HADMÉRNÖK
VÉDELEMINFORMATIKA

18. évfolyam (2023) 3. szám 121–144.
DOI: 10.32567/hm.2023.3.9

Debrecceniné Deák Veronika[1]

Prototípus-implementáció kibervédelmi technikák gyakorlati oktatására

Prototype Implementation of Cybersecurity Techniques for Practical Education

Absztrakt

A kiberbiztonsági gyakorlatok feladata felkészíteni a felhasználókat a kibervédelmi stratégiák aktív és hatékony végrehajtására. Azonban számos jelenleg rendelkezésre álló platform és oktatási anyag alkalmazása szükségessé teszi a mélyebb informatikai ismereteket, így leginkább az IT-biztonság területén végzett szakértők képesek eredményesen ellátni ezeket a feladatokat.
A cél egy olyan oktatási anyag kidolgozása, amelyet akár a közszolgálatban, így például a közigazgatásban, illetve a honvédelemben részt vevő különböző szervezetekben vagy akár a magánszférában is képesek lehetnek alkalmazni olyan foglalkoztatottak továbbképzésére, akik nem rendelkeznek mélyebb informatikai előképzettséggel.
Jelen tanulmány célja a közszolgálati kiberbiztonsági gyakorlati oktatás keretében megvalósított szimulációs keretrendszer működésének definiálása, amelyben a hallgatók kibertámadások segítségével sajátíthatják el a védekezési mechanizmusok végrehajtásához szükséges készségeket, képességeket és ismereteket.

Kulcsszavak: kiberbiztonság, gyakorlati oktatás, szimulációs környezet, kibertámadás

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: deak.veronika@uni-nke.hu

Abstract

The aim of cyber security practices is to prepare employees to execute cybersecurity strategies actively and effectively. However, the use of several currently available platforms and educational materials requires deeper IT knowledge, hence mostly IT security experts are capable of performing these tasks effectively.
The ultimate goal is to develop educational materials that can be used to train employees without deeper IT background, either in various organizations of the public service, such as public administration or defence, or even in the private sector.
The aim of the present paper is to define the operation of a simulation framework implemented in the framework of public service cybersecurity training, in which students can acquire the skills, abilities and knowledge necessary to execute defence mechanisms in case of cyberattacks.

Keywords: cybersecurity, practical education, simulation environment, cyberattack

Bevezetés

A kiberbiztonság szerepe egyre nagyobb teret nyer az infokommunikációs eszközök és technológiák folyamatos fejlődésének köszönhetően. A hackerek sok esetben a felhasználók előtt járnak egy lépéssel, így mindig újabb és újabb kihívásokkal kell megküzdeni, ha biztonságban szeretnénk tudni információinkat és eszközeinket.

Számos, kibertérből érkező támadás veszélyeztetheti a saját infokommunikációs eszközeinket így például hordozható számítógépünket, mobiltelefonunkat, televíziónkat, okosóránkat és egyéb okoseszközeinket. Azonban gyakran tapasztalható, hogy a felhasználók csak felületesen ismerik eszközeik biztonságának összetevőit, valamint a hatékony és eredményes védekezési módszereket. Ebből következik, hogy a kiberbiztonság legnagyobb rizikóját a gyakorlati képességek hiánya okozza, amit már számos tanulmányban rögzítettek. Conklin, Cline és Roosa[2] szerint a kiberbiztonsági oktatás egyik legnagyobb problémája a hallgatók gyakorlati tapasztalatainak hiánya, ami azt eredményezi, hogy az elsajátított készségek nem felelnek meg az ipar igényeinek.

Több kutatás is vizsgálta már a kiberbiztonság oktatásának lehetőségeit, aminek keretében olyan platformokat is kialakítottak, amelyekkel a kibertámadások a gyakorlatban is kipróbálhatók. A probléma azonban sajnos az, hogy a legtöbb felhasználó nem rendelkezik részletes informatikai szaktudással, ami miatt az így átadható tudást nehezen vagy egyáltalán nem képesek felszívni. A meglévő platformok lehetőséget adnak a védelmi stratégiák kipróbálására, azonban olyan jellegű megoldásokat nehéz találni, amelyek elsősorban a védekezésre fókuszálnak.

Emiatt fontos feladat egy olyan gyakorlati képzés kialakítása, ahol a részt vevő hallgatók valós helyzetekben élhetik át a kibertámadásokat, és a védekezésre fókuszálnak úgy, hogy a támadás részletes felépítését, kialakítását, technikai hátterét nem kell ismerni. Egy ilyen gyakorlati képzés kialakítása komplex támadások implementációját

[2] Conklin–Cline–Roosa 2014: 2006–2014.

igényli mind szervezeti szinten (szerverkomponensek, VPN, egyéb perifériák stb.), mind személyes szinten (hordozható laptopok, mobiltelefonok stb.). Ezek alapján a gyakorlati képzést két szinten kell megvalósítani: saját infokommunikációs eszközök védelme, illetve szervezeti szintű rendszerek üzemeltetése és védelme.[3]

Jelen publikációban a saját infokommunikációs eszközök védelmére vonatkozó gyakorlati oktatásra készítettem egy egyszerűsített szimulációs környezetet, amelynek célja mély informatikai tudással nem rendelkező hallgatók kibervédelmi képességeinek fejlesztése és ezek gyakorlása.

Hipotézisek

A fentiek igazolására az alábbi hipotéziseket állítottam fel:

- H1 Szükséges egy olyan szimulációs környezet kidolgozása, amelynek segítségével kibervédelmi technikák gyakorolhatók.
- H2 Szimulálható olyan kibertámadás, amelynek azonosításához és megoldásához nem szükséges mély informatikai tudás.

Kutatásmódszertan

A fentebb említett hipotézisek megválaszolására az alábbi módszereket használtam fel:

A H1 hipotézis igazolására megvizsgáltam a jelenleg publikusan elérhető, kiberbiztonsághoz kapcsolódó platformokat, amelyeken részletes összehasonlító elemzést végeztem, hogy képesek-e kibertámadások szimulálására és ezzel a kibervédelmi képességek fejlesztésére.

A H2 hipotézis esetén kibertámadási forgatókönyveket definiáltam és szimuláltam egy általam kialakított platformon, amelyet mély informatikai tudás nélküli hallgatói csoporton értékeltem ki.

Előzetes technikai és fogalmi áttekintés

Ahhoz, hogy a jelen tanulmányban definiált szimulációs keretrendszer-prototípus minden részletre kiterjedő bemutatása megvalósulhasson, elengedhetetlen a kapcsolódó főbb fogalmak meghatározása.

Kibertámadások

Az első ilyen fogalom a *kibertámadás,* amelynek meghatározására számos definíció létezik. Az Egyesült Államok Kiberparancsnoksága által kiadott lexikon szerint a kibertámadás: számítógép vagy kapcsolódó hálózatok vagy rendszerek segítségével

[3] Deák 2020a: 159–177.

végrehajtott ellenséges cselekedet, amelynek célja egy ellenfél kritikus kiberrendszereinek, eszközeinek vagy funkcióinak megzavarása és/vagy megsemmisítése.[4] Hathaway és szerzőtársai szerint a kibertámadás minden olyan intézkedést magában foglal, amelyet politikai vagy nemzetbiztonsági célok eléréséért, a számítógépes hálózat funkcióinak aláásása érdekében hajtanak végre.[5] Owens meghatározása alapján a kibertámadás olyan szándékos cselekedetek végrehajtása, amelyek célja az ellenfél számítógépes rendszereinek vagy hálózatainak, illetve az ezekben a rendszerekben vagy hálózatokban maradó vagy azokon átmenő információk és/vagy programok megváltoztatása, megzavarása, megtévesztése vagy megsemmisítése.[6] Uma és Padmavathi szerint a kibertámadás a kibertér kiaknázása bizalmas információk megszerzése érdekében, ami magában foglalja például a kémkedést, a hálózatok letiltását, valamint adatok és pénz illetéktelen eltulajdonítását.[7]

A kibertámadások az alkalmazott technikától függően rendkívül sokfélék lehetnek, a teljesség igénye nélkül többek között ide sorolhatók a DoS-, DDoS-támadások, adathalászat, kártékony programok, keylogger programok, jelszavakra irányuló támadások, SQL-injektálás, közbeékelődéses (man-in-the middle) támadások.

A jelen tanulmányban ismertetett prototípusban a szolgáltatásmegtagadásos támadás (DoS), az adathalászat *(phishing)* és a hátsóajtó programok *(backdoor)* alkalmazását mutatom be a gyakorlatban, így ezen fogalmak ismerete is elengedhetetlen.

A DoS (Denial of Service), más néven *szolgáltatásmegtagadással járó támadás* lényege, hogy olyan sok kéréssel támadják meg a hálózatot, vagy azon keresztül valamelyik alkalmazást, amennyit a fogadó oldal már nem tud feldolgozni. Ennek következtében nem lesz elérhető az adott szolgáltatás, mivel nem tud kiszolgálni egyszerre ennyi kérést a szerver.[8] A támadás irányulhat a célpont hálózati kapcsolatának vagy pedig a célpont rendszerében működő valamely – szolgáltatást nyújtó – alkalmazásának túlterhelésére, amelynek során a támadó célja a célpont erőforrásainak lefoglalása.[9]

Az *adathalászat,* más néven phishing lényege abban rejlik, hogy az adathalászok a felhasználókat valamilyen elektronikus csatornán keresztül – például e-mailben, azonnali üzenetben vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában azonban egy hamis weboldalra irányítják, ahol arra kérik őket, hogy adják meg bizalmas adataikat. Az adathalászatnak számos válfaja van, aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra.[10]

A hátsóajtó-alkalmazás *(backdoor)* a felhasználók számára általában nem látható elem, amely a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti

[4] Cartwright 2011.
[5] Hathaway et al. 2012: 817–885.
[6] Owens–Dam–Lin 2009.
[7] Uma–Padmavathi 2013: 390–396.
[8] Fehér 2016.
[9] Gyányi 2007.
[10] Muha–Krasznay 2018.

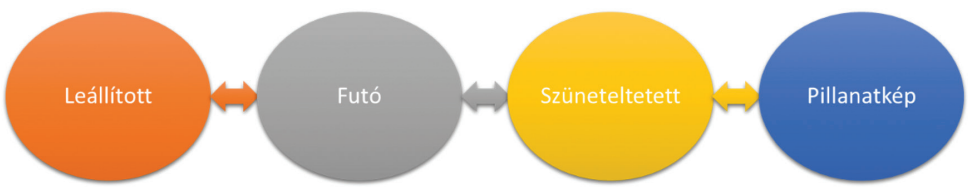
a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nemcsak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti.[11]

Virtualizáció

A *virtualizáció* több számítógép szimulációja egy hardverkonfiguráción, vagyis hardverek emulációja szoftveres környezetben. Ez lehetővé teszi egy eszköz erőforrásainak felosztását több környezet között. A virtualizáció céljai közé tartozik a meglévő erőforrások kihasználtságának maximalizálása, az IT-szolgáltatások rugalmasságának fejlesztése, a rendszerek biztonságának növelése és a leállások szükséges idejének csökkentése, valamint a meglévő rendszerek kezelésének egyszerűsítése, költségeinek csökkentése.[12]

A virtualizációt csoportosíthatjuk például aszerint, hogy a fizikai eszközöktől milyen szinten választják el a rendszert. Jelen tanulmányban a prototípus elkészítése szempontjából releváns virtualizációtípus az operációs rendszer virtualizációja. Amikor operációs rendszert virtualizálunk, általában egy gazda *(host)* operációs rendszeren futtatunk egy vagy több vendég *(guest)* operációs rendszert.[13]

Egy virtuális gép állapotait, általános struktúráját szemlélteti az 1. ábra, illetve látható, hogy mely állapotokból mely állapotokba lehet jutni. A virtuális gépeket először is leállított formában hozzuk létre. A leállított virtuális gépet el lehet indítani, aminek hatására futó állapotba kerül. A futó állapotban természetesen a virtuális gép leállítható, illetve szüneteltethető. A szüneteltethető állapotban a virtuális gép nem áll le, csak felfüggesztjük a működését, és elmentjük a memória tartalmát. A szüneteltetésből azonnal folytatható a működés, ekkor futó állapotba kerül, illetve a szüneteltetett állapotban pillanatkép készíthető. A pillanatképből a virtuális gép automatikusan elindítható úgy, hogy a szüneteltetett állapotba kerül.



1. ábra: Virtuális gépek állapotai
Forrás: a szerző szerkesztése

[11] Deák 2019: 256–271.
[12] Varga 2010.
[13] Varga 2010.

Kibergyakorlatok csoportosítása

A gyakorlati kiberbiztonsági ismeretek átadására már számos technológia áll rendelkezésünkre. Fő szempont, amely megkülönbözteti őket egymástól, hogy a támadók és a védekezők aktív vagy passzív szerepet vállalnak a kibergyakorlatokban. Ezek alapján az alábbi típusokat különböztethetjük meg:

- *aktív-aktív:* a támadó és a védekező oldalt is valós személy képviseli, avagy valós személy irányítja a támadást, illetve a védekezést (Elsősorban csapatjátékok, ahol az egyik csapat megpróbálja feltörni a másik csapat rendszerét, miközben a másik csapat védekezik. Ilyen például a Capture the Flag, Red-Blue Team gyakorlatok.);
- *aktív-passzív:* az áldozat egy passzív rendszer, míg a gyakorlat során a hallgatóknak kell a támadó szerepét megszemélyesíteni annak érdekében, hogy az áldozat infrastruktúra gyenge pontjait felderítve adatokat szerezzen meg;
- *passzív-aktív:* a támadó egy passzív rendszer, amely előre beállított támadási szekvenciát játszik le automatizáltan, külső felügyelet nélkül, míg a hallgatóknak az áldozat szerepét kell megvalósítaniuk, amelynek során fel kell ismerniük az aktuális támadásokat, és azokat meg kell akadályozniuk, helyre kell állítaniuk és reagálniuk kell a már bekövetkezett eseményekre;
- *passzív-passzív:* elsősorban tesztelési célból, illetve kibertámadások szemléltetésére alkalmazzák, valamint többek között olyan automatizált kibervédelmi rendszerek tesztelésére, amelyeknek célja helyettesíteni, kiváltani az áldozatot, ezáltal külső felügyelet nélkül megakadályozni a kibertámadásokat;
- *általános:* olyan kiberbiztonsági gyakorlatok végrehajtására alkalmas platformok, amelyeken az előbb felsorolt típusok bármelyike megvalósítható. Legtöbb esetben hálózatok és számítógépek emulálását végzik, amelyen keresztül tetszőleges kibergyakorlat szimulálható;
- *egyéb:* olyan kiberbiztonsági gyakorlatok, amelyek az előző kategóriákba nem sorolhatók, de szorosan kapcsolódnak a kibergyakorlatokhoz és a kiberbiztonsági ismeretek gyakorlati oktatásához, így különösen társasjátékok, számítógépes játékok.

Publikusan elérhető kiberbiztonsági platformok összehasonlítása

A H1 hipotézis vizsgálatához szükséges áttekinteni az aktuálisan publikusan elérhető kiberbiztonsági gyakorlatokhoz használható platformokat, amelyeket a korábban bevezetett csoportosítás alapján mutatok be. Az 1. táblázat szemlélteti kategóriánként a rendelkezésre álló releváns technológiákat, platformokat és azok jellemzőit.

1. táblázat: Kiberbiztonsági platformok összehasonlítása

Technológia	Kategória	Elérhetőség	Célközönség	Telepítés
KYPO	aktív-aktív	online	akadémia/kutatás	×
CDX	aktív-aktív	offline	hallgatók/szakértők	×
Emulab	általános	offline	akadémia/kutatás	komplex
Cytrone	általános	offline	akadémia/kutatás	komplex
Leaf	általános	offline	hallgatók/szakértők	komplex
Cyber-Physical Security Testbed	általános	offline	hallgatók/szakértők	komplex
VulnHub	aktív-passzív	offline	hallgatók/szakértők	szabadkéz
TryHackMe	aktív-passzív	online	hallgatók/szakértők	×
WebGoat	passzív-aktív	online	hallgatók/szakértők	×
Metasploitable	aktív-passzív	offline	hallgatók/szakértők	szabadkéz
Blackjack	passzív-passzív	offline	hallgatók/szakértők	komplex
ACD	passzív-passzív	offline	hallgatók/szakértők	komplex
Cyber Defence Tower Game	egyéb	offline	gyerekek	egyszerű
Riskio	egyéb	offline	gyerekek	×

Forrás: a szerző szerkesztése

Kategória

A feldolgozott technológiákat, eszközöket több csoportba lehet sorolni aszerint, hogy a kibergyakorlatok korábban nevesített osztályozása alapján melyik csoportba oszthatók.

Az Emulab, a Cytrone, a Leaf és a Cyber Security Testbed általános platformokat definiálnak. Az Emulab[14] egy olyan rugalmas felépítésű gyakorlati kurzus, amely során valódi hackertámadások végrehajtásával mutatják be a kibertámadások egyes módszereit, ami irányítható környezetet biztosít a támadó és védekező kiberbiztonsági kísérletek előkészítésére és mérésére. A Cytrone[15] nevű integrált kiberbiztonsági képzési keretrendszer magában foglalja a támadásorientált, az elemzésorientált, valamint a védelemorientált képzést. Ennek keretében speciálisan erre a célra létrehozott képzési környezetben végrehajtható gyakorlati feladatokat biztosítanak a hallgatók számára. A keretrendszer elemei közé sorolhatók a következők: a felhasználói felület, a képzési adatbázis, a menedzsmentmodul, lehetséges további hozzáadható modulok, valamint a szerverek és hálózati eszközök infrastruktúrája. A Leaf[16] kiberinfrastruktúrák szimulálására, valósághű IoT-forgatókönyvek reprodukálására és versenyképes kiberbiztonsági tréningek végrehajtására szolgáló nyílt forráskódú platform. A Cyber

[14] Kuo et al. 2018: 2245–2258.
[15] Beuran et al. 2017: 157–166.
[16] Ficco–Palmieri 2019: 107–129.

Security Testbed[17] egy kiberfizikai biztonsági platform, amely alkalmas kibertámadások szimulálására és kiértékelésére, valamint a segítségével végrehajtott behatolástesztek által feltárhatók az elektromos hálózatokra irányuló kibertámadások következményei és hatásai.

A KYPO és a CDX elsősorban olyan környezetet határoznak meg, ahol Capture The Flag jellegű feladatok hajthatók végre, vagyis mind a támadó, mind a védekező félnek aktívnak kell lennie. A KYPO[18] egy kibergyakorlati és kutatási platform, amely komplex számítógépes rendszerek és hálózatok modellezésére és szimulálására összpontosít. A platform virtualizált környezetet biztosít előre meghatározott forgatókönyv szerinti, komplex kibernetikai támadások végrehajtásához egy szimulált kritikus infrastruktúra ellen. A CDX[19] gyakorlat sajátossága, hogy a részt vevő csapatoknak saját magunknak kell kialakítani hálózatukat, azon elvégezni a biztonsági beállításokat, amit a támadás külső fél általi végrehajtása követ. A biztonsági kihívások megértése és az incidensekre való reagálás, valamint a csapatmunkával kapcsolatos készségek fejlesztése egyaránt célja a gyakorlatnak.[20]

A Vulnhub,[21] a TryHackMe[22] és a Metasploitable[23] elsősorban a támadó felek számára biztosítanak lehetőséget a fejlődésre (aktív-passzív), míg a WebGoat[24] alkalmazás elsősorban védekezésorientált (passzív-aktív).

Automatizált kibervédelemmel kapcsolatos technológiák a Blackjack,[25] illetve az ACD,[26] amelyek célja, hogy emberi beavatkozás nélkül képesek legyenek a támadások elhárítására, emiatt ők a passzív-passzív kategóriába sorolhatók.

Végül a Cyber Defence Tower Game[27] egy egyszerű számítógépes Tower Defense játék, míg a Riskio[28] egy társas táblajáték, amelyek inkább kedvcsináló és ösztönző eszközök lehetnek az oktatásban, mintsem konkrét tudásátadásra használható technológiák.

Elérhetőség

A technológiák kiválasztásánál fontos szempont lehet az is, hogy a felhasználó képes-e internetelérés nélkül is használni a technológiát. Ez alapján a kapcsolódó munkák lehetnek

- *online elérhetők,* vagyis internethálózatra van szükség ahhoz, hogy a feladatokat megoldják,

[17] Hong et al. 2015.
[18] Čeleda et al. 2015.
[19] Schepens–James 2003: 4300–4305.
[20] Szabó 2018: 286–301.
[21] Lásd: www.vulnhub.com
[22] Lásd: https://tryhackme.com
[23] Kennedy et al. 2011.
[24] Lásd: https://owasp.org/www-project-webgoat
[25] Heckman et al. 2013: 72–77.
[26] Herring–Willett 2014: 46–55.
[27] Jin et al. 2018: 68–73.
[28] Hart et al. 2020.

- *offline elérhetők,* vagyis nem szükséges az internethálózat, a felhasználó a saját lokális számítógépén is előállíthatja a környezetet.

Míg a KYPO, a TryHackMe és a WebGoat esetében szükséges az internetelérés, addig a többi esetben offline elérhető technológiákról beszélhetünk.

Célközönség

A különböző technológiák különböző célközönséget szólítanak meg. Ez alapján az alábbiak lehetnek:

- *akadémia/kutatás:* elsősorban az akadémiai életben használják a technológiát, leginkább prototípus szinten, mintsem termékként. Az elért eredményeket pedig kutatási célokra is felhasználják.
- *hallgatók/szakértők:* olyan kiforrott maga a technológia, hogy arra már termékként is tekinthetünk, amelyeken szervezett oktatás zajlik kiberbiztonsági szakértők számára, akik már jártasak az informatikai ismeretekben is.
- *gyerekek:* azok a technológiák, amelyek elsősorban figyelemfelhívásra, a tudatosság növelésére, esetleg kedvcsinálásra és motiválásra alkalmasak.

A KYPO, a Cytrone és az Emulab rendszer elsősorban akadémiai célból készült, míg a Riskio, valamint a Cyber Defence Tower Game a biztonságtudatosság növelését célozza minden korosztály számára. A többi technológia a célcsoportot tekintve a szakértők kategóriába sorolható, vagyis mély informatikai tudással rendelkező, önmagukat képezni kívánó szakembereket szólít meg.

Telepítés

A vizsgált technológiák kategorizálhatók aszerint, hogy a kibergyakorlatok során alkalmazott technológiák telepítése hogyan történik:

- *komplex*: amely során komplex rendszereket, többféle alkalmazást, programot szükséges telepíteni, továbbá számos beállítás, virtualizáció indokolt;
- *szabadkéz*: nincs meghatározva, hogy mit kell telepítenie a felhasználónak, egy virtuális gépet kap, amelyet szabadon felhasználhat;
- *egyszerű*: a telepítéshez nem szükséges mélyebb informatikai tudás.

A Vulnhub és a Metasploit nem definiál részletes környezetet a gyakorlatok elvégzéséhez, mindössze egy-egy virtuális gépet kell letöltenie a felhasználónak, amelyet oly módon használ, ahogyan csak szeretne. Az Emulab, a Cytrone, a Leaf és a Cyber-Physical Security Testbed esetén egy teljes architektúrát kell előállítani különböző programok segítségével, amelyhez bár részletes leírás tartozik, mégis komplex műveletnek tekinthető. Végül a Cyber Tower Defence Game esetében egy egyszerű programról van szó, amelyet a számítógépünkre kell telepíteni. A többi technológiához kapcsolódóan nincs szükség telepítés elvégzésére.

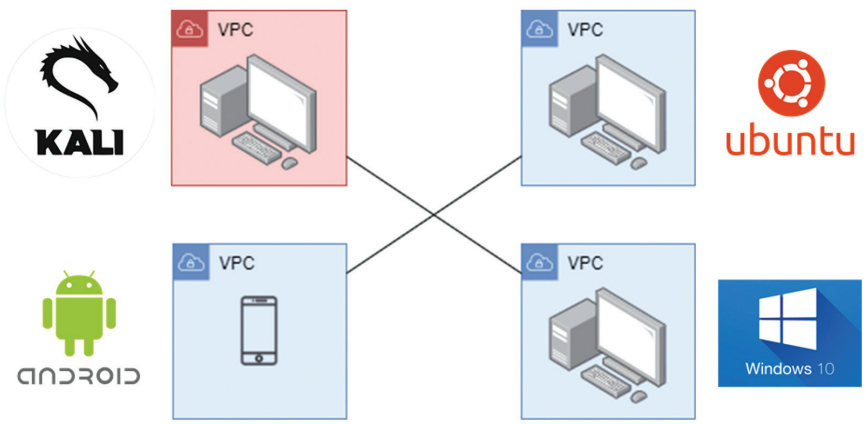
Következtetések

A bemutatott összehasonlítás alapján a H1 hipotézist érdemes tovább pontosítani a fejezetben meghatározott kategóriák mentén. Ezek alapján a H1 hipotézist az alábbiak szerint módosítom: Szükséges egy olyan *passzív-aktív, offline, hallgatók számára elérhető* szimulációs környezet kidolgozása, amelynek segítségével kibervédelmi technikák gyakorolhatók.

A részletes összehasonlítás alapján megállapítható, hogy jelenleg nem elérhető olyan kibervédelmi platform, amely támogatja a H1 módosított hipotézisben megfogalmazott tulajdonságokat. Ezek alapján a *H1 hipotézist bizonyítottnak* tekintem.

Egyszerűsített szimulációs környezet

A H2 hipotézis vizsgálatához létrehoztam egy egyszerűsített szimulációs környezetet, amely megfelel a H1 hipotézisben meghatározottaknak, vagyis képes a passzív-aktív végrehajtásra, elérhető offline módon, és a hallgatók számára is könnyen biztosítható. Az egyszerűsített környezet architektúráját a 2. ábra szemlélteti.



2. ábra: Szimulációs hálózat
Forrás: a szerző szerkesztése

Infrastruktúra

Az infrastruktúra összesen négy komponensből épül fel, amelynek célja egy támadó komponens, illetve több infokommunikációs eszköz szimulálása, amit a közszolgálatban dolgozó emberek is használhatnak a mindennapjaik során. Minden komponens egy-egy virtuális gép, amelyekre különböző operációs rendszereket telepítettem.

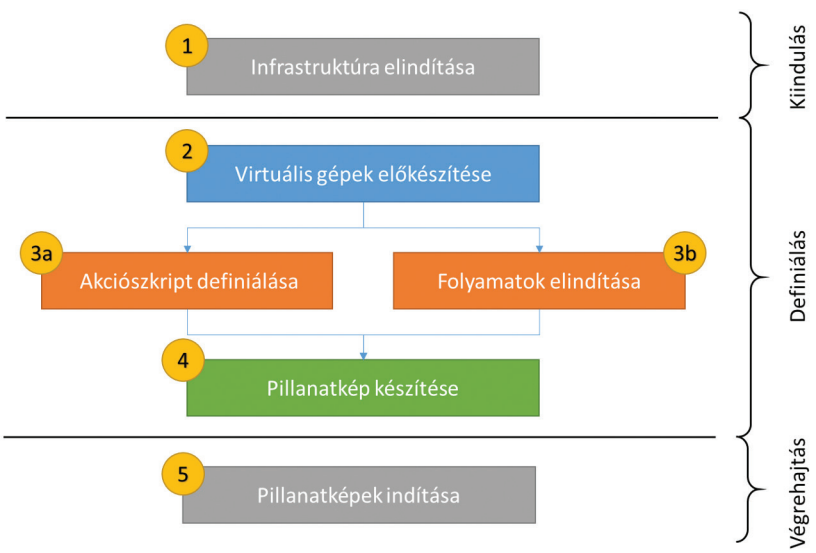
- Kali Linux: Sérülékenységvizsgálatra és behatolástesztelésre kialakított Linux-disztribúció. Olyan alkalmazásokat és eszközöket tartalmaz előre telepített

formában, amelyek segítségével etikus támadások indíthatók a hálózatban található eszközök ellen.
- Ubuntu: Az egyik legszélesebb körben használt Linux-alapú operációs rendszer. Fő erőssége, hogy a mindennapokban szükséges feladatok elvégzéséhez is található rajta megfelelő alkalmazás. A kiválasztás oka, hogy sok szervezeten belül gyakran találkozhatunk Linux-/Unix-alapú operációs rendszerekkel.
- Windows: A legelterjedtebb operációs rendszer személyi számítógépekre, amelyet egyetemek, vállalatok és (közszolgálati) szervezetek is előszeretettel használnak.
- Android: Az egyik legelterjedtebb mobil operációs rendszer, amely megtalálható mobiltelefonokon, tableteken és egyéb infokommunikációs eszközökön egyaránt.

Az összes virtuális komponenst egyetlen hálózatra csatlakoztattam, amelyen keresztül képesek egymással kommunikálni. Minden komponensnek fix hálózati címet állítottam be (IP-cím), ezáltal minden egyes újraindítás során ugyanazon a címen érhetők el.

Támadás meghatározása és végrehajtása

A definiált infrastruktúrán felvehetők, rögzíthetők és végrehajthatók kibertámadások a komponensek között. A támadó fél minden esetben a Kali Linuxszal rendelkező virtuális gép volt. A támadás meghatározásához a 3. ábra szerinti feladatokat kell elvégezni. A meghatározás során elsődleges cél, hogy a támadás elmenthető és automatizáltan újra végrehajtható legyen.



3. ábra: Támadás szimulációjának előkészítése
Forrás: a szerző szerkesztése

A támadás szimulációjának előkészítése három szakaszból áll. A kiindulás szakaszában kerül sor első lépésként az *infrastruktúra elindítására,* ami mindössze annyit jelent, hogy azokat a virtuális gépeket, amelyeknek szerepük lesz a szimuláció során, elindítjuk.

A definiálás folyamat során a virtuális gépeket úgy módosítjuk, hogy a kibertámadás végrehajtható legyen. Ezek a módosítások magukban foglalják a virtuális gépek előkészítését, az akciószkript definiálását és a támadáshoz kapcsolódó folyamatok elindítását.

A *virtuális gépek előkészítése* során az egyes virtuális gépeken elvégezzük a szükséges támadásspecifikus módosításokat, beállításokat. Ha szükséges, ezek érvényre juttatásához újraindítjuk őket.

A következő lépést jelentősen meghatározza, hogy a támadás komplex, több lépésből álló szekvenciális folyamat (3a), vagy folyamatos támadás lesz (3b), amelyekhez olyan szolgáltatásokat kell elindítani, amelyek megállás nélkül futhatnak.

A szekvenciális folyamat során *akciószkript deifinálása* indokolt, ilyenkor lépések sorozatát írjuk le. Az egyik lépés felhasználhatja az előző lépés kimenetét, de minden esetben, minden lépés befejeződik a támadás végrehajtása során. A támadás lépései shell szkript[29] segítségével definiálhatók a Kali Linuxot kiszolgáló virtuális gépen, amit az asztalon található *start.sh* fájlban kell eltárolni. Ennek a fájlnak sajátossága, hogy hozzáadtam a *crontable* konfigurációhoz, emiatt minden újraindításkor automatikusan végrehajtódik a fájl tartalma. Ha a szkript írása befejeződött, és elmentettük, akkor a gépet állítsuk le, továbbá a többi komponenst is leállíthatjuk.

Folyamatos támadás esetén kerül sor a *folyamatok elindítására,* amely során a támadáshoz kapcsolódó szolgáltatásokat kell elindítani, amelyek folyamatosan futni fognak a támadás során. Ebben az esetben a virtuális gépeket nem állítjuk le, csak szüneteltetjük. (Természetesen ez a fajta folyamat is megoldható lenne a 3a lépéssel, azonban ebben az esetben nincs szükség a szkript megírására, ezáltal sokkal gyorsabb és a könnyebb a támadás definiálása.)

Az eddig bemutatott lépésekkel sikeresen elindíthatók a támadások, azonban a cél, hogy ezek a támadások könnyen hordozhatók és újra végrehajthatók legyenek. Emiatt szükséges a folyamat utolsó lépése. Mivel a virtuális gépeken módosításokat hajtottunk végre, pillanatképeket kell készíteni róluk. A pillanatkép készítésének célja, hogy a számítógépet abba az állapotba töltsük vissza, amikor a kibertámadás éppen zajlott. Minden elindított komponens esetén azonos nevet adtam a pillanatképeknek, hogy könnyen azonosítható legyen, mely támadáshoz mely pillanatkép tartozik.

Utolsó lépésként a támadások szimulálásához az előzőekben ismertetett módon elkészített *pillanatképeket* kell *elindítani.* Ez a jelenlegi implementációban manuálisan történt meg, de a virtuális gépek automatikusan is indíthatók.

Kibertámadások szimulációja

A szimulációs környezetbe három korábban ismertetett kibertámadási típust implementáltam a szolgáltatásmegtagadásos támadás *(DoS),* az adathalászat *(phishing)*

[29] Garrels 2004.

és a hátsóajtó programok *(backdoor)*. Ezeket úgy alakítottam ki, hogy különböző infokommunikációs eszközökön, operációs rendszereken lehessen szimulálni.

Minden egyes támadás leírása során a következő felosztást alkalmazom:

1. Támadó gép beállítása: bemutatja, hogy melyek azok a fontosabb lépések, amelyeket a támadó gépen elvégeztem a támadás szimulációjához.
2. Áldozat gép beállítása: bemutatja, hogy melyek azok a fontosabb beállítások, amelyeket az áldozat eszközén végrehajtottam annak érdekében, hogy a támadás sikeres legyen.
3. Támadás érzékelése: bemutatja, hogy az áldozat/támadó mit tapasztal a támadás során.
4. Megszerezhető tudás: bemutatja, hogy mi az a tudáshalmaz, amelyet a szimuláció során az áldozat megismerhet.

Szolgáltatásmegtagadásos támadás (DoS)

Támadó gép beállítása

A DoS-támadáshoz a Kali Linuxon előretelepített *hping3*[30] alkalmazást használtam az alábbi paraméterezéssel:

```
hping3 10.0.2.5 –icmp –flood
```

A kiadott parancs hatására a támadó gép a hálózaton található 10.0.2.5 IP-címmel rendelkező eszközt szólítja meg az úgynevezett Internet Control Message Protocol[31] (ICMP) protokollban meghatározott kérésekkel. A támadógép pillanatképét akkor készítettem el, amikor a parancsot kiadtam. Ezáltal újraindítás után a kiadott parancs fog futni.

Áldozat gép beállítása

A DoS-támadáshoz kapcsolódóan a Windows operációs rendszerrel rendelkező virtuális gépet választottam. A Windows alapértelmezetten nem reagál az ICMP-kérésekre, ezért módosítottam a tűzfalat úgy, hogy egy olyan bemenő szabályt vettem fel, amely engedélyezi az ICMP-kérésekre való válaszadást (4. ábra). Az áldozat pillanatképét a szabály aktiválása után kikapcsolt állapotban készítettem el.

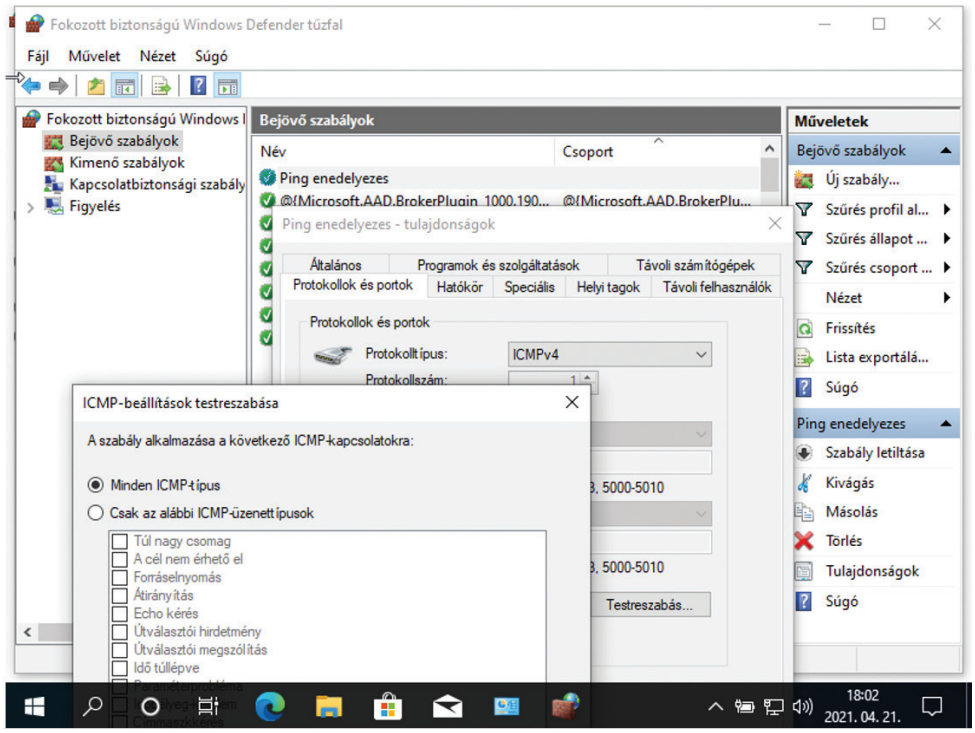
Támadás érzékelése

A szimulációs környezet elindítása után, amikor az áldozat gépe csatlakozik a hálózathoz, teljes mértékben használhatatlanná válik a rengeteg kérés kiszolgálása miatt. Elsősorban a processzor lesz túlterhelve, ami miatt az áldozat nem képes a rendszert használni.

[30] hping3, Kali Tools, https://tools.kali.org/information-gathering/hping3
[31] ICMP, IETF Standards, https://tools.ietf.org/html/rfc792

Megszerezhető tudás

Az áldozat ebben a szimulációban szembesül azzal, hogy fizikai beavatkozásra is szükség van ahhoz, hogy egy kibertámadást elhárítson, hiszen a hálózati kábelt ki kell húznia a gépből (esetleg a routert le kell állítani). Ezenkívül megismerkedik az áldozat a Windows tűzfal beállításaival és képes lesz értelmezni a bejövő és kimenő szabályokat.



4. ábra: Windows tűzfal szabályok beállítása
Forrás: a szerző szerkesztése

Adathalászat (phishing)

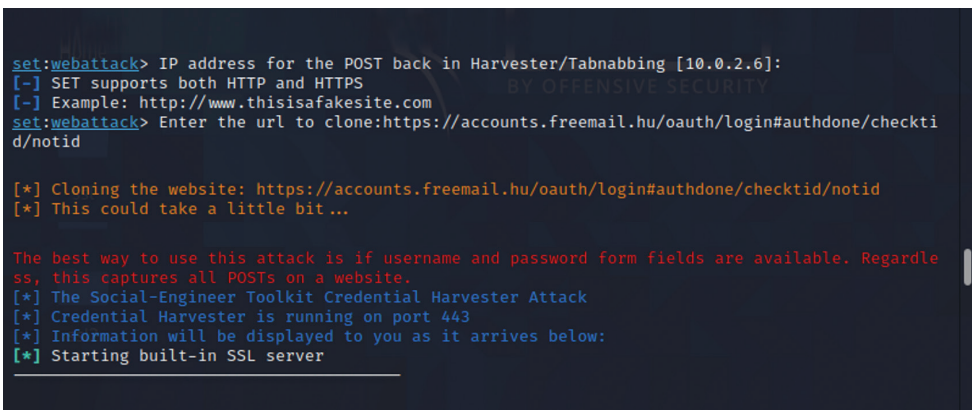
Támadó gép beállítása

Ehhez a támadáshoz a Kali Linuxon lévő *SEToolkit* csomagjában található *credential harvester* alkalmazást használtam, annak érdekében, hogy lemásoljam a https://freemail.hu levelező oldal bejelentkező felületét és megszerezzem az áldozat e-mail-címét és jelszavát. A beállítás során engedélyeztem a biztonságos *https*

kapcsolatot, amihez az *openssl* alkalmazás segítségével létrehoztam egy tanúsítványt is. Ennek célja, hogy a felhasználóval elhitessük, hogy egy biztonságos weboldalra látogat.

A pillanatkép elkészítéséhez két fontos alkalmazásnak kellett futnia:

- Egy egyszerű webszerver fut abban a mappában, amelyben megtalálható az a tanúsítvány, amelyet a kliensnek telepítenie kell a böngészőben.
- python2 -m SimpleHTTPServer 80
- A credential harvester fut, vagyis várja, hogy az áldozat meglátogassa a támadó által klónozott weboldalt (5. ábra).



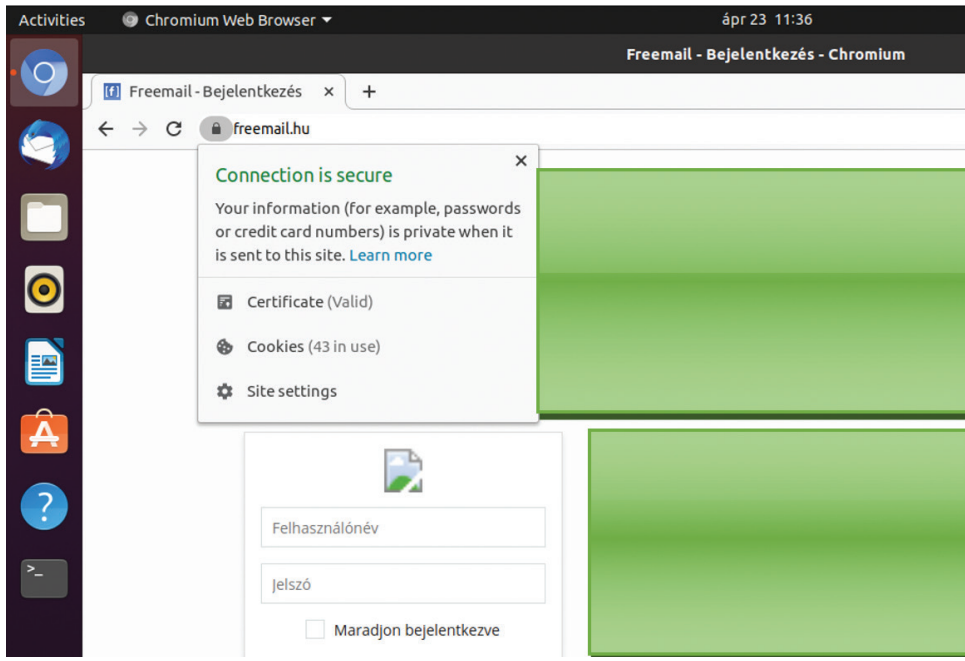
5. ábra: A támadó gép várakozik, hogy valaki meglátogassa az áloldalt
Forrás: a szerző szerkesztése

Áldozat gép beállítása

Az áldozat gépe jelen támadás során az Ubuntu operációs rendszerrel rendelkező virtuális gép, amelyen az előkészület során két fontos módosítást kellett végrehajtani. Először is az alapértelmezett böngészőn keresztül letöltöttem és telepítettem a megfelelő tanúsítványt úgy, hogy az engedélyezze a támadó gépen lévő oldallal való biztonságos kommunikációt. Majd az */etc/hosts* fájlhoz kellett felvennem az alábbi sort:

10.0.2.4 freemail.hu

Ennek segítségével a támadó által előállított weboldal az ismert domaincímen keresztül is elérhető, ahogy azt a 6. ábra is mutatja:



6. ábra: A kliensoldalon biztonságosnak tűnő megtévesztő oldal
Forrás: a szerző szerkesztése

Támadás érzékelése

A felhasználó megpróbál belépni az e-mail-fiókjába, beírja felhasználónevét és jelszavát, azonban az oldal elsőre újratöltődik, viszont másodjára sikeresen be lehet jelentkezni az e-mail-fiókba. A támadás észlelését korlátozza, hogy a kommunikáció biztonságos, mivel a megfelelő tanúsítványok rendelkezésre állnak. Azonban a weboldalhoz kapcsolódó domainnévhez tartozó IP-cím lekérdezésével láthatóvá válik, hogy a hálózaton belüli szerverhez kapcsolódik a felhasználó, amiből már sejthető, hogy támadás érte.

Fontos feladat az áldozat számára megmutatni a támadó felhasználói felületét és jelezni, hogy ténylegesen megkapja a támadó a beírt adatokat, hiszen ennek segítségével még valóságosabbá válik a támadás (7. ábra).

```
10.0.2.4 - - [22/Apr/2021 22:17:00] "GET / HTTP/1.1" 200 -
10.0.2.4 - - [22/Apr/2021 22:17:01] "GET /fng-static/images/cbn.svg HTTP/1.1" 404 -
10.0.2.4 - - [22/Apr/2021 22:17:01] "GET /fng-static/images/logo.svg HTTP/1.1" 404 -
10.0.2.4 - - [22/Apr/2021 22:20:49] "GET / HTTP/1.1" 200 -
10.0.2.4 - - [22/Apr/2021 22:20:51] "GET /fng-static/images/cbn.svg HTTP/1.1" 404 -
10.0.2.4 - - [22/Apr/2021 22:20:51] "GET /fng-static/images/logo.svg HTTP/1.1" 404 -
10.0.2.4 - - [22/Apr/2021 22:20:51] "GET /loader.gif HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=teszt.elek
POSSIBLE PASSWORD FIELD FOUND: password=AzÂnJelszavam11#
POSSIBLE USERNAME FIELD FOUND: loginBtn=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

7. ábra: A támadó sikeresen ellopta az adatokat
Forrás: a szerző szerkesztése

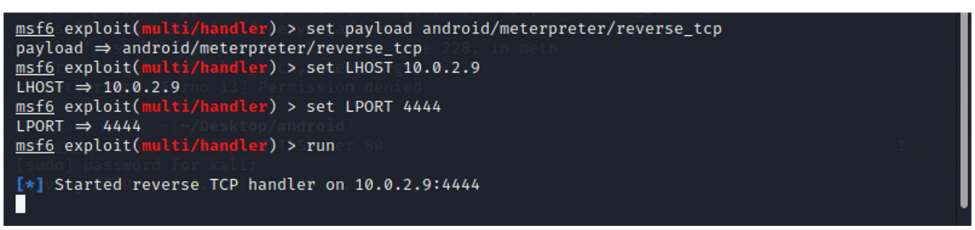
Megszerezhető tudás
Az áldozat megismerkedik a tanúsítványok *(certificate)* szerkezetével és jellemzőivel, a böngészők limitációival, illetve az SSL-kapcsolat jelentésével. Ezenkívül a DNS szerverek alapjaival, a domainnév feloldásával, illetve az operációs rendszerek *hosts* fájljával.

Hátsóajtó program (Backdoor)

Támadó gép beállítása
A Kali Linuxon található *metasploit* keretrendszer segítségével lehetőség van olyan androidos telepítő alkalmazás létrehozására, amely egy hátsó kaput nyit azon az androidos eszközön, amely telepíti az így létrehozott alkalmazást. Az alkalmazást az alábbi paranccsal lehet létrehozni, ahol azt az IP-címet és portot kell megadni, amelyen a támadó gép figyelni fog, és várni fogja, hogy az áldozat elindítsa az alkalmazást:

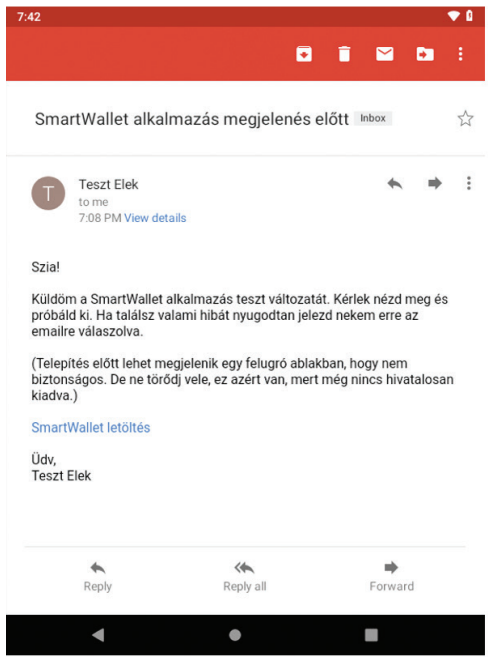
```
msfvenom -p android/meterpreter/reverse_tcp
        LHOST=10.0.2.4 LPORT=4444 R
```

Az alkalmazás elkészülte után el kell indítani a várakozást, amihez a *metasploit* keretrendszer *exploit/multi/handler* alkalmazását szükséges elindítani megfelelő paraméterezéssel (8. ábra). Végül ahhoz, hogy az áldozathoz is eljusson a kívánt telepítő, egy üzenetet küldtem az áldozat e-mail-címére a letöltő linkkel együtt (9. ábra).

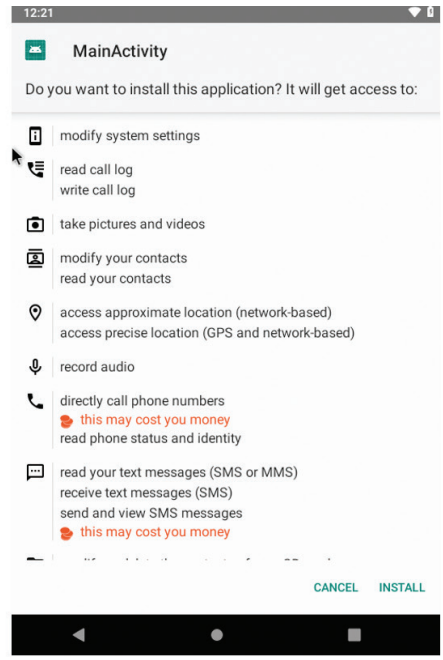


8. ábra: A támadó gép várakozik backdoor indítására
Forrás: a szerző szerkesztése

Áldozat gép beállítása
Az áldozat gépe az Android operációs rendszert futtató virtuális gép, amely megszemélyesíthet mobiltelefont, tabletet, tv-t vagy bármilyen egyéb okoseszközt. Az áldozat gépén engedélyezni kellett az ismeretlen alkalmazások telepítését a Google Chrome alkalmazásból, aminek hatására az áldozat képes telepíteni olyan alkalmazásokat, amelyeket nem a hitelesített Play Áruházból tölt le.



9. ábra: Megtévesztő e-mail
Forrás: a szerző szerkesztése

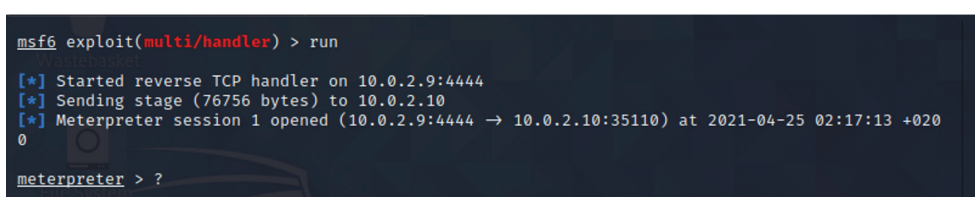


10. ábra: Alkalmazás telepítése
Forrás: a szerző szerkesztése

Támadás érzékelése

A támadás érzékeléséhez az áldozatnak telepítenie kell a létrehozott alkalmazást (10. ábra). Ahhoz, hogy az áldozat lássa, milyen hatása lehet annak, ha egy ilyen alkalmazást telepít, érdemes megmutatni neki a támadó terminálját (11. ábra), amelyen keresztül néhány parancs beírásával könnyedén szembesülhet azzal, hogy mi minden elérhető távolról. A teljesség igénye nélkül az alábbi parancsokat lehet érdemes megmutatni:

- *dump_sms*: az összes sms letöltése a támadó gépére;
- *dump_contacts*: az összes névjegy letöltése a támadó gépére;
- *webcam_stream*: a kamera képének továbbítása a támadó gépére;
- *geolocation*: a telefon helyzetének elküldése a támadó gépére.



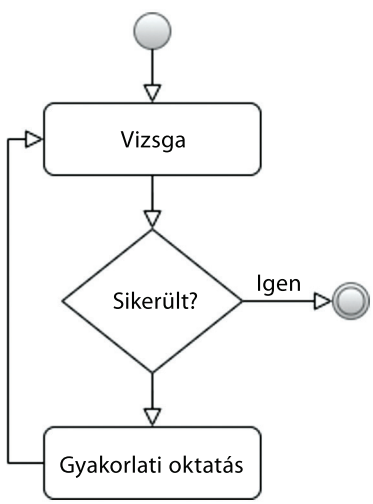
11. ábra: A backdoor aktivizálódott a támadó gépén
Forrás: a szerző szerkesztése

Megszerezhető tudás
Az áldozat szembesül a megtévesztő e-mailek céljával és legfőbb típusával, az Androidhoz kapcsolódó telepítőfájlokkal és beállításokkal, a Play Protect alkalmazás fontosságával.

Kiértékelés

A kiértékelést úgy folytattam le, hogy egy előre kiválasztott, mély informatikai tudással nem rendelkező felhasználói csoporton kísérletet hajtottam végre, amely során a szimuláció működését és a tudásátadás hatékonyságát vizsgáltam. A kiértékelés során a csoportnak vizsgán és gyakorlaton kellett részt vennie. Ezeken a korábban bemutatott kibertámadások szimulációja zajlott, minimális paraméterbeli eltérésekkel (például más weboldal álcázása, más IP-címek használata stb.), illetve a gyakorlati rész során egy oktatási segédanyag is rendelkezésre állt.

A kiértékelés igazolása lehet a H2 hipotézisnek, amely szerint szimulálható olyan kibertámadás, amelynek azonosításához és megoldásához nem szükséges mély informatikai tudás. Ehhez két feltételt kellett ellenőrizni. A résztvevők technikai segítségnyújtás nélkül képesek a gyakorlatot és a vizsgát végrehajtani, illetve a résztvevők mély informatikai tudás nélkül is képesek teljesíteni a vizsgát.



12. ábra: Kiértékelés folyamata
Forrás: a szerző szerkesztése

A kiértékelés menetét a 12. ábra mutatja be, miszerint a résztvevők először megpróbálkoztak a vizsga teljesítésével, amennyiben az rosszul sikerült, akkor a gyakorlati oktatás keretében sajátították el a vizsga teljesítéséhez szükséges ismereteket, ezután ismételten megpróbálkoztak a vizsga végrehajtásával. A gyakorlati oktatást addig

hajtották végre, amíg a vizsga sikeresen nem zárult. Annak az oka, hogy a résztvevőket rögtön a vizsgakérdésekkel szembesítjük, mindössze az volt, hogy ellenőrizzük, tényleg szükséges-e a gyakorlati oktatás megtartása és elvégzése, vagy esetleg rendelkeznek már a megfelelő informatikai tudással.

Résztvevők

Összesen 12 résztvevővel végeztem el a kísérletet, akik között vegyesen találhatók nők és férfiak is. A 24–56 éves korosztályból, megfelelően elosztott mértékben választottam személyeket, többségében a közszolgálatból, de egyéb szakmák is képviseltették magukat, ahol az informatikai tudás nem jelentkezett követelményként, előfeltételként.

Eredmények

A résztvevők által a környezet összeállítása és a vizsga végrehajtása teljesen önállóan zajlott, azonban a gyakorlati oktatás során személyesen is jelen voltam, aminek fő célja, hogy az oktatási anyag minőségét fejlesszem. Abban az esetben, ha valamilyen oktatási rész nehezen érthető volt, vagy a résztvevő érdeklődését felkeltette az adott téma, személyesen válaszoltam a felmerült kérdésekre.

A kiértékelés során a személyek azonos teljesítményt értek el, mindössze a teljesítés idejében voltak eltérések. Egyetlen résztvevő sem volt képes a vizsgát gyakorlati oktatás nélkül teljesíteni, viszont a gyakorlati oktatás után mindenki teljesítette azt.

A virtuális gépek előkészítése és elindítása a résztvevők többségének könnyedén ment, de néhány esetben indokolt volt a technikai segítségnyújtás arra vonatkozóan, hogy a virtuális gépeket és a pillanatképeket milyen módon lehet kiválasztani és elindítani.

Tapasztalatok

A résztvevők többsége korábban nem tapasztalt a gyakorlat során bemutatottakhoz hasonló kibertámadásokat, kizárólag e-mailben érkező adathalász-támadással találkoztak, amelyet a legtöbb esetben az üzenet helytelen magyarsággal íródott tartalma miatt ismertek fel. Éppen ezért a szimulációs oktatás előnyeként emelték ki a különféle támadási technikák bemutatását, azok felismerésének lehetőségeit, hiszen a támadás elhárítására irányuló intézkedések csak akkor alkalmazhatók eredményesen, ha a támadás észlelése megtörtént.

A támadások szimulálása során a résztvevők felismerték, hogy a kibertámadások típusai és céljai rendkívül sokrétűek. A szimulációs gyakorlati oktatást követően a résztvevők azt nyilatkozták, hogy a jövőre nézve sokkal elővigyázatosabbak lesznek, továbbá sokkal tudatosabban használják majd különféle infokommunikációs eszközeiket és az online platformokat, kiemelt figyelmet fordítva az általános védelmi intézkedésekre és az esetleges fenyegetések felismerésére.

Minden résztvevő kiemelte, hogy a támadó gép megmutatása a támadás után sokkal jobban motiválta és meglepte őket, mintha csak az áldozat gépén kellett volna végrehajtaniuk a védelmi intézkedéseket a gyakorlat során, hiszen így azt is megtapasztalhatták, hogy milyen információkhoz férhet hozzá a támadó, így még valósághűbbnek tűnt a gyakorlat. Több résztvevő is jelezte, hogy a támadások valóságos átélése ráébresztette őket a biztonságtudatosság fontosságára, a szükséges védelmi intézkedések megismerésének, betartásának és kivitelezésének szerepére, a kibertérből érkező fenyegetések káros következményeinek mérséklése érdekében. A gyakorlat előnyeként fogalmazták meg azt a véleményt, hogy segítségével nemcsak elméletben tanulják meg, hogyan reagáljanak a különféle támadásokra, hanem a „saját bőrükön" tapasztalják, milyen szembesülni egy valódi kibertámadással, így sokkal hatékonyabban képesek megjegyezni a védekezés során alkalmazandó intézkedéseket, hiszen így a gyakorlatban ki is próbálhatják az egyes lépéseket.

Összegezve, a tapasztalatok alapján megállapítható, hogy a szimulációs gyakorlat során olyan tudást sikerült átadni, amelynek segítségével elérhető, hogy a résztvevőket ne érje váratlanul egy valós támadás, illetve a már megszerzett tudást éles helyzetekbe is képesek legyenek átültetni.

Következtetés

Az eredmények alapján összegezhető, hogy a résztvevők közül senki sem volt képes gyakorlat nélkül teljesíteni a vizsgát, ami alátámasztja, hogy nem rendelkeztek mély informatikai tudással. Képesek voltak azonban a gyakorlati oktatás után önállóan és eredményesen végrehajtani a vizsgát. Ezek alapján teljesült az a két feltétel, amely szükséges ahhoz, hogy a H2 hipotézist bizonyítottnak tekintsük, vagyis *a résztvevők technikai segítségnyújtás nélkül képesek a gyakorlatot és a vizsgát végrehajtani, illetve a résztvevők mély informatikai tudás nélkül is képesek teljesíteni a vizsgát.* Ezek alapján a *H2 hipotézist bizonyítottnak* tekintem.

Összefoglalás és jövőbeni tervek

Ebben a publikációban megvizsgáltam a nyilvánosan elérhető kiberbiztonsági keretrendszereket, amelyek felhasználhatók a kiberbiztonsági ismeretek gyakorlati oktatására. Ezeket több szempontból is értékeltem, amely alapján kijelenthető, hogy szükség van egy olyan passzív-aktív offline szimulációs platformra, amely képes a kibervédelmi technikák gyakorlati kipróbálására.

Ehhez kapcsolódóan bemutattam egy egyszerűsített architektúrát a kibertámadások automatikus szimulációjára. A kibertámadások során virtuális gépeket lehet használni, amelyeket akár a saját számítógépünkön is elindíthatunk. A szimulációk definiálására pillanatképeket lehet használni, illetve szükség szerint szkripteket is lehet írni, amelyek a virtuális gépek indításakor automatikusan lefutnak.

Az így kialakított architektúrán megvalósítottam egy DoS-, egy backdoor és egy phishing támadást is különböző platformokon, amelyek más és más infokommunikációs

eszközt szimbolizáltak (asztali számítógép, mobiltelefon, tablet stb.). A szimulációhoz kapcsolódóan a feladatokat csak az áldozat gépen kellett végrehajtani, de szemléltetésképpen a támadó gépen található konzolt is meg lehetett tekinteni.

Az így kialakított rendszert különböző, mély informatikai tudással nem rendelkező személyekkel teszteltem le. Mindenki az előre elkészített szimulációs környezetében próbálta ki a vizsgafeladatokat és a gyakorlati oktatást. Ezek alapján kijelenthető, hogy szimulálható olyan kibertámadás, amelynek azonosításához és megoldásához nem szükséges mély informatikai tudás.

A kutatás folytatásaként szeretném kibővíteni a meglévő támadásokat további példákkal, mivel a hosszú távú cél, hogy az így kialakított gyakorlat a közszolgálati kiberbiztonsági képzés keretében a saját infokommunikációs eszközök védelme című tantárgy teljes gyakorlati anyagát lefedhesse.[32] Ezután a kiértékelés körét érdemes kibővíteni nagyobb létszámra és a képzéshez kapcsolódóan részletesebb méréseket végrehajtani. Végül az architektúrát szeretném úgy kibővíteni, hogy ne csak saját infokommunikációs eszközökön történő támadásokat lehessen szimulálni, hanem szervezeti szintű kiberfenyegetéseket is.

Irodalomjegyzék

Beuran, Razvan et al. (2017): CyTrONE: An Integrated Cybersecurity Training Framework. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy, Porto, Portugal,* 157–166. Online https://doi.org/10.5220/0006206401570166

Cartwright, General James (2011): *Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5.* Washington, D.C.: Department of Defense.

Čeleda, Pavel et al. (2015): *KYPO – A Platform for Cyber Defence Exercises. M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence.* NATO Science and Technology Organization. Online: http://dx.doi.org/10.14339/STO-MP-MSG-133-08-doc

Conklin, Arthur – Cline, Raymond – Roosa, Tiffany (2014): Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. In *47th Hawaii International Conference on System Sciences,* 2006–2014. Online: https://doi.org/10.1109/HICSS.2014.254

Deák Veronika (2019): Kártékony programok terjedése social engineering technikákon keresztül. *Hadmérnök,* 14(2), 256–271. Online: https://doi.org/10.32567/hm.2019.2.21

Deák Veronika (2020a): A közszolgálati kiberbiztonsági képzés helye nemzetközi viszonylatban. *Hadmérnök,* 15(4), 159–177. Online: hhttps://doi.org/10.32567/hm.2020.4.11

[32] Deák 2020b: 157–178.

Deák Veronika. (2020b): A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon. *Hadmérnök,* 15(3), 157–178. Online: hhttps://doi.org/10.32567/hm.2020.3.9
Fehér Krisztián (2016): *Kezdő hackerek kézikönyve.* Budapest: BBS-INFO Könyvkiadó és Informatikai Kft.
Ficco, Massimo – Palmieri, Francesco (2019): Leaf: An Open-source Cybersecurity Training Platform for Realistic Edge-IoT Scenarios. *Journal of Systems Architecture,* 97, 107–129. Online: https://doi.org/10.1016/j.sysarc.2019.04.004
Garrels, Machtelt (2004): *Bash Guide for Beginners.* United Kingdom: Fultus Corporation.
Gyányi Sándor (2007): DDOS támadások veszélyei és az ellenük való védekezés. *Hadmérnök,* Különszám. Online: http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html
Hart, Stephen et al. (2020): Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security,* 95. Online: https://doi.org/10.1016/j.cose.2020.101827
Hathaway, Oona et al. (2012): The Law of Cyber-attack. *California Law Review,* 100(4), 817–885. Online: https://doi.org/10.15779/Z38CR6N
Heckman, Kristin et al. (2013): Active Cyber Defense with Denial and Deception: A Cyber-Wargame Experiment. *Computers & Security,* 37, 72–77. Online: https://doi.org/10.1016/j.cose.2013.03.015
Herring, Michael – Willett, Keith (2014): Active Cyber Defense: A Vision for Real-time Cyber Defense. *Journal of Information Warfare,* 13(2), 46–55. Online: www.jstor.org/stable/26487121
Hong, Junho et al. (2015): *Cyber-physical Security Test Bed: A Platform for Enabling Collaborative Cyber Defense Methods.* PACWorld Americas Conference.
Jin, Ge et al. (2018) Game Based Cybersecurity Training for High School Students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education, Baltimore,* 68–73. Online: https://doi.org/10.1145/3159450.3159591
Kennedy, David et al. (2011): *Metasploit: The Penetration Tester's Guide.* San Francisco: No Starch Press.
Kuo, Cheng-Chung et al. (2018): Cyber Attack and Defense Training: Using EMULAB as a Platform. *International Journal of Innovative Computing, Information and Control,* 14, 2245–2258. Online: https://doi.org/10.24507/ijicic.14.06.2245
Muha Lajos – Krasznay Csaba (2018): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem. Online: http://hdl.handle.net/11410/11173
Owens, William – Dam, Kenneth E. – Lin, Herbert S. (2009): *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities.* Washington, D.C.: The National Academies Press. Online: https://doi.org/10.17226/12651
Schepens, Wayne – James, John (2003): Architecture of a Cyber Defense Competition. In *2003 IEEE International Conference on Systems, Man and Cybernetics, Washington,* 4300–4305. Online: https://doi.org/10.1109/ICSMC.2003.1245660
Szabó András (2018): Technikai kiberbiztonsági gyakorlatok – Nemzetközi kitekintés. *Hadmérnök,* 13(1), 286–301.

Uma, M. – Padmavathi, Ganapathi (2013): A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security,* 15(5), 390–396. Online: https://doi.org/10.6633/IJNS.201309.15(5).09

Varga Máté (2010): *Számítógépes virtualizáció.* Online: https://docplayer.hu/2946347-Szamitogepes-virtualizacio.html