

Data security testing

Lab 2: Port scan

Timo Lehosvuori, M3426@student.jamk.fi

Raportti

Data Security Testing, Markku Vajaranta

Syksy 2020

Tieto- ja viestintätekniikan koulutusohjelma

Tekniikan ja liikenteen ala

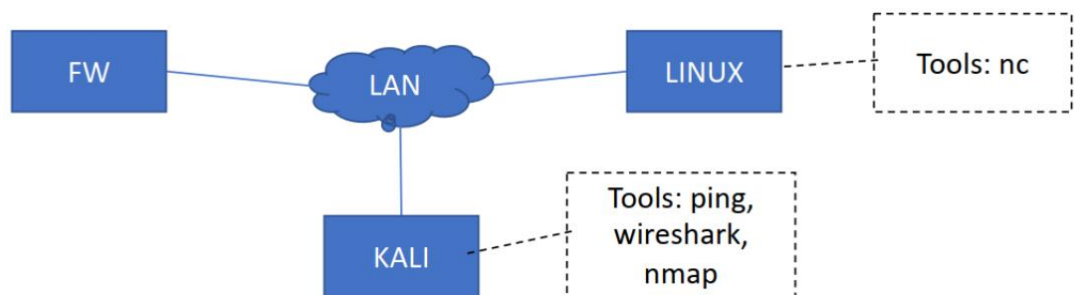
Sisällysluettelo

1	Port scans.....	2
1.1	Topologia ja ip-avaruudet.....	2
2	Tehtävä 1	3
3	Tehtävä 2	8
4	Tehtävä 3	9
5	Tehtävä 4	11
6	Tehtävä 5	13

1 Port scans

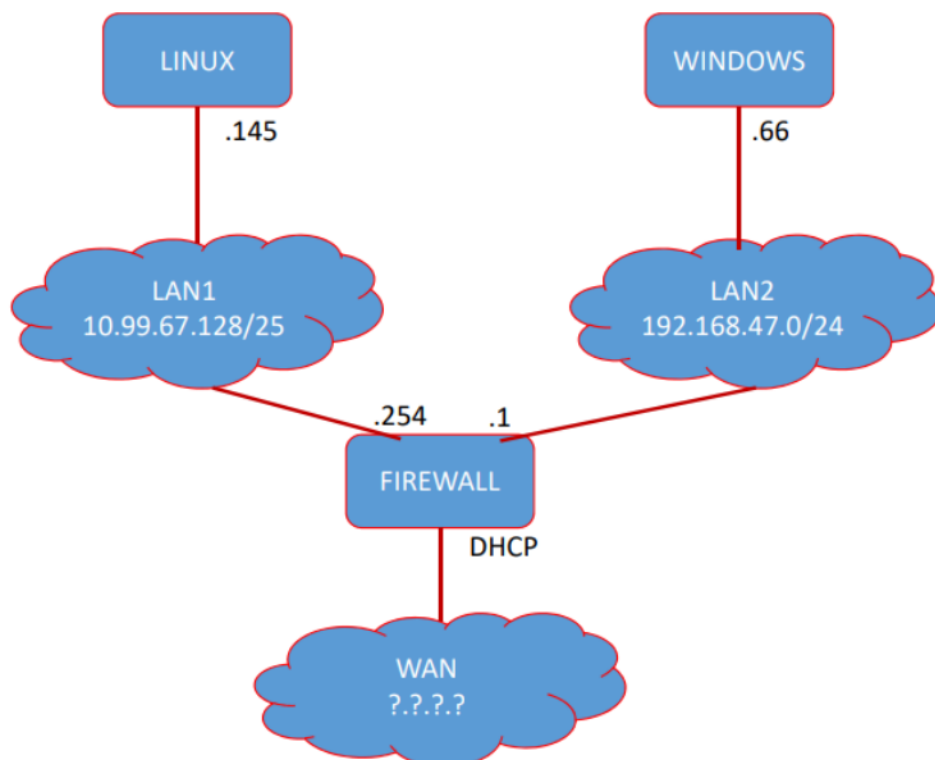
1.1 Topologia ja ip-avaruudet

Verkon topologia. Kuvan LAN-verkko on sama kuin LAN1-verkko



Kuva 1: Topologia.

Ip-avaruudet ja osoitteet



Kuva 2: Verkkojen koko ja koneiden ip-osoitteet.

2 Tehtävä 1

- start netcat on Linux (terminal, nc -lk -p888, starts netcat listener on port 888)
- start wireshark on KALI
- run following scans and look from wireshark what happens
 - nmap -sL x.x.x.x/yy (scan whole network)
 - nmap -sn x.x.x.x/yy (scan whole network)
 - nmap -sT -p888 x.x.x.x (scan single target)
 - nmap -sS -p888 x.x.x.x (scan single target)
 - nmap -sU -p888 x.x.x.x (scan single target) - what did you get as a result? Why?
 - nmap -sV -p888 x.x.x.x (scan single target) - what do you see in netcat listener? Why?

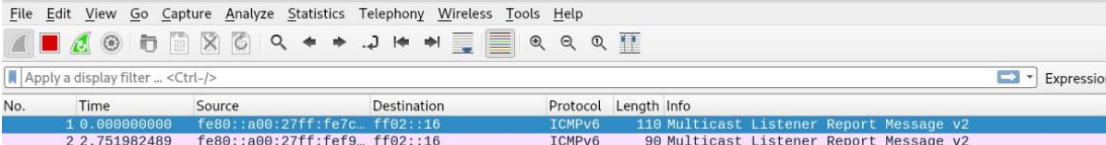
Kuva 3: Tehtävä 1.

Ensimmäisenä käynnistin kaikki tarvittavat virtuaalikoneet: Linux (10.99.67.145), Palomuuuri (10.99.67.254) ja Kali linux (10.99.67.132), sekä varmistin että kaikki koneet ovat samassa LAN-verkossa. Seuraavaksi laitoin netcatin päälle Linuxista,

```
root@localhost ~]# nc -lk -p888
```

Kuva 4: Netcat.

käynnistin wiresharkin Kalista ja aloitin scannailun.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::a00:27ff:fe7c...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
2	2.751982489	fe80::a00:27ff:fef9...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

Kuva 5: Wireshark.

Ensimmäisen skannasin koko LAN1-verkon komennolla nmap -sL 10.99.67.128/25, missä parametri -sL tarkoittaa "list scan". Komento tulostaa kaikki koneet verkosta (mitkä se löytää).

```
Nmap scan report for 10.99.67.253
Nmap scan report for TheGreatFirewall.localdomain (10.99.67.254)
Nmap scan report for 10.99.67.255
Nmap done: 256 IP addresses (0 hosts up) scanned in 6.51 seconds
root@kali:~#
```

Kuva 6: Nmap -sL.

Tulosteesta nähdään, että nmap löysin vain palomuurin. Wiresharkissa nmap näkyi arp kyselyinä ja muutaman DSN-kyselyinä.

670	147.076489491	PcsCompu_7c:8e:8e	PcsCompu_f9:e8:f0	ARP	42 Who has 10.99.67.254? Tell 10.99.67.132
671	147.076838689	PcsCompu_f9:e8:f0	PcsCompu_7c:8e:8e	ARP	60 10.99.67.254 is at 08:00:27:f9:e8:f0

Kuva 7: ARP-kysely.

654	142.062892831	10.99.67.132	10.99.67.254	DNS	84 Standard query
655	142.062925488	10.99.67.132	10.99.67.254	DNS	84 Standard query
656	142.062970740	10.99.67.132	10.99.67.254	DNS	84 Standard query
657	142.063086278	10.99.67.254	10.99.67.132	DNS	142 Standard query
658	142.063259670	10.99.67.254	10.99.67.132	DNS	142 Standard query

Kuva 8: DNS-kysely.

Seuraavaksi skannasin saman verkon käyttäen komentoa `nmap -sn 10.99.67.128/25`, missä parametri `-sn` tarkoittaa "No port scan". Komento tulostaa kanssa kaikki koneet verkosta, mutta on hieman enemmän "tunkeileva".

```
sudouser@kali:~$ nmap -sn 10.99.67.128/25
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-23 12:23 EDT
Nmap scan report for 10.99.67.132
Host is up (0.00055s latency).
Nmap scan report for 10.99.67.145
Host is up (0.00043s latency).
Nmap scan report for TheGreatFirewall.localdomain (10.99.67.254)
Host is up (0.0019s latency).
Nmap done: 128 IP addresses (3 hosts up) scanned in 1.99 seconds
sudouser@kali:~$
```

Kuva 9: Nmap -sn.

Tulosteesta nähdään että, yhden koneen sijaan löytyi kolme konetta, eli kaikki koneet mitkä verkossa olivat. Wiresharkissa skannaus näkyi monena ARP-kyselyinä

2166	1099.6483104...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.254? Tell 10.99.67.132
2167	1099.6484531...	PcsCompu_f9:e8:f0	PcsCompu_7c:8e:8e	ARP	60 10.99.67.254 is at 08:00:27:f9:e8:f0
2168	1099.6509809...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.140? Tell 10.99.67.132
2169	1099.6510170...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.141? Tell 10.99.67.132
2170	1099.6510303...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.142? Tell 10.99.67.132
2171	1099.6510422...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.143? Tell 10.99.67.132
2172	1099.6510607...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.145? Tell 10.99.67.132
2173	1099.6510817...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.146? Tell 10.99.67.132
2174	1099.6511003...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.156? Tell 10.99.67.132
2175	1099.6511422...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.157? Tell 10.99.67.132
2176	1099.6511721...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.158? Tell 10.99.67.132
2177	1099.6512160...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.159? Tell 10.99.67.132
2178	1099.6512398...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.160? Tell 10.99.67.132
2179	1099.6512441...	PcsCompu_bb:7d:d0	PcsCompu_7c:8e:8e	ARP	60 10.99.67.145 is at 08:00:27:bb:7d:d0
2180	1099.6512558...	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.161? Tell 10.99.67.132

Kuva 10: ARP-kysely (nmap -sn).

Jatkoi skannauksia, mutta siirryin koko verkon skannaamisesta yksittäisen koneen skannailuun. Päätin skannata Linuxia ja käytin komentoa `nmap -sT -p888`

10.99.67.145, missä parametri -sT tarkoittaa "TCP connect scan" ja -p888 porttia 888.

Komento siis jo skannaa porttia, pelkän "host" listauksen sijaan.

```

sudouser@kali:~$ nmap -sT -p888 10.99.67.145
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-19 07:45 EDT
Nmap scan report for 10.99.67.145
Host is up (0.00050s latency).

PORT      STATE SERVICE
888/tcp   open  accessbuilder

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
sudouser@kali:~$

```

Kuva 11: Nmap -sT -p888.

Komento antoi tulokseksi avonaisen portin 888 (netcat). Wiresharkissa tämä näkyi jo melko sekavana, mutta sisälsi myös tutun ARP-kyselyn.

1	0.000000000	10.99.67.132	10.99.67.145	TCP	74 56844 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
2	0.000107924	10.99.67.132	10.99.67.145	TCP	74 47404 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
3	0.000408504	10.99.67.145	10.99.67.132	TCP	74 80 → 56844 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
4	0.000408592	10.99.67.145	10.99.67.132	TCP	60 443 → 47404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.000426209	10.99.67.132	10.99.67.145	TCP	66 56844 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1
6	0.000489946	10.99.67.132	10.99.67.145	TCP	66 56844 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1
7	0.000764164	10.99.67.132	10.99.67.254	DNS	85 Standard query 0xb0f9 PTR 145.67.99.10.in-addr.arpa
8	0.001136942	10.99.67.254	10.99.67.132	DNS	144 Standard query response 0xb0f9 No such name PTR 145.
9	0.001215967	10.99.67.132	10.99.67.145	TCP	74 46758 → 888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
10	0.001511533	10.99.67.145	10.99.67.132	TCP	74 888 → 46758 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460
11	0.001526093	10.99.67.132	10.99.67.145	TCP	66 46758 → 888 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1
12	0.001563724	10.99.67.132	10.99.67.145	TCP	66 46758 → 888 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
13	5.004793310	PcsCompu_bb:7d:d0	PcsCompu_7c:8e:8e	ARP	60 Who has 10.99.67.132? Tell 10.99.67.145
14	5.004807699	PcsCompu_7c:8e:8e	PcsCompu_bb:7d:d0	ARP	42 10.99.67.132 is at 08:00:27:7c:8e:8e
15	5.240708867	PcsCompu_7c:8e:8e	PcsCompu_f9:e8:f0	ARP	42 Who has 10.99.67.254? Tell 10.99.67.132
16	5.240801858	PcsCompu_7c:8e:8e	PcsCompu_bb:7d:d0	ARP	42 Who has 10.99.67.145? Tell 10.99.67.132
17	5.241120556	PcsCompu_f9:e8:f0	PcsCompu_7c:8e:8e	ARP	60 10.99.67.254 is at 08:00:27:f9:e8:f0
18	5.241120633	PcsCompu_bb:7d:d0	PcsCompu_7c:8e:8e	ARP	60 10.99.67.145 is at 08:00:27:bb:7d:d0
19	8.2990605369	fe80::a00:27ff:fe90::1	ff02::1	ICMPv6	166 Router Advertisement from 08:00:27:f9:e8:f0
20	8.300811026	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24::	DNS	105 Standard query 0x9960 PTR 145.67.99.10.in-addr.arpa
21	8.300972624	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24::	DNS	74 Standard query response 0x9960 Refused

Kuva 12: Wireshark tuloste (nmap -sT -p888).

Jatkoin Linuxin skannailua komennolla nmap -sS -p888 10.99.67.145, parametri -sS tarkoittaa "TCP SYN stealth scan".

```

root@kali:~# nmap -sS -p888 10.99.67.145
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-13 04:58 EDT
Nmap scan report for 10.99.67.145
Host is up (0.00038s latency).
Jarmo-
PORT      STATE SERVICE
888/tcp   filtered accessbuilder
MAC Address: 08:00:27:BB:7D:D0 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
root@kali:~#

```

Kuva 13: Nmap -sS -p888.

Tuloste ei juuri eroa aiemmasta TCP-skannista muuten kuin kestoaltaan, eikä skanni saanut selvyttä oliko portti auki vai ei. Wiresharkissa ei näkynyt muuta kuin ARP-kysely.

8	9.776709900	fe80::a00:27ff:fe7c...	ff02::16	ICMPv6	110 Multicast Listener Report Message v2
9	12.553083455	PcsCompu_7c:8e:8e	Broadcast	ARP	42 Who has 10.99.67.145? Tell 10.99.67.132
10	12.553440671	PcsCompu_bb:7d:d0	PcsCompu_7c:8e:8e	ARP	60 10.99.67.145 is at 08:00:27:bb:7d:d0
11	12.628446664	fe80::a00:27ff:fe7c...	ff02::1:ff00:0	ICMPv6	86 Neighbor Solicitation for :: from 08:00:27:7c:8e:8e
12	12.628531588	fe80::afd1:63d7:9f25	fe80::afd1:63d7:9f25	DNS	105 Standard query 0x41a2 PTR 145.67.99.10.in-addr.arpa
13	12.628923709	fe80::afd1:63d7:9f25	fe80::afd1:63d7:9f25	DNS	74 Standard query response 0x41a2 Refused
14	12.628977371	fe80::a00:27ff:fe7c...	ff02::1:ff00:0	ICMPv6	86 Neighbor Solicitation for :: from 08:00:27:7c:8e:8e
15	15.159408783	fe80::afd1:63d7:9f25	fe80::afd1:63d7:9f25	DNS	105 Standard query 0x41a3 PTR 145.67.99.10.in-addr.arpa
16	15.159804092	fe80::afd1:63d7:9f25	fe80::afd1:63d7:9f25	DNS	74 Standard query response 0x41a3 Refused

Kuva 14: Wireshark (nmap -sS -p888).

Tämän jälkeen skannasin koneen vielä parametreillä -sU ja sV, missä sU tarkoittaa "UDP scan" ja sV "Version detection".

```
root@kali:~# nmap -sU -p888 10.99.67.145
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-13 05:03 EDT
Nmap scan report for 10.99.67.145
Host is up (0.00044s latency).
Jarmo-
PORT      STATE      SERVICE
888/udp   filtered  accessbuilder
MAC Address: 08:00:27:BB:7D:D0 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 6.72 seconds
root@kali:~#
```

Kuva 15: Nmap -sU -p888.

```
sudouser@kali:~$ sudo nmap -sV -p888 10.99.67.145
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-19 07:05 EDT
Nmap scan report for 10.99.67.145
Host is up (0.00054s latency).
PORT      STATE      SERVICE      VERSION
888/tcp   open      accessbuilder?
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port888-TCP:V=7.91%I=7%D=10/19%Time=5F8D7312P=x86_64-pc-linux-gnu%r(NU
SF:LL,1,"\\n")%r(GetRequest,1,"\\n");
MAC Address: 08:00:27:BB:7D:D0 (Oracle VirtualBox virtual NIC)
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.20 seconds
sudouser@kali:~$
```

Kuva 16: Nmap -sV -p888.

Skannaus parametrilla -sU antaa tuloksen 888/udp eli, portti 888 on auki ja tukee protokollaa UDP. Tulos on juuri sellainen mitä odotin. Haattiinko tässä jotain muuta tulosta? Tehtävänanto viittaisi siihen.

Skannaus parametrilla -sV pitäisi näkyä netcatissä, mutta Linuxin palomuuuri esti tämän joten, joudin sammuttamaan palomuurin komennolla "systemctl stop firewallld".

```
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]# systemctl status firewalld
■ firewalld.service - firewalld - dynamic firewall manager
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; vendor preset: enabled)
   Active: inactive (dead) since Fri 2020-10-23 11:04:11 CEST; 1min 11s ago
```


3 Tehtävä 2

- Run NMAP from KALI terminal
 - Run ICMP -scan against target network
 - Run TCP and UDP scans against target(s)
 - Run Service detection scan against target(s)
- ! Use output parameter to save results to file (-oA filename, -oX filename, etc)

Kuva 20: Tehtävä 2.

Jatkoin Linuxin skannailua ja ajoin kolme skannausta, mutta tallensin tulokset tiedostoon käyttämällä parametria -oG.

ICMP -scan: `sudo nmap -sP -PI -oG icmp.txt 10.99.67.129/25`. Parametri -sP tarkoittaa, että nmap tekee vain ping skannauksen ja parametri -PI taas kertoo, että nmap lähettää "echo request" viestejä

```

GNU nano 5.2                                icmp.txt
# Nmap 7.91 scan initiated Fri Oct 23 12:28:21 2020 as: nmap -sP -PI -oG icmp.txt 10.99.67.128/25
Host: 10.99.67.145 () Status: Up
Host: 10.99.67.254 () Status: Up
Host: 10.99.67.132 () Status: Up
# Nmap done at Fri Oct 23 12:28:23 2020 -- 128 IP addresses (3 hosts up) scanned in 1.91 seconds

```

Kuva 21: ICMP-scan.

TCP and UDP scan: `sudo nmap -sU -sT -p1-100 -Pn -T4 -oG udp_tcp.txt 10.99.67.145`. Parametri -p1-100 tarkoittaa, että skannaus kohdistuu portteihin 1-100, -Pn tarkoittaa, ettei nmap tee ping skannausta ja -T4 (T1-T5) kuvaa nopeutta (Isompi on nopeampi ja helpommin huomattava). Tiedosto oli helpompi lukea komennolla "cat" sillä komennolla "nano" kaikki teksti tulee yhdelle riville.

```

sudouser@kali:~$ cat udp_tcp.txt
# Nmap 7.91 scan initiated Mon Oct 19 08:28:59 2020 as: nmap -sU -sT -p1-100 -Pn -T4 -oG udp_tcp.txt 10.99.67.145
Host: 10.99.67.145 () Status: Up
Host: 10.99.67.145 () Ports: 22/open/tcp//ssh///, 80/open/tcp//http///, 9/open|filtered/udp//discard///, 11/open|filtered/udp//systat///, 17/open|filtered/udp//qotd///, 23/open|filtered/udp//telnet///, 29/open|filtered/udp//msg-icp///, 32/open|filtered/udp///// , 34/open|filtered/udp///// , 35/open|filtered/udp//priv-print///, 42/open|filtered/udp//nameserver///, 46/open|filtered/udp//mpm-snd///, 52/open|filtered/udp//xns-time///, 56/open|filtered/udp//xns-auth///, 58/open|filtered/udp//xns-mail///, 69/open|filtered/udp//tftp///, 74/open|filtered/udp//netrjs-4///, 75/open|filtered/udp//priv-dial///, 76/open|filtered/udp//d eos///, 79/open|filtered/udp//finger///, 83/open|filtered/udp//mit-ml-dev///, 84/open|filtered/udp//ctf// /, 87/open|filtered/udp///// , 96/open|filtered/udp//dixie///, 98/open|filtered/udp//tacnews/// Ignored S
tate: closed (175)
# Nmap done at Mon Oct 19 08:30:14 2020 -- 1 IP address (1 host up) scanned in 75.02 seconds
sudouser@kali:~$

```

Kuva 22: TCP/UDP scan.

Service detection scan: `sudo nmap -sV -p1-65535 -T4 -oG sv.txt 10.99.67.145`

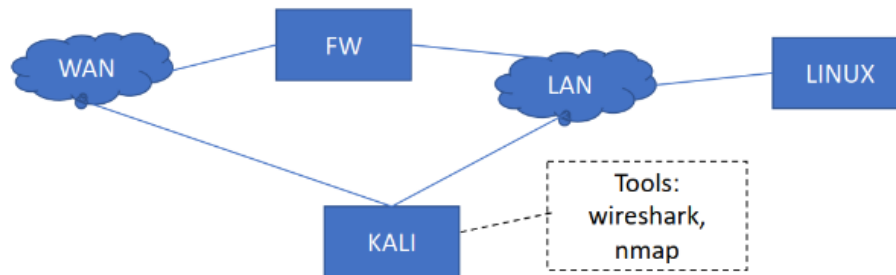
```

GNU nano 5.2 sv.txt
# Nmap 7.91 scan initiated Mon Oct 19 08:50:31 2020 as: nmap -sV -p1-65535 -T4 -oG sv.txt 10.99.67.145
Host: 10.99.67.145 () Status: Up
Host: 10.99.67.145 () Ports: 22/open/tcp//ssh//OpenSSH 7.4 (protocol 2.0)/, 80/open/tcp//http//Apache
# Nmap done at Mon Oct 19 08:50:44 2020 -- 1 IP address (1 host up) scanned in 12.57 seconds

```

Kuva 23: Service detection scan.

4 Tehtävä 3



Kuva 24: Uusi topologia

- Start wireshark on LAN interface
- Generate full scan from WAN to firewall interface
- Look from the Wireshark if you see any traffic from your KALI machine WAN-network ip-address

Kuva 25: Tehtävä 3.

Tehtävää kolme varten lisäsin Kali Linuxiin uuden verkkoadapterin, jotta voin skannata palomuuria ulkoverkosta. Laitoin myös Wiresharkin kuuntelemaan sisäverkkoa. Tehtävänannossa pyydetään tekemään "full scan" mutta ei tarkenneta mitä se käytännössä tarkoittaa nii käytin komentoa `nmap -e -eth1 -A -p1-65535 192.168.43.72`. Parametri `-e -eth1` tarkoittaa, että nmap skannaa adapterilla eth1 ja parametri `-A` sisältää komennot: `-O "OS detection"`, `-sV "Version detection"`, `-sC "Script scan"` ja `-traceroute`.

```

sudouser@kali:~$ nmap -e eth1 -A -p1-65535 192.168.43.72
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-22 09:13 EDT
Nmap scan report for TheGreatFirewall (192.168.43.72)
Host is up (0.0011s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         nginx
|_http-title: Login
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-cert: Subject: commonName=IE8WIN7
|_Not valid before: 2020-10-05T19:23:01
|_Not valid after: 2021-04-06T19:23:01
|_ssl-date: 2020-10-22T13:15:56+00:00; +3s from scanner time.

Host script results:
|_clock-skew: 2s

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.86 seconds
sudouser@kali:~$

```

Kuva 26: Nmap ulkoverkosta.

Portti skannaus kertoo, että portit 80 ja 3389 ovat auki. Portissa 3389 pyörii ms-wbt-serveri, joka tarkoittaa Remote Desktop protokollaa. Wiresharkista näkee, että mikään skannaus ei päässyt sisäverkkoon asti. Tästä voidaan päätellä, että palomuurin säännöt toimivat ja estivät skannauksen pääsemästä sisäverkkoon asti.

Capturing from eth0					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	fe80::a00:27ff:fe9...	ff02::1	ICMPv6	166 Router Advertisement from 08:00:27:f9:e8:f0
2	0.001912021	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	105 Standard query 0x5b28 PTR 145.67.99.10.in-addr.arpa
3	0.002326534	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	74 Standard query response 0x5b28 Refused
4	5.011849755	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	105 Standard query 0x5b28 PTR 145.67.99.10.in-addr.arpa
5	5.012064037	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	74 Standard query response 0x5b28 Refused
6	6.303041498	fe80::a00:27ff:fe9...	ff02::1	ICMPv6	166 Router Advertisement from 08:00:27:f9:e8:f0
7	6.304193878	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	105 Standard query 0x9771 PTR 145.67.99.10.in-addr.arpa
8	6.304453467	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	74 Standard query response 0x9771 Refused
9	6.451404046	fe80::a00:27ff:fe9...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
10	8.453044708	fe80::a00:27ff:fe9...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
11	10.021599456	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	ICMPv6	86 Neighbor Solicitation for fe80::afd1:63d7:9f23:aa11
12	10.021855932	fe80::a00:27ff:fe9...	fe80::afd1:63d7:9f24	ICMPv6	78 Neighbor Advertisement fe80::afd1:63d7:9f23:aa11 (rt
13	11.312986015	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	105 Standard query 0x9771 PTR 145.67.99.10.in-addr.arpa
14	11.313211746	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	74 Standard query response 0x9771 Refused
15	24.711483811	fe80::a00:27ff:fe9...	ff02::1	ICMPv6	166 Router Advertisement from 08:00:27:f9:e8:f0
16	24.712612875	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	105 Standard query 0x05f0 PTR 145.67.99.10.in-addr.arpa
17	24.712854622	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	74 Standard query response 0x05f0 Refused
18	29.721725085	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	105 Standard query 0x05f0 PTR 145.67.99.10.in-addr.arpa
19	29.721956373	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	74 Standard query response 0x05f0 Refused
20	34.738179166	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	ICMPv6	86 Neighbor Solicitation for fe80::afd1:63d7:9f23:aa11
21	34.738395120	fe80::a00:27ff:fe9...	fe80::afd1:63d7:9f24	ICMPv6	78 Neighbor Advertisement fe80::afd1:63d7:9f23:aa11 (rt
22	39.923441530	fe80::a00:27ff:fe9...	fe80::afd1:63d7:9f24	ICMPv6	86 Neighbor Solicitation for fe80::afd1:63d7:9f24 from
23	39.923909466	fe80::afd1:63d7:9f24	fe80::a00:27ff:fe9...	ICMPv6	78 Neighbor Advertisement fe80::afd1:63d7:9f24 (sol)
24	41.129958601	fe80::a00:27ff:fe9...	ff02::1	ICMPv6	166 Router Advertisement from 08:00:27:f9:e8:f0
25	41.130912158	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	105 Standard query 0x180a PTR 145.67.99.10.in-addr.arpa
26	41.148178430	fe80::afd1:63d7:9f24	fe80::afd1:63d7:9f24	DNS	74 Standard query response 0x180a Refused
27	41.268803939	fe80::a00:27ff:fe9...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
28	44.069594542	fe80::a00:27ff:fe9...	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
29	44.941866738	fe80::afd1:63d7:9f24	fe80::a00:27ff:fe9...	ICMPv6	86 Neighbor Solicitation for fe80::a00:27ff:fe9:e8f0 f

Kuva 27: Wireshark LAN adapteri.

5 Tehtävä 4

More scans!

- Run NMAP scans also against the Windows machine, and other Firewall interface
- Document the results

Kuva 28: Tehtävä 4.

Jatkoi samalla linjalla kuin aikaisemmin eli, skannailin lisää. Tällä kertaa skannasin Windows 7 ja palomuurin LAN1 ja 2 rajapintoja.

Palomuurin LAN1 & 2 skannaukset: `nmap -A -p165535 10.99.67.254/192.168.47.1`.

```
sudouser@kali:~$ nmap -A -p1-65535 10.99.67.254
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-22 10:08 EDT
Nmap scan report for 10.99.67.254
Host is up (0.0010s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain Unbound
80/tcp    open  http   nginx
|_http-title: Login

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 203.11 seconds
sudouser@kali:~$
```

Kuva 29: Palomuurin LAN1 skannaus.

```
sudouser@kali:~$ nmap -A -p1-65535 192.168.47.1
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-22 10:14 EDT
Nmap scan report for 192.168.47.1
Host is up (0.0015s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain Unbound
80/tcp    open  http   nginx
|_http-title: Login

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 196.67 seconds
sudouser@kali:~$
```

Kuva 30: Palomuurin LAN2 skannaus.

Molemmat skannaukset ovat identtiset. Portit 53 ja 80 ovat auki molemmissa.

Windows 7 skannaus: `nmap -A -p1-65535 192.168.47.66`


```

sudouser@kali:~$ nmap -A -p1-65535 192.168.47.66
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-22 09:54 EDT
Stats: 0:02:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 73.74% done; ETC: 09:57 (0:00:55 remaining)
Stats: 0:04:26 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 88.08% done; ETC: 09:59 (0:00:36 remaining)
Stats: 0:06:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 58.82% done; ETC: 10:01 (0:00:22 remaining)
Nmap scan report for 192.168.47.66
Host is up (0.00068s latency).
Not shown: 65518 closed ports
PORT      STATE SERVICE          VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime          Microsoft Windows USA daytime
17/tcp    open  qotd             Windows qotd (English)
19/tcp    open  chargen
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds      Windows 7 Enterprise 7601 Service Pack 1 micros
t-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-cert: Subject: commonName=IE8WIN7
|_Not valid before: 2020-10-05T19:23:01
|_Not valid after: 2021-04-06T19:23:01
|_ssl-date: 2020-10-22T14:03:15+00:00; +2s from scanner time.
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found

```

Kuva 31: Windows skannaus 1.

```

47001/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49156/tcp open  msrpc            Microsoft Windows RPC
49158/tcp open  msrpc            Microsoft Windows RPC
Service Info: Host: IE8WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h45m03s, deviation: 3h30m02s, median: 1s
|_smb-os-discovery:
|_OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|_OS CPE: cpe:/o:microsoft:windows_7::sp1
|_Computer name: IE8WIN7
|_NetBIOS computer name: IE8WIN7\x00
|_Workgroup: WORKGROUP\x00
|_System time: 2020-10-22T07:03:05-07:00
|_smb-security-mode:
|_account_used: guest
|_authentication_level: user
|_challenge_response: supported
|_message_signing: disabled (dangerous, but default)
|_smb2-security-mode:
|_2.02:
|_Message signing enabled but not required
|_smb2-time:
|_date: 2020-10-22T14:03:02
|_start_date: 2020-10-22T13:53:46

Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 535.12 seconds
sudouser@kali:~$

```

Kuva 32: Windows skannaus 2.

Skannauksen tulosteesta nähdään että, Windows 7 koneella on monia portteja auki ja monta eri palvelua. Tuloksesta nähdään myös palveluiden ja käyttöjärjestelmän versiot. Palveluiden ja porttien määrä näkyi myös skannauksen kestossa, joka kesti n. 9 minuuttia.

6 Tehtävä 5

Validate results!

- With NMAP you can only find services that are running in targets!
- List all running network services by using netstat -command
 - from windows -machine
 - from linux -machine
- Are there any differences in listed network services an scanning results?

Kuva 33: Tehtävä 5.

Viimeisenä tehtävänä piti vertailla nmapin ja netsatin tuloksia. Ajoin "netstat" komennon Windows 7 ja Linux koneella. Komento ei antanut minulle minkäänlaista tulosta "winkkarilla". Ajattelin että se johtui siitä, kun en ollut käynnistänyt komentoriviä pääkäyttäjänä, mutta sekään ei ratkaissut ongelmaa. En löytänyt vikaan ratkaisua, joten en pystynyt vertailemaan tuloksia.



```

Administrator: Command Prompt
C:\Windows\system32>netstat
Active Connections
  Proto  Local Address           Foreign Address         State
  
```

Kuva 34: Netstat Windows.

Ajoin saman komennon Linuxilla ja komento tulosti minulle rivitolkulla eri portteja ja palveluita.


```

GNU nano 2.3.1      File: netstat.txt

Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp6      0      0 localhost.localdo:47792 fe80::afd1:63d7::domain ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags      Type       State       I-Node      Path
unix  2      [ ]      DGRAM          6914      /run/systemd/notify
unix  2      [ ]      DGRAM          6916      /run/systemd/cgroups$
unix  6      [ ]      DGRAM          6928      /run/systemd/journal$
unix 13      [ ]      DGRAM          6930      /dev/log
unix  2      [ ]      DGRAM          11490     /run/systemd/shutdown$
unix  3      [ ]      STREAM        CONNECTED  14704
unix  3      [ ]      DGRAM          12313
unix  3      [ ]      STREAM        CONNECTED  14705      /var/run/dbus/system$
unix  3      [ ]      DGRAM          12312
unix  3      [ ]      STREAM        CONNECTED  16558      /run/systemd/journal$
unix  2      [ ]      DGRAM          14123
unix  3      [ ]      STREAM        CONNECTED  14178
unix  3      [ ]      STREAM        CONNECTED  17608
unix  3      [ ]      STREAM        CONNECTED  17587
unix  3      [ ]      STREAM        CONNECTED  14431

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell

```

Kuva 35: Netstat Linux.

Linuxin tuloksia vertaillen huomataan että "netstat" antaa huomattavasti enemmän tietoa mitä palveluita koneella on, kun taas "nmap" antoi vain hieman. Ero johtuu siitä että "nmap" kertoo vain mitkä palvelut pyörivät koneella kun "netstat" taas kertoo kaikki.