1. projekt do předmětu BIS

Sára Škutová, xskuto00

30. listopadu 2019

1 Zmapování vnitřní sítě

Pomocí příkazu `$ ifconfig` jsem zjistila rozsah ip adres, které se nachází v dané sítí. Následně pomocí `$ nmap 192.168.122.1-254` jsem provedla skenování sítě, čímž jsem zjistila, že mezi studentskými servery se nacházejí následují nepojmenované servery s tajemstvím (nepojmenovaných serverů je více, ale tyto uchovávají tajemství):

Nmap scan report for 192.168.122.38

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

Nmap scan report for 192.168.122.77

PORT	STATE	SERVICE
22/tcp	open	ssh
111/tcp	open	rpcbind

Nmap scan report for 192.168.122.105

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
111/tcp	open	rpcbind
3306/tcp	open	mysql

Nmap scan report for 192.168.122.169

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
111/tcp	open	rpcbind

Nmap scan report for 192.168.122.220

PORT	STATE	SERVICE
22/tcp	open	ssh
23/tcp	open	telnet
80/tcp	open	http

Jelikož servery nejsou pojmenované a pro urychlení čtení a zápisu se jednotlivé testovací servery budou značit jejích posledním oktetem.

Krátce po zveřejnění projektu měl server .220 uzavřený port 80, po nějaké době ho ale někdo otevřel.

Při pozdějším podrobnějším skenování jednotlivých serveru pomocí přepínačů **-p-** a **-A** jsem zjistila, že na .169 se nachází také ftp na portu 42424.

2 Klientská stanice

Při prohledávání souborů klientské stanice jsem se dozvěděla, že stanice zná server .220 společně s uživatelem **smith**. Dále jsem také ve složce **.ssh** nalezla klíč, díky kterému se lze přihlásit na .220:

```
$ ssh smith@192.168.122.220
```

3 192.168.122.220

Hned v úvodu jsem si všimla, že se zde nachází dva soubory a to **agg** a **agg2**. Nevím, zda to jsou soubory, které byly nachystané či jsou to zbytky po nějakém studentovi, ale poté co mi souborový analyzátor návrh, že se jedná o sobory z tcpdump capture, tak jsem je otevřela ve Wiresharku. Tam jsem zjistila, že jsou tam zachycené telnet pakety, posílané mezi servery .1 a .220. V nich se pak nacházejí přihlašovací údaje uživatele **ada** s heslem **nachystejteuzenace**. Později jsem si to ověřila, když jsem sama zachytávala pakety na serveru .220. Po přihlášení na uživatele adu jsem pak v jejím domovském adresáři nalezla soubor **secret.txt**, který obsahoval **tajemství D**.

Tajemství E jsem prakticky získala náhodou. Po mých zkušenostech z minulého roku jsem věděla, že se soubory s tajemstvím často jmenují secret*.txt. Po – té co jsem vypotřebovala pokusy na prolomení přihlašovací stránky na webovém serveru, jsem vyzkoušela, zda web nemá daný textový soubor, a ejhle tajemství je na světě.

```
$ curl localhost/secret.txt
```

Na závěr jsem ještě si ještě nechala prohledat všechny soubory, a hledala jsem ty co v sobě může obsahovat slovo secret:

```
$ ls /* -latR | grep 'secret'
```

To mi nalezlo několik souborů, pomocí příkazu `find` jsem nalezla jejích umístění. Důležitým se pak ukázal soubor **show-secret**, který jak se později ukázalo je spustitelným souborem v /**usr**/**bin**/, a který zobrazí **tajemství H**.

```
$ find / -name show-secret
```

4 192.168.122.38

Na .38 se nachází FTP server po kontrole o jakou verzi se jedná (`nmap -A 192.168.122.38`), jsem zjistila, že se jedná o vsftpd 2.3.4. Tahle verze ftp je známá tím, že se pomocí řetězce *:)* vloženého do středu nebo na konec loginu (může být jakýkoliv) můžeme dostat na ftp server aniž bychom vůbec museli zadávat heslo. Po připojení na ftp pomocí `$ ftp 192.168.122.38`, zadání loginu ve tvaru *log:)in* a odentrování hesla jsem získala přístup na ftp server, kde mi bylo sděleno, že se mám podívat na nově otevřený port *53778*. Po připojení na daný port na .38 (`$ nc 192.168.122.38 53778 -v`) se mi zobrazilo **tajemství G**.

Na .38 se také nachází webový server se seznamem zaměstnanců. Nejdříve jsem si vůbec nevšimla textového zadávacího políčka při filtrování a pokoušela jsem různé o metody při přidávání zaměstnanců. Při pozdějším prozkoumávání jsem si políčka již všimla a zjistila jsem, že se pomocí něho a daných tlačítek filtrují výsledky tabulky. Jelikož šlo uživatele přidávat a tabulka dané hodnoty musí odněkud číst, tak mi došlo, že ačkoliv na .38 není msql služba, tak webový server používá nějakou externí databázi, což znamená, že by šlo použít SLQ injection. Zkoušela jsem základní známe verze toho útoku, ale vždy mi to nalezlo údaje, které již někdo zadal při přidání zaměstnance. Pak mě napadlo zadat něco co by mohlo způsobit syntetickou chybu v dotazu. Při "– se mi vypsala chyba zároveň i s dotazem, který se používá. Od toho pak již bylo jednoduché sestavit text tak aby se mi vypsalo co jsem požadovala. Následujícím příkazem se mi pak vypsaly údaje s loginy a hesly, které se zadávají při přidávaní zaměstnance. V políčku hesla admina se pak nacházelo **tajemství A**.

```
% " UNION SELECT login as id, passwd as name, 3, 4 FROM auth; --
```

Informace, co a z jaké tabulky vybírat jsem získala při zkoumání html kódu formuláře pro přidávání zaměstnanců.

5 192.168.122.77

Na tento server jsem narazila, když jsem hledala, který další bezejmenný server by mi dovolil se na něho přihlásit. .77 byl první, který mi toto dovolil. Po několika pokusech o přihlášení se základním loginem a heslem, jsem přišla na login: **root** a heslo: **root**. V domovském adresáři jsem pak nalezla soubor **secret.txt**, který mi vypsal **tajemství J**.

6 192.168.122.169

Po přihlášení na webový server .169 pomocí programu **elinks**, a po prohledání souborů co se tam nachází jsem v /**etc**/**raddb**/ nalezla soubor **sql.conf**, který měl v políčku password **tajemství C**.

Později po důkladnějším skenování sítě s nmap pomocí přepínačů -p- a -A, jsem na .169 nalezla ftp službu, která se pomocí základního nastavení nmap nezobrazila. Při skenování se mi zároveň zobrazilo, že se zde nachází soubor **secret.txt**. Také se mi zobrazila informace, že je povoleno anonymní přihlášení. Po přihlášení na `$ ftp 192.168.122.169 42424`, zadání loginu: anonymous, odentrování hesla, a stáhnutí souboru secret.txt (`get secret.txt`) jsem si mohla zobrazit z něho **tajemství B**.

7 192.168.122.105

Po přihlášení na .105 pomocí programu **elinks** se zobrazuje chybová stránka s tím, že Tracy není schopná zalogovat chybu. Při prozkoumání internetu zjišťuji, že Tracy, známá taky jako laděnka, se používá jako pomoc při debuggování php kódu, a že byla vytvořena tvůrci Nette frameworku. K Tracy se mi nepodařilo nalézt žádnou známou chybu, ale z dřívějších pokusů jsem věděla, že můžu zobrazit soubor v `192.168.122.105/www/robots.txt` a složku `192.168.122.105/log/`. Po neúspěšných pokusech se přihlásit pomocí ssh na .105 a hledání souboru secret.txt v adresáři www, mě napadlo se podívat jakou má nette strukturu adresářů. To se ukázalo jako správný nápad, když v souboru `192.168.122.105/app/config/local.neon` jsem nalezla **tajemství I**.

8 192.168.122.227

Server .227 byl druhým z nepojmenovaných, který mi dovolil zadat heslo. Po pokusech s přihlášením (nejčastěji používané loginy, hesla a zdravicí text při přihlašování), jsem se na server dostala s kombinaci **teacher** a **teacher**. Po různém pohledávání souborů, zkoušení zachytávání paketů pomocí tcpdump (nebylo dovoleno odchytávat z daného rozhraní), zkoumání dns záznamů pomocí nástroje dig (žádné informace se nenalezly) jsem začala prohledávat informace na internetu o možných chybách na samotném Linuxu a linuxových programech. Díky tomu jsem nalezla informaci, že se před nedávnem nalezla chyba v příkazu **sudo** a jeho konfiguračním souboru **sudoers**[1], která umožňovala, aby ne-rootovský uživatel mohl spouštět programy a dostávat se do míst, kde mohl jenom uživatel s root oprávněním. Tato zranitelnost má být opravená ve verzi 1.8.28. Na .227 je ovšem verze 1.8.19p2, neboli ta, ve které se vyskytuje chyba. Zkusila jsem tedy `sudo -u#-1 id -u` a po odentrování hesla teacher se mi skutečně vypsala 0 (neboli id uživatele root). Dala jsem tedy vyhledat možná tajemství `$sudo -u#-1 ls /* -latR | grep 'secret'`, které mi nalezlo, že se někde ukrývá soubor **secret.txt**. S `$sudo -u#-1 find / -name secret.txt` jsem zjistila, že se daný soubor nachází v adresáři /**root**/. `$sudo -u#-1 cat /root/secret.txt` mi pak vypsal **tajemství F**.

[1] https://www.sudo.ws/alerts/minus_1_uid.html