

XXXII. ORSZÁGOS TUDOMÁNYOS DIÁKKÖRI KONFERENCIA
HAD- ÉS RENDÉSZETTUDOMÁNYI SEKCIÓ
GÖDÖLLŐ, 2015. ÁPRILIS 15-17.
SZENT ISTVÁN EGYETEM GAZDASÁG- ÉS TÁRSADALOMTUDOMÁNYI KAR
NEMZETI KÖZSZOLGÁLATI EGYETEM

INFORMATIKAI HÁLÓZATOK VIZSGÁLATA ETIKUS
HACKER SZEMSZÖGBŐL

JELIGE: EXILES

PÁLYAMUNKA LEZÁRÁSÁNAK IDŐPONTJA: 2015.01.07

2015.

TARTALOMJEGYZÉK:

Bevezetés:	4
1. Az informatikai biztonság és az Etikus Hackelés kérdése:.....	6
1.1 A legjelentősebb kiber támadások bemutatása:.....	6
1.2 A kibertér védelmét szolgáló irányelvek, stratégiák és szabályzók:	7
1.3 A hekkelésről általában:	9
1.3.1 Fogalmi magyarázat:	9
1.3.2 Az etikus hackelés bemutatása, általános tudnivalók:.....	10
1.3.3 Egy támadás lépéseinek bemutatása:.....	11
2. Fejezet Speciális rész	13
2.1 A Tesztkörnyezet kialakítása:	13
2.1.1.A Potenciális környezet megismerése/felderítése:	13
2.2 Speciális szakmai fogások, tapasztalatok	14
2.2.1 Externális & Internális URL-ek felderítése:.....	15
2.2.2 Környezeti Információk:	15
2.2.3 WHOIS Lookup:	16
2.2.4 Email vizsgálat:	17
2.3 Hálózat teljes körű vizsgálata:	18
2.3.1 IP (Internet-Protocol) címek vizsgálata a hálózaton:	19
2.3.2 Banner grabbing:	20
2.3.3 Portok vizsgálata:	20
2.3.4 Reguláris Port vizsgálat:.....	22
2.3.5 Ping Scan & Traceroute:	23
2.3.6 Intense Scan plus UDP:.....	24
2.3.7 Vizsgálatok összegzése:	26
2.4. Hálózati Sebezhetőség vizsgálata:.....	27
2.4.1 A Sebezhetőség:	27
2.5. Információ Lopás a hálózati elemektől:	29
2.5.1 Sniffing/Metasploit:	29
2.5.2 Legfőbb Webes hibák:	30
2.5.3 Keyloggerrel végzett információ lopás:.....	31
2.6 Statisztikák a felhasználóról:.....	33
3. Tudatosság mint védelmi eszköz:.....	35
Összefoglalás:.....	38

Felhasznált Irodalom	40
Ábra és Táblázat jegyzék	42
Melléklet:	43
Táblázat: Externális & Internális URL-ek	43
Táblázat: WHOIS Lookup.....	45
Táblázat: Hagyományos IP címek vizsgálata:	46
Táblázat: Portok Vizsgálata:	47
Táblázat: Banner Grabbing:.....	50
Táblázat: Intense Scann and UDP.....	51

BEVEZETÉS:

Az Informatika napjaink leggyorsabban fejlődő tudományágak egyike. Ma már nem tudunk sémaszerűen informatikáról beszélni, hiszen a technikai előrelépések következtében számos speciális területre ágazott szét.

Személyes témám az informatikai biztonság, mint egyik legfontosabb és nélkülözhetetlen területe mindennapjainknak. Legyünk akár diákok, alkalmazottak, vezetők, vagy egyéb felelős beosztást betöltő személyek egy terület mindenkép közös lesz bennünk, amely nem más, mint az elektronikus formában tárolt adataink biztonságának a megőrzésére való törekvés. Feltételezhetően senki nem szeretné, ha ezen adatok illetéktelen kézbe kerülnének. Sajnos az új kiaknázatlan lehetőségek csábítóan hatnak a bűnözésre is, amely a tradicionális fizikai dimenzióból egyre jobban a kibertér irányába mozdul el. A „digitális” fejlődés mindkét oldal számára új területek kiaknázását tette lehetővé, ebből adódóan párhuzamosan jelentek és jelennek meg olyan támadó szándékú szereplők, akik célja az új típusú sérülékenységek kiaknázása. Gondolok itt minden személyes és üzleti jellegű információra, bankszámla adatokra, tranzakciókra, hivatalbeli minősített dokumentumokra, avagy akár csak a privát családi fényképek, videók összességére.

A rohamtempóban fejlődő technika által biztosított ingyenes adattárolási felhőszolgáltatások, arra ösztönzik a felhasználókat, hogy már ne egy a hálózattól elszigetelt helyi számítógép háttértárolóját vegyék igénybe, hanem a bárhol elérhető online tárhelyeket. Ennek hatására bőszen is alkalmazzák a felhasználók az online tárhelyek által adta lehetőségeket, ahol GB¹ méretű adatokat tudunk tárolni. [1] A hagyományos papír alapú levelezés, a borítékba zárt kommunikáció egyre jobban háttérbe szorul és ezzel párhuzamosan a helyét egyértelműen az internet által biztosított kapcsolattartás veszi át. Manapság az interneten keresztül osztjuk meg hozzátartozóinkkal, ügyfeleinkkel az információk többségét, amely költséghatékonyan, globális távolságokat másodpercek alatt leküzdve, közel a fény sebességével szállítja az információkat. Az Internet a legfőbb kommunikációs csatornává nőtte ki magát, kialakítva egy olyan határtalan virtuális világot, amely a laikus ember számára inkább tűnik csábító lehetőségnek, mint veszélyes területnek. Azonban, ha figyelemmel követjük a mindennapi híreket, akkor láthatóvá válik a sötét oldala is. Számos olyan esetről hallhatunk, amely arról számol be, hogy bizonyos csoportok

¹ Felhő alapú tárolás: Dropbox - 729€ /év – 5TB felhasználható tárhely

személyes adatokhoz fértek hozzá, számlaszámokat szereztek meg, pénzt tulajdonítottak el, szervereket s egyéb kiszolgáló egységeket állítottak le és még hosszasan sorolhatnánk tovább ezt a sort. A hálózathoz való csatlakozás nem más, mint egy olyan szükséges kapu a virtuális világhoz, amely egyrészt átjáró az információáramláshoz, másrészt kellő odafigyelés nélkül utat nyithat az áldozattá válás irányába is.

A dolgozatom megírásánál fontos szerepet játszott a személyes elköteleződés az iránt, hogy minden esetben az aktuális környezetemhez- és leendő beosztásomhoz kapcsolódó informatikai infrastruktúrában a kockázatokkal arányos lehető legjobb védelmet alakítsam ki.

Ebből adódóan egyrészt célul tűztem magam elé, hogy összefoglaljam azokat az általános és speciális ismereteket, amelyek elősegítik az informatikai biztonság megértéséhez, illetve megteremtéséhez vezető út mélyebb megismerését, másrészt az általam összeállított heterogén tesztkörnyezetben szemléltessem az egyes eljárások működését, eredményeit.

A célom elérése érdekében elsőként betekintést nyújtok a vonatkozó irányelvek, szabályzók körébe. Ezt követően általánosságban bemutatom azokat a lépéseket, amelyek egy jó megtervezett támadás végrehajtásához szükségesek. A következő fejezetben egy általam kialakított tesztkörnyezetben mutatom be a hálózatok kivizsgálásának bizonyos szegmenseit ötvözve, a szociális képességek felhasználásával. Tüzetesebben megvizsgálom a hálózaton keresztül áramló csomagokat, a mozgási mechanizmusokat, amelyek alapkövét jelentik a kommunikáció ezen formájának. Dolgozatom további részében áttekintem a felhasználók által preferált operációs rendszerek, illetve védelmi programok hasznosságát és biztonságát. Továbbá összehasonlítok számos nemzetközi statisztikát a saját vizsgálataimból származó eredménnyel is. Fontosnak tartom a dolgozatban kiemelni a felhasználók biztonságtudatosságának a fontosságát is, amellyel számos biztonsági kockázatot minimális mértékűre lehetne csökkenteni.

1. ÁLTALÁNOS ISMERETEK

1.1 A legjelentősebb kiber támadások bemutatása:

Az informatikai rendszerek tervezésénél szervezésénél, karbantartásánál, üzembe helyezésénél, s folyamatos működtetésénél számos jogszabálynak eleget kell tenni, hogy a megfelelő biztonsági szintet az adott szervezet fent tudja tartani. Az informatikai biztonságra vonatkozó rendeletek, jogszabályok, működtetésre vonatkozó szabályozók napjainkra forrták ki magukat egy nemzetközileg is elfogadható szintre. [2],[3] Korábbi évekre visszatekintve le tudjuk vonni a megfelelő konzekvenciát az események sokaságából, hogy mennyire is gyerekcipőben járt a jogszabályrendszer informatikai biztonságra vonatkozó része. [4] Mire is gondolok ez alatt?

A kiber hadviselés történelmének egyik legnagyobb nemzetközi konfliktusára az Orosz Észti kiber háborúra. A konfliktus informatikai szemszögének legfőbb része, hogy az Észti kormányzati weboldalakat rengeteg támadás érte, amely blokkolta azok elérhetőségét. A hivatalos kommunikációs csatornákat képesek voltak zavarni, teljes mértékben lebénítani. Mindezek mellett a mobil eszközökön beindultak a lázító üzenet szórások, amik elősegítették a fegyveres konfliktusok kialakulását. Mai tudásunk alapján megállapíthatjuk hogy egyértelműen egy túlterheléses támadás volt a háttérben, hiszen az Észti hálózatok forgalma az átlagos szint közel ezer szeresére nőtt. Ennek következtében az „átlag” felhasználók számára is elérhetetlennek bizonyult számos weboldal, állami és önkormányzati szerverek. Megfelelő szakemberek bizonyos útvonalakat vissza tudtak nyomozni egészen az Orosz területen lévő szerverekig.[5] Fontos megemlíteni, hogy a NATO egyik tagállama ellen indított támadás, olyannak minősül mintha az összes tagállam ellen indítottak volna támadást. (Kollektív Védelem elve)².

A továbbiakban szeretnék megemlíteni párat a legnagyobb vitát kiváltó események közül.

- 1999, Moonlight Maze – USA
 - Bizonyos feltételezések szerint az Orosz állam által felbérelt hackerek megtámadták a NASA rendszerét, és titkosított információkhoz jutottak hozzá.

² A washingtoni szerződés (1949. április 4.) 5. cikke

- 2003, Titan Rain – USA
 - Kínai hackerek hajtottak végre egy kiber térben történő kémkedést, aminek révén a védelmi rendszerek hatásosságát és működését vizsgálták.
- 2008, Grúzia – Oroszország
 - A fegyveres konfliktus mellett az Orosz állam teljes mértékben uralma alá vette a Grúz Internet forgalmat. Kormányzati oldalak teljes mértékű megbénítása, tartalmuk módosítása.

1.2 A kibertér védelmét szolgáló irányelvek, stratégiák és szabályzók:

A kiber hadviselés megerősödésével, a támadások gyarapodásával párhuzamosan fejlődtek a vonatkozó irányelvek és szabályzók is, amelyek legfőbb célja a védelem kialakításához szükséges iránymutatások és jogi alapok lefektetése volt. A számos dokumentumból ki kívánom emelni az alábbi hármat, amelyből kettőnek úttörő hazai, még a harmadiknak európai szintű jelentősége van [6].

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről
- Európai Bizottság által kialakított Európai Digitális Menetrend

Az Elektronikus Információs rendszerek teljes körű védelmét biztosítani kell, ami alatt értem a benne kezelt dokumentumok bizalmasságának, sértetlenségének és rendelkezésre állásának összességét. Fizikai és adminisztratív védelemre való törekvés, amely alatt értem a megelőzést, avagy a korai figyelmeztetést, az észlelést, a kellő reagálást és végül a biztonsági események kezelését.

Szükséges a szegmentált biztonsági osztályokba történő besorolás. Ez alatt értem, hogy külön osztályt képez mind a bizalmasság, mind a sértetlenség, mind pedig a rendelkezésre állás. Minden osztályba sorolást megelőz egy kockázat elemzési folyamat. Szabvány alapján

szükséges ennek az elvégzése, de az alapja (papír, program) nincs meghatározva. A rendeletek kitérnek a közvetlen illetve közvetett anyagi károkra is egyaránt.

A biztonsági osztályokba történő besorolásnál 5 különböző szintű osztályt kell figyelembe venni. Jelentéktelen káresemény, csekély káresemény, közepes káresemény, nagy káresemény, végül pedig a kiemelkedően nagy káresemény.

A kellő konklúziót levonva rájöhettünk arra, hogy mindezen szabályzók kimondják hogy az adott rendszert minden esetben 3 osztályba kell besorolnunk, ami megadja számunkra a megfelelő biztonsági szintet. A következő sorokban szeretnék említeni egy idézetet, ami a korábban taglalt tényeket a lehető legjobb módon mutatja be.

„Az informatikai biztonság a védelmi rendszer olyan, a védő számára kielégítő mértékű állapota, amely az informatikai rendszerben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.“

(Muha Lajos-2013)[1].



1.ábra – A kiber hadviselés hajnala [2].

1.3 A hekkelésről általában:

Olyan tevékenységi formula, amely az informatikai világ sajátosságait használja fegyverként. Kihasználva a sérülékeny programokat, rendszereket információ szerzés, bénítás céljából történik.[7]

1.3.1 Fogalmi magyarázat:

Hacker: Kiemelkedő informatikai tudással rendelkező személy, aki a különféle operációs rendszerek, program nyelvek, hálózatok, szerverek üzemeltetése ismeretében képes információt szerezni, sebezhetőséget felfedezni, s azon behatolni az általa definiált rendszerbe. Fontos megemlíteni, hogy egy hackert nem feltétlen a rossz cél vezérli. Többnyire felhívja a figyelmet a problémákra, és készíti az ellenkező oldalon álló felet a korrekcióra.[8] Három típusát különböztetjük meg:

- Fehér kalapos- vagy etikus hacker (White-hat)
- Szürke kalapos-felderítés,hibadetektálás(Grey-hat)
- Fekete kalapos – régi időkben cracker (Black-hat)

Cracker: Az alap koncepciót tekintve, hogy rendkívüli informatikai tudással rendelkezik ugyanúgy igaz a crackerre is, mint a hackerre. Legfőbb különbség azonban, hogy míg a hackert nem vezérli semmilyen önös érdek sem, addig a cracker többnyire hátsó szándékkal tevékenykedik. Információt lop, adatokat módosít, rendszereket tör fel és helyez el rajtuk kártevőket. Többnyire a programkódok visszafejtésével foglalkoznak, hiszen az az alapkőve annak, hogy vírust implementáljunk egy adott programba.

Etikus Hacker: Olyan tevékenységeket folytat, mint a korábban említett két típus, ellenben ő a defenzív oldalon dolgozik. Célja, és szándéka az adott informatikai rendszer sebezhetőségének vizsgálata, és azok kiküszöbölése. Manapság az etikus hackerek alkalmazása olyan jelleget öltött, mint 10 évvel ezelőtt a rendszergazda. Érdemes megemlíteni, hogy Kína közel 30000 fős kiber hadsereggel rendelkezik.

Penetráció: A hacker tevékenység azon folyamata, amikor a tényleges behatolás megtörténik. Amikor penetrálnak egy hálózatot fény derül minden sebezhető pontra. Informatikai berkeken belül alkalmaznak már penetration tester csapatokat is, akiknek a fő feladata a gyengeségek, sérülékenységek felderítése.

1.3.2 Az etikus hackelés bemutatása, általános tudnivalók:

A nem is olyan távoli múltba visszatekintve, a köztudatban megkülönböztettünk hackereket illetve crackereket. A legfőbb különbség ezen két informatikai specifikum között nem volt más mint a megszerzett információ felhasználásának módja. Köztudottá vált, hogy a hackerek az információval nem visszaélnek, hanem az adott sebezhető program, hálózat, informatikai rendszer fejlesztése érdekében kapcsolatba lépnek a fejlesztőkkel.[9]

Mindezzel szemben a crackerek egyértelműen az internetes alvilág számára, avagy önös érdek által vezérelve használják fel az eltulajdonított tartalmakat. Napjainkra kialakult az informatika világában egy úgynevezett Etikus Hacker megnevezés, ami az informatikai biztonságért felelős szegmensén ténykedő embereket öleli fel.

Mit is csinál valójában egy Etikus Hacker ?

Képesek az általános felhasználó számítógépekről is olyan tevékenységeket folytatni, amelyekkel bizonyos hálózatokat, rendszereket tudnak tönkretenni, avagy ezzel ellentétben a rendszer tönkretételét valamilyen formában megakadályozni.

Mivel minden etikus hackeléssel kapcsolatos tevékenység különböző, így mindig a legfekészültebb ember, vagy csoport kiválasztása szükséges. Minden feladat élére olyan embert kell állítani, aki képes átlátni a teljes folyamatot s azt megszervezni, összehangolni, s levezetni.

- A kellő tudással bíró személyek kiválogatása
- Szerződések, tervek, jogosultságok beszerzése
- Felderítés/Felmérés
- Tesztkörnyezet kialakítása
- Sérülékenység felderítése/hozzárendelése
- Kihasználás/Kiterjesztés
- Incidenskezelés tesztelése
- Záró fázis/Véglegesítés
- Jegyzőkönyvek készítése/Jelentések megírása

1.3.3 Egy támadás lépéseinek bemutatása:

Feltérképezés/Felderítés:

- Feltérképezés: Egy hacker minden folyamat végrehajtása előtt teljes körű elemzést végez a számára potenciális célpontról. Az internet adta lehetőségeket kihasználva tömördek információ megszerzésére nyílik alkalmunk. Google Earth, Street View segítségével számos környezeti tényezőt felderíthetünk, amikkel a későbbiekben dolgozni is tudunk. A Feltérképezés legfőbb célja a lehetséges menekülési útvonalak kialakítása, illetve a probléma esetén adódó gyors áttekintés/szervezés.
- Felderítés: Egy támadás megkezdése előtt számos információt szükséges begyűjteni. Mindez természetesen attól függ, hogy mi a cél, mi a célpont. Hálózat törése esetén, teljes körű hálózat vizsgálatra van szükség, ahol megismerjük a kommunikációs csatornákat, a protokollok rendszerét, felderítjük a tűzfalakat, útválasztókat, háttértárolókat.[10] Nem szabad elfeledkeznünk a hálózatra csatlakozó perifériákról sem. A felderítésbe bele kell vennünk a felhasználói bázist is, hiszen sokszor a legegyszerűbb az információk megszerzése a felhasználókon keresztül.

Információgyűjtés:

- Információgyűjtés alatt azt értem, hogy a vizsgált rendszeren belül lévő összes elemnek az összes begyűjthető információjának megszerzése. Hálózati/Megosztási információk, felhasználók, csoportok, csoport nevek, irányítótáblák, operációs rendszerek, kisegítő programok, verziószámok definiálása. Ez a része a folyamatnak azért fontos, mert egy hackelési folyamat legtöbbször elavult verziószámú programokon keresztül történik. Ez nem jelenti azt, hogy a teljesen friss illesztőprogrammal rendelkező program törhetetlen, de az kijelenthető hogy sokkal kisebb a kockázati tényező.

Rendszer törés:

- Ezen fázis alá tartozik minden olyan művelet, amely valamilyen formában is a rendszer biztonságát fenyegeti. A jelszavak megszerzése akár nyers erő felhasználásával (Brute Force), vagy meta adatok alkalmazásával. Autentikációs lehetőségek módosítása, jogosultságok kiosztásának megváltoztatása, jogosultságok kibővítése. Ezek a műveletek nem vonzanak

magukkal kártevő alkalmazásokat. Ezekkel ellentétben számos olyan folyamat jöhet szóba, ami egy vagy több kártevő rendszerbe juttatásával tudunk elvégezni. Keylogger által végrehajtott jelszó lopás, Trójai által kiküldetett információk.

Social Engineering:

- Számomra az egyik legszimpatikusabb eljárás, amelyet egy informatikus alkalmazni tud. A személyes képességek felhasználásával, a saját kreativitásunkkal átszőtt megtévesztések fontos szerepet játszanak az Etikus hacker világban. Kevin Mitnick nevéhez kapcsoljuk a „társadalom mérnökséget”, mint hacker tevékenységet. Ő volt az a személy, aki definiálta és szakággá növelte ezt a témakört. A Social Engineering bebizonyítja, hogy minden rendszer biztonságának a legnagyobb fenyegetettséget az ember okozza.[11] A laikus számára semmit sem jelentő információ egy hackernek a megoldást jelentheti.

A Social Engineering is hasonlít az összes etikus hacker folyamatra. Mindegyik project más. Ebből kiindulva szükséges a megfelelő forgatókönyv felépítése. Miből is áll ez ?

- Információszerzés
- Kapcsolatépítés
- Kapcsolatok felhasználása/kihasználása
- Végrehajtás, célunk megvalósítása

Social Engineering lépései:

Információszerzés: Szükségessé válik minden információ megszerzése, hogy a kellő szintű kapcsolatokat képesek legyünk kiépíteni. Minél több információ szükséges, hogy a kapcsolat építése s megtartása kellő képen hiteles maradjon.

Információszerzési mechanizmusok:	Telefonos megkeresés
	Célzott levél
	Kukaátvizsgálás
	Vállszörf

Kapcsolatépítés: A további lépésekhez nélkülözhetetlen a megfelelő kapcsolati tőke kialakítása, ami által olyan információkhoz juthatunk a továbbiakban, amelyek kulcsfontosságú szerepet fognak játszani.

Kapcsolat felhasználása: Mindazon által, ha sikerült a korábbi két pontot megfelelően teljesíteni, alkalmunk nyílik a kapcsolatunk bizalmi körébe férközni, könnyen felhasználhatjuk az összes tőle megszerzett információt saját, valós érdekünkben.

2. SPECIÁLIS ISMERETEK

2.1 A Tesztkörnyezet kialakítása:

Munkám során szükségesnek bizonyult egy tesztkörnyezet kialakítása, mivel olyan programokkal és olyan folyamatokat végeztem, amelyek bizonyos területeken a világban jogszabályba ütköznek. Mindezek mellett a folyamatok sosem garantálják a sikert így számolni kell azzal is hogy fordítva sül el a dolog. Mivel programokba implementált kártevőkkel dolgoztam így fontos szerepe volt a tesztkörnyezetnek, hogy ne szabaduljon ki a valós rendszerbe.

2.1.1.A Potenciális környezet megismerése/felderítése:

Napról napra nő azon számítógépek száma, melyek az internetre csatlakozás következtében kiteszik magukat különféle hacker támadásoknak. A felhasználók böngésznek, e-maileket olvasnak, programokat töltenek le, közösségi hálózatokon cserélnék információt. Eközben előfordulhat, hogy akaratlanul rosszindulatú programkódot juttatnak be a számítógép hálózatába, például férgeket, vírusokat vagy trójai falovakat. Az Internet kapcsolatot ugyan rengeteg tűzfal védi, de nem nagyon jellemző a behatolás-érzékelő rendszerek vírusvédelmi programcsaládok használata, vagy további biztonsági intézkedések megléte személyes otthoni környezetben. A hackerek ilyenkor megtalálják a módját a károkozásnak az Internetre kapcsolt gépek, sőt egész hálózatok „lefagyasztásával” - vagy, ami még rosszabb, az ezekbe való betöréssel és az értékes üzleti információk eltulajdonításával vagy megsemmisítésével. Az alábbi táblázat megmutatja, hogy milyen szegmensek vizsgálata szükséges számunkra a tényleges törési folyamatok megkezdése előtt.

Hálózati Információk

Domain Nevek	Nemzetközi Domain Nevek	Hálózati Blokkok
Internet Protocollok	TCP/UDP szolgáltatások	ACL's, hitelesítési kontroll
Hálózati Protokollok	VPN pontok	IDS'es alkalmazások
Analóg Telefonszámok	Digitális Telefonszámok	Autentikációs folyamatok
Rendszer sebezhetőségek	Portok Vizsgálata	Forgalom ellenőrzés

1.táblázat: Hálózati információk[3].

Rendszer Információk

Felhasználónevek	Csoportnevek	Rendszer banner
Útválasztó táblázat	SNMP információk	Rendszer architektúra
Távoli hozzáférés	Rendszernév	Jelszavak

2.táblázat: Rendszer információk [4].

Szervezeti Információk

Alkalmazottak adatai	Szervezeti Weboldalak	Cég Könyvtár
Geográfiai adatok	Címek és telefonszámok	HTML megjegyzések
Biztonsági előírások	Web server linkek	Vállalati háttér

3.táblázat: Szervezeti információk [5].

2.2 Speciális szakmai fogások, tapasztalatok:

Ebben a fejezetben az általános környezeti információkat szeretném bemutatni, amelyek a továbbiakban létfontosságú szerepet játszanak. A rendszer törése megkezdése előtt, az adott hálózatot körülményes módon számos vizsgálat alá kell vetni. Elsődleges feladatunk az úgynevezett „Footprinting” folyamatsorozat, ami alatt számos különböző részt különböztetünk meg. „Footprinting” folyamatok alatt értem az összes olyan internetes tevékenységet, amihez informatikai/biztonságtechnikai szaktudásra egyáltalán nincs szükség. Egész egyszerűen a felhasználóknak kínált lehetőségek összessége az, ami hozzásegít minket egy rendszer/hálózat vagy egy adott személy sok-sok digitális adattest !

Amennyiben tudjuk, hogy egy felhasználó éppen azon a hálózaton ténykedik, amivel nekünk valamiféle szándékunk van, gyorsan és egyszerűen információt tudunk kinyerni mind róla mind pedig magáról a hálózatról. [12]

2.2.1 Externális & Internális URL-ek felderítése:

http://hhk.uni-nke.hu
http://hhk.uni-nke.hu/kutatas-es-tudomanyos-elet/eu-palyazatok/kmop-4_2_1-b
http://intranet.uni-nke.hu/
http://ktk.uni-nke.hu

4.táblázat: URL címek [6]

Az URL³ címek vizsgálata azért szükséges számunkra, mert sok olyan alcím létezik egy weboldal mögött, amit a szokványos úton meglehetősen nehezen érünk el. Mivel az elsődleges célja egy rosszindulatú hackernek, hogy blokkolja a weboldal forgalmát, vagy információt lopjon a háttérfolyamatokról, vagy leállítsa, így fontos tisztában lennünk azzal, hogy hogyan is épül fel a weboldalunk. Számos olyan esettel találkoztam személy szerint én is, ahol egy alcímen keresztül lehetőségem nyílt bárminemű .jpg kiterjesztésű dokumentum feltöltése egy ellenőrizetlen útvonalon. Ezzel semmi probléma nem lenne, ha laikus ember találkozna egy ilyen stílusú felülettel. Amennyiben tovább gondoljuk a történetet, azonnal rá lehet jönni, hogy ha a feltöltési felület védtelen, akkor a .jpg fájlba implementált kártevővel sok mindenre képesek vagyunk.

2.2.2 Környezeti Információk:

Amennyiben tudomásunk van a cél hálózat helyzetéről, az internet adta lehetőségek gyanánt képesek vagyunk szinte teljes mértékben lokalizálni a helyszínt. A Google MAPS, Google Street View betekintést enged számunkra a világ szinte minden pontjára így meglehetősen egyszerű az információ szerzés.[13]

Ezen felderítési forma is a Social Engineering egyik alapeleme, hiszen ki lehet szűrni a biztonsági problémákat (kamerákat riasztórendszereket), néhol még bizonyos hálózati eszközök (public wifi) elhelyezkedésére. A Social Engineering mint már korábban említettem számomra egy preferált terület. Nem szükséges informatikai szaktudás ahhoz, hogy valaki a szociális képességeit alkalmazni tudja, s ezáltal manipuláljon, megtévesszen

³ URL - Uniform Resource Locator

embereket információ szerzés céljából. Social Engineeringbe tartozik több adathalászati formula is. Ezek közül a köztudatban a két legismertebb van jelen:

- Phishing – Előre definiált célcsoport számára elküldött üzenet, akik rendelkeznek közös érdeklődési tényezőkkel. (Üzletek vevőkörei, Sport klub tagok, Banki ügyfelek)
- Whaling – Célközönsége lényegesebb kisebb létszámmal bír, mivel egy specifikusan a cél felső vezetésére irányuló folyamat.

A továbbiakban megkülönböztetünk még három különféle eljárást:

- Telefonos adathalászat
- Farmolás
- Információ ellesés

2.2.3 WHOIS Lookup:

A WHOIS bárki számára elérhető kereső motor, ami tulajdonképpen nem csinál mást, csak megvizsgálja az általunk megadott IP címet avagy az adott Domain címet. Számos információt tudunk kinyerni egy ilyen folyamat elvégzését követően. Gondolok itt nevekre, címekre, telefonszámokra, fax címekre, információkra a szolgáltatásról s rengeteg más adatra, ami a továbbiakban kifejezetten előnyös lehet egy támadás végrehajtása során. Korábbi évek során a biztonsági referensek figyelmét elkerülte az, hogy sokhelyütt személyi igazolványszámok, lakcímek is megjelenítésre kerültek. Mára már ezt a problémát sikeresen kiküszöbölték.

A WHOIS kialakulását tekintve a következők állapíthatóak meg: Az adatok nyilvánosságát az internet határok nélküli, nemzetközi volta, valamint a rendkívül nagy mennyiségű domain indokolja. Az adatok nyilvánosságra hozatalával ugyanis bármilyen probléma (például műszaki jellegű kérdések, nyomozóhatóság eljárása, esetleg személyiségi jogok sérelme) esetén közvetlenül a domain kezelőivel, birtokosaival lehet felvenni a kapcsolatot. Egyéb esetben ez csak közvetítők (külföldi bíróság, rendőrség) segítségével lenne – talán – megoldható. A domain név regisztrációt kérők a regisztrációval elfogadják a már említett szabályzatot, mely tartalmazza, hogy az adatok nyilvánosságra kerülnek.

A domain név regisztrációjával a regisztrációt kérő hozzájárul adatai kezeléséhez, nyilvánosságra hozatalához. A nyilvánosság mindezekén felül is indokolt az iménti érvek

alapján; így az adatkezelés megfelel a célhoz kötöttség követelményének is. A világháló fontos eleme a nyilvánosság. Ennek korlátozása az internetet lényegétől fosztaná meg. Az viszont, hogy világszerte bárki, bármit közzétehet a saját oldalán, indokolja azt, hogy az oldal "birtokosát", üzemeltetőjét könnyen el lehessen érni.

A fentiek alapján az adatvédelmi biztos álláspontja szerint a Magyarországi Internet Szolgáltatók Tanácsának a domain regisztrációval kapcsolatos eljárása, ezen belül az adatok nyilvánosságra hozatala nem jogsértő.

„To receive output for a database update, use the "-B" flag.

Information related to '193.224.76.0 - 193.224.76.255'

Abuse contact for '193.224.76.0 - 193.224.76.255' is 'abuse@iif.hu'”

Melléklet tartalmazza a táblázatokat:[7],[8],[9]

2.2.4 Email vizsgálat:

A következő lépés, hogy megpróbáljuk analizálni az e-mail címet. A felhasználói név /username/ elárulhat bizonyos dolgokat az áldozatról. (pl név, becenév születési idő, kedvenc hobby, és sok minden más is egyaránt) Az, hogy mit választ valaki /nick/ névnek egy e-mail címbe (amit minden nap használ) elárul róla számos fontos információt.

Tart-e valamit fontosnak, amit visszatükröz a nevében, van-e valami speciális érdeklődési köre, stb. Az e-mail cím második része (a @ utáni) pedig elárulja, hogy hol van a postafiókja melyik szolgáltatónál. Itt két eset lehetséges: publikus szolgáltató vagy nem publikus (céges) levelező rendszer.[14] Amennyiben publikus szolgáltatóról van szó célszerű nyitni oda egy e-mail fiókot, hogy lássuk azt a felületet, amelyet feltehetően a felhasználó is használ levelezéskor. Megtudhatunk pár dolgot ezzel kapcsolatban. Elérési lehetőségeket (csak webes mail vagy pop3-on⁴, imapon is elérhető) tárhely korlát, kinézet.. Ráadásul itt is működik a "hasonlóság" pszichológiája.

Ha egy freemail-esnek küldünk levelet egy szintén freemail-es címről ezzel máris azt sugalljuk, hogy van bennünk valami közös. Ha más nem, akkor az, hogy a levelező

⁴ Post Office Protocol

szolgáltatónk megegyezik. Ezeket az információkat különböző trükkökkel lehet felhasználni social engineeringben.

Amennyiben a levelezési cím nem publikus - vagyis céges, akkor ezek a mechanizmusok nem használhatóak helyette azt kellene kideríteni, hogy az adott céges levelező milyen alapokon működik (outlook, exchange vagy más gyakori vállalati levelező rendszer) ennek is célszerű utánajárni még az elején. A második része az e-mail címnek azt is elárulja nekünk, hogy hol lehet a levelező szerver. Ha például .com-ra végződik, akkor feltehetően külföldi illetőségű a cég, ha pedig .hu-ra végződik, akkor valószínű, hogy magyar székhelyű céggel van dolgunk. Mivel nem a levelezőszerver a célpont ennek sok jelentősége nincs, de ez is egy részlet, amelyet érdemes tudni. (PL: más törvények vonatkozhatnak egyik, illetve a másik szolgáltatóra, mert más-más országban van a működtető cég székhelye)

- A küldő fél email szerverének címére;
- Azonosító rendszerre;
- Üzenet küldésének idejére;
- Üzenet azonosító kódra;
- A küldő nevére;
- A küldő IP címére;
- A küldést végző eszköz helyére.

2.3 Hálózat teljes körű vizsgálata:

Ezen fejezet taglalja a folyamatok azon részeit, amikhez specifikus programok tulajdonképpen nem is szükségesek. Az Internet lehetőséget ad számunkra, hogy elvégezzük ezek többségét. Ahhoz, hogy bárminemű törési mechanizmus alkalmazzunk, mindenképpen össze kell gyűjtenünk a felhasználható adatokat amelyek alapján el tudjuk kezdeni a folyamatot. Első és legfontosabb információ számunkra a célállomás/kiszolgáló egység IP címe. Ez az azonosító számunkra olyan, mint egy átlag ember számára a lakáskulcsa.[15] Az IP cím megkaparintását követően szinte pillanatok alatt hozzá is férhetünk a fizikai címhez⁵. Miután ezen címek a rendelkezésünkre állnak, számos olyan program létezik amivel tudjuk ellenőrizni a portokat. A portok fontosságáról a későbbiek folyamán bővebb

⁵ Media Acces Controll

információt adok. Amennyiben markunkban vannak a nyitott portok már meg is lehet kezdeni az első lépéseket, hiszen ez az egyik legáltalánosabb hozzáférési út a célszámítógéphez.

2.3.1 IP (Internet-Protocol) címek vizsgálata a hálózaton:

A hálózaton lévő összes eszköz megjelenítésére egy alapvető folyamatot hajtottam végre, ami nem csinál mást csak kilistázza az összes IP címet. Az alapelv, amely alapján ez történik nem sokban különbözik mint a CLI (Command Line Interface)-n keresztül történő „pingelés”. [16] Egy meghatározott méretű adat csomag kiküldésre kerül a hálózaton, hasonlóan mintha egy szórási üzenetet küldene az adott hálózati eszköz, s ez alapján képes felderíteni az összes „live/dead” eszközt az Advanced IP Scanner programcsalád.

A címzés az interneten az IP-címzésen alapul. Az interneten minden erőforrás egy egyértelmű számmal, az IP- címmel érhető el. Az IP-címek kiosztása hierarchikus, ami azt jelenti, hogy egy ügyfél a szolgáltatójától kapja meg a szükséges IP-címet, a szolgáltató megint csak a hálózattól kölcsönzi az IP-címeit, amelyre csatlakozik, miközben a hálózatok üzemeltetői időbeli korlátozás nélkül, blokkokban kölcsönzik IP-címeiket, az IP Numbering Authorities-től. [17] Európában a RIPE (<http://www.ripe.net/>) felelős az IP-címek kiosztásáért. [18]

Hogyan néz ki egy IP-cím? A jelenleg használt IP-protokoll az IPv4. Minden IP-cím 32 bitből áll. Mivel az ilyen számkombinációk igen körülményesek, többnyire a pontozott tizedes írásmódot használják, amelynél a 32 bit 8 bitekre van felosztva, és ezeket decimális számként írják le.

Státusz	Név	IP	Gyártó	MAC Cím
OK	172.25.136.1	172.25.136.1	Aruba Network	00:oB:86:61:A3:D8
OK	172.25.136.2	172.25.136.2	Aruba Network	00:0B:86:6E:AF:D8
OK	172.25.136.25	172.25.136.25	Hon Hai Precision Ind. Co.,Ltd.	E4:D5:3D:60:AD:6F

8.táblázat: IPv4 [10].

Az adott IP címek valóságát a CMD-n keresztül egy ping paranccsal megvizsgáltam így kiderült, hogy élő hálózati azonosítókat derített fel a program. 32bájtnyi adatcsomag küldésével kiderült, hogy van e kommunikáció a hálózaton a számítógépek között.

C:/Users/Admin>ping 172.25.136.91				Samsung Electronic	
172.25.136.91 pingelése - 32 bájtnyi adattal:					
Válasz:	172.25.136.91	bájt=32	idő=173	TTL=64	
Válasz:	172.25.136.91	bájt=32	idő=788	TTL=64	
Válasz:	172.25.136.91	bájt=32	idő=119	TTL=64	
Válasz:	172.25.136.91	bájt=32	idő=900	TTL=64	
	Csomagok:	küldött=4	fogadott=4	elveszett=0	
		o% veszteség			

9.táblázat: PING [11].

A fentebb lévő táblázatból egyértelműen kiderül, hogy a kommunikációs csatorna, tökéletesen/veszteség mentesen működik. Így feltételezhető hogy a hálózaton ilyen jellegű (kommunikációs) akadály nem adódik.

2.3.2 Banner grabbing:

A folyamat során egy webes infrastruktúra felderítését vesszük véghez, ami által hozzáférünk olyan jellegű információkhoz mint például: IP cím a weben, Server típusa, Kódolás. Mindezek között a legfontosabb, hogy megtudhatjuk a nyitott portokon futó folyamatokat is. Ez a későbbiekben nagy segítségünkre lehet.

www.uni-nke.hu	
Initiating server query	
Looking up IP address for domain:	www.uni-nke.hu
The IP address for the domain is:	193.224.76.29
Connecting to the server on standard HTTP port:	80
[Connected] Requesting the server's default page	

10.táblázat: Banner Grabbing [12].

2.3.3 Portok vizsgálata:

A portok hálózati kommunikációt szolgálnak. A protokollokkal együtt települnek és ezeken be is lehet "hatolni. A Portok felderítéséből tudunk következtetni arra, azaz pontosabban fogalmazva egy automatizált folyamat következtében kiderülnek, hogy milyen szolgáltatások is futnak az adott szerveren (hálózaton) avagy csak egy egyszerű felhasználói számítógépen.[19]

A portok vizsgálata előtt érdemes egy ping tesztet végrehajtani, ami tulajdonképpen nem más mint egy előre beállított méretű adat csomag küldése. Ezt nevezik pingelési fázisnak. A folyamat akkor helyes, ha ennek végeredménye a pong fázis, azaz hogy a végpont válaszol a kérésre azaz visszaküldi a csomagot a feladó egységnek.

Ezt követően véleményem szerint feltétlenül meg kell ejteni egy traceroute parancsot, ami pedig kilistázza számunkra a kezdő illetve végpont között állomásozó összes hálózati eszközt. Legyen az HUB, SWITCH, ROUTER...

Rendszerint a portscan következtében az adott host-on futó alkalmazás/szolgáltatás verzió számát is megkapjuk, amiből már egész egyszerűen tudunk következtetni a lehetséges operációs rendszerre is.

Process Name	Process ID	Protocol	Local Port	Local Address
HideMyIpSrv.exe	5072	TCP	51535	127.0.0.1
javaw.exe	1360	TCP	1196	172.25.138.209
javaw.exe	1360	TCP	1198	172.25.138.209
macromedia.exe	4824	TCP	12584	172.25.138.209
SecurityManagerPlus.exe	2856	TCP	12594	127.0.0.1

11.táblázat: Protocol&Port lista [13].

A számítógépek/végpontok a hálózaton keresztül a Portok biztosítják a megfelelő kommunikációt. Amikor egy felhasználó csatlakozik egy klienshez/weboldalhoz, avagy csupán üzemel a számítógépe és kapcsolódik az internethez/hálózathoz, kinyílnak a portok. Minden portnak meg van a maga szerepe. Fontos tudni, hogy ha kifelé van adat áramlás, akkor ez jelenti azt is hogy befele is történik adatfolyam. A portok vizsgálata megadja számunkra, hogy hol lehetséges a betörés az adott számítógépbe. Ezek védelme s a portok

mögött lévő eszközök naprakészen tartása prioritást élvez, hiszen az egyik legveszélyesebb pontról beszélünk.

2.3.4 Reguláris Port vizsgálat:

- Nyitott vagy elfogadott: a host egy választ küldött, jelezve ezzel, hogy egy szolgáltatás hallgatja a portot.
- Zárt vagy nem engedélyezett vagy nem hallgató: a host küldött egy üzenetet, ezzel jelezve, hogy a kapcsolatokat elutasítja (nem engedélyezi) ezen a porton. /pl.: tűzfalból reject, azaz egy TCP RST-vel⁶ válaszol/
- Szűrt vagy blokkolt: nem volt válasz a hosttól. (filtered – a port egyáltalán nem válaszol /pl.: tűzfalból drop/) (wrapped – a port nyitva van, de a mögötte levő alkalmazás zárja be a portot /pl.: /etc/hosts.deny miatt/)

A nyitott portok két sebezhetőséget jelentenek, amikkel óvatosságnak kell lenniük az adminisztrátoroknak:

- biztonsági és stabilitási aggodalmak a program megbízhatóságával kapcsolatban, hogy azokat a szolgáltatásokat nyújtsa.
- biztonsági és stabilitási aggodalmak az operációs rendszerrel kapcsolatban, ami a hoston fut.

A zárt portok csak a másodikként említett hozhatók kapcsolatba a két nyitott portokra vonatkozó sebezhetőségek közül.

A blokkolt portok pedig semmilyen sebezhetőséget nem jelentenek. Habár megvan az esélye annak is, hogy nincs semmilyen ismert sebezhetőség sem a szoftverben, sem az operációs rendszerben abban a pillanatban.

Nmap scan report for INFOSZCS_221_02.connectify (192.168.135.1) Host alive (0.031s latency). Not shown: 996 filtered ports
--

⁶ Transmission Control Protocol Reset

PORT	STATE	SERVICE
• 53/tcp	open	domain
• 139/tcp	open	netbios-ssn
• 445/tcp	open	microsoft-ds
• 6789/tcp	open	ibm-db2-admin
MAC Cím : 02:87:40:92:51:BE (Unknown)		

12.táblázat: Reguláris Portvizsgálat [14]

A portszkennelést azok is tudják használni, akik a biztonságot szándékoznak veszélyeztetni. Sok lehetőség van a portszkenben arra, hogy nyitott portokat találjunk, amin nagy mennyiségű adatot küldve megpróbálhatjuk kiváltani azt az állapotot, amit úgy hívnak, hogy puffertúlsordulás (angolul buffer overflow). Az ilyen magatartás veszélyeztetheti a hálózat biztonságát és a benne lévő számítógépeket is, ahhoz vezetve ezzel, hogy érzékeny információkat veszítsünk el, vagy fedjünk fel, valamint hogy dolgozhassunk.

Nmap scan report for AsusX54H.connectify (192.168.135.51)		
Host is up (0.0075s latency).		
Not shown: 993 filtered ports		
PORT	STATE	SERVICE
• 135/tcp	open	msrpc
• 139/tcp	open	netbios-ssn
• 445/tcp	open	microsoft-ds
• 554/tcp	open	rtsp
• 2869/tcp	open	icslap
• 5357/tcp	open	wsdapi
• 10243/tcp	open	unknown
MAC Address: 60:D8:19:07:20:59 (Hon Hai Precision Ind. Co.)		

13.táblázat: Reguláris Portvizsgálat [15].

2.3.5 Ping Scan & Traceroute:

Starting Nmap 6.47 (<http://nmap.org>) at 2014-10-29 19:09 Közép-európai téli idő

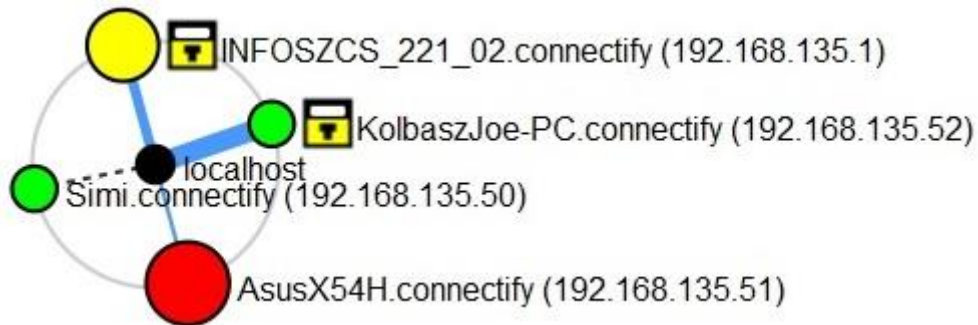
Nmap scan report for SzaboDaniel2.kollegium.hhk.uni-nke.hu (172.23.14.73)

Host is up (0.0010s latency).

MAC Address: BC:AE:C5:67:75:25 (Asustek Computer)

Nmap done: 1 IP address (1 host up) scanned in 4.47 seconds

13.táblázat: Ping Scann&Traceroute [15]



2.ábra (Simon Zoltán)

2.3.6 Intense Scan plus UDP:

Az UDP⁷ portok vizsgálata azért fontos számunkra egy hálózat elemzésénél, mert ez az internet egyik alap protokolljának az egyike. Tulajdonképpen nem szolgál másra, mint a datagram alapú szolgáltatások biztosítására, azaz rövid s gyors üzenetek küldésére használjuk. Legnagyobb hátránya, hogy nem megbízható tehát nem garantálja az üzenet (csomag) célba érkezését. (A DNS⁸ is egy ilyen szolgáltatás)

Az UDP kommunikáció az UDP portokon keresztül zajlik. Minden porthoz tartozik egy várólista. Ide gyűlnek a bejövő adatok és a programok ezt a listát figyelik. Ennek következtében lehetőség nyílik egy alkalmazás számára egy időben több információ eljuttatására. Minden olyan port szám ami 1024 alatt van előre definiált adatforgalmat bonyolít le. Az útválasztók rendszerint úgy vannak konfigurálva, hogy UDP forgalmat nem engednek át, ebből kifolyólag csupán alhálózaton belüli adatküldést lehet velük végrehajtani.

- Az UDP-t a Windows rendszerint a hálózatos bejelentkezésnél, névfeloldásnál és a hálózati tallózás szolgáltatásnál használja. Legismertebb szolgáltatás ami UDP-t

⁷ User Datagram Protocol

⁸ Domain Name System

használ az az SNMP hálózatfigyelő rendszer. Az UDP alkalmazásának legfőbb indoka, hogy kisebb helyigénnyel tárolja az adatokat, mint a TCP

Az UDP Portok vizsgálata egyszerűségükből fakadóan sokkalta bonyolultabban lehet ellenőrizni/szkennelni. Mindezek ellenére a hostok többsége küld számunkra egy ICMP PORT UNREACH hibát, amennyiben csomagot küldünk arra a portra. Ebből arra tudunk következtetni, hogy melyik port nincs nyitva. Ahonnan nem kapunk válasz üzenetet értelem szerűen /open/ fázisban van. Mint ahogy azt már korábban említettem az UDP nem képes garanciát vállalni a csomagok kézbesítésére, így nekünk kell odafigyelni az újraküldések beépítésére, hogy ki tudjuk szűrni a megfelelő portokat.

Host is up (0.0082s latency).

Not shown: 998 open|filtered ports, 993 filtered ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

- | | | | |
|------------|------|-------------|---|
| • 135/tcp | open | msrpc | Microsoft Windows RPC |
| • 139/tcp | open | netbios-ssn | |
| • 445/tcp | open | netbios-ssn | |
| • 554/tcp | open | rtsp? | |
| • 2869/tcp | open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |
| • 5357/tcp | open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |

http-methods: No Allow or Public header in OPTIONS response (status code 503)

http-title: Service Unavailable

- | | | | |
|-------------|------|------|---|
| • 10243/tcp | open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |
|-------------|------|------|---|

http-methods: No Allow or Public header in OPTIONS response (status code 404)

http-title: Not Found

- | | | | |
|------------|------|------------|--|
| • 137/udp | open | netbios-ns | Microsoft Windows netbios-ssn (workgroup: WORKGROUP) |
| • 1900/udp | open | upnp? | |

14.táblázat: UDP Scann [16]

TCP/UDP portok ellenőrzésére alkalmas programok:

- Nmap Security Scanner
- Free Port Scanner
- Advanced IP Scanner

- Angry IP Scanner
- Zone Alarm

Lehetőségünk van online port vizsgálat elvégzésére is webes felületen keresztül:

- Gibson Research Corporation

A vizsgálat során lezajlottak különféle eljárások. ARP⁹ Ping vizsgálat, Párhuzamos DNS vizsgálat illetve egy Script alapú vizsgálat. Ezek összessége adja azon információkat, amelyekre mi valójában kíváncsiak voltunk. Egyértelműen megjelennek számunkra a nyitott portok (139,445,554,135,5357,10243,2869).

A Script alapú vizsgálat kiadja számunkra a számítógép típusszámát, illetve a rajta futó operációs rendszert. Meghatározásra került a háttérben futó szerver típusa, MAC címe, a hálózati kártya gyártójának nevével. Ami azért nagy előny, mert így máris lehet keresgélni az Interneten található sebezhetőségek között. A hálózaton belüli távolságra is fény derül, amiből ki tudjuk következtetni a kezdő illetve cél állomás közötti egyéb hálózati eszközöket. Végül de nem utolsó sorban, megkapjuk az autentikációs szintet.

2.3.7 Vizsgálatok összegzése:

Mint az a vizsgálatokból kiderül, sikerült számunkra az összes olyan információ megszerzése amikből már képesek vagyunk egy további fejezet megkezdésének.

A rendszereken futó szolgáltatások és alkalmazások jelentik a legnagyobb sebezhetőségek egyikét a védelemnek. Minden scannelésnek a lehető legprecízebbnek kell lenni, s nagyon fontos, hogy minden apró részletre odafigyeljünk. Sok időt meg tudunk azzal spórolni a vizsgálat megkezdése előtt ha kellő precizitással tudjuk definiálni a tartományokat, és magát a vizsgálatot is tudatosan végezzük.

Véleményem szerint célszerű elsősorban az alacsony port számokat megvizsgálni, mivel úgy gondolom, hogy ott futhatnak számunkra érdekes dolgok. Amennyiben nem találunk semmi felhasználható lehetőséget, érdemes az UDP vizsgálatokat megcsinálni a magasabb port számokon. Érdemesnek tartom azt a minimális erőfeszítést megtenni, hogy biztosak legyünk a dolgokban, amikor ugyanis elvégzünk egy Ping Scannelést. Ezzel

⁹ Address Resolution Protocol

meggyőződven arról hogy a csomagok kellő képen elérték e az általunk definiált IP¹⁰ címet, Domain címet.

Ezek után képesek vagyunk a következő lépésnek nekiállni, ahol a sebezhetőségeket derítjük fel, összegezzük és tervezzük meg a további folyamatokat. A továbbiakban szemléltetni fogom az előbb említett sebezhetőségeket, és az ezekből fakadó problémákat.

2.4. Hálózati Sebezhetőség vizsgálata:

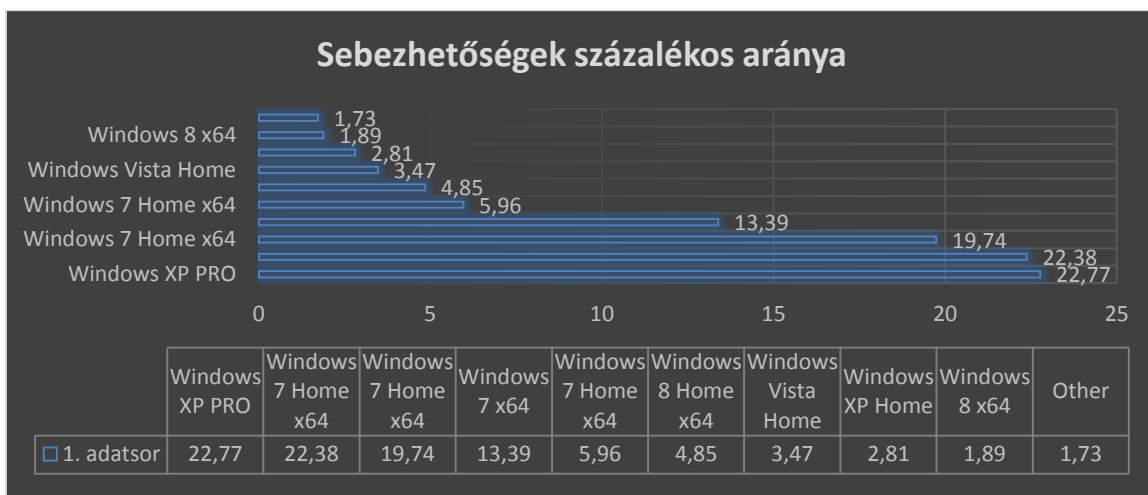
2.4.1 A Sebezhetőség:

Szoftverhiba, amely az egyébként érvényes szabályok kikerülésével teszi lehetővé műveletek végrehajtását, vagy adatokhoz történő hozzáférést. A sebezhetőséget a hátsó kapuval szemben a szoftverekben nem szándékosan hozzák létre, hanem a fejlesztők figyelmetlenségének köszönhetően kerülnek a programokba.[20],[21] A sebezhetőségek által nyitott biztonsági rések javítására a fejlesztők foltokat adnak ki.

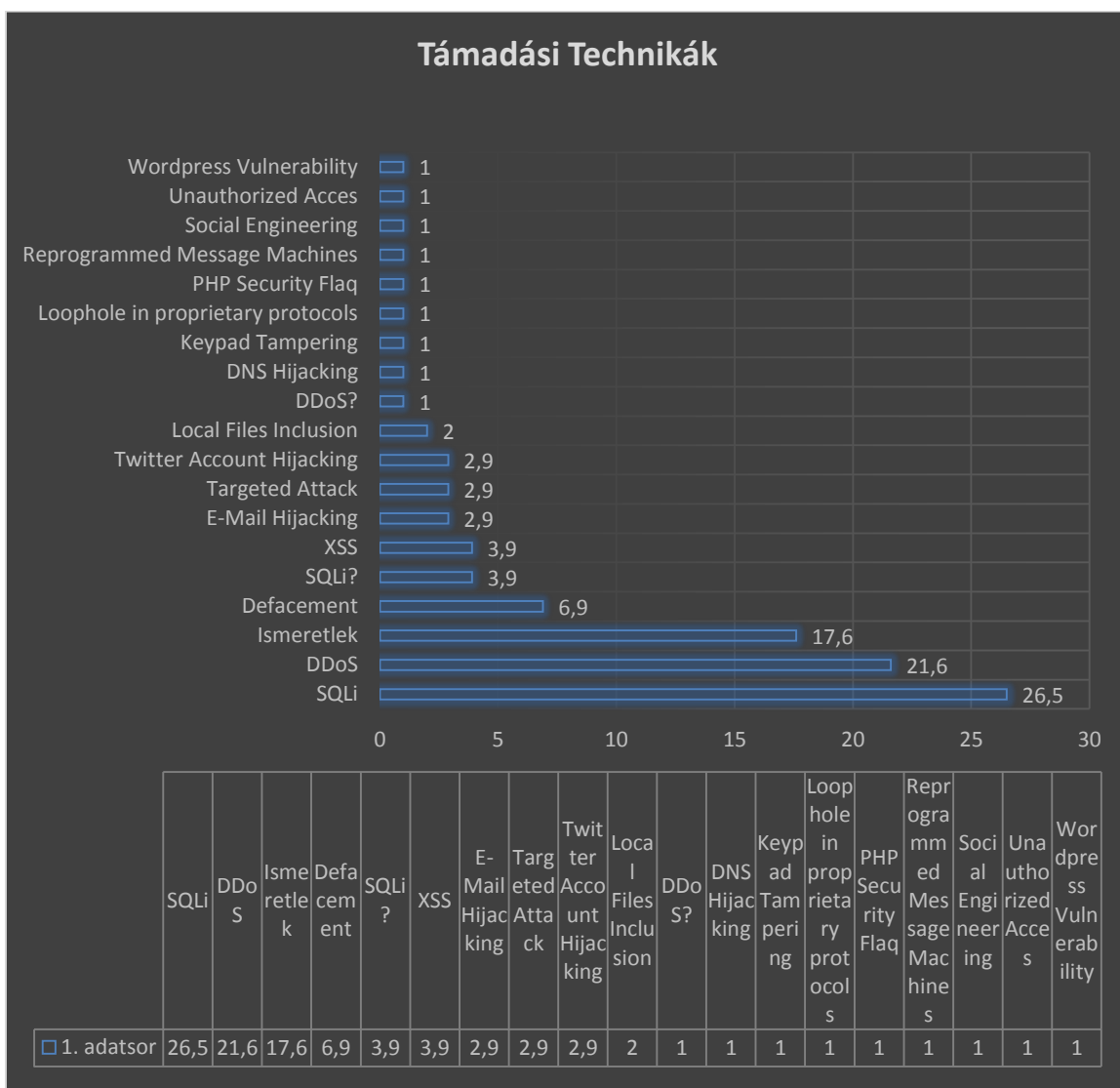
2.4.1.1Helyi támadás: Az áldozatul kiszemelt gépen futó program segítségével indított támadás. A helyi támadások kivitelezéséhez a támadónak fizikai hozzáféréssel kell rendelkeznie a megtámadni kívánt géphez, vagy egy távoli exploit segítségével programok helyben történő futtatására kell jogosultságot és lehetőséget szereznie.

2.4.1.2Távoli támadás: Az áldozatul kiszemelt gép ellen távolról (hálózaton keresztül) indított támadás. A távoli támadások a helyi támadásoknál általában kedvezőbb módszerek a hackerek körében, mert nem igényelnek programok helyi futtatására lehetőséget adó jogosultságokat a megtámadott gépen, és így általában a támadó identitásának lekövetését is erősen megnehezítik.

¹⁰ Internet Protocol



15.táblázat: Sebezhetőségek [17]



16.táblázat: Támadások [17]

2.5. Információ Lopás a hálózati elemektől:

Megszámolni sem lehet, hogy hány különféle információ lopási mechanizmus létezik, amit hálózatokon/interneten keresztül végre lehet hajtani. A Következőkben az általam kipróbált, s szegmentált lehetőségeket mutatom be, melyek a véleményem szerint a legjobban hatnak a célközönségre.

2.5.1 Sniffing/Metasploit:

Számomra a legkedveltebb információ szerzési mechanizmus (felhasználónevek/email címek) eltulajdonítására, amelyhez különösképpen hálózati hozzáférés sem szükséges a célpont gépéhez a „metasplotable” elveken alapuló /sniffer/ módszer.[22]

Az alapja az egész folyamatnak a felhasználó becsapása egy hamis weboldallal. Ez az egész tulajdonképpen nem más, mint egy klón oldal készítése, ami mögött fut egy alternatív server, ahova ugyanis az információt a felhasználó elküldi nekünk. Természetesen mindez az ő tudatán kívül történik. Amennyiben megnyitja az általunk készített hivatkozást, s beírja az ő személyes adatait, a küldés/bejelentkezés gombbal aktiválásra kerül, s mi azonnal megkapjuk azt a csomagot, amely tartalmazza a bevitt karaktereket. A weboldal másolata egy az egyben ugyan az, mint az eredeti, hiszen egy jelen idejű képet csinál számunkra a „metahacker”. Személy szerint két alternatív megoldást alkalmaztam a továbbiakban:

1. A felhasználó szembesül azzal, hogy hibásan írta be a jelszót, de mindeközben a frissített oldal, már az eredeti URL-en érhető el, nem pedig az általunk megadott IP címen.
2. Kettős átirányítást alkalmaztam, amely során a hibaüzenet sem jelent meg, hiszen az információ egy azon időn belül két különböző csatornán került továbbításra. Egyik az eredeti URL-cím, másik pedig természetesen az általunk definiált cím.

A folyamat során a legnagyobb veszélyforrás, hogy felfedjük szándékunkat abban rejlik, ha a felhasználó tudatos internet használó s mielőtt bármit is tenne rátekint a böngészőben az URL sorra. Jelen tudomásom szerint még nincs rá semmilyen metodika sem, amely képes lenne a lefedettséget ott is biztosítani.

A folyamat összegzése:

1. Közösségi oldal/Email kliens ellen történő támadás
2. Weboldal elleni vektor készítése
3. Java alapú applikáción keresztül történő hozzáférés
4. Weboldal klón készítése/Template készítése
5. Klónozendó oldal URL-jének meghatározása
6. Saját IP címünk definiálása
7. Snifferelés megkezdése

A végeredmény számunkra, vagy a futó folyamat közben kerül kiírásra, vagy pedig a Rendszer főkönyvtárán belül található „var” mappának a „www” al mappáján belül lévő html-fileban.[23]

2.5.2 Legfőbb Webes hibák:

- Cross Site Scripting (XSS)
- Beszúrásos hibák (pl. SQL injection)
- Kártékony fájlvégrehajtás (pl. fájlfeltöltés)
- Nem biztonságos direkt referencia (pl. direkt fájlhivatkozás)
- Cross Site Request Forgery (CSRF)
- Információszivárgás és nem megfelelő hibakezelés (pl. beszédes hibaüzenetek)
- Feltört hitelesítés és session kezelés (pl. megjósolható session azonosítók)
- Nem megfelelő kriptográfia a tárolásnál (pl. XOR¹¹ használat)
- Nem biztonságos kommunikáció (pl. gyenge SSL)
- Az URL hozzáférés tiltásának a hibája (pl. olyan fájlok, könyvtárak felderítése, melyeket nem lehetne látni – directory traversal)

¹¹ XOR – Logikai Kapu

2.5.3 Keyloggerrel végzett információ lopás:

A keyloggerek a kezdetektől fogva léteznek az informatika világában. Korai időkben legfőképpen hardware-es keyloggereket alkalmaztak a hackerek, hiszen ez jelentősen egyszerűbb volt, mint a számítógép rendszerébe implementált változat. Napjainkra oda jutott ezen ágazat, hogy képes akármilyen jellegű rádiójellel közvetíteni az információt a billentyűzet illetve a vizsgálatot folytató személy között. Én személy szerint a software-es keyloggerek alkalmazását szeretném bemutatni, mert úgy gondolom, hogy ez az egyik leggyakoribb formulája az információ szerzésnek.

Olyannyira kinőtték magukat az ilyen stílusú programok, hogy mára már nem csak a billentyűzet leütéseket képes figyelni, hanem az általunk megszabott időközönként képes képernyőképet is küldeni az általunk definiált módon. (Egy virtuális szerveren azonnali kapcsolattal is lehetséges, emailen keresztül egyaránt.)

Legnagyobb előnye hogy képesek rejtett üzemmódban működni, ami a kevésbé hozzáértő emberek számára jelent főként kockázatot, hiszen nem nézik naponta a Program Fájl mappa teljes tartalmát. A programcsalád gyengepontja, hogy megjelenik a Program Filesban, amennyiben nem „rootkit „módban futtatjuk.

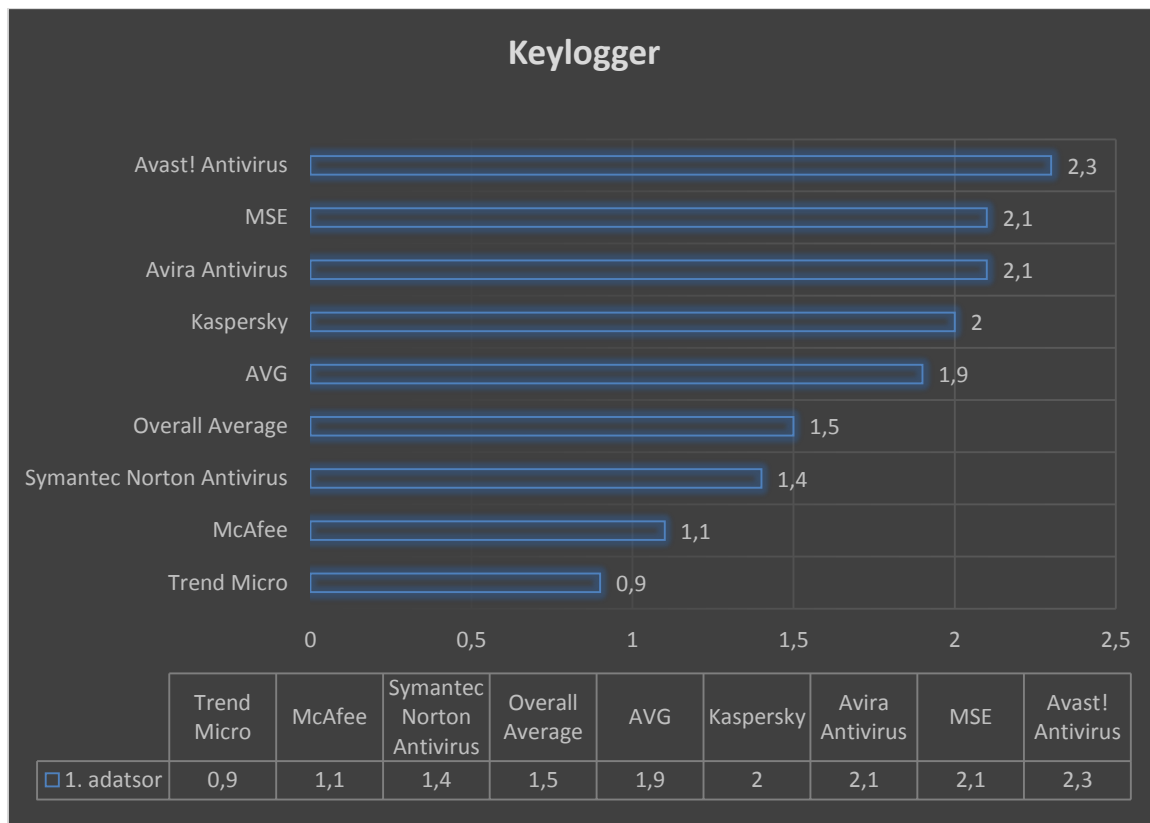
Az interneten annyi változata fellelhető a keyloggereknek, hogy már szinte Dunát lehetne belőlük rekeszteni. Véleményem szerint nem szükséges részletesen taglalni a különböző programok működési elvét hiszen szinte mindegyik ugyan azon a metodikán üzemelnek, néhány extra kiegészítéssel.

Első körben definiálnunk kell a saját paramétereinket, ahova az információkat várjuk. Itt szerintem célszerű SMTP szervert beállítani, hogy emailen keresztül tudjuk az információkat megkapni. Miután meghatároztuk a cél címet, alkalmunk nyílik meghatározni azt, hogy honnan s miből is szerezzünk információt. Fontos beállítási rész, az automatikus indítás lehetőség. Számunkra ez azért szükséges, mert így nem szükséges az állandó figyelem, hogy mikor is fusson a kártevőnk, hanem ahogy a felhasználó igénybe veszi a számítógépet azonnal elindul a háttérben a keyloggerük.

Számos információt megkapunk a cél számítógépről, amiket a későbbiekben felhasználhatunk ellene. Gondolok itt az operációs rendszerre, böngészőre, böngésző

verziószámára. Lehetőségünk adódik a kódok összekevertetésére. Ez miért is fontos számunkra ? A vírus irtó cégek nagyobb figyelmet fektetnek az ilyen jellegű támadásokra így a védelmi software-jeik érzékenyebbek a keyloggerekre. A Kódok összekeverésével nehezebben jön rá, hogy mi is zajlik valójában a rendszerben.[24]

Másik érdekleges funkciónak tartom a párhuzamos programfuttatási lehetőséget. Ezalatt azt értem, hogy képesek vagyunk távoli kontaktban más programokat egy időben futtatni a mi kártevőnkkel. A keyloggerek ellen a védekezés legfőbb szegmense az nem más mint a tudatos internet felhasználás. Minimális odafigyelést igényel, hogy szokatlan, kéretlen hivatkozásokat nem nyitunk meg, s odafigyelünk a böngészőnk URL sávjának tartalmára.



17.táblázat: Keylogger [18]

A fentebbi táblázat azon kutatást bizonyítja, hogy melyik vírus védelmi software a legalkalmasabb a keyloggerek elleni védekezésre. Mint látjuk a táblázat is jól mutatja, hogy a Trend Micro terméke győzött, hiszen azon számítógépeken amelyeken ez a program szerepelt, csupán 0,9%-án sikerült keyloggert futtatnunk. A kutatásnak 100 számítógépet vetettek alá.

2.6 Statisztikák a felhasználóról:

Kutatásom során felmértem azt, hogy mik a felhasználók által leggyakrabban használt operációs rendszerek, illetve védelemre orientált program családok. A felmérést közösségi fórumokon keresztül végeztem el. A felmérést 288 hallgató társam töltötte ki, s az eredmény az alábbi táblázatban lett összesítve.

Windows 8.1:	38
Windows 8:	12
Windows 7:	183
Windows Vista:	7
Windows XP:	25
MAC:	4
Linux/Unix:	2
Egyéb:	17

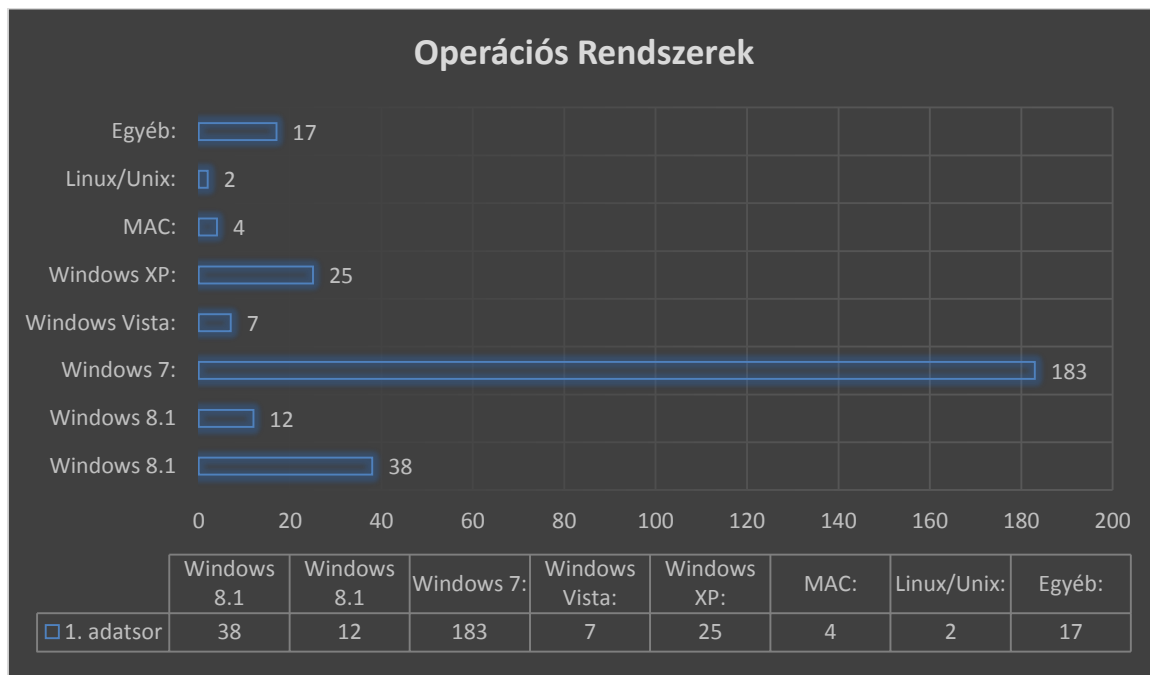
18.táblázat: Rendszer [19]

A biztonsági programokra is kiterjedt a közvélemény kutatásom, amely során kiderült hogy többnyire a felhasználók a legközkedveltebb termékcsaládokat alkalmazzák. Az AVAST, NOD32, NORTON Antivírus napjaink piacvezető programjai, amelyek kellő biztonságot adnak a felhasználók számára.

Avast	67
Everest	21
ESET NOD32	40
Panda	9
Norton Antivirus	55
Avira Free Antivirus	2
AVG-Antivirus	43
Microsoft Security Essentials	44
Nem alkalmaz védelmi software-t	7

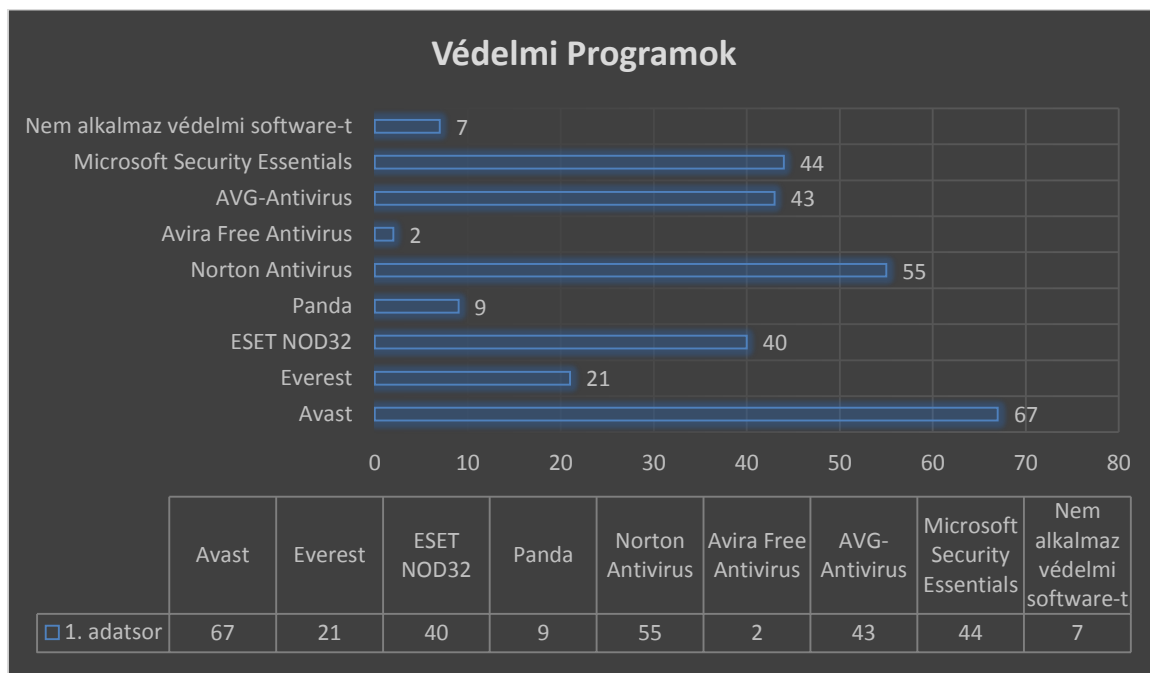
19.táblázat: Antivirus [20]

8.1 Operációs Rendszerek:



20.táblázat: Rendszer [21]

8.2 Védelmi Szoftverek:



21.táblázat: Antivirus [22]

3. TUDATOSSÁG MINT VÉDELMI ESZKÖZ:

A kiber tér bővülésével mint azt korábban is említettem nőtt a digitális bűncselekmények száma. Ennek következtében előtérbe került a kiber biztonság kérdése is. Mint tudjuk az emberi tényező jelenti a legnagyobb kockázatot egy adott rendszer védelmét tekintve. A hibák többsége szándékon kívüli, a tudatlanságból avagy az információ hiányából, fegyelemhiányból fakad. A szánt szándékkal történő károkozás kifejezetten ritka, ellenben hatalmas károkat képes okozni. Éppúgy vizsgálhatjuk a szituációt a szándékosság oldaláról mint a szándékon kívüli károkozás oldaláról, egy dolog teljesen biztos, hogy kiemelkedő mértékű kockázattal kell számolni a személyes védelem szempontjából. Mindezek következtében gondolom azt, hogy a felhasználókra fordítandó biztonságtudatosságra sokkal nagyobb figyelmet kellene szentelni. Mire is gondolok valójában ?

Megtanítani a felhasználókat olyan alap tevékenységi formákra, amik megkönnyítik mind a rendszerért felelős személyek munkáját, mind pedig a sajátjukat. [25]

Egy olyan tematika kialakítását tartom szükségesnek, ahol nem csupán a számítógépen végzett munkát tenné biztonságosabbá, hanem a mindennapi életben is alkalmazni tudná a felhasználó az elsajátított tudást. Véleményem szerint két nagy részre kell szétbontani egy ilyen felkészítést, mégpedig egy számítógépes biztonsági szegmensre illetve egy Social Engineering általános ismertetésre.

Mint azt már említettem, sokszor olyan információkat árul el a felhasználó, amire nem is gondolna, hogy ebből kár keletkezhet. Amennyiben képesek lennének elsajátítani azt, hogy ne egyénként gondolkodjanak, hanem rendszerszinten, megfelelő rendszerszemléleti tudással, egyszerűbbnek bizonyulna a tudatosság integrálása a mindennapokba. Alapkőnek tekintheti Kevin Mitnick¹² A megtévesztés művészete könyv, amely részletesen taglalja a verbális információ lopást.

Nagy hangsúlyt kell fektetni a böngészők megfelelő használatára. Az URL sáv fontosságára, a kéretlen hivatkozások jellegére. Tanulható folyamatok közé tartozik a nem informatikai beállítottságú személyek számára is hogy mikor nem szabad megtenni azt a bizonyos kattintást. A nem megszokott címekről érkező üzenetek kiszűrését ugyan nagy

¹² Kevin Mitnick – Legnagyobb Hacker Legenda

részben elvégzik a megfelelő szűrő programok, de mindig akad olyan, ami átszökik a védelmen. Tudjuk, hogy a hackerek szempontjából pont az az egy pont kell.

A mobil eszközök terjedése újabb nehézséget okoz a biztonsági szakembereknek, hiszen ezzel párhuzamosan számos mobil eszközre készült vírus került napvilágra.

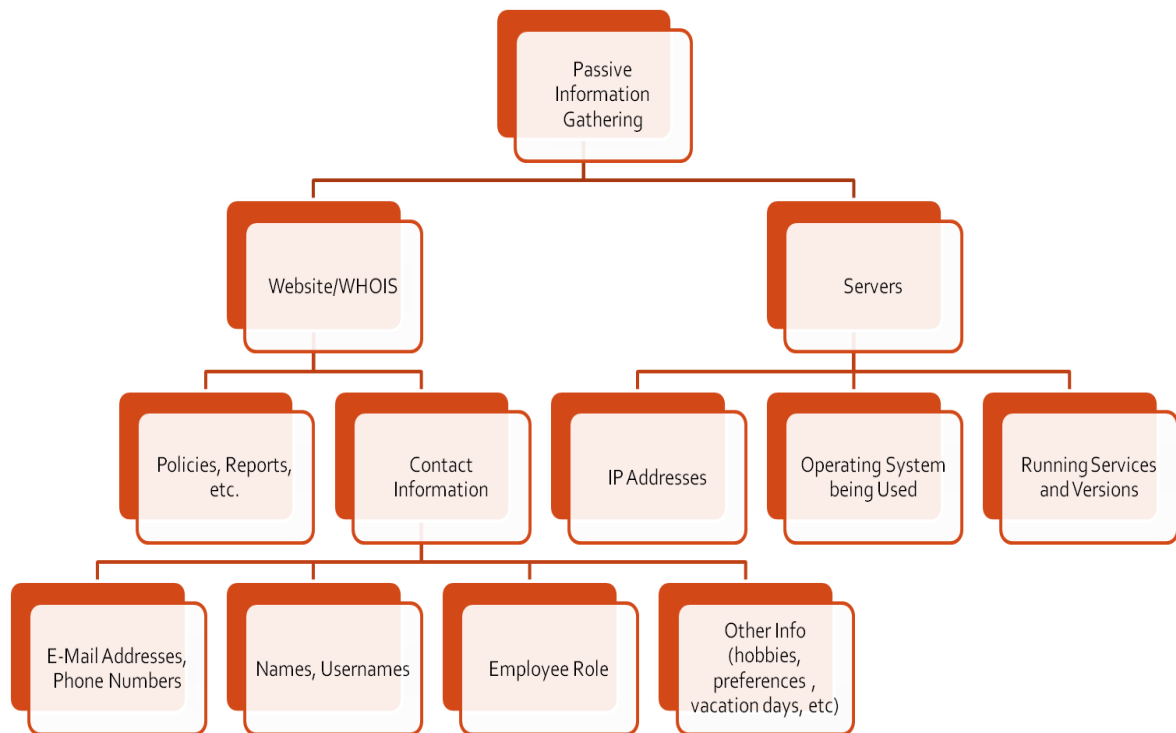
A technikai eszközök fejlődése magával vonzotta az ezeken megjelenő platformok sokaságát. Ennek következtében a közösségi hálók globális szintre nőttek ki magukat. A közösségi hálók az információ éhes hackerek Mekkája. Az emberek rendszerint olyan információkat osztanak meg, amiknek kifejezetten nagy értéke van a kártevők számára. Sokszor a teljes fedettséget sem lehet elérni, hiszen az élet minden részletét megosztják a felhasználók, s szinte elkerülhetetlen hogy egy-egy képen elő ne forduljon olyan személy, aki nem regisztrált tagja az adatbázisnak.[26],[27]

Ebből kifolyólag gondolom azt, hogy a tudatosságra történő felkészítés nélkülözhetetlen eleme egy jól működő informatikai rendszernek.

A tudatosságra neveléssel szemben nagy figyelmet fordítanék a kellő átvizsgálásra is a bekerülést megelőzően. Mivel a kár okozás esetén számolhatunk azzal is hogy szándékos tettről beszélünk, így kénytelenek vagyunk azt feltételezni, hogy valaki önös érdekből cselekszik.

Saját meglátásom alapján, a kellő figyelem felkeltés mellett szükségesnek bizonyulna egy olyan program kialakítása amely a felhasználót rákényszeríti az odafigyelő magatartás statuálására. Az alap koncepció nem lenne más, mint egy felugró ablakokat illetve funkciókat blokkoló program lenne. Ez lehetővé tenné azt, hogy a felhasználó mindig kapna egy értesítést arról amit a programba integráltak.

Gondolok itt olyan felugró buborékokra, amelyek megjelenítik többször egy böngészés során, hogy figyeljen oda az URL sáv tartalmára. Ne kattintson az oldalakon megjelenő hivatkozásokra, reklámokra átgondolatlanul. Ha mindez működne, a felhasználó is gyorsabban tanulva, hiszen tudjuk, hogy a gyakorlatiasság sokkalta effektívebb mint a nyers tananyag.



3.ábra: Social Engineering [23]

A korlátozások terén pedig azt érteném, amelyeket egy böngészést, levelezést támogató vírusirtó jelenleg is alkalmaz a felhasználóval szemben. A korlátozások mellett mindig feltüntetésre kerülne az, hogy milyen veszélyeket is tartalmazhat az oldal, útvonal, vagy esetleges letöltés. Ebből tanulhatna a felhasználó, s a későbbiekben emlékezne a figyelmeztetésre, így már tudatosan reagálni. A fejlesztést böngészőre telepíthető bővítményként lehetne futtatni, aminek nagy előnye, hogy költséghatékony, kevés helyet foglal, s a rendszer erőforrásainak igénybevétele sem magas.

ÖSSZEFOGLALÁS:

Dolgozatom során bemutattam a kiber hadviselés legfőbb mérföldköveit az ezekből kialakuló legfőbb rendeleteket, szabályzókat. Mint az a dolgozat során is kiderült, hogy ezekre nagyon nagy szükség van, mivel szeretnénk képesek lenni korlátozni a lehetőségeket. A kutatás legfőbb részében bemutattam, hogy miképpen is lehetséges információkat kinyerni egy adott hálózatról. A tesztkörnyezet kialakítását azért tartottam célszerűnek, mert így szemléltetni tudjuk egy nagyobb komplexebb hálózat sebezhetőségét, felderíthetőségét. Továbbgondolva a lehetőségeinket egyértelműen kimondható hogy innen már nem sok kell ahhoz, hogy a behatolás megtörténjen. A behatolást követően alkalmunk nyílna bármilyen kártevő integrálására, vészkijáratok telepítésére, vagy csupán figyelő programok alkalmazására, amelyek naprakész és hiteles információt adnak nekünk a belső folyamatok összességéről.

Napjainkban az Informatikai Biztonság fénykorát éli. A hacker csoportok létszámának gyarapodásával, a kiber hadviselési szabályok létrejöttével és az újdonsült kiber osztagok rendszerbe állításával egy még komplexebb dimenzió elé állunk. Ezek mind arra ösztönöznek engem, hogy személyes kihívásként tekintsek az informatika ezen szakágára.

A hozzám legközelebb álló szegmensét próbáltam meg teljesen lefedni a hackertevékenységnek. Ez nem volt más, mint a hálózat felderítése, feltérképezése. Több szemszögből is megvizsgáltam a hálózatot, s leszűrtem a kellő konzekvenciát. Egy rövid fejezetben bemutattam azokat a folyamatokat, amelyekkel a legegyszerűbb módon képes bárki hozzáférni felhasználó nevekhez, jelszavakhoz.

A sebezhetőségek kiértékelését követően egy egyértelmű táblázat keretein belül összevetésre került az általam alkalmazott törési mechanizmusok sikere a világszinten vett statisztikákkal.

Kifejezetten fontosnak tartottam a felhasználók megfelelő szintű felkészítését a tudatos Internet használatra, amely alatt természetesen a munkahelyi hálózaton történő magaviseletet is beleérttem. Ami egy laikusnak csupán egy számösszetétel az egy szakmabeli ember számára a jogosítvány a bejutáshoz. Véleményem szerint mindaddig, amíg az

alkalmazói szféra nincs kellően tájékoztatva illetve nem érzik a dolgok súlyát, rendkívül nehéz dolga lesz az informatikai szakembereknek is. Mint tudjuk egy rendszer leggyengébb pontja mindig az ember aki a számítógép előtt ül.

A Social Engineering megjelenésével is csak az bizonyítható hogy rohamos tempóban fejlődik az új hadviselési formula, ahol a káosz kialakulását véleményem szerint nem lehet elkerülni. A legfőbb probléma ezzel, hogy a káosz sokak számára eszköz, és lehetőség egyaránt. Ezt kihasználva szinte nyomon követhetetlen egy adott folyamat. Social Engineering ellen védekezni az egyik legnehezebb s legösszetettebb dolog manapság. Meggyőződésem, hogy sokkal nagyobb hangsúlyt kellene erre a területre fektetni, mint amit a jelenlegi vállalati stratégiák prezentálnak.

Amennyiben követjük azt az alapelvet, hogy ez számunkra egy kihívás akkor mondhatni ez a legérdekesebb szakterület, ami csak létezik. Nem elég tudni az informatikai alapokat, s nem elég jónak lenni egy-egy szakterületen. A naprakészség és az információ éhség nélkülözhetetlen modulja a mindennapi életben mindazon személyek számára, akik elhivatottan szeretnék a biztonságot megteremteni s fenntartani. Nem szabad megfélekednünk arról, hogy tökéletes biztonság nem létezik, de kemény munkával fent lehet tartani egy megfelelőnek bizonyuló szintet.

FELHASZNÁLT IRODALOM

- [1]Vangie Beal- Cloud Storage http://www.webopedia.com/TERM/C/cloud_storage.html
2014
- [2]Phant0m - Hackers' Guide - Volume 1
- [3]Phant0m - Hackers' Guide - Volume 2
- [4]Muha Lajos Alezredes - Informatikai Biztonság Jegyzet
- [5]Cameron Stevens – Casualties of Cyber Warfare
<http://thediplomat.com/2014/08/casualties-of-cyber-warfare/>
- [6]Muha Lajos – Szabványok és ajánlások az informatikai biztonság területén –
HACKTIVITY – 2013
- [7]McClure, Scambray, Kurtz: Hacking Exposed – Fifth Edition
- [8] Allen harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams
- Gray Hat Hacking Third Edition
- [9]Keller Tamás – A Hacker Etika
- [10]Phant0m - Hackers' Guide - Volume 3
- [11]Kevin Mitnick – A megtévesztés Művészete - 2003
- [12] McClure, Scambray, Kurtz: Hacking Exposed – Fifth Edition
- [13]<https://www.google.com/maps/views/streetview?gl=us>
- [14]Topp Gergely – Elektronikus Levelezés
<http://www.incedy.hu/~szikszai/foisk/emeil.pdf> -2008
- [15]Gordon Lyon - Nmap Network Scanning
- [16]Laura Chappell - Wireshark Network Analysis Second Edition
- [17] Topp Gergely – Informatikai hálózatok http://www.bbap-vasvar.sulinet.hu/iskola/kiegeszitesek/informatika/hlzatok_eszkzk.html - 2008
- [18]<http://www.internetassignednumbersauthority.org/>
- [19]Othmar Kyas - Számítógép Hálózatok Biztonságtechnikája
- [20] Tóth Gergely, Hornák Zoltán - Számítógépes rendszerek sebezhetőségének
- [21]David Kennedy, Jim O’Gorman, Devon Kearns, Mari Aharoni - Metasploit – The Penetration Tester’s Guide

[22]<https://community.rapid7.com/docs/DOC-1875>

[23] McClure - No Starch Metasploit 2011

[24]Microsoft Developer – Hogyan biztosíthatom a számítógép vírusok elleni védetségét ?
<http://windows.microsoft.com/hu-hu/windows/how-protect-computer-from-viruses#how-protect-computer-from-viruses=windows-7>

[25]<http://www.social-engineer.org/>

[26]Kovács Zoltán - Hordozható Infokommunikációs Eszközök Használatához
Kapocsódó Biztonságtudatossági Képzési Tematika Védett Vezetők Számára – 2014

[27] Krasznay Csaba – Open Academy - 2012

ÁBRA ÉS TÁBLÁZAT JEGYZÉK

[1] idézet – Muha Lajos -Szabványok és ajánlások az informatikai biztonság területén - 2013

[2] ábra - The Dawn of Cyber Warfare

Forrás: <http://malwarelife.blogspot.hu/2010/06/dawn-of-cyber-warfare.html>

[3] táblázat: Hálózati információk

Forrás: CEH Ehical Hacking Learning Guide v8

[4] táblázat: Rendszer információk

Forrás: CEH Ehical Hacking Learning Guide v8

[5] táblázat: Szervezeti információk

Forrás: CEH Ehical Hacking Learning Guide v8

[6] táblázat: URL címek

[7], [8], [9] Melléklet tartalmazza a táblázatokat:

[10] táblázat:IPV4

[11] táblázat: PING

[12] táblázat: Banner Grabbing

[13] táblázat: Protocol&Port lista

[14].táblázat: Reguláris Portvizsgálat

[15] táblázat: Reguláris Portvizsgálat

[16] táblázat: Ping Scan&Traceroute

[17] ábra: Advanced IP Scanner (Simon Zoltán)

[18] táblázat: UDP Scan

[19] táblázat: Sebezhetőségek

Forrás: <http://securelist.com/analysis/kaspersky-security-bulletin>

[20] táblázat: Támadások

Forrás: <http://securelist.com/kaspersky>

[21] táblázat: Keylogger

[22].táblázat: Rendszer

[23].táblázat: Antivirus

[23].táblázat: Rendszer

[25].táblázat: Antivirus

[26].ábra: Social Engineering

MELLÉKLET:

Táblázat: Externális & Internális URL-ek

Melléklete: 4.1 Externális & Internális URL-ek

http://hhk.uni-nke.hu
http://hhk.uni-nke.hu/kutatas-es-tudomanyos-elet/eu-palyazatok/kmop-4_2_1-b
http://intranet.uni-nke.hu/
http://ktk.uni-nke.hu
http://kvi.uni-nke.hu
http://ludovika-campus.hu
http://nbi.uni-nke.hu
http://nit.uni-nke.hu
http://nkeszolgaltato.hu/
http://nkeszolgaltato.hu/ertekesitesi-pontok/
http://old.uni-nke.hu
http://otdk2015.uni-nke.hu/
http://rtk.uni-nke.hu
http://uni-nke.hu
http://uni-nke.hu/egyetem/allaspalyazatok
http://uni-nke.hu/egyetem/az-egyetem-vezetese
http://uni-nke.hu/egyetem/egyeb-palyazatok/osztondijak-egyetemi-polgaroknak
http://uni-nke.hu/egyetem/egyuttmukodes/hirek
http://uni-nke.hu/egyetem/elerhetosegek
http://uni-nke.hu/egyetem/kituntetettek/az-egyetem-diszpolgara
http://uni-nke.hu/egyetem/kozerdeku-informaciok/alapito-okirat
http://uni-nke.hu/egyetem/minosegbiztositas
http://uni-nke.hu/egyetem/rektori-koszonto
http://uni-nke.hu/egyetem/sajto/kmr-csoport
http://uni-nke.hu/egyetem/szabalyzatok_-dokumentumok/szervezeti-es-mukodesi-rend
http://uni-nke.hu/egyetem/szenatus/a_szenatus_tagjai
http://uni-nke.hu/egyetem/szervezet

http://uni-nke.hu/hallgatoknak
http://uni-nke.hu/hallgatoknak/diakhitel-kisokos-vegzosoknek
http://uni-nke.hu/hallgatoknak/diakigazolvany-igenyles-utmutato
http://uni-nke.hu/hallgatoknak/egyetemi-emlekguru
http://uni-nke.hu/hallgatoknak/hallgatoi-onkormanyzatok
http://uni-nke.hu/hallgatoknak/kollegium
http://uni-nke.hu/hallgatoknak/munka-es-tuzvedelmi-oktatas
http://uni-nke.hu/hallgatoknak/neptun/neptun-elherhetosegek
http://uni-nke.hu/hallgatoknak/osztondijak/kozzszolgalati-osztondij-2014
http://uni-nke.hu/hallgatoknak/palyazatok/jo-tanulo-jo-sportolo-dij-2014-ben
http://uni-nke.hu/hallgatoknak/szerzodesek/kepzesi-szerzodes
http://uni-nke.hu/hallgatoknak/tanulmanyi-kerelem-mintak

4.táblázat: URL címek [6]

Táblázat: WHOIS Lookup

Melléklete: 4.3 Whois Lookup:

Inetnum	193.224.76.0 - 193.224.76.255
Netname	ZMKA
Description	Zrinyi Miklos Nemzetvedelmi Egyetem Zrinyi Miklos Military Academy Budapest
Country	Hungary
Admin-c	LT11-RIPE
Tech-c	SK35-RIPE
Status	ASSIGNED PA
Remarks	hrcode=81539e0dc
mnt-by	NIIF-MNT
Source	RIPE Filtered

Táblázat: Whois Lookup[7]

Person	Livia Tamaska	Sandor Kubicsko
Address	Zrinyi Miklos Military Academy	Zrinyi Miklos Military Academy
Address	Hungaria krt. 9-11.	Hungaria krt. 9-11.
Address	P.O.B. 15.	P.O.B. 15.
Address	H-1581 Budapest	H-1581 Budapest
Address	Hungary	Hungary
Phone	+36 1 1340740 ext. 1247	+36 1 1340740 ext. 1242
Fax-no	+36 1 1340740 ext. 1246	+36 1 1340163
NIC-hdl	LT11-RIPE	SK35-RIPE
Source	RIPE Filtered	RIPE Filtered

Táblázat: Whois Lookup[8]

route:	193.224.0.0/15
descr:	HBONE/HUNGARNET Block 02
origin:	AS1955
mnt-by:	AS1955-MNT
source:	RIPE Filtered

Táblázat: Whois Lookup[9]

Táblázat: Hagyományos IP címek vizsgálata:

Melléklete: 5.1.2 Hagyományos IP Címek

Státusz	Név	IP	Gyártó	MAC Cím
OK	172.25.136.1	172.25.136.1	Aruba Network	00:0B:86:61:A3:D8
OK	172.25.136.2	172.25.136.2	Aruba Network	00:0B:86:6E:AF:D8
OK	172.25.136.25	172.25.136.25	Hon Hai Precision Ind. Co.,Ltd.	E4:D5:3D:60:AD:6F
DEAD	172.25.136.68	172.25.136.68	Universal Global Scientific	70:F3:95:E2:AD:15
DEAD	172.25.136.79	172.25.136.79	Hon Hai Precision Ind. Co.,Ltd.	60:D8:19:06:FA:CF
OK	172.25.136.83	172.25.136.83	Wistron Neweb Corp.	90:A4:DE:3C:E6:16
DEAD	172.25.136.93	172.25.136.93	Apple, Inc.	0C:74:C2:8B:AD:BD 172.25.136.93
OK	172.25.136.113	172.25.136.113	Apple, Inc.	6C:C2:6B:58:A3:7F
OK	172.25.136.134	172.25.136.134	ASUSTEK COMPUTER INC.	10:BF:48:E8:AD:0B
OK	172.25.136.171	172.25.136.171	Intel Corporate	0C:8B:FD:BB:8E:DD

8.táblázat:IPV4 [10].

Táblázat: Portok Vizsgálata:

Melléklete: 5.3 Portok vizsgálata

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address
HideMyIpSrv.exe	5072	TCP	51535		127.0.0.1
javaw.exe	1360	TCP	1196		172.25.138.209
javaw.exe	1360	TCP	1198		172.25.138.209
macromedia.exe	4824	TCP	12584		172.25.138.209
SecurityManagerPlus.exe	2856	TCP	12594		127.0.0.1
spiceworks-httpd.exe	928	TCP	80	http	0.0.0.0
spiceworks-httpd.exe	928	TCP	443	https	0.0.0.0
spiceworks-httpd.exe	928	TCP	80	http	::
spiceworks-httpd.exe	928	TCP	443	https	::
spiceworks.exe	1116	TCP	1052		127.0.0.1
spiceworks.exe	1116	UDP	162	snmptrap	0.0.0.0
spiceworks.exe	1116	UDP	49154		127.0.0.1
sqlbrowser.exe	2288	UDP	1434	ms-sql-m	0.0.0.0
sqlbrowser.exe	2288	UDP	1434	ms-sql-m	::
System	764	TCP	135	epmap	0.0.0.0
System	4	TCP	139	netbios-ssn	172.25.138.209
System	5080	TCP	554	rtsp	0.0.0.0
System	432	TCP	1025		0.0.0.0
System	964	TCP	1026		0.0.0.0
System	500	TCP	1027		0.0.0.0

System	304	TCP	1028		0.0.0.0
System	484	TCP	1041		0.0.0.0
System	3656	TCP	1241		0.0.0.0
System	3656	TCP	8834		0.0.0.0
System	304	TCP	12548		172.25.138.20 9
System	4	TCP	445	microsoft- ds	0.0.0.0
System	4	TCP	2869	icslap	0.0.0.0
System	4	TCP	5357	wsd	0.0.0.0
System	4	TCP	10243		0.0.0.0
System	4	UDP	137	netbios-ns	172.25.138.20 9
System	4	UDP	138	netbios- dgm	172.25.138.20 9
System	1672	UDP	1900	ssdp	127.0.0.1
System	1672	UDP	1900	ssdp	172.25.138.20 9
System	112	UDP	3702	ws- discovery	0.0.0.0
System	1672	UDP	3702	ws- discovery	0.0.0.0
System	5080	UDP	5004		0.0.0.0
System	5080	UDP	5005		0.0.0.0
System	1176	UDP	5355	llmnr	0.0.0.0
System	1672	UDP	49152		0.0.0.0
System	112	UDP	49279		0.0.0.0
System	112	UDP	63203		0.0.0.0
System	1672	UDP	64927		172.25.138.20 9
System	1672	UDP	64928		127.0.0.1
System	764	TCP	135	epmap	::

System	4	TCP	445	microsoft-	::
System	5080	TCP	554	rtsp	::
System	432	TCP	1025		::
System	964	TCP	1026		::
System	500	TCP	1027		::
System	304	TCP	1028		::
System	484	TCP	1041		::
System	3656	TCP	1241		::
System	4	TCP	2869	icslap	::
System	5252	TCP	3587	p2pgroup	::
System	4	TCP	5357	wsd	::
System	4	TCP	10243		::
System	1672	UDP	1900	ssdp	::1
System	1672	UDP	1900	ssdp	fe80::db3:9f6d :ea42:ea5
System	5252	UDP	3540	pnrp-port	::
System	1672	UDP	3702	ws- discovery	::
System	112	UDP	3702	ws- discovery	::
System	5080	UDP	5004		::
System	5080	UDP	5005		::
System	1176	UDP	5355	llmnr	::
System	1672	UDP	49153		::
System	112	UDP	49280		::
System	112	UDP	63204		::
System	1672	UDP	64925		fe80::db3:9f6d :ea42:ea5
System	1672	UDP	64926		::1
Unknown	0	TCP	1052		127.0.0.1
Unknown	0	TCP	12591		127.0.0.1

11.táblázat: Protocol&Port lista [13].

Táblázat: Banner Grabbing:

Melléklete: 5.2 Banner Grabbing:

www.uni-nke.hu	
Initiating server query	
Looking up IP address for domain:	www.uni-nke.hu
The IP address for the domain is:	193.224.76.29
Connecting to the server on standard HTTP port:	80
[Connected] Requesting the server's default page	
The server returned the following response headers:	HTTP/1.0 301 Moved Permanently
Date:	Wed, 17 Sep 2014 21:05:23 GMT
Server:	Apache/2.2.12
Location:	http://uni-nke.hu/
Content-Length:	226
Content-Type:	text/html; charset=iso-8859-1
X-Cache:	MISS from portalpxy.uni-nke.hu
X-Cache-Lookup:	MISS from portalpxy.uni-nke.hu:3128
Via:	1.1 portalpxy.uni-nke.hu:3128 (squid/2.7.STABLE5)
Connection:	Close

Táblázat: Intense Scann and UDP

Melléklete: 5.6 Intense Scann and UDP

NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 08:55
Scanning 192.168.135.51 [1 port]
Completed ARP Ping Scan at 08:55, 0.45s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:55
Completed Parallel DNS resolution of 1 host. at 08:55, 5.50s elapsed
Initiating SYN Stealth Scan at 08:55
Scanning AsusX54H.connectify (192.168.135.51) [1000 ports]

- Discovered open port 139/tcp on 192.168.135.51
- Discovered open port 445/tcp on 192.168.135.51
- Discovered open port 554/tcp on 192.168.135.51
- Discovered open port 135/tcp on 192.168.135.51
- Discovered open port 5357/tcp on 192.168.135.51
- Discovered open port 10243/tcp on 192.168.135.51
- Discovered open port 2869/tcp on 192.168.135.51

Completed SYN Stealth Scan at 08:55, 4.54s elapsed (1000 total ports)
Initiating UDP Scan at 08:55
Scanning AsusX54H.connectify (192.168.135.51) [1000 ports]
Discovered open port 137/udp on 192.168.135.51
Completed UDP Scan at 08:55, 4.20s elapsed (1000 total ports)
Initiating Service scan at 08:55
Scanning 1007 services on AsusX54H.connectify (192.168.135.51)

- **Service scan Timing: About 0.79% done**
- **Service scan Timing: About 3.77% done; ETC: 10:08 (1:10:08 remaining)**
- **Service scan Timing: About 9.73% done; ETC: 09:51 (0:51:01 remaining)**
- **Service scan Timing: About 15.69% done; ETC: 09:47 (0:44:20 remaining)**
- **Service scan Timing: About 97.62% done; ETC: 09:41 (0:01:07 remaining)**

Completed Service scan at 09:42, 2805.30s elapsed (1007 services on 1 host)

Initiating OS detection (try #1) against AsusX54H.connectify (192.168.135.51)

NSE: Script scanning 192.168.135.51.

Initiating NSE at 09:42

- **NSE Timing: About 2.44% done; ETC: 10:03 (0:20:40 remaining)**
- **NSE Timing: About 4.31% done; ETC: 10:06 (0:22:36 remaining)**
- **NSE Timing: About 49.77% done; ETC: 10:06 (0:12:14 remaining)**
- **NSE Timing: About 55.63% done; ETC: 10:06 (0:10:52 remaining)**

Discovered open port 1900/udp on 192.168.135.51

- **NSE Timing: About 61.12% done; ETC: 10:07 (0:09:37 remaining)**
- **NSE Timing: About 91.49% done; ETC: 10:07 (0:02:06 remaining)**
- **NSE Timing: About 96.61% done; ETC: 10:07 (0:00:50 remaining)**

Completed NSE at 10:07, 1480.75s elapsed

upnp-info: 192.168.135.51
Server: Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
Location: http://192.168.135.51:2869/upnpghost/udhisapi.dll?content=uuid:378ae88e-6578-4ef2-b976-c27b2060accc
MAC Address: 60:D8:19:07:20:59 (Hon Hai Precision Ind. Co.)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose phone
Running: Microsoft Windows 2008 7 Phone Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Windows Server 2008 R2, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008

Uptime guess: 2.538 days (since Mon Oct 27 21:12:47 2014)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: ASUSX54H; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

nbstat: NetBIOS name: ASUSX54H, NetBIOS user: <unknown>, NetBIOS MAC: 60:d8:19:07:20:59 (Hon Hai Precision Ind. Co.)

Names:

- ASUSX54H<00> Flags: <unique><active>
- WORKGROUP<00> Flags: <group><active>
- ASUSX54H<20> Flags: <unique><active>
- smb-os-discovery:
- OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
- OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
- Computer name: AsusX54H
- NetBIOS computer name: ASUSX54H
- Workgroup: WORKGROUP
- System time: 2014-10-30T09:45:34+01:00
- smb-security-mode:
- Account that was used for smb scripts: <blank>
- User-level authentication
- SMB Security: Challenge/response passwords supported
- Message signing disabled (dangerous, but default)
- smb2-enabled: Server supports SMBv2 protocol