Bezpečnost informačních systémů
Projekt

Bc. David Kolečkář, xkolec07
xkolec07@stud.fit.vutbr.cz

28. listopadu 2019

1 Úvod

Cílem projektu bylo získat všechna možná tajemství (jsou to řetězce, které vždy obsahují slovo "tajemství") ukrytá na privátních serverech v síti BIS.

2 Zmapování sítě

Po připojení na server zjistím pomocí příkazu `ifconfig` adresu sítě (192.168.122.55). Následně příkazem `nmap 192.168.122.0/24 -Pn | grep "for 192"` zjistím všechny možné servery obsahující tajemství a zároveň příkaz vyfiltruje klientské stanice. Následně pro každý získaný server spustím příkaz `nmap -p- 192.168.122.XXX` a získám všechny služby spuštěné na uvedeném serveru:

```
Nmap scan report for 192.168.122.1 = SSH 22, RPCBIND 111, DOMAIN 53, NFS 2049,
                                     MYSQL 3306, UNKOWN 20048, 43584, 45970
Nmap scan report for 192.168.122.38 = SSH 22,HTTP 80, FTP 21
Nmap scan report for 192.168.122.42 = SSH 22, RPCBIND 111
Nmap scan report for 192.168.122.77 = SSH 22, RPCBIND 111
Nmap scan report for 192.168.122.83 = SSH 22, RPCBIND 111
Nmap scan report for 192.168.122.105 = SSH 22, RPCBIND 111, HTTP 80, MYSQL 3306
Nmap scan report for 192.168.122.150 = SSH 22, RPCBIND 111
Nmap scan report for 192.168.122.155 = SSH 22, RPCBIND 111
Nmap scan report for 192.168.122.169 = SSH 22, RPCBIND 111, HTTP 80, UNKOWN 42424
Nmap scan report for 192.168.122.206  = SSH 22, RPCBIND 111
Nmap scan report for 192.168.122.215 = SSH 22, RPCBIND 111
Nmap scan report for 192.168.122.220 = SSH 22, RPCBIND 111, TELNET 23, HTTP 80
Nmap scan report for 192.168.122.227 =  SSH 22, RPCBIND 111
```

3 Tajemství A

Na serveru 192.168.122.38 běží služba HTTP. Zkouším pomocí `elinks` procházet web. Nachází se zde web pro správu zaměstnanců včetně formuláře pro jejich filtrování. Takže zkouším využít SQL injekce. Do pole pro filtrování zkouším zadat `"AND 1=0"`, vyskočí hláška špatné SQL syntaxe, takže útok bude možný. Napřed si vypíšu názvy všech tabulek v databázi:
`"union all select table_name as name, 0 as id, "ad" as address, "email" as email from information_schema.tables WHERE "name"Like"`. Procházím jednotlivé tabulky a objevím tajemství v tabulce auth.

```
"union all select passwd as name, 0 as id, "ad" as address, "email" as email from auth
where "name"Like"
```

4 Tajemství B

Na serveru 192.168.122.169 běží na portu 42424 neznámá služba. Zkouším `elinks 192.168.122.169:42424`. Zjistím, že se zde nachází FTP(vsFTPd 3.0.2). Použiji příkaz `ftp` na připojení k serveru s uživatelským jménem anonymous bez hesla. Úspěšně se přihlásím a nachází se zde soubor secret.txt.

5 Tajemství C

Na serveru 192.168.122.169 běží HTTP služba. Pomocí příkazu `elinks 192.168.122.169` se připojím na server. Zde se nachází adresářová struktura, kterou procházím. Ve složce etc/raddb/sql.conf se nachází tajemství C.

6 Tajemství D

Připojím se k serveru 192.168.122.220 jako uživatel smith (jelikož bez zadání uživatele je zobrazena hláška Hello, Smith!). Vím, že zde běží služba telnet. Zkouším zachytit provoz pomocí `tcpdump` do souboru pcap. Následně tento soubor přesunu na svůj lokální PC, kde ho analyzuju pomocí Wiresharku. Zjistím, že zde probíhá komunikace telnet, kde lze zjistit jméno uživatele a heslo (jméno: ada, heslo: nachystejteuzenace). Spouštím tedy příkaz `telnet 192.168.122.220` s těmito přihlašovacími údaji. Nachází se zde soubor secret.txt obsahující tajemství D.

7 Tajemství E

Na serveru 192.168.122.220 běží služba HTTP, zkouším nalézt soubor secret.txt
`curl -i 192.168.122.220/secret.txt`. Nalezeno další tajemství.

8 Tajemství F

Po připojení na server 192.168.122.227 jako uživatel teacher s heslem teacher, zde nemůžu nic užitečného naleznout. Až na studentské adresáře 1-3, které nelze procházet pro nedostatečná práva. Nacházím zranitelný příkaz sudo (Sudo Vulnerability CVE-2019-14287). Kde se lze pomocí příkazu `sudo -u#-1 bash` přepnout na uživatele root. Pak jen vyhledám pomocí příkazu `find -name secret.txt` a zjistím, že se tajemství nachází ve složce: `./root/secret.txt`

9 Tajemství G

Server 192.168.122.38 má spuštěnou službu FTP na portu 21. Zkouším se připojit a dozvídám se, že zde běží vsFTPd 2.3.4. Nacházím exploit, kdy uživatelské jméno končí „:)“, přihlásím se tedy jako uživatel a:) bez hesla. Následně dostanu hlášku: `220 Opened port 57738, take a look ;)`. Otevírám tedy znovu FTP připojení, tentokrát na jiném portu 57738 a získám tajemství G.

```
Connected to 192.168.122.38 (192.168.122.38).
220 (vsFTPd 2.3.4)
Name (192.168.122.38:student): a:)
331 Please specify the password.
```

```
Password:
220 Opened port 57738, take a look ;)

ftp 192.168.122.38 57738
Connected to 192.168.122.38 (192.168.122.38).
```

10 Tajemství H

Po přihlášení na serveru 192.168.122.220 přes telnet na uživatele ada, spouštím příkaz: `ls / -laR | grep "secret"`. Nacházím spustitelný soubor `./show-secret` ve složce `/usr/bin/`. Po jeho spuštění nalézám další tajemství.

11 Tajemství I

Na serveru 192.168.122.105 běží HTTP služba, zkouším `elinks 192.168.122.105`. Zde se dozvídám o adresáři /www. Znovu použiji elinks na tento adresář a dostávám error 500, který vypíše Tracy. Jelikož Tracy běží v Nette frameworku, zkouším i jiné adresáře. V adresáři /app/config/local.neon nacházím tajemství.

12 Tajemství J

Jelikož nemůžu najít další přihlašovací údaje a tajemství. Zkouším jednoduchý slovníkový útok (python script) na servery, kde jsem nic nenalezl s uživatelskými jmény (ada, smith, root, admin, administrator). Na serveru 192.168.122.77 se mi podaří přihlásit jako root s heslem root. Nachází se zde souboru secret.txt obsahující další tajemství.