HADMÉRNÖK

XII. Évfolyam 1. különszám – 2017. július

WEBKAMERA HACK – PENETRATION TESZT

WEBCAM HACK VIA PENTEST

PARÁDA István

(ORCID: 0000-0002-3083-6015)

parada.istvan@uni-nke.hu

Absztrakt

A jelenlegi nemzetközi és hazai eseményeket tekintve, egyre erősödő az informatikai szakterülettel kapcsolatos tevékenységek száma, valamint jelentősége. Figyelemfelkeltő például a 2016-os amerikai elnökválasztás nem bizonyított, mégis a CIA jelentésekből is megalapozott orosz hacker műveletek végrehajtása. Vagy csak a magyarországi CEU ügy kapcsán okozott Dos támadás az origo ellen. Rendkívül fontos az informatikai biztonság tudatosságának oktatása, nevelése, mely igazi technikai illetve technológia bizonyításokkal szemléltethető és felhívja a kibervédelem, informatikai biztonság, illetve elektronikus információbiztonság szerepét mind hazai, mind nemzetközi vonatkozásban. Éppen ezért a publikáció, mint részterületeként specifikusan a web kamera hackelést taglalja, mint specifikus kontextust kiemelve ebből a tág szakterületből.

Kulcsszavak: *webkamera, hack, exploit, payload*

Abstract

In terms of current international and domestic events, the number and significance of IT operations are increasing. For example the 2016 US presidential election where CIA reports are conducting robust Russian hacking operations. Or just because of the CEU case in Hungary caused Dos attack against origo. It is important to educate awareness of IT security, presenting technical and technical evidence, and calling for the role of cyber security, information security and electronic information security both domestically and internationally. For this reason, this publication as a subfield specifically analyzes a web camera hacking as a specific context highlighted in this wide field of expertise.

Keywords: *webcam, hack, exploit, payload*

A kézirat benyújtásának dátuma (Date of the submission): 2017.06.06.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.06.24.

BEVEZETÉS

Fontos, hogy időben, sőt még térben is elhelyezzük a vizsgált témakört, hisz olyan szakterületet ölel fel, mely rengeteg ember számára még idegen, számos szakmai átfedéssel és még mindig jelentős tematikai nézetkülönbségekkel. Ezen felül, olyan technológia alapokra támaszkodó tudományág, melyet a mai világban a legnagyobb ütemű fejlődés jellemez. (A Nemzeti Közszolgálati Egyetem főbb kutatási területeinek irányai, témakörei is tartalmazzák a szerző által vizsgált területet. [1]; [2] Ebből kifolyólag néha elfogadnak tematikai nézőpontokat, de nem példa nélküli, hogy a fiatalabb generáció ezt máshogy látja, és alkalmazza, számtalanszor hatékonyabban. A technikai fejlődés gyorsasága, pedig rendkívül változékony, flexibilis területet eredményez, mely technológiai szempontból hihetetlenül széles spektrumot rajzol ki. Ennek révén érzem szükségesnek feltüntetni az dátumot, hisz elképzelhető, sőt valószínű, hogy a jövőben az általam kihasznált sérülékenységet javítják, így ez által legfeljebb maga az eljárás metodikája követhető és elemezhető, de a támadás művelete nem az elvárt eredményt produkálja. Leszögezem e fent megjelenített dátum idejében több áldozat számítógépen is végrehajtva a műveletet, Windows Denfender [1]és bizonyos vírusirtók folyamatos futása mellet is sikeresen végrehajtható a web kamerák távoli elérésű bekapcsolása és a videóanyagok rögzítése. Windows XP, VISTA, 7,8,8.1,10 [2]operációs rendszerek alatt.

A fentiekben leírt témakör az Informatikai biztonság, azaz az Elektronikus információvédelem, illetve másik nevén Kibervédelem, de hogy pontosítsam a nem szabályos megfogalmazást Hackelés[3]. Sorolható lenne még különféle jelzőkkel a vizsgálni kívánt szakterület. A nevesített behatárolást kompetensebb emberekre bízom, a publikációban, a továbbiakban szakmai szemmel egy teszt lépéseit kívánom feltárni, és elemezni azt. Természetesen a művelet előtt tisztázni szeretném az aktualitást, az okokat, a miérteket, valamint ezen felül a végrehajtás során felhasznált eszközöket, szoftvereket. Végül az eredmények összegzését és a konklúziók levonását kívánom kifejteni.

AKTUALITÁS, OKOK

A New York Times (www.nytimes.com/news-event/russian-election-hacking) és számos nemzetközi információ és publikálások hirdetik napjainkban, hogy a 2016-os Amerikai Egyesült Államok elnökválasztást adatok és tények elferdítésével hamísításával hajtották végre. [3] Az egyik jelölt előnyős pozícióba kerülése, sőt győzelme volt a cél, melyet informatikai rendszerek segítségével értek el az erre törekvők. Valószínűsítik, hogy orosz befolyás és tevékenység állhat az informatikai adatokhoz kapcsolódó műveletek hátterébe. Sőt az alábbi idézet szerint hivatalos tényként ezt kezelni:

"*Az Egyesült Államok feloldotta a titkosítást a hírszerzés anyagain az orosz hackertámadásokkal kapcsolatban. Már régóta hangoztatták, hogy az támadások Oroszországból indultak, amit Donald Trump még a nap során, január 6-án adott interjújában is tagadott. Míg a megválasztott elnök "politikai boszorkányüldözésnek" nevezte*

[1] Windows Defender teljes körű védelmet biztosít a kártevőkkel szemben. A kártevő programok vírusok, kémprogramok és egyéb kéretlen szoftverek.
[2] Microsoft cég által forgalmazott operációs rendszerek adott típusai
[3] A hack szó mai jelentése valószínűleg az amerikai MIT egyetemen elkövetett diákcsínyekből ered. Az informatikai területen megkülönböztetnek több hackercsoportot, de végső soron mindegyik az informatikai biztonsággal foglalkozik. Az ilyen folyamatot nevezik hackelésnek

az ügyet, a hírszerzés kiadott egy 15 oldalas tanulmányt, ami bizonyítja: Vlagyimir Putyin elnök támadó kampányt indított a 2016-os amerikai elnökválasztás ellen.
A tanulmány kimondja: "Vlagyimir Putyin orosz elnök rendelte el a 2016-os amerikai elnökválasztás elleni kampányt. Oroszország célja az volt, hogy aláássa az amerikai demokratikus folyamatokba vetett bizalmat, rágalmazzák Hillary Clintont és csökkentsék a megválasztásának esélyét."

A tanulmány részletezi, hogy hogyan vitték végig az oroszok a tervet, kezdve a Demokrata Pártkongresszus meghackelésével, amit a hírszerzés az orosz kormányhoz kötött, egészen a propaganda és álhírek terjesztéséig."[3]

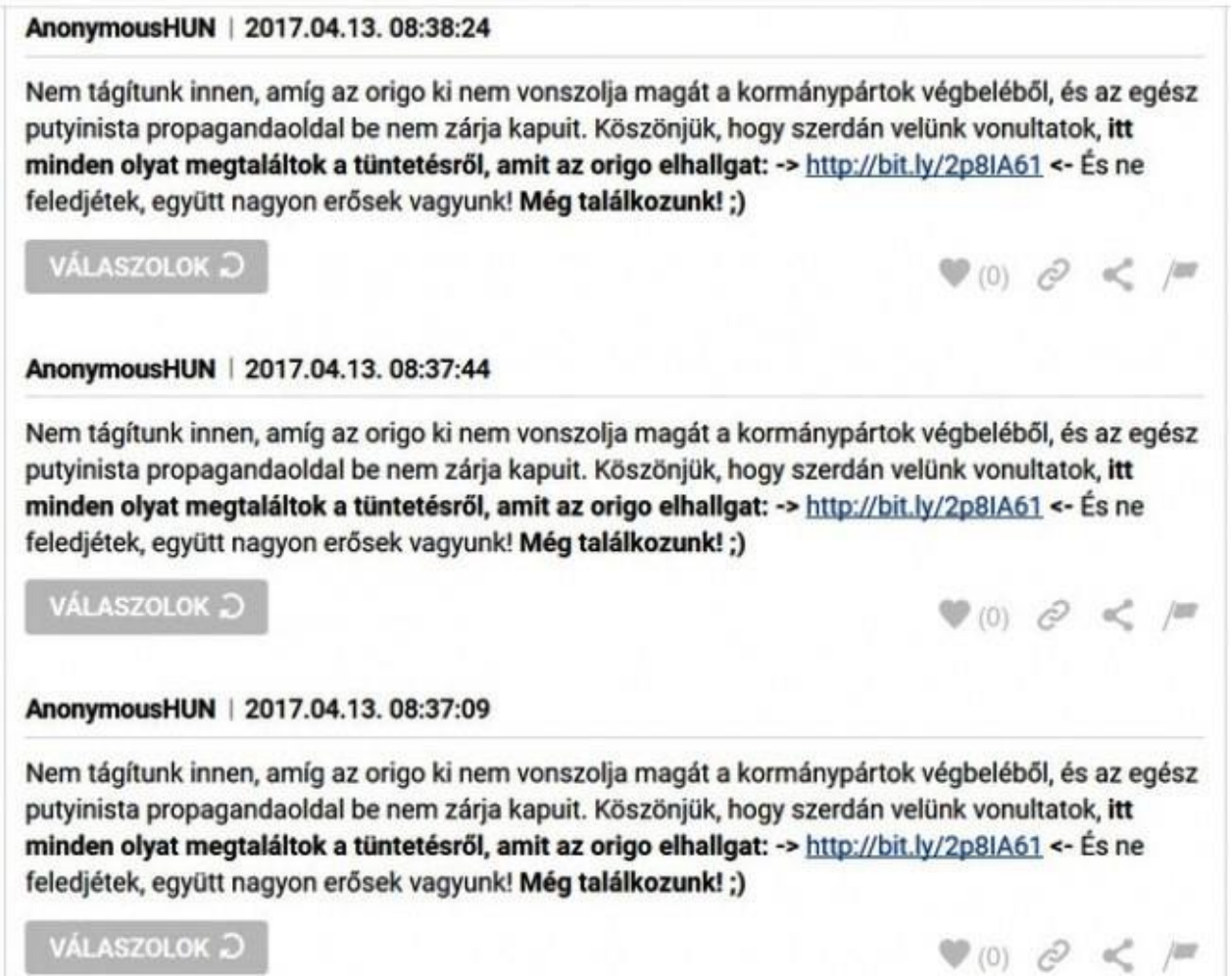
Az aktualitás alátámasztására továbbmenve egy régebbi példát kívánok megemlíteni, mely szorosabban kapcsolódik web kamera hack-elés gyakorlati vizsgálatomra, és nagymértékben inspirált a konklúziók levonásában. Ez nem más, mint az a bizonyos „*Snowden ügy*".
A fent említett ügy konkrétabban egy személy, Edward Joseph Snowden. 1983-ban született az Amerikai Egyesült Államokban, ahol számítógépes szakemberként dolgozott az amerikai Nemzetbiztonsági Ügynökségnél (NSA), valamint a Központi Hírszerző Ügynökségnél (CIA). Majd 2013 májusában, hossza egyeztetések után bizonyos újságíróknak szivárogtatott, hozott nyilvánosságra, olyan szigorúan titkos dokumentumokat, információkat, melyek bizonyítják, hogy az amerikai titkosszolgálatok megfigyelik az emberek mobiltelefonos illetve internetes tevékenységét mind az Amerikai Egyesült Államokban mind a világon globálisan. A következő kémprogramok létezését és működését hozta nyilvánosságra:

- PRISM;[4]
- NSA telefonhívás-adatbázis;
- Boundless Informant[5];
- Tempra, a brit titkosszolgálat hasonló kémprogramja.

Snowden az információkat HongKong-ban hozta nyilvánosságra, de itt fontolgatták kiadását, így Oroszországba menekült, ahol ideiglenes menekültjogot és 3 évig ideiglenes tartózkodási engedélyt kapott. Majd ebben az évben 2017. január 18-án közölte az orosz állam, hogy újabb két évvel meghosszabbították az ideiglenes tartózkodási jogát.[4]
Folytatva a felfűzött gondolatmenetet, nem kell nemzetközi illetve globális kitekintés annak felismerésére, hogy hacker műveletek olyan politikai és gazdasági valamint társadalmi eseményekkel is összeköthető vagy felhasználható, amely egyik legfontosabb képzési és képességi szakterületé teszi napjainkban.

2017. április a Magyar Kormány CEU [6]törvényként emlegetett törvénymódosítást fogadott el, mely e publikáció szempontjából elhanyagolható, és pártatlan nézőpontból való vizsgálatokat készít el. Viszont ez az esemény óriási megosztást eredményezett hazai és nemzetközi emberek összességében. Az esemény leírását, és a háttér információkat nem kívánom megosztani, hisz a publikáció témája teljesen más irányvonulatot hivatott kibontakoztatni. Viszont egy jelentős, gyors reagálást váltott ki az informatikai tudással rendelkező személyekből is. A Magyar Nemzet és még rengeteg nyomtatott illetve internetes sajtó jeleníti meg azt, hogy „*Meghackelték az Origót*". [5]

[4] Egy program neve melyet az NSA Internet adatok gyűjtésére használt, kilenc fő Internet szolgáltató cégtől.
[5] Adat analizáló program. Az NSA globális szinten alkalmazott szoftvere az adtok kezelésére.
[6] Central Europe University



1. ábra Origo elleneni hacktámadás következménye[6]

A fent megjelent cikkben a következő olvasható:

„Nem tágítunk innen, amíg az origo ki nem vonszolja magát a kormánypártok végbeléből, és az egész putyinista propagandaoldal be nem zárja kapuit" – ezzel a szöveggel kezdődött a kormánypárti hírportál összes cikke alatt ugyanaz a több tucat, helyeként több száz komment. Az AnonymusHUN néven, a kommentek számából és intenzitásából adódóan vélhetően automatikusan, botokkal írt hozzászólások szerda éjszaka jelentek meg a portál cikkei alatt, de még csütörtökön kora hajnalban is sorra élesedtek – szúrta ki az Index.

A kommentek szerzője azt kifogásolja, hogy a portál a szerdai esti, a civiltörvény módosítása és a CEU-törvény miatt rendezett fővárosi demonstrációról csak érintőlegesen számolt be.

Az Origo reggel több cikk alatt is letiltotta a hozzászólásokat, ezeknél jelenleg azt írják, „*ez a cikk nem kommentelhető*".[6]

A téma aktualitását és naprakészen való igényét, egy sekélyesebb, társadalmilag is felszínesebb bizonyítással kívánom lezárni. Napjainkban szinte mindenki hallott azokról az eseményekről, ahol híresség eknek törték fel vagy számítógépükön, vagy telefonunkon a web kamerákat. Ezáltal személyes fényképekhez, videókhoz juttatva a célközönséget, aki ezekben a konkrét ez esetben az egész világ.

Ezek az úgynevezett leaked[7] fényképek, melyek rengeteg híresség kikerült személyes képek halmazát takarja, melyet valamilyen sérülékenység réven sikerült beszerezniük a hackereknek. Egy gyanús link vagy kémprogram futtatásával eredményesen kapcsolták be távolról az eszközök web kameráit, és vagy stream[8] formájában vagy snapshotok[9] segítségével kompromittáló anyagokat szereztek be, majd tették ezeket közzé az Interneten[10]. Egy ilyen cikk a számos közül: http://www.dailyedge.ie/emma-watson-photos-hacked-3289934-Mar2017/ Valerie Loftus Mar 15th 2017, 8:34 PM [7]

Mivel mind a négy hivatkozás jelentősen kihat társadalmi, politikai, és magánéletünkre véleményem szerint egyik legfontosabb teendők megérteni és átlátni az e mögött húzódó technikai illetve technológia megoldásokat. Ezek után pedig természetesen a védelme kérdéskörére összpontosítva megtalálni a lehetséges megoldásokat az ilyen események bekövetkezésének lecsökkentésére, elkerülésére. A fenti példákban egyértelműen kirajzolódik, hogy nem csak egyszemélyes kíváncsi embereket kell elképzelnünk a támadók alakjában, hanem országos erre a célra létrehozzon szakmai csoportokat, akik adatbázis formában kívánják beszerezni a legtöbb információt életünk legrészletesebb szegmenseiről is. Ebből eredően a támadások és védekezések elemzésén túl a következő legnagyobb feladat, az informatikai biztonságra való nevelés, oktatás, mely megfelelő alapot nyújt felhasználói szinten is az adatok, vállalati valamint személyes védelmére.

A fentiekben felsorolt aktuális kibertámadások kapcsán, fontos észrevenni a technikai eszközökbe épített kamerák sérülékenységét. Ezek mind munkahelyi mind magánéleti területekre kihatást gyakorolhatnak, melyek komoly következményekkel is járhatnak. A legtöbb számítástechnikai eszközben már beépítve található a webkamera, amely magas mértékben növeli az informatikai támadások kockázatát. Ezen támadások megértése érdekében, meg kell vizsgálni, le kell szimulálni és ki kell elemezni a támadási metódus folyamatát. A következő fejezetben ezeket a mérések, modellezések, valós végrehajtás és annak eredményi kerülnek ismertetésre

TESZT SORÁN ALKALMAZOTT SZOFTVEREK

A cikk jelen fejezetében bemutatásra kerül egy olyan webkamera hack módszer melynek segítségével maga a támadási mechanizmus a Windows Defender és az elavultabb Vírusírtó programok előtt is rejtve marad. Ezt a módszert a szerző végrehajtja, illetve megvizsgálja. A teszt során alkalmazott legfontosabb szoftverek:

- Kali Linux
- Metasploit
- Veil framework

[7] Tükörfordításban rés, hézag. A szövegben a kiszivárogtatott képekre utal.
[8] Adatfolyam, általában videó alapú élő közvetítéseknél használatos fogalom
[9] Egy rendszer vagy adathalmaz egy adott pillanatban érvényes állapotát rögzítő mentést. A publikáció kontextusában kép alapú pillanatfelvétel.
[10] Hálózatok hálózata, globális hálózat

Kali Linux

Legrövidebb meghatározása: operációs rendszer. 2013. március 13-án adták ki ez a backtrack5 továbbfejlesztett változata, Debian [11]alapokon. Penetration [12]és biztonsági tesztekre használható. A Kaliban megtalálható szinte mindegyik program, ami a Backtrackben is volt, hálózati biztonsági tesztelő programok, kezdve, a proxy[13], fuzzer[14], crawler[15], minden, ami szükséges a biztonsági rések teszteléséhez hackeléshez. A BackTrack egy Debian Linux alapú, számítógépek sebezhetőségével foglalkozó, teljesen ingyenes operációs rendszer. Nevét a backtracking kereső algoritmus után kapta. Hackerek és biztonsági szakemberek körében nagyon népszerű. Operációs rendszerek (jellemzően Microsoft Windows) sebezhetőségeinek felderítésére és kihasználására alkalmas. Rengeteg sikeres betörést hajtottak vele végre szerte a világon. Első helyen áll, hisz továbbiakban tárgyalt tesztekhez ez lesz a támadó számítógép operációs rendszere. [8]

Metasploit

A Metasploit egy Penetration tesztelésre kifejlesztett nyílt forráskódú platform, melynek segítségével hardveres vagy szoftveres sérülékenysége, informatikai biztonsági rések vizsgálhatóak, kihasználhatóak. Ezáltal előidézhető az alapvető üzemi állapottól való eltérő működtetése az informatikai eszközöknek. Számos módszert beleértve általánosságban itt ezek a folyamatok a rendszergazdai jogosultág megszerzésére vagy szolgáltatás megtagadására irányulnak (DoS[16]). A Metasploit projekten belül - amely a fentiekben leírt funkciókat biztosítja – a Metasploit Framework –mint alprojekt - teszi lehetővé az Exploitok[17] elkészítését és futtatását.

Az *Exploit* egy olyan forráskódot, programot vagy parancssorozatot jelent, mely alkalmas a biztonsági rések kihasználásra. Ezen felül *Payload-nak*[18] nevezik az a kódhalmazt, amit az Exploit-hoz csatolnak és a megfelelő jogosultság megszerzése következtében lefut. Általában egy Exploit egy sérülékenységet képes kihasználni. A legtöbb esetben az Exploit nyilvánosságra hozatala után a szoftver gyártója egy javítást, patch-et ad ki a támadható programhoz. Ezek után az adott sérülékenységnek kihasználása már nem vezet

[11] A Debian elnevezés egy gyűjtőfogalom. A többség azonban a népszerű Linux-disztribúciót érti rajta, aminek a helyes megnevezése Debian GNU/Linux, ezzel is jelezve, hogy az adott rendszer a Linux kernelt és nyílt forráskódú, szabad felhasználású (GNU licenc alatt publikált) szoftverek együttesét használja.

[12] Tükörfordításban behatolás, informatikai szaknyelvben a számítógépbe való betörés teszteknél használatos definíció

[13] Olyan szerver (számítógép vagy szerveralkalmazás), amely a kliensek kéréseit köztes elemként más szerverekhez továbbítja. A kliens csatlakozik a proxyhoz, majd valamilyen szolgáltatást (fájlt, csatlakozást, weboldalt vagy más erőforrást) igényel, ami egy másik szerveren található. A proxy szerver a kliens nevében eljárva csatlakozik a megadott szerverhez, és igényli az erőforrást a számára.

[14] Automatizált szoftvertesztelési technika, amely magában foglalja az érvénytelen, váratlan vagy véletlenszerű adatok bevitelét egy számítógépes program bemeneteként.

[15] Olyan internet bot, amely szisztematikusan böngészi a World Wide Web-t, jellemzően a webes indexelés céljából.

[16] Egy számítógépes támadás, ahol az elkövető az internetre csatlakozó gazda szolgáltatásainak ideiglenes vagy végtelenségig történő megszakítását célozza meg.

[17] Sérülékenységet, vulnerability-t kihasználó program, programkód, általában a célja, hogy információt szivárogtasson, a payload-ot lefuttassa, vagy a célpontot megbénítsa.

[18] Az exploit része, a hacker által futtatni kívánt programkódot tartalmazza.

működőképességre. Ez az oka annak, hogy a black-hat hackerek [19]általában nem, vagy csak más crackerek[20] számára teszik hozzáférhetővé Exploit-jaikat. Az ilyen Exploit-okat (illetve amelyek ellen még nem készült biztonsági javítás) nulladik napi támadásnak nevezik. [9] Az Exlpoit-okat két csoportba soroljuk be:

- aktív (konkrét számítógépre specializálódtak, programkód befejezésénél kilépnek, például a brute force [21]metódusok amint megnyílt egy shell[22] az áldozat gépéről, úgy kilépnek)
- passzív (itt az Exploit-ok várják a számítógépeket, és amint csatlakoztak rájuk végrehajtják a műveleteket. Főleg FTP[23], E-mail kliens és Web böngésző munkaállomásokra fókuszálnak.) [9]

Veil Framework

Olyan Metasploit Payload-okat tudunk generálni vele, amiket a legtöbb vírusirtó nem tud felismerni. A programban jelenleg 26 féle módszer van implementálva. A program elindítása után egy jól megszokott "keret rendszerforma" fogad bennünket.[10]

Ezek a parancsok állnak a rendelkezésünkre:

use	Egy meghatározott Payload használata. (pl. use 3)
info	Információk egy megadott Payload-ról. (pl. info 22)
list	Kilistázza az összes elérhető Payload-ot.
update	Frissíti a Veil az elérhető legfrissebb verzióra.
clean	Kiüríti a Payload mappát.
checkvt	Leellenőrzi, hogy VirusTotal[24]-on fent vannak-e a Payload-ok hash[25]-jei.
exit	Bezárja a Veil-t. [8]

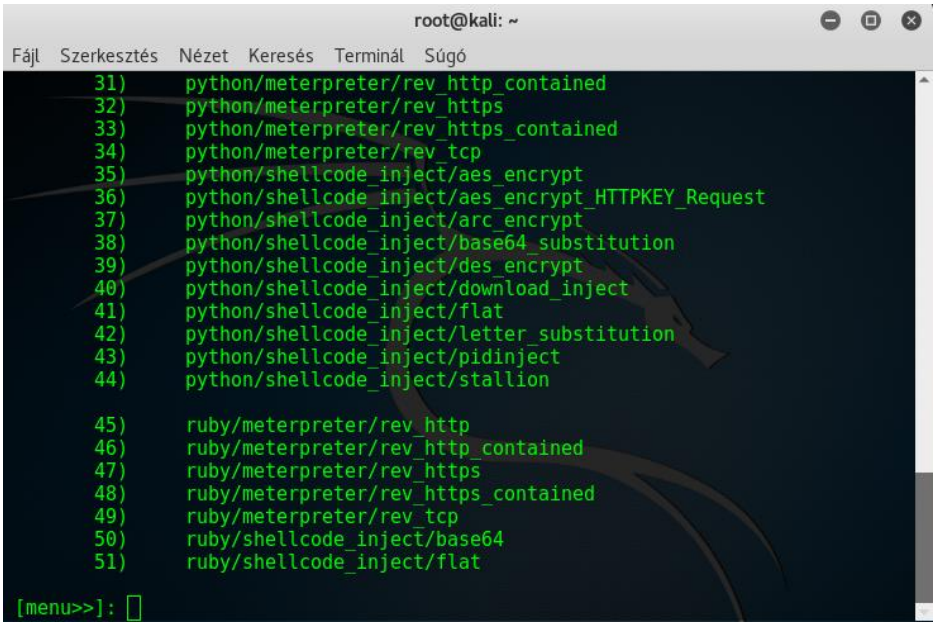
WEBCAM HACK – PENETRATION TESZT

Kezdetben először is le kell szögezni a használt operációs rendszereket, szoftvereket, valamint magát a hálózati környezetet. A támadó számítógép szerepét egy Kali Linux operációs rendszert futtató Laptop látja el, melyen a már gyárilag hozzáadott Penetration teszteléssel kapcsolatos szoftvereken kívül, a Veil keretrendszer feltelepítését is végrehajtásra került. Az áldozat gépet, gépeket több operációs rendszerrel kísérletezve lettek kipróbálva kezdve a Windows 7, Windows 8.1 és bezárva a sort a Windows 10-es verziókkal. A kártevő szoftvert bejuttatása web alapon lett előkészítve, így a Linux rendszeren egy Apache web szervert is fut, ahol publikálásra kerül egy teszt .php oldalt. Ebben az oldalban lesz elrejtve egy AdobeFlash.exe nevezetű fájl, amely letöltéskor és futtatáskor megnyitja a Meterpreter session-t az áldozat gépére. A Veil AES titkosított Reverse-tcp folyamat segít a Payload-ot,

[19] A 'rosszfiúk', szintúgy biztonsággal foglalkozó emberek, akik nem feltétlenül jóra használják fel a 'kutatási eredményeiket' - vagy eladják a legtöbbet fizető ajánlattevőnek, vagy kihasználják a hibát a saját céljaikra.
[20] A crackerek elsősorban a rombolás élvezetéért tevékenykednek, vélt vagy valós sérelmeikért állnak bosszút látványos, hírekbe kerülő akciókban.
[21] A teljes kipróbálás módszere, egy, a titkosító rendszerekkel szemben alkalmazott támadási mód, ami elvileg mindig eredményes.
[22] Parancssor, konzol, mely hozzáférést ad az operációs rendszerhez egy szöveges kezelőfelületen keresztül.
[23] File Transfer Protocol – Fájlátvitelre használt szabvány
[24] A VirusTotal számos vírusirtó terméket és online keresőmotort tartalmaz, hogy ellenőrizze a vírusokat.
[25] Olyan informatikában használt eljárások, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le. Az így kapott véges adat neve hash/hasító érték.

olyan állapotban megírni, hogy azt a vírusirtó programok és a Windows Defender nem ismerje fel, ne figyelmeztessen futtatáskor.

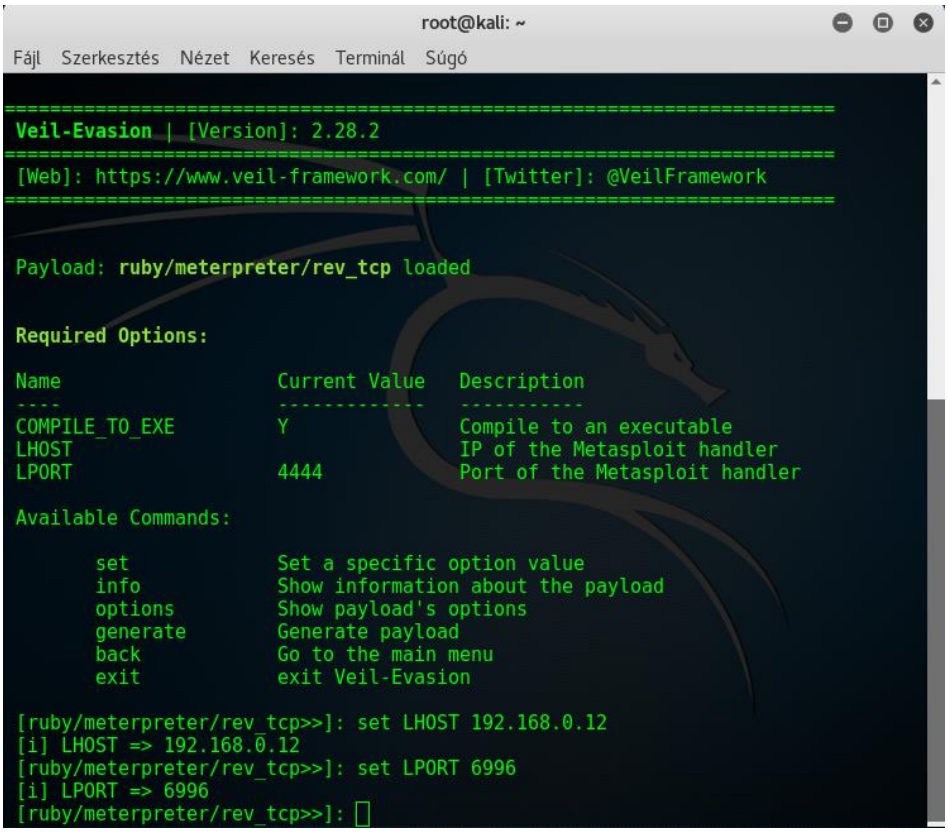
1. A Kali-ban a Terminál ablakot megnyitva futtatásra kerül a „*veil-evasion*” parancsot, mely behozza a keretrendszert, amely az Payload-okat különböző paraméterek segítségével Perl programozó nyelvben megadott utasítások alapján legenerálja azt. A keretrendszer rengeteg variációs Payload-ot támogat a kivitelezés függvényében, ahogy ezt a 2. ábra is szemlélteti. Jelen támadásban a 49.-es számú „*ruby/meterpreter/reverse_tcp*” kerül végrehajtásra. Mely egy visszafordított tcp kapcsolatot fog engedélyezni az áldozat számítógépén. Ezt a „*use 49*” parancs kiadásával hajtható végre.



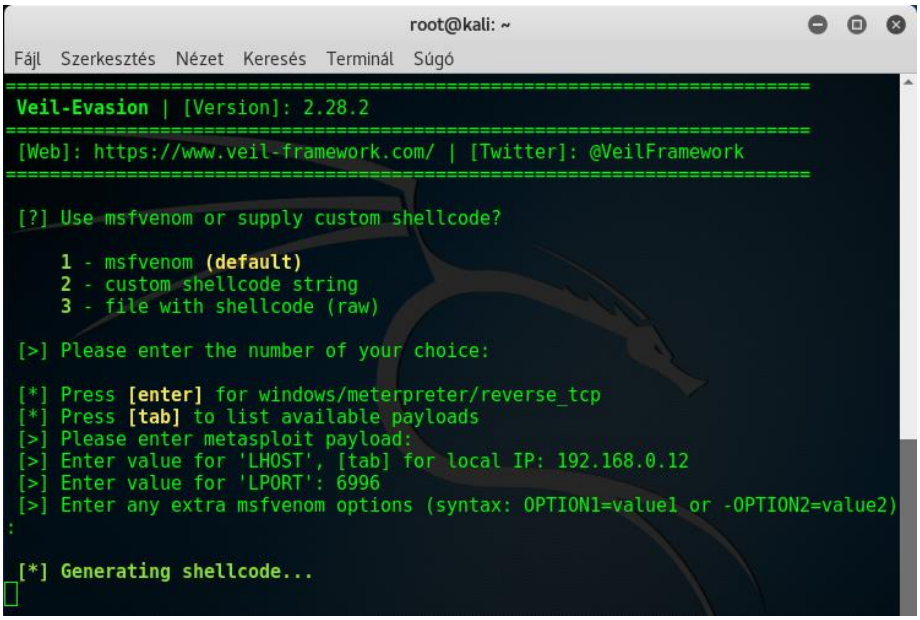
2. ábra Veil keretrendszer kilistázott payload-jai (saját szerkesztés)

A 3.-as ábrán látható, hogy betölti a Payload-ot, majd be kell állítani a Metaspolitot kezelő számítógép IP címét és a kapcsolatra használni kívánt portját. Ezeket az
“set LHOST <az adott IP cím: tesztemben 192.168.0.12>” és az
“set LPORT <az adott portszám: tesztemben 6996>” parancsok kiadásával kerül beállításra.
A következőkben már csak az opcionális beállításokat szükséges teljesíteni és legenerálni azt a *„generate”* parancs segítségével.
Amint ezzel a műveletsor lezárul, szintén legenerálásra kerül egy hasonló Payload, viszont itt már a 35-ös sorszámú *„python/shellcode_injcet/aes-encrypt”* változót használva az előzőleg legenerált „*reverse_tcp shellcode-ba*”egy *AES* titkosítást injektálva az Exploitot a Windows Defender és számos vírusirtó program számára nem detektálható téve. Ezáltal a számítógép nem jelez, amint az .exe fájlt futtatja valaki, kinyitva a támadó gép felé a már megadott portszámot. Természetesen ez esetben is be kell állítani a támadó számítógép IP címét valamint portszámát. Ezen felül egy paramétert szükséges beállítani mindkettő Exploit esetében, mégpedig a nevét. Fontos kiemelni a név választásánál, hogy gyanútlan, vagy mindennapos használat esetén is előforduló név legyen. A tesztelés során a Flashpalyer.exe kerül megadásnak az Exploit-nak. Felhívom a figyelmet, hogy a továbbiakban a Flashplayer

széleskörű ismeretét, böngészők esetében követelmény tulajdonságát kerül kihasználásra az Exploit bejuttatására illetve futtatására.



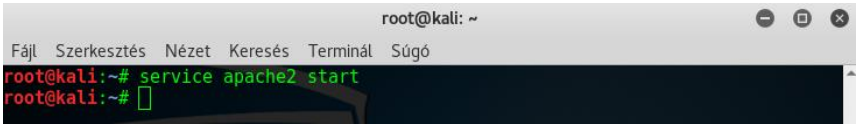
3. ábra Reserve Tcp forrás IP cím és portszám megadása (saját szerkesztés)



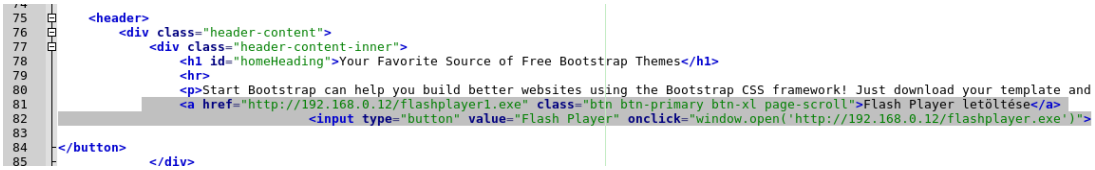
4. ábra Payload generálása exploit .exe fájlokba (saját szerkesztés)

2. Kész a titkosított Payload-al rendelkező Exploit, melynek fájlkiterjesztése .exe. Az áldozat gépére mindenképpen úgy érdemes bejutatni az Exploitot, hogy az ne keltsen gyanút. Többféle megoldás létezik, mint például a hamísított e-mail, pendrive-on keresztül stb. Web szerveren keresztüli gyanútlan letöltést választottam. Így mint az az

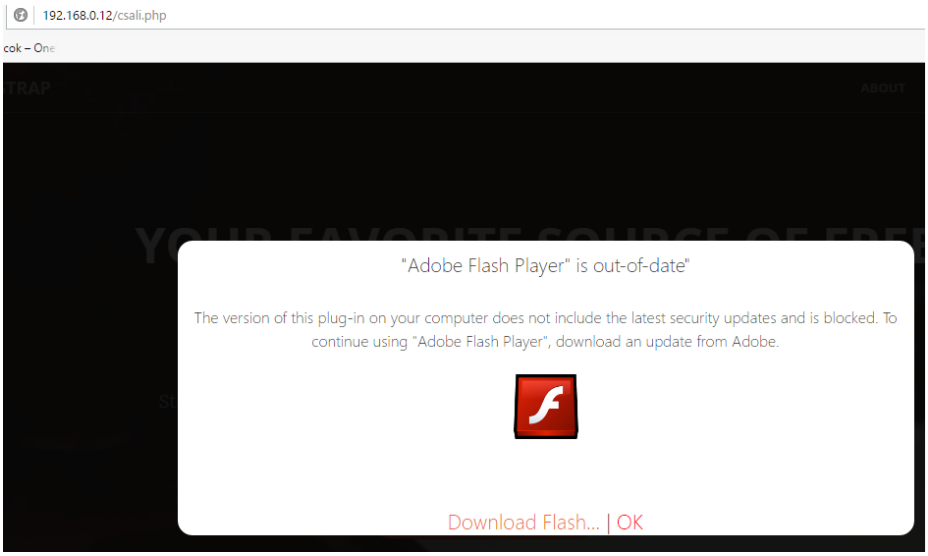
5-ös és 6-os ábrán is látható elindításra került a Kali-n az Apache2 web szerver szolgáltatást, majd .php fájlban egy alapvető oldalt készült el. A .php kódot kiegészítetésre került egy felugró ablak Javascript-el. Ez azt eredményezi, hogy az oldal megnyitása esetén automatikusan felugrik egy ablak, mely figyelmeztet az Adobe Flash Player komponens elavultságára és felajánlja a letöltést. Rákattintva a letöltésre, és elindítva a fájlt, mindenféle jelzés nélkül kiépül a kapcsolat az áldozat és a támadó gép között az adott porton. (A vírusirtó és a Windows Defender valamint tűzfal nem jelez!)
Feltéve, ha a támadó gépen elindítottuk a lentiekben tárgyalt 3. lépést.



5. ábra Apache2 web szerver szolgáltatás elindítása (saját szerkesztés)

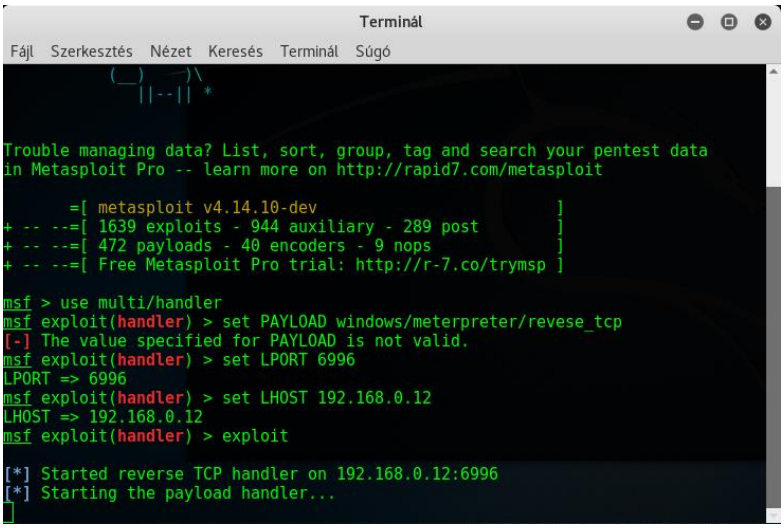


6. ábra .exe beágyazása a .php felugró ablakába (saját szerkesztés)



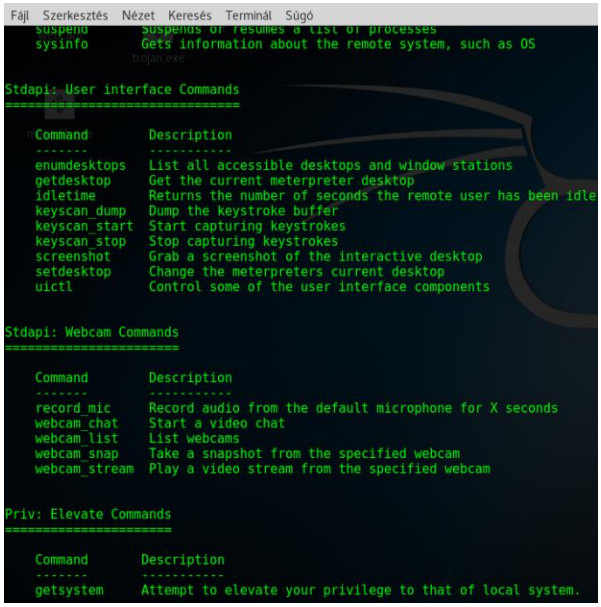
7. ábra Felugró ablakba ágyazott FlashPlayer-nek álcázott exploit (saját szerkesztés)

3. Az weboldal publikálása után, elindításra kerül a Metaspolit programot, majd a következő parancsok begépelésével be kell várni a reverse_tcp adott IP címen és porton való kezelését, azaz a kapcsolat létrejöttét, valamit magát a kihasználást, kiaknázást:
   „use /multi/handler”
   „set LPORT <portszám: testelésemben 6996>”
   „set LHOST <IP cím: tesztelésemben 192.168.0.12>”
   „exploit”



8. ábra Metspolit segítségével az exploit végrehajtása (saját szerkesztés)

4. Az Adobefalshplayer.exe áldozat felőli futtatása, és a támadó felőli Exploit futtatása során kiépül a kapcsolat, és Meterpreter rengeteg lehetőséget kínál fel. Az adminisztrátori jogok átvétele az áldozat számítógépe feletti lehetőségen keresztül a rajta lévő adatok másolásáig, törléséig, felülírásáig, a web kamera és mikrofon opciókkal bezárólag.



9. ábra Meterpreter által felkínált opciók (saját szerkesztés)

5. A „webcam stream”-et kiválasztva elindítani az áldozat gépén lévő web kamerát. Látható, hogy az élő videó stream a támadó Linux gépen nyílik meg egy HTML ablakban, míg az áldozat gépei Windows XP-től Windows 10 operációs rendszerig működik.

KÖVETKEZTETÉSEK

A publikációban taglalt témakör aktualitása megkérdőjelezhetetlen, hisz az IoT világában kihat életünk minden szegmensére. Csakúgy, mint a magánéletre, úgy a nemzetközi, hazai politikai életre, és társadalmi élet szerepköreire is egyre nagyobb teret nyerve meghökkentő hatást gyakorol. Ezen túlmenően személyiségjogi kérdésköröket, és terület behatárolási kérdéseket is felvet, mely fokozottan bonyolulttá teszi az informatikai biztonság vagy kiber műveletek szakterületét.

Meglátásom szerint, az ezzel kapcsolatos megfelelő oktatás, és biztonságtudat hirdetése és gyakorlása elengedhetetlen. A mai oktatási rendszer nincs felkészülve, és nem helyes tematikával oktatja az informatikával kapcsolatos tudásanyagot, egyértelműen középiskolai szinten is reformációra van szükség. Természetesen vannak erőfeszítések ennek irányában, de a folyamatos gyors fejlődése az informatikai szakterületnek csak újabb hátrányokat képez, mely ezeknek a törekvéseknek szintén akadály. Konklúzióként mégis az állapítható meg, hogy az informatika mind az oktatás, mind a munkafolyamatok, és műveletek terén az idővel és a naprakészen mindig az aktuális, viszonylag modern technikai megoldásokkal szembeni szélmalomharc fog jellemezni. Hasonlóan a biztonsággal kapcsolatos területen, ahol a szakemberek nagy átlaga által vallott nézőpont, hogy 100%-os biztonság nem létezik. Mégis mindkettő szakterületen törekedni kell a kornak megfelelő helytállást biztosítani.

Ezeknek a helytállásoknak tesz eleget a technikai és technológiai folyamatok vizsgálata, megértése, és használata mely biztosítja a exponenciálisan megugró fejlődés követését.

Tudományos eredménynek tekintem a személyes Payload létrehozását, mely minden generálásnál olyan Perl alapú karaktereket tesz a Exploit payload-jába, melyet így egyedinek lehet tekinteni és ezáltal a vírusirtók és a tűzfal alapú megoldások megkerülhetőek. Fontos megemlíteni az Exploit-ok sérülékenységeket használnak ki a rendszeren, melyeket az adott rendszer kibocsátói annak nyilvánosságra kerülésekor javítanak. Tehát a publikációban leírt metódus, jelenleg működőképes, de a későbbiekben lehet nem az elvárt eredményt fogja produkálni. Ennek révén egy idézettel zárnám összegzésemet:

„Keep in mind, though, that there is NEVER a single, final solution. The hacker must be persistent and creative in finding ways past these devices, so if one method fails, try another, then try another, until you find one that works." [10]

Ismeretlen szerző

Mely lényege, hogy sosincs egy végső megoldás. Egy hacker-nek kitartónak és kreatívnak kell lennie, hogy megtalálja az informatikai eszközökhöz vezető kapcsolat módját, és ha az egyik nem vezet sikerre, addig kell próbálkozni, amíg az egyik működik.

FELHASZNÁLT IRODALOM

[1] BLESZITY J. [et al.]: *Műszaki kutatások és hatékony kormányzás*; Hadmérnök 10. évf. 3. szám (2016. szeptember), pp. 221-242.

[2] BODA J. [et al.]: *Fókusz és együttműködés*, A hadtudomány kutatási feladatai; Honvédségi Szemle 144. évf. 3. szám (2016/3.), pp.3-19.

[3] *Russian Hacking in the U.S. Election Share Tweet More Complete coverage of Russia's campaign to disrupt the 2016 presidential election*. www.nytimes.com/news-event/russian-election-hacking (letöltve 2017.04.10)

[4] Hivatalos: *Putyin megtámadta az amerikai elnökválasztást* Csarnó Ella és Klág Dávid 2017.01.06.http://index.hu/kulfold/usa/feher_haz/2017/01/06/hivatalos_putyin_tamadta_meg_az_elnokvalasztast/ (letöltve 2017.04.10)

[5] GREENWALD, G: No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State, US, 2014, Metropolitan Books, ISBN: 978-1627790734

[6] Meghackelték az Origót, Magyar Nemzet 2017. április 13., csütörtök 07:25, frissítve: csütörtök 09:57 https://mno.hu/media/meghackeltek-az-origot-2394595 (letöltve 2017.04.10)

[7] *Emma Watson is the latest victim of hackers after her private photos were leaked online*, Valerie Loftus Mar 15th 2017, 8:34 PM http://www.dailyedge.ie/emma-watson-photos-hacked-3289934-Mar2017 (letöltve 2017.04.10)

[8] *Basic Security Testing with Kali Linux 2*, Daniel W. Dieterle, March 24, 2016 https://www.kali.org (letöltve 2017.04.10)

[9] METASPLOIT: *The Penetration Tester's Guide by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni* (Metasploit-The Penetration Tester s Guide.pdf) (letöltve 2017.04.10)

[10] Mastering Kali Linux for Advanced Penetration Testing, Robert W. Beggs, June 2014 https://www.veil-framework.com (letöltve 2017.04.10)