

# Bezpečnost informačních systémů – projekt 1

## Vysoké učení technické v Brně

Petr Stehlík <xstehl14@stud.fit.vutbr.cz>

23. listopadu 2016

## 1 Mapování serverů

Po připojení na server bis.fit.vutbr.cz jsem prvně zmapoval celou lokální síť, která sídlí v rozsahu 192.168.122.0/24, což jsem zjistil z nástroje ifconfig. Síť jsem mapoval pomocí dostupného nástroje nmap s následnými parametry: `nmap -v -sn 192.168.122.0/24`.

Z výsledků jsem následně zjistil, že je připojeno velké množství studentů, ty jsem odfiltroval z výsledku a našel jsem celkem 4 servery ptest1 – ptest4, které jsem následně analyzoval.

Provedl jsem mapování portů a služeb, co na nich běží.

### 1.1 ptest1

```
$ nmap -p- ptest1
PORT STATE SERVICE
22/tcp open  ssh
80/tcp open  http
8080/tcp open http-proxy
```

### 1.2 ptest2

```
$ nmap -p- ptest2
PORT STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
3306/tcp open mysql
```

### 1.3 ptest3

```
$ nmap -p- ptest3
PORT STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
```

### 1.4 ptest4

```
$ nmap -p- ptest4
PORT STATE SERVICE
22/tcp open  ssh
80/tcp open  http
41337/tcp open unknown
```

## 2 Získání jednotlivých tajemství

Tajemství jsem získával náhodně dle postupného prohledávání a zkoumání serverů. Zde je uvedu v abecedním pořadí.

### 2.1 Tajemství A

Toto tajemství je umístěno na serveru ptest1 a je získatelné přes HTTP proxy na portu 8080. Zde je umístěn velmi jednoduchý přihlašovací formulář. Analyzoval jsem HTTP hlavičky odpovědi serveru a zjistil jsem, že server při neúspěšném přihlášení nastaví cookie LOGGED\_IN na hodnotu **False**. Tuto cookie jsem upravil a nastavil její hodnotu na **True**. Poté stačilo znova poslat požadavek na server a byl jsem přihlášen. Na dané stránce bylo tajemství umístěné.

### 2.2 Tajemství B

Tajemství B je též umístěno na serveru ptest1. Po prozkoumání internetové stránky na portu 80 jsem si všiml, že se vždy přesměruje na adresu ptest1/xsmith07. Pročetl jsem celý obsah stránek a usoudil, že se zkusím připojit přes SSH na ptest1 pomocí uživatele xsmith07. Jedno z nejpoužívanějších hesel je jméno domácího mazlíčka, které je zmíněno hned na hlavní stránce (Micák). Toto heslo jsem zkusil v několika kombinacích a heslo jsem uhádl. Tajemství B je přímo v domovském adresáři uživatele xsmith07.

### 2.3 Tajemství C

Na serveru ptest2 je na portu 80 umístěna další webová stránka s databází zaměstnanců. Prvním a správným nápadem bylo vytvořit SQL Injection dotaz, kterým jsem se dostal k obsahu jiných tabulek v databázi. Prvně jsem zjistil jaký SQL dotaz je zadáván skriptem do databáze. Ten jsem zjistil pomocí chybové hlášky, která je vytisknuta při chybném dotazu (např. syntax error). Následně jsem vytvořil SQL dotaz na vypsání všech sloupců všech tabulek v databázi:

```
ý%" UNION SELECT table_schema, table_name, column_name, 0
FROM information_schema.columns
UNION SELECT id, name, email, address FROM contact WHERE name LIKE "%á
```

Z výpisu jsem zjistil, že je zde tabulka auth, která obsahuje sloupec passwd. Ten je nejčastějším cílem útoku a proto jsem se na něj zaměřil pomocí následujícího dotazu, kterým jsem získal tajemství C, které bylo heslo uživatele admin.

```
ý%" UNION SELECT id, passwd, login, 0 FROM auth UNION SELECT id, name, email, address FROM
contact WHERE name LIKE "%á
```

### 2.4 Tajemství D

Portscan serveru ptest2 obhalil otevřený port 21 s běžící službou FTP. Pokusil jsem se na službu připojit a server oznámil svou verzi (VSFTPD 2.3.4). Tuto verzi jsem našel jako zranitelnou skrze "smajlíkový exploit". Ten dovoluje se přihlásit jako jakýkoliv uživatel, aniž by FTP server kontroloval heslo (příp. přijme libovolné heslo). Následně FTP server zareagoval, otevřel náhodný port na ptest2, který při jakémkoliv požadavku odpovídal tajemstvím D.

## 2.5 Tajemství E

Ve složce `.ssh` na serveru `bis.fit.vutbr.cz` se nacházel privátní klíč pro uživatele `smith`. Z config souboru jsem zjistil, že tento privátní klíč je pro server `pctest3`. Díky němu jsem se přihlásil na daný server, kde ale nic nebylo. Nicméně na serveru `pctest3` je otevřený port se službou `telnet`. Ta nešifruje svůj provoz a tudíž jsem zahájil odposlouchávání `telnet` komunikace pomocí nástroje `tcpdump`. Mezitím jsem prošel dostupné části serveru `pctest3` a zjistil existenci druhého uživatele `"ada"`. Na toto uživatelské jméno jsem se zaměřil v zachycené `telnet` komunikaci a našel heslo pro uživatele `ada` pro přihlášení na server `pctest3`. Uživatel `ada` měl již tajemství E uložené ve své domovské složce.

## 2.6 Tajemství F

Po portscanu `pctest4` jsem našel otevřený nestandardní port, na který jsem se zkusil připojit pomocí různých služeb. Na tomto portu běžel FTP server. Připojil jsem se na něj a běžel v anonymouse režimu. To znamená, že uživatel `anonymous` nevyžaduje heslo. Připojil jsem se na server a po příkazu `DIR` jsem našel tajemství F přímo v domovské složce.

## 2.7 Tajemství G

Tajemství G jsem získal skrze program `ZSNES`, na který máme v naší domovské složce na serveru `bis.fit.vutbr.cz` symlink. Zjistil jsem verzi programu a našel exploit pomocí `stack-based buffer overflow`. Přímo tento exploit jsem našel implementovaný v jazyku `Python`. Skript jsem spustil na serveru a tajemství bylo vyraženo.

## 2.8 Tajemství H

Připojil jsem na server `pctest4` na port 80, kde běžel webový server, který měl povolený `directory listing`. Prošel jsem všechny dostupné soubory na webovém serveru a našel `sql.conf` (cesta `etc/raddb/sql.conf`), které obsahovalo tajemství H.

## 2.9 Tajemství I

Tajemství I je umístěno stejně jako tajemství H v souboru dostupném na webovém serveru `pctest4`, avšak je schováno v PDF souboru `Internal.pdf` v Keyword metainformaci.

## 3 Závěr

Podařilo se mi získat všechna tajemství dostupná na serverech. Využil jsem mnoho odlišných přístupů a vyzkoušel vždy několik útoků.