DOKTORI (PHD) ÉRTEKEZÉS SZERZŐI ISMERTETŐJE

NEMZETI KÖZSZOLGÁLATI EGYETEM
Doktori Tanács

PARÁDA ISTVÁN

A kiberműveletekben alkalmazható penetrációs teszt módszertana

című Doktori (PhD) értekezés szerzői ismertetése

Témavezető:
Dr. Kovács László egyetemi tanár

Budapest, 2022

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

[1] Cooperative Cyber Defence Centre of Excellence - Kooperatív Kibervédelmi Kiválósági Központ.

[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.

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.

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.

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

Doktori (PhD) értekezésem elkészítése során az alábbi kutatási hipotéziseket fogalmaztam meg:

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.

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

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

Doktori (PhD) értekezésem elkészítése során alapvető célkitűzésnek tekintettem:

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.

KUTATÁSI MÓDSZEREK

Doktori (PhD) értekezésem elkészítése során az alábbi kutatási módszereket alkalmaztam:

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.
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[4] operációs rendszerrel hajtom végre;
8. A kísérleti méréseken alapuló adatok értékeléséből következtetéseket vonok le, és állapítok meg.

[4] 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.

AZ ELVÉGZETT VIZSGÁLAT TÖMÖR LEÍRÁSA FEJEZETENKÉNT

Értekezésem, felépítését tekintve négy fejezetet tartalmaz, melyek mindegyikét egy konklúzió formájában megfogalmazott, részkövetkeztetéseket, megállapításokat, részösszegzéseket tartalmazó résszel zárok le.

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.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Feldolgoztam és értelmeztem a kibertérrel, kiberművelettel 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.

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.

PUBLIKÁCIÓS JEGYZÉK

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)

SZAKMAI ÖNÉLETRAJZ

Személyes adatok:

Név: Paráda István
Születési hely, idő: Kisvárda 1991.02.08
Családi állapot: házas, két gyermek édesapja
Állandó lakcím: 6400 Kiskunhalas Kármán utca 27.
Telefonszám: 06-30-203-7729
E-mail: paradaistvan@gmail.com

MUNKAHELYI TAPASZTALAT

2021-	NSPA NATO TÁMOGATÓ ÉS BESZERZÉSI ÜGYNÖKSÉG CIS OPERATIONS OFFICER
2019- 2021	MERCEDES-BENZ MANUFACTURING HUNGARY KFT. IT PROJEKTMENEDZSER / HÁLÓZATI MÉRNÖK
2016-2019	NEMZETI KÖZSZOLGÁLATI EGYETEM HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR KATONAI ÜZEMELTETŐ INTÉZET HÍRADÓ TANSZÉK – TANÁRSEGÉD, CISCO INSTRUKTOR
2013 -2015	MH INFORMATIKAI FŐKÖZPONT – HÁLÓZATI RENDSZERMÉRNÖK

TANULMÁNYOK

2016-	Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola Doktorandusz
2013 - 2015	Óbudai Egyetem Kandó Kálmán villamosmérnöki kar (MSc) Villamosmérnök
2009-2013	Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar (BSc) Had és Biztonságtechnikai mérnök

NYELVISMERET

Angol Felsőfok C1
Német Alapfok B1

SZAKMAI MINŐSÍTETT
IRATOK, KÉPZÉSEK

- Crypto Administration (0004-221064 NCIA)
- Cards for NATO Crypto Custodian (0006-221080 NCIA)
- Cisco Certified Network Associate Routing and Switching (CCNA) 437794169816JODK
- Cisco Certified Entry Networking Technician (CCENT) 435274170890HLYG
- Elektronikus információs rendszerek védelméért felelős vezető PN-0277-1401-MS
- Incidensmenedzsment PN-0449-1710-MS-C1
- Célzott kibertámadások PN-0470-1712-MS-C1
- CCNA Cyber security Operations
- CISCO ICND1. Instruktor
- CISCO ICND2. Instruktor
- EUROPEAN SECURITY AND DEFENCE COLLEGE Kurzus (ESDC-CEPOL-NKE)
- CYBER DEFENCE AT OPERATIONAL LEVEL Kurzus (NATO CCDCOE)
- IST-143 - LS on Cyber Security Science & Engineering
- CNA Introduction to Cyber security
- CNA Cyber security Essentials
- CNA Connecting Things

TUDOMÁNYOS
ELISMERÉSEK, DÍJAK

- Az év információvédelmi szak- és diplomadolgozata – 2013” 1. helyzet.
- Magyar Hadtudományi Társaság emlékérem

TUDOMÁNYOS
KUTATÁSOK, ELŐADÁSOK

Tudományos kutatás:

- „Good Governance Knowledge Transfer Program NUPS – USA” kutatói pályázat 2018.01.03-2018.05.06 University of North Georgia Dahlonega USA

Kutatói előadások/óratartások:

- David Aghmashenebeli National Defence Academy of Georgia (under Russia in Gori) Cybersecurity tanfolyam;
- Nicolae Bălcescu Land Forces Academy, Sibiu, Romania – IT Networking tanfolyam;
- University of Defence, Brno, Czech Republic - Cyber Security tanfolyam;

- The Armed Forces Academy of General Milan Rastislav Štefánik, Liptovský Mikuláš, Slovak Republic - Cyber Security tanfolyam;
- Kutatók éjszakája előadás
- Kommunikáció konferencia előadás
- Katonai információvédelmi konferencia előadás

KÜLFÖLDI TAPASZTALATOK

- 2018. 5 hónap „Good Governance Knowledge Transfer Program NUPS – USA” 2018.01.03-2018.05.06 University of North Georgia Dahlonega USA
- 2018. Május, Románia Nagyszeben, Csehország Brno Erasmus
- 2017. Saber Guardian NATO gyakorlat– Multi National Division, IT Planning Officer beosztásban, Bulgária
- 2017. Október Szlovákia Liptószentmiklós Erasmus
- 2012. 5 hónap ERASMUS tanulmány, Lengyelország, Varsó

EGYÉB

- A Puskás Tivadar Híradó Bajtársi Egyesület tagja
- A Puskás Tivadar Műszaki Szakkollégium tiszteletbeli tagja