

Bezpečnost informačních systémů – projekt 1

Vysoké učení technické v Brně

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

18. 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
41326/tcp closed unknown
41327/tcp closed unknown
```

41328/tcp closed unknown
41329/tcp closed unknown
41330/tcp closed unknown
41331/tcp closed unknown
41332/tcp closed unknown
41333/tcp closed unknown
41334/tcp closed unknown
41335/tcp closed unknown
41336/tcp closed unknown
41337/tcp open unknown

2 Získání jednotlivých tajemství