



Jesenji semestar, 2022/23

PREDMET: IT381 - Zaštita i bezbednost informacija

Domaći Zadatak br. 5

Student: **Aleksa Cekić 4173**

Profesor: **dr Milena Bogdanović**

Asistent: **mr Goran Stamenović**

Datum izrade: **14.03.2023**

Tekst Zadataka

1. Nmap

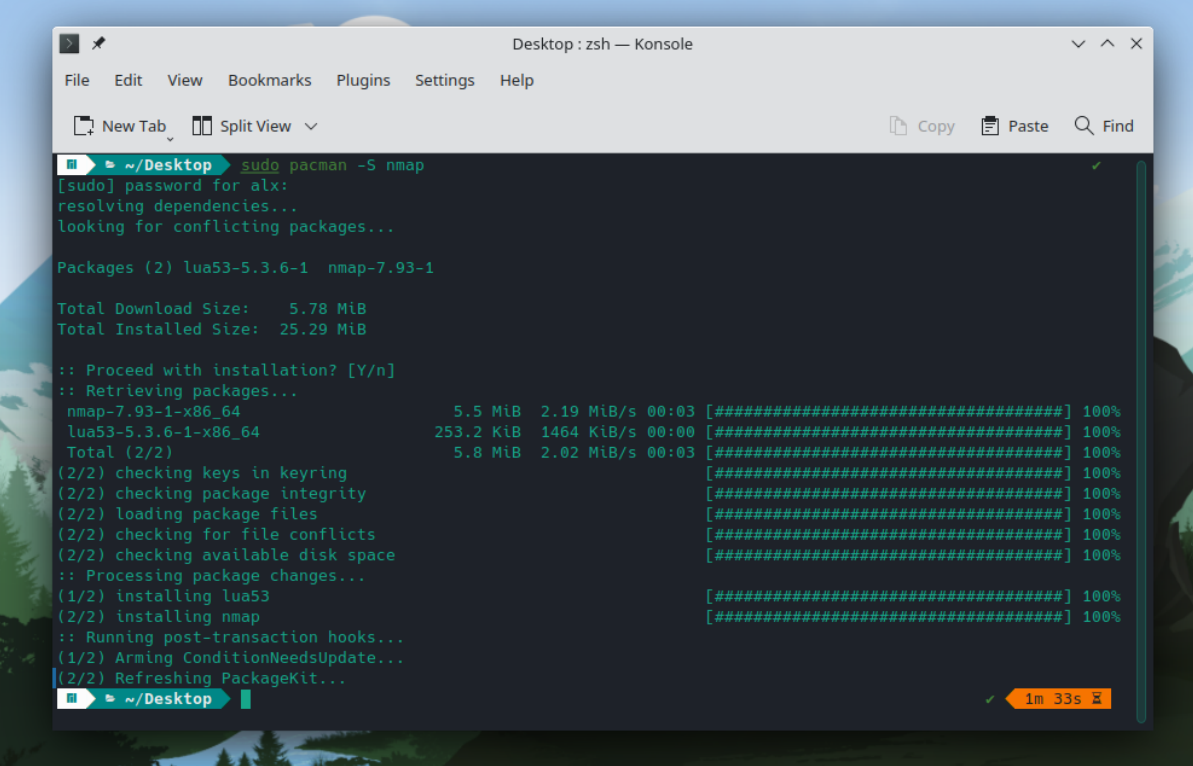
2. Wireshark Zadatak: Uraditi kompletno skeniranje vaše mreže koristeći komandu `nmap -sP 192.168.1.1/24` I uporediti sa skeniranjem mreže preko porta 80 (`nmap -sP -PT80 192.168.1.1/24`). Skenirajte jedan računar a predstavite se kao neko drugi – spoofing (`nmap -sS „victim“ -D „spoof“`). Skenirajte svoj računar, koji portovi su mu otvoreni koristeći komandu `nmap localhost`.

Zadatak: Uraditi kompletno skeniranje vaše mreže koristeći komandu `nmap -sP 192.168.1.1/24` I uporediti sa skeniranjem mreže preko porta 80 (`nmap -sP -PT80 192.168.1.1/24`). Skenirajte jedan računar a predstavite se kao neko drugi – spoofing (`nmap -sS „victim“ -D „spoof“`).

Rešenje zadataka

Za prikaz ovog domaćeg zadatka koristio sam O.S. Manjaro Linux.

Instaliranje nmap paketa preko packet manager-a.



```
Desktop : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help

New Tab Split View Copy Paste Find

~/Desktop sudo pacman -S nmap
[sudo] password for alx:
resolving dependencies...
looking for conflicting packages...

Packages (2) lua53-5.3.6-1 nmap-7.93-1

Total Download Size: 5.78 MiB
Total Installed Size: 25.29 MiB

:: Proceed with installation? [Y/n]
:: Retrieving packages...
nmap-7.93-1-x86_64 5.5 MiB 2.19 MiB/s 00:03 [#####] 100%
lua53-5.3.6-1-x86_64 253.2 KiB 1464 KiB/s 00:00 [#####] 100%
Total (2/2) 5.8 MiB 2.02 MiB/s 00:03 [#####] 100%
(2/2) checking keys in keyring [#####] 100%
(2/2) checking package integrity [#####] 100%
(2/2) loading package files [#####] 100%
(2/2) checking for file conflicts [#####] 100%
(2/2) checking available disk space [#####] 100%
:: Processing package changes...
(1/2) installing lua53 [#####] 100%
(2/2) installing nmap [#####] 100%
:: Running post-transaction hooks...
(1/2) Arming ConditionNeedsUpdate...
(2/2) Refreshing PackageKit...

~/Desktop 1m 33s
```

```
... Running post-transaction hooks...
~ /Desktop sudo nmap -sP 192.168.1.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 18:28 EDT
Nmap scan report for 192.168.1.0 (192.168.1.0)
Host is up (0.0023s latency).
Nmap scan report for csp1.zte.com.cn (192.168.1.1)
Host is up (0.0029s latency).
Nmap scan report for 192.168.1.3 (192.168.1.3)
Host is up (0.0012s latency).
Nmap scan report for huawei_p10_lite-50994eb3b (192.168.1.4)
Host is up (0.0014s latency).
Nmap scan report for huawei_y6s-ab1f677c1d1de8 (192.168.1.5)
Host is up (0.0014s latency).
Nmap scan report for uredaj-a32-korisnika-jana (192.168.1.6)
Host is up (0.00038s latency).
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.00033s latency).
Nmap scan report for desktop-qbdtnnr (192.168.1.8)
Host is up (0.00031s latency).
Nmap scan report for desktop-0839opl (192.168.1.9)
Host is up (0.0034s latency).
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.0014s latency).
```

```
...
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.248 (192.168.1.248)
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.249 (192.168.1.249)
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.250 (192.168.1.250)
Host is up (0.0020s latency).
Nmap scan report for 192.168.1.251 (192.168.1.251)
Host is up (0.0019s latency).
Nmap scan report for 192.168.1.252 (192.168.1.252)
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.253 (192.168.1.253)
Host is up (0.0011s latency).
Nmap scan report for 192.168.1.254 (192.168.1.254)
Host is up (0.0023s latency).
Nmap scan report for 192.168.1.255 (192.168.1.255)
Host is up (0.0023s latency).
Nmap done: 256 IP addresses (255 hosts up) scanned in 3.59 seconds
```

```
~ nmap -sP -PT80 192.168.1.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 18:54 EDT
Nmap scan report for csp3.zte.com.cn (192.168.1.1)
Host is up (0.0077s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 1.94 seconds
```

Traženje operativnih sistema na mreži

```
alx@kali:~$ sudo nmap -O 192.168.1.1 192.168.1.255
[sudo] password for alx:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 18:56 EDT
Nmap scan report for csp1.zte.com.cn (192.168.1.1)
Host is up (0.0011s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp    open  https
52869/tcp open  unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge[general purpose]
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for 192.168.1.255 (192.168.1.255)
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.255 (192.168.1.255) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 11.21 seconds
```

```
alx@kali:~$ sudo nmap -sS 192.168.1.1
[sudo] password for alx:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 18:33 EDT
Nmap scan report for csp3.zte.com.cn (192.168.1.1)
Host is up (0.0032s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp    open  https
52869/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 5.42 seconds
```

```
nmap localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 18:34 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000096s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
631/tcp   open ipp
```

Prikazani paketi u program Wireshark.

1888	2.852436715	10.0.2.15	192.168.1.213	TCP	74 60246 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1889	2.852769533	10.0.2.15	192.168.1.175	TCP	74 47588 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1890	2.853346932	10.0.2.15	192.168.1.221	TCP	74 41484 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1891	2.853642425	10.0.2.15	192.168.1.224	TCP	74 55226 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1892	2.853996167	10.0.2.15	192.168.1.179	TCP	74 38816 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1893	2.854292411	10.0.2.15	192.168.1.190	TCP	74 52622 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1894	2.854609747	10.0.2.15	192.168.1.229	TCP	74 55464 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1895	2.854960281	10.0.2.15	192.168.1.232	TCP	74 55318 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1896	2.858961454	10.0.2.15	192.168.1.61	TCP	74 52782 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1897	2.858420964	10.0.2.15	192.168.1.61	TCP	74 44572 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...	...
1898	2.858769718	10.0.2.15	192.168.1.66	TCP	74 54478 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.859119194	10.0.2.15	192.168.1.66	TCP	74 50826 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...	...
1899	2.859446637	10.0.2.15	192.168.1.69	TCP	74 34894 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.859924209	10.0.2.15	192.168.1.69	TCP	74 39886 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...	...
1899	2.861089441	10.0.2.15	192.168.1.240	TCP	74 44864 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.862221289	10.0.2.15	192.168.1.216	TCP	74 53530 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.862966973	10.0.2.15	192.168.1.218	TCP	74 48222 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.862279819	10.0.2.15	192.168.1.208	TCP	74 33896 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.8627629812	10.0.2.15	192.168.1.213	TCP	74 68258 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.866735159	10.0.2.15	192.168.1.221	TCP	74 41498 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.862878438	10.0.2.15	192.168.1.224	TCP	74 55242 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.864343748	10.0.2.15	192.168.1.229	TCP	74 55472 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.866011676	10.0.2.15	192.168.1.232	TCP	74 55332 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.867278363	10.0.2.15	192.168.1.216	TCP	74 53532 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.868021761	10.0.2.15	192.168.1.218	TCP	74 48228 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	2.869618739	10.0.2.15	192.168.1.240	TCP	74 44872 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	...
1899	3.079215517	10.0.2.15	192.168.1.1	DNS	84 Standard query 0x6239 PTR 1.1.168.192.in-addr.arpa	...
1899	3.089973859	192.168.1.1	10.0.2.15	DNS	171 Standard query response 0x6239 PTR 1.1.168.192.in-addr.arpa P...	...
1899	3.095708365	192.168.1.3	10.0.2.15	TCP	60 80 → 52616 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	...
1899	3.123649609	192.168.1.8	10.0.2.15	TCP	60 80 → 43252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	...
1899	3.438017945	192.168.1.8	10.0.2.15	TCP	60 443 → 39292 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	...
1899	3.538842476	192.168.1.8	10.0.2.15	TCP	60 443 → 39384 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	...