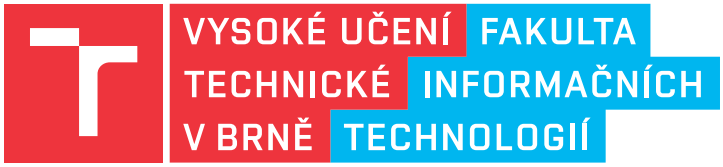
Fakulta informačních technologií
Vysoké učení technické v Brně




# BIS

## Bezpečnost informačních systémů

**Projekt**

Bc. Peter Šuhaj (xsuhaj02)

30. novembra 2019

# 1 Zmapovanie siete

Po pripojení na server ako prvé som pomocou príkazu `ifconfig` zistil informácie o siete a preskenoval celú sieť pomocou `nmap -Pn 192.168.122.1/24`. Týmto som získal informácie o zariadeniach na sieti a otvorených portoch.

```
Nmap scan report for 192.168.122.1
Host is up (0.00019s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
111/tcp  open  rpcbind
2049/tcp open  nfs
3306/tcp open  mysql
MAC Address: 52:54:00:52:BE:C2 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.38
Host is up (0.00035s latency).
Not shown: 970 filtered ports, 27 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 52:54:00:07:85:00 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.42
Host is up (0.00037s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:C0:29:C0 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.77
Host is up (0.00034s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:D4:0D:75 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.83
Host is up (0.00040s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:C2:A1:60 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.105
Host is up (0.00031s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
3306/tcp open  mysql
MAC Address: 52:54:00:AD:2F:85 (QEMU Virtual NIC)
```

```
Nmap scan report for 192.168.122.150
Host is up (0.00042s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:71:10:A5 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.155
Host is up (0.00041s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:49:02:85 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.169
Host is up (0.00038s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
MAC Address: 52:54:00:5A:B6:76 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.206
Host is up (0.00035s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:EC:02:F7 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.215
Host is up (0.00033s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:49:52:E4 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.220
Host is up (0.00067s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
MAC Address: 52:54:00:27:58:18 (QEMU Virtual NIC)

Nmap scan report for 192.168.122.227
Host is up (0.00032s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 52:54:00:8E:17:1B (QEMU Virtual NIC)
```

## 2 Tajomstvo G

Na 192.168.122.38 beží ftp. Po zadaní príkazu `ftp 192.168.122.38` som zistil že tu beží vsFTPd 2.3.4, vyhľadal či nemá nejakú zraniteľnosť a zistil že má. Pridaním znakov :) na koniec prihlasovacieho mena a stlačením Enteru pri hesle som dostal otvorený port. Chcel som sa cez `telnet` pripojiť na získaný port ale na serveri študent nie je `telnet`. Pozrel som sa do histórie kde na začiatku nachádzam informáciu že užívateľ smith si vygeneroval ssh kľúč na server 192.168.122.220. Skúšam `ssh -i .ssh/id_rsa smith@192.168.122.220`, čo funguje. Na tomto stroji už je `telnet`, opakujem pokus o pripojenie čo sa podarí a získavam tajomstvo.

## 3 Tajomstvo C

Po výpisu súborov v domovskom priečinku používateľa `smith` som našiel skrytý priečinok `.elinks`, čo indikuje že je nainštalovaný prehliadač `elinks`. Začal som teda otvárať IP adresy, na ktorých je otvorený port `http`. Na 192.168.122.169 sa dali prehľadávať adresáre, kde v `etc/raddb/mysql.conf` som narazil na tajomstvo.

## 4 Tajomstvo D

Po výpisu súborov som užívateľa `smith` som narazil na súbory `agg`, `agg2`, pomocou príkazu `file` som zistil že ide o súbory `tcpdump capture file`. Pomocou scp som ich stiahol na lokálny počítač a otvoril vo programe `Wireshark`. V súboru `agg2` vidím paket, ktorý obsahuje reťazec `Password:`, na ktorú je odpoveďou `nachystejteuzenace\r`, ďalej vidím paket s obsahom `[ada@localhost ]$`, ide teda o užívateľa `ada` na tom istom počítači ako je `smith`. Pri prehľadávaní priečinku `/home` vidím že tam naozaj je užívateľ `ada`. Po zadaní príkazu `su ada` a zadaním vyššie uvedeného hesla sa úspešne prihlasujem a v domovskom priečinku nachádzam súbor `secret.txt`, ktorý obsahuje tajomstvo.

## 5 Tajomstvo A

Pokračoval som so skúmaním webstránok pomocou `elinks`, na stroji 192.168.122.38 sa nachádza stránka, kam sa dá registrovať. Pokúšam sa najprv registrovať užívateľa čo sa mi aj zobrazí, je tam teda nejaká databáza. Idem skúsiť SQL injection vo vyhľadávacom poli. Najprv sa mi podarí zadať chybný dotaz, dostal som chybovú hlášku ktorá ale zobrazuje aj formát dotazu a že ide o `MariaDB`. Ako prvé idem teda zistiť schému databáze, aké tabuľky obsahuje s akými atribútami. Pomocou `'' AND 1=2 UNION SELECT table_name, column_name, 1, 2 FROM informaauth_schema.columns;#` sa mi to podarilo vypísať, vo výpise sa nachádza tabuľka `auth` s atribútmi `id`, `login`, `passwd`. Pomocou `'' AND 1=2 UNION SELECT id, login, passwd, 2 FROM auth;#` som si vypísal obsah tabuľky `auth` kde som našiel tajomstvo.

## 6 Tajomstvo H

Stále som na stroji 192.168.122.220, kde som si dal vypísať premennú prostredia `$PATH`, kde sú priečinky pre spustiteľné súbory. Postupne ich prechádzam, v priečinku `/usr/bin` nachádzam súbor s názvom `show-secret`. Spustím ho a získavam tajomstvo.

## 7 Tajomstvo E

Na 192.168.122.220 je otvorený port 80, skúšam `elinks localhost` čo ale nefunguje. Skúšam na študentskom serveri príkaz `elinks 192.168.122.220`, čo už funguje a vidím prihlasovací formulár.

Skúšam rôzne kombinácie ale nejde. Skúsil som použiť príkaz `curl`, kde nič nového som nenašiel. Tak ešte som zadal `curl -v`, teda verbose čím získavam informácie o HTTP dotaze, kde mi upúta pozornosť riadok `Set-Cookie: LOGGED_IN=False`. Stránka používa nejaké cookie s týmto názvom, čo pravdepodobne slúži na automatické prihlásenie. Pokúsim sa nastaviť cookie pomocou `curl -b "LOGGED_IN=True"192.168.122.220` s čím sa dostanem na stránku a získavam tajomstvo.

## 8 Tajomstvo I

Pokračujem ešte v prehľadávaní webstránok, na 192.168.122.105 ma najprv presmeruje na `/www`, zadávam `elinks 192.168.122.105/www` kde dostávam `Server Error`, ktorý pochádza od `Tracy`. Vyhľadávam čo to je vlastne a zistím že ladiaca knihovna pre PHP framework `Nette`. Vyhľadám ako vyzerá štruktúra bežného `Nette` projektu, ktorý obsahuje priečinky `app, log, temp, tools, vendor, www,` atď. Skúšam namiesto `elinks 192.168.122.105/www` použiť najprv `elinks 192.168.122.105/app`, kde sa dostanem do tohto priečinku a začnem prehľadávať súbory. V `/app/config/local.neon` som našiel tajomstvo.

## 9 Tajomstvo B

V dokumentácií `nmap` som sa dočítal že skenuje iba najčastejších 1000 portov pre každý protokol. Vyhľadávam teda ako preskenovať všetky porty, zistím že pomocou prepínača `-p-`. Zadávam `nmap -p- 192.168.122.1/24` a zisťujem že ešte sú otvorené nejaké porty na 192.168.122.1 a na 192.168.122.169. Skúšam aké to môžu byť služby, či `ssh`, `telnet`, `ftp`, atď. Na 192.168.122.169 na porte 42424 ma privíta `ftp`. Skúšam sa prihlásiť, nejde. Pokúsim sa teda o anonymné prihlásenie zadaním loginu `anonymous` a náhodného hesla, čím sa pripojím a vidím súbor `secret.txt`. Pomocou `get secret.txt` si ho stiahnem. Po zobrazení obsahu získavam tajomstvo.

## 10 Tajomstvo F

Začal som prechádzať servery (študentské nie) s otvoreným portom `ssh`. Skúšal som sa na nich pripájať, server 192.168.122.227 mi odpovedá že sa mám prihlásiť pod študentským účtom alebo ako `teacher`. Skúšam teda `ssh student@192.168.122.227` a rôzne heslá, napr. password, student, 12345678, asdfghjkl, atď. , bez úspechu. Pokúšam sa teda pripojiť ako `teacher`, kde pri zadaní hesla `teacher` uspejem. Prehľadávam súbory pomocou `find / -type f | grep secret` ale nič, podobne prehľadávam obsahy súborov, kde hľadám reťazec Tajemství, stále nič. Skúšam aj ako `sudo`, zadám heslo `teacher`, systém ale ma upozorní že nemám právo spúšťať daný príkaz ako `root`. Existuje ale celkom nová zraniteľnosť `sudo`, o ktorej som nedávno čítal, ktorá umožní zmeniť `UID` užívateľa na `UID` užívateľa `root` pomocou `-u#-1`. Zadávam `sudo -u#-1 find / -type f | grep secret`, vo výsledku sa mi objaví ďalší súbor, ktorý som bez `sudo` nedostal, a to súbor `/root/secret.txt`. Zadaním príkazu `sudo -u#-1 cat /root/secret.txt` získavam tajomstvo.

## 11 Tajomstvo J

Posledné tajomstvo som získal pomocou brute-force prihlasovania na jednotlivé servery, kde beží `ssh` a ešte som sa tam zatiaľ nedostal. Podarilo sa mi prihlásiť na stanicu 192.168.122.77 pomocou užívateľského mena a aj hesla `root`. Po prihlásení v domovskom adresári bol súbor `secret.txt`, ktorý obsahoval tajomstvo.