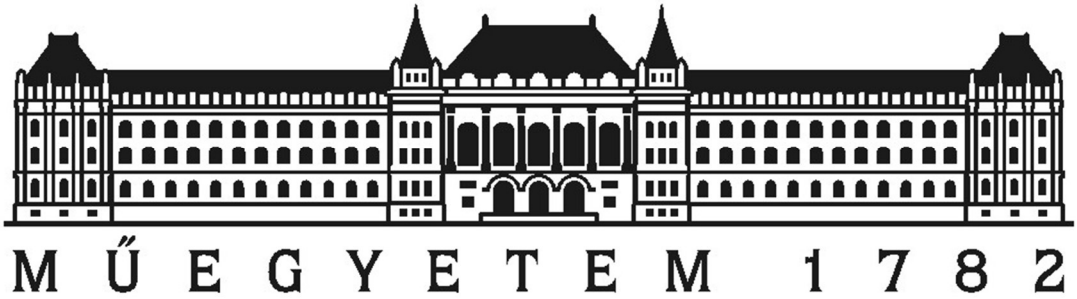
PARIPA program
Hallgatói kutató munka ismertetése

Téma: MFA – megvalósítása

Készítette: Sztán-Kovács Barnabás



Az MFA

Az „MFA (jelentése: Multi-Factor Authentication) – megvalósítása” gyakorlati szempontból nagyon gyakran a TFA (Two-Factor Authentication) megoldást jelenti. Első körben érdemes tisztázni a faktorok jelentését. Egy faktor egy autentikációs pontnak minősül, a legközismertebb ilyen a felhasználónév-jelszó párosítás, de ugyanígy beszélhetünk PIN-kódról, ujjlenyomatról, és bármilyen más azonosítási módszerről. Az MFA faktorait általában – példának okáért, a Microsoft Azure is így osztályozza – három kategóriába szokás sorolni.

A faktorok három kategóriája: valami amit a felhasználó tud (mint például egy jelszó, PIN-kód), valami amit a felhasználó birtokol (mint egy kulcs-token, telefon amire kaphat SMS-t), vagy valami, ami a felhasználó része (ez alatt értjük a biometrikus azonosítást, mint ujjlenyomat, írisz, stb.).

Mivel egy faktor egy autentikációért felel, ebből következik, hogy a multi-faktoros azt jelenti, hogy a bejelentkezés során a felhasználó egynél többször kerül azonosításra hitelesítés céljából, a másik oldalról nézve pedig egy illetéktelen hozzáférőnek egynél több akadályon kell magát átküzdenie a felhasználó nevében bejutáshoz. Jelszavak ellopására számtalan módszer létezik, ezért lehet érdemes egy második faktort bevezetni, ezzel a potenciális támadókat egy második akadály elé állítva, és bejutási lehetőségüket töredékére csökkenteni.

A két faktorból az egyik nagy valószínűséggel egy jelszó, míg a második faktor választható a fent említett másik két kategóriából. Az üzleti életben könnyebb megoldani egy birtokolt eszköz használatát, mint például RSA SecurID® hardware token disztributálása a dolgozóknak, smart kártyák használata, vagy Microsoft szerverek esetén a Microsoft Azure szolgáltatásai, mint például egy SMS-ben a felhasználók (akár céges telefonjának a) számára elküldött ideiglenes jelszó. Mivel a biometrikus azonosításra az eszközök nagy volumenben komoly költségeket vonnak maguk után, meghibásodásuk esetén pedig drága a csere, ezért nem annyira népszerűek nagyvállalati környezetben.

TFA megvalósítása Microsoft Server környezetben

Ahhoz, hogy a Microsoft Azure szolgáltatáson keresztül igénybe lehessen venni az egyszer használatos jelszó kiküldését SMS-en keresztül, egy Active Directory-t (AD) kell üzemeltetni ami egy vállalati infrastruktúra alapját képezi Microsoft szerver esetén.

A Federal Services (AD FS) ennek egy kiegészített verziója, melynek számos más lehetősége is van, mint például más AD FS szerverekkel „Trust kapcsolatokat” kiépíteni. Ennek nagy előnye (és hátránya), hogy ha két domain Trust-kapcsolatban van, akkor aki az egyik hálózatot használhatja, az a másik hálózaton azonosíttathatja magát a saját hálózatán található adatbázisból. Így az egymásban megbízó vállalatok egymás hálózatát használhatják úgy, hogy mindenkinek csak a saját adatbázisát kell karbantartania. Ez biztonsági rést jelent olyan szempontból, hogy így az egyik vállalathoz bejutó támadó a másiknál is hozzáféréssel bír.

Az AD FS jelenléte magával vonja a Web Application Proxy (WAP) szükségességét is, ez minden AD FS implementáció kötelező komponense. A WAP további lehetőségeket is nyújt

webbiztonság téren, például ha egy alkalmazást a WAP-n keresztül teszünk publikussá, akkor a végfelhasználók csak azokat a tartalmakat érik el, amit publikussá tettünk, valamint proxyként működik az AD FS felé a hálózaton belül.

A szerverre való bejelentkezés folyamatát hat fő lépésre bontva érdemes vizsgálni:

1. Firewall – a tűzfal whitelisting alapon működik, azaz csak engedélyezett IP címekről lehet elérni a szervereket, így külső címekről a hozzáférés nem lehetséges.
2. Web Application Proxy (WAP) A Web Application Proxyval találkozik először a belépő felhasználó, a WAP továbbítja autentikáció céljából az AD FS felé.
3. AD FS → AD – az AD FS ugyebár TFA-képes, ezért a felhasználót első körben, első faktorként az AD bejegyzése alapján azonosítja, ez a hagyományos felhasználónév-jelszó páros.
4. Vissza az ADFS-hez, Ha az AD-ban sikeres volt az autentikáció.
5. 2. faktoros azonosítás – ez a lépés az AD FS-en belül történik meg, itt zajlik le a második faktoros autentikáció, a fentebb említett Azure szolgáltatás felhasználásával.
6. Client Access Server (CAS) – miután az TFA megtörtént, a Client Access Server hozzáférést nyújt az elérni kívánt tartalomhoz.

Az MFA tesztkörnyezet megtervezése

Felvetődött a kérdés, hogy egy ilyen rendszerbe van-e lehetőség úgy bejutni kívülről, hogy egy éppen használatban lévő második faktoros kulcsot ellopunk valahogy. Ennek egy lehetséges módja, hogy a mimikatz nevű eszköz segítségével, Pass-the-Hash támadással ellopjuk a hitelesítő adatokat amivel bejelentkezett (és a második faktoron is átjutott) a felhasználó. A mimikatznak van lehetősége arra, hogy pusztán memóriából fusson valamint a memóriából is olvassa ki a felhasználó adatait, ezért „nyom nélkül” tud dolgozni, nincsenek látható nyomai, teljes mértékben felfedetlen marad a támadás.

A valósághoz képest egy redukáltabb modellt szerettünk volna létrehozni a teszteléshez, egy Client Access Server (CAS) helyett egy sima webszerver volt a célpont. Az IIS a Microsoft beépített webszervere a szerver termékeiben, ezt használtuk erre a célra. Az AD-t egy Domain Controller (DC) képviseli majd. A tervezett tesztkörnyezet szerint három virtuális gépre van szükség. Az IIS és a DC egy gépen osztozhat, a másik két szolgáltatás külön szervert kap. Ezen tesztkörnyezet sikeres felépítése után lehet majd a fent említett támadást kipróbálni.

Megvalósítás

A megvalósítás során közös megegyezés alapján arra jutottunk, hogy fel kell állítani egy tesztkörnyezetet, amelyen később a teszteseteket végezzük. Közös koordinációval sikerült a megfelelő tesztkörnyezetet felállítani a feladathoz, és a tesztelés szempontjából a megfelelő szoftvereket, szerverkörnyezetet feltelepíteni.

A CrySyS Lab által az egyetemen üzemeltetett ESXi6-os virtuális gépen volt lehetőségem létrehozni a tesztkörnyezetet. A megvalósítás során a gépek Windows Server 2016 x64 – Desktop Experience operációs rendszerek kerültek a gépekre, mindegyik szerver a saját szerepének megfelelően fel is lett konfigurálva.

Források

https://www.tag-cyber.com/articles/using-clever-deception-to-secure-your-active-directory

https://adsecurity.org/?page_id=1821

https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication

https://github.com/gentilkiwi/mimikatz

https://blog.cobaltstrike.com/2015/05/21/how-to-pass-the-hash-with-mimikatz/

https://support.microsoft.com/hu-hu/help/2617468/microsoft-exchange-2010-client-access-server-cas-not-present-in-site

https://technet.microsoft.com/en-us/library/dn584113(v=ws.11).aspx

https://technet.microsoft.com/en-us/library/hh831725(v=ws.11).aspx

https://msdn.microsoft.com/en-us/library/bb897402.aspx

https://technet.microsoft.com/en-us/library/jj657718(v=exchg.160).aspx

https://technet.microsoft.com/en-us/library/cc725691(v=ws.11).aspx