányítási megközelítést, amelyet az Átfogó Nemzeti Kiberbiztonsági Kezdeményezés [55] követ (továbbiakban CNCI[24]) iránymutatásokkal. A CNCI kijelenti, hogy védelmet nyújt a fenyegetések legközvetlenebb és legteljesebb spektruma ellen, és megerősíti a jövőbeli biztonsági környezetet egy átfogó megközelítés biztosításával, amely magában foglalja a bűnüldözést, hírszerzést/kémelhárítást és a katonai képességeket. A CNCI megfelelő integrációjának, finanszírozásának és a kongresszussal, illetve a magánszektorral való megfelelő integrációjának, finanszírozásának és összehangolásának biztosítása érdekében Obama elnök 2009-ben egy 60 napos kiberűr-politikai áttekintés elnevezésű cyber-kormányzati

[22] National Infrastructure Protection Plan - Országos Infrastruktúra-védelmi Terv
[23] Department of Defense - Nemzetvédelmi minisztérium
[24] Comprehensive National Cybersecurity Initiative - Átfogó Nemzeti Kiberbiztonsági Kezdeményezés

felülvizsgálatot indított. [56] A felülvizsgálat egy erősebb Fehér Házra, valamint a szövetségi vezetés és az internetes biztonság elszámoltathatóságának erősítésére adott javaslatot. 10 rövid távú intézkedést és 14 középtávú intézkedést határozott meg a CNCI általános célkitűzéseinek támogatására.

A szélesebb körű nemzetbiztonsági és védelmi stratégiák szintén körvonalazzák a kiberbiztonság céljait. A 2010. évi nemzetbiztonsági stratégia [47] volt az első amerikai nemzetbiztonsági stratégia, amely figyelmet fordított a kiberfenyegetésekre, és a szövetségi kormány kiemelte a kiberfenyegetéseket, hangsúlyozva a nem állami terrorizmust. A 2010. évi négyévenkénti honbiztonsági áttekintés kiemelte a „kibertér védelmét és biztonságát", mint az öt fő nemzetbiztonsági küldetést. [48] A kiberbiztonsági folyamatokhoz közeledő katonai védelmi megfontolások alapján az Amerikai Kiberparancsnokság (továbbiakban USCYBERCOM[25]) 2010-ben jött létre, és ugyanabban az évben kezdte meg működését. [49] A nemzetbiztonsági stratégia végrehajtása és a Quadrennial Homeland Security Review [48] által kitűzött célok elérése érdekében a DHS kidolgozott egy cselekvési tervet, amely 2011-ben a Blueprint for Secure Cyber Future [50] elnevezést kapta, amely két területre terjed ki: „*a kritikus információs infrastruktúra és a számítógépes környezet."* 2011 májusában a Fehér Ház kiadta a nemzetközi kibertér stratégiáját [51], amely tükrözi az Egyesült Államok megközelítését a nemzetközi kapcsolatokban és a nemzeti prioritások közlésében. A stratégia általános célja a következő: *„Az Egyesült Államok olyan nemzetközi, nyitott, interoperábilis, biztonságos és megbízható információs és kommunikációs infrastruktúrát fog működtetni, amely támogatja a nemzetközi kereskedelmet, erősíti a nemzetközi biztonságot, előmozdítja a szabad véleménynyilvánítást és az innovációt. E cél elérése érdekében olyan környezetet építünk és tartunk fenn, amelyben a felelősségteljes magatartási normák szabályozzák az államok tevékenységét, fenntartják a partnerségeket és támogatják a jogállamiságot a kibertérben."* A kibertér nemzetközi stratégiája miatt az Egyesült Államok Nemzeti Minisztérium Stratégiája (2011) elismerte, hogy a kibertér önmagában hadszíntérré alakult, és hogy az Egyesült Államok növeli a levegő, az űr és a kibertér elrettentését, és javítja az Egyesült Államok azon képességét, hogy legyőzze a rendszerek vagy infrastruktúrák elleni támadásokat.

2012-ben az Obama adminisztráció támogatta azt a jogszabályt, amely felhatalmazást adna a DHS-nek a kritikus infrastruktúra-hálózatok védelmére, a törvényjavaslatot azonban kétszer nem fogadta el a Kongresszus. Válaszul Obama kiadta a - A kritikus infrastruktúra kiberbiztonságának javítása (EO 13636) [52] című kiadványt. Ez az elnökség számára kötelező

[25] U.S. Cyber Command's - Az amerikai kiberparancsnokság

érvényű dokumentum kiegészíti az összes korábbi dokumentumot, és jobb információcserét biztosít a szövetségi kormány és a magánszektor között. Ezen túl minimális kritériumokat is meghatároz a kritikus infrastruktúrák biztonságának javítása érdekében. Az EO 13636 szám alatt kiadott, a kritikus infrastruktúrák biztonságáról és ellenálló képességéről szóló elnöki irányelv (PPD-21) [53] nem tett jelentős változásokat a politikában, a szerepekben, a felelősségvállalásban és a programokban, ugyanakkor felszólította a meglévő köz- és magánszféra szereplőit a hatékony információcserére és az ennek alapjául szolgáló adatok és rendszerkövetelmények, valamint a helyzettudatosság fejlesztésének értékelésére. [54] Felhívta a figyelmet Nemzeti Infrastruktúra Védelmi Terv (NIPP) felülvizsgálatára, és végül a terv 2013-as harmadik felülvizsgálatának átdolgozására. A 2013. évi Nemzeti Kiberbiztonsági és Kritikus Infrastruktúra Védelem továbbiakban NCCIP[26]) [55] biztosítja a DHS szerepét a kiberbiztonság megelőzésében és reagálásában, valamint információcsere-partnerséget hoz létre a DHS és a kritikus infrastruktúra tulajdonosai és üzemeltetői között. A Quadrennial Homeland Security Review-et 2014-ben felülvizsgálták. A vizsgálat feltárta a DoD felelősségét egy új és kibővített teljes spektrumú kibertér képesség kifejlesztésében, hogy megvédjék országukat és támogassák a katonai missziókat világszerte. A DoD 2014. évi negyedéves védelmi áttekintése meghatározza a DoD legfontosabb szerepét a kibertérben miszerint védje a DoD hálózatainak integritását, védje a legfontosabb rendszereinket és hálózatainkat, hajtson végre tengerentúli műveleteket, és védje meg a nemzetet a küszöbön álló, destruktív kibertámadások ellen. A kiber-elektromágneses tevékenységek (FM 3-38) című dokumentum [56], amelyet az Egyesült Államok Hadserege 2014-ben tett közzé, útmutatást nyújt a kiber-elektromágneses tevékenységekhez, valamint taktikát és eljárásokat tervez, integrál és szinkronizál. A doktrína összehasonlítja a hadsereg műveleteit az elektronikus hadviseléssel. Ezenkívül a közös kibertér-műveletek[27] (JP 3–12) című dokumentum [57] a katonai műveletek egyediségével foglalkoznak a kibertérben. 2014-ben a szövetségi kormány létrehozott egy önkéntes kiberbiztonsági keretet, amelyet Kritikus Infrastruktúra Fejlesztési Keretnek [58] hívtak, és amely iránymutatásokat, gyakorlatokat és önkéntes szabványokat tartalmaz a magánszektor számára a kritikus infrastruktúra védelmének biztosítása érdekében.

Katonai szempontból a jelenlegi nemzetbiztonsági stratégia, amelyet 2015 elején fogadtak el, a korábbi 2011-es kiadás frissített verziója, felismeri a pusztító kiber-támadások növekvő veszélyét, és bejelenti az Egyesült Államok azon szándékát, hogy erősítse a kritikus

[26] National Cybersecurity and Critical Infrastructure Protection - Nemzeti Kiberbiztonsági és Kritikus Infrastruktúra Védelem
[27] Joint Cyberspace Operations - Közös Kibertér-műveletek

infrastruktúrák kiberbiztonságát. A dokumentum elsősorban az Egyesült Államok azon szándékára összpontosít, hogy előmozdítsa a nemzetközi szabványokat a kibertérben. Az új stratégia nagyobb átláthatóságot biztosít a DoD saját támadó és operatív képességei tekintetében.

Összességében megállapítható, hogy a kiberműveletek esetében a kiberfölény kialakításának alapvető törekvésnek kell lennie, valamint, hogy a kiberműveleteket végre lehet hajtani támadó és védekező céllal. Ezen felül vitathatatlan, hogy a NATO, illetve az USA időben felismerte a kibertérrel, kiberműveletekkel és azok biztonsági aspektusaival kapcsolatos kihívásokat.

1.3 KÖVETKEZTETÉSEK

Értekezésem első, bevezető fejezetében több célkitűzésem elérését valósítottam meg azért, hogy egy egységes keretet adjak kutatásaimnak, valamint részletezzek minden olyan releváns, a kutatási témám által érintett részterületet, amelyeknek ismertetése, bemutatása megteremtik az alapját a tudományos eredményeimnek.

Feldolgoztam a kibertérrel, kiberművelettel kapcsolatos alapfogalmakat, és végrehajtottam annak értelmezéseit. **Összefoglaltam** a kibertérműveletek lényegi elemeit, többek közt a jellemzőit, elveit, típusait.

Megvizsgáltam és bemutattam két fő kibervédelmi fejlődést a NATO, illetve az USA szemszögéből, az utóbbit a „Good Governance Knowledge Transfer Program NUPS – USA" program keretein belül volt szerencsém egy fél éves kutatásban megvalósítani a University of North Georgia (a továbbiakban UNG) egyetemen.

A fejezet eredményei alapján az alábbi rész-következtetéseket fogalmazom meg:

1. A hálózatok értelmezése napjainkra lényegesen megváltozott, az a kiberfizikai eszközök hálózatával, valamint az emberek révén létrehozott közösségi hálózatokkal egészült ki. A kibertér hálózatos lehetőségei miatt, az információs műveleti képességek és hatások a katonai műveletekben is megmutatkoznak. A kibertérnek a fizikai, a logikai és a kognitív tartományai azonos fontossággal bírnak, amelyek mindegyikében kivitelezhető kibertéri tevékenység. A kibertérben egyaránt megjelennek a technikai és a kognitív információs képességek.

2. A kiberműveletek felhasználhatók befolyásolásra, ellentevékenységre és védelemre egyaránt.
3. Egyértelműen látszik, hogy a NATO felismerte az új biztonsági kihívásokat, és lépéseivel reagálni kíván a kibertérben zajló eseményekre és a folyamatosan változó helyzetre. Ezen túlmenően fejleszteni akarja az eddig elért és alkalmazott képességeit a kérdéskörrel kapcsolatban. Véleményem szerint a NATO időben felismerte a kibervédelem és a kiberműveletek fontosságát. Jelentős erőfeszítéseket tett, és fog tenni az ehhez kapcsolódó képességek kialakítására és fejlesztésére, ezért, mint NATO tagállam, Magyarországnak és a Magyar Honvédségnek is hasonlóképpen kell eljárnia. A Magyar Honvédségen belül a kiberbiztonsági stratégiával összhangban a kiberbiztonsági képességek fejlesztése létfontosságú lehet a jövőben elvégzendő feladatok szempontjából.
4. Az Egyesült Államokban a kiberbiztonsági irányelv manapság részleges intézkedésekből áll, hasonlóképpen a jogalkotásokhoz melyek kevésbé átfogóak és inkább helyi, lokális jellegűek. Mivel nincs átfogó keret, amely ezeket a dokumentumokat szintetizálja, vagy átfogóan leírja a jelenlegi stratégiát, a világos megértés, valamint az általános stratégiai célok és prioritások meghatározása bonyolult feladat. Az Egyesült Államok kormánya a biztonságpolitika révén már a 90-es évektől gyökerezteti a kiberstratégiára vonatkozó irányelvalkotást, és egyértelműen felismerte az új biztonsági kihívásokat, illetve reagálni akar a felmerült eseményekre és helyzetekre.

2 KIBERMŰVELETI PENETRÁCIÓS TESZT ALAPJAI ÉS OSZTÁLYOZÁSA

Napjainkban általános és magától értetődő dolog, hogy a szervezetek az informatikai és kommunikációs rendszereik biztonságára törekszenek. Ennek egy része a rendszerek vizsgálata és ellenőrzése. A tesztek kiberbiztonsági nézőpontból is elvégezhetők, melyeknek egyik legfontosabb eleme a penetrációs teszt. A penetrációs teszt azt mutatja meg, hogy az informatikai biztonságot milyen mértékben fenyegetik a támadók, valamint a biztonsági intézkedések képesek-e megfelelő informatikai biztonságot nyújtani a támadások ellenére is. A feltárt fenyegetések leküzdéséhez az informatikai biztonság javítására irányuló intézkedésekre van szükség. A vállalati IT biztonsági rendszabályokkal összhangban minden ilyen intézkedést az egész szervezetre vonatkozó informatikai biztonsági koncepció ír le. Fontos megérteni a kibervédelmen belül a penetrációs tesztek folyamatát, és hogy ez nem egyenlő a köztudatban megjelent hack-eléssel. A penetrációs teszt egy összetett folyamat, mely technikai úton átfogó és reális képet ad az infokommunikációs rendszer sérülékenységeiről. Ebben a fejezetben bemutatom a penetrációs teszt alapjainak meghatározását, a sebezhetőségi elemzés helyét és szerepét, valamint a teszt alapvető paramétereit.

A penetrációs tesztet évek óta használják, és számos módszer létezik a rendszer műszaki biztonságának tesztelésére. Könnyű összekeverni a műszaki biztonsági tesztelés más formáival, különösen a sérülékenységelemzéssel. Számos szervezet kínál biztonsági funkciókat és megoldásokat, például a biztonsági auditot, a hálózati vagy kockázatértékelést, valamint egymást átfedő alkalmazásokat, melyek összekeverhetők a penetrációs teszteléssel.
Manapság számos ingyenes és kereskedelmi biztonsági szkenner létezik, amelyek többsége frissített adatbázisokat tartalmaz az ismert hardver- és szoftverhibákról. Ezek az eszközök alkalmasak a vizsgált rendszerek sebezhetőségének azonosítására, és ezért a velük kapcsolatos kockázatok meghatározására. Az ilyen eszközök által nyújtott információk általában tartalmazzák a biztonsági rés technikai leírását, és útmutatást nyújtanak a gyenge portok vagy pontok kiküszöbölésére a konfigurációs beállítások megváltoztatásával vagy a rendszer összetevőinek frissítésével, azonban a felderítések és a sérülékenységek kihasználása, valamint azok módszerbe fűzése mégsem történik meg.

Krasznay Csaba, a Nemzeti Közszolgálati Egyetem docense és a Kiberbiztonsági Kutatóintézet igazgatója szerint: „*A biztonsági tesztelési módszertanok csoportosítására*

jelenleg nincs egyezményes megállapodás, a tesztelt rendszerek ismeretétől kezdve, a hozzáférés mértékén át, a bevetett tesztelési eszközökig számos taxonómia létezik. Néhány fogalom azonban gyakran előfordul a szakirodalomban, melyek jól bemutatják a lehetséges módszereket". [59] [60] A fenti állásponttal teljes mértékben egyetértek, így ez volt kiindulópontom az alapvető fogalmak és paraméterek rendszerezésénél, a módszertanok elemzésénél, illetve a penetrációs tesztek saját osztályzásának megalkotásánál. Továbbá jelentősen tükrözi miért is fontos a módszertanok, vagy saját módszertannak a katonai vonatkozású kutatása, illetve a Magyar Honvédséggel való kapcsolatának vizsgálata.

2.1 PENETRÁCIÓS TESZT KULCS KONCEPCIÓK

2.1.1 A penetrációs teszt definíciója

A behatolási tesztelés számos manuális és automatizált technikát használ a szervezet biztonsági információs rendszere támadásának szimulálására. Ezt szakképzett penetrációs tesztelő szakértők végzik. A behatolási tesztelés kihasználja az ismert sebezhetőségeket, de tesztelési szakértelemre is szükség van a szervezet biztonsági rendszerei konkrét gyengeségeinek - ismeretlen biztonsági réseinek azonosításához. [61]

A penetrációs tesztelési folyamat a célrendszer aktív elemzése, a helytelen rendszerkonfiguráció, az ismert és ismeretlen hardver- vagy szoftverhibák, valamint a technológiai ellenintézkedések működési hiányosságai miatt fellépő esetleges sérülékenységek ellen irányuló tevékenység. Ezt az elemzést általában egy potenciális támadó szempontjából végzik, és magában foglalhatja a sebezhetőség kihasználását. Tehát a penetrációs teszt olyan szimulálási mód, amelyet egy támadó felhasználhat a rendszerünk elleni informatikai felderítéshez, és ezen túl a rendszer irányításának átvételéhez vagy egy magasabb szintű hozzáférés eléréséhez. Maga a folyamat magában foglalja a sebezhetőség és a biztonsági kockázati tényezők kiszűrését és összegyűjtését, majd támadásoknak való kihasználását. A penetrációs teszt több mint egy tesztet lefuttatni szkennereken vagy automatizált eszközökön, majd arról jelentést készíteni. A penetrációs teszt megbecsüli, hogy a sebezhetőség valós vagy hamis-e. Például egy ellenőrzés vagy felmérés olyan szkennelő eszközöket használhat, amelyek számos lehetséges sérülékenységet eredményezhetnek több rendszeren. A penetrációs teszt ugyanúgy próbálja megtámadni ezeket a sebezhetőségeket, mint egy rosszindulatú hacker, és ellenőrizni, hogy melyek a valódi sérülékenységek, csökkentve ez által a biztonsági rések valóságos listáját egyes biztonsági hiányosságok esetén. [62]

A behatolásteszt, amelyet az angol kifejezés, azaz a *penetration test* után gyakran pentestnek is rövidítenek, egy folyamat, amelyet alapos biztonsági értékelés vagy audit céljából végeznek. A módszertan meghatározza az információ és informatikai biztonsági ellenőrzési projekt által követett és végrehajtott szabályokat, gyakorlatokat és eljárásokat. **A penetrációs tesztelési módszertan meghatároz egy ütemtervet, amely gyakorlati ötleteket és bevált gyakorlatokat szolgáltat, amelyek nyomon követhetők egy hálózat, alkalmazás, rendszer vagy ezek bármely kombinációjának valódi biztonsági helyzetének felmérésekor.** A behatolásteszt elvégezhető külön-külön vagy egy informatikai biztonsági kockázatkezelési folyamat részeként, amely integrálható az informatikai, kiberbiztonsági fejlesztési életciklusba. A penetrációs teszt a biztonsági értékelés utolsó és leginkább agresszív formája. A penetrációs tesztelés eredménye általában több részre oszlik, amely foglalkozik a célkörnyezet jelenlegi helyzetében feltárt hiányosságaival, azok kihasználásának lehetséges következményeivel, majd javasolja a lehetséges ellenintézkedéseket és egyéb helyreállítási javaslatokat. A módszertani megközelítés alkalmazásának jelentős előnyei vannak annak érdekében, hogy a tesztelő megértse és kritikusan elemezze a jelenlegi védelem integritását a tesztelési folyamat minden szakaszában. A penetrációs tesztelési módszer oka az a tény, hogy a legtöbb támadó hasonló megközelítést követ, hasonló felderítési és kiaknázási lépéseken megy keresztül, amikor belép a rendszerbe. A penetrációs teszt során a tesztelőt olyan erőforrások korlátozzák, mint az idő, a képzetségi szint, a számítógépes erőforrások, valamint a berendezésekhez való hozzáférés. A penetrációs teszt a betolakodó által alkalmazott módszereket szimulálja, amelyek jogosulatlan hozzáférést biztosítanak a szervezet hálózatához és veszélyeztetik azt. Ide tartozik a saját és a nyílt forráskódú eszközök használata. Az automatizált technikák mellett a behatolási tesztek tartalmaznak manuális technikákat a célzott rendszerek tesztelésére és annak biztosítására, hogy ne létezzen olyan biztonsági rés, amelyet korábban nem fedeztek fel. [63]

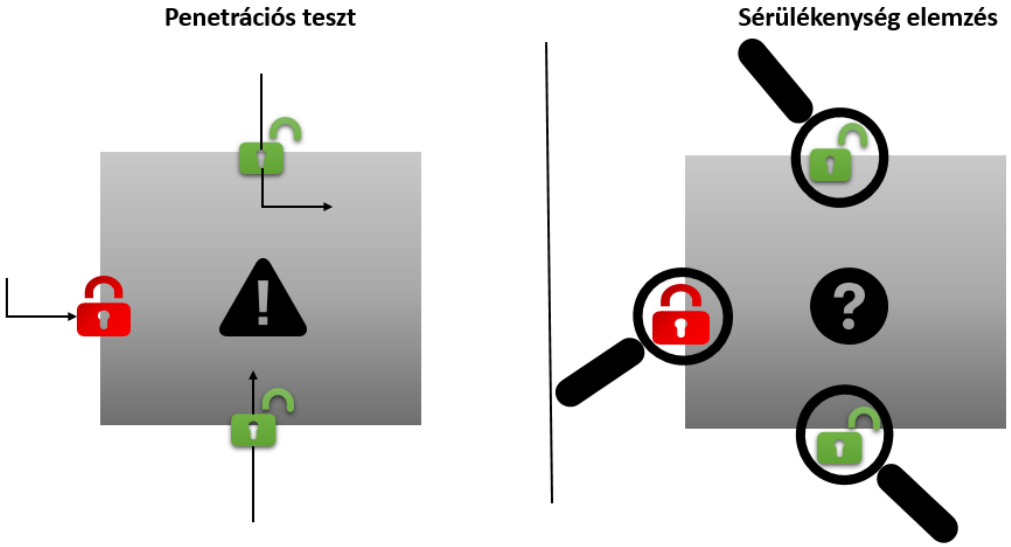
2.1.2 Sérülékenységelemzés

A sérülékenységelemzés automatizált eszközök használata a rendszer jól ismert biztonsági réseinek azonosítására. A biztonsági rés kiértékelő eszközei megvizsgálják az információs rendszereket annak meghatározása érdekében, hogy a biztonsági beállítások be vannak-e kapcsolva és alkalmazhatók-e, valamint, hogy a megfelelő biztonsági javításokat alkalmazták-e. A sérülékenységelemzést általában a minimális biztonsági szint érvényesítésére használják, és gyakran egy speciálisabb penetrációs teszt előfutára. Nem kategorizálja és azonosítja a lehetséges felhasználható támadásokat annak valódi újbóli beindításához, és nem veszi figyelembe a rendszer alapú felügyeleti folyamatok és eljárások általános biztonságát. A

sérülékenységelemzés hálózati eszközök, operációs rendszerek és alkalmazások vizsgálatának folyamata az ismert és ismeretlen sérülékenységek azonosítása céljából. A biztonsági rés hiányosság, hiba vagy gyengeség a rendszer tervezésében, használatában és védelmében. A sérülékenységelemzés kihasználása jogosulatlan hozzáférést, előjogot, szolgáltatás megtagadását vagy egyéb kimenetelt eredményezhet, amely tevékenységeket a sérülékenységelemzés már nem képes végrehajtani.

2.1.3 Penetrációs teszt és sérülékenységelemzés

A sérülékenységelemzés és a penetrációs tesztelés közötti fő különbség az, hogy a penetrációs tesztek meghaladják a sérülékenység-azonosítási szintet, amely kiaknázási folyamathoz, a jogosultságok növekedéséhez és a célrendszerekhez való hozzáférés fenntartásához vezet. Másrészt a sebezhetőség vizsgálat átfogó képet nyújt a rendszerhibákról anélkül, hogy figyelembe venné ezeknek a hibáknak a tesztelt rendszerre gyakorolt hatását. A másik két jelentős különbség a két kifejezés között az, hogy a penetrációs teszt sokkal durvább módszereket használ, mint a sebezhetőség felmérése, illetve az összes technikai módszert agresszív módon használja az informatikai környezet előnyeinek kihasználásához. A sebezhetőség kiértékelési folyamata azonban nem invazív módon, hanem gondosan azonosítja és számszerűsíti az összes ismert sebezhetőséget.



1. ábra *Különbség a penetrációs teszt és sérülékenységelemzés között (saját szerkesztés)*

Ahogy az 1. ábrán is bemutattam, a sérülékenységelemzés szkennelésével egyéni sebezhetőségek találhatók, a penetrációs tesztelés azonban aktívan felderíti és megpróbálja ellenőrizni, hogy ezeket a sebezhetőségeket ki lehet-e használni a célkörnyezetben. A behatolási tesztek a biztonsági értékelések területén egy lépéssel meghaladják a sebezhetőségi

teszteket. A sebezhetőségi tesztelés egy folyamat, amely megvizsgálja az egyes számítógépek, hálózati eszközök vagy alkalmazások biztonságát, a penetrációs teszt kiértékeli a teljes hálózat biztonsági modelljét. A behatolási tesztelés feltárja az informatikai vezetők, a biztonsági vezetők, a hálózati- és rendszer-adminisztrátorok számára a hálózat valódi támadásának lehetséges következményeit. A behatolási tesztek kiemelik azokat a jellemző biztonsági hiányosságokat, amelyeket kihagytak a sebezhetőségi teszt során. A penetrációs teszt rámutat a sérülékenységekre, és dokumentál minden olyan eredményt, amely segítségével ezeket a gyengeségeket ki lehet használni. Ez azt is mutatja, hogy a támadó számos kisebb sebezhetőséget képes kihasználni, amelyek veszélyeztetik a végberendezéseket vagy a hálózatot. A behatolási tesztek rávilágítanak a szervezeti biztonsági modellezés hiányára, és segítik a szervezeteket az egyensúly megteremtésében a műszaki teljesítmény és az alaprendeltetésű funkciók között a lehetséges biztonsági sérülékenységek esetén. [63]

A legtöbb sebezhetőséget csak a szoftverek és konfigurációk nézőpontjából értékelik, a többi lehetséges típusú biztonsági kérdéskör nem kerül további elemzésre. Például az emberi tényezők és folyamatok is lehetnek a sebezhetőségek fontos forrásai. A penetrációs teszt egy etikus támadásszimuláció, amelynek célja a biztonsági ellenőrzések hatékonyságának bizonyítása vagy érvényesítése egy adott környezetben a valódi kockázatot jelentő, kihasználható biztonsági rések által. Egy manuális tesztelési folyamat köré épül, amelynek célja az általános válaszok, a hamis pozitív eredmények és a hiányos automatizált alkalmazásminősítések (például a sebezhetőség felmérése során használt eszközök) figyelem kívül hagyása, így a lényegi és értékes eredmények begyűjtése. [61]

Mindent összevetve kijelenthető, hogy a penetrációs teszt, meghaladja a sérülékenységelemzés azonosítási képességét, amely kiaknázási folyamathoz, a jogosultságok növekedéséhez és a célrendszerekhez való hozzáférés fenntartásához vezet. A kiberbiztonsági penetrációs teszt az informatikai rendszerek alapos tanulmányozását biztosítja.

2.2 A PENETRÁCIÓS TESZT FŐ PARAMÉTEREI

2.2.1 Célok

A célok világos meghatározása elengedhetetlen. Ha a célokat nem lehet elérni, vagy azok nem érhetők el hatékonyan, a tesztelőnek az előkészítő szakaszban tájékoztatnia kell a tesztelt szervezetet, és alternatív eljárásokat kell javasolnia. Az informatikai rendszerek penetráció tesztjének ezért nem csupán a létező sebezhetőségek felsorolásának kell lennie,

hanem ideális esetben konkrét megoldásokat és javaslatokat is tartalmaznia kell. Egy szervezet a következő célok elérése érdekében hajt végre behatolástesztet:

- a műszaki rendszerek biztonságának javítása;
- sebezhetőségek azonosítása;
- az informatikai biztonság megerősítése;
- a szervezeti és a személyi infrastruktúra biztonságának javítása;
- a biztonsági és ellenőrzési hatékonyság megvizsgálása és megerősítése;
- hasznos információk szolgáltatása az ellenőrző csoportok számára, amelyek adatokat gyűjtenek a jogszabályok betartásával összhangban;
- a biztonsági ellenőrzések költségeinek minimalizálása az alaprendeltetésű képességek átfogó, részletes és reális bizonyítékainak bemutatásával;
- a vonatkozó javítások relevanciájának jelentett vagy az ismert biztonsági résekkel szembeni növelése;
- a szervezet hálózatai és rendszerei jelenlegi kockázatainak feltárása;
- a hálózati biztonsági eszközök, például tűzfalak hatékonyságának értékelése;
- átfogó megközelítés kidolgozása a jövőbeli technikai behatolások megelőzésére;
- annak kiderítése, hogy van-e szükség meglévő szoftver, hardver, hálózati infrastruktúra módosítására vagy frissítésére.

A legtöbb penetrációs tesztet a műszaki rendszerek biztonságának javítása érdekében rendelik meg. A tesztek olyan műszaki rendszerekre korlátozódnak, mint a tűzfalak, routerek, szerverek. A szervezeti és a személyi infrastruktúrát általában nem vizsgálják külön. Fontos megjegyezni, hogy a penetrációs teszt csak egy bizonyos időpontban tükrözi a helyzetet, ezért nem adhat nyilatkozatot a jövőbeli biztonsági szintről. [64]

2.2.2 A jó teszt tulajdonságai

A következő tevékenységek biztosítják a jó penetrációt:

- a penetrációs teszt paraméterek, például célok, korlátozások és az eljárások indoklásának meghatározása;
- magasan képzett és tapasztalt szakemberek toborzása;
- jogi kontaktszemély kijelölése, aki betartja és betartatja a felmondási megállapodás szabályait;

- jól megtervezett módszertan, annak követése olyan dokumentációval, amely gondosan rögzíti az eredményeket, és érthetővé teszi azokat az ügyfél számára;
- a penetrációs tesztelőnek rendelkezésre kell állnia, hogy szükség esetén bármilyen kérdést megválaszoljon;
- zárójelentés, amely egyértelműen leírja a megállapításokat és az ajánlásokat.

2.2.3 Korlátok

A penetrációs teszt futtatása segít megvizsgálni néhány informatikai, kiberbiztonsági intézkedést, és hozzájárul ezek fejlesztéséhez, de vannak korlátok. Például egy penetrációs teszt:

- csak a célzott alkalmazást, infrastruktúrát vagy a kiválasztott környezetet fedi le;
- a műszaki infrastruktúra felfedezésére összpontosít;
- a humán erőforrás átvilágításának csak egy kis részét fedi le;
- csak egy pillanatkép a rendszerről egy adott időben;
- jogi vagy kereskedelmi megfontolások alapján a teszt szélessége vagy mélysége korlátozható;
- az összes biztonsági hiányosságot nem fedezheti fel, például a korlátozott hatály vagy a nem megfelelő tesztelés miatt;
- olyan eredményeket nyújt, amelyek gyakran technikai jellegűek, és alaprendeltetésű feladatok kontextusában értelmezendők;

2.2.4 Kihívások

A szervezetek általában a következő nehézségekkel szembesülnek:

- a teszt lefedésének, mélységének és szélességének meghatározása;
- a szükséges penetrációs teszt típusának meghatározása;
- a penetrációs teszt és a sérülékenységelemzés közti különbség megértése;
- a lehetséges rendszerhibákkal és az érzékeny adatok nyilvánosságra hozatalával kapcsolatos kockázatok azonosítása;
- a célok és a tesztek gyakorisága;
- a penetrációs teszt során felfedezett sebezhetőségek javítása érdekében annak bizonyítása, hogy a rendszer valóban "biztonságos". [61]

Összegezve leszögezhető, hogy a penetrációs teszt paraméterei elősegítik a teszt megtervezését, felhívják a figyelmet a sarkalatos pontokra, mint korlátok és kihívások. Ebből

az a **következtetést vonom le**, hogy a penetrációs teszt paramétereinek ismerete nélkül nem érdemes megtervezni a tesztet, illetve ennek hiánya jelentősen megnehezíti a kezdeti lépéseket.

2.3 NEMZETKÖZI SZABVÁNYOK

Ebben az alfejezetben bemutatásra és összehasonlításra kerülnek a penetrációs tesztek kiválasztott módszerei. Először ismertetem hátterüket és konkrét céljaikat, másodsorban pedig áttekintést adok a fázisokról és a speciális jellemzőkről.

2.3.1 Cyber Kill Chain

A Cyber Kill Chain olyan lépések sorozata, amelyek nyomon követik a kibertámadás szakaszait a korai felderítési szakasztól az adatok kiszűréséig. A Kill Chain segít megérteni és leküzdeni a zsarolóvírusokat, a biztonsági réseket és a fejlett tartós támadásokat.

2. ábra *Cyber Kill Chain Forrás: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Letöltés időpontja: 2021.11.29.)*

A Lockheed Martin egy katonai modellből származtatta a Kill Chain keretrendszerét, amelyet eredetileg a cél azonosítására, a támadásra való felkészülésre, a harcra és a megsemmisítésére hoztak létre. Megjelenése óta a Kill Chain úgy fejlődött, hogy jobban előre jelezze és felismerje a bennfentes fenyegetéseket, a társadalmi manipulációt, a fejlett ransomware-eket és az innovatív támadásokat. A modellt a következő hét lépés határozza meg:

- Felderítés: A támadó meghatározza célpontját, a lehető legtöbb információt kapja meg tőle, és megpróbálja megtalálni a célinfrastruktúra sebezhetőségét.
- Fegyverzet: A támadó kiberfegyvert hoz létre, amely lehetővé teszi a célinfrastruktúra távoli elérését. Ez általában egy rosszindulatú program, például egy vírus vagy féreg, amely egy vagy több azonosított biztonsági rést kihasznál.
- Szállítás: A támadó fegyvert szállít az áldozatnak. Továbbítható e-mail mellékleteken, webhelyeken vagy USB-meghajtón keresztül.
- Kizsákmányolás: A kiberfegyver életbe lép, és kihasználja a célhálózat sebezhető pontjait.
- Telepítés: A kiberfegyver távoli kapcsolatot nyit meg, általában hátsó ajtót, és lehetővé teszi a támadó számára a célinfrastruktúra elérését.
- Parancs és irányítás: a már megnyitott hozzáférésen keresztül a kiberfegyver lehetővé teszi a támadó számára, hogy továbbra is jelen legyen az áldozat infrastruktúrájában.
- Célkitűzések: mivel a támadónak célja van, megteszi a szükséges lépéseket feléjük, például adatszűrést, adatok megsemmisítését vagy váltságdíj titkosítását. [65]

2.3.2 NIST[28]

A NIST kiberbiztonsági keretrendszer keretet biztosít a számítógépes biztonsági útmutatásoknak arról, hogy az Egyesült Államok magánszektorbeli szervezetei hogyan tudják felmérni és javítani a kibertámadások megelőzésének, felderítésének és az azokra való reagálásnak a képességét. A NIST SP 800-115 címe: „Technikai útmutató az információbiztonsági teszteléshez és értékeléshez”, amelyet 2008-ban az Egyesült Államok Kereskedelmi Minisztériumának része, a Nemzeti Szabványügyi és Technológiai Intézet dolgozott ki, és tett közzé. Az útmutató az információbiztonsági értékelést úgy határozza meg, mint azt a folyamatot, amely meghatározza, hogy az értékelt entitás (például. számítógép, rendszer, hálózat, eljárás, személy - az úgynevezett értékelési objektum) mennyire hatékonyan

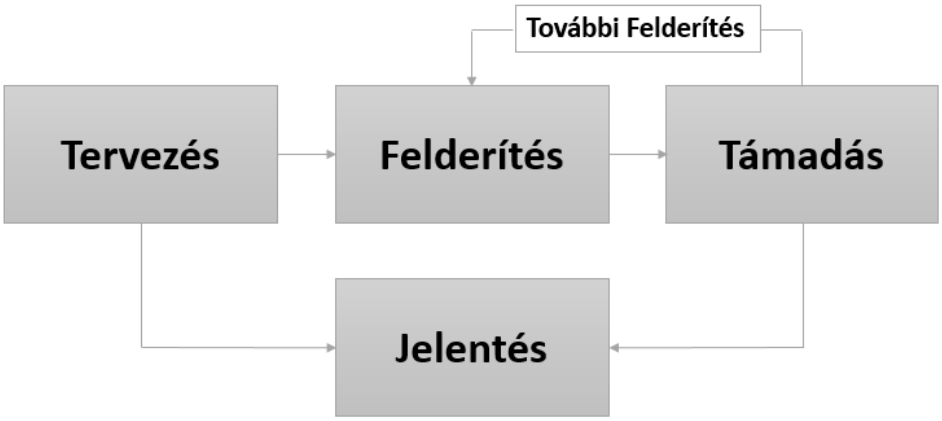
[28] National Institute of Standards and Technology - Nemzeti Szabványügyi és Techológiai Intézet

teljesíti a meghatározott biztonsági célokat. Az útmutató háromféle értékelési módszert ír le: tesztelés, vizsga és interjú.

Három lehetséges módja van ennek a célnak:

- Tesztelésen keresztül, az értékelési objektumok gyakorlása révén, összehasonlítva a tényleges és a várható viselkedésformákat;
- Vizsgálaton keresztül, elemezve az értékelési objektumokat és megérteni működésüket;
- Interjúkészítéssel, széles körű megbeszéléseket folytatva a szervezetekkel és szakértőkkel a lehetséges problémák azonosításáról.

Az útmutató szakaszos információbiztonsági értékelési módszert ajánl, amelynek legalább a következő fázisokat kell tartalmaznia: „tervezés", „végrehajtás" és „utóvégrehajtás". A NIST SP 800-115 számos elfogadott módszert ír le erre a célra. A NIST SP 800-115 szerepét úgy írják le, hogy ez a kiadvány olyan műszaki tesztelési és vizsgálati technikákra vonatkozó ajánlásokat kínál, amelyek számos értékelési módszerhez használhatók, és számos értékelési célra felhasználhatók. Tehát a NIST SP 800-115 követése nem jelenti azt, hogy nem lehet más módszert követni.



3. ábra *NIST folyamat (saját szerkesztés)*

A tesztelési szempontok ismertetése után az útmutató leírja a (passzív) áttekintési technikákat, beleértve a hálózati sniffing módszert is. Az útmutató 4. fejezete a technikai célpont-azonosítási- és elemzési technikákkal foglalkozik, amelyek az aktív eszközök és a hozzájuk kapcsolódó portok és szolgáltatások azonosítására, valamint a lehetséges sebezhetőségek elemzésére összpontosítanak. Az útmutató a hálózatfelderítési technikákra, a hálózati port- és szolgáltatásazonosításra, a sebezhetőség-vizsgálatra és a vezeték nélküli vizsgálatra összpontosít. Az útmutató 5.2. fejezete kifejezetten a behatolási tesztelésre összpontosít, amelynek meghatározása szerint a biztonsági tesztelés során valós támadásokat utánoznak, hogy azonosítsák az alkalmazás, a rendszer vagy a hálózat biztonsági jellemzőinek

megkerülésére szolgáló módszereket. Az útmutató a penetrációs tesztelés négy fázisát mutatja be, nevezetesen a tervezést, felfedezést, támadást, jelentést.

A tervezési szakaszban meghatározzák a szabályokat, véglegesítik és dokumentálják a vezetői jóváhagyást, és meghatározzák a tesztelési célokat. A felfedezési szakasz két részből áll, az első rész a tényleges tesztelés kezdete, és az információgyűjtést és a szkennelést foglalja magában. A második rész sebezhetőség-elemzést tartalmaz, amely magában foglalja a vizsgált számítógépek szolgáltatásainak, alkalmazásainak és operációs rendszereinek összehasonlítását a sebezhetőségi adatbázisokkal és a tesztelők saját sebezhetőségi tudásával. A harmadik fázis a támadás végrehajtása, ami minden penetrációs teszt középpontjában áll. Az útmutató négy lépést ír le, amelyekből létezik a „támadás fázis, nevezetesen: hozzáférés megszerzése, jogosultságok kiterjesztése, rendszerböngészés és további eszközök telepítése. Az utolsó, jelentési fázis a penetrációs teszt másik három fázisával egyidejűleg történik. Ennek a szakasznak a végén általában egy jelentést készítenek, amely leírja az azonosított sebezhetőségeket, bemutatja a kockázati besorolást, és útmutatást ad a felfedezett gyengeségek enyhítésére. [66]

2.3.3 OSSTMM[29]

A nyílt forráskódú biztonsági tesztelési módszertan kézikönyve (továbbiakban OSSTMM) a biztonsági tesztek nyílt szabványmódszere. Az OSSTMM-et Pete Herzog és Marta Barcelo hozta létre, és a Spanyolországban és az Egyesült Államokban működő ISECOM[30] fejlesztette ki. Az egyik nyilvánosan elérhető penetrációs tesztelési módszer. A kézikönyv 213 oldalból áll, és 14 fő fejezetre oszlik.

Barcelo és Herzog azzal kezdi, hogy kijelenti, hogy szükség van egy ellenőrizhető eredményre, mondván: amikor a biztonsági teszt művészet, akkor az eredmény ellenőrizhetetlen, és ez aláássa a teszt értékét. Az egyik módja annak, hogy biztosítsuk a biztonsági teszt értékét, ha tudjuk, hogy a tesztet megfelelően végezték-e el. Ehhez formális módszertant kell használni. Az OSSTMM célja, hogy az legyen. Az OSSTMM auditot úgy írják le, mint a biztonság pontos mérését olyan működési szinten, amely mentes a feltételezésektől, konzisztens és megismételhető. Elsődleges célja, hogy tudományos módszertant nyújtson a működési biztonság pontos jellemzésére a teszteredmények következetes és megbízható módon történő vizsgálata és korrelációja révén. Ezen az elsődleges célon túlmenően meghatároznak

[29] Open Source Security Testing Methodology Manual - Nyílt forráskódú biztonsági tesztelési módszertan kézikönyve
[30] Institute for Security and Open Methodologies - Biztonsági és Nyílt Módszertani Intézet

egy másodlagos célt is, amely iránymutatások biztosítása, amelyek helyes betartása esetén lehetővé teszik a tesztelő számára, hogy hitelesített OSSTMM auditot végezzen. Az első fejezetben az OSSTMM mögött meghúzódó gondolatot ismertetik, és meghatározzák a fontos kifejezéseket. Az OSSTMM a működési biztonságról szól. A szerzők a következő fő gondolatmenetet vallják az elválasztás és a vezérlés kombinációja. Kifejtik, hogy ahhoz, hogy egy fenyegetés hatékony legyen, közvetlenül vagy közvetve kölcsönhatásba kell lépnie az eszközzel. A fenyegetés és az eszköz elkülönítése annyi, mint az esetleges interakció elkerülése. A működési biztonság összefüggésében biztonságnak nevezzük az eszköz és a fenyegetés szétválasztását. Az elválasztás mértékét „porozitásként" jellemezzük. Minél nagyobb a porozitás, annál kisebb a távolság az eszköz és a fenyegetés között.

Az OSSTMM hét lépést ír le, amelyeket követni kell egy megfelelően meghatározott biztonsági teszt elvégzéséhez. Az első lépésben meg kell határozni, hogy mely eszközöket kell védeni. A megfelelő eszközök azonosítása fontos, mivel ennek következtében lehet azonosítani és kiválasztani azokat a vezérlőket, felügyeleteket, amelyeket a behatolási teszt során tesztelni fognak. A második lépésben meg kell határozni a „foglalkozási zónát", amely az eszközök körüli terület, amely magában foglalja a védelmi mechanizmusokat és az eszközök köré épített folyamatokat vagy szolgáltatásokat. A harmadik lépésben meg kell határozni a hatókört. Ebbe beletartozik minden az elköteleződési zónán kívül, amire szüksége van ahhoz, hogy eszközei működőképesek legyenek. Ez magában foglalhat olyan dolgokat is, amelyeket nem tudunk közvetlenül befolyásolni. Például információkat, jogszabályokat, rendeleteket és kollégákat. A negyedik lépés magában foglalja a hatókörön belüli és kívüli entitásokkal való interakciók meghatározását. Az interakciókat „vektoroknak" nevezik, és lehetnek olyan kölcsönhatások, mint az egyik osztálytól egy másik részlegig. Az ötödik lépés annak meghatározása, hogy mely korábban leírt csatornákon keresztül kell tesztelni, és milyen berendezésekre lesz szükség az egyes tesztekhez. A hatodik lépésben meg kell határozni, hogy milyen típusú tesztet kell végrehajtani. Az utolsó lépés annak biztosítása, hogy a teszt megfelel-e az OSSTMM-ben bemutatott Elköteleződési Szabályzatnak. Ezek a szabályok 42 iránymutatást tartalmaznak, amelyek meghatározzák az elfogadható gyakorlatok működési irányelveit, a tesztelés marketingjét a tesztelési munka elvégzése és a tesztelési megbízás eredményeinek kezelése terén.

A teszt eredményeinek jelentésére az OSSTMM a STAR-t (Security Test Audit Report) írja le, amelynek célja, hogy a precíz számítás összefoglalójaként szolgáljon, amely tartalmazza az adott területen tesztelt célpontok támadási felületét. [67]

2.3.4 OWASP[31]

Az OWASP világszerte ingyenes és nyílt közösség, amely az alkalmazásszoftverek biztonságának javítására összpontosít.

Küldetését úgy írja le, hogy láthatóvá tegye az alkalmazások biztonságát, hogy az emberek és a szervezetek megalapozott döntéseket hozhassanak az alkalmazások biztonsági kockázatairól. Az OWASP számos projektet tartalmaz, beleértve az OWASP Alkalmazásbiztonsági Ellenőrzési Standard Projektet, az OWASP Top 10 -et és az OWASP Zed Attack Proxy -t (ZAP). Ezt az útmutatót szabványos de facto útmutatóként írják le a webalkalmazások behatolásának teszteléséhez, és célja, hogy segítsen az embereknek megérteni, hogy mit, miért, mikor, hol és hogyan tesztelnek.

A bevezető után az útmutató második fejezete leírja, hogy mi a tesztelés, mikor és mit kell tesztelni, valamint néhány alapvető tesztelési elvet. Ezen kívül néhány tesztelési technikát, köztük előnyeiket és hátrányaikat is elmagyarázzák, mint például a kézi ellenőrzések és felülvizsgálatok, a fenyegetésmodellezés, a forráskód-felülvizsgálat és a penetrációs teszt.

A 4. fejezetben a Webalkalmazás-penetrációs tesztelési módszertan leírása található. A webalkalmazás-biztonsági tesztet úgy határozza meg, mint egy számítógépes rendszer vagy hálózat biztonságának értékelésére szolgáló módszert az alkalmazásbiztonsági ellenőrzések módszeres érvényesítésével és hatékonyságának ellenőrzésével. A módszertan célja, hogy összegyűjtse az összes lehetséges tesztelési technikát, elmagyarázza ezeket a technikákat, és naprakészen tartsa az útmutatót. A leírt teszt 2 fázisra oszlik, egy passzív módra és egy aktív módra. Passzív módban a tesztelő megpróbálja megérteni az alkalmazás logikáját, és játszik az alkalmazással.

Az aktív mód egy sor aktív tesztből áll, amelyek 11 alkategóriára vannak felosztva, összesen 91 kontrollhoz. Ez a tizenegy alkategória a következőket tartalmazza: információgyűjtés, konfiguráció- és telepítéskezelési tesztelés, identitáskezelési tesztelés, hitelesítési tesztelés, engedélyezési tesztelés, munkamenet-kezelési tesztelés, bemenet-ellenőrzés tesztelése, hibakezelés, kriptográfia, üzleti logikai tesztelés és ügyféloldali tesztelés. Az útmutató fennmaradó fejezeteinek többsége részletes műszaki útmutatást ad a 11 alkategórián belüli tesztek végrehajtására vonatkozóan. Az utolsó fejezet, az 5. fejezet leírja, hogy hogyan kell egy tesztet jelenteni. Az OWASP leírja, hogy a jelentésnek három fő részből kell állnia, egy összefoglalónak, a tesztparamétereknek és a megállapításoknak. A vezetői összefoglaló összefoglalja az értékelés általános megállapításait, és magas szintű képet ad az

[31] Open Web Application Security Project – Nyílt webalkalmazásbiztonsági projekt

üzleti vezetőknek és a rendszertulajdonosoknak a felfedezett sebezhetőségekről. A második szakasz a tesztparamétereket tartalmazza, amelyek a következő címsorokat tartalmazhatják: a projekt célja, a projekt hatóköre, a projekt ütemezése, célok. Az utolsó rész műszaki információkat tartalmaz a talált sebezhetőségekről és a megoldásukhoz szükséges lépésekről. [68]

2.3.5 PTES[32]

A PTES fejlesztését 2009 elején egy körülbelül hat fős csoport kezdte meg, és jelenleg egy körülbelül 20 vezető információbiztonsági szakemberből álló csoport fejleszti, elsősorban az Egyesült Államokban. A szabványt úgy írják le, mint új szabványt, amelynek célja, hogy mind a vállalkozások, mind a biztonsági szolgáltatók számára közös nyelvet és teret biztosítson a penetrációs tesztek elvégzéséhez. A PTES célközönsége két fő közösséget tartalmaz: a szolgáltatást igénylő vállalkozásokat és a szolgáltatókat. A vállalkozások számára az a cél, hogy lehetővé tegyék számukra, hogy a pentest keretében meghatározott alapszintű munkát követeljenek meg. A szolgáltatók számára az a cél, hogy kiindulópontot biztosítsanak a szükséges tevékenységekhez, és tudják mit kell figyelembe venni a jelentéskészítésen és a teljesítésen átnyúló korlátozásoktól számított pentest részeként. A PTES hét szakaszból és egy további útmutatóból áll, amely műszaki iránymutatásokat tartalmaz. A hét szakasz a következőket tartalmazza: Az elkötelezettség előtti interakciók, a felderítés és adatösszegyűjtés, a fenyegetésmodellezés, a sebezhetőségi elemzés, a kizsákmányolás, a kizsákmányolás után, a jelentések.

Az elköteleződés előtti interakciók szakasz célja az elérhető eszközök és technikák bemutatása és magyarázata, amelyek elősegítik a behatolási teszt sikeres elköteleződést megelőző lépését. Ebben a részben 19 különböző témát ismertettem beleértve a behatolási teszt hatókörét, milyen kérdéseket kell feltenni, hogyan kell bánni harmadik felekkel, hogyan határozzuk meg a fizetési feltételeket, hogyan határozzuk meg a célokat, hogyan alakítsuk ki a kommunikációs vonalakat, és hogy hogyan teszteljék az elköteleződés meghatározott szabályai szerint.

A következő szakasz meghatározza a behatolási teszt információgyűjtés tevékenységeit. Ennek a dokumentumnak az a célja, hogy egy olyan szabványt nyújtson, amelyet kifejezetten a célpont (jellemzően vállalati, katonai vagy kapcsolódó) ellen felderítést végző pentester számára terveztek. A dokumentum részletezi a gondolkodás folyamatát és célját.

[32] Penetration Testing Execution Standard - Penetrációs tesztelés végrehajtási szabvány

A fenyegetés modellezése szakasz meghatározza a fenyegetésmodellezési megközelítést, amely szükséges a behatolási teszt helyes végrehajtásához. Ezek a szakaszok információkat tartalmaznak arról, hogy hogyan kell elvégezni egy üzleti vagyonelemzést, egy üzleti folyamatelemzést, egy közösség elemzését, egy fenyegetettségi képesség elemzést, hogyan modellezhetjük a közösségek motivációját, és végül hogyan találhatunk releváns híreket a hasonló szervezetekről.

A sebezhetőség-elemzés rész a rendszerek és alkalmazások azon hibái feltárásának folyamatára összpontosít, amelyeket a támadó kihasználhat. Ez a rész tartalmazza az aktív tesztelési technikák, a passzív tesztelési technikák, a validációs technikák leírását, valamint azt, hogy milyen kutatásokat kell végezni a sebezhetőségek keresése és validálása során. A kihasználás szakasz leírja, hogy a penetrációs teszt kiaknázási szakasza kizárólag a rendszerhez vagy erőforráshoz való hozzáférés megteremtésére összpontosít a biztonsági korlátozások megkerülésével. Ez a rész információkat tartalmaz az ellenintézkedések elkerüléséről, a tipikus megközelítések leírásáról, a testre szabott kihasználások használatára vonatkozó információkról.

A következő szakasz, a kihasználás utáni rész célja a kompromittált gép értékének meghatározása és a gép feletti irányítás fenntartása a későbbi használatra. Ez az érték elsősorban a rajta tárolt adatok érzékenységén és a gépek hasznosságán alapul a hálózat további veszélyeztetésében. Ez a rész információkat tartalmaz arról, hogy hogyan lehet megvédeni az ügyfeleket és a szolgáltatókat, hogyan lehet elemezni az infrastruktúrát egy feltört gépen, hogyan lehet érzékeny információkat szerezni a feltört gépekről, hogyan lehet azonosítani a nagy értékű célpontokat, hogyan lehet kiszűrni az adatokat, hogyan lehet tartósan jelen lenni a feltört gépeken.

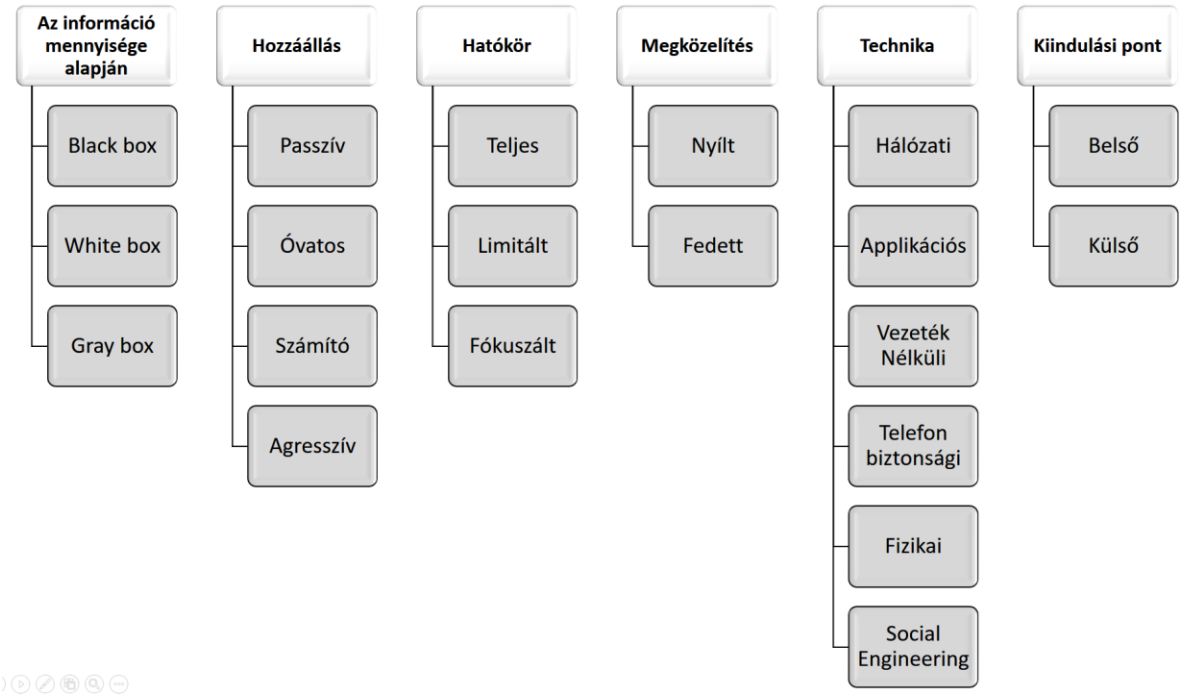
Az utolsó rész a jelentéstételre összpontosít, és meg kívánja határozni a penetrációs tesztek jelentésének alapkritériumait. Ebben a részben a jelentés felépítésére vonatkozó információk találhatók, beleértve a vezetői összefoglalót és a technikai jelentést. A PTES-hez csatolt műszaki irányelvek segítenek meghatározni bizonyos eljárásokat, amelyeket a behatolási teszt során követni kell. [69]

Összességében levontam a következtetést, miszerint a módszertanok a célok és a gyakorlati értékelési irányelveinek szemszögeiből nézve más megközelítést alkalmaznak a penetrációs teszt vagy biztonsági teszt elvégzésére. Valamint egyik alapvető módszertannál sem jelentős tényező az infokommunikációs rendszereknek a katonai felhasználásának figyelemebe vétele.

2.4 KIBERMŰVELETI PENETRÁCIÓS TESZTEK OSZTÁLYOZÁSA

Az információs forradalom és a digitalizáció megjelenése eredményeként az infokommunikációs rendszerek és eszközök jelentős kihívásokkal néznek szembe. Egyértelmű, hogy ezeknek a rendszereknek a biztonság alapvető követelménye. A biztonságot az ellenőrzések, a kockázatkezelés, a tesztek és sok más módszer biztosíthatják. Az infokommunikációs rendszerek védelmének e fontos vizsgálati módszereinek egyike a penetrációs teszt. Az ilyen komplex elemzés megvizsgálja a támadó perspektíváját, követi a támadó lépéseket, felfedezi és kihasználja a sebezhetőségeket. A behatolási tesztelés számos manuális és automatizált technikát használ a szervezet biztonsági információs rendszere támadásának szimulálására. A behatolási tesztelés kihasználja az ismert sebezhetőségeket, de tesztelési szakértelemre is szükség van a szervezet biztonsági rendszerei konkrét gyengeségeinek és ismeretlen sérülékenységeinek azonosításához.

Fontos kérdések merülnek fel a behatolási tesztelések vonatkozásában, mégpedig, hogy milyen kritériumok alapján írható le egy penetrációs teszt, vagy mi különbözteti meg az egyik penetrációt a másiktól. A 4. ábrán kutatásaim alapján összefoglaltam, hogy a megkülönböztető jellemzők között szerepel például a vizsgált rendszerek mérete, szerkezete, a tesztek elővigyázatossági vagy agresszív jellege. Azokat a jellemzőket, amelyek egy adott penetrációs tesztre vonatkoznak, a teszt céljához kell igazítani annak érdekében, hogy hatékony és eredményes vizsgálatot lehessen végezni. Meg kell jegyezni, hogy nem minden lehetséges kombináció eredményez hasznos tesztet, még akkor sem, ha az osztályozási kritériumokat a lehető legszélesebb módon tartják fenn. A besorolás számos szemponton alapulhat, azonban számos szakértő ugyanazon kritériumok alapján osztályozza a penetrációs tesztek típusait. [70]



4. ábra *A penetrációs teszt lehetséges osztályozása (saját szerkesztés)*

2.4.1 Az információ mennyisége alapján történő osztályozás

A 4. számú ábrán látható, hogy a penetrációs teszteket hat szempont alapján osztályoztam, melyek közül az első a rendelkezésre álló információk alapján különíti el a különböző tesztelési módszereket. A valódi támadások szimulálására és a hamis eredmények minimalizálására a penetrációs tesztelők fekete-doboz tesztelést (black-box testing) alkalmaznak (vagy nullaszintű tudásvizsgálatot [zero knowledge testing], ha nincs információ vagy segítség az ügyfél oldaláról), és diszkréten feltérképezik a hálózatot, miközben felsorolják a szolgáltatásokat, a megosztott fájlrendszereket, és az operációs rendszereket. Ezen kívül a penetrációs tesztelő elősegítheti a rendelkezésre álló kiszolgáltatott hozzáférési pontok felismerését, feltéve, hogy ezek a tevékenységek a projekt hatálya alá tartoznak. A fekete dobozos tesztelés során a tesztelők nem rendelkeznek előzetes ismeretekkel a vizsgált infrastruktúráról, és nem ismerik a rendszer belső működését. Ezt a tesztet csak a szervezet alapos kutatása után hajtják végre. A fekete doboz teszt reálisan szimulálja a tipikus internetes hackerek támadását. A tesztelő megtámadja a célt anélkül, hogy ismerné a védekezést, az erősségeket vagy a kommunikációs csatornákat. A vizsgált szervezetet nem értesítik az ellenőrzés, a tesztelt csatornák vagy a tesztvektorok hatóköréről. Az ellenőrzés az elemző készségeket és a cél ismeretlen változókra való felkészültségét vizsgálja a teszt során. A teszt mérete és mélysége csak olyan lehet, mint a tesztelő tudása és hatékonysága. Meg kell vizsgálnia a nyilvánosan elérhető adatbázisokban tárolt információkat. Ez a teszt a valódi

támadó folyamatokat szimulálja. A fekete doboz tesztelése időigényes és költséges, illetve funkcionális tesztként is ismert.

Amennyiben a szervezetnek ki kell értékelnie biztonságát, egy adott támadás vagy egy cél elérése érdekében a fehér dobozos tesztelést (white box testing) alkalmazzák. Ez a teszt teljes információt nyújthat a szervezet hálózatáról a penetrációs tesztelőnek. A nyújtott információ tartalmazhat hálózati topológiai dokumentumokat, eszközleltárt és értékelési információkat. Általában egy szervezet ezt választja, amikor a biztonság teljes ellenőrzése a cél. Fontos megjegyezni, hogy mindazonáltal az információbiztonsági folyamat és a penetrációs teszt pillanatképet ad a szervezet akkori biztonsági helyzetéről. A fehér doboz tesztelést teljes tudástesztelésnek (full skill testing) is nevezik. A tesztelő számos különféle információval rendelkezik a teszttel kapcsolatban, mielőtt a white box tesztet elvégeznék.

A sebezhetőség tesztelésének leggyakoribb módszere a szürke doboz penetrációs tesztelés (gray box testing). Ez a tesztelési folyamat úgy működik, mint egy fekete doboz teszt. Mind a tesztelő, mind a normál felhasználó ugyanazokkal a jogosultságokkal rendelkezik. A tesztek célja egy rosszindulatú bennfentes támadás szimulálása. A szürke doboz penetrációs teszt magában foglalja a biztonsági értékelést és a belső tesztet; a teszt folyamat megvizsgálja a bennfentesek hozzáférését a szervezet hálózatához. Itt a tesztelőnek általában korlátozott információ áll rendelkezésre. [64] [71]

2.4.2 A hozzáállás szerinti osztályzás

A vizsgálat céljából következő módszerek és eljárások vonatkozásában négy agresszivitási szintet azonosíthatunk:

- A legalacsonyabb szinten - **passzív** - a tesztobjektumokat csak passzív módon tesztelik, azaz a feltárt sebezhetőségeket nem használják ki.
- A második szint azonosított sebezhetőségei - **óvatosak** - csak akkor használja ki a sebezhetőségeket, ha a tesztelt rendszer nem befolyásolja.
- A következő szinten - **számító** - a tesztelő megpróbálja kihasználni a biztonsági réseket is, amelyek rendszerhibákhoz vezethetnek. Ez magában foglalja például a jelszavak automatikus tesztelését és az ismert puffer túlcsordulások felhasználását a célrendszerekben. Mielőtt ezt megtenné, a tesztelő megvizsgálja, mennyire valószínű a támadások sikere, és milyen súlyos következményekkel járhatnak.
- A legmagasabb szinten - **agresszív** - a tesztelő megpróbálja kihasználni az összes lehetséges sebezhetőséget, például pufferek használata azonosítatlan célrendszereken,

vagy szándékos DoS[33] támadásokkal a biztonsági rendszerek kikapcsolása. A tesztelőnek tisztában kell lennie azzal, hogy a tesztelt rendszerek mellett a szomszédos rendszerek vagy hálózati alkatrészek is károsodhatnak. [72]

2.4.3 A hatókör szerinti osztályzás

A penetrációs teszt első elvégzésekor teljes tesztet kell elvégezni annak biztosítása érdekében, hogy a nem vizsgált rendszerek biztonsági réseit figyelmen kívül hagyjuk. Ugyanazon és majdnem azonos rendszereket gyakran tesztelnek egyetlen teszttel, de mivel az esetek nagyon nagy többségében a hálózatok különböző konfigurációkkal rendelkeznek, így minden rendszert külön kell kezelni:

- **Összpontosított**: Ha csak egy adott alhálózatot, rendszert vagy szolgáltatást kell tesztelni, akkor a penetrációs tesztet e vizsgálat szempontjából összpontosítottnak kell tekinteni. Ezzel a módszerrel a teszt hatóköre módosul, például a rendszer képének módosítása vagy kibővítése után. Az ilyen teszt természetesen csak információkat szolgáltat a tesztelt rendszerről, nem nyújt általános információt az informatikai biztonságról.
- **Korlátozott**: Korlátozott számú rendszert vagy szolgáltatást tesztelnek korlátozott penetrációs teszttel.
- **Teljes**: A teljes teszt lefedi az összes rendelkezésre álló rendszert.

2.4.4 A megközelítés szerinti osztályzás

Ha az elsődleges biztonsági rendszerek mellett olyan másodlagos rendszereket, mint például IDS[34]-t, szervezeti vagy személyes struktúrákat (például eszkalációs folyamatokat) kell tesztelni, a tesztelési megközelítések az alábbiak szerint alakulnak:

- **Rejtett**: A másodlagos biztonsági rendszerek behatolási tesztjeinek és a meglévő eszkalációs folyamatoknak legalább kezdetben titokban kell maradniuk, tehát a kezdeti értékelési szakaszban csak azokat a módszereket használják, amelyeket a rendszer támadási kísérletei közvetlenül nem azonosítanak. Magában foglalja a támadások szimulációját és megvalósítását, de ebben az esetben nincs információ a szervezetről. A

[33] Denial of Service - más néven túlterheléses támadás, illetve az elosztott szolgáltatásmegtagadással járó támadás (Distributed Denial of Service, DDoS) informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése.

[34]Intrusion Detection System A hálózat és adatvédelmi rendszerek legbonyolultabb és érdekesebb típusa az illetéktelen hálózati behatolást jelző rendszer. Az IDS legfontosabb célja és feladata, hogy azonosítsa a hálózatban a gyanús vagy kártékony aktivitásokat, észrevegyen minden olyan tevékenységet, amely eltér a rendszerek normális működésétől. Naplózza, katalogizálja és osztályozza a rendszerfolyamatokat.

rejtett teszt teszteli a belső biztonsági csapat képességét a támadások észlelésére és a támadásokra való reagálásra. Az ilyen típusú teszt több időt és pénzt, valamint sokkal több tudást és képességet igényel. A penetrációs tesztelő szemében az ilyen mérés előnyösebb, mivel ez áll a legközelebb a valódi támadás szimulálásához.

- **Nyílt**: Ha a rejtett megközelítés nem ad választ, akkor a tesztelő a szervezettel együttműködésben elvégzi a white box tesztet. Ebben az esetben nyílt módszereket alkalmaznak, például kiterjesztett portok keresését közvetlen kapcsolatokkal. Az ügyfelek csatlakozhatnak a csapathoz egy nyílt fehér doboz teszttel. Ez különösen ajánlott rendkívül kritikus rendszerek esetében, mivel azt jelenti, hogy a tesztelők gyorsabban reagálnak a váratlan problémákra, amikor együttműködnek a szervezettel a potenciális biztonsági fenyegetések azonosításában. Az egyik nagy előnye az, hogy képes elindítani a kívánt hozzáférési és belső ismeretek támadásait a blokkolás veszélye nélkül. Másrészt, ez hátrányos a biztonsági program azonosításában, azaz az egyes támadások felderítésében. [73] [66]

2.4.5 A technika szerinti osztályzás

A hagyományos penetrációs teszt során a rendszereket csak a hálózaton keresztül támadják meg. Ezen kívül azonban még fizikai támadások és más típusú social engineering technikák is felhasználhatók a rendszerek támadására.

- **Hálózati**: A hálózati alapú penetrációs teszt a hackerek támadásának jellemző módszerét szimulálja. A legtöbb informatikai hálózat jelenleg TCP/IP[35]-t használ, így ezeket a teszteket IP alapú penetrációs teszteknek is nevezik. A hálózati biztonsági teszt olyan kockázatokat és sebezhetőségeket azonosít, amelyek károsíthatják a hálózati és biztonsági irányelveket. A hálózat penetrációjának tesztelése elengedhetetlen a szervezet szempontjából, ami a hálózat és a rendszer biztonsági kockázatainak és sebezhetőségének támadó szempontjából történő értékelésére szolgál. A hálózati penetráció tesztelése hálózati folyamatokat és eszközöket használ a TCP/IP jellegű sebezhetőségek kivizsgálására, és segít a szervezeteknek a biztonsági politikák kidolgozásában és betartásában. Ez a teszt megpróbálja veszélyeztetni a hálózat rendszereit, elemeit és eszközeit, majd részletesen ismerteti az eredményeket.
- **Applikációs**: Nem lehet megakadályozni, hogy egy gyenge alkalmazás potenciálisan a szervezet eszközein vagy között fusson, még egy jól megalapozott és biztonságos

[35] A TCP/IP betűszó az angol Transmission Control Protocol/Internet Protocol (átviteli vezérlő protokoll/internetprotokoll) rövidítése, mely az internetet felépítő protokollstruktúrát takarja.

infrastruktúrában sem. Az ilyen típusú tesztelés célja annak biztosítása, hogy az alkalmazás ne észlelje magát a hozzáférést. Következő lépésként biztosítani kell a hozzáférést a hálózaton belüli központi szerverekhez és a szoftverekhez. A szoftvertesztelés a szoftverfejlesztési folyamat lényeges része, és segít meghatározni a kifejlesztett szoftververziók pontosságát és teljességét. Az alkalmazások tesztelése magában foglalja a szoftveralkalmazások és a webes alkalmazások tesztelését is. A webes alkalmazások sebezhetőségét a webalkalmazások tesztelésével lehet azonosítani. A teszt végrehajtásának legjobb módja az alkalmazás különféle sebezhetőségeinek felhasználása rendszeres és ismétlődő tesztek sorozatán keresztül. Az alkalmazás tesztelésének néhány fontos szempontja:

- Forráskód felülvizsgálata: A forráskód felülvizsgálata segíti annak biztosítását, hogy a szoftver nem tartalmaz olyan fontos információt, amelyet a támadó felhasználhat egy alkalmazás kihasználására. Például egy rendelkezésre álló szoftverkód tartalmazhat tesztkéréseket, neveket vagy tiszta szöveges jelszavakat, amelyek releváns adatokat vagy információkat tartalmazhatnak a tesztelő számára.
- Engedélyezési tesztelés: Tesztelési rendszerek engedélyezése a felhasználói munkamenetek megkezdéséhez és fenntartásához. Ez magában foglalja a bejelentkezési hitelesítő adatok tesztelését, a sütik biztonságát és a kizárás tesztelését annak biztosítása érdekében, hogy az érvényes munkamenetek ne legyenek elterelhetők. Az engedélyezési teszteket a bejelentett rendszerek engedélyezési állapotának azonosításához, és az illetéktelen hozzáférés azonosításának céljából hajtják végre.
- Funkcionalitás tesztelése: A funkcionalitás tesztelése az alkalmazás működéséért felelős rendszereket teszteli. Ez magában foglalja a karakterek és a megadott URL[36] bemenetek érvényesítésének tesztelését.
- Web penetrációs teszt: A webes penetráció tesztelése magában foglalja a web alapú szövegek ellenőrzését olyan nyelveken, mint a J2EE[37], ASP.NET[38] és

[36] Az URL (Uniform Resource Locator [egységes erőforráshely] rövidítése), az interneten megtalálható bizonyos erőforrások szabványosított címe.
[37] A Java Platform, Enterprise Edition, röviden Java EE egy széles körben használt szerveroldali Java programozási platform. Az 1.4 verzióig a neve Java 2 Platform, Enterprise Edition, röviden J2EE volt. A következő verzió neve már egyszerűen csak Java EE 5 lett. A jelenlegi verzió a Java EE 8.
[38] Dinamikus weboldalak készítését lehetővé tévő osztályok és komponensek együttese. Az ASP.NET-tel a szerveren (tipikusan egy webszerver vagy Internet információs szerver) tárolt adatokból állítunk elő HTML-oldalakat, amit a kliensek könnyen megjeleníthetnek -- használjanak bármilyen webböngészőt, Netscape-et vagy mást.

PHP[39]. Ebben a tesztben a tesztelők jelentéseket kapnak különböző szintű jogosultságú alkalmazásokról, lehetővé téve a tesztelők számára az OWASP biztonsági réseik megtalálását. A webes penetráció tesztelése segít azonosítani a webalkalmazás biztonsági réseit, mint például az SQL[40] befecskendezési problémák, XSS[41], XSRF[42], gyenge hitelesítés és forráskód-felfedezés.

- Vezeték nélküli/távoli hozzáférési biztonsági tesztelés: A vezeték nélküli eszközökkel kapcsolatos biztonsági kockázatokkal foglalkozik. Néhány vezeték nélküli eszköz biztonsági fenyegetésnek van kitéve a 802.11 vezeték nélküli hálózat valamint a más szabványcsaládba tartozó hálózatok (például. Bluetooth, BLE, GSM/UMTS/LTE/5G, Zigbee, LoraWAN, ipari és IoT szabványok stb.) miatt. Óvintézkedéseket kell tenni annak biztosítása érdekében, hogy az ilyen megoldások architektúrája, tervezése és telepítése biztonságos legyen. A vezeték nélküli/távoli hozzáférési tesztelést mobil munkaerőt foglalkoztató szervezet biztonsági szintjének felmérésére használják. Az egységes kockázatkezelés hatékony kezelésének biztosításához elengedhetetlen a megoldások tervezéséhez és telepítéséhez való hozzájárulás.
- Telefonbiztonsági tesztelés: A TCP/IP hálózatokon kívül más kommunikációs hálózatok is használhatók a támadások végrehajtásához. Idetartoznak a telefonhálózatok és a mobil vezeték nélküli hálózatok. A telefonbiztonsági teszt a hangbiztonsági kérdésekkel foglalkozik a technológiákat tekintve. A behatoló tesztelők ellenőrizhetik a hangátvitel (VoIP[43]) integrációját, a jogosulatlan modemhasználatot és a kapcsolódó kockázatokat. A telefonbiztonsági értékelés segít felmérni a vállalati telefonhálózattal kapcsolatos biztonsági kérdéseket.

[39] A PHP egy általános szerveroldali szkriptnyelv dinamikus weblapok készítésére. Az első szkriptnyelvek egyike, amely külső fájl használata helyett HTML oldalba ágyazható.
[40] Az SQL, azaz Structured Query Language (strukturált lekérdezőnyelv) relációsadatbázis-kezelők lekérdezési nyelve.
[41] Az XSS a számítógépes sebezhetőség egy fajtája, amely tipikusan web alkalmazásoknál fordul elő: egy rosszindulatú web-felhasználó olyan kódot illeszt egy weblapra, amit más felhasználó is lát. Például ilyen kód lehet a HTML kód vagy egy kliens oldali script. Ha egy támadó egy XSS sebezhetőséget felfedez, azt - többek között - felhasználhatja arra, hogy a hozzáférési ellenőrzést kikerülje, például avval, hogy a böngésző által kapott weblap nem az eredeti forrásból származik (de megjelenésében azonos lehet az eredetivel). Manapság ezt a támadásfajtát az ún. phishing támadás végrehajtásánál alkalmazzák. A Cross Site Scripting-et eredetileg CSS-nek rövidítették, de ez a rövidítés ütközött a Cascading Style Sheet rövidítésével, ezért változtattak rajta.
[42] A cross-site request forgery, más néven one-click attack session riding, rövidítve CSRF vagy XSRF (magyar fordításban kb. oldalon-keresztüli kéréshamisítás), egy exploit típus, ahol a weboldalaknak küldenek nem-autorizált parancsot felhasználóként, amelyben megbízik az oldal.
[43] Az internetprotokoll feletti hangátvitel – elterjedt nevén VoIP, Voice over IP vagy IP-telefónia – a távközlés egy olyan formája, ahol a beszélgetés nem a hagyományos telefonhálózaton, hanem az interneten vagy más, szintén IP-alapú adathálózaton folyik.

- Fizikai biztonsági tesztelés: Manapság a biztonsági rendszerek, mint például a tűzfalak, széles körben elterjedtek, és ezeknek a rendszereknek a konfigurálása általában magas szintű biztonságot nyújt, ami azt jelenti, hogy rendkívül nehéz, de nem lehetetlen, hogy az ilyen rendszerek támadása káros hatást gyakoroljon. Gyakran könnyebb és gyorsabb a szükséges vagy megkövetelt adatok megszerzése, ha ezek ellen a rendszerek ellen közvetlen fizikai támadást hajtanak végre. A fizikai támadás, mint például az adatokhoz, az épülethez és/vagy a kiszolgálóterülethez való jogosulatlan hozzáférés után a támadó közvetlenül hozzáfér egy nem jelszóval védett munkaállomáshoz.
- Social Engineering: Az emberek gyakran a biztonsági lánc leggyengébb láncszemei, így a nem megfelelő biztonsági ismeretek vagy az elégtelen biztonsági tudatosságot kihasználó social engineering technikák gyakran sikeresek. Az ilyen tesztek megfelelőek az általános biztonsági politika bevezetése után, például annak végrehajtása és/vagy elfogadása mértékének megvizsgálására. A biztonsági politika állítólagos hatékonyságával kapcsolatos hamis feltételezések gyakran olyan biztonsági kockázatokat eredményeznek, amelyeket a helyzet pontos felmérése esetén további lépésekkel lehet csökkenteni. A social engineering olyan technika, amelyet a támadók használnak az emberi sebezhetőség kihasználására a hálózaton belül. A social engineering a befolyás és a meggyőzés felhasználása az emberek információcseréhez való megtévesztése céljából. A social engineering technikák pszichológiai trükköket használnak érzékeny információk, például kapcsolattartási címek, jelszavak, felhasználónevek és hitelkártya-információk megszerzésére. Az emberi segítségre való hajlandóság és a bizalom az információk gyűjtésére számos módon felhasználható. A környezettől vagy a körülményektől függően a social engineering-et számítógépes vagy közvetlen kapcsolaton keresztül valósítják meg. Néhány social engineering trükk magában foglalja például a hamis telefonhívásokat, az e-mailekkel való csalást és az adathalászatot. A technikák között szerepel a hamisítás is, például készpénz vagy nyeremények felajánlása postafiókban vagy látszólag ártatlan kérdések feltevése, amelyek felfedhetik a személyes információkat. Egy jó social engineering tesztelő alapos háttérkutatást végez a szervezetnél, hogy megismerje a vállalat alapvető természetét és még néhány alkalmazott nevét is. Ezek az információk elősegítik a támadók fizikai hozzáférését a szervezet információs rendszereihez azáltal, hogy kijátsszák az ellenőrzéseket a fontos információk ellopásával. [64]

2.4.6 A kiindulási pont szerinti osztályozás

A penetrációs teszt kiindulási pontja, azaz az, ahol a penetrációs tesztelő számítógépe csatlakozik a hálózathoz, vagy ahonnan támadási kísérletek származnak, lehet az ügyfél hálózatán, a szervezet épületen kívül vagy belül.

- Általában az adott hálózatot az internet kapcsolatán keresztül támadják meg. A penetrációs teszt képes felismerni és kiértékelni egy ilyen kívülről érkező támadás potenciális kockázatát. Az ilyen tesztek során általában megvizsgálják a DMZ[44] és a RAS[45] kapcsolatok tűzfalait és rendszerét.
- Az informatikai rendszer belsejéből a tesztelőnek általában nem szabad felülírnia a tűzfalakat vagy a hozzáférési vezérlőket a belső hálózatokhoz való hozzáféréshez. Ezért egy belső teszttel fel lehet mérni a tűzfalkonfigurációt és a belső hálózathoz hozzáférő emberek támadásainak hatásait. [74][75]

Összességében megállapítható, hogy a penetrációs teszt osztályzásának jellemzői a teszt célját hivatott segíteni annak érdekében, hogy hatékony és eredményes vizsgálatot lehessen végezni. **Azt a következtetést vonom le,** hogy az osztályzást érdemes kombinálva használni.

2.5 KÖVETKEZTETÉSEK

E fejezetben a nemzetközi leírások feldolgozásával és tapasztalataimmal összhangban **feldolgoztam** a nemzetközi szabványok iránymutatásait, penetrációs teszttel kapcsolatos alapfogalmait és annak értelmezéseit.

Mindezekre támaszkodva **meghatároztam** a penetrációs teszt és a sérülékenységelemzés fogalmát, valamint **bemutattam és értelmeztem** a két fogalom és eljárás közötti főbb különbségeket.

Összefoglaltam a különböző penetrációs teszt rendszermodellek lényegi elemeit, többek közt a célokat, tulajdonságokat, korlátokat és kihívásokat.

Részletesen **elemeztem** a nyíltan elérhető legnépszerűbb penetrációs teszt szabványokat, ajánlásokat.

[44] Demilitarizált zóna, más néven demarkációs zóna vagy határhálózat egy olyan fizikai vagy logikai alhálózat, ami egy szervezet belső szolgáltatásait tartalmazza és tárja fel egy nagyobb, nem megbízható hálózatnak, általában az internetnek.
[45] Remote Access Services - Távoli hozzáférési szolgáltatások

Feldolgoztam és értelmeztem, valamint a nemzetközi szakirodalom alapján **csoportosítottam** a penetrációs teszt osztályzását.

A fejezet eredményei alapján az alábbi következtetéseket fogalmazom meg:

1. A kiberbiztonsági penetrációs teszt az informatikai rendszerek alapos tanulmányozását biztosítja. Ez a tesztelési módszer komplex elemzést nyújt, amely lefedi a rendszer és a szervezet informatikai-biztonsági és kiberbiztonsági kérdéseit, és nagyban hozzájárulhat a Magyar Honvédség kiberműveleti erőfeszítéseihez.
2. A módszertanok más megközelítést alkalmaznak a penetrációs teszt vagy biztonsági teszt elvégzésére. E különbségek megértése érdekében összehasonlítottam a különböző módszertanokat, megvizsgálva azok céljait, a gyakorlatban végzett tesztek tevékenységeit. A módszerek összehasonlításával világossá válik, hogy mind a négy módszertan eltérő megközelítést kínál a penetrációs teszt elvégzéséhez, és nem feltétlenül kompatibilisek egymással. A szabványosítás és a konzisztens szemlélet kialakítása érdekében ezért figyelemre méltó, hogy általában a különböző szervezetek a különböző módszertanok különböző elemeit alkalmazzák belső módszertanuk megalkotásához. A módszertanok céljainak szempontjából az OSSTMM tudományos módszertan a tényleges biztonság mérésére törekszik. A PTES az üzleti és biztonsági szolgáltatók számára a közös nyelvet és hatókört, valamint a munka alapvonalát biztosítja. A NIST SP 800-115 számos módszertanhoz és értékelési célra felhasználható tesztelési ajánlásokat nyújt. Az OWASP az összes vizsgálati technika összegyűjtését és magyarázatát, valamint következetes és reprodukálható módszertan biztosítását tűzte ki célul. A módszertanok gyakorlati értékelési irányelveinek perspektívájából az OSSTMM-ben a fő hangsúly az információgyűjtésen és a sebezhetőség elemzésén, valamint a RAV-ok meghatározásán, az üzembiztonságon, a korlátozásokon és az ellenőrzéseken van. A PTES nagyon praktikus és specifikus tevékenységeket tartalmaz, beleértve azt is, hogy milyen eszközöket és technikákat kell használni. A NIST 800-115 a tevékenységek magas szintű leírását takarja, beleértve más módszerek alkalmazásának ajánlását. Végül az OWASP nagyon gyakorlati tevékenységeket ölel fel, többek között a sebezhetőségek széles skálájának tesztelésével kapcsolatban.
3. A tesztek osztályzásánál a megkülönböztető jellemzők között szerepel például a vizsgált rendszerek mérete, szerkezete, a tesztek elővigyázatossági vagy agresszív jellege. Azokat a jellemzőket, amelyek egy adott penetrációs tesztre vonatkoznak, a teszt céljához kell igazítani annak érdekében, hogy hatékony és eredményes vizsgálatot lehessen végezni. Meg kell jegyezni, hogy nem minden lehetséges kombináció eredményez hasznos tesztet,

még akkor sem, ha az osztályozási kritériumokat a lehető legszélesebb módon tartják fenn.

A tudományos irodalomkutatást elvégezve **megállapítom,** hogy a penetrációs tesztelés jelentős különbségeket mutat a sérülékenységelemzéssel szemben, hisz a támadó szempontjából átfogóbb megközelítést biztosít. Véleményem szerint a teszttel az azonosított biztonsági hiányosságok nemcsak összegyűjtve és rendszerezve állnak rendelkezésre, hanem kihasználható és felhasználható sebezhetőségek elemzéséhez, kiaknázásához, ezzel bizonyítva egy kiberfenyegetés reális esélyét.

Számos nemzetközi szabvány figyelembevételével **kijelentem**, hogy sok meghatározási és megközelítési különbség létezik. A vonatkozó szabványok a biztonság vonatkozásában alapvetően megegyeznek, de sok eltérés és rengeteg variáció van mind technikai, mind fogalmi és módszertani szinten is. Fontosnak tartom **az alapvető meghatározások, célok és jellemzők meghatározását**. A lehetséges osztályozás remélhetőleg megkönnyíti az ilyen tesztek előkészítő szakaszát.

Mindezen előzményeket figyelembe véve, jelen fejezetem alapján arra az **összegzett részkövetkeztetésre jutottam**, hogy a vizsgált fogalomtár nemzetközi szinten számos tudományos kiber, illetve informatikai szövegkörnyezetben megtalálható, mégis a penetráció tesztelés vagy annak osztályzása kevés, vagy csak említés szintjén jelenik meg a Magyar Honvédséggel és a kiberműveleti feladataival összeköthető tudományos művekben. Véleményem szerint egyik alapvető és meghatározó eleme kell, hogy legyen a kibervédelem és informatikai biztonság tesztelési kérdéskörének. **Támogatni kell** a támadó nézőpontjából működő technikai tesztek, gyakorlatok megszervezését, végrehajtását, az ebből származó tudományos eredmények publikálását.

3 KIBERMŰVELETI HÁLÓZATI PENETRÁCIÓS TESZT ÉS ANNAK MUNKAFOLYAMATA

Az értekezés jelen részében egy, a már megtörtént nemzetközi és hazai példák tanulmányozása révén készített saját módszertan kerül bemutatásra. A tesztelési módszertan, mint általános keret, illetve munkafolyamat kerül részletezésre, majd a technikai felderítés szintjén javasolt módszerek és gyakorlatok konkrét megvalósításokon keresztül igazolják a módszertan használhatóságát, hasznosíthatóságát és hatásfokát. Mindenképpen fontos leszögezni, hogy a kutatások során a penetrációs teszt módszertanok a rengeteg különbséget mutatnak, mégis egy fő irányvonalon haladnak. Természetesen a teszt osztályozásánál is számos különböző nézőpontot lett feltárva. A fő irányvonal a módszertanoknál is hasonló, de nem azonos. Így fontos a kielemzett példákon keresztül a lényeges szintek, lépések, fázisok megtartása, valamint összegyűjtése, de a felesleges dolgok szelektálása.

3.1 A MÓDSZERTAN MAGYAR HONVÉDSÉGGEL VALÓ KAPCSOLATA ÉS MUNKAFOLYAMATA

A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról a Nemzeti Kibervédelmi Intézet részeként alapította meg a Kormányzati Hálózati Eseménykezelő Központot (GovCERT-Hungary). A magyar kiberbiztonsági eseménykezelő szervezetek és az általuk felügyelt informatikai rendszerek:

- Kormányzati Eseménykezelő Központ: állami és önkormányzati nyílt informatikai rendszerek;
- Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja: nemzeti létfontosságú rendszerek és létesítmények informatikai rendszerei;
- Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ: honvédelmi célú informatikai rendszerek, és a katonai nemzetbiztonsági műveleti hálózat, valamint az MH Kormányzati Célú Elkülönült Hírközlő Hálózat;
- Információs Hivatal Eseménykezelő Központja: a polgári hírszerzés informatikai rendszerei és a polgári nemzetbiztonsági műveleti hálózat;

- SZTAKI Hun-CERT munkacsoport: az Internet Szolgáltatók Tanácsa tagszervezetei által üzemeltetett informatikai rendszerek, hálózatok;
- KIFÜ CSIRT csoport: az NIIF program hálózata és az ahhoz csatlakozó informatikai rendszerek. [76]

A Honvédelmi Minisztérium a Katonai Nemzetbiztonsági Szolgálat (a továbbiakban KNBSZ) keretein belül működteti saját, honvédelmi célú zárt és nyílt rendszerei kibervédelmét biztosító és mind az incidenskezelési feladatokat, mind pedig a hatósági funkciókat ellátó szervezetét. [77] A Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ a KNBSZ szervezetében működő ágazati szervezet, amelynek rendeltetése a honvédelmi célú informatikai rendszerek biztonságának támogatása, a rendszerek működése során bekövetkező biztonsági események ágazati szintű kezelése, a sérülékenység vizsgálatok végrehajtása és a fenyegetettségek kezelése. Ez a szervezet a szakfeladat szerint elkülönülő – a honvédelemért felelős miniszter irányítása, vezetése alatt álló szervnél, szervezetnél működő – eseménykezelő központokkal együtt látja el a biztonsági események és fenyegetések kezelését. A HM a honvédelmi szervezetek 2016. évi fő célkitűzéseinek és fő feladatainak, valamint a 2017–2018. évi tevékenysége fő irányainak meghatározásáról szóló 3/2016. (I. 22.) HM utasításban Military Computer Emergency Response Team, MilCERT[46] megnevezéssel azonosította a szervezetet. [78]

A Magyar Honvédség szereplőinek egy olyan módszert kell alkalmazni az informatikai és kiberműveletek tesztelésére, ami tartalmazza a jogszabályi előírásoknak való megfelelést, mely követelmény jól látható B. Müller Tamás publikációjából: *„Magyarországon a stratégiai dokumentumokban már 2012-ben megfogalmazódott a kibertér fenyegetéseivel szembeni védelem jelentősége, és megjelent a kibertér hadszíntérként való meghatározása is. A kibertér önálló műveleti területként végül 2018-ban törvényi szinten is beépült a magyar jogrendbe." [79]* A Nemzeti Katonai Stratégia (2012), a 2013-ban elfogadott Nemzeti Kibervédelmi Stratégia, a Honvédség Kibervédelmi Koncepciója (2013), illetve a Zrínyi 2026-os fejlesztési program alkotja a magyar katonai kiberképességek kialakításának fő kereteit.

„Ma a Honvédség kibervédelmében gyakorlati szinten részt vesz az MH Híradó és Informatikai Rendszerfőközpont, de a 15/2017. HM utasítás szerint - hasonlóan pl. Csehországhoz vagy Szlovákiához – a kiberműveletek fő letéteményese és felügyeleti szerve a Katonai Nemzetbiztonsági Szolgálat (KNBSZ). Jelenleg azonban sem a csapásmérés, sem a

[46] Military Computer Emergency Readiness Team - Katonai Eseménykezelő Központ

válaszadás módja nem fogalmazódik meg a jogrendben" [80]. A KNBSZ hatásköre főként a felderítő képességek, valamint a kiberincidensek kezelésére összpontosító képességek fejlesztése volt az elmúlt években. [81]

Napjainkig a Honvédség a 2018. évi feladatairól szóló utasítással összhangban a hadsereg kezdeti kiberképességének és ágazati információbiztonsági rendszerének továbbfejlesztésén dolgozott. *„A Honvéd vezérkar főnöke 2019-es országgyűlési meghallgatásán jelezte, hogy a még nem létező kiberképességeket a jövőben tervezik kialakítani. Ennek állomásaként 2019-ben megnyitott a Honvédség Kiberakadémiája, de a Zrínyi 2026 program keretében további fejlesztések várhatók."* [82]

A Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat [83] alapján a KNBSZ egyik fő feladata közé tartozik a digitális környezet iránti bizalom erősítése. Ezt főképpen a szakmai együttműködés erősítésével, a hatóságok, az állami és civil szervezetek, valamint az eseménykezelő központok közötti információ-megosztással, kibergyakorlatok megtartásával, a kiber-bűnüldözés fejlesztésével, illetve összehangolt megelőzési, feltárási, mérséklési és reagálási mechanizmusok létrehozásával tervezik elérni, mint például:

- részvétel, ágazati szakmai támogatás biztosítása a kiberkoordinátor által szervezett rendezvényeken;
- a kiberkoordinátor, az NBSZ NKI által szervezett rendezvényen az együttműködési feladatok áttekintése;
- közös éves továbbképzés, témaorientált szakmai konferencia végrehajtása;
- elektronikus információbiztonsági eseménykezelési, sérülékenységvizsgálati tapasztalatok áttekintése;
- hatósági, információbiztonsági események kivizsgálási eljárások tapasztalatainak áttekintése;
- honvédelmi gyakorlatok kibervédelmi feladatainak tervezése, szervezése és végrehajtása. (A katonai gyakorlatok során a tevékenység jellegéhez köthető, valós vezetési és irányítási képességet nem veszélyeztető törzsvezetési, vagy technikai elemeket tartalmazó lépések bedolgozása a valós eseménykezelési eljárásrendet követve. Részvétel a nemzeti kormányzati kibervédelmi gyakorlatok végrehajtásában.)
- a társágazati szereplőkkel történő kapcsolattartás erősítése (aktív együttműködés és információmegosztás az illetékes szervek a kiber-bűncselekmények elleni hazai, valamint nemzetközi szervezetekkel, összefogásokkal)

A 1838/2018. (XII. 28.) Korm. határozat szerint a KNBSZ másik fő feladatköre a digitális infrastruktúra védelem. Ezen belül a nemzetközi együttműködés erősítése, az alapvető szolgáltatások, valamint a létfontosságú infrastruktúrák és szolgáltatásaik védelme, valamint kiber- védekező elhárító és reagáló képességek fejlesztése, melyeket a következő intézkedésekkel kívánnak elérni:

- nemzetközi szintű kiberbiztonsági gyakorlatokon való részvétel (különösen az ENISA és NATO által szervezett kiberbiztonsági gyakorlatokon való részvétel);
- a nemzetközi (NATO) katonai kibervédelmi gyakorlatok tervezése, szervezése és végrehajtása, EU (NKI által szervezett) gyakorlatokon részvétel;
- NATO, multilaterális (pl. V4), illetve bilaterális szakmai keretrendszeren belüli információ és tapasztalatcsere;
- stratégiai tanulmány készítése a katonai nemzetbiztonsági vonatkozású hatások kibervédelmi vonatkozásairól és az ezekkel kapcsolatos lehetséges fejlesztési irányokról;
- az ágazati szintű kockázatértékelés, kockázat-elemzés módszertanának kidolgozása. (A kiberkoordinátor által szervezett rendezvényeken az együttműködési feladatok áttekintése, központi irányelvek kidolgozása, kiadása);
- az észlelési, feldolgozási, felderítési képességek fejlesztése, amelyek lehetővé teszik a fenyegetések, illetve támadások felismerését, osztályozását és forrásának megállapítását;
- a nemzeti kiberteret fenyegető korai előrejelző képesség kialakítása, növelése. Olyan passzív kibervédekezési eszközök informatikai infrastruktúrában történő elhelyezése, amelyek a fenyegetések elleni védelmi funkciót töltenek be, illetve biztosítják a fenyegetésekre vonatkozó információk kellő időben történő rendelkezésre állását. A kívánt kiberbiztonsági szint fenntartásához a megfelelő, az adott helyzetben szükséges és az adott fenyegetéshez illeszkedő arányos ellenintézkedések végrehajtása;
- a gyors helyzetfelismerés, az értékelés és a kockázatelemzés rendszerének kialakítása. (A fenyegetések és tapasztalatok alapján a kialakított eljárásrendek kidolgozása.);
- a kiberfenyegetésekre történő különböző fokozatú reagálás eszközrendszerének kifejlesztése.

A penetrációs tesztelés módszertana egy folyamat, amely a nemzetközi szabványok, kibervédelmi stratégiák és műszaki leírások vizsgálata alapján egy lehetséges eljárást ír le. A

saját penetrációvizsgálati módszertan foglalkozik a fenti kérdésekkel, és olyan hálózati megközelítést biztosít, amely képes a fajlagos legjobb értékelésére a már használt módszerek, a különbségek egyesítése és a korlátozások leküzdése révén. Az egységes hálózati megközelítés lehetővé teszi a súlyos problémák és veszélyek észlelését a kibertérben működő infrastruktúrán belül, és végül hozzájárul az ilyen rendszerek biztonságának általános javításához. A saját penetrációs teszt értékelési módszertanának elképzelése olyan folyamat, amely átveszi az általános struktúrát és terminológiát, illetve bizonyos elemeket ezekből a standard módszertanokból, de mégis kibővíti, és az elvárásoknak megfelelően taglalja, és sorolja be azokat. Nem a szabványok helyettesítése, lecserélése a cél, de átgondolása a létező módszertanoknak, azok javítása, bővítése, frissítése, és a Magyar Honvédségre való szabása.

A saját módszertan kidolgozásának eredménye egy hálózati penetrációs tesztelési módszertan, amely a Magyar Honvédség infokommunikációs rendszereinek sajátosságaihoz, korlátjaihoz igazítva biztosítja a tesztelést. Továbbá ezen szervezeti sajátosságokból adódó tulajdonságok figyelembevételével egy szervezeti csoportra szabott kötelezettségvállalást és hatókörmeghatározást foglal magába. Ez egy implementálható formát nyújt az adott döntéshozók irányába. A tesztnek mindig meg kell felelnie a Magyar Honvédség szervezeteinek, céljainak. Ez azt jelenti, hogy a teszt meghatározza a célokat, felvázolja a cél eléréséhez szükséges vizsgálati lépéseket, vagy elmagyarázza, hogy egy penetrációs teszt egyáltalán alkalmas-e ezek elérésére. Egy modul-alapú megközelítés ajánlott az egyes vizsgálati lépések csoportosításához, mivel ez lehetővé teszi, hogy a behatolási vizsgálatban szereplő lépések tematikusan kategorizálva legyenek. Ez a teszt egyértelmű keretet biztosít, és lehetővé teszi a tesztelő számára, hogy megfelelő teszt lebonyolítást dolgozzon ki egyes modulok kiválasztásával vagy kizárásával.

A korszerű katonai rendszerek ma már alapvetően digitális rendszerek. Ahogyan jelenlegi munkakörömben, a NATO Támogatási és Beszerzési Ügynökségben Kommunikációs és Információs Műveleti Tisztként (NSPA[47] CIS Operations Officer a SAC[48] katonai programon) eltöltött idő tapasztalata is alátámasztja, alapvető követelmény a katonai digitális infokommunikációs hálózatokkal szemben a penetrációs teszt. Ez a követelmény annak érdekében kerül meghatározásra és végrehajtásra, hogy ne legyenek sérülékenységekkel, magas biztonsági kockázati tulajdonsággal rendelkező hálózatelemek, szoftverelemek a katonai infokommunikációs rendszerünkben. Tehát a penetrációs teszt elengedhetetlen, ha meg akarjuk védeni katonai infokommunikációs rendszerünket. Ezen felül e tapasztalatok támpontot is

[47] NATO Support and Procurement Agency - Támogatási és Beszerzési Ügynökség
[48] Strategic Airlift Capability - Stratégiai Légiszállítási Képesség

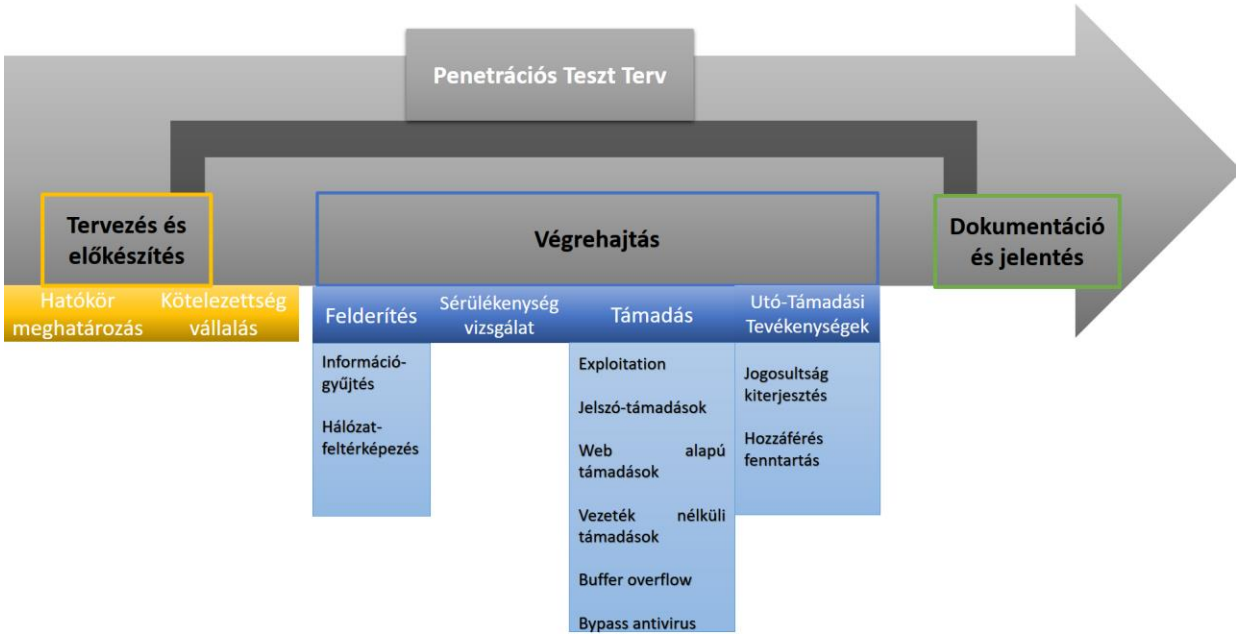
adhatnak arra, hogy a szembenálló felet mely kibertéri rétegben és hogyan kellene vagy lehetséges támadni. A kibertérben való katonai infokommunikációs rendszerek támadása pedig akkor is katonai tevékenységnek minősül, ha azt nyílt forráskódú technikákon keresztül valósítjuk meg.

A Nemzeti Közszolgálati Egyetem a Good Governance Knowledge Transfer Program, NUPS – USA" program keretein belül fél éves kutatási ideje alatt az Egyesült Államok beli UNG egyetemen rendszereztem, elemeztem, és megvizsgáltam a különböző nemzetközi penetrációs teszteket, azok modelljének módszertanának szerkezetét. Ezeknek a részletezését és a következtések levonását a 2. fejezetben ismertettem.

Ezen kutatásra, valamint a szakmai tapasztalatom alapján a következő Penetrációs teszt tervet alkottam meg, melyet az 5. ábrán mutatok be. A terv megalkotásának oka, hogy véleményem szerint a nemzetközi példák nem ültethetők át teljes mértékben, hiszen egy katonai szervezet nyílt penetrációs módszertanának használata alapvetően gátolja a kiberfölény elérését, megtartását, hiszen a szemben álló felek egyértelműen a felhasznált információ birtokában vannak. Ezért fontos egy saját megközelítésű, hasonló mégis eltérő módszertan alkalmazása, amely nagyobb mértékben hozzájárul a kiberfölény kialakításához.

Három fő részt hoztam létre: Tervezés és előkészítés; Végrehajtás; Dokumentáció és jelentés.

Az első, valamint az utolsó rész alapvető kritériumai és ajánlásai a továbbiakban bemutatásra kerülnek. A második részt optimális felbontással hoztam létre, melyből főként a Felderítés szakaszban az Információgyűjtést és Hálózatfeltérképezést mutatom be tesztkörnyezetben végrehajtott demonstrációk segítségével, mellyel a módszertan gyakorlati alkalmazhatóságára hívom fel a figyelmet.



5. ábra *A lehetséges Penetrációs teszt munkafolyamat (saját szerkesztés)*

Mindent egybevetve kijelenthető, hogy a penetrációs teszt elengedhetetlen, ha meg akarjuk védeni katonai infokommunikációs rendszerünket. A jelenlegi hazai jogszabályok és szabályzók alapján a KNBSZ, amely támogatja a honvédelmi célú informatikai rendszerek biztonságát, a bekövetkező biztonsági események ágazati szintű kezelését, és a sérülékenység vizsgálatok végrehajtását. **Az a következtetést vonom le,** hogy ennek a feladatkörnek a része a penetrációs teszt lehetséges megtervezése és végrehajtása a Magyar Honvédség különböző szervezeteire.

3.2 TERVEZÉS ÉS ELŐKÉSZÍTÉS A PENETRÁCIÓS TESZTBEN

Az informatikai rendszerek tulajdonságuknál fogva számos helyen tartalmazhatnak sérülékenységet az alkalmazás szinttől az infrastruktúra szintig, ezért nagyrészt sikeresen támadhatók. Megfogalmazódhat a gondolat a döntéshozókban, hogy a sérülékenységeket a helyi üzemeltetés miért ne tudná feltárni egy teszt keretein belül. Nem azért nem tudja felderíteni egy szervezet a saját sérülékenységeit, mert nem lenne rá képes vagy, mert nem megfelelő a szakállomány képzettsége, hanem leginkább azért, mert más a motiváció. A helyi üzemeltetés feladata az, hogy működjön a hálózat, biztosítsák a szolgáltatások elérhetőségét, a felhasználók munkavégzését. A vizsgálatot végző beosztott állomány azonban megtalálja azokat a pontokat a rendszerben, ahol a rendszer kompromittálható, hisz nekik ez a feladatuk.

Ezt a nézőpontot Tihanyi Norbert, Vargha Gergely és Frész Ferenc is kifejtik a Biztonsági tesztelés a gyakorlatban című publikációjukban:

„Az igény felmerülhet akár az IT üzemeltetésen, akár a szervezet biztonsági egységében, akár döntéshozókban, egy közös jellemző van, általában mindenki tart a végeredménytől és nem feltétlenül támogatja a vizsgálat megrendelését/elvégzését. Az információ biztonság területén dolgozókban megjelenhet az a félelem, hogy a vizsgálat végeredménye azt fogja mutatni, hogy nem végzik jól a munkájukat. Ilyenkor fontos megnyugtatni, az érintetteket, hogy a vizsgálat alapvetően nem ellenük, hanem értük van. A feltárt állapot lehet, hogy nem lesz majd nagyon pozitív, de mindenképpen egy olyan alapállapotot rögzít, amihez képest mérhető majd az elmozdulás, amit a vizsgálat eredményeként előálló dokumentumok alapján az adott szervezet munkatársai önerőből, vagy külső segítséggel meg tudnak oldani. Ennek eredménye egyrészt egy lényegesen biztonságosabb informatikai rendszer lesz, amit könnyebb majd felügyelni, másrészt felhívja a döntéshozók figyelmét a terület fontosságára és erőforrás igényére.” [84]

3.2.1 A penetrációs teszt terv

A penetrációs teszt terv az átfogó biztonsági terv része, amely meghatározza a teszt alapszabályait. **A terv elemeiként a következőket határozom meg:**

- a teszt célja: meghatározza a teszt céljait;
- a tesztelés erőfeszítése: meghatározza a penetrációs tesztelési folyamat hatókörét;
- az erőforrások és a költségvetés: meghatározza a tesztfolyamat végrehajtásához szükséges erőforrásokat és költségvetést;
- elemzés és áttekintések: elemzi a penetrációs tesztelési folyamatot, és rendszeresen áttekintést ad a teszt folyamatáról;
- változások vezérlése, kommunikáció és a kulcsfontosságú tevékenységek koordinálása: részletezi a változások vezérlését, kommunikációját és a penetrációs teszt során alkalmazott főbb tevékenységeket.

A tesztet indítványozó és fogadó döntéshozóknak tisztában kell lenniük azzal, hogy mit várnak el célként a vizsgálattól, és mi az elérendő cél.

Amennyiben a sérülékenységvizsgálat célja beazonosításra került, meghatározásra kerülhet, hogy pontosan mi kerüljön megvizsgálásra a rendszeren. Általános hibalehetőség a túl tág, illetve a túl szűk vizsgálati célterület („scope”) meghatározása. Egy teljes szervezet minden elemére kiterjedő vizsgálatának jelentős erőforrásigénye van, és nem is minden esetben célszerű azt egyben lefolytatni. Ugyanakkor egy nagyon szűkre szabott vizsgálati célterület

meghatározása után a vizsgálat nem tudja feltárni a célterületet körülvevő rendszer sérülékenységeit vagy hálózati kapcsolódási hiányosságait, így könnyen abba a hibába futhat a vizsgálat, hogy kimutatja, hogy az adott rendszer biztonságos, közben esetleg egy „mellette" lévő eszköz vagy alkalmazás sérülékenysége miatt a vizsgált elem is könnyedén kompromittálható. A Magyar Honvédség esetében célszerű a szervezeti struktúrát figyelembe venni, és haderőnemenként, majd alakulatonként lebontani a vizsgált egységeket, alegységeket. Külön figyelmet kell fordítani az informatikai szempontból központosított szolgáltatásokat biztosító alakulatokra, háttérintézményekre, melyeket szintén külön tesztelni kívánt egységenként kellene azonosítani függetlenül vagy kivételként kezelve a Magyar Honvédség szervezeti struktúrájától. Amennyiben a vizsgálandó célterület beazonosításra került, az mindenképpen jelenjen meg a vizsgálati parancsban annak érdekében, hogy ez később ellenőrizhető, számon kérhető legyen.

Célszerű olyan a tesztért felelős vezetőt kinevezni mind a végrehajtói, mind a teszt fogadói oldalon, akiknek mind a lehetősége, mind a képessége megvan a hatékony intézkedésre. Ezzel összhangban javasolt a Kibervédelmi szemlélőség kinevezése, mint tesztért felelős szervezet, és javasolt a fogadói szervezet részéről a parancsnok, valamint a híradó, informatikai és információvédelmi főnök kinevezése, mint tesztért felelős érintettek.

Javasolt a legalább heti vezetői konzultáció, ahol megbeszélésre kerülnek az aktuálisan elvégzett feladatok és a tervezett vizsgálatok. Belső vizsgálat esetén a fogadó szervezetnek biztosítania kell egy helyiséget, ahol a vizsgálatot folytató személyek dolgozni tudnak, valamint a helyiségben lennie kell alapértelmezett beállítású hálózati végpontnak. A vizsgálat későbbi fázisaiban szükség lehet alapértelmezett konfigurációjú munkaállomás biztosítására. A különböző jogosultsági szintű vizsgálatokhoz (greybox, whitebox) szükséges adott jogosultságú felhasználói vagy adott esetben adminisztrátori hozzáférés létrehozása külön a vizsgálat idejére. [84]

3.2.2 A hatókörmeghatározás

A hatókör meghatározása vitathatatlanul a penetrációs teszt egyik legfontosabb alkotóeleme, ugyanakkor ez is a leginkább figyelmen kívül hagyott. Noha rengeteg könyv és publikáció írt a felhasználható különféle eszközökről és technikákról a hálózathoz való hozzáférésről, mégis nagyon kevés írás található a behatolást megelőző témáról, az előkészítésről. A projekt hatóköre kifejezetten meghatározza, hogy mit kell tesztelni. A tesztelőnek meg kell értenie a különbséget egy olyan teszt között, amely egyetlen alkalmazásra összpontosít és nagy intenzitású, valamint egy olyan teszt között, amelyben a vizsgált szervezet

széles IP-cím tartományt biztosít a teszteléshez, és a cél a hálózathoz való hozzáférés. A hatókör meghatározásához a következő kulcspontokat kell azonosítani és lefektetni:

3.2.2.1 A cél

Minden penetrációs tesztnek célorientáltnak kell lennie. Ez azt jelenti, hogy a teszt célja olyan speciális sebezhetőségek azonosítása, amelyek a vizsgált szervezet küldetési céljainak veszélyeztetéséhez vezetnek. A kockázat azonosításáról van szó, amely hátrányosan befolyásolja a szervezetet. A teszt elsődleges célja nem a megfelelés. A Magyar Honvédségben alkalmazott penterációs teszt elsődleges céljaként a hálózati sérülékenységek felderítése kell, hogy legyen, hisz így a TCP/IP alapú rendszer alapvető sérülékenységei, hibás beállításai kerülnek felderítésre az adott szervezetnél. Továbbá ez megfelelő kiindulási alapot biztosít a további kiberműveleti penetrációs tesztelésekhez.

3.2.2.2 A kezdő és a záró dátumok megadása

A kezdő és záró dátumok megadása lehetővé teszi, hogy legyen egy határozott vége a projektnek. Minden jó projektnek jól definiált kezdete és vége van. Szükség van egy aláírt dokumentumra, amely meghatározza a szükséges munkát és órákat, a tesztelés befejezésének idejét, vagy, ha további tesztelés vagy munka szükséges, az ez utáni órák számát. Ezt a Magyar Honvédség munkaidőt szabályzó rendelkezéseivel összhangban kell végrehajtani.

3.2.2.3 A hatókörmeghatározás

A hatókör meghatározási értekezlet célja annak megvitatása, hogy mit tesztelnek, milyen rendszereket, alkalmazásokat vagy más lehetséges célokat. Szükséges egy szakmai konzultáció a vizsgált szervezet vezetőjével és a szakmai (informatikai, biztonsági) előjárókkal a feltételek érvényesítése céljából. Először egyértelműen meg kell határozni, hogy az IP - tartományok mely területeire terjed ki a vizsgálat. Például ellenőrizni kell, hogy a szervezet az összes célkörnyezetet birtokolja, beleértve a DNS[49]-kiszolgálót, az e-mail szervert, a tényleges hardvert, amelyen webszervereik futnak és a tűzfal/IDS/IPS[50] megoldásokat. Ezen kívül meg kell határozni azokat a fizikai helyszíneket, valamint logikai tartományokat, amelyekben a

[49] A Domain Name System (DNS), azaz a tartománynévrendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára.

[50] Az informatikai biztonság területén behatolásvédelemről beszélünk, amikor a rendszer olyan gyanús viselkedéseit igyekszünk megfigyelni és kiszűrni, melyek veszélyt jelenthetnek a tárolt adatok és a rendszer elemeinek bizalmasságára, sértetlenségére, rendelkezésre állására nézve. A cél tehát minden olyan folyamat észlelése, mely a rendszer biztonságos állapotát sértheti. Eszköze lehet IDS (intrusion detection system) vagy IPS (intrusion detection and prevention system).

célkörnyezetek működnek. A Magyar Honvédség szemszögéből fontos bevonni a meghatározás folyamatába a Magyar Honvédség Parancsnoksága Infokommunikációs és Információvédelmi Csoportfőnökséget.

3.2.2.4 Az IP tartományok megadása

A penetrációs teszt megkezdése előtt minden célt meg kell határozni. Ezeket a célokat a tesztet indítványozótól és a tesztelt szervezettől kell beszerezni egy kezdeti kérdőív segítségével. A célok megadhatók konkrét IP-címek, hálózati tartományok vagy domain nevek formájában. Fontos meghatározni, hogy a rendszerek, például tűzfalak és az IDS/IPS vagy hálózati eszközök, amelyek a tesztelő és a végső cél között vannak, szintén részét képezik-e a hatókörnek Továbbá azonosítani kell az elemeket, például az upstream szolgáltatókat és más harmadik fél szolgáltatókat.

3.2.2.5 Harmadik felekkel való kapcsolattartás

Számos olyan helyzet van, amikor egy megbízás magában foglal olyan jelenleg működő szolgáltatást vagy alkalmazást, melynek üzemeltetését harmadik fél látja el. Ez az elmúlt években egyre gyakoribbá vált, mivel a „felhő" szolgáltatások egyre népszerűbbek lettek. A legfontosabb dolog, amit figyelembe kell venni, hogy bár az adott szervezet engedélyt adott a tesztelésre, az nem garantált, hogy tájékoztatták a harmadik fél szolgáltatót. Ezért engedélyt kell szerezni tőlük is a hosztolt rendszerek teszteléséhez. A megfelelő engedélyek elmulasztása, mint mindig, magával hordozza a törvény megsértésének lehetőségét.

3.2.2.6 A kommunikációs csatornák

A penetrációs teszt egyik legfontosabb szempontja a tesztelt szervezettel való kommunikáció. Felmerülhetnek vészhelyzetek, ezért kapcsolattartási pontot kell létrehozni azok kezeléséhez, melyhez egy vészhelyzet kapcsolati lista létrehozása javasolt. Ez a lista tartalmazza a tesztelés hatálya alá tartozó összes fél elérhetőségét. Miután létrehozták, a vészhelyzeti névjegylistát, meg kell osztani azt a listán szereplőkkel.

Véleményem szerint a következő adatokat szükséges minden sürgősségi kapcsolattartótól bekérni, illetve a többiek irányába megosztani az adatvédelmi törvény maradéktalan betartásával:

- Teljes név;
- Cím és üzemeltetési felelősség;

- Felhatalmazás a tesztelési tevékenységek részleteinek megvitatására, ha még nincs meghatározva;
- A 24/7 azonnali kapcsolat formája, például mobiltelefon;
- A biztonságos internetes kommunikáció egyik formája, például titkosított e-mail.

3.2.2.7 A kérdőívek

Az első kommunikáció során számos kérdés merül fel, amelyekre az adott szervezet vezetőjének válaszolnia kell. Ehhez előre gondosan elkészített kérdőívek készíthetők, melyeket a jobb megértés érdekében arra terveztek, hogy megválaszolják, mit akar elérni a vezetés a penetrációs teszt révén, valamint miért szükséges az adott szervezetnek a teszt végrehajtása, illetve melyek is az adott szervezet informatikai rendszerének tulajdonságai. [69]

3.2.3 A kötelezettségvállalás

A penetrációs teszt általában pénzügyi díjazású szolgáltatás. Ebben az esetben, mivel a Magyar Honvédség számára kerül kifejlesztésre a teszt módszertana, tervezetten azt az adott fegyveres erő szakállománya végezné, így személyügyi, valamint közvetlen pénzügyi vetülete a tesztnek a katonai szakállománnyal és annak képzésével állna szoros kapcsolatban. Mégis szükséges egy minimális kötelezettségvállalást definiálni, amelyet a következők alapján lehet meghatározni:

3.2.3.1 A tesztelési parancs tárgya és általános feltételek

Ha a tesztelőnek vannak általános feltételei, ezeket be kell építeni a tesztelési parancsba. Az adott fegyveres szervezetnek ennek tudatában és ezeknek érvényességének beleegyezésével kell elkezdeni a teszt végrehajtását. A penetrációs teszt céljain túl a feleknek a tesztelési parancsba meg kell határozniuk az alkalmazandó eszközök és technikák jellegét és terjedelmét.

A tesztelési parancsnak egyértelműen meg kell határoznia azt a célt, amelynek elérésére a behatolási teszt elvégzését megbízó szervezet törekszik. A legfontosabb releváns célok a következők:

- A Magyar Honvédség műszaki rendszerei biztonságának növelése: A legtöbb penetrációs tesztet azzal a céllal rendelik el, hogy javítsák a műszaki rendszerek biztonságát. A tesztek olyan technikai rendszerekre korlátozódnak, mint a tűzfalak, útvonalválasztók, webszerverek;
- Tanúsítás/megerősítés megszerzése külső harmadik féltől: Behatolási tesztet is lehet végezni független külső harmadik féltől történő megerősítés megszerzése céljából;

- A Magyar Honvédség szervezeti/személyi infrastruktúra biztonságának növelése: A műszaki infrastruktúra tesztelésén túl egy penetrációs teszt is tesztelheti a szervezeti és a személyi infrastruktúrát, például az eszkalációs eljárások figyelemmel kísérése érdekében, a tesztek körét és/vagy agresszivitását fokozatosan növelve. A social engineering technikák, például a jelszavak telefonos igénylése felhasználhatók az általános biztonság tudatosság szintjének, valamint a biztonsági irányelvek és a felhasználói megállapodások hatékonyságának felmérésére.

A következő osztályozási kritériumok javasoltak:

- információmennyisége alapján (fekete doboz, fehér doboz teszt vagy szürke doboz);
- hozzáállás (passzív/óvatos/kiszámított/agresszív);
- hatókör (teljes, korlátozott vagy összpontosított);
- megközelítés (rejtett vagy nyílt);
- technika (hálózati alapú, egyéb kommunikáció, fizikai hozzáférés, social engineering);
- kiindulási pont (kívülről vagy belülről).

A penetrációs vizsgálat során alkalmazott egyedi technikákat részletesebben kell leírni, ha ez lehetséges és megfelelő, különösen az alkalmazandó social engineering technikákat és a hozzáférés-ellenőrzés aktív tesztelését kell leírni. Mivel a social engineering technikák természetüknél fogva problematikusak és esetleg etikátlanok, helyénvaló meghatározni nekik egy világos keretet (például el kell kerülni a munkavállalók etikátlan viselkedésre ösztönzését). A hozzáférés-ellenőrzések aktív tesztelése megkísérli megkerülni a fizikai biztonsági intézkedéseket, amelyeket betörésnek lehet tekinteni. E tekintetben a teszt lefolytatásának, körülményeinek magyarázata is szükséges. Fontos továbbá azon támadó technikák kizárása, amelyeket kifejezetten nem használnak.

3.2.3.2 Az adott szervezet kötelezettségei

A penetrációs tesztelő érdekében a tesztelési parancsnak meg kell határoznia az adott szervezet jogi kötelezettségét, hogy a lehető legrészletesebben együttműködjön. A következő elemeket kell figyelembe venni:

- Információszolgáltatás a penetrációs teszt jellegétől függően: A penetrációs teszt jellegétől függően a penetrációs tesztelő támaszkodhat az adott szervezettől kapott széles körű információkra. Például egy fehér doboz teszt információt igényel a DNS-

nevekről, IP-címekről, biztonsági politikákról, rendszerkonfigurációkról, tűzfalszabályokról, eszkalációs folyamatokról, illetve a tesztelési parancsban meg kell határozni, hogy ezeket a szükséges információkat időben rendelkezésre bocsássák;

- A potenciálisan érintett harmadik féltől származó információk: A nyilvános hálózatokban zajló normál adatforgalom során a penetrációs teszt harmadik féltől származó rendszereket is használ (például egy szolgáltató kommunikációs szervere). Mivel lehetetlen kizárni e rendszerek teljesítményének romlását, ezért tanácsos, hogy előre jelezni kell a behatolási teszteket minden harmadik fél számára, akit érinthet. Ezeket az információs feladatokat átruházhatják az adott szervezetre, mivel jobb helyzetben van annak megítélésére, hogy mely harmadik feleket érinthetik a tesztek;
- Az előre nem látható rendszerhibák elleni védőintézkedések: Mivel nem zárható ki teljesen, hogy a tesztelés során a rendszereket olyan mértékben rontják, hogy az adatok elvesznek, az adott szervezet saját érdeke, hogy biztonsági mentéseket készítsen a magas kockázatú és releváns rendszerekről, ahol ezt még nem tették meg az általános számítógépes számviteli rendszerek elfogadott alapelvei szerint. Az adatmentések biztosítják az adatok helyreállítását, ha szükséges, és enyhítik az adatvesztés potenciálisan káros hatásait.

3.2.3.3 A tesztelő kötelezettségei

Az adott szervezt érdekében a tesztelőt a következő kötelezettségekkel kell felruházni:

- Titoktartás: A penetrációs teszt során a penetrációs tesztelő hozzáférhet az adott szervezet hálózatának sebezhetőségével kapcsolatos nagyon érzékeny információkhoz. Ezt az információt nem szabad harmadik fél számára rendelkezésére bocsátani. Ezért a tesztelők kötelesek titokban tartani a rendelkezésükre bocsátott, valamint a tesztelés során tudomásukra jutott információkat.
- A vizsgálati eljárások és eredmények dokumentálása: A vizsgálati eljárások dokumentációjának természetét és terjedelmét, valamint az eredményeket a tesztelési parancsban meg kell határozni. A tesztelőt kötelezni kell arra, hogy pontos dokumentációt nyújtson be a tesztelési eljárásairól. Ez biztosítja azt, hogy az általa alkalmazott technikák nyomon követhetők legyenek kár esetén. Ezen kívül a feleknek meg kell állapodniuk az eredmények bemutatásának formájában (jelentés, prezentáció, a felhasznált biztonsági eszközök elemzése).
- A kellő gondosság általános kötelezettsége: A penetrációs tesztelőnek kellő gondossággal kell eljárnia a tesztelési eljárások végrehajtása közben. Például súlyos

gondatlanság lenne, ha a penetrációs tesztelő „véletlenül” támadna meg egy be nem vett harmadik fél rendszerét, mert összetévesztette a DNS-nevet. Ezért a tesztelési parancsnak rendelkeznie kell arról, hogy a penetrációs tesztelőnek a tevékenysége során kellő gondossággal kell eljárnia, tekintettel az esetleges károkra.

3.2.3.4 A szerződés teljesítése

Meg kell határozni a tesztelési parancs kezdési és befejezési dátumát. A penetrációs tesztet ebben az időszakban kell elvégezni. Ez biztosítja, hogy az ezen időszak után bekövetkező behatolási kísérletek egyértelműen azonosíthatók harmadik felek valódi támadásaként, elkerülve ezzel a félreértéseket. Meg kell jegyezni, hogy a penetrációs tesztelő csak a megállapodás szerinti időtartamon belül végezhet vizsgálatokat.

3.2.3.5 Felmondási jog

A penetrációs tesztelés során olyan körülmények léphetnek fel, amelyek akadályozhatják a tesztek előrehaladását (például egy kritikus rendszer összeomlik, és kiterjedt kézi tisztítási munkát igényel). Az ilyen esetekre a felmondás különleges joga beilleszthető a tesztelési parancsba. Ezen túlmenően a szolgáltatási szerződések felmondására vonatkozó általános szabályokat kell alkalmazni. [72]

Összességében kijelenthető, hogy a penetrációs tesztnél szükségszerű ez részletes tervet készíteni, mely tartalmazza a teszt célját, hatókörét, a végrehajtásához szükséges erőforrásokat és költségvetést. Ez a terv magába foglalva kommunikáció rendjét valamint a mérvadó tevékenységek koordinálását rendszeres áttekintést biztosíthat a teszt folyamatáról.

3.3 DOKUMENTÁCIÓ ÉS JELENTÉS

A penetrációs teszt elvégzésének végéhez közeledve, fontos egy, az írásbeli jelentéssel bíró dokumentáció, amely többek között tartalmazza a teszt során feltárt megállapításokat, valamint az ajánlott helyreállítási technikákat, és igazodik a Magyar Honvédség dokemuntációkezelési felépítéséhez. Ez a jelentés a vezetés számára helyreállítási ütemtervet biztosít, és a penetrációs teszt fontos tárgyaként szolgál. A dokumentáció reprezentálhatja a teszt befejezését is.

3.3.1 A penetrációs tesztjelentés

Nincs olyan univerzális sablon, amelyet be kell tartani a penetrációs tesztjelentés megtervezésekor. Függetlenül attól, hogy egy esetlegesen már kialakult sablonból indulunk-e ki, jó gyakorlat, ha a jelentést több fontos szakaszra osztjuk. A penetrációs tesztjelentések egyik közös szerkezete a következő szakaszokat tartalmazza sorrendben:

- vezetői összefoglaló;
- megállapítások és orvoslás;
- módszertan;
- következtetés.

3.3.1.1 A vezetői összefoglaló

A vezetői összefoglaló messze a jelentés legfontosabb része. Gyakran ez az egyetlen szakasz, amelyet sokan el fognak olvasni, ezért azt úgy kell megírni, hogy a jelentés összes fontos következtetését világosan érthető módon közvetítse. A szakasz címe a közönséget is leírja: vezetői. Tehát nem feltétlenül technikai beállítottságú emberekről van szó. Itt nem szükséges, vagy sokszor nem szabad mélyen értelmezni a penetrációs tesztelési módszertan technikai részleteit. Lehetőleg egyszerűen fel kell tárni a fenyegető kockázatokat és azokra magyarázatot adni. A vezetői összefoglalót tömören érdemes megtartani, célszerű ezt a szakaszt csak pár oldalas verzióban elkészíteni. Az összefoglaló lehet, hogy az első szakasz, amely megjelenik az írásbeli jelentésben, de ez legyen az utolsó szakasz, amely megírásra kerül. A penetrációs tesztjelentés többi részének elkészítése segít véglegesíteni a megállapításokat, kidolgozni a helyreállítási javaslatokat és megérteni a kontextust.

3.3.1.2 Megállapítások és orvoslás

A megállapítások és a helyreállítási szakasz a behatolási vizsgálati jelentés magja. Itt kerülnek ismertetése a penetrációs teszt során felfedezett biztonsági kérdések, és javaslatok fogalmazódnak meg arra vonatkozóan, hogy a szervezet hogyan orvosolhatja ezeket a problémákat a kiberbiztonsági kockázat csökkentése érdekében.

3.3.1.3 A módszertan

A jelentés módszertani szakasza lehetőséget kínál arra, hogy a technikai részletek mélyen elemezve megjelenjenek. Az elvégzett tesztelés típusai, az alkalmazott eszközök és az elvégzett megfigyelések kerülnek elmagyarázásra ebben a részben. A jelentés ezen szakaszának közönsége abból a technikai szakállományból áll, akik áttekintik az eredményeket, és az

eredmények alapján intézkednek. Ideális esetben egy képzett biztonsági szakembernek képesnek kell lennie arra, hogy a jelentés módszertani részét elolvasva, felhasználva az eredményeket, reprodukálja azt. Bár a módszertan szakaszának technikai részletekbe kell kimerülnie, nem célszerű hosszú kódlistákat, vizsgálati jelentéseket vagy más unalmas eredményeket felvenni ebbe a szakaszba. Ha ezek az elemek fontosak a jelentés szempontjából, a függelékbe kell elhelyezni azokat, majd egyszerűen utalni kell a jelentés törzsében található függelékre.

3.3.1.4 A következtetés

Össze kell foglalni a következtetéseket, és ajánlásokat kell megfogalmazni a további munkához. Például, ha a penetrációs teszt hatóköre kizárja a webalkalmazások tesztelését, akkor javasolható, hogy ezt a tesztet a végrehajtás során mégis végre kell hajtani. A következtetés arra is jó, hogy a jelentésben azonosított kockázati besorolások a szervezet kockázatvállalási hajlandósága érdekében összehasonlításra kerüljenek. A menedzsmentnek kockázatalapú döntéseket kell hoznia arról, hogy hol alkalmazza a korlátozott kármentesítési erőforrásait az egyes kockázati besorolások jellege és a szervezet kockázattűrése alapján.

3.3.1.5 A jelentések biztonságos kezelése és megsemmisítése

A penetrációs tesztjelentések gyakran rendkívül érzékeny információkat tartalmaznak egy szervezetről. A jelentés módszertani szakasza tartalmazza azokat a részletes lépéseket, amelyeket a tesztelők a szervezet biztonságának veszélyeztetése érdekében követtek. Ezek az utasítások útitervként szolgálhatnak egy támadó számára, aki hozzáférést kíván kapni a szervezethez.

A behatolási tesztek másolatának felfedezése a végső győzelem a szervezet felderítését végző támadó számára. Ezért rendkívül fontos, hogy bárki, aki hozzáfér a penetrációs tesztjelentéshez, biztonságosan kezelje azt. A jelentéseket csak titkosított formában szabad továbbítani és tárolni, a papír példányokat pedig zár alatt kell tartani. A jelentés digitális és papíralapú példányait biztonságosan meg kell semmisíteni, ha azok már nem szükségesek. A behatolási teszt megállapodásnak világosan meg kell határoznia a jelentés tárolási idejét. Ha ez az idő lejár, a jelentést biztonságosan törölni kell.

3.3.2 A kötelezettség befejezése

A penetrációs teszt jelentésének elkészítése minden bizonnyal a mérföldkő az elkötelezettségben, és gyakran a projekt végének tartják.

A penetrációs tesztelő munkája azonban nem zárul le egyszerűen azért, mert leadták a jelentést. A tesztelőknek a projekt lezárása előtt be kell fejezniük a jelentést követő fontos tevékenységeket.

3.3.2.1 Kötelezettség utáni takarítás

A penetrációs tesztelők sokféle eszközt és technikát alkalmaznak, miközben az ügyfélhálózaton keresztül dolgoznak. Ezek a tevékenységek gyakran maradványokat hagynak maguk után, amelyek maguk is veszélyeztethetik a biztonságot. A megbízás során a tesztelőknek egyértelműen dokumentálniuk kell a rendszerekben végrehajtott minden változtatást, és a teszt végén újra meg kell vizsgálniuk ezt a dokumentációt annak biztosítása érdekében, hogy teljesen eltávolítsák munkájuk nyomát.

Három fontos elkötelezettség utáni takarítási tevékenység:

- A behatolási teszt során a rendszerekre telepített shellek eltávolítása;
- A teszt során a tesztelők által létrehozott fiókok, hitelesítő adatok vagy hátsó ajtók eltávolítása;
- A behatolási teszt során alkalmazott tool-ok eltávolítása.

Természetesen ez a három cselekvés csak kiindulópont. Az az alapelv, amelyet a tesztelőknek be kell tartaniuk az elkötelezettség utáni tisztítás során, hogy vissza kell állítaniuk a rendszert az eredeti, tesztelés előtti állapotába.

3.3.2.2 Adott szervezet jóváhagyása

Meg kell szerezni az adott szervezet hivatalos jóváhagyását a teljesítéshez. Ez lehet egyszerűen a zárójelentés írásbeli visszaigazolása, de tipikusabban személyes találkozót is magában foglal, ahol a tesztelők megvitatják az együttműködés eredményeit a vezetőkkel, és válaszolnak a felmerülő kérdésekre. A jóváhagyás a kliens elkötelezettségének végét jelenti, és az a hivatalos megállapodás, hogy a tesztelők sikeresen teljesítették a megbeszélt munkakört.

3.3.2.3 Tanulságok

Egy csapat akár évente egy, akár hetente több penetrációs tesztet végez, mindig van mit tanulni magából a folyamatból. A csapattagoknak szabadon kell beszélniük a tesztről, és javaslatot kell tenniük a fejlesztésre. A levont tanulságok irányított átbeszélése jó alkalom arra, hogy bemutassák a teszt során alkalmazott minden olyan innovatív technikát, amelyet a jövőben fel lehet használni.

A penetrációs tesztjelentés a végtermék, amely a teszt tárgyaként szolgál, és közli a vezetéssel a módszertant, a megállapításokat, az ajánlott javításokat és következtetéseket. A

jelentésnek tartalmaznia kell egy egyszerű nyelvezetű összefoglalót is, amely elérhető a nem műszaki vezetők számára, segítve őket megérteni a teszt célját és eredményeit, valamint a szervezetet fenyegető kockázatokat. [85]

Együttvéve a következtetést levonva megállíptható, hogy a penetrációs tesztnél teljeskörű lezárásához a dokumentáción túl több kisebb folyamatot kell végrehajtani. Ezek maradéktalanul szükségesek az infokommunikációs rendszer biztonságának értékeléséhez, annak növeléséhez, esetleges korrektiváló tevékenységek végrehajtásához.

3.4 KÖVETKEZTETÉSEK

E fejezetben a hazai jogi szabályzók segítségével **meghatároztam** a penetrációs teszt módszertanának a Magyar Honvédséggel való kapcsolatát működési és szervezeti szinten, valamint **definiáltam a teszt katonai jellegét.**

A nemzetközi leírások, feldolgozásával és az azokkal kapcsolatos kutatási eredményekre építve **javaslatot tettem** a penetrációs teszt munkafolyamatára, **meghatároztam** annak tervezésének és előkészítésének nehézségeit, valamint a dokumentáció és jelentés fontosságát.

Mindezekre támaszkodva **kialakítottam** a különböző elemeit egy kiberműveleti penetrációs teszt terv dokumentumnak. Ez a dokumentum tartalmazza a teszt célját, erőfeszítését, a korlátozásokat, a változások vezérlését, valamint a kommunikáció és a kulcsfontosságú tevékenységek koordinálását.

Meghatároztam a hatókör kérdéskörét, melyben részletezem a célt, a kezdő és a záró dátumok megadását, valamint az IP cím tartomány behatárolását.

Meghatároztam a kommunikációs csatornák követelményeit.

Meghatároztam és bemutattam az általános feltételeket és a kötelezettségek elemeit, tulajdonságait.

Megalkottam azt a dokumentáció és jelentési rendszert, mely figyelembe veszi a Magyar Honvédség struktúráját.

A fejezet eredményei alapján az alábbi következtetéseket fogalmazom meg:

1. A katonai rendszerek ma már digitális rendszerek. Ahogyan jelenlegi munkakörömben (NSPA CIS Operations Officer a SAC katonai programon belül) eltöltött idő tapasztalata is alátámasztja, alapvető követelmény a katonai digitális infokommunikációs hálózatokkal szemben a penetrációs teszt. Tehát a penetrációs teszt elengedhetetlen, ha meg akarjuk védeni katonai infokommunikációs rendszerünket.

Ezen felül e tapasztalatok támpontot is adhatnak arra, hogy a szembenálló felet mely kibertéri rétegben és hogyan kellene vagy lehetséges támadni. A kibertérben való katonai infokommunikációs rendszerek támadása pedig akkor is katonai tevékenységnek minősül, ha azt nyílt forráskódú technikákon keresztül valósítjuk meg.

2. A jelenlegi hazai jogszabályok és szabályzók alapján a Honvédelmi Minisztérium a KNBSZ keretein belül működteti saját, honvédelmi célú zárt és nyílt rendszerei kibervédelmét biztosító szervezetét. A Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ a KNBSZ szervezetében működő ágazati szervezet, amely támogatja a honvédelmi célú informatikai rendszerek biztonságát, a bekövetkező biztonsági események ágazati szintű kezelését, és a sérülékenység vizsgálatok végrehajtását.
3. A kiberműveleti penetrációs teszt módszertan, egy alapvető keretet nyújt a fontos kezdeti és vizsgálat utáni információk lefektetésében, melyet az egyes alakulatok felhasználhatnak a KNBSZ által elvégezni kívánt auditok, ellenőrzések előtti felkészülésre. A kiberműveleti penetrációs teszt terv és tesztjelentés alkalmazása lehetővé teszi a hatékonyabb információáramlást, a döntéshozói és a végrehajtói szintek eredményesebb együttműködését, a közös feladat-végrehajtását az informatikai biztonság és kiberbiztonság területén.

A módszertan megalkotását követően értekezésem témaválasztásának alapján **azt kell kutatásaim fókuszába emelni**, hogy milyen módon lehet végrehajtani a hálózati felderítés technikai lépéseit a képességfejlesztési célok elérésére. Ennek érdekében a következő fejezetben meghatározott technikai lépésekkel kívánom demonstrálni a hálózati felderítés jelentőségét, amely érinti a kibertér mindhárom rétegét. Meghatározott tesztkörnyezetben végrehajtott méréseket végzek, összpontosítva a közétett adatok és DNS információk kinyerésére, a célpont felfedésére és a portszkennelésre.

4 HÁLÓZATI FELDERÍTÉS A PENETRÁCIÓS TESZTBEN

Jelen fejezetben a penetrációs tesztek szakaszán belül a hálózati felderítés szintjeinek bemutatásával foglalkozom, ezen belül a penterációs teszt modellnek a hálózati felderítés szakaszát szemléltetem előre meghatározott módszerekkel, technikai lépésekkel, előre meghatározott virtualizációs tesztkörnyezetekben.

A virtualizáció a szűkebb értelemben több számítógép emulációja egy fizikai számítógépen, másszóval hardverek emulációja szoftveres környezetben. Ez a fajta virtualizáció az úgynevezett teljes virtualizáció, mely lehetővé teszi egy eszköz erőforrásainak felosztását több környezet között. A virtualizációs technológiák legfontosabb céljai:

- A meglévő erőforrások kihasználtságának maximalizálása;
- A meglévő rendszerek kezelésének egyszerűsítése, költségeinek csökkentése;
- Az IT szolgáltatások rugalmasságának fejlesztése;
- A rendszerek biztonságának növelése, és a szükséges leállások idejének minimalizálása.

A hálózati felderítési technikákat különböző programok segítségével vagy parancssoros alkalmazások révén hajtottam végre. Ezen felül több megközelítési mód is létezik, saját tevékenységeim során szubjektív okokból választottam a majd később megemlített programokat, parancsokat.

A vizsgálat célja:

- Megvilágítani a hálózatbiztonság és a hálózati felderítés fontosságát;
- Felhívni a figyelmet a támadások egyszerűségére és a folyamatuk, illetve leírásuk könnyű elérésére;
- A támadó nézőpontjából bemutatni a támadási folyamatokat, programokat, a használt lehetőségeket;
- Rávilágítani milyen információk nyerhetők ki a felderítési szakasz folyamán, melyeket később a penetrációs teszt modelljének, módszertanának folytatásával hatékonyan fel lehet használni.

Hálózati Felderítés lépései:

- Információgyűjtési technikák;
    - A közzétett adatok elemzése;

- Alapvető DNS-információk lekérdezése és vizsgálata.

- Hálózat feltérképezés;
  - Célpont felfedés;
  - Port szkennelés;
  - IDS/tűzfal-kijátszási technikák;
  - Távoli operációs rendszer detektálása;
  - Felsorolási technika- Enumeration;
  - Hálózati forgalom lehallgatás és elkapás.

Jelen fejezet az Információgyűjtési technikák egy részét, valamint a Hálózatfeltérképezésen belül a célpontfelfedés, portszkennelés és snmp felsorolási technika egy szeletét hivatott demonstrálni.

4.1 INFORMÁCIÓGYŰJTÉSI TECHNIKÁK

Az egyik alapvető szemlélet szerint a kiberműveletekben és az informatikában vett penetrációs tesztek felderítési szintjén lévő információgyűjtési tevékenységek azonosítják (kockázati szinten) a szervezetekhez kapcsolódó, a nyilvánosság számára hozzáférhető információkat. Az információgyűjtés a penetrációsteszt-végrehajtás lépésének első szakasza, amely a célhálózatról és célkörnyezetről való információk begyűjtését takarja. Az információgyűjtési technikákat használva számos lehetőség nyílik a célszervezet hálózatának illetéktelen hozzáférésére. Ennek segítségével létrehozható egy biztonsági profil a célszervezet hálózatáról, rendszeréről és részben magáról a szervezetről is. Nincs egységes módszer az információgyűjtésre, hiszen azok számos módon beszerezhetők. Viszont a lehető legtöbb információt be kell gyűjteni, így érdemes ezt a fázist szervezett módon végrehajtani. [86]

Az információgyűjtés a penetrációsteszt-végrehajtás lépésének első szakasza, amely a célhálózatról és célkörnyezetről való nyilvános információk begyűjtését takarja, informatikai és informatikához kapcsolódó technikákon, módszereken keresztül. Az információ gyűjtése magában foglalja a kibertéri műveletek közül az elektronikai felderítés OSINT[51]-fajtáját, amely

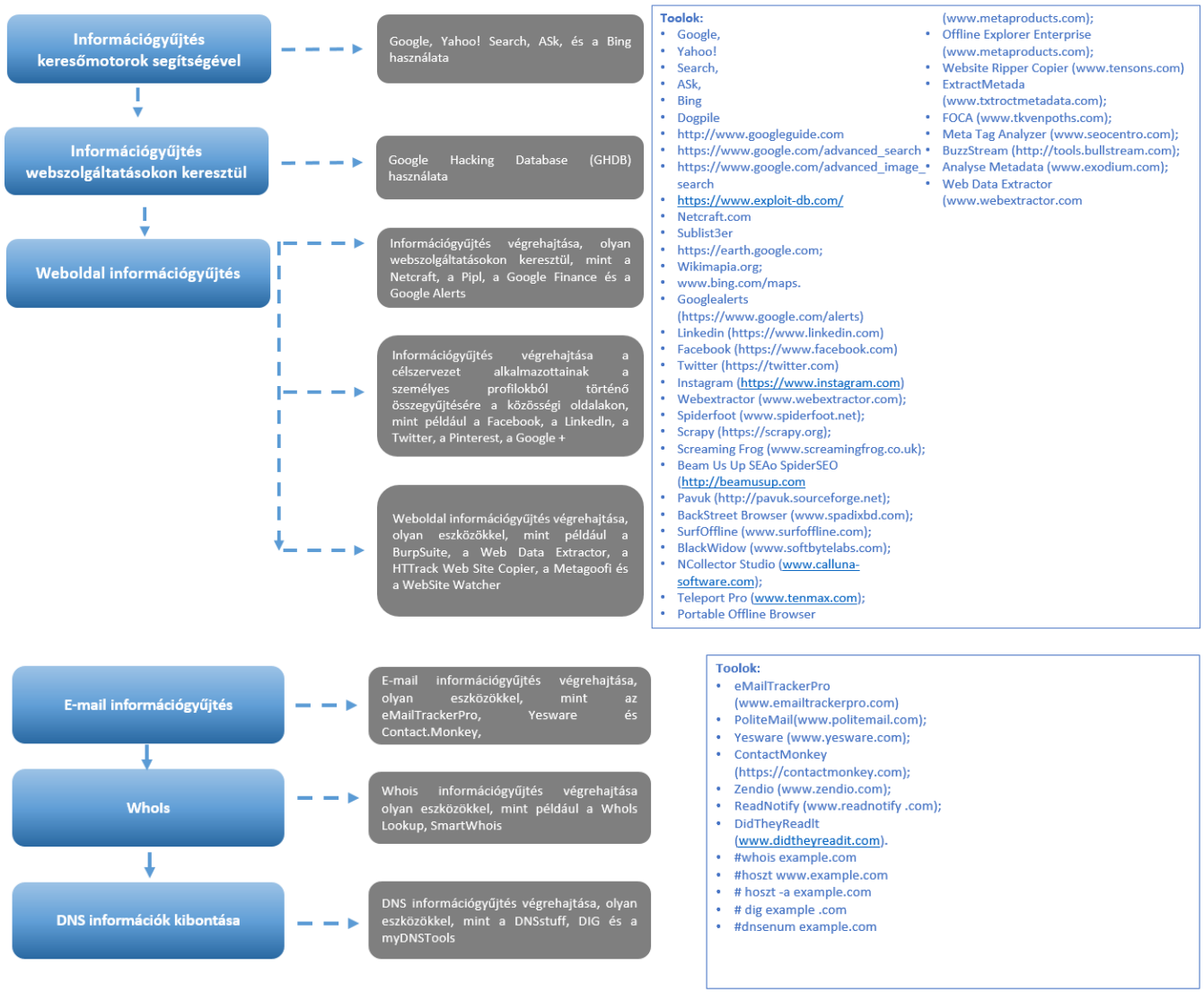
[51] Az OSINT (Open Source Intelligence) a nyílt forrású hírszerzés nemzetközileg is elfogadott angol nyelvű rövidítése. Az OSINT fő forrásait a NATO OSINT kézikönyve a következők szerint határozza meg:
- nyomtatott és elektronikus média;
- internet, beleértve a láthatatlan web információit;
- kereskedelmi (fizetős) online szolgáltatók tanulmányai, adattárai;
- „szürke irodalom", azaz nem publikált, de nem is minősített, szűk körben hozzáférhető, nyomtatott és digitális dokumentumok, tanulmányok;
- személyes tapasztalatok;

a széles körben hozzáférhető, nyílt adatforrások felhasználásával gyűjt adatokat, illetve a számítógéphálózati műveletek felderítés fajtáját, melyeknek fogalmát Haig Zsolt az Információs műveletek a kibertérben című publikációjában definiálta: „*A számítógép-hálózati felderítés a hálózatok struktúrájának feltérképezését, az adatbázisokhoz való illetéktelen hozzáférést és a támadható pontok meghatározását jelenti. Megvalósulhat a szemben álló fél számítógépes rendszereibe való szoftveres vagy hardveres úton való behatolással. Célja az adatbázisokban tárolt adatokhoz, információkhoz való hozzáférés és azok felderítési céllal való hasznosítása, illetve a későbbi károkozással járó támadás kivitelezéséhez a hálózat támadható pontjainak és a támadás leghatékonyabb formáinak meghatározása. A felderítés az elszenvedő hálózat részéről általában nem észlelhető formában valósul meg, így a hálózat üzemeltetője és felhasználója számára a felderítés ténye többnyire nem ismert*”. [18]

A 6. ábrán **kutatásaim alapján megalkottam a közzétett adatok elemzésének lépéseit,** melyeket technikai kommentárokkal, iránymutatásokkal, valamint javasolt tool-ok eszköztárával láttam el:

- Információgyűjtés keresőmotorok segítségével;
- Információgyűjtés webszolgáltatásokon keresztül;
    - A célpont legfelső szintű domain-jei és aldomain-jei;
    - A cél földrajzi helyzetének megkeresése;
    - Információgyűjtés közösségi oldalakon keresztül;
    - A cél figyelése riasztással;
    - Információgyűjtés fórumok, blogok segítségével.
- Weboldal információgyűjtés;
    - A HTML-forráskód vizsgálata;
    - Sütik vizsgálata;
    - Web spider programok használata;
    - Teljes webhely tükrözése;
    - Metaadatok kibontása nyilvános dokumentumokból.
- E-mail-információgyűjtés;
    - Információ gyűjtése az e-mail-fejlécből;
    - E-mail-követő tool-ok .

- kereskedelmi műholdak felvételei. Ezek pontossága a 21. században gyakran megközelíti a katonai műholdak teljesítményét;
- tudományos kutatószervezetek, egyetemek.

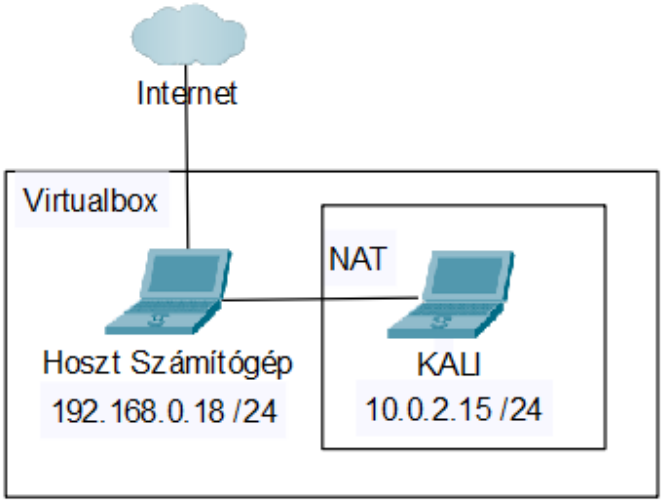


6. ábra *Az információgyűjtés teljes folyamata (saját szerkesztés)*

Az alábbiakban a kiberműveletek részeinek is tekinthető penetrációs teszt módszertanon belül **a hálózati felderítésnek az információgyűjtési technikáit mutatom be**, melyeknek **reprodukálható informatikai mérésekkel, vizsgálatokkal és végrehajtásokkal bizonyítom használhatóságát, valamint létjogosultságát.**

Ehhez a következő laborkörnyezetet használom:
Topológia 1. – Közétett adatok információgyűjtése
Szükséges erőforrások:

- Kali Linux operációs rendszer;
- Internet elérés;
- Hoszt számítógép legalább 8 GB RAM-mal és 45 GB szabad lemezterülettel.



7. ábra *Közétett adatok információgyűjtése teszkörnyezet (saját szerkesztés)*

Virtuális gép	Operációs rendszer	OVA méret	Lemez terület	RAM	IP ím
Kali	Kali Linux	4.1GB	10 GB	1 GB	192.168.1.89/24

1. táblázat: Közétett adatok információgyűjtése teszkörnyezet (saját szerkesztés)

4.1.1 A közzétett adatok elemzése

A kiberműveletek képességein belül a számítógép-hálózatokba való bejutást, azok felderítését, az adatbázisokhoz való hozzáférést, azok módosítását, tönkretételét, valamint a távközlési hálózatok lehallgatását a közzétett adatok elemzésével érdemes kezdeni. Az

információgyűjtés-módszertan egy eljárás a célszervezettel kapcsolatos információk gyűjtésére az összes kibertérben rendelkezésre álló forrásból. A közétett adatok elemzése megmutatja a célszervezettel kapcsolatos információkat, mint például az URL helyét, a telephely adatait, az alkalmazottak számát, a domain nevek konkrét tartományát, elérhetőségi adatait és egyéb kapcsolódó információkat. Itt nem feltétlenül technikai információk begyűjtése a cél, inkább a keresési mechanizmus legjobb hatásfokkal való alkalmazása.

4.1.1.1 Információgyűjtés keresőmotorok segítségével

Az internetes keresőmotorok a fő források a célszervezettel kapcsolatos kulcsinformációk megkereséséhez. A keresőmotorok, kinyerhetik a célokról szóló információkat, beleértve például technológiai platformokat, alkalmazottak adatait, bejelentkezési oldalakat, intranetportálokat, elérhetőségeket és így tovább. Ezért fontos szerepet töltenek be a kritikus részletek felderítése terén, hiszen ezek a viszonylag egyszerűen kinyert információk képezhetik az alapját vagy előkészületét egy támadás indításának. Egyfajta információs adatbázist képezhetnek, amelyből szükség esetén már összegyűjtve és nagyobb támadáshoz rendszerezve, előkészítve lehet meríteni a támadások támogatásához. Ez az információ segíti a támadót a social engineering és más típusú támadások végrehajtásában. A keresési eredmények böngészései gyakran értékes információkat nyújtanak például a fizikai helyről, elérhetőségekről, a szolgáltatásokról, az alkalmazottak számáról és így tovább.

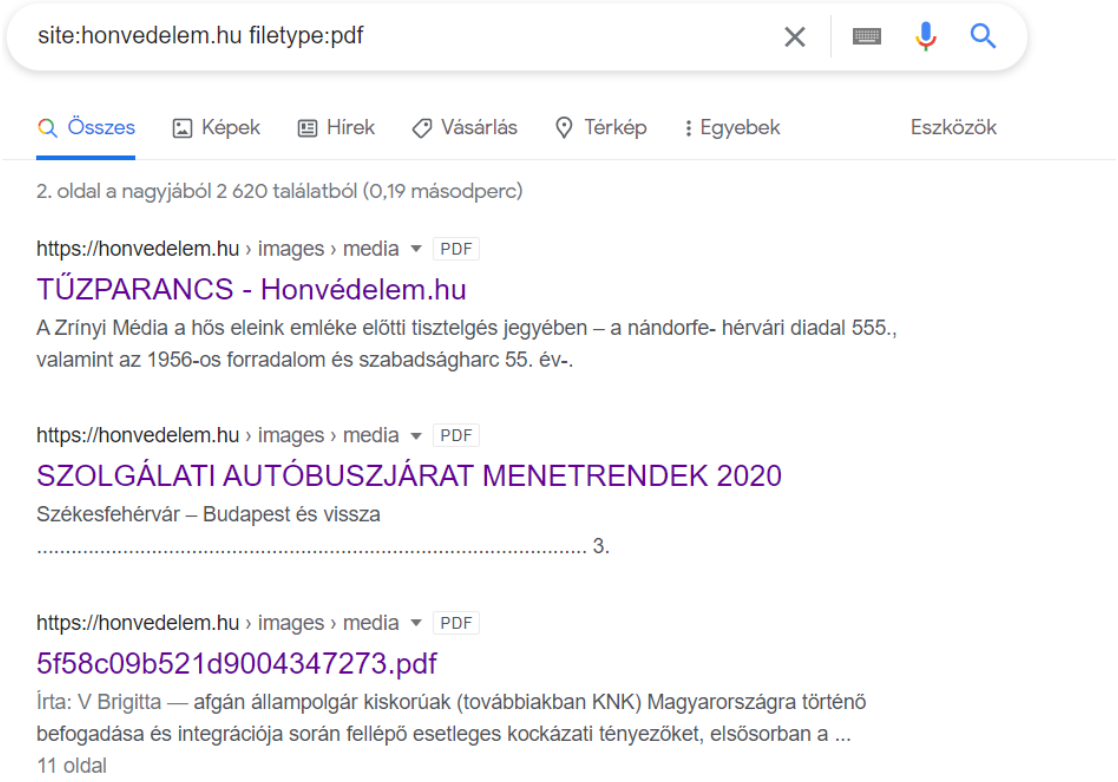
A támadók [87] az ezekkel a keresőmotorokkal elérhető speciális keresési operátorokat használhatják, és létrehozhatnak kötelező lekérdezéseket a célhoz kapcsolódó információk keresésére, szűrésére és rendezésére. A Google ackelés mint kifejezés, a fejlett Google keresési operátorok használatára utal - amelyek az 8. ábrán is láthatók - annak érdekében, hogy összetett keresési lekérdezéseket hozzon létre az érzékeny vagy rejtett információk kinyerésére. Ezután a támadók a hozzáférhető információkat a sebezhető célok felkutatására használják. Az információgyűjtés fejlett Google-hackelési technikákkal történő összegyűjtésével a Google a keresési eredmények speciális szövegrészeit egy speciális operátor és a Google keresőmotorja segítségével hajtja végre. Google-operátorok segítenek megtalálni a szükséges szöveget és elkerülni az irreleváns adatokat, azaz segítenek a keresési lekérdezés szűkítése, a legrelevánsabb és pontosabb kimenet elérése érdekében.

A keresőmotoros információgyűjtés napjaink egyik legalapvetőbb információbeszerzési módszere. Az internet széles körű elterjedése és globális tulajdonsága miatt a legkönnyebben és legegyszerűbben használható információforrás. A rajta lévő keresőmotoroknak

információszerzésre való kifinomult, részletes és tudatos használata a penetrációs teszt feladatvégrehajtásában jelentős könnyítéseket, előkészületi fázisokat, annak a már-már készségszinten való használatát teszi lehetővé. A keresőmotorok megfelelő hatásfokkal való használata keresési időt, erőforrást takaríthat meg, valamint leszűrheti a lényegtelen, nem releváns információkat. Ezek a felesleges többletinformációk hátráltatást jelentenek egy munkafolyamat során. Egy kiberműveleti penetrációs teszt munkafolyamatának szemszögéből az effektív munkavégzést segíti.

Egyszerű operátorok	Haladó operátorok
Filetype: • Csak a megadott kiterjesztésű (például PPT, pdf) fájlokat adja vissza a Google.	Allintext/intext: • Az allintext kifejezést a keresés elején kell használni. Csak olyan oldalakat fog visszaadni a Google, ahol a szövegben minden szó szerepel, ami az allintext után van írva.
Site: • Csak a megadott domainen belül fog keresni és találatokat adni. A „site" operátort ki lehet egészíteni kifejezésekkel is, és akkor csak az adott oldalon belül fog keresni a megadott kifejezésekre.	Intitle /allintitle: • Működése teljesen hasonló az intext/allintext párosához, annyi a különbség, hogy itt a keresés a címben történik.
Related: • Ennek az operátornak a segítségével meg lehet találni egy adott oldalhoz hasonló oldalakat. Fontos megjegyezni, hogy csak domainekkel és URL-ekkel működik, keresőszavakkal nem. Illetve, ha a kettőspont után szóköz kerül, akkor csak egy sima keresés lesz. Ez főleg angol nyelvű oldalak esetében működik jól.	Inurl/allinurl: • Az előző kettőhöz hasonlít ezeknek az operátoroknak is a működése, viszont itt a keresés az URL-ben történik.
Cache: • Ennek az operátornak a segítségével meg lehet nézni egy adott oldalnak a Google által utoljára eltárolt (cache-elt) változatát. Hasznos lehet olyan oldalak esetében, amelyeket már esetleg valamilyen okból töröltek.	Inanchor/allinanchor • Ennek a párosnak az esetében pedig a keresés a horgonyszövegekben történik.
Define: • A keresett kifejezésnek a definícióját dobja ki a Google. Csak angol kifejezések esetében működik.	
Location: • Akkor érdemes ezt az operátort használni, hogyha egy adott földrajzi helyre szűkítve történik a keresés.	

8. ábra *Főbb operátork [102]*



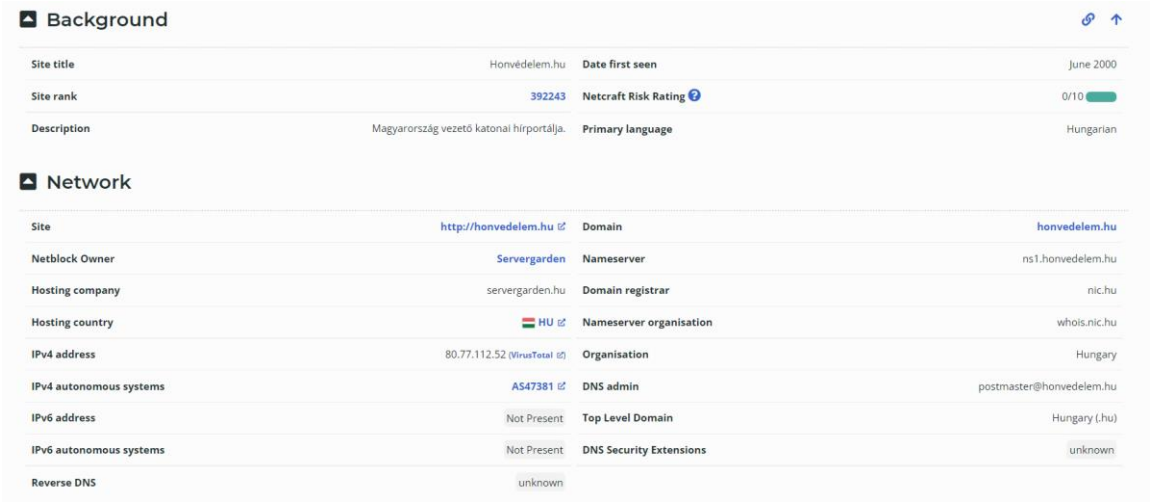
9. ábra *Speciális keresés a honvedelem.hu weboldalon (saját szerkesztés)*

A site: és filetype: segítségével csak a honvedelem.hu domain-en belül, csak a pdf kiterjesztésű fájlokra kerestem rá. 20. oldalig vizsgáltam az eredményt, melyből a következő következtetést vontam le: Mivel általában csak publikus folyóiratot találtam, kivéve egy 2020. évi autóbuszjárat menetrendet, - melyet nem sorolok az infokommunikációs rendszerek biztonsági teszteléséhez való közvetlenül felhasználható információnak – a domain erre a speciális keresésre vonatkozóan biztonságosnak minősül. Nehéz a teszteléshez felhasználható információt kinyerni.

4.1.1.2 Információgyűjtés webszolgáltatásokon keresztül

Ennél a tesztnél a célpont legfelső szintű domain-jeire és aldomain-jeire összpontosítottam. Tehát a cél földrajzi helyzetének megkeresésére, valamint a közösségi oldalakon, fórumokon, blogokon és riasztásokon keresztüli információgyűjtést nem demonstráltam. A vállalati felső domain és aldomain-ek sok hasznos információt nyújthatnak a támadó számára. A nyilvános webhelyeket arra tervezték, hogy megmutassák egy szervezet jelenlétét az interneten. Ingyenesen elérhetők és bárki el is érheti azokat, az ügyfelek és partnerek vonzására szolgálnak. Tartalmazhatnak olyan információkat, mint például a

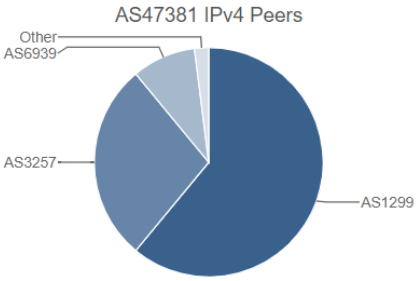
szervezeti előzmények, szolgáltatások és termékek, valamint elérhetőségi adatok. A Netcraft internetes biztonsági szolgáltatásokat nyújt, ideértve a csalás és az adathalászok, az alkalmazások tesztelését és a PCI-szkennning[52] szolgáltatásait is. Elemzi továbbá a webszerverek, az operációs rendszerek, a hoszt-szolgáltatók és az SSL-tanúsító[53] hatóságok piaci részesedését és az internet egyéb paramétereit.



10. ábra *NETCRAFT oldalon keresztüli információgyűjtés Forrás: Netcraft.hu (Letöltés időpontja: 2021.11.19.)*

A kinyert információkból levontam azt a következtetést, miszerint a weboldalt hosztoló cég a servergarden.hu és az ország Magyarország.

Ezen felül megtudtam az oldal IP címét, az Autonóm Azonosító számot, illetve a névszerver nevét: 80.77.112.52, AS47381, ns1.honvedelem.hu Megvizsgálva az AS számot megállapítottam a peer-ek számát, amely leírja a kapcsolódási pontokat.

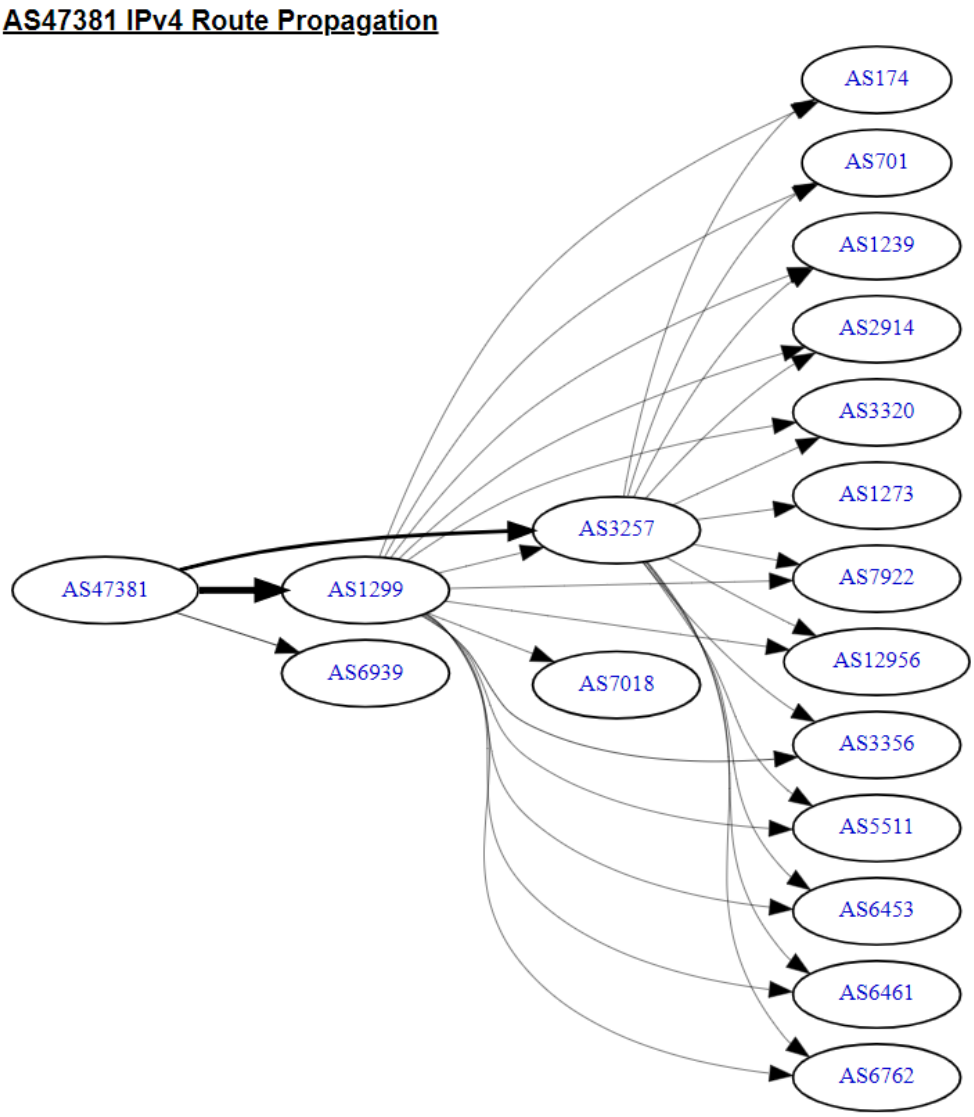


ASN	Name
AS1299	Telia Company AB
AS3257	GTT Communications Inc.
AS6939	Hurricane Electric LLC

11. ábra *AS Peer-ek vizsgálata Forrás: https://bgp.he.net/AS47381#_asinfo (Letöltés időpontja: 2021.11.19.)*

[52] A PCI-vizsgálat általában a negyedéves külső sebezhetőségi vizsgálatokra vonatkozik, amelyeket a PCI-jóváhagyott gyártónak kell elvégeznie. A PCI (Payment Card Industry) adatbiztonsági szabványa a Visa és a MasterCard közötti együttműködés eredményeként jött létre, hogy közös ipari biztonsági követelményeket hozzon létre.

[53] Az SSL tanúsítványok arra szolgálnak, hogy létrejöhessen egy biztonságos, titkosított csatorna a kliens és a szerver között. Bizonyos információknak, mint a hitelkártya adatok, fiókbelépéshez szükséges adatok és egyéb kényes információk átvitelének titkosítás alatt kell történnie..



12. ábra *AS Peer-ek vizsgálata https://bgp.he.net/AS47381#_graph4 (Letöltés időpontja:2021.11.20.)*

A jelenlegi és korábbi szerver típusát és operációs rendszerének információt is sikerült kinyernem, amiból egyértelműen megállapítható, hogy a Honvedelem.hu webszervere Linux platformon ngnix-es típusú webszerver alapokon üzemel:

Netblock owner	IP address	OS	Web server	Last seen
Servergarden Shared Server Hosting	80.77.112.52	Linux	nginx	5-Nov-2021
23VNet - Serverhosting range	94.199.48.179	Linux	Apache/2.2.9	7-May-2011

13. ábra *A célzott webszerver platformja (Letöltés időpontja:2021.11.20.)*

4.1.1.3 Weboldal információgyűjtés

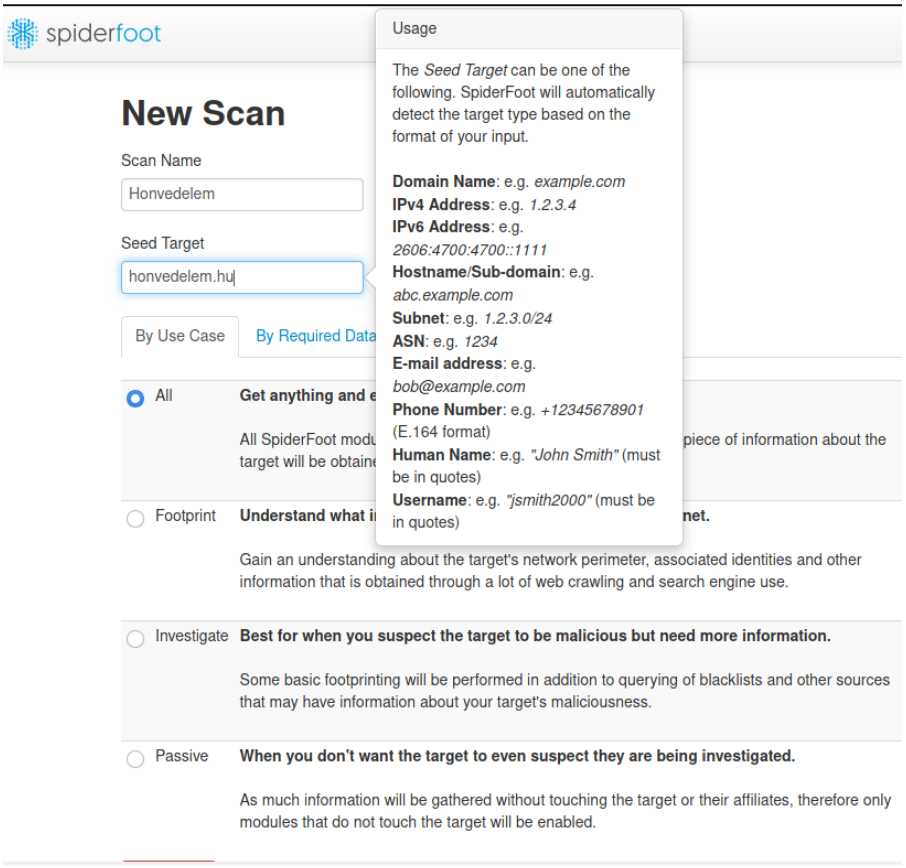
A webhelyről való információgyűjtés a célszervezet weboldalának figyelemmel kísérése és elemzése. Itt már a technikai információk kinyerése is a célok között szerepel. A támadó elkészítheti a weboldal szerkezetének és architektúrájának részletes térképét anélkül, hogy a rendszergazda gyanúját felkeltené.

A céloldal böngészése jellemzően a következő információkat nyújtja:

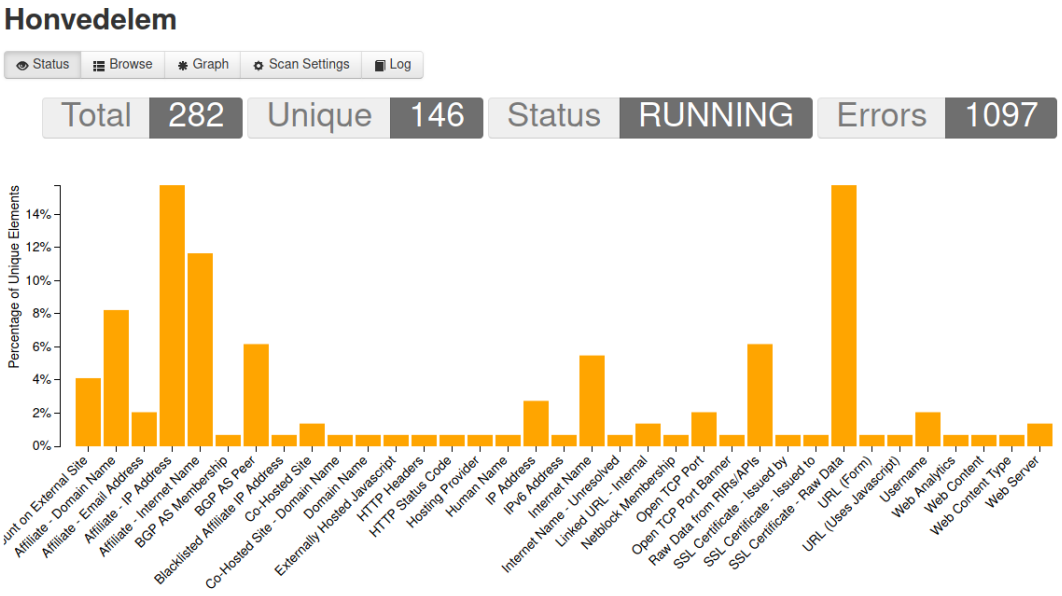
- Használt szoftver és verziója: A támadó könnyedén megtalálja a használt szoftver-verziót;
- Használt operációs rendszer: Általában a használt operációs rendszer is meghatározható;
- Alkönyvtárak és paraméterek: A keresések feltárják az alkönyvtárakat és a paramétereket azáltal, hogy feljegyezik az URL-eket, miközben a célwebhelyet böngészik;
- Fájlnév, elérési út, adatbázis-mezőnév vagy lekérdezés: A támadó gyakran alaposan vizsgál minden olyan lekérdezést, amely fájlnév, elérési út, adatbázis-mezőnév vagy lekérdezésnek tűnik, annak ellenőrzése érdekében, hogy az lehetőséget kínál-e az SQL-befecskendezéses támadásra;
- Szkripting platform: A szkriptfájlnév-kiterjesztések segítségével, például .php,, .asp vagy .jsp, könnyen meghatározható a szkript[54] platform, amelyet a célwebhely használ;
- Kapcsolatfelvételi részletek és CMS[55]-adatok: A kapcsolattartó oldalak szokásos részleteket tartalmaznak, például neveket, telefonszámokat, e-mail-címeket és az adminisztrátorok vagy támogató személyek adatait. A támadó ezeket az adatokat felhasználhatja social engineering támadások végrehajtására.

[54] Az informatikában a szkript névvel rövid programokat illetnek, amelyek gyakran egy-egy részfeladat automatizálására szolgálnak.

[55] A CMS magyarul tartalomkezelő rendszer, az elnevezésből pedig következik, hogy segítségével a tartalmaidat tudod létrehozni vagy változtatni. A CMS tulajdonképpen egy webes szoftvercsomag a weboldalad kezeléséhez.



14. ábra *SpiderFoot szkenn indítása (saját szerkesztés)*



15. ábra *SpiderFoot szkenn eredménye 1. (saját szerkesztés)*

Honvedelem

Status | Browse | Graph | Scan Settings | Log

Search...

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	6	12	2021-11-06 09:42:11
Affiliate - Domain Name	12	17	2021-11-06 10:02:42
Affiliate - Email Address	3	3	2021-11-06 09:37:21
Affiliate - IP Address	23	23	2021-11-06 09:57:20
Affiliate - Internet Name	17	21	2021-11-06 10:02:41
BGP AS Membership	1	1	2021-11-06 10:02:12
BGP AS Peer	9	9	2021-11-06 10:02:19
Blacklisted Affiliate IP Address	1	1	2021-11-06 09:55:12
Co-Hosted Site	2	4	2021-11-06 09:59:23
Co-Hosted Site - Domain Name	1	2	2021-11-06 09:59:10
Domain Name	1	5	2021-11-06 10:08:24
Externally Hosted Javascript	1	1	2021-11-06 09:40:55
HTTP Headers	2	2	2021-11-06 10:08:13
HTTP Status Code	2	2	2021-11-06 10:08:13
Hosting Provider	1	1	2021-11-06 09:59:18
Human Name	1	1	2021-11-06 09:37:21
IP Address	4	6	2021-11-06 10:08:15
IPv6 Address	1	39	2021-11-06 10:08:23
Internet Name	8	75	2021-11-06 10:08:23
Internet Name - Unresolved	1	1	2021-11-06 09:58:08
Linked URL - Internal	4	4	2021-11-06 10:08:13
Netblock Membership	1	1	2021-11-06 10:02:06
Non-Standard HTTP Header	1	1	2021-11-06 10:08:13
Open TCP Port	4	9	2021-11-06 10:08:23
Open TCP Port Banner	1	2	2021-11-06 10:02:04
Raw Data from RIRs/APIs	10	11	2021-11-06 10:08:23
SSL Certificate - Issued by	1	4	2021-11-06 10:08:23
SSL Certificate - Issued to	2	4	2021-11-06 10:08:23
SSL Certificate - Raw Data	23	43	2021-11-06 10:08:23
URL (Form)	1	1	2021-11-06 09:40:55
URL (Purely Static)	1	1	2021-11-06 10:08:13
URL (Uses Javascript)	1	1	2021-11-06 09:40:55
Username	3	3	2021-11-06 09:41:35
Web Analytics	1	2	2021-11-06 09:40:55
Web Content	2	2	2021-11-06 10:08:13
Web Content Type	2	2	2021-11-06 10:08:13

16. ábra *SpiderFoot szken eredménye 3. (saját szerkesztés)*

A SpiderFoot segítségével olyan adatokat sikerült kinyernem a Honvedelem.hu weboldalról, mint IP címek, BGP kapcsolatok, Domain nevek, nyitott TCP portok, SSL certificate-ek. Mivel nem találtam felesleges nyitott portokat, viszont érzékeltem feltehetőleg előre előkészített támadóknak szánt csali és figyelmeztető al-elemket az oldalt futtató szerveren, megállapítottam, hogy a weboldal megfelelő biztonsági beállításokkal üzemel.

4.1.1.4 További fontos információgyűjtési technikák

A fent végrehajtott információgyűjtésen kívül e szakaszban érdemes kellő figyelmet fordítani a HTML[56]-forráskód vizsgálatára is. A támadók érzékeny információkat gyűjthetnek a HTML forráskódjának megvizsgálásával, valamint a manuálisan beillesztett vagy a CMS-rendszer által létrehozott megjegyzések követésével. A megjegyzések utalást adhatnak a háttérben futó eseményekre. Ez akár a webes fejlesztő vagy az adminisztrátor részletes adatait is tartalmazhatja. [88]

A Sütik[57] vizsgálata is fontos lépés ebben a szakaszban, a futó szoftver és annak viselkedése meghatározásához. Azonosítani lehet a szkript platformokat munkamenetek és más támogató sütik megfigyelésével A sütik nevére, értékére, domain méretére vonatkozó információk szintén kibonthatók.. [89]

Ezen felül a Web spider programok használata is javasolt, amely egy olyan program vagy automata szkript, amely módszeresen böngészi a webhelyeket, hogy összegyűjtse a meghatározott információkat, például a munkavállalók nevét, e-mail-címét és így tovább. [90]

Továbbá egyik lehetőség lehet a teljes webhely tükrözése. Ilyenkor az eredeti webhely pontos mását vagy klónját hozzák létre. A felhasználók a weboldalak másolatát a HTTrack Web Site Copier és az NCollector Studio tükröző tool-jaival is elvégezhetik. Ezek a tool-ok letöltik a weboldalt egy helyi könyvtárba, rekurzív módon felépítve az összesen mappát (HTML, képek, flash, videók és egyéb fájlok) a webszerverről egy másik számítógépre. Természetesen más módszer is alkalmazható, megfelelő weboldalkészítési tudás birtokában, melynek rövid leírása megtalálható Bodnár István és Paráda István Hírvillámban megjelent Jelszó ellopás social engineering, e-mail spoofing és fake url segítségével című kiadványban. [103]

Ezeken felül alapvető lépéshez sorolható az információgyűjtése e-mail fejlécekből. Az e-mail-fejléc tartalmazza a feladó adatait, a routing-információkat[58], a dátumot, a tárgyat és a címzettet. Mindegyik kiváló információforrás a támadó számára a cél elleni támadások indításához. Az e-mail-fejléc megtekintésének folyamata a különböző e-mail-programoktól függ. Az e-mail fejléce a következő információkat tartalmazza:

---

[56] A HyperText Markup Language egy leíró nyelv, amelyet weboldalak készítéséhez fejlesztettek ki. HTML általában szöveges állományokban található meg olyan számítógépeken, melyek az internethez kapcsolódnak. Ezek az állományok tartalmazzák azokat a szimbólumokat, amelyek a megjelenítő programnak leírják, hogyan is kell megjeleníteni illetve feldolgozni az adott állomány tartalmát. Megjelenítő program lehet egy webböngésző vagy levelezőprogram.

[57] A HTTP-süti (általában egyszerűen süti, illetve angolul cookie) egy információcsomag, amelyet a szerver küld a webböngészőnek, majd a böngésző visszaküld a szervernek minden, a szerver felé irányított kérés alkalmával.

[58] Az útválasztás, hálózati forgalomirányítás vagy routing az informatikában annak kiválasztását jelenti, hogy a hálózatban milyen útvonalon haladjon a hálózati forgalom.

- a feladó e-mail-szerver;
- a feladó e-mail-szerverei által kapott adatok és idő;
- a feladó e-mail-szervere által használt hitelesítési rendszer;
- az adatok és az üzenet elküldésének ideje;
- az mr.google.com által kiosztott egyedi szám, amely azonosítja az üzenetet;
- a feladó teljes neve;
- a feladó IP-címe és a cím, ahonnan az üzenet el lett küldve.

A támadó a teljes e-mail fejlécének részletes elemzésével nyomon tudja követni, és összegyűjti ezeket az információkat.

Végül de nem utolsó sorban a kibertér dimenziót is figyelembe véve, fontos megemlteni a közösségi oldalakon keresztüli infromációgyűjtést. Egy adott személyre való keresés a közösségi oldalakon könnyebb, mint ahogy a legtöbb ember gondolná. A közösségi hálózati hálózatok olyan online szolgáltatások, platformok vagy webhelyek, amelyek a társadalmi hálózatok kiépítésére vagy az emberek közötti társadalmi kapcsolatok elősegítésére koncentrálnak. Ezek a webhelyek olyan információkat tartalmaznak, amelyeket a felhasználók profiljukban nyújtanak. Segítik az emberek közvetlen vagy közvetett kapcsolatát egymással, olyan különböző területeken keresztül, mint a közös érdekek, a munkahely és az oktatási közösségek. A közösségi oldalak olyan online szolgáltatások, platformok vagy egyéb webhelyek, amelyek lehetővé teszik az emberek számára, hogy kapcsolatba lépjenek egymással és személyes kapcsolatokat építsenek ki. Az ilyen webhelyek például a LinkedIn, a Facebook, a Twitter, a Google, az Instagram stb. A közösségi oldalak lehetővé teszik az emberek számára az információk gyors megosztását, mivel valós időben frissíthetik személyes adataikat. Minden közösségi hálózati webhelynek megvan a maga célja és funkciója. Az egyik oldal kapcsolatba hozhatja a barátokat, ismerősöket, míg a másik segít a felhasználóknak megosztani a munkahelyi profilokat. A közösségi oldalak mindenki számára nyitva állnak. A támadók kihasználhatják ezt a lehetőséget, hogy érzékeny információkat gyűjtsenek a felhasználóktól, akár a felhasználók böngészésével, akár hamis profil készítésével. Egyes webhelyek lehetővé teszik a felhasználók számára, hogy ellenőrizzék, aktív-e egy fiók, amely ezután információt nyújt a keresett személy állapotáról. A közösségi oldalak lehetővé teszik a támadónak, hogy név, kulcsszó alapján keressen embereket, társaságokat, iskolákat, a célpont barátait, kollégáit és a körülöttük élő embereket. Ezeken a webhelyeken keresve személyes információk érhetők el, például névről, beosztásról, a szervezet nevéről, jelenlegi helyéről és oktatási képesítésekről. Ezen kívül olyan professzionális információkat is találhat, mint például a vállalat vagy az üzleti vállalkozás, a telefonszám, e-mail, fényképek, videók és így tovább. A szociális hálózati

webhelyek, például a Twitter, tanácsok, hírek, aggodalmak, vélemények, pletykák, és tények gyűjtőhelye. A közösségi hálózati szolgáltatásokon keresztüli keresés révén a támadó kritikákat gyűjthet össze, olyan információkat, amelyek hasznosak a social engineering vagy más típusú támadások végrehajtásában. [104]

Összességében megállapítható, hogy a közzétett adatokon keresztül kinyert információk felhasználhatók az infokommunikációs rendszerek kezdeti feltérképezéséhez, alapvető rendszeradatok megszerzéséhez. Ezen túlmenően a kibertér különböző rétegeiben katonai kiberműveleteknek minősülhet, amennyiben a felhasználás célja és kontextusa az ellenféllel szembeni katonai kiberfölény kialakítása. Így kiemelt fontosságú kezdeti információk biztosíthatók általa, melyek segíthetik a kiberműveletek kezdeti szakaszait.

4.1.2 Alapvető DNS-információk lekérdezése és vizsgálata

Ebben a fejezetben látható, hogy számos tool használható, amelyek hasonló eredményeket generálnak. Ennek oka az, hogy ellenőriznünk kell az összegyűjtött információkat. Ha azok egynél több tool segítségével is kinyerhetők, akkor megbízhatóbbak. A felsorolt lehetőségek főként nyílt forráskódú szoftvereken, tool-okon keresztül alapvető technikai információk begyűjtésére szolgálnak, amelyek így a közzétett adatokkal összhangban egy optimális, várhatóan elegendő információhalmazt hoznak létre. [63]

A Domain Name System információk kibontása információt szolgáltat a DNS-zónaadatokról. A DNS zone-adatok tartalmazzák a DNS-domain neveket, a számítógépneveket, az IP-címeket és sok más részletet a hálózatról. Az DNS-információk kibontása segít a cél DNS-re vonatkozó következő rekordok meghatározásában (15. ábra):

A	Rámutat a hoszt IP címére
MX	Rámutat a domain levelező szerverére
NS	Rámutat a hoszt név szerverére
CNAME	Kanonikus elnevezés lehetővé teszi az alias, nevek használatát a hoszt
SOA	Irányadó információk a DNS-zónáról; az elsődleges névkiszolgáló, a tartomány rendszergazdájának e-mail-címe, a tartomány sorozatszáma, a zóna frissítési időközei.
SRV	Általános szolgáltatás-helymeghatározó rekord, újabb protokollok számára, elkerülendő a protokoll-specifikus rekordokat, mint az MX.
PTR	Kanonikus névre mutat. A CNAME-től eltérően nem történik további, DNS-beli feldolgozás, maga a név a visszatérési érték. Leggyakrabban reverse DNS-lekérdezéseknél használják, de pl. az Apple DNS-SD-jében is használják.
RP	A tartományhoz rendelt felelős személy. Általában egy e-mail-cím, amiben a @ karaktert . helyettesíti
TXT	Text rekord (szöveges rekord)

17. ábra *DNS-rekordok [60] (saját szerkesztés)*

4.1.2.1 WhoIs

A WhoIs egy lekérdezési és válaszprotokoll olyan adatbázisok lekérdezésére, amelyek tárolják a regisztrált felhasználókat vagy internetes erőforrások jogosultjait, például egy domain nevet, egy IP-cím-blokkot vagy egy autonóm rendszert. Ez a protokoll a 43-as porton lévő kérésekre vonatkozik. A regionális internetes nyilvántartások (RIR[59]) tartják fenn a WhoIs-adatbázisokat, amelyek a domain tulajdonosok személyes adatait tartalmazzák. Minden egyes erőforrás esetében a WhoIs-adatbázis szöveges nyilvántartásokat tartalmaz magáról az erőforrásról, valamint a meghatalmazottakról, regisztrálókról és az adminisztrátori információkról (létrehozás és lejárati dátum). [91]

A WHOIS lekérdezéseket következőképen hajtottam végre:

```
┌──(kali㉿kali)-[~]
└─$ whois honvedelem.hu
% Whois server 3.0 serving the hu ccTLD

domain:         honvedelem.hu
record created: 2000-04-14 00:01:47
Tovabbi adatokert ld.:
https://www.domain.hu/domain-kereses/
For further data see:
https://www.domain.hu/domain-search/
```

18. ábra *Whois (saját szerkesztés)*

Az eredményből megkaptam a domain nevet, illetve a record létrehozásának dátumát.

4.1.2.2 Whatweb

Miután megkaptuk a DNS-kiszolgáló adatait, a következő lépés a további információ kinyerése. **A whatweb parancsot** a **következőképpen hajtottam végre:**

```
root@kali:~# whatweb honvedelem.hu
http://honvedelem.hu [301 Moved Permanently] Country[HUNGARY][HU], HTTPServer[nginx], IP[80.77.112.52],
RedirectLocation[https://honvedelem.hu/], Title[301 Moved Permanently], nginx
https://honvedelem.hu/ [200 OK] Country[HUNGARY][HU], Email[szerkesztoseg@honvedelem.hu], Frame, HTML5,
HTTPServer[nginx], IP[80.77.112.52], Open-Graph-Protocol[article], Script[application/ld+json,text/javas
cript], Strict-Transport-Security[max-age=63072000], Title[Honvédelem.hu], UncommonHeaders[link,x-page-s
peed], X-XSS-Protection[1; mode=block], nginx
```

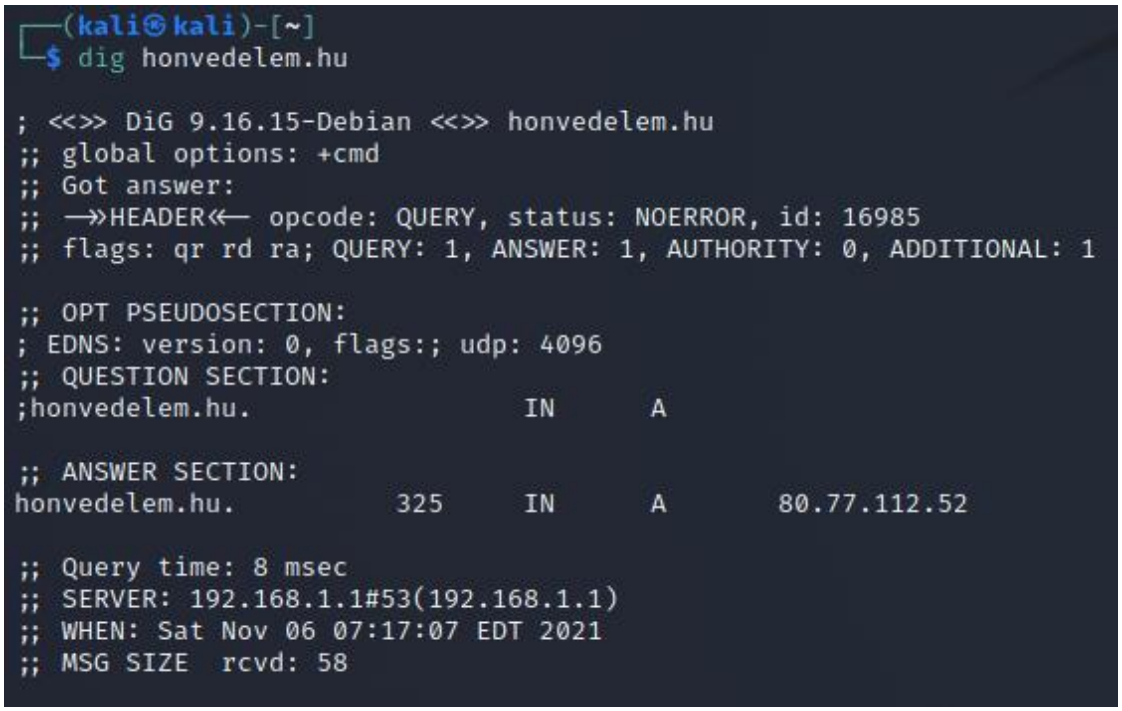
19. ábra *WhatWeb (saját szerkesztés)*

[59] A regionális internetes regiszter (RIR) olyan szervezet, amely az IP-címek blokkjait földrajzi hatáskörébe helyezi. 1996-ban az RFC 2050 meghatározza a RIR szerepét, nevezetesen: címmegőrzés, amely magában foglalja az erőforrások igazságos és hatékony elosztását, összesítés, amely abból áll, hogy a CIDR technikáknak köszönhetően az internet útvonala stabil maradjon, dokumentáció és regisztráció, amely biztosítja a címek használatának egyediségét és nyilvánosságát.

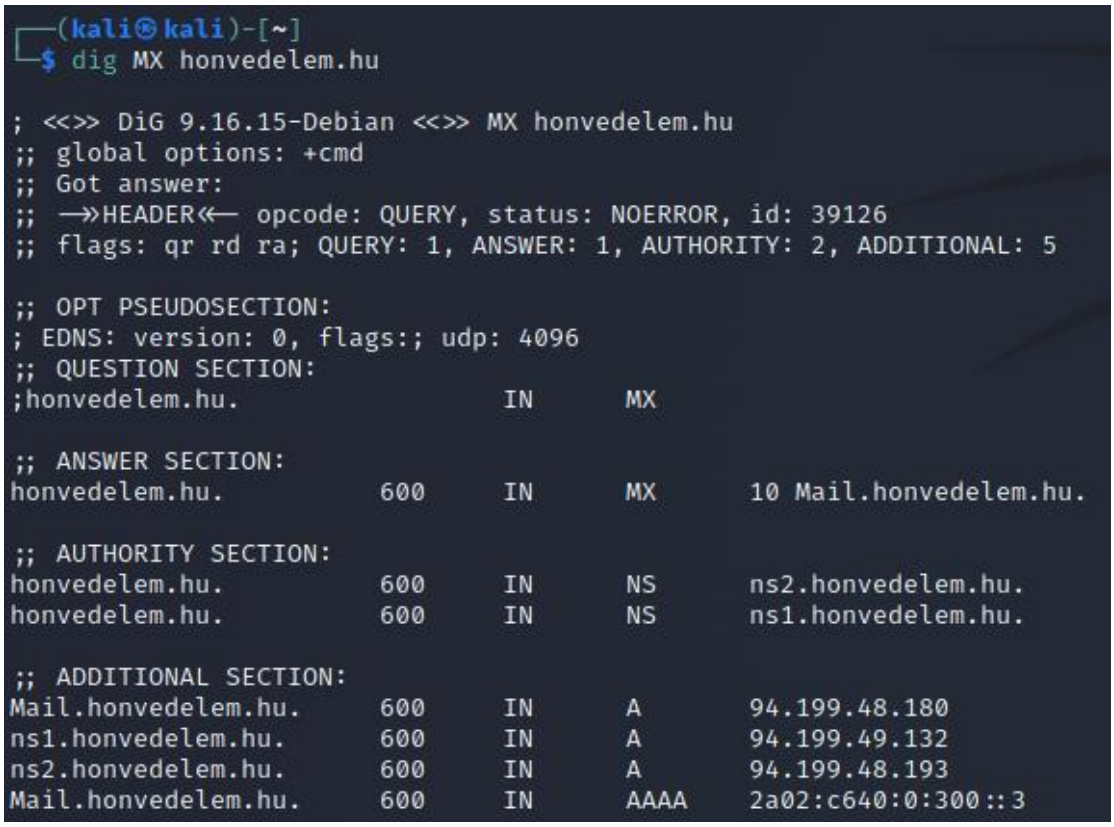
Az eredményt tekintve megismertem az IPv4 címét, a hosztolt szerver lokalizációját országra nézve (Magyarország), a szerver szolgáltatásának típusát, amely jelen esetben webszerver szolgáltatást takar (HTTPServer) és annak típusát a *www.honvedelem*.hu-ra nézve.

4.1.2.3 Dig

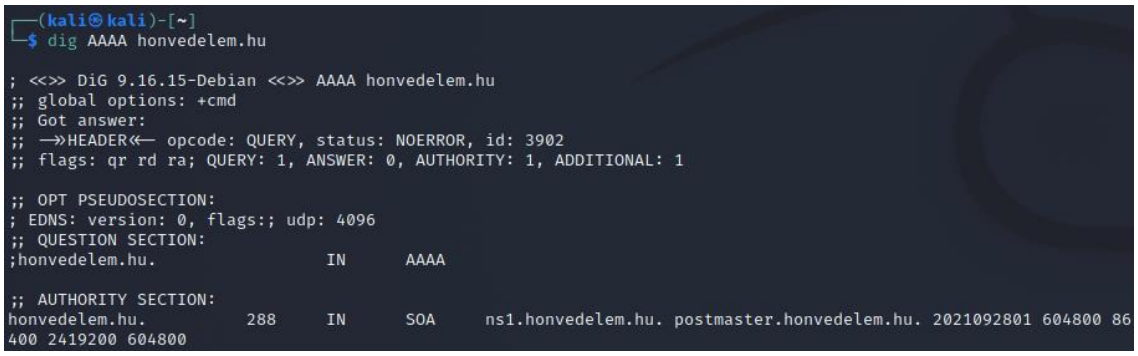
A Dig felhasználásával az A-, AAAA, MX- és NS- DNS rekordok kinyerését hajtottam végre:



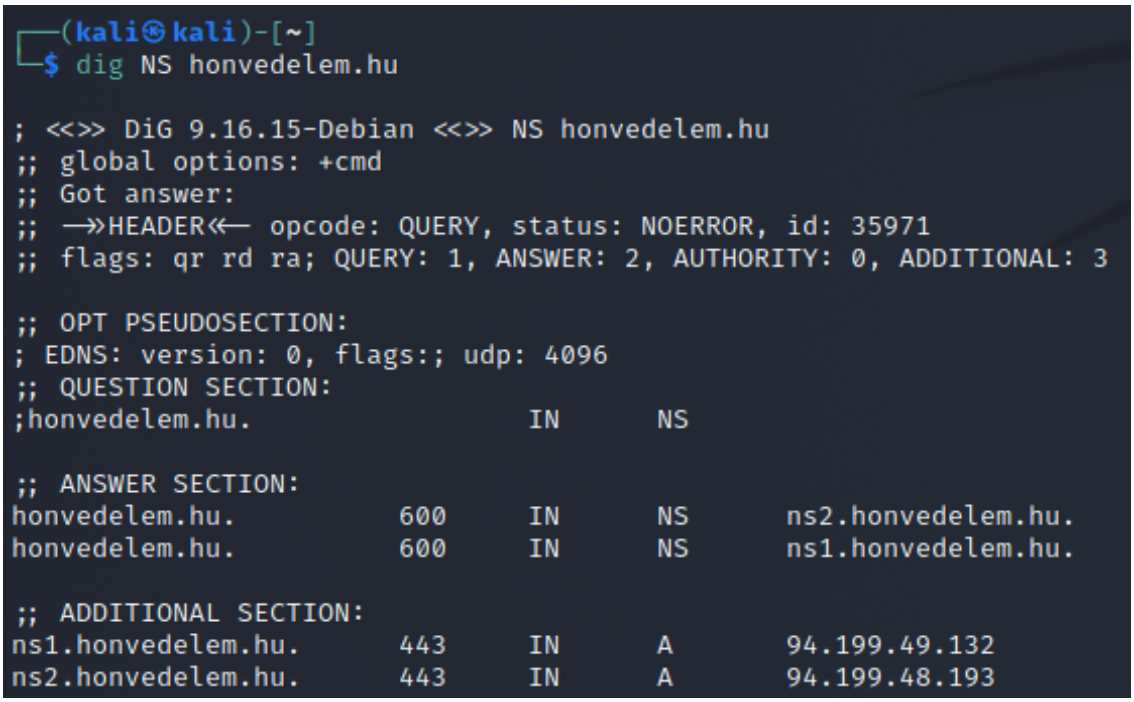
20. ábra *A dig parancs kimenetele (saját szerkesztés)*



21. ábra *dig MX (saját szerkesztés)*



22. ábra *dig AAAA (saját szerkesztés)*



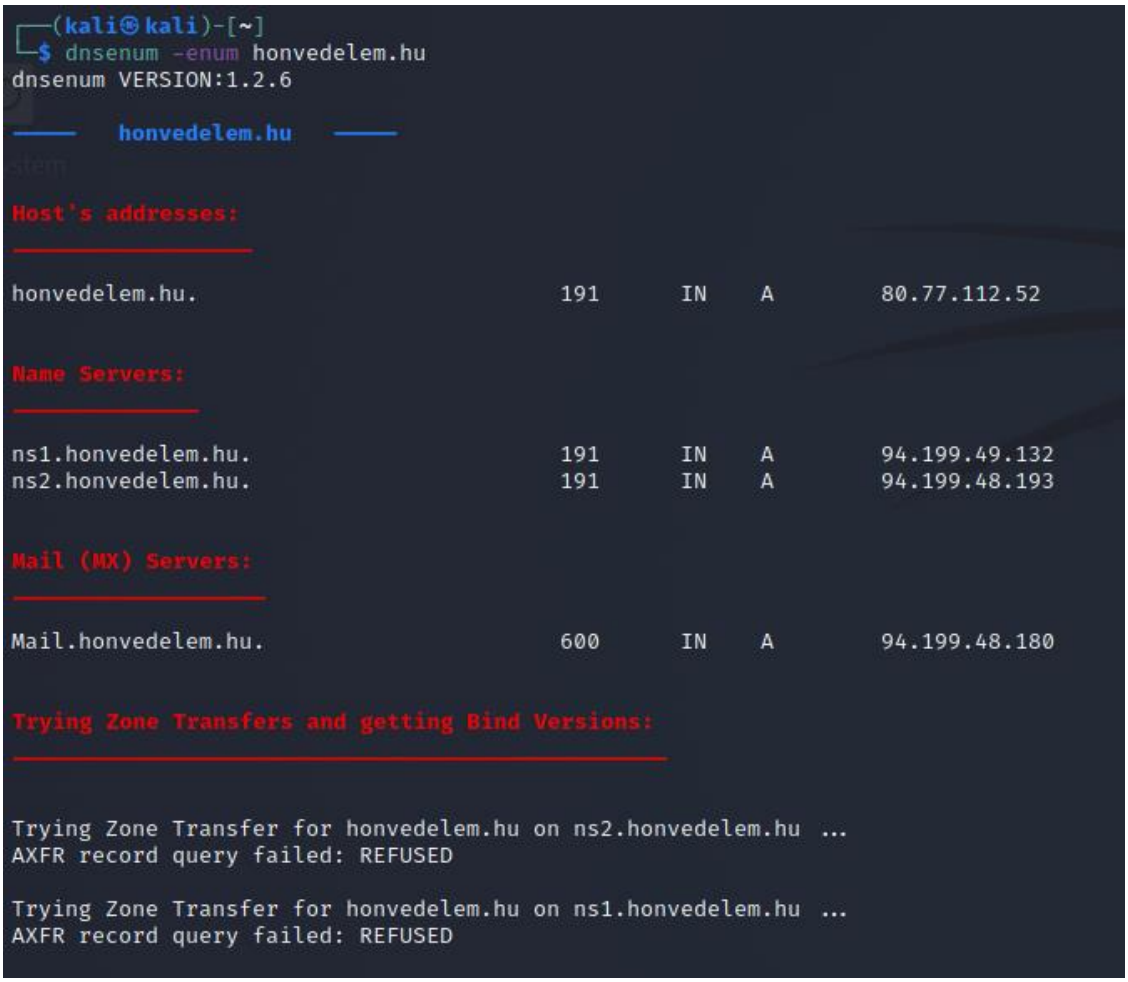
23. ábra *dig NS (saját szerkesztés)*

Ezekből az információkból levontam a megfelelő következtetéseket és tényeket. A Dig segítségének révén birtokában vagyok a honvedelm.hu szerver IPv4 és IPv6 címének, a szerver levelezőszerver szolgáltatás nevének és a névszerver nevének.

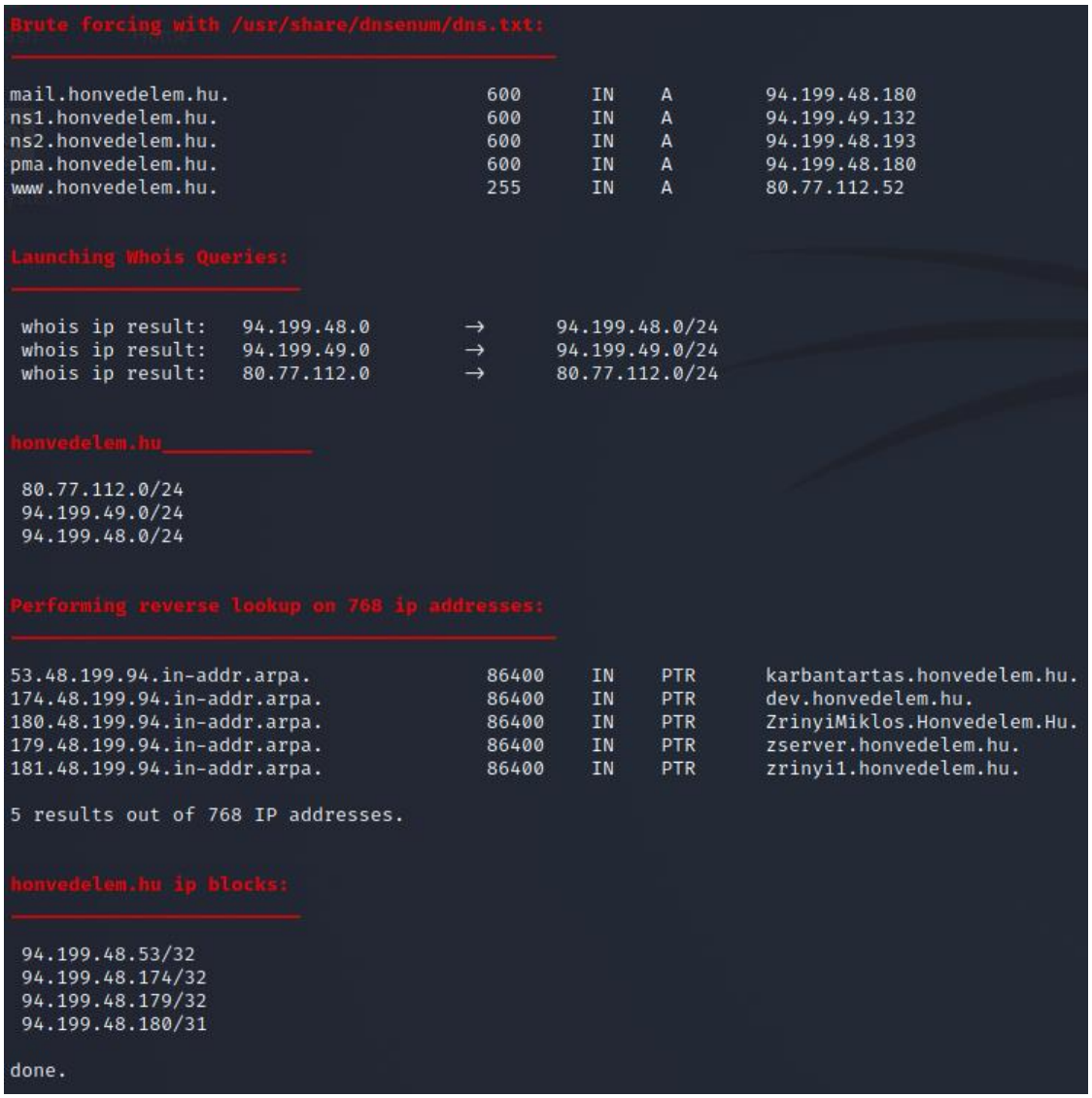
4.1.2.4 A dnsenum

A dnsenum egy DNS-felsorolási eszköz, amely egy szervezet összes DNS-kiszolgálóját és DNS-bejegyzését hivatott kilistázni. A DNS-felsorolás lehetővé teszi számunkra, hogy kritikus információkat gyűjtsünk a szervezetről, például felhasználóneveket, számítógépneveket, IP-címeket.

DNSenum információszerzést hajtottam végre a honvedelem.hu vonatkozásában:



24. ábra *dnsenum (saját szerkesztés)*



25. ábra *A dnsenum által összegyűjtött információk (saját szerkesztés)*

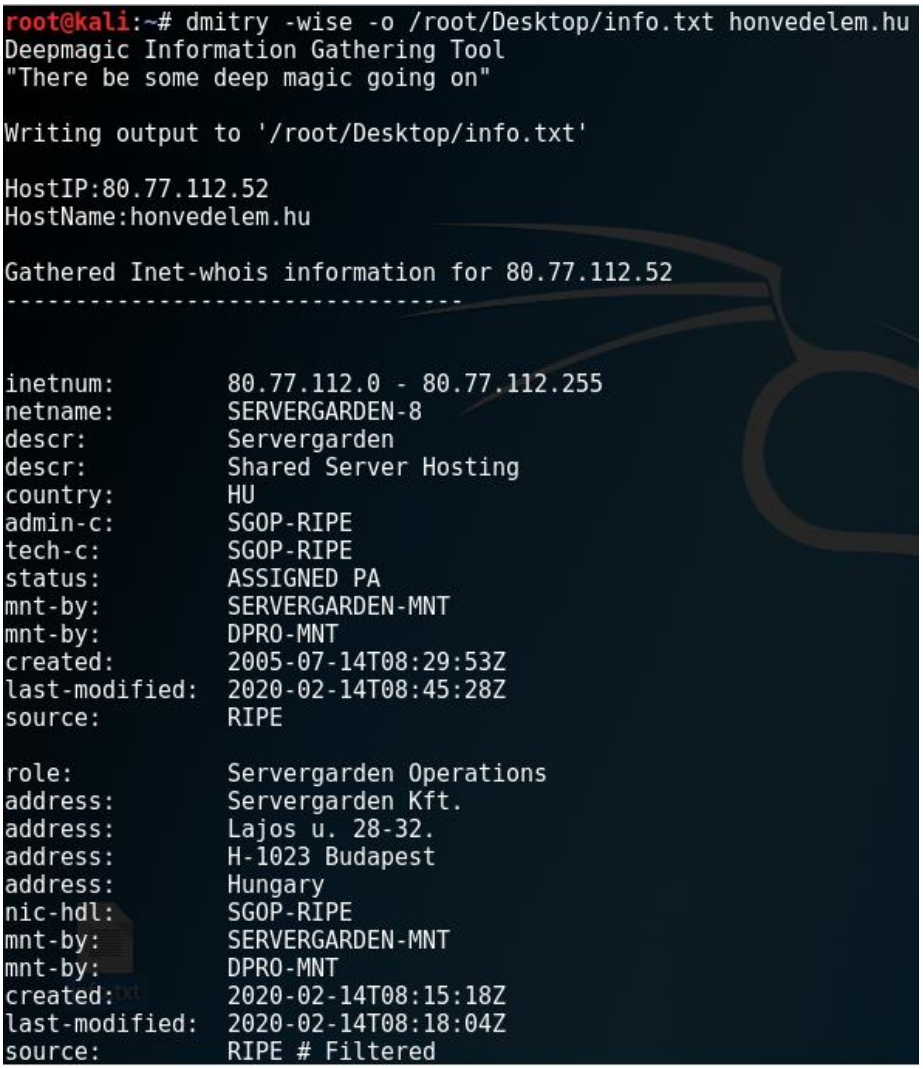
Az előzőkben alkalmazott parancsok a technikai DNS-információk lekérdezésére alkalmasak. Ezáltal olyan információkhoz segít hozzáférni, amelyek akár kulcsfontosságúak is lehetnek egy teszt vagy támadás felépítése, de legalábbis előkészítése során. A segítségükkel kinyertem, hogy a célpont melyik szervezetnél regisztrált domain-nevet, mi a szerver IP-címe, mi a levelezőszervere, mi a névszervere, mikor regisztrált, mikor jár le a regisztráció, ki a kontakt és még pár nagyon hasznos információ, amelyeket a közzétett adatok elemzésével együtt használva egy erős információs adatbázist képezhet a munkafolyamat első lépcsőjében.

4.1.2.5 DMitry

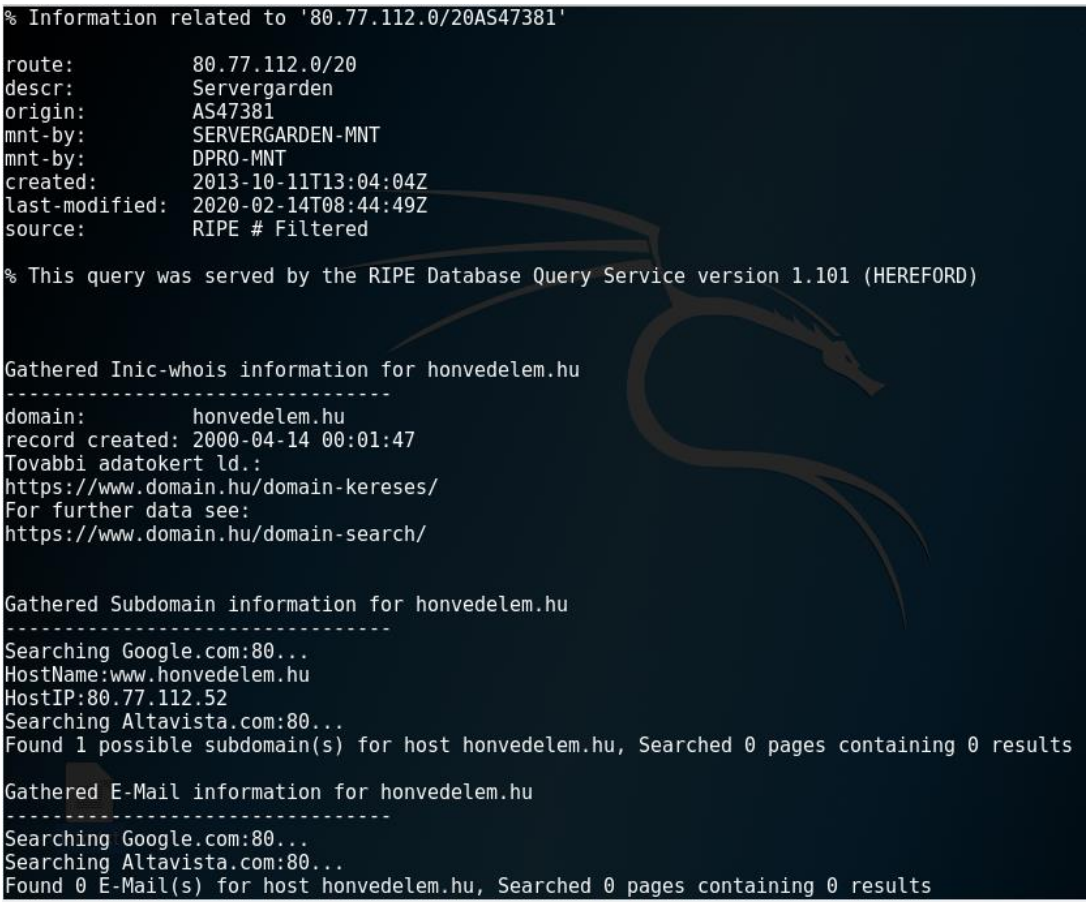
A Dmitry egy ingyenes és nyílt forráskódú eszköz, amely elérhető a GitHubon. Az eszköz információgyűjtésre szolgál.

Dmitry Tool használható:

- a cél aldomain-jeinek megkeresésére;
- célrendszer nyitott portjainak megtalálására;
- a TCP szkennelésre;
- netcraft szolgáltatással a cél információk, például az operációs rendszer, a webszerver részletei, a webtárhely adatai, a tárhelyszolgáltatás adatok kinyerésére;
- a whois szolgáltatással a célinformációk kinyerése, mint például a regisztrált domain, név, cím, a regisztráló személy elérhetősége;
- a cél domain-jéhez társított e-mail címek beszerzésére.



26. ábra *dmitry (saját szerkesztés)*



27. ábra *dmitry2 (saját szerkesztés)*

Amint a 24. és 25. ábrán is bemutattam, a dmitry használatával az IP címen túl, a domainnév birtokos cég fizikai lokációját is kinyomozhatjuk.

4.1.2.6 Harvester

A Harvester egy egyszerű, de rendkívül hatékony Python-szkript, amelyet Christian Martorella írt az Edge Security-től. [92] Ezzel az eszközzel gyorsan és pontosan katalogizálhatjuk a célunkhoz közvetlenül kapcsolódó e-mail címeket és aldomain-eket. Fontos, hogy mindig a Harvester legújabb verzióját használjuk, mivel sok keresőmotor rendszeresen frissíti és módosítja rendszerét. A Harvester segítségével a Google és a Bing szerverein kereshetünk e-maileket, hoszt-gépeket és aldomain-eket, valamint a LinkedIn-en felhasználóneveket.

28. ábra *Harvester (saját szerkesztés)*

Amíg a Harvester alkalmazása a google keresőmotorral nem ad felhasználható eredményt, addig ahogy a 26. ábrán is látható, a sublist3r alkalmazásával 5 hosztot is felderített. Ezeket további vizsgálatokra lehet továbbvinni, illetve részeredményként a dokumentáció részben feltüntetni.

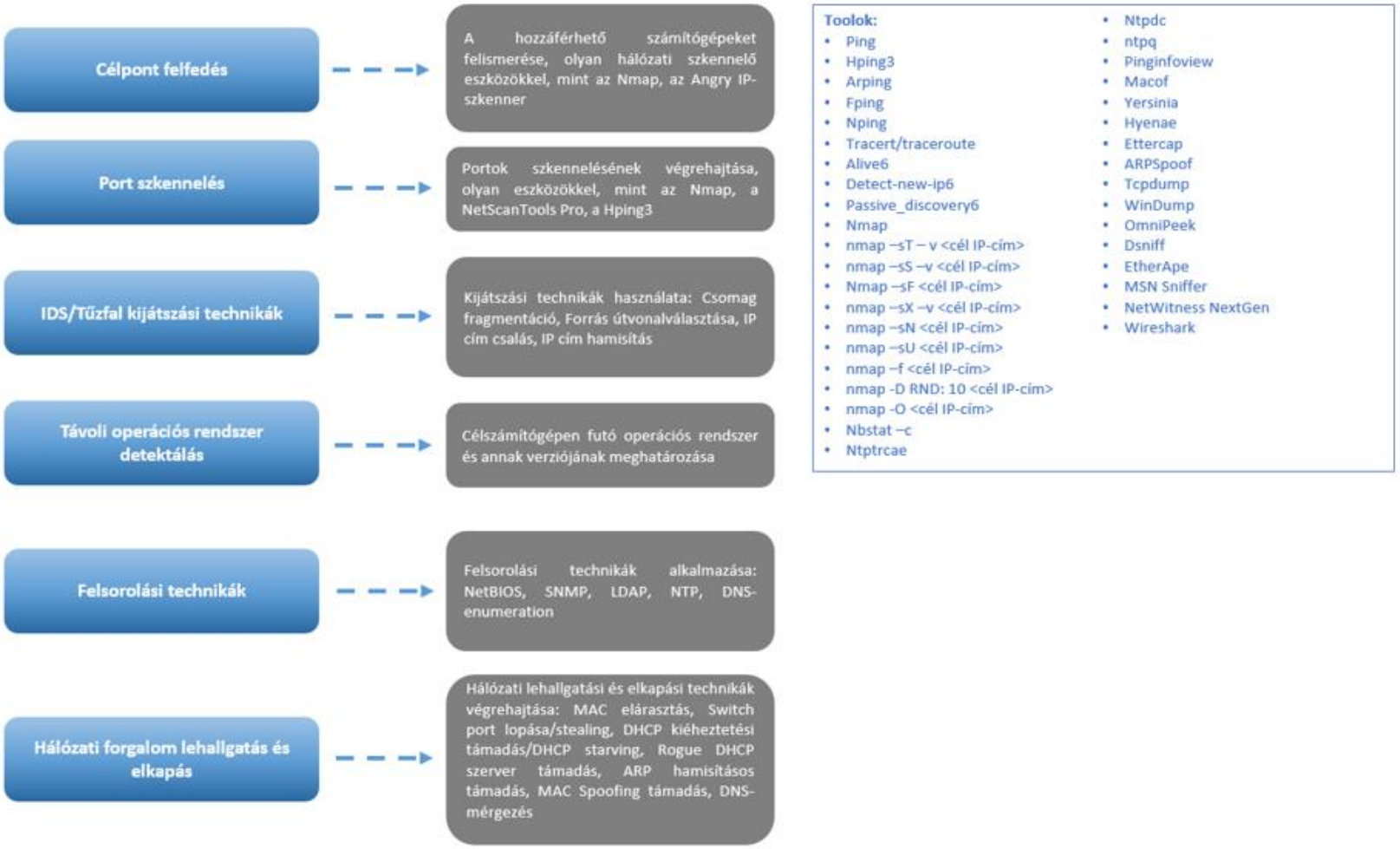
Összességében kijelenthető, hogy az alapvető DNS-információk lekérdezése és vizsgálata teljesen alkalmas a DNS rekordok alapos és mély kinyerésére, ami további felhasználásra alkalmas. Hozzájárulhat a katonai kiberműveletek kiberfölényének kialakításához.

4.2 HÁLÓZAT-FELTÉRKÉPEZÉS

A hálózat-feltérképezés a penetrációsteszt-végrehajtás lépésének második szakasza, amely „életben lévő” és reagáló rendszerekről gyűjt információt a hálózaton. A portszkennelési technikák segítenek a támadónak a megcélzott szerver vagy hoszt nyitott portjainak azonosításában. A rendszergazdák gyakran portszkennelési technikákat használnak a hálózatok biztonsági politikájának ellenőrzésére, míg a támadók ezeket használják a futó szolgáltatások azonosítására egy hoszton, de ők a rendszergazdákkal ellentétben már a hálózat veszélyeztetése céljából. A 28. ábrán **kutatásaim alapján megalkottam a hálózat feltérképezés lépéseit**:

- Célpont felfedés;
- Port Szkennelés;
  - TCP;
  - UDP[60].
- IDS/tűzfal-kijátszási technikák;
  - Csomagtördelés;
  - Forrás Útvonalválasztás;
  - IP cím csalás;
  - IP cím Spoofing.
- Távoli operációs rendszer detektálása;
- Felsorolási technika- Enumeration.

[60] A User Datagram Protocol az internet egyik alapprotokollja. Feladata datagram alapú szolgáltatás biztosítása, azaz rövid, gyors üzenetek küldése.



29. ábra *Hálózat-feltérképezés folyamat (saját szerkesztés)*

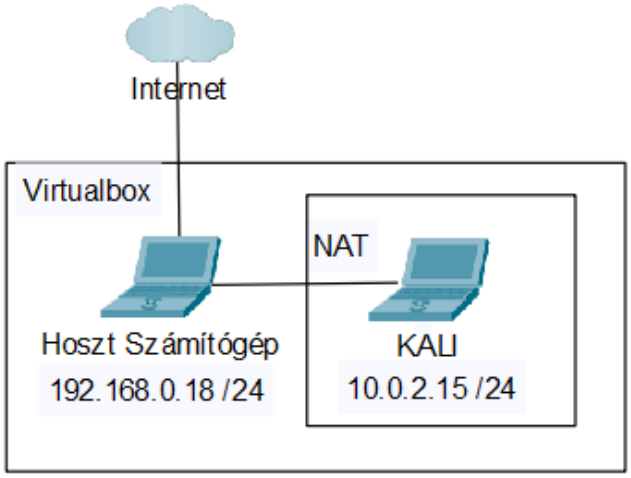
4.2.1 Célpontfelfedés

A célpont felfedése műveletekbe tartozó tool-ok azonosítják azokat a célgépeket, amelyekhez hozzá lehet férni.

Topológia 1. – Közétett adatok információgyűjtése

Szükséges erőforrások:

- Kali Linux operációs rendszer;
- Internet elérés;
- Hoszt számítógép legalább 8 GB RAM-mal és 45 GB szabad lemezterülettel.



30. ábra *Célpontfelfedési tesztkörnyezet (saját ábra)*

Virtuális gép	Operációs rendszer	OVA méret	Lemezterület	RAM
Kali	Kali Linux	4.1GB	10 GB	1 GB

2. Táblázat: Célpontfelfedési tesztkörnyezet adatok (saját szerkesztés)

A ping eszköz a leghíresebb eszköz, amelyet annak ellenőrzésére használnak, hogy egy adott hoszt elérhető-e. A ping eszköz úgy működik, hogy egy Internet Control Message Protocol, ICMP[61] visszhangkérési csomagot küld a célszámítógép számára. Ha a célszámítógép elérhető, és a tűzfal nem blokkolja az ICMP visszhangkérési csomagot, az ICMP visszhang visszaválaszol. [93]

[61] Az Internet Control Message Protocol egy interneten használt protokoll, melynek segítségével értesülhetünk a hibákról illetve azok típusáról, valamint hálózati diagnosztizálásban lehet a segítségünkre. Az ICMP (az UDP-hez hasonlóan) datagram-orientált kommunikációs protokoll, mert egyáltalán nem garantált a csomagok megérkezése vagy sorrendje.

A ping parancsot végrehajtottam a célpont elérésének ellenőrzése érdekében:

```
┌──(kali㉿kali)-[~]
└─$ ping honvedelem.hu
PING honvedelem.hu (80.77.112.52) 56(84) bytes of data.
64 bytes from 80.77.112.52 (80.77.112.52): icmp_seq=1 ttl=53 time=23.0 ms
64 bytes from 80.77.112.52 (80.77.112.52): icmp_seq=2 ttl=53 time=25.9 ms
64 bytes from 80.77.112.52 (80.77.112.52): icmp_seq=3 ttl=53 time=27.2 ms
64 bytes from 80.77.112.52 (80.77.112.52): icmp_seq=4 ttl=53 time=23.4 ms
^C
--- honvedelem.hu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3082ms
rtt min/avg/max/mdev = 23.019/24.876/27.191/1.720 ms

┌──(kali㉿kali)-[~]
└─$ fping honvedelem.hu
honvedelem.hu is alive
```

31. ábra *A ping parancs használata (saját szerkesztés)*

A Hping2/Hping3 egy parancssor orientált hálózati szkennelési és csomagmegmunkáló eszköz a TCP/IP protokollhoz, amely elküldi az ICMP visszhangkéréseket, és támogatja a TCP, UDP, ICMP protokollokat. [94]

Ahogy az a 29. ábrán is látható, a traceroute kapcsolóval a célpont felfedés mellett az útvonalat is sikerült felderítenem.

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --traceroute -V -1 honvedelem.hu

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for kali:
using eth0, addr: 10.0.2.15, MTU: 1500
HPING honvedelem.hu (eth0 80.77.112.52): icmp mode set, 28 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=10.0.2.2 name=UNKNOWN
hop=1 hoprtt=8.4 ms
hop=2 TTL 0 during transit from ip=192.168.1.1 name=sagemcom
hop=2 hoprtt=7.7 ms
hop=3 TTL 0 during transit from ip=145.236.238.142 name=lo1.bsr4-szolnok.net.telekom.hu
hop=3 hoprtt=10.2 ms
hop=4 TTL 0 during transit from ip=84.1.64.36 name=Te0-10-0-21.core0-dataplex.net.telekom.hu
hop=4 hoprtt=17.7 ms
hop=5 TTL 0 during transit from ip=81.183.3.95 name=UNKNOWN
hop=5 hoprtt=28.0 ms
hop=6 TTL 0 during transit from ip=217.243.178.14 name=UNKNOWN
hop=6 hoprtt=23.8 ms
hop=7 TTL 0 during transit from ip=87.128.239.253 name=UNKNOWN
hop=7 hoprtt=26.6 ms
hop=8 TTL 0 during transit from ip=62.115.114.184 name=win-bb3-link.ip.twelve99.net
hop=8 hoprtt=26.6 ms
hop=9 TTL 0 during transit from ip=62.115.119.39 name=bpt-b2-link.ip.twelve99.net
hop=9 hoprtt=30.3 ms
hop=10 TTL 0 during transit from ip=62.115.40.34 name=doclerweb-ic305025-bpt-b2.ip.twelve99-cust.net
hop=10 hoprtt=23.4 ms
```

32. ábra *Hping3 alkalmazása (saját szerkesztés)*

Az nping eszköz olyan eszköz, amely lehetővé teszi a felhasználók számára a protokollok széles skálájának (TCP, UDP, ICMP és ARP[62]) hálózati csomagjainak előállítását. Testre szabhatja a mezőket a protokoll fejlécében, például a TCP és az UDP forrás- és célportját. [95]

Végrehajtottam futtatását parancssorba: *# nping*

```
┌──(kali㉿kali)-[~]
└─$ nping honvedelem.hu

Starting Nping 0.7.91 ( https://nmap.org/nping ) at 2021-11-06 09:06 EDT
SENT (0.0342s) Starting TCP Handshake > honvedelem.hu:80 (80.77.112.52:80)
RCVD (0.0627s) Handshake with honvedelem.hu:80 (80.77.112.52:80) completed
SENT (1.0432s) Starting TCP Handshake > honvedelem.hu:80 (80.77.112.52:80)
RCVD (1.0700s) Handshake with honvedelem.hu:80 (80.77.112.52:80) completed
SENT (2.0461s) Starting TCP Handshake > honvedelem.hu:80 (80.77.112.52:80)
RCVD (2.0746s) Handshake with honvedelem.hu:80 (80.77.112.52:80) completed
SENT (3.0538s) Starting TCP Handshake > honvedelem.hu:80 (80.77.112.52:80)
RCVD (3.0802s) Handshake with honvedelem.hu:80 (80.77.112.52:80) completed
SENT (4.0566s) Starting TCP Handshake > honvedelem.hu:80 (80.77.112.52:80)
RCVD (4.0810s) Handshake with honvedelem.hu:80 (80.77.112.52:80) completed

Max rtt: 28.527ms | Min rtt: 24.046ms | Avg rtt: 26.794ms
TCP connection attempts: 5 | Successful connections: 5 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 4.09 seconds
```

33. ábra *nping használata (saját szerkesztés)*

Összességében kijelenthető, hogy célpontfelfedés sikeres volt, a **célpont elérhető**, a fenti ábrákon látható, hogy csomagvesztés nem történt, dokumentálhatók az időtartományok, a felépített TCP kapcsolatok, valamint a h3ping traceroute-tal való kiterjesztése esetében az elérés útvonala is.

4.2.2 Port Szkennelés

Minél több információ áll rendelkezésre a célszervezetről, annál nagyobb az esély a hálózat biztonsági profiljának megismerésére, és ennek következtében a jogosulatlan hozzáférésre.

Néhány cél a hálózat szkennelésére:

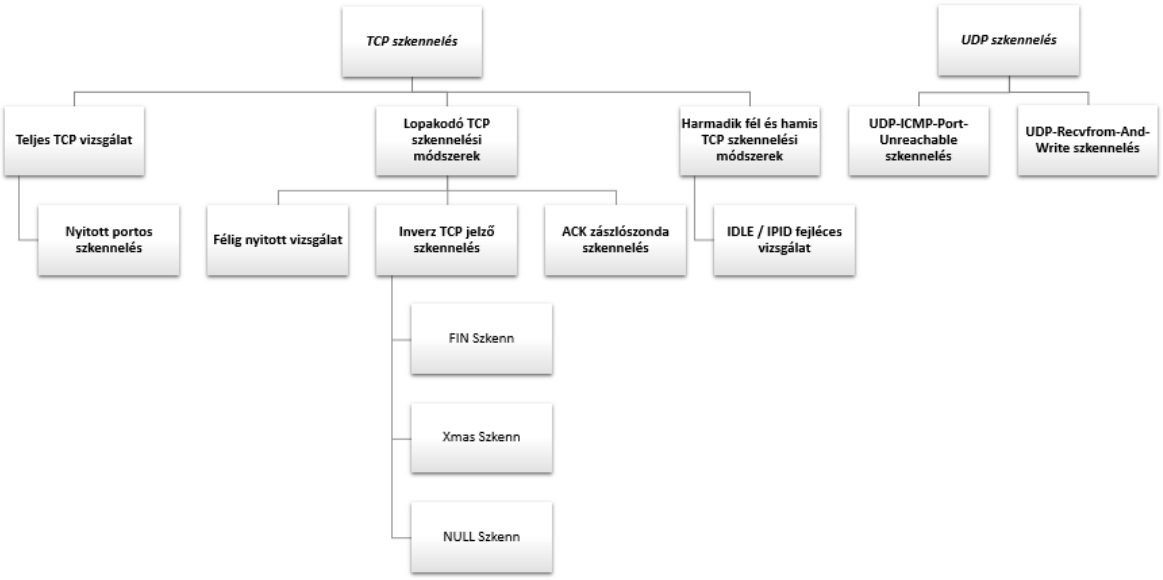
- Hálózati számítógépek, IP-címek és az élő portok felfedezése. Nyitott portok használatával a támadó meghatározza a rendszerbe való belépés legjobb módját.
- Cél operációs rendszer és rendszer-architektúra felfedezése. Ezt ujjlenyomatnak is

[62] Address Resolution Protocol, azaz címfeloldási protokoll az informatikában a számítógépes hálózatokon használatos módszer az IP-címek és MAC-címek (fizikai címek) egymáshoz rendeléséhez. Gyakorlatilag az IP-cím ismeretében hozzájutunk a 48 bites hálózati kártya gyártója által meghatározott fizikai címhez. Az IPv4 és az Ethernet széles körű elterjedtsége miatt általában IP-címek és Ethernet-címek közötti fordításra használják, de ATM- vagy FDDI-hálózatokban is működőképes.

nevezik.

- Célrendszeren futó/hallgató szolgáltatások felfedezése.
- Egy adott szolgáltatás alkalmazásának vagy verziójának meghatározása.
- A hálózati rendszerek sebezhetőségének meghatározása.

A szkennelés olyan folyamat, amely aktív és reagáló rendszerekről gyűjt információt a hálózaton. A portszkennelési technikák segítenek a támadónak a megcélzott szerver vagy hoszt nyitott portjainak az azonosításában. A rendszergazdák gyakran portszkennelési technikákat használnak a hálózatok biztonsági politikájának ellenőrzésére, míg a támadók ezeket használják a futó szolgáltatások azonosítására egy hoszton, de már a hálózat veszélyeztetése céljából. [96]



34. ábra *A szkennelés csoportosítása (saját szerkesztés)*

A szkennelési technikákat tovább osztják kettő kategóriába, az alábbiak szerint:

- TCP hálózati szolgáltatások:
  - TCP Teljes nyitott vizsgálat;
  - Lopakodó TCP szkennelési módszerek;
    - Félig nyitott szkennelés;
    - Inverz TCP jelző szkennelés;
      - Xmas Szkenn;
      - FIN szkennelés;
      - NULLSzkenn.
    - ACK zászlószonda szkennelés;

- Harmadik fél és hamis TCP szkennelési módszerek.
  - IDLE/IPID fejléc[63] szkennelés.

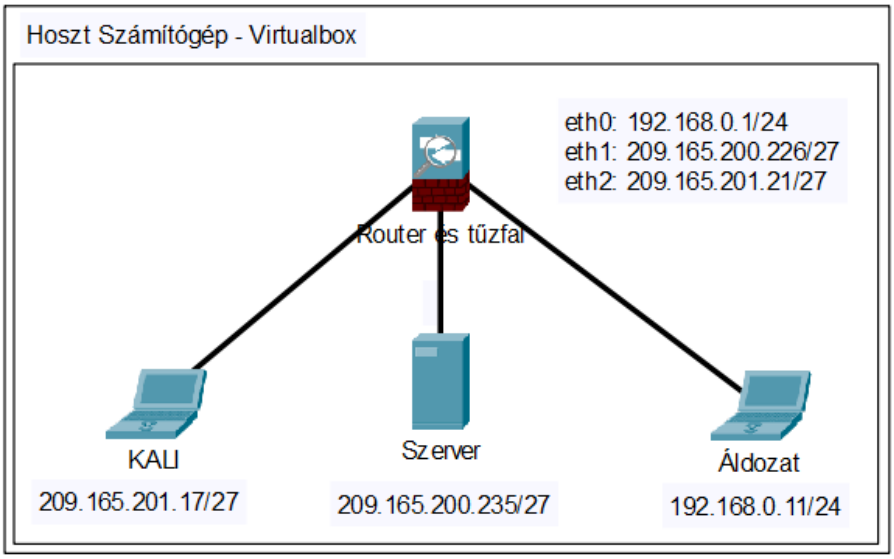
- UDP NetworkServices szkennelése:
  - UDP Szkennning.

A portszkennelés demonstrálásához a következő laborkörnyezetet használtam:

Topológia 2. – Portszkennelés

Szükséges erőforrások:

- Kali Linux operációs rendszer;
- Arch Linux operációs rendszer;
- Ubuntu Linux (szerver operációs rendszer);
- Ubuntu Linux (router firewall rendszer);
- Hoszt-számítógép legalább 8 GB RAM-mal és 45 GB szabad lemezterülettel.



35. ábra *Portszkennelési tesztkörnyezet (saját szerkesztés)*

[63] IP Internet Identification - Ez a mező a fragmens-ek összeszerelése során használt IP-csomagok azonosítását szolgálja.

Virtuális gép	Operációs rendszer	OVA méret	Lemez terület	RAM
Áldozat	Arch Linux	2.23 GB	7 GB	1 GB
Kali	Kali Linux	3.07 GB	10 GB	1 GB
Szerver	Ubuntu Linux	851 MB	8 GB	512 MB
Router és tűzfal	Ubuntu Linux	2.35 GB	10 GB	4 GB
	Összesen	**8.5 GB**	**45 GB**	**6.5 GB**

3. Táblázat: Portszkennelési tesztkörnyezet adatok (saját szerkesztés)

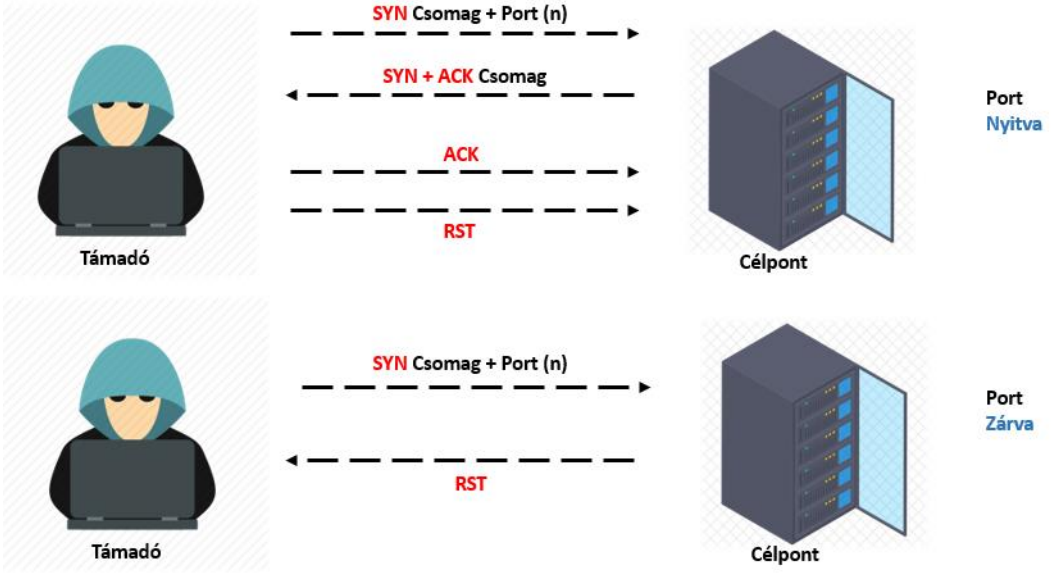
Ezen felül a vizsgálatokat az Nmap nevezetű program segítségével hajtottam végre. Az Nmap egy hálózat-feltérképező eszköz és biztonsági portszkenner program. Az Nmap a hálózat átvizsgálására és a hálózaton elérhető hosztgépek és szolgáltatások meghatározására szolgál. Az Nmap egyes funkciói közé tartozik a hosztgép-felderítés, a portellenőrzés és az operációs rendszer észlelése. Az Nmap általánosan használható biztonsági ellenőrzésekre, nyitott portok azonosítására, hálózati leltárra és a hálózat sebezhetőségeinek felderítésére.

4.2.2.1 TCP vizsgálat

A teljes vagy nyitott portos vizsgálat csak egy újabb módszer annak megállapítására, hogy a háromutas kézfogás megvalósul-e a célrendszer portjain azért, hogy meghatározzák, hogy melyik nyitott és melyik zárt. Ha a port hallgat, akkor a csatlakozási meghívás sikeres kapcsolatot hoz létre az adott port számítógépével, egyébként hibaüzenetet küld, amely kijelenti, hogy a port nem érhető el. A teljesen nyitott szkenn előnye, hogy a vizsgálat során azonnali pozitív visszajelzés kapható arról, hogy egy port nyitva vagy zárva van. Ennek a szkennelésnek azonban a hátránya az, hogy visszavezet a háromirányú kézfogás használatához.

Köztudott, hogy a háromutas kézfogás célja annak megerősítése, hogy mindkét fél kommunikálni fog. Viszont, ha mindkét fél megerősíti jelenlétét és részvételét a kapcsolatban, akkor mindenki tudja, hogy mindkét fél ott van, és kik ők. A TCP háromutas kézfogásban a támadó SYN csomagot küld, amelyet a címzett egy SYN + ACK csomaggal nyugtáz. A támadó

nyugtázza a SYN + ACK csomagot egy ACK csomaggal. Ezután a szkennelő RST[64] csomagot küld a kapcsolat megszakításához. [97] Nyitott port esetén a válasz olyan, mint egy normál háromutas kézfogás esetén, azonban egy zárt port esetén csak RST csomagot kap. A válaszmintázat ismeretével meghatározható, hogy a port véglegesen nyitva van-e vagy sem.



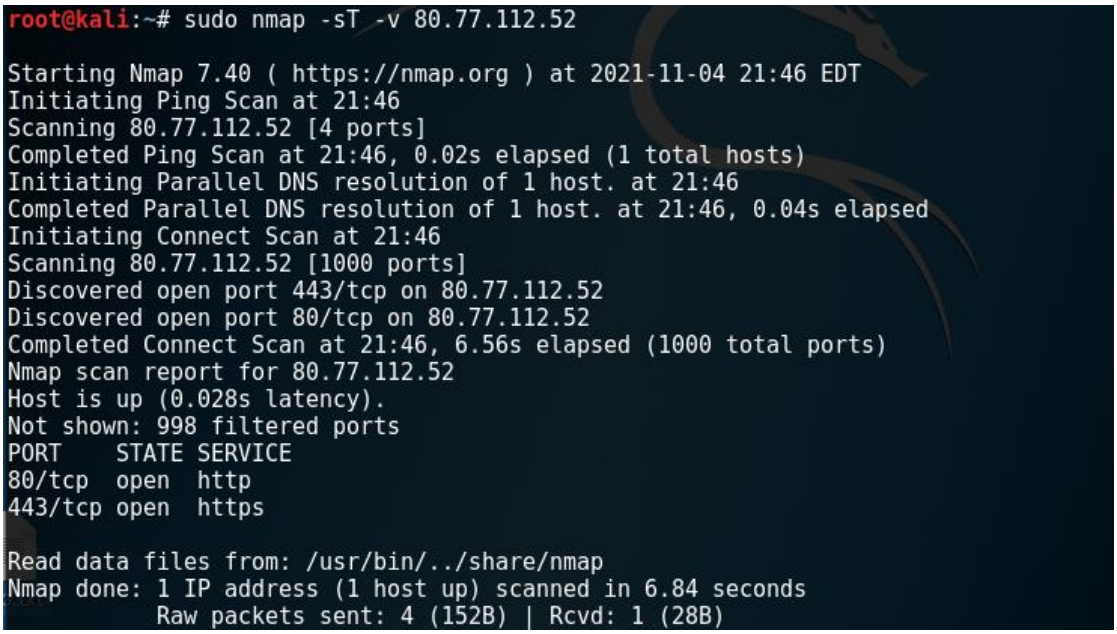
36. ábra *Teljes vagy nyitott portos vizsgálat (saját szerkesztés)*

Az nmap teljes nyitott vizsgálatát a következőképpen hajtottam végre: *nmap –sT –v <cél IP-cím>*

A Honvedelem.hu példát tesztelve látható a 34. ábrán, hogy 2 port van nyitva, a 80/tcp: http és 443/tcp: https szolgáltatást biztosító. Szerverszolgáltatás üzemeltetésénél ez nem meglepő eredmény.

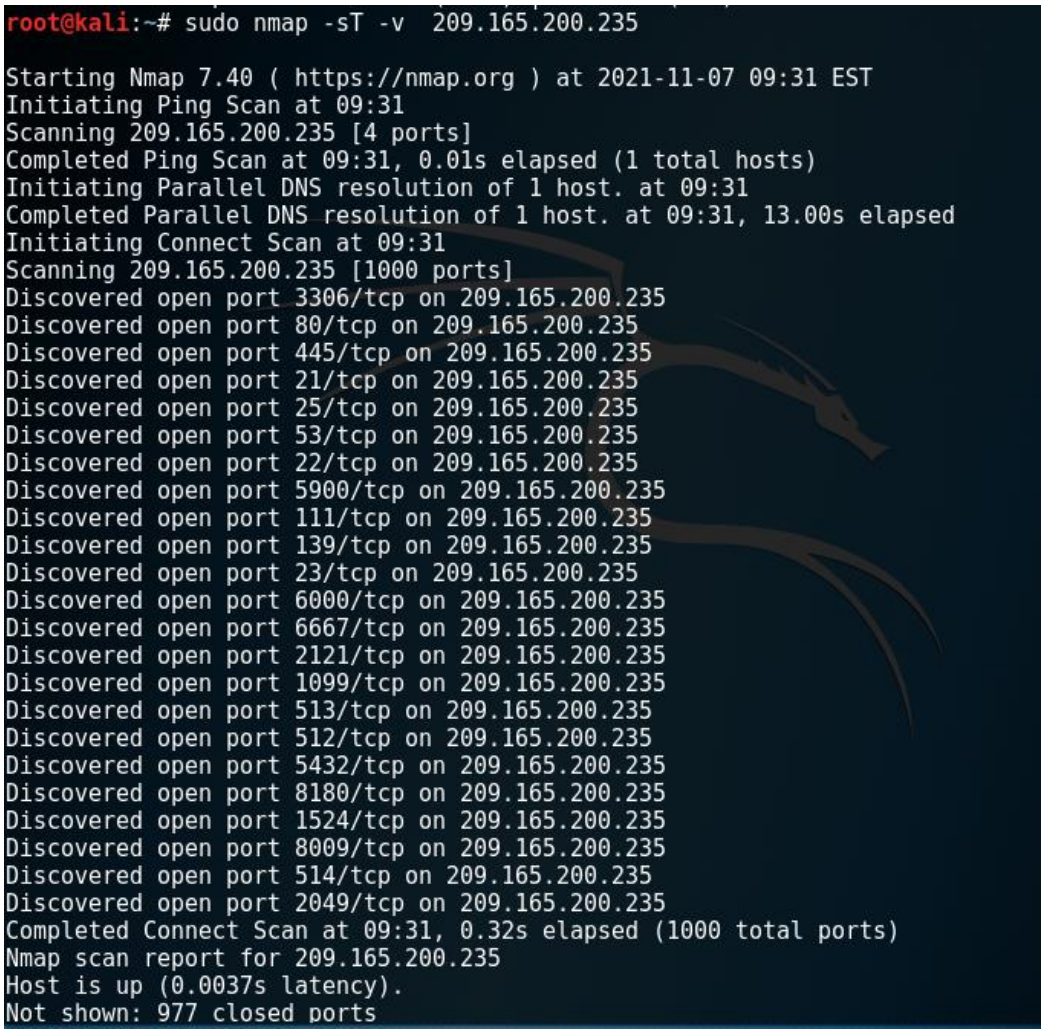
A -sT kapcsoló- TCP SYN/Connect() letapogatás jelzi, a –v a bőbeszédű üzemmód beállítását.

[64] Reset



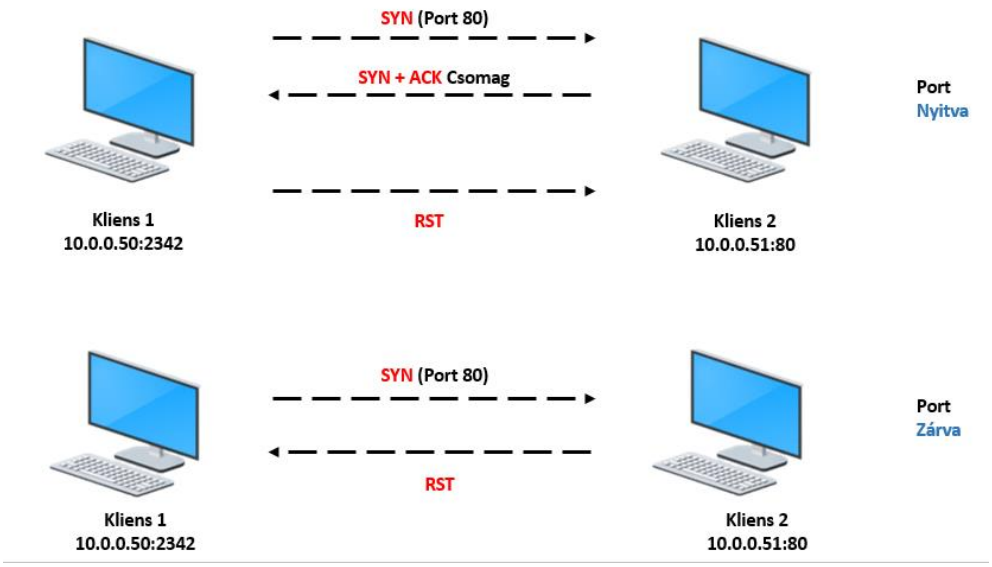
37. ábra *Teljes nyitott szkenn (saját szerkesztés)*

A saját tesztkörnyezetben letapogatott szerver viszont rengeteg nyitott portot tartalmaz (35. ábra), például a 21, 22, 23, 25, 53, 111, 139, 445, 512, 513, 514, 1099 portok. Ezek a portok a következő szolgáltatásokat takarják, melyek közül sok egyáltalán nem minősül biztonságosnak: FTP, SSH, Telnet, SMTP, DNS, Sun Protocol, NetBIOS, Microsotf-DS. Ezáltal a tesztkörnyezetben futtatott szerver jól felderíthető, és a portszkenn megfelelő előkészületet biztosít további penetrációs exploitok futtatásához.



38. ábra *Teljes vagy nyitott portos vizsgálat nmap segítségével (saját szerkesztés)*

A TCP vizsgálatok másik irányvonala a nyitott portos vizsgálat mellett a lopakodó TCP vizsgálat. A lopakodó TCP szkennelési módszerek közül az egyik a félig nyitott vizsgálat (Stealth scan), mely nagyban hasonlít a teljes nyílt szkennelésre, néhány különbséggel, ami kidolgozottabbá teszi azt. A Stealth vizsgálat magában foglalja a kliens és a szerver közötti TCP kapcsolat hirtelen alaphelyzetbe állítását, mielőtt a háromirányú kézfogás jelei befejeződnének, tehát a kapcsolat félig nyitott lesz. A lopakodó vizsgálat egyetlen keretet küld a TCP-portra bármilyen TCP-kézfogás vagy további csomagátvitel nélkül. Az ilyen típusú szkennelés egyetlen keretet küld, egyetlen választ várva. A lopakodó vizsgálatot SYN vizsgálatnak is nevezik, mivel csak a SYN csomagot küldi el. [98]



39. ábra *A félig nyitott vagy lopakodó szkennelés (saját szerkesztés)*

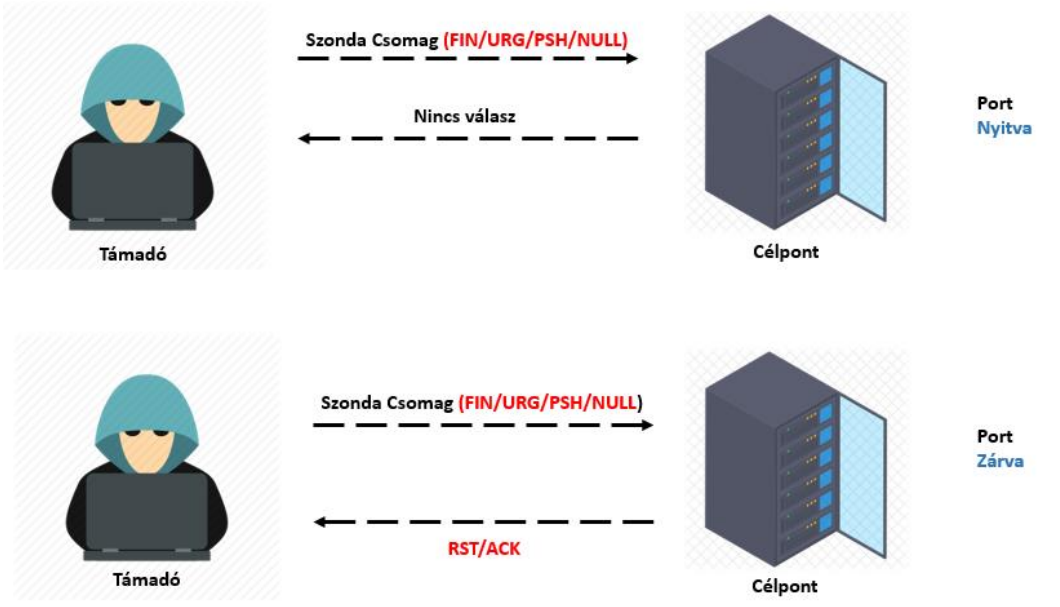
A félig nyitott szkennelés vizsgálatát a következőképpen hajtottam végre: *nmap –sS –v <cél IP-cím>*

```
root@kali:~# sudo nmap -sS -v 192.168.0.11

Starting Nmap 7.40 ( https://nmap.org ) at 2021-11-07 09:34 EST
Initiating Ping Scan at 09:34
Scanning 192.168.0.11 [4 ports]
Completed Ping Scan at 09:34, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:34
Completed Parallel DNS resolution of 1 host. at 09:35, 13.00s elapsed
Initiating SYN Stealth Scan at 09:35
Scanning 192.168.0.11 [1000 ports]
Discovered open port 21/tcp on 192.168.0.11
Discovered open port 22/tcp on 192.168.0.11
Completed SYN Stealth Scan at 09:35, 0.26s elapsed (1000 total ports)
Nmap scan report for 192.168.0.11
Host is up (0.0029s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds
           Raw packets sent: 1004 (44.152KB) | Rcvd: 1001 (40.036KB)
```

40. ábra Stealth szkenn (félig nyitott vizsgálat) nmap segítségével *(saját szerkesztés)*

A saját tesztkörnyezetben lévő áldozat számítógépét tesztelve látható a 38. ábrán, hogy 2 port van nyitva, a 21/tcp: ftp és a 22/tcp: ssh szolgáltatást biztosító. Az ftp szolgáltatás elérése, annak dokumentálása után nagyszerű lehetőség egy következő fázis végrehajtásához, például vsFTPd Metasploittal való exploit-jának végrehajtására. [99]

A lopakodó TCP szkennelési módszerek másik csoportja az inverz TCP jelző szkennelés. Ez esetben a támadók TCP-próbacsomagokat küldenek beállított TCP-jelzőkkel, zászlókkal (FIN, URG, PSH) vagy zászlók nélkül. Amikor a portok nyitva vannak, a támadó nem kap semmilyen választ a számítógéptől, de a portok bezárásakor RST-t kap a célgépektől. A biztonsági mechanizmusok, mint például a tűzfalak és az IDS, felismerik a megcélzott állomások érzékeny portjaihoz küldött SYN csomagokat. A félig nyitott SYN zászlóval végzett vizsgálatok naplózására olyan programok érhetők el, mint például a Synlogger és a Courtney. Időnként a TCP zászlókkal engedélyezett próbacsomagok észlelés nélkül átjuthatnak a szűrőkön, a telepített biztonsági mechanizmusoktól függően. Az invertált technika a cél felmérése félig nyitott SYN zászló használatával, mivel a zárt portok csak a választ küldik vissza. Az RFC 793 szerint a kapcsolatra küldött RST/ACK csomag alaphelyzetbe áll, amikor a számítógép bezár egy portot. A támadók kihasználják ezt a funkciót, hogy TCP-próbacsomagokat küldjenek a célállomás minden egyes portjára, különféle TCP-jelzőkkel beállítva.



41. ábra *Inverz TCP jelző szkennelés (saját szerkesztés)*

A szondacsomaghoz használt általános zászlókonfigurációk a következők:

- FIN-szonda a beállított FIN TCP jelzővel;
- XMAS szonda a FIN, URG és PUSHTCP zászlókkal;
- NULL szonda, nincs beállítva TCP jelző;
- SYN/ACK szonda.

FIN Szkenn

A FIN-vizsgálat akkor fordul elő, amikor a támadó TCP szegmenseket küld az áldozatoknak a beállított FIN-jelzővel. A kapcsolat bezárását kéri, mivel további információk nem kerülnek elküldésre. Ennek a műveletnek az eredménye, hogy a célzott rendszer nem ad választ, ha a port inaktív, de ha a port nyitva van, akkor egy RST kerül visszaadásra, hasonlóan az Xmas tree vizsgálatához

A FIN-vizsgálatot nmap-ben a következőképpen hajtottam végre: *Nmap –sF <target IP address>*

```
root@kali:~# sudo nmap -sF -v  209.165.200.235

Starting Nmap 7.40 ( https://nmap.org ) at 2021-11-07 09:37 EST
Initiating Ping Scan at 09:37
Scanning 209.165.200.235 [4 ports]
Completed Ping Scan at 09:37, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:37
Completed Parallel DNS resolution of 1 host. at 09:37, 13.00s elapsed
Initiating FIN Scan at 09:37
Scanning 209.165.200.235 [1000 ports]
Completed FIN Scan at 09:37, 1.45s elapsed (1000 total ports)
Nmap scan report for 209.165.200.235
Host is up (0.0034s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
```

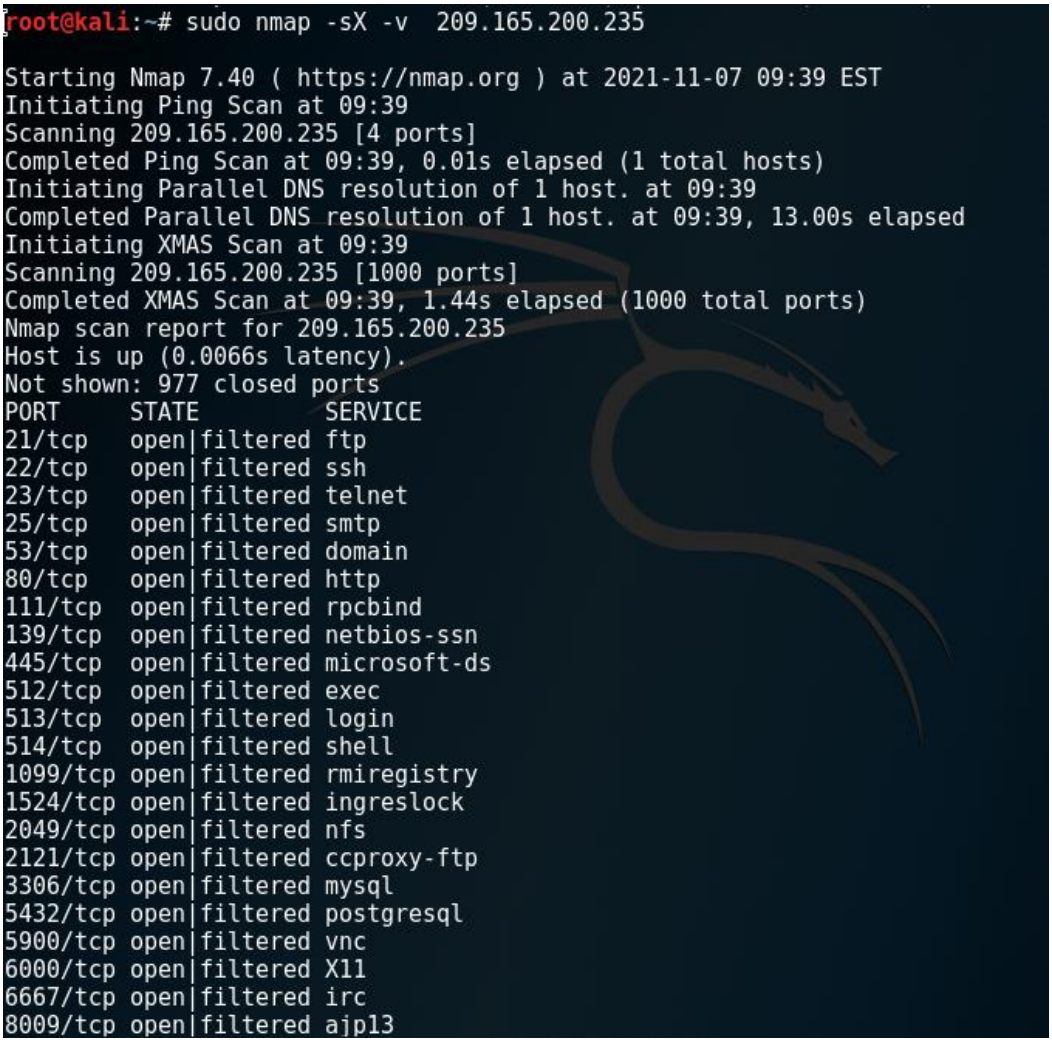
42. ábra *FIN szkenn nmap segítségével (saját szerkesztés)*

Xmas Szkenn

Az ilyen típusú szkennelés során több jelző van beállítva, ami azt jelenti, hogy egy csomagot egy ügyfélnek küldünk a SYN, PSH, URG és FIN segítségével, egyszerre beállítva ugyanazon a csomagon. Ha a célpont megnyitotta a portot, akkor a távoli rendszer nem fog

válaszolni. Ha a cél lezárta a portot, akkor távoli rendszer váltást fog kapni egy RST-vel. Az összes zászló beállítása után néhány rendszer lefagy, így a leggyakrabban beállított zászlók az URG, PSH, FIN értelmetlen mintája. A támadók a TCP XMAS szkenneléssel ellenőrzik, hogy az RST csomag segítségével a portok zárva vannak-e a célgépen. Ha a célrendszer elfogadja a csomagot, és nem válaszol, akkor azt jelenti, hogy a port nyitva van. Ha a célrendszer RST jelzőt küld, akkor egyszerűsíti a port bezárását. [100]

Az Xmas szkenn nmap-ben való vizsgálatát a következőképpen hajtottam végre: *nmap –sX –v <target IP address>*



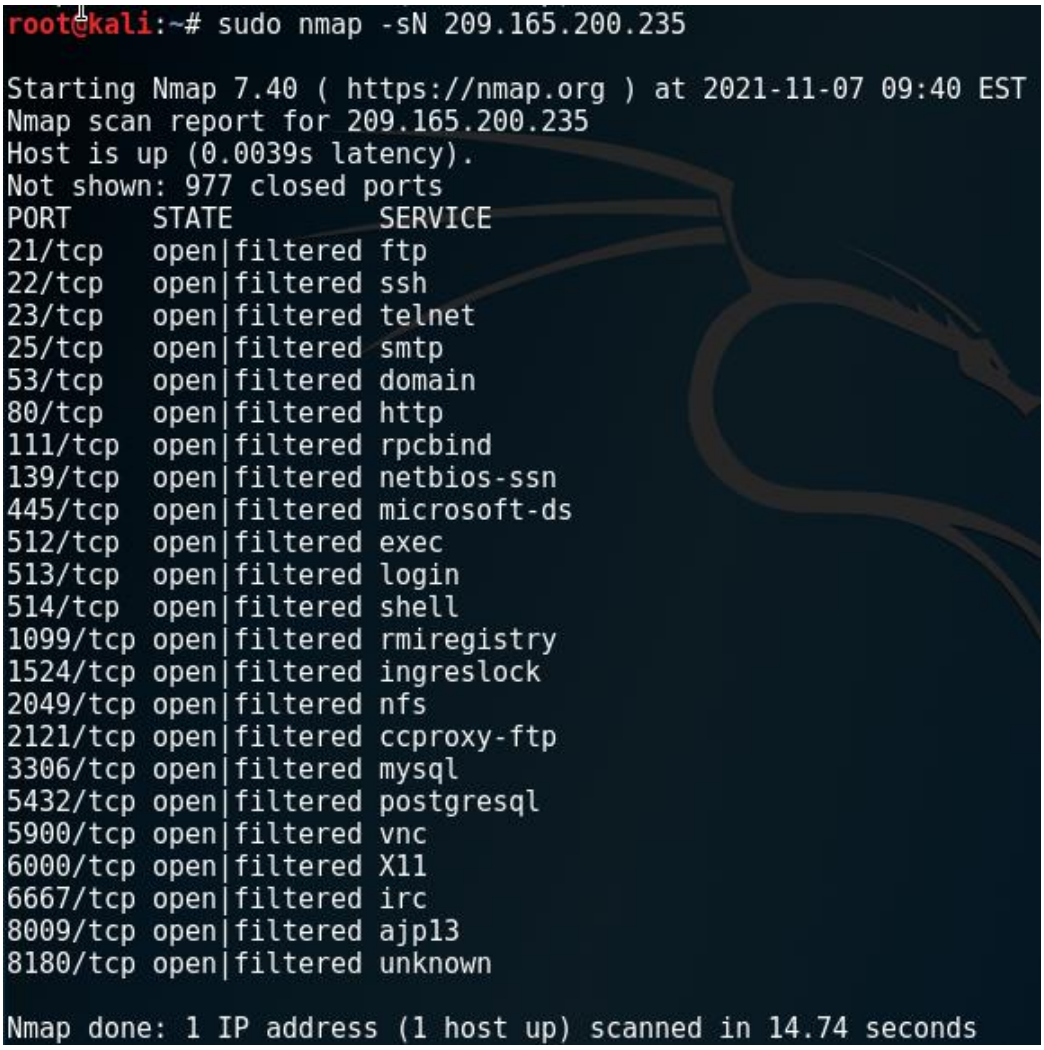
43. ábra *Xmas szkenn nmap segítségével (saját szerkesztés)*

NULL Szkenn

A NULL vizsgálat egy másik érdekes vizsgálat, amelyet végre lehet hajtani, és amely bizonyos módon ellentétes a Xmas vizsgálatával. A NULL vizsgálat elvégzéséhez egy csomag kerül küldésre egyáltalán nem beállított zászlókkal, és az eredmények megmutatják, hogy a port

nyitva vagy zárva van-e. A nyitott port nem válaszol, a zárt pedig egy RST-t ad vissza, ahogy azt a 41. ábra mutatja. [96]

A NULL szkenn nmap-ben való vizsgálatát a következőképpen hajtottam végre: *nmap –sN <target IP address>*



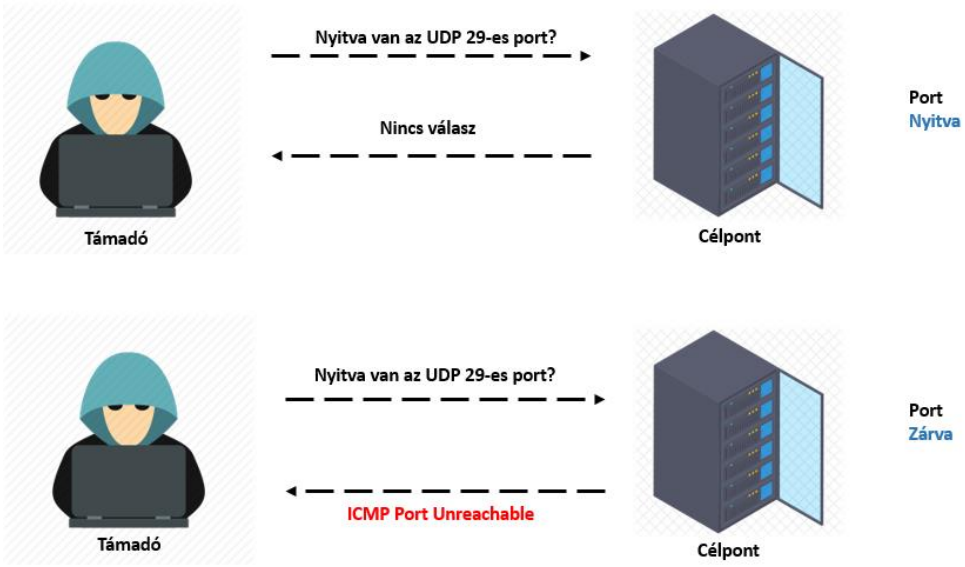
44. ábra *NULL szkenn nmap segítségével (saját szerkesztés)*

A FIN-szonda, XMAS szonda, NULL szonda segítségével alkalmazott felderítés alapján kijelenthető, hogy a tesztkörnyezetben található szerver rengeteg nyitott portot foglal magába, mint például a 21, 22, 23, 25, 53, 111, 139, 445, 512, 513, 514, 1099 portok. Ezek mind potenciális behatolási pontok, melyek alkalmasak a további felderítési és támadási tervek megalkotásához és végrehajtásához. Ha ezek a tervek a kibertéren belül katonai célpontokra vonatkoznak, és a saját kiberfölény elérését biztosítják, az katonai kiberműveletnek minősül.

4.2.2.2 UDP szkennelés

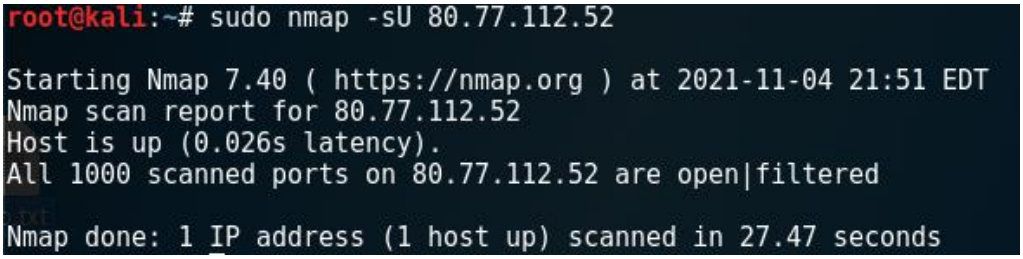
Az UDP, más protokollokkal ellentétben nem igazolja vissza a fogadást. Csak a lezárt port küld vissza egy üzenetet, hogy a port nem elérhető. Tehát szkenneljük a portokat, és várunk egy UDP-ICMP-PORT-UNREACH üzenetre. A szkennelésnek ez a módja nagyon hosszadalmas, és a pontossága nagymértékben a szkennelt számítógép kihasználtságától, illetve rendszererőforrásaitól függ. Ráadásul csak Linux operációs rendszer alatt működik, és azok a felhasználók, akik rootként vannak bejelentkezve, megkapják az ICMP PORT UNREACH üzeneteket. Ezeket a szkenneléseket csak a rendszergazda tudja elvégezni, hiszen rendszer admin jogok kellenek hozzá.

UDP-Recvfrom-And-Write szkennelés esetében, ellentétben az UDP-ICMP-PORT-UNREACH szkenneléssel, amelynél csak azok a felhasználók kapnak pozitív visszajelzést, akik rootként vannak bejelentkezve, az UDP-Recvfrom-And-Write szkennelés egy normál módon bejelentkezett felhasználónak is lehetővé teszi, hogy „érdekes" jelzéseket kapjon. A háttérben ismét egy bug áll: ha megpróbálunk egy portra írni, amelyik az UDP-ICMP-PORT-UNREACH szkennelésre ICMP-PORT-UNREACH választ adott (amiről normál felhasználóként nem értesülünk), akkor többnyire ezt az üzenetet kapjuk: Error 13 - Try Again, a normál Error 111 - Connection refused üzenet helyett. Ennél az eljárásnál tehát minden portot kétszer szkennelnek, egyszer, hogy a számítógép kiadjon egy választ, amit sajnos nem látunk, és másodszor, hogy mégis kapjunk informatív visszajelzést - 13-as hibánál a port le van zárva. Természetesen ez az eljárás is nagyon időigényes, és gyakran megbízhatatlan. [101]



45. ábra *UDP-Recvfrom-And-Write szkennelés (saját szerkesztés)*

Az általam végrehajtott UDP szkennelés: *nmap –sU <target IP address>*



46. ábra *UDP szkenn (saját szerkesztés)*

Az UDP kevésbé ismeri fel a nyitott portot, mivel nincs TCP kézfogás. Ha azonban az ICMP válaszol az egyes nem elérhető portokra, akkor az összes keretek száma meghaladhatja a TCP lekérdezésnél megadott keretek számát. Microsoft-alapú operációs rendszerek általában nem valósítanak meg ICMP-sebességkorlátozást, tehát ez a vizsgálat nagyon hatékonyan működik Windows-alapú eszközökön, amit egyértelműen előnynek minősítek. Viszont hátránynak vélem a teszt során, hogy az UDP vizsgálat csak portinformációt szolgáltat. Ha szükségesek további információ részletek is, akkor a vizsgálatot ki kell egészíteni egy verzió-detektálással (-sV) vagy az operációs rendszer ujjlenyomat-bekapcsolásával (-0). A legtöbb hálózat hatalmas mennyiségű TCP-forgalommal rendelkezik. Ennek eredményeként az UDP szkennelés hatékonysága elveszik.

Összességében kijelenthető, hogy a TCP és UDP porszkennelés teljesen alkalmas a nyitott portok és szolgáltatások feltárására, valamint az esetleges sérülékenységek predesztinálásához, ami további felhasználásra alkalmas. Hozzájárulhat a katonai kiberműveletekben a kiberfölény kialakításához.

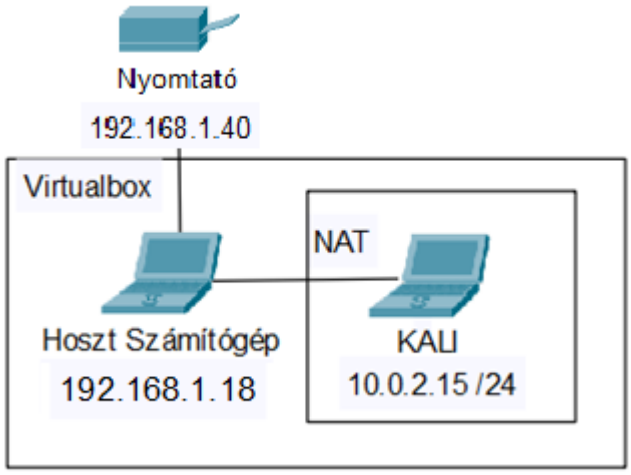
4.2.3 Felsorolási technika- Enumeration

Az enumeration a felhasználónevek, gépnevek, hálózati erőforrások, megosztások és szolgáltatások felsorolása vagy kinyerése egy rendszerből vagy hálózatból. Az enumeration szakaszban a támadó aktív kapcsolatokat hoz létre a rendszerrel, és irányított lekérdezéseket hajt végre, hogy további információkat szerezzen a célokról. A támadók az enumeration révén összegyűjtött információkat felhasználják a rendszerbiztonság sebezhetőségének vagy gyenge pontjainak azonosítására, ami elősegíti számukra a célrendszer kihasználását. Ez lehetővé teszi a támadók számára a jelszótámadásokat, annak érdekében, hogy jogosulatlan hozzáférést szerezzenek az információs rendszer erőforrásaihoz. [96]

Topológia 3. – SNMP felsorolási adatok információgyűjtése

Szükséges erőforrások:

- Kali Linux operációs rendszer;
- Internet elérés;
- Hoszt számítógép legalább 8 GB RAM-mal és 45 GB szabad lemezterülettel.



47. ábra *SNMP felsorolási technika alkalmazása (saját szerkesztés)*

Virtuális gép	Operációs rendszer	OVA méret	Lemezterület	RAM
Kali	Kali Linux	4.1GB	10 GB	1 GB

4. Táblázat: Célpontfelfedési tesztkörnyezet adatok (saját szerkesztés)

4.2.3.1 SNMP enumeration

Az SNMP felsorolja a felhasználói fiókok és eszközök listájának létrehozását a célszámítógépen. Az SNMP a kommunikációhoz kétféle szoftver komponenst alkalmaz. Ezek az SNMP ügynök és az SNMP felügyeleti állomás. Az SNMP ügynök a hálózati eszközön található, és az SNMP kezelő állomás kommunikál az ügyféllel. Szinte az összes hálózati infrastruktúra - eszköz, például routerek, switchek stb. tartalmaznak egy SNMP ügynököt a rendszer vagy eszközök kezelésére. Mind a kérések, mind a válaszok az ügynök szoftver által elérhető konfigurációs változók. Az SNMP felügyeleti állomások bizonyos változókhoz értékeket állítanak be. A csapdák értesítik a felügyeleti állomást, ha történt valami az ügynök oldalán, például újraindítás, interfész hiba vagy bármilyen más rendellenes esemény. [105]

Az SNMP két jelszót tartalmaz, amelyekkel konfigurálhatja és elérheti az SNMP ügynököt a felügyeleti státuszból. A két SNMP jelszó a következő:

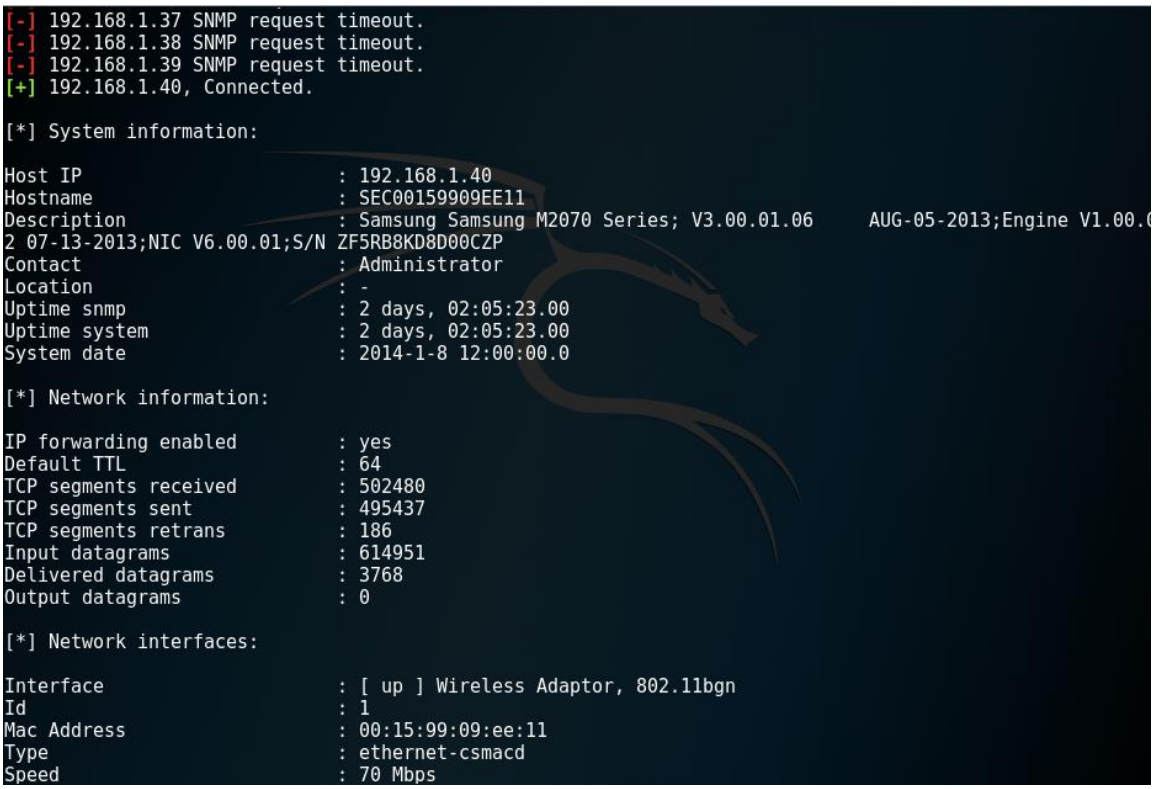
- Olvasási közösségi karakterlánc:
    - Az eszköz vagy rendszer konfigurációja ennek a jelszónak a segítségével tekinthető meg;
    - Ezek a karakterláncok nyilvánosak.
- Olvasási/írási Közösségi karakterlánc:
    - Az eszköz konfigurációja megváltoztatható vagy szerkeszthető ezzel a jelszóval;
    - Ezek a karakterláncok privát jellegűek.

Amikor a rendszergazdák az alapértelmezett beállításnál hagyják a közösségi karakterláncokat, a támadó ezeket az alapértelmezett közösségi karakterláncokat (jelszavakat) felhasználhatja az eszköz vagy rendszer konfigurációjának megváltoztatására vagy megtekintésére. Az SNMP felhasználható, hálózati erőforrásokról, például a hosztok, routerek, eszközökről, megosztásokról való infromációkinyerésre.

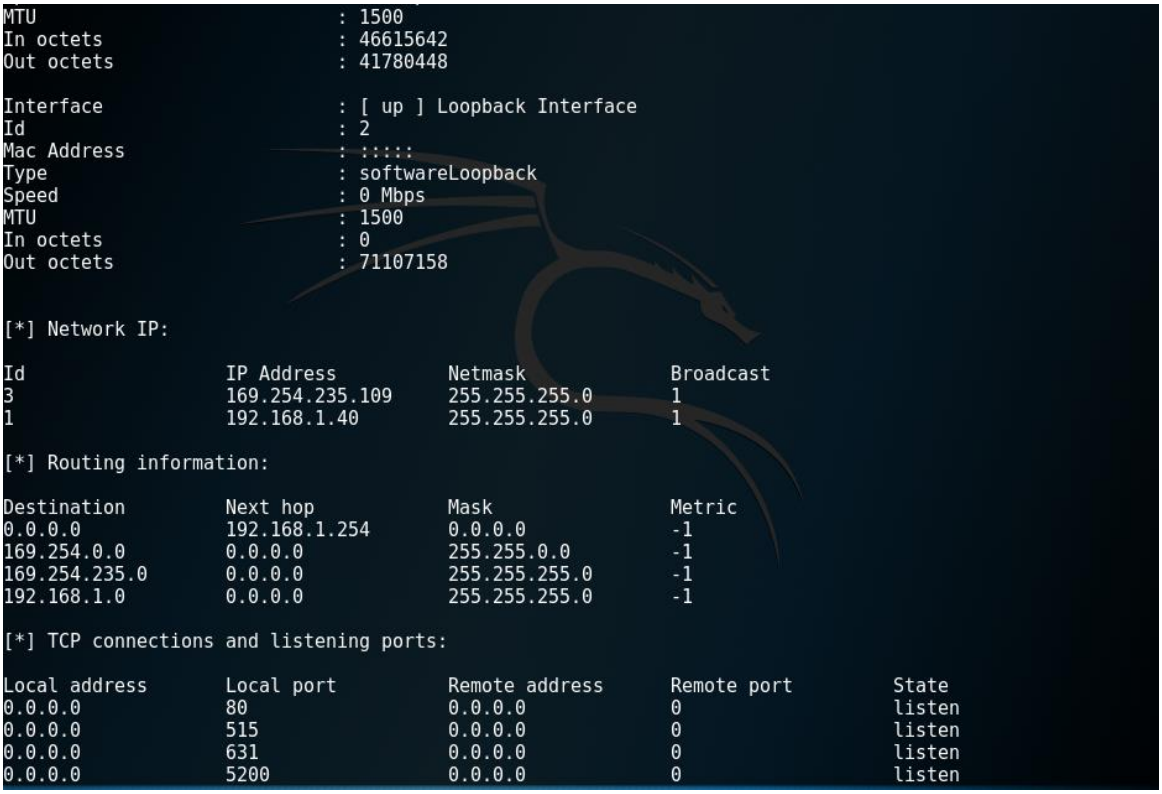
Végrehajtottam az SNMP enumerációt az MSFconsole segítségével:

```
msf auxiliary(snmp_enum) > set RHOSTS 192.168.1.0-192.168.1.254
RHOSTS => 192.168.1.0-192.168.1.254
msf auxiliary(snmp_enum) > run
```

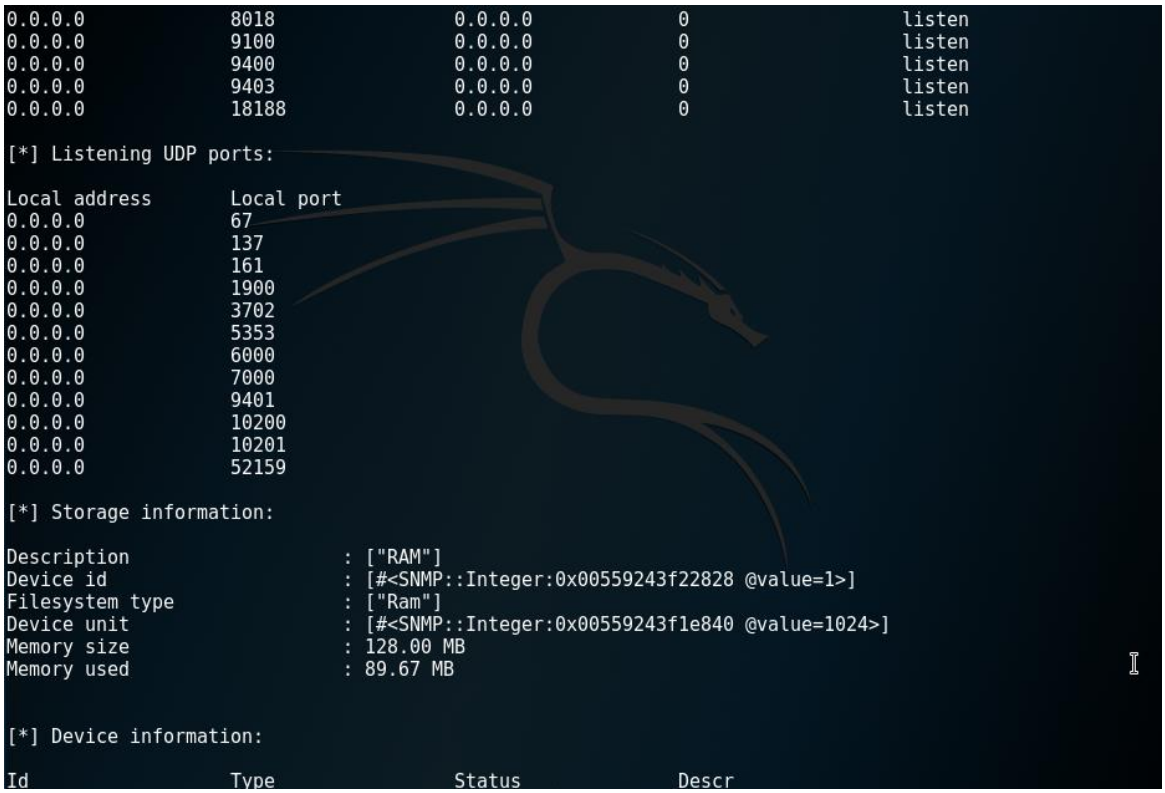
48. ábra *SNMP_enum használata (saját szerkesztés)*



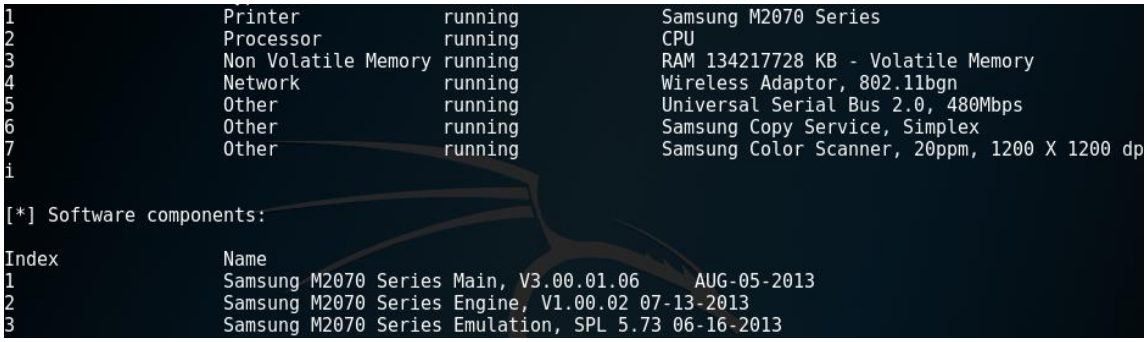
49. ábra *SNMP_enum által kinyert információ 1. (saját szerkesztés)*



50. ábra *SNMP_enum által kinyert információ 2. (saját szerkesztés)*



51. ábra *SNMP_enum által kinyert információ 3. (saját szerkesztés)*



52. ábra *SNMP_enum által kinyert információ 4. (saját szerkesztés)*

Összességében kijelenthető, hogy a felsorolási techikák közül az snmp enumarationt használva, az alapértelmezett snmp karakterláncok alkalmazása, vagy azok átálításának rendszeradminisztátori elmulasztása esetében, ahogy az a fenti ábrákon is látható, kilistáztható az adott eszköz IP címe, hoszt neve, hálózati kártyájának adatai (mint támogatott sebesség, típus, MAC cím). Ezen felül kinyerthető az eszköz memória, hardwer és szoftver komponensek adatai. Ezek alapvető kiindulási pontot jelenthetnek egy penetrációs teszt során.

4.3 KÖVETKEZTETÉSEK

A jelen kor katonai műveleteiben a modern technológia, a technikai alrendszerek kiberalapú kialakítása egyre inkább nagy jelentőséggel bír. Az értekezésben taglalt kibertér és kiberműveletek tulajdonságai tökéletesen jellemzik korunk műszaki innovációs fejlődésének igényét, ami a katonai műszaki rendszerekben is törvényszerűen meg kell, hogy jelenjen. A polgári fejlesztések eredményeképpen már működő eljárások katonai adaptációjára törekedve állítottam össze a fejezetet.

Ebben a fejezetben **meghatároztam** az információgyűjtés és hálózat-feltérképezés lépéseit, azok műszaki jellegű leírásait és elméleti hátterüket.

Alátámasztottam a technikai lépések jelentőségét, alkalmazásuk lehetőségét.

Interneten keresztüli mérésekkel és tesztekkel igazoltam a lépések alkalmazhatóságát, valamint **végrehajtottam** a keresőmotoros, webszolgáltatáson keresztüli, weboldal információgyűjtés, valamint a WhoIs és a DNS információk kibontásán keresztüli információgyűjtés műveleti és műszaki alkalmazásainak lényegi elemeit.

Saját tesztkörnyezetben mérésekkel és tesztekkel igazoltam a lépések alkalmazhatóságát, valamint **végrehajtottam** a célpont felfedés, portszkennelés, snmp fesorolási technika műveleti és műszaki alkalmazásainak lényegi elemeit.

Megalkottam a kiberműveletekben alkalmazható penetrációs teszt módszertanának alapstruktúráját, a hálózati felderítés technikai vonatkozásában.

Kidolgoztam és rendszereztem a felderítési műszaki lépéseket.

A fejezetben összefoglalt kutatásaim eredménye alapján az alábbi következtetéseket fogalmazom meg:

1. A civil informatikai rendszerekben már eredményesen alkalmazott adaptív eljárások térnyerése és sikere alapot szolgáltat azok katonai alkalmazásának áttekintésére. Katonai adaptáció esetén vizsgálni kell az érvényben lévő NATO és egyéb nemzetek szabványrendszereit.
2. A katonai penetrációs teszt módszertana alapján, a hálózati felderítés technikai folyamatában is lehetőség van az információgyűjtés és hálózat-feltérképezés megvalósítására külön a katonai alkalmazásokra tervezett műszaki dokumentáció és jelentés eljárások alkalmazásával, valamint a motiváció kihangsúlyozásával.
3. A civil informatikai hálózatok felderítési technikáinak mintájára a katonai kiberműveleti és informatikai penetrációs módszertanok is megtervezhetők a katonai

sajátosságok maximális figyelembevételével. Ez esetben kiemelt figyelmet kell fordítani a rendszerbiztonsági követelményeknek való megfelelésre.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Feldolgoztam és értelmeztem a kibertérrel, kiberműveletekkel kapcsolatos alapfogalmakat. Összefoglaltam a kibertérműveletek lényegi elemeit, többek közt a jellemzőit, elveit, típusait. Megvizsgáltam, és bemutattam két fő kibervédelmi fejlődési irányvonalait a NATO, illetve az USA szemszögéből. Ezekből azt a következtetést vontam le, hogy a hálózatok értelmezése napjainkra lényegesen megváltozott, az a kiberfizikai eszközök hálózatával, valamint az emberek révén létrehozott közösségi hálózatokkal egészült ki. A kibertér hálózatos lehetőségei miatt az információs műveleti képességek és hatások a katonai műveletekben is megmutatkoznak. A kiberműveletek felhasználhatók befolyásolásra, ellentevékenységre és védelemre egyaránt. Véleményem szerint a NATO jelentős erőfeszítéseket tett és fog tenni a kiberműveletekhez kapcsolódó képességek kialakítására és fejlesztésére, így mint NATO tagállam Magyarországnak és a Magyar Honvédségnek is hasonlóképpen kell eljárnia. A Magyar Honvédségen belül, a kiberbiztonsági stratégiával összhangban, a kiberbiztonsági képességek fejlesztése létfontosságú lehet a jövőben elvégzendő feladatok szempontjából.

Feldolgoztam a nemzetközi szabványok iránymutatásait, penetrációs teszttel kapcsolatos alapfogalmait és annak értelmezéseit. Összefoglaltam a különböző penetrációs teszt rendszermodellek lényegi elemeit, részletesen elemeztem a nyíltan elérhető legnépszerűbb penetrációs teszt szabványokat, ajánlásokat. Ezekből azt állapítottam meg, hogy a kiberbiztonsági penetrációs teszt az informatikai rendszerek alapos tanulmányozását biztosítja. Ez a tesztelési módszer komplex elemzést nyújt, amely lefedi a rendszer és a szervezet informatikai-biztonsági és kiberbiztonsági kérdéseit, és nagyban hozzájárulhat a Magyar Honvédség kiberműveleti erőfeszítéseihez. A módszertanok más megközelítést alkalmaznak a penetrációs teszt vagy biztonsági teszt elvégzésére. E különbségek megértése érdekében összehasonlítottam a különböző módszertanokat, megvizsgálva azok céljait, a gyakorlatban végzett tesztek tevékenységeit. A módszerek összehasonlításával világossá válik, hogy mind a négy módszertan eltérő megközelítést kínál a penetrációs teszt elvégzéséhez, és azok nem feltétlenül kompatibilisek egymással. Feldolgoztam és értelmeztem, valamint a nemzetközi szakirodalom alapján csoportosítottam a penetrációs teszt osztályzását. A tesztek osztályzásánál a megkülönböztető jellemzők között szerepel például a vizsgált rendszerek mérete, szerkezete, a tesztek elővigyázatossági vagy agresszív jellege. Azokat a jellemzőket,

amelyek egy adott penetrációs tesztre vonatkoznak, a teszt céljához kell igazítani annak érdekében, hogy hatékony és eredményes vizsgálatot lehessen végezni.

Meghatároztam a penetrációs teszt módszertanának a Magyar Honvédséggel való kapcsolatát működési és szervezeti szinten, valamint definiáltam a teszt katonai jellegét. Javaslatot tettem a penetrációs teszt munkafolyamatára. Mindezekre támaszkodva kialakítottam egy kiberműveleti penetrációs teszt terv dokumentumnak a különböző elemeit. Ezek alapján kijelentem, hogy a katonai rendszerek ma már digitális rendszerek, ezért alapvető követelmény a katonai digitális infokommunikációs hálózatokkal szemben a penetrációs teszt. Ezek a tapasztalatok támpontot adhatnak arra, hogy a szembenálló felet mely kibertéri rétegben és hogyan kellene vagy lehetséges támadni. A kibertérben történő katonai infokommunikációs rendszerek támadása katonai tevékenységnek minősül. A jelenlegi hazai jogszabályok és szabályzók alapján a Honvédelmi Minisztérium a KNBSZ keretein belül működteti saját, honvédelmi célú zárt és nyílt rendszerei kibervédelmét biztosító szervezetét, amely támogatja a honvédelmi célú informatikai rendszerek biztonságát, a bekövetkező biztonsági események ágazati szintű kezelését, és a sérülékenység vizsgálatok végrehajtását. A kiberműveleti penetrációs teszt módszertan egy alapvető keretet nyújt a fontos kezdeti és vizsgálat utáni információk lefektetésében, melyet az egyes alakulatok felhasználhatnak a KNBSZ által elvégezni kívánt auditok, ellenőrzések előtti felkészülésre. A kiberműveleti penetrációs teszt terv és tesztjelentés alkalmazása lehetővé teszi a hatékonyabb információáramlást, a döntéshozói és a végrehajtói szintek eredményesebb együttműködését, közös feladat-végrehajtását az informatikai biztonság és a kiberbiztonság területén.

Meghatároztam az információgyűjtés és hálózat-feltérképezés lépéseit, azok műszaki jellegű leírásait és elméleti hátterüket. Interneten keresztüli mérésekkel és tesztekkel igazoltam, valamint végrehajtottam a keresőmotoros, a webszolgáltatáson keresztüli, a weboldal információgyűjtés, valamint a WhoIs és a DNS információk kibontásán keresztüli információgyűjtés műveleti és műszaki alkalmazásainak lényegi elemeit. Saját tesztkörnyezetben mérésekkel és tesztekkel igazoltam, valamint végrehajtottam a célpont felfedés, portszkennelés műveleti és műszaki alkalmazásainak lényegi elemeit. Ezek alapján arra a következtetésre jutottam, hogy a civil informatikai rendszerekben már eredményesen alkalmazott adaptív eljárások térnyerése és sikere alapot szolgáltat azok katonai alkalmazásának áttekintésére. Katonai adaptáció esetén vizsgálni kell az érvényben lévő NATO és egyéb nemzetek szabványrendszereit. A katonai penetrációs teszt módszertanának alapján, a hálózati felderítés technikai folyamatában is lehetőség van az információgyűjtés és hálózat-feltérképezés megvalósítására külön a katonai alkalmazásokra tervezett műszaki dokumentáció

és jelentés eljárások alkalmazásával, valamint a motiváció kihangsúlyozásával. A civil informatikai hálózatok felderítési technikáinak mintájára a katonai kiberműveleti és informatikai penetrációs módszertanok is megtervezhetők a katonai sajátosságok maximális figyelembevételével. Ez esetben kiemelt figyelmet kell fordítani a rendszerbiztonsági követelményeknek való megfelelésre.

ÚJ TUDOMÁNYOS EREDMÉNYEK

1. **Megvizsgáltam** a kibertér, kibervédelem, kiberművelet definícióit, valamint **elemeztem és feldolgoztam** a NATO és az USA kibervédelmének fejlődését.
2. **Elemeztem** a nemzetközi penetrációs teszt modelleket. **Meghatároztam** az alapdefiníciókat, a teszt kulcsfontosságú tulajdonságait, valamint a főbb nemzetközi infokommunikációs biztonsági tesztelések felépítését. Mindezek alapján **létrehoztam** a penetrációs tesztek **saját megközelítésű osztályozását.**
3. **Értékeltem** a Magyar Honvédségre vonatkoztatott jogszabályi háttér előírásait, valamint kapcsolódási pontjait egy penetrációs teszttel, és ezek alapján **megalkottam** a penetrációs teszt Magyar Honvédségben alkalmazható folyamatának modelljét. **Létrehoztam** a kiberműveletekben alkalmazható penetrációs teszt módszertan végrehajtásának lépéseit.
4. **Megalkottam**, és saját megközelítésű módszertannal összhangban az általam **létrehozot**t osztályzási struktúrában **bemutattam** a kiberműveletekben alkalmazható penetrációs teszt módszertan hálózati felderítés elemeinek műszaki megvalósításának lépéseit, kiemelten a nyílt forráskódú technikai információgyűjtés és hálózat-feltérképezés megoldásaira. Műszaki **végrehajtásokon keresztül igazoltam és bizonyítottam** a lépések alkalmazhatóságát, annak eredményeit.

AJÁNLÁSOK

1. A kiberműveletekben alkalmazható penetrációs teszt módszertan technikai folyamata általam kialakított modelljét javaslom – kiber, illetve híradó és informatikai rendszergyakorlatok keretében – megvizsgálni, a gyakorlati tapasztalatokat integrálni a folyamatosan átalakuló, változó híradó támogatási rendszerbe.
2. Javaslom a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozattal összhangban, hogy a KNBSZ és a Magyarországon, az MH Pápa Bázisrepülőtéren települt, a nemzetközi Stratégiai Légiszállítási Képesség (SAC) és az azt támogató NATO Támogatási és Beszerzési Ügynökség közti kibervédelmet biztosító incidenskezelési jelentési lánc és kapcsolat létrehozását, beleértve a sérülékenységelemzés kiberműveleti képességét.
3. Értekezésemet, kutatásaim eredményeit javaslom feldolgozni mindhárom vezetési szinten szolgálatot teljesítő, a kiberműveletek, illetve híradó és informatikai perspektivikus vezetésének és irányításának kialakításában részt vállaló, arra kijelölt tiszti/főtiszti állománynak.
4. A kiberműveletekben alkalmazható penetrációs teszt módszertan elvi rendszerének áttekintését és oktatását javaslom a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar szaktanszékein.
5. A kiberműveletekben alkalmazható penetrációs teszt módszertan technikai felderítés műszaki megoldások vizsgálatát javaslom további kutatási alapként kezelni.

RÖVIDÍTÉSEK JEGYZÉKE

Rövidítés	Idegen Nyelvű Kifejtés	Magyar Nyelvű Kifejtés
ACK	Acknowledgement	Nyugta
APT	Advanced Persistent Threats	Előrehaladott tartós fenyegetések
ARP	Address Resolution Protocol	Címfeloldási Protokoll
AS	Autonomous System	Autonóm rendszer
CCDCOE	Cooperative Cyber Defence Centre Of Excellence	Kooperatív Kibervédelmi Kiválósági Központ
CERT-EU	Computer Emergency Response Team for the EU	Európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja
CMS	Content Management System	Tartalomkezelő Rendszer
CNCI	Comprehensive National Cybersecurity Initiative	Átfogó Nemzeti Kiberbiztonsági Kezdeményezés
DHCP	Dynamic Host Configuration Protocol	Dinamikus Hoszt Konfigurációs Protokoll
DHS	Department of Homeland Security	Belbiztonsági osztály
DMZ	Demilitarized Zone	Demilitarizált Zóna
DNS	Domain Name System	Domain Név Rendszer
DoD	Department of Defense	Védelmi Minisztérium
ENISA	European Union Agency for Cybersecurity	Európai Uniós Kiberbiztonsági Ügynökség
EU	Europian Union	Európai Unió
FCIO	Federal Chief Information Officer	információs vezérigazgató-helyettes
FedRamp	Federal Risk And Authorization Management Program	Szövetségi Kockázat- És Engedélykezelési Program
FISMA	Federal Information Security Management Act	Szövetségi Információbiztonsági Gazdálkodási Törvény
FTP	File Transfer Protocol	Fájlátviteli Protokoll
GHDB	Google Hacking Database	Google Hacking Adatbázis
HM	Ministry of Defense	Honvédelmi Minisztérium
HTML	Hypertext Markup Language	Hypertext Jelölőnyelv
HTTP	Hypertext Transfer Protocol	Hipertext Átviteli Protokoll
ICMP	Internet Control Message Protocol	Internet Vezérlés Üzenetprotokoll
IDS	Intrusion Detection System	Behatolás-Észlelő Rendszer
IETF	Internet Engineering Task Force	Internetes Mérnöki Munkacsoport
IoE	Internet Of Everything	Mindenek Internete

IoT	Internet Of Thing	Dolgok Internete
IP	Internet Protocol	Internet Protokoll
IPID	Ip Internet Identification	Ip Internetes Azonosító
IPS/IDS	Intrusion Prevention System/Intrusion Detection System	Behatolás-Megelőző Rendszer/Behatolás-Észlelő Rendszer
ISECOM	Institute for Security and Open Methodologies	Biztonsági és Nyílt Módszertani Intézet
IT	Information Technology	Informatika
ITU	International Telecommunication Union	Nemzetközi Távközlési Egyesület
J2EE	Java Platform, Enterprise Edition	Java Platform, Enterprise Kiadás
KNBSZ	-	Katonai Nemzetbiztonsági Szolgálat
MH BHD MH HIRFK IFK	-	Magyar Honvédség Vitéz Szurmay Sándor Budapest Helyőrség Dandár, Híradó És Informatikai Rendszerfőközpont, Informatikai Főközpont
Milcert	Military Computer Emergency Readiness Team	Katonai Eseménykezelő Központ
NATO	North Atlantic Treaty Organisation	Észak-Atlanti Szerződés Szervezete
NCCIP	National Cybersecurity and Critical Infrastructure Protection	Nemzeti Kiberbiztonsági és Kritikus Infrastruktúra Védelem
NCIRC	NATO Computer Incident Response Capability	Számítógépes Incidenskezelő Képesség
NIPP	National Infrastructure Protection Plan	Nemzeti infrastruktúravédelmi terv
NIST	National Institute Of Standards And Technology	Nemzeti Szabványügyi És Technológiai Intézet
NKE	National University of Public Service	Nemzeti Közszolgálati Egyetem
NSPA	NATO Support and Procurement Agency	Támogatási és Beszerzési Ügynökség
OMB	Office of Management and Budget	Igazgatási és Költségvetési Iroda
OSINT	Open Source Intelligence	Nyílt Forrású Hírszerzés
OSSTMM	Open Source Security Testing Methodology Manual	Nyílt Forráskódú Biztonsági Tesztelési Módszertan Kézikönyve
OWASP	Open Web Application Security Project	Nyílt Webalkalmazás Biztonsági Projekt
PCI	Payment Card Industry	Fizetési Kártya Ipar
PCI DSS	Payment Card Industry Data Security Standard	Fizetési Kártya Iparági Adatbiztonsági Szabvány
PDD	Presidential Decision Directive	elnöki határozati irányelv
PHP	Personal Home Page	Személyes Honlap
PTES	Penetration Testing Execution Standard	Penetrációs Vizsgálat Végrehajtási Szabvány
RAM	Random Access Memory	Tetszőleges Hozzáférésű Memória

RAS	Remote Access Services	Távoli Hozzáférési Szolgáltatások
RFC	Request For Comments	Vitára Bocsátott Anyag
RIR	Regional Internet Registry	Regionális Internetes Regiszter
RST	Reset	Visszaállító Üzenet
SAC	Strategic Airlift Capability	Stratégiai Légiszállítási Képesség
SMTP	Simple Mail Transfer Protocol	kommunikációs protokoll az e-mailek Interneten történő továbbítására
SMS	Short Message Service	Rövidüzenet-Szolgáltatás
SQL	Structured Query Language	Strukturált Lekérdezőnyelv
SSL	Secure Sockets Layer	Biztonsági Foglalat Réteg
SYN	Synchronization	Szinkronizációs Üzenet
TCP	Transmission Control Protocol	Átviteli Vezérlő Protokoll
TCP/IP	Transmission Control Protocol/Internet Protocol	Átviteli Vezérlő Protokoll/Internetprotokoll
TTL	Time-To-Live	Élettartam
UDP	User Datagram Protocol	Felhasználói Datagram Protokoll
URL	Uniform Resource Locator	Egységes Erőforráshely
Voip	Voice Over IP	Internetprotokoll Feletti Hangátvitel
WIFI	-Wireless Fidelity	Vezeték Nélküli Mikrohullámú Kommunikációt Megvalósító Szabvány
XSRF	Cross-Site Request Forgery	Oldalon-Keresztüli Kéréshamisítás
XSS	Cross Site Scripting	Keresztoldal Szkriptelés

ÁBRÁK JEGYZÉKE

HIVATKOZÁSOK

[1] Jens Stoltenberg*: Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference. London.* 2019.05.23. Elérhető: https://www.nato.int/cps/en/natohq/opinions_166039.htm (Letöltés időpontja: 2022. 02. 05.)

[2] NATO: *Declaration, Prague Summit issued by the Heads of State and Government participating in the meeting of the North Atlantic Council*, Prága, Cseh Köztársaság, 2002.11.21. Elérhető: https://www.nato.int/cps/en/natohq/official_texts_19552.htm (Letöltés időpontja: 2022. 02. 05.)

[3] NATO: *Declaration, Riga Summit Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council*, Lettország Riga 2006.11.29. Elérhető: https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en (Letöltés időpontja: 2022. 02. 05.)

[4] Kovács László: *Az e-közszolgálatfejlesztés nemzetbiztonsági és hadtudományi kérdései. Nemeslaki András (szerk.): E-közszolgálat fejlesztés: Elméleti alapok és tudományos kutatási módszerek.* Nemzeti Közszolgálati Egyetem, Budapest, 2014, Elérhető: http://real.mtak.hu/33733/1/E_kozszolgfejlesztes-nemeslaki.pdf (Letöltés időpontja: 2022. 02. 05.)

[5] NATO: *Warsaw Summit Communiqué.* Elérhető: www.nato.int/cps/en/natohq/official_texts_133169.htm (Letöltés időpontja: 2022. 02. 05.)

[6] Draveczki-Ury Ádám: *Átadták a Magyar Honvédség Kiber Képzési Központját* 2019.06.15. Elérhető: https://honvedelem.hu/galeriak/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat/ (Letöltés időpontja: 2022. 02. 05.)

[7] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról 2012/19 (február 21.) 1378 Elérhető: www.kozlonyok.hu/nkonline/MKPDF/hiteles/mk12019.pdf (Letöltés időpontja: 2022. 02. 05.)

[8] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2020/81., 2101–2119. Elérhető: https://magyarkozlony.hu/dokumentumok/6c9e9f4be48fd1bc620655a7f249f81681f8ba67/letoltes (Letöltés időpontja: 2022. 02. 05.)

[9] 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról. Magyar Közlöny 2012/175 (december 20.) 29705 Elérhető: www.kozlonyok.hu/nkonline/MKPDF/hiteles/mk12175.pdf http://webcache.googleusercontent.com/search?q=cache:w6VP9rionhoJ:2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf+&cd=1&hl=hu&ct=clnk&gl=hu&client=firefox-b-d (Letöltés időpontja: 2022. 02. 05.)

[10] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[11] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (Letöltés időpontja: 2022. 02. 05.)

[12] Balogh Fatime – Fekete Csanád - Németh András - Németh József Lajos: *A hibrid hadviselés különös tekintettel a mobil kommunikációra.* Hadmérnök, 10. évf. 4. sz. 2015. Elérhető: http://www.hadmernok.hu/154_12_balogf_na_joe.pdf (Letöltés időpontja: 2022. 02. 05.)

[13] ITU-T: *X.1205: Overview of cybersecurity*. 2008. Elérhető: https://www.itu.int/rec/t-rec-x.1205-200804-i (Letöltés időpontja: 2022. 02. 11.)

[14] DoD: *National Military Strategy for Cyberspace Operations*. 2006. Elérhető: https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-023.pdf (Letöltés időpontja: 2022. 02. 11.)

[15] DoD: *Terms & Definitions of Interest for DoD Counterintelligence Professionals*. 2011. Elérhető: https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf (Letöltés időpontja: 2022. 02. 11.)

[16] NATO: *NATO STANDARD AJP-3.20 ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS* Edition A Version 1 JANUARY 2020 Elérhető: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (Letöltés időpontja: 2022. 02. 11.)

[17] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról

[18] Haig Zsolt: *Információs műveletek a kibertérben* Budapest Dialóg Campus kiadó 2018.

[19] Haig Zsolt – Várhegyi István: *A cybertér és a cyberhadviselés értelmezése.* Hadtudomány, 18. évf. elektr. sz. 2008. Elérhető: http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf (Letöltés időpontja: 2022. 02. 11.)

[20] Haig Zsolt – Várhegyi István: *Hadviselés az információs hadszíntéren*. Budapest, Zrínyi. 2005.

[21] JP 3-12 (R): *Cyberspace Operations* 2013 Elérhető: https://fas.org/irp/doddir/dod/jp3_12r.pdf (Letöltés időpontja: 2022. 02. 11.)

[23] Kovács László: *Offenzív kiberműveletek 1.: Az offenzív kiberműveletek természete* Hadmérnök 16. évfolyam (2021) 2. szám., ISSN1788-1929 2018.09.

[24] FM 3-12 (2017): *Cyberspace and Electronic Warfare Operations*. Washington, D.C., Headquarters, Department of the Army. Elérhető: https://fas.org/irp/doddir/army/fm3-12.pdf (Letöltés időpontja: 2022. 02. 11.)

[25] Jobbágy Szabolcs: *Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő.* Hadmérnök IV. évfolyam 1. szám, 03. 2009. Elérhető: http://www.hadmernok.hu/2009_1_jobbagy.pdf (Letöltés időpontja: 2022. 02. 11.)

[26] ITU-T: *ITU-T X.1205 telecommunication standardization sector of ITU (04/2008) series x: data networks, open system communications and security telecommunication security overview of cybersecurity*. 8. Elérhető: https://www.itu.int/rec/T-REC-X.1205-200804-I. (Letöltés időpontja: 2022. 02. 11.)

[27] „Az Észak-atlanti Szerződés, Washington DC„1. 5. Cikk," 04. 04. 1949. Elérhető: https://www.nato.int/cps/ic/natohq/official_texts_17120.htm?Selectedlocale=hu. (Letöltés időpontja: 2022. 02. 13.)

[28] Kovács László – Szentgáli Gergely: *National Cyber Security Organization: Hungary 11*. 2015. Elérhető: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_HUNGARY_2015-10-12.pdf. (Letöltés időpontja: 2022. 02. 13.)

[29] NATO: *Bucharest Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council* in Bucharest, 03. 04. 2008. Elérhető: https://www.nato.int/cps/en/natolive/official_texts_8443.htm. (Letöltés időpontja: 2022. 02. 13.)

[30] Szentgáli Gergely: *A NATO kibervédelmi politikájának fejlődése*, 80 –85. Bolyai Szemle XXI. évf. 2. szám, 2012. Elérhető: http://archiv.uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf. (Letöltés időpontja: 2022. 02. 13.)

[31] NATO: *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Lisbon, Heads of State and Government at the NATO Summit*, 2010. Elérhető: https://www.nato.int/cps/ua/natohq/official. (Letöltés időpontja: 2022. 02. 13.)

[32] J. P. 3.-1. (R): *Cyberspace Operations*, 5. 02. 2013. Elérhető: http://www.dtic.mil/doctrine/new_ pubs/jp3_12R.pdf. (Letöltés időpontja: 2022. 02. 13.)

[33] Balla Tibor: *Hibrid hadviselés a NATO-ban,* Honvédségi Szemle 6. évfolyam 6. szám, HU ISSN 2060-1506," 11. 2010. Elérhető: http://193.22Ő.76.Ő/download/konyvtar/digitgy/tartalomjegyz/honv_szemle_2010_6.pdf. (Letöltés időpontja: 2022. 02. 13.)

[34] NATO: *NATO Summit Guide Warsaw*, 8–9. 07. 2016. Elérhető: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-SummitGuide_2016_ENG.pdf. (Letöltés időpontja: 2022. 02. 13.)

[35] The White House: *'The National Strategy to Secure Cyberspace',* 2003. Elérhető: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf. (Letöltés időpontja: 2022. 02. 13.)

[36] E. O. 13025, Amendment to Executive Order 13010, the President's Commission on Critical Infrastructure Protection, 1996.11.13 Elérhető: https://www.gpo.gov/fdsys/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2390-3.pdf. (Letöltés időpontja: 2022. 02. 13.)

[37] The White House: *PRESIDENTIAL DECISION DIRECTIVE/NSC-63* 1998.05.12 Elérhető: https://fas.org/irp/offdocs/pdd/pdd-63.pdf. (Letöltés időpontja: 2022. 02. 13.)

[38] Newmeyer, Kevin P.: *Who Should Lead U.S. Cybersecurity Efforts?*" 2012. Elérhető: http://cco.ndu.edu/Portals/96/Documents/prism/prism_3-2/prism115-126_newmeyer.pdf. (Letöltés időpontja: 2022. 02. 13.)

[39] The United States Congress: '*H.R.2458 –E-Government Act of 2002. 107th Congress (2001-2002)*' 2002. Elérhető: https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf. (Letöltés időpontja: 2022. 02. 13.)

[40] Public law 107–296: *107th Congress an Act To establish the Department of Homeland Security*, and for other purposes. 2002. 11. 25. Elérhető: https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf. (Letöltés időpontja: 2022. 02. 13.)

[41] U.S. Department of Homeland Security: *'Homeland Security Presidential Directive 7: Critical Infra-structure Identification, Prioritization, and Protection'*, 2003. Elérhető: http://www.dhs.gov/homeland-security-presidential-directive-7. (Letöltés időpontja: 2022. 02. 13.)

[42] National Infrastructure Protection Plan 2006. Elérhető: https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf. (Letöltés időpontja: 2022. 02. 13.)

[43] National Military Strategy for Cyberspace Operations Chairman of the Joint Chiefs of Staff Washington, 12. 2006. Elérhető: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf. (Letöltés időpontja: 2022. 02. 13.)

[44] The White House: *National Security Presidential Directive 54/ Homeland Security Presidential Directive 23*, 2008. Elérhető: https://fas.org/irp/offdocs/nspd/nspd-54.pdf. (Letöltés időpontja: 2022. 02. 13.)

[45] Comprehensive National Cybersecurity Initiative (CNCI), Elérhető: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf. (Letöltés időpontja: 2022. 02. 13.)

[46] Cyberspace Policy Review, Elérhető: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-028.pdf (Letöltés időpontja: 2022. 02. 13.)

[47] National Security Strategy Elérhető: http://nssarchive.us/NSSR/2010.pdf. (Letöltés időpontja: 2022. 02. 13.)

[48] Quadrennial Homeland Security Review, Elérhető: https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf. (Letöltés időpontja: 2022. 02. 13.)

[49] US Department of Defense U.S. Cyber Command Fact Sheet, Elérhető: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf (Letöltés időpontja: 2022. 02. 13.)

[50] Blueprint for Secure Cyber Future, Elérhető: https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf. (Letöltés időpontja: 2022. 02. 13.)

[51] International Strategy for Cyberspace, Elérhető: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. (Letöltés időpontja: 2022. 02. 13.)

[52] Improving Critical Infrastructure CyberSecurity (EO 13636), Elérhető:https://www.dhs.gov/sites/default/files/publications/EO-13636-Improving-Critical-Infrastructure-Cybersecurity-508.pdf. (Letöltés időpontja: 2022. 02. 13.)

[53] Presidential Policy Directive The Critical Infrastructure Security and Resilience 55, Elérhető: https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf. (Letöltés időpontja: 2022. 02. 13.)

[54] Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience, Elérhető: https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf. (Letöltés időpontja: 2022. 02. 13.)

[55] National Cybersecurity and Critical Infrastructure Protection (NCCIP), Elérhető: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf. (Letöltés időpontja: 2022. 02. 13.)

[56] U.S. Department of Army: *Cyber Electromagnetic Activities, No. 3-38,* Washington, 2014. Elérhető: http://fas.org/irp/doddir/army/fm3-38.pdf. (Letöltés időpontja: 2022. 02. 13.)

[57] Joint Cyberspace Operations Cyberspace Operations, Elérhető: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf (Letöltés időpontja: 2022. 02. 13.)

[58] Framework for Improving Critical Infrastructure, Elérhető: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. (Letöltés időpontja: 2022. 02. 13.)

[59] Krasznay Csaba: *A rendszer próbája: az etikus hackelés és penetrációs tesztelés.* krasznay.hu. 2008. június 18. Elérhető:

http://www.krasznay.hu/presentation/ethical_hacking_krasznay.ppt (Letöltés időpontja: 2022. 02. 13.)

[60] Krasznay Csaba: *E-közigazgatási rendszerek és alkalmazások sebezhetőségi vizsgálata* Hadmérnök V. Évfolyam 3. szám - 2010. szeptember

[61] Creasey, Jason – Glover, Ian: *A guide for running an effective Penetration Testing programme* 2017.04. Elérhető: https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf (Letöltés időpontja: 2022. 02. 13.)

[62] Georgia, Weidman: *Penetration testing A Hands-On Introduction to Hacking;* San Francisco ISBN-10: 1-59327-564-1 ISBN-13: 978-1-59327-564-8 2017. Elérhető: https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf (Letöltés időpontja: 2022. 02. 13.)

[63] Heriyanto, Tedi – Allen, Lee – Ali, Shakeel: Kali Linux –*Assuring Security by Penetration Testing,* Birmingham ISBN 978-1-84951-948-9; 2014.

[64] EC-council certified security analyst press: *Penetration Testing Procedures and Methodologies* ISBN-13: 978-1-4354-8367-5 ISBN-10: 1-4354-8367-7, USA 2011.

[65] Sági Gábor: *Informatikai rendszer támadási folyamata* XXVII. évfolyam, 2017. 3. szám Elérhető: https://folyoirat.ludovika.hu/index.php/mkk/article/view/1890/1178 (Letöltés időpontja: 2022. 02. 13.)

[66] NIST Special Publication 800-53A Revision 4: *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* Elérhető: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf (Letöltés időpontja: 2022. 02. 13.)

[67] Herzog, Pete: *OSSTMM 3 The Open Source Security Testing Methodology Manual,* ISECOM, Catalonia, 2010. Elérhető: https://www.isecom.org/OSSTMM.3.pdf (Letöltés időpontja: 2022. 02. 13.)

[68] OWASP: *OWASP Testing Guide Retrieved* 2014. Elérhető: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwierO6u9t7sAhV07eAKHWCACdYQFjAAegQIAxAC&url=https%3A%2F%2Fowasp.org%2Fwww-project-web-security-testing-guide%2Fassets%2Farchive%2FOWASP_Testing_Guide_v4.pdf&usg=AOvVaw2wUPlgVIRlP91IDkD-csvM (Letöltés időpontja: 2022. 02. 13.)

[69] The Penetration Testing Execution Standard Documentation Release 1.1 The PTES Team February 08, 2017.

[70] Shanley, Aleatha – N. Johnstone, Michael: *Selection of penetration testing methodologies: A comparison and evaluation* 2015 DOI: 10.4225/75/57b69c4ed938d

[71] Khan, Mohd. Ehmer – Khan, Farmeena: *A Comparative Study of White Box, Black Box and Grey Box Testing Techniques,* (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.6, 2012. ISSN 2156-5570

[72] Federal office for information security (bsi) study: *A Penetration Testing Model*; Bonn Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html (Letöltés időpontja: 2022. 02. 13.)

[73] Kennedy, David – O'Gorman, Jim – Kearns, Devon – Aharoni, Mati: *The Penetration Tester's Guide*, ISBN-10: 1-59327-288-X, ISBN-13: 978-1-59327-288-3 Elérhető: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiJp8DCk-HsAhWLlosKHY3iBP0QFjAFegQIBhAC&url=https%3A%2F%2Folinux.net%2Fwp-content%2Fuploads%2F2019%2F01%2FMetasploit-The-Penetration-Tester-s-Guide.pdf&usg=AOvVaw21RIut5zdE3KIlLdlNQQn8 (Letöltés időpontja: 2022. 02. 13.)

[74] Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1A 2006.

[75] Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B, Penetration testing Framework (PTF) 2006.

[76] Munk Sándor: *Kiberbiztonsági eseménykezelő szervezetek rendeltetése, feladatai*, XIII. Évfolyam 3. szám – 2018. június Elérhető: http://hadmernok.hu/182_30_munk.pdf (Letöltés időpontja: 2022. 02. 13.)

[77] 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

[78] Kovács Zoltán: *Kibervédelem és biztonság. In: Kibervédelem a bűnügyi tudományokban*, Ludovika Egyetemi Kiadó Nonprofit Kft. – Ludovika Press, Budapest, ISBN 9789635310302 2020. Elérhető: http://real.mtak.hu/107378/7/web_PDF_Kibervedelem_bunugyi_tudomanyokban-66-91.pdf (Letöltés időpontja: 2022. 02. 21.)

[79] 2011. évi CXIII. törvény, 80.§. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1100113.tv (Letöltés időpontja: 2022. 02. 21.)

[80] Krasznay Csaba: *A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban,* Nemzet és Biztonság 2017/3. szám |Elérhető: http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_3_05_krasznay_csaba_-_a_kiberbiztonsag_strategiai_vetuleteinek_oktatasi_kerdesei_a_kozszolgalatban.pdf (Letöltés időpontja: 2022. 02. 21.)

[81] 85/2014. (XII. 23.) HM utasítás a honvédelmi szervezetek 2015. évi fő célkitűzéseinek és fő feladatainak, valamint a 2016–2017. évi tevékenysége fő irányainak meghatározásáról Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=173364.286909 (Letöltés időpontja: 2022. 02. 21.)

[82] B. Müller Tamás: *Kiberhadviselés és katonai kibervédelem,* Infojegyzet országgyűlés hivatala közgyűjteményi és közművelődés igazgatóság képviselői információs szolgálat 2019. november 15.

[83] 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról

[84] Tihanyi Norbert – Vargha Gergely- Frész Ferenc: *Biztonsági tesztelés a gyakorlatban*, SBN 978-615-5491-59-7 2014. Elérhető: https://cmsadmin-pub.uni-nke.hu/document/vtkk-uni-nke-hu/biztonsagi-teszteles-a-gyakorlatban.original%20(1).pdf (Letöltés időpontja: 2022. 02. 21.)

[85] Chapple, Mike – Seidl, David: *CompTIA PenTest Study Guide*, ISBN: 978-1-119-50422-1 Indianapolis 2019.

[86] Paráda István: *Basic of cybersecurity penetration test*, Hadmérnök, 13. évf. 3. sz., ISSN1788-1929 2018.09.

[87] Kovács László: *A kibertér védelme*, Budapest: Dialóg Campus Kiadó, 2018.

[88] Alkhozae, Mona Ghotaish – Batarfi, Omar Abdullah: Phishing *Websites Detection based on Phishing Characteristics in the Webpage Source Code*, Volume 1 No. 6, October 2011 ISSN-2223-4985 International Journal of Information and Communication Technology Research

[89] Kovács Zoltán: *Webes nyomkövetési trendek vizsgálata,* Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar 2016. Elérhető: https://pet-portal.eu/files/articles/2017/Webes-nyomkovetesi-trendek-vizsgalata-Dolgozat-4.pdf (Letöltés időpontja: 2022. 02. 25.)

[90] Shrivastava, Vandana: *A Methodical Study of Web Crawler*, ISSN: 2248-9622 Vol. 8, Issue 11 (Part -I) Nov 2018, Elérhető: www.academia.edu/download/62956286/A081101010820200414-32205-ga36br.pdf (Letöltés időpontja: 2022. 02. 25.)

[91] Zhang, Wei – Wang, Wei – Zhang, Xinchang – Shi, Huiling*: Research on Privacy Protection of WHOIS Information in DNS*, DOI https://doi.org/10.1007/978-3-662-45402-2_11 Computer Science and its Applications Berlin, Heidelberg 2015. Online ISBN 978-3-662-45402-2 Elérhető: https://link.springer.com/chapter/10.1007/978-3-662-45402-2_11 (Letöltés időpontja: 2022. 02. 25.)

[92] What is the Harvester? Elérhető: https://www.cybervie.com/blog/what-is-the-harvester/ (Letöltés időpontja: 2021. 09. 12.)

[93] W. Beggs, Robert: *Mastering Kali Linux for Advanced Penetration Testing.* Birmingham: Packt Publishing, 2014. (Letöltés ideje: 2022. 02. 25.)

[94] Samant, Neha: *Automated penetration testing* (2011). Master's Projects. 180. DOI: https://doi.org/10.31979/etd.fxpj-pt6k Elérhető: https://scholarworks.sjsu.edu/etd_projects/180 (Letöltés időpontja: 2022. 02. 25.)

[95] Marchetta, Pietro – Donato, Walter de – Pescap, Antonio: *Detecting Third-Party Addresses in Traceroute Traces with IP Timestamp Option Passive and Active Measurement,* 14th International Conference, PAM 2013 Hong Kong, China, March 18-19, 2013 Proceedings e-ISSN 1611-3349, e-ISBN 978-3-642-36516-4, DOI 10.1007/978-3-642-36516-4 Elérhető: https://link.springer.com/chapter/10.1007/978-3-642-36516-4_3 (Letöltés időpontja: 2022. 02. 25.)

[96] Oriyano, Sean-Philip: *CEH™v9. [Certified Ethical Hacker]* 2016. Elérhető: DOI: https://doi.org/10.1002/9781119419303 (Letöltés időpontja: 2022. 02. 25.)

[97] Lyon, Gordon: The Official Nmap Project Guide to Network Discovery and Security Scanning ISBN: 978-0-9799587-1-7 Elérhető: http://insecure.org (Letöltés időpontja: 2022. 02. 25.)

[98] Patel, Satyendra Kumar - Sonker, Abhilash: *Rule-Based Network Intrusion Detection System for Port Scanning with Efficient Port Scan Detection Rules Using Snort,* International Journal of Future Generation Communication and Networking Vol. 9, No. 6 (2016), http://dx.doi.org/10.14257/ijfgcn. 2016.9.6.32 ISSN: 2233-7857 IJFGCN Elérhető: https://pdfs.semanticscholar.org/ce02/29f8e85305f52e759d172b00adecc626dbbc.pdf (Letöltés időpontja: 2022. 02. 25.)

[99] Paráda István – Tóth András: *A Metasploit tulajdonságai egy biztonságos FTP démon exploit tükrében,* Hadmérnök 15. évfolyam (2020) 3. szám Elérhető: DOI: 10.32567/hm.2020.3.12

[100] Fuertes, Walter - Zambrano, Patricio - Sánchez, Marco - Gamboa Pablo: *Alternative Engine to Detect and Block Port Scan Attacks using Virtual Network Environments,* IJCSNS International Journal of Computer Science and Network S 14 ecurity, VOL.11 No.11, November 2011. Elérhető: repositorio.espe.edu.ec/bitstream/21000/7037/1/AC-RIC-ESPE-047113.pdf (Letöltés időpontja: 2022. 02. 25.)

[101] Kumar, Sumit – Sudarsan, Sithu D,: *An Innovative UDP Port Scanning Technique,* International Journal of Future Computer and Communication, Vol. 3, No. 6, December 2014. Elérhető: www.ijfcc.org/papers/332-N0012.pdf (Letöltés időpontja: 2022. 02. 25.)

[102] Papp Gábor: *Google Search: a keresési operátorok teljes listája,* 2019., Elérhető: https://thepitch.hu/google-keresesi-operatorok-listaja/ (Letöltés időpontja: 2022. 02. 25.)

[103] Paráda, István - Bodnár, István: *Jelszó ellopás social engineering, e-mail spoofing és fake url segítségével* HÍRVILLÁM 7. 2016. Elérhető:https://docplayer.hu/25303188-Hirvillam-signal-badge-a-nemzeti-kozszolgalati-egyetem-hirado-tanszek-szakmai-tudomanyos-kiadvanya.html (Letöltés időpontja: 2022. 02. 25.)

[104] Bányász Péter: *A közösségi média, mint a nyílt forrású információszerzés fontos területe,* Nemzetbiztonsági Szemle, 2015. https://folyoirat.ludovika.hu/index.php/nbsz/article/download/1974/1259 (Letöltés időpontja: 2022. 02. 25.)

[105] Rafay Baloch: *Ethical Hacking and Penetration Testing Guide* International Standard Book Number-13: 978-1-4822-3162-5 2015.

A TÉMÁHOZ KAPCSOLÓDÓ PUBLIKÁCIÓIM

Lektorált folyóiratban megjelent cikkek:

1. Paráda, István: Műholdas antennarendszerek gyakorlati alkalmazhatósága a Magyar Honvédségben. Kommunikáció Budapest: Magyarország Zrínyi Miklós Nemzetvédelmi Egyetem, (2010) pp. 327-336. 10 p.
2. Paráda, István: NATO-ban használt műholdas antennarendszerek. HÍRVILLÁM = SIGNAL BADGE 2010: 1 pp. 100-105. Paper: 2061-9499, 6 p. (2010)
3. Pándi Erik, Paráda István, Jobbágy Szabolcs: A hálózat aktív és passzív eszközeinek, protokolljainak sebezhetőségére épülő támadások, szolgáltatások HÍRVILLÁM = SIGNAL BADGE V: 1 pp. 167-186., 20 p. (2014)
4. Bodnár István, Paráda István: Jelszó ellopás social engineering, e-mail spoofing és fake URL segítségével HÍRVILLÁM = SIGNAL BADGE 7: 1 pp. 139-147., 9 p. (2016)
5. Paráda, István: SNMP alapú hálózat monitoring program fejlesztése és alkalmazása-I. HÍRVILLÁM = SIGNAL BADGE 6: 1 pp. 73-88. Paper: 2061-9499, 16 p. (2015)
6. Pándi Erik, Paráda István: Network monitoring program development based on SNMP protocol HÍRVILLÁM = SIGNAL BADGE 6: 1 pp. 177-184., 8 p. (2015)
7. Paráda, István: Webkamera Hack – Penetration test, Hadmérnök XII: különszám pp. 204-216., 13 p. (2017)
8. Paráda, István: A NATO kibervédelmi irányelveinek fejlődése Honvédségi szemle: A magyar honvédség központi folyóirata 146: 3 pp. 3-13., 10 p. (2018)
9. Paráda, István: Requirements for developing the Cisco Net Academy to Pearson Vue Exam Center HÍRVILLÁM = SIGNAL BADGE 9: 1 pp. 20-36., 17 p. (2018)
10. Paráda, István: Felderítés és analízis a penetrációs tesztben – 1. Információgyűjtési technikák, Hadmérnök 15: 1 pp. 159-182., 24 p. (2020)
11. „A Metasploit tulajdonságai egy biztonságos FTP démon exploit tükrében”, Hadmérnök 15: 3 pp. 219-230., 12 p. (2020)

Idegen nyelvű kiadványban megjelent cikkek:

1. Social engineering in inforamtion infrastucture – cybersapce In: Ivan, MAJCHÚT; Vladimír, ANDRASSY; Štefan, GANOCZY; Michal, HRNČIAR; Ondrej, KREDATUS; Gabriela, KREDATUSOVÁ; Jakub, SASARÁK; Juraj, ŠIMKO; Jaroslav, VARECHA; Lubomír, BELAN; Stanislav, MORONG (szerk.) 8. medzinárodná vedecká konferencia: "NATIONAL AND INTERNATIONAL SECURITY 2017" Liptovsky Mikulas, Szlovákia: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, (2017) pp. 344-351., 8 p.
2. Possible classification of cybersecurity penetration test, Hadmérnök 13: 4 pp. 329-339., 11 p. (2018)
3. Cyberstrategy of united States – Cronology Process in the Light of the Goals, Hadtudományi szemle XI: 3 pp. 137-153., 17 p. (2018)
4. Basic of cybersecurity penetration test, Hadmérnök 13.: 3. pp. 435-442., 8 p. (2018)