VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

BIS – Bezpečnost informačních sytémů
The FITfather

Radek Duchoň, xducho07 22. 12. 2021

1 Zmapování vnitřní sítě

K zmapování byl využit příkaz *sudo nmap 192.168.10.0/24 -Pn*. Zapsány budou jen důležité adresy a jejich služby. Po prozkoumání přiděleného uzlu bylo bylo navíc zjištěno, že je ve složce .ssh již nakonfigurováno ssh připojení na server sv2.

Nmap scan report for sv6 (192.168.10.145)

PORT	STATE	SERVICE
22/tcp	open	ssh
5000/tcp	open	upnp

Nmap scan report for sv1 (192.168.10.150)

PORT	STATE	SERVICE
22/tcp	open	ssh
2049/tcp	open	nfs

Nmap scan report for sv2 (192.168.10.166)

PORT	STATE	SERVICE
22/tcp	open	ssh

Nmap scan report for sv3 (192.168.10.170)

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
443/tcp	closed	https
3306/tcp	open	mysql

Nmap scan report for sv4 (192.168.10.199)

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh

2 Zisk tajemství

Po prozkoumání sítě bylo postupně nalezeno 10 tajemství, postup pro jejich získání bude vysvětlen v textu níže.

2.1 Tajemství A

Na serveru SV3 je otevřený html port. Pomocí příkazu *curl 192.168.10.170* byl nalezen odkaz na *192.168.10.170/admin.html* a zde pak na skript *192.168.10.170/index.js*. Zde bylo zadání hesla kontrolováno pomocí jednoduchého spočítání checksum, stačilo tedy od chtěného výsledku spočítat opačné operace a dojít tak k heslu 6230 a následně spustit skript, tím bylo získáno tajemství A.

2.2 Tajemství B

Tajemství B je též na serveru SV3. K jeho nalezení jsem si zobrazil stránku pomocí příkazu *elinks 192.168.10.170*. Dále jsem provedl SQL injection tím, že jsem do pole Login zadal *admin* a do kolonky Password vyplnil řetězec *' OR '' = '*. Po odeslání formuláře se zobrazilo tajemství B.

2.3 Tajemství C

Tajemství C je posledním na serveru SV3. K jeho nalezení bylo zapotřebí oskenovat IP adresu příkazem *sudo nmap -sV --script=http-enum 192.168.10.170*. Tím byla nalezena složka *hidden*, v níž se dále nacházel odkaz na soubor *secret.php*, v němž se nachází tajemství C.

2.4 Tajemství D

Tajemství D se nachází na serveru SV6, kde je otevřený port 5000 se službou upnp, nachází se zde tedy docker. Ke katalogu se dostaneme příkazem *curl 192.168.10.145:5000/v2/_catalog*. Dozvíme se zde o *docker_fun*. Přihlásíme se na root uživatele pomocí příkazu *sudo su root*, následně zadáme příkaz *docker login 192.168.10.145:5000* a zadáme (zřejmě libovolné) uživatelské jméno a heslo. Po přihlášení si můžeme docker stáhnou t k sobě příkazem *docker pull 192.168.10.145:5000/docker_fun*. Poté si zjistíme info o dockeru, zadáme tedy příkaz *docker images*, abychom zjistili jeho ID a následně *docker inspect <id>,* z výpisu zjistíme, že docker při spuštění vykoná příkaz *rm -rf /tmp/secret.txt*, docker tedy nespustíme, ale radši nalezneme příkazem *find / -regex ".*/tmp/secret\.txt"*. Tím nalezneme překvapivě 4 soubory, v jednom z nich je aktuální tajemství D.

2.5 Tajemství E

Tajemství E se nachází na serveru SV2, kam se můžeme připojit pomocí ssh. Po prozkoumání tohoto serveru bylo ve složce */trash* nalezeno několik souborů tvářících se jako zip patřících uživateli iperesini. Některé jsou ve skutečnosti binární data a manuálové stránky programů, skutečným zipem je zřejmě jen soubor *crack_me.zip*. Po puštění programu *Advanced Archive Password Recovery* na mém počítači bylo heslo prolomeno během několika ms, jelikož má pouze 3 znaky „ /$“. V zipu se nacházel textový soubor geheimnis.txt s tajemstvím E a nápovědou v podobě uživatelského jména Fredek na server SV1.

2.6 Tajemství F

Tajemství F se nachází také na serveru SV2. K jeho nalezení posloužil příkaz *find / -user iperesini 2>/dev/null*, který vypsal několik řádků se soubory, mezi nimi */mnt/root/was_es_ist*. V souboru se nacházela nečitelná změť písmen, po vypsání šesti různých hesel po půl hodině jsem dokázal identifikovat 7 oblastí (první a poslední o délce 3, ostatní o délce 6 písmen), kde jsou písmena buď konstantní, nebo se mění periodicky. Jelikož měl text celkem 122 znaků, tajemství mají 91 znaků a odhadnutelná oblast měla 36 znaků, kdežto odhadnutelná část tajemství má 27, je vidět, že to nejspíš není náhodné (poměr je v obou případech 4:3). Jelikož to nemohla být pouhá substituční šifra, a byla tu nápověda v prodloužení (a přitom využívání pouze tisknutelných znaků zřejmě pod hodnotou 128) napadlo mě zkusit base64, kdy jsem zakódoval předpokládaný text tajemství, výsledná písmena seděla s danými regiony odhadnutelných písmen. Tím již v podstatě nebylo o base64 pochyb. Dále bylo nutné zjistit, jak jsou data přeskládána. Po povšimnutí, že 1. písmeno je v 1. regionu, 2. ve druhém atd. nebylo těžké odvodit zbytek (8. písmeno v 6. regionu… 13. písmeno v 1. regionu…) a napsat krátký kód, který data přeskládal zpět, poté stačilo dekódovat zprávu pomocí base64 a bylo získáno tajemství F.

2.7 Tajemství G

Tajemství G se nachází na serveru SV4, na kterém běží služba ftp. Na serveru byla nalezena složka pub příkazem *curl ftp://192.168.10.199* a v ní 4 soubory, tajemství se nacházelo v souboru secret.asc, ve kterém se nacházela PGP zpráva. Její klíč však v nedohlednu, nalezl jsem ho až o mnoho později na serveru SV1, kde běží služba nfs, kvůli které jsem na svůj uzel doinstalovával balík nfs-utils a jeho závislosti. Předtím jsem se však musel připojit pomocí ssh, přihlašovací jméno Fredek jsme zjistili v tajemství E, následně byl proveden slovníkový útok (naštěstí bylo cílové heslo jen 22. v seznamu nejběžnějších hesel https://nordpass.com/most-common-passwords-list/) s výsledkem iloveyou. Poté zde byla nalezena o adresář nad výchozím umístěním složka shared_dir, která byla následně namountována pomocí příkazu *sudo mount -t nfs 192.168.10.150:/home/shared_dir /mnt*. Ve složce /mnt je nyní soubor private.key, který má na konci zprávu passphrase is "123". S privátním klíčem a heslem 123 tak byla PGP zpráva konečně dešifrována a získáno tajemství G.

2.8 Tajemství H

Tajemství H se nacházelo na serveru SV1, po namountování složky shared_dir (vizte předchozí tajemství) se u privátního klíče k PGP zprávě nacházel také soubor secret, který obsahoval tajemství H.

2.9 Tajemství I

Tajemství I se rovněž nacházelo na serveru SV1. Vedle klíče k tajemství G a souboru s tajemstvím H se ve složce nacházelo ještě několik obrázků, jeden z nich měl jiné datum poslední změny oproti ostatním. Vyzkoušel jsem na něj tedy použít https://aperisolve.fr/. V části strings se objevil jeden řetězec s čísly z formátu tajemství, po dešifrování Caesarovy šifry (posunem o 19) bylo získáno tajemství I.

2.10 Tajemství J

Tajemství J se nacházelo na serveru SV4. Jeden obrázek měl oproti ostatním souborům jinak nastavená práva pro zápis, byl tedy podezřelý, po prohnání skrz https://aperisolve.fr/ bylo v outguess nalezeno tajemství J.