VERKON VALVONTA: CASE-ESIMERKIT WIRESHARK JA NMAP

Johanna Hakonen

Sisällysluettelo

1 Johdanto

Kyberturvariskejä hallitaan esimerkiksi valvomalla tietoverkkoa hyödyntämällä erilaisia analysointityökaluja kuten kolmannen osapuolen ohjelmia, esimerkiksi Wiresharkia (Wireshark Foundation, 2025).

Toteutettiin verkonvalvonnan suunnitelmasta (liite 4a) poikkeavan verkkoliikenteen havaitseminen työasemassa Wiresharkilla siten, että tehdään Nmap-skannauksia samaan aikaan ja tutkitaan, miten skannaukset näkyvät. Ympäristönä käytettiin Windows-palvelinta ja -työasemaa sekä Kali Linux-konetta VMwaressa.

Käynnistettiin Windows-palvelin, päivitettiin VMware Tools ja Windows Updaten kautta Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.423.136.0). Käynnistettiin wks2-physio-työasema, päivitettiin VMware Tools. Poistettiin Wireshark 4.4.3 ja asennettiin versio 4.4.5 ja avattiin se. Käynnistettiin Kali Linux-kone ja tehtiin Nmap-skannauksia. Käytettiin Hack the Box -sivuston Network Enumeration with Nmap -moduulin (Hack the Box, 2025) komentoja ja ChatGPT:tä (OpenAI, 2025) selventämään joitain kohtia.

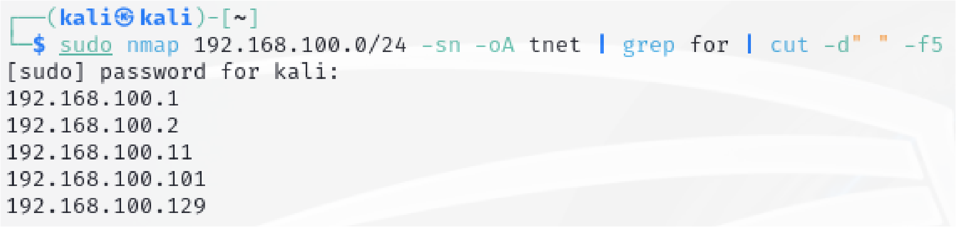
1.1 Kohteiden listaus

Aloitettiin tarkistamalla, mitkä IP-osoitteet ovat käytössä eli skannataan koko verkkoalue ilman porttiskannausta (-sn) (20250227_1 klo 13.47):

sudo nmap 192.168.100.0/24 -sn -oA tnet | grep for | cut -d" " -f5

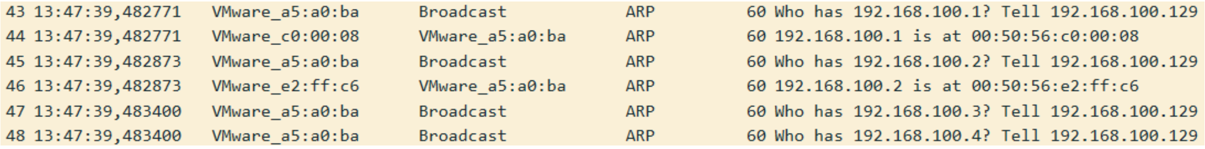
- -oA tnet: Tallentaa skannauksen tulokset kaikkiin kolmeen tiedostomuotoon: tnet.nmap (normaali tekstimuoto), tnet.gnmap (Grep-ystävällinen muoto) ja tnet.xml (XML-muoto)
- grep for: suodattaa rivit, jotka sisältävät sanan "for", kuten "Nmap scan report for 10.129.2.5"
- cut: Komento leikkaa rivin osiin määritellyn erotinmerkin avulla
- -d" ": erotinmerkkinä käytetään välilyöntiä
- -f5: valitaan rivin 5. kenttä eli IP-osoite

Tuloksena saatiin käytössä olevat IP-osoitteet: VMware 192.168.100.1, oletusyhdyskäytävä 192.168.100.2, palvelin 192.168.100.11, työasema 192.168.100.101 ja Linux-kone 192.168.100.129:



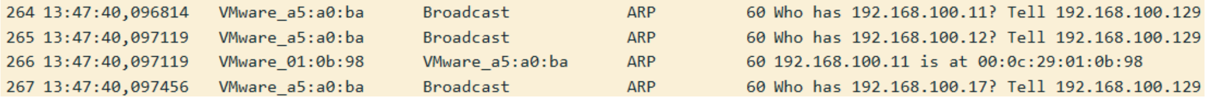
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.0/24 -sn -oA tnet | grep for | cut -d" " -f5
[sudo] password for kali:
192.168.100.1
192.168.100.2
192.168.100.11
192.168.100.101
192.168.100.129
```

Tämä komento lähettää lähiverkossa ensin ARP-pingin eikä ollenkaan ICMP-pingiä, jolloin vastaus on myös ARP. Työaseman Wiresharkissa näkyivät kaikkien IP-osoitteiden läpikäynti ARP-pingauksena (keltainen) ja lisäksi DNS-kyselyt (sininen):



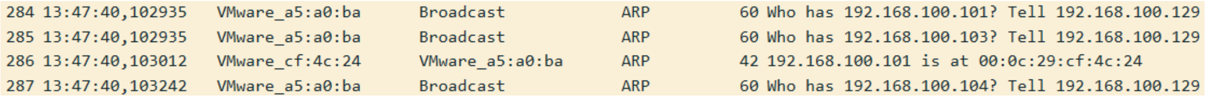
```
43 13:47:39,482771    VMware_a5:a0:ba      Broadcast          ARP        60 Who has 192.168.100.1? Tell 192.168.100.129
44 13:47:39,482771    VMware_c0:00:08      VMware_a5:a0:ba    ARP        60 192.168.100.1 is at 00:50:56:c0:00:08
45 13:47:39,482873    VMware_a5:a0:ba      Broadcast          ARP        60 Who has 192.168.100.2? Tell 192.168.100.129
46 13:47:39,482873    VMware_e2:ff:c6      VMware_a5:a0:ba    ARP        60 192.168.100.2 is at 00:50:56:e2:ff:c6
47 13:47:39,483400    VMware_a5:a0:ba      Broadcast          ARP        60 Who has 192.168.100.3? Tell 192.168.100.129
48 13:47:39,483400    VMware_a5:a0:ba      Broadcast          ARP        60 Who has 192.168.100.4? Tell 192.168.100.129
```

…



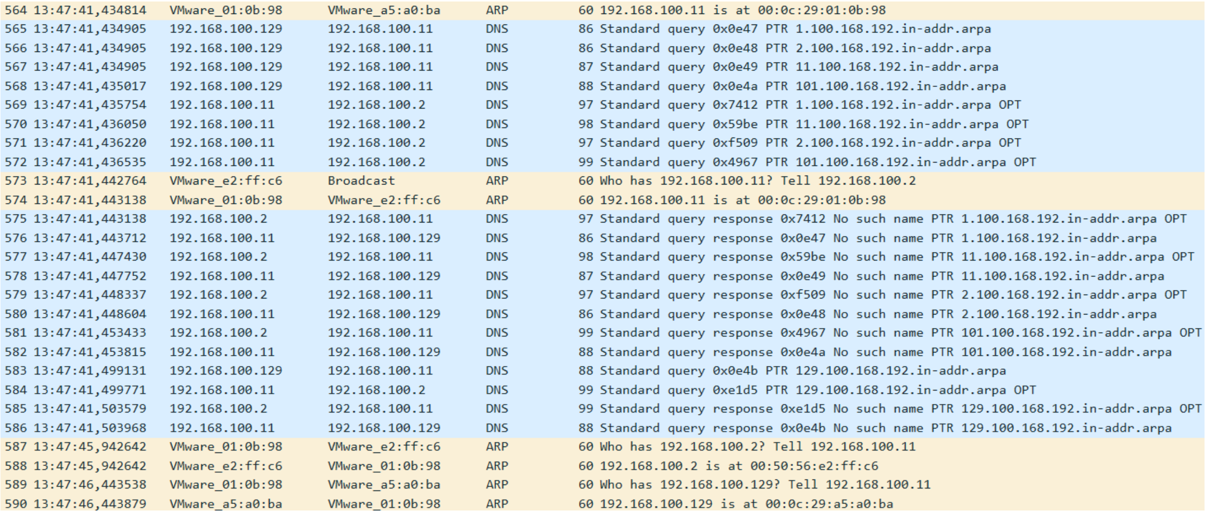
```
264 13:47:40,096814    VMware_a5:a0:ba      Broadcast          ARP        60 Who has 192.168.100.11? Tell 192.168.100.129
265 13:47:40,097119    VMware_a5:a0:ba      Broadcast          ARP        60 Who has 192.168.100.12? Tell 192.168.100.129
266 13:47:40,097119    VMware_01:0b:98      VMware_a5:a0:ba    ARP        60 192.168.100.11 is at 00:0c:29:01:0b:98
267 13:47:40,097456    VMware_a5:a0:ba      Broadcast          ARP        60 Who has 192.168.100.17? Tell 192.168.100.129
```

…



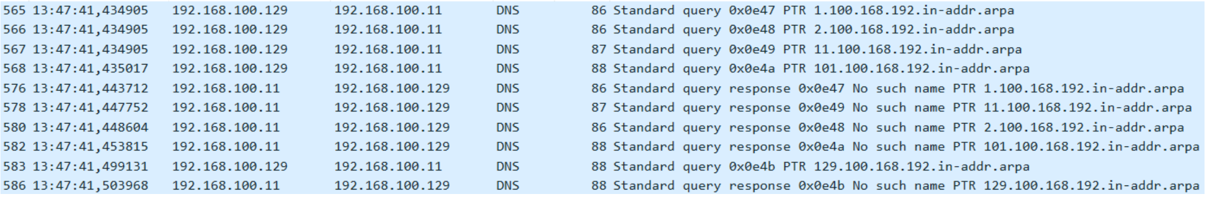
```
284 13:47:40,102935    VMware_a5:a0:ba      Broadcast          ARP        60 Who has 192.168.100.101? Tell 192.168.100.129
285 13:47:40,102935    VMware_a5:a0:ba      Broadcast          ARP        60 Who has 192.168.100.103? Tell 192.168.100.129
286 13:47:40,103012    VMware_cf:4c:24      VMware_a5:a0:ba    ARP        42 192.168.100.101 is at 00:0c:29:cf:4c:24
287 13:47:40,103242    VMware_a5:a0:ba      Broadcast          ARP        60 Who has 192.168.100.104? Tell 192.168.100.129
```

…



```
564 13:47:41,434814  VMware_01:0b:98    VMware_a5:a0:ba    ARP       60 192.168.100.11 is at 00:0c:29:01:0b:98
565 13:47:41,434905  192.168.100.129    192.168.100.11     DNS       86 Standard query 0x0e47 PTR 1.100.168.192.in-addr.arpa
566 13:47:41,434905  192.168.100.129    192.168.100.11     DNS       86 Standard query 0x0e48 PTR 2.100.168.192.in-addr.arpa
567 13:47:41,434905  192.168.100.129    192.168.100.11     DNS       87 Standard query 0x0e49 PTR 11.100.168.192.in-addr.arpa
568 13:47:41,435017  192.168.100.129    192.168.100.11     DNS       88 Standard query 0x0e4a PTR 101.100.168.192.in-addr.arpa
569 13:47:41,435754  192.168.100.11     192.168.100.2      DNS       97 Standard query 0x7412 PTR 1.100.168.192.in-addr.arpa OPT
570 13:47:41,436050  192.168.100.11     192.168.100.2      DNS       98 Standard query 0x59be PTR 11.100.168.192.in-addr.arpa OPT
571 13:47:41,436220  192.168.100.11     192.168.100.2      DNS       97 Standard query 0xf509 PTR 2.100.168.192.in-addr.arpa OPT
572 13:47:41,436535  192.168.100.11     192.168.100.2      DNS       99 Standard query 0x4967 PTR 101.100.168.192.in-addr.arpa OPT
573 13:47:41,442764  VMware_e2:ff:c6    Broadcast          ARP       60 Who has 192.168.100.11? Tell 192.168.100.2
574 13:47:41,443138  VMware_01:0b:98    VMware_e2:ff:c6    ARP       60 192.168.100.11 is at 00:0c:29:01:0b:98
575 13:47:41,443138  192.168.100.2      192.168.100.11     DNS       97 Standard query response 0x7412 No such name PTR 1.100.168.192.in-addr.arpa OPT
576 13:47:41,443712  192.168.100.11     192.168.100.129    DNS       86 Standard query response 0x0e47 No such name PTR 1.100.168.192.in-addr.arpa
577 13:47:41,447430  192.168.100.2      192.168.100.11     DNS       98 Standard query response 0x59be No such name PTR 11.100.168.192.in-addr.arpa OPT
578 13:47:41,447752  192.168.100.11     192.168.100.129    DNS       87 Standard query response 0x0e49 No such name PTR 11.100.168.192.in-addr.arpa
579 13:47:41,448337  192.168.100.2      192.168.100.11     DNS       97 Standard query response 0xf509 No such name PTR 2.100.168.192.in-addr.arpa OPT
580 13:47:41,448604  192.168.100.11     192.168.100.129    DNS       86 Standard query response 0x0e48 No such name PTR 2.100.168.192.in-addr.arpa
581 13:47:41,453433  192.168.100.2      192.168.100.11     DNS       99 Standard query response 0x4967 No such name PTR 101.100.168.192.in-addr.arpa OPT
582 13:47:41,453815  192.168.100.11     192.168.100.129    DNS       88 Standard query response 0x0e4a No such name PTR 101.100.168.192.in-addr.arpa
583 13:47:41,499131  192.168.100.129    192.168.100.11     DNS       88 Standard query 0x0e4b PTR 129.100.168.192.in-addr.arpa
584 13:47:41,499771  192.168.100.11     192.168.100.2      DNS       99 Standard query 0xe1d5 PTR 129.100.168.192.in-addr.arpa OPT
585 13:47:41,503579  192.168.100.2      192.168.100.11     DNS       99 Standard query response 0xe1d5 No such name PTR 129.100.168.192.in-addr.arpa OPT
586 13:47:41,503968  192.168.100.11     192.168.100.129    DNS       88 Standard query response 0x0e4b No such name PTR 129.100.168.192.in-addr.arpa
587 13:47:45,942642  VMware_01:0b:98    VMware_e2:ff:c6    ARP       60 Who has 192.168.100.2? Tell 192.168.100.11
588 13:47:45,942642  VMware_e2:ff:c6    VMware_01:0b:98    ARP       60 192.168.100.2 is at 00:50:56:e2:ff:c6
589 13:47:46,443538  VMware_01:0b:98    VMware_a5:a0:ba    ARP       60 Who has 192.168.100.129? Tell 192.168.100.11
590 13:47:46,443879  VMware_a5:a0:ba    VMware_01:0b:98    ARP       60 192.168.100.129 is at 00:0c:29:a5:a0:ba
```

Kokeiltiin IP-suodatusta (ip.addr == 192.168.100.129) ja saatiin DNS-kyselyt:



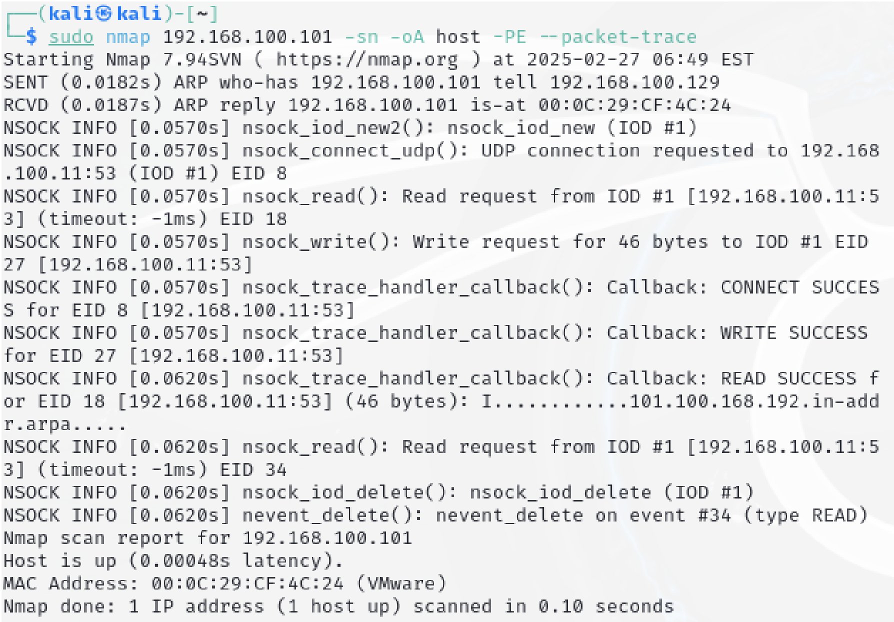
```
565 13:47:41,434905   192.168.100.129    192.168.100.11     DNS       86 Standard query 0x0e47 PTR 1.100.168.192.in-addr.arpa
566 13:47:41,434905   192.168.100.129    192.168.100.11     DNS       86 Standard query 0x0e48 PTR 2.100.168.192.in-addr.arpa
567 13:47:41,434905   192.168.100.129    192.168.100.11     DNS       87 Standard query 0x0e49 PTR 11.100.168.192.in-addr.arpa
568 13:47:41,435017   192.168.100.129    192.168.100.11     DNS       88 Standard query 0x0e4a PTR 101.100.168.192.in-addr.arpa
576 13:47:41,443712   192.168.100.11     192.168.100.129    DNS       86 Standard query response 0x0e47 No such name PTR 1.100.168.192.in-addr.arpa
578 13:47:41,447752   192.168.100.11     192.168.100.129    DNS       87 Standard query response 0x0e49 No such name PTR 11.100.168.192.in-addr.arpa
580 13:47:41,448604   192.168.100.11     192.168.100.129    DNS       86 Standard query response 0x0e48 No such name PTR 2.100.168.192.in-addr.arpa
582 13:47:41,453815   192.168.100.11     192.168.100.129    DNS       88 Standard query response 0x0e4a No such name PTR 101.100.168.192.in-addr.arpa
583 13:47:41,499131   192.168.100.129    192.168.100.11     DNS       88 Standard query 0x0e4b PTR 129.100.168.192.in-addr.arpa
586 13:47:41,503968   192.168.100.11     192.168.100.129    DNS       88 Standard query response 0x0e4b No such name PTR 129.100.168.192.in-addr.arpa
```

Tarkistettiin, estääkö palomuuri työaseman ICMP-pingit pakottamalla ne (-sn -PE) ja varmistamalla se (--packet-trace).

Komennolla (20250227 klo 13.49) ei kuitenkaan saatu ICMP-pingausta lähtemään:

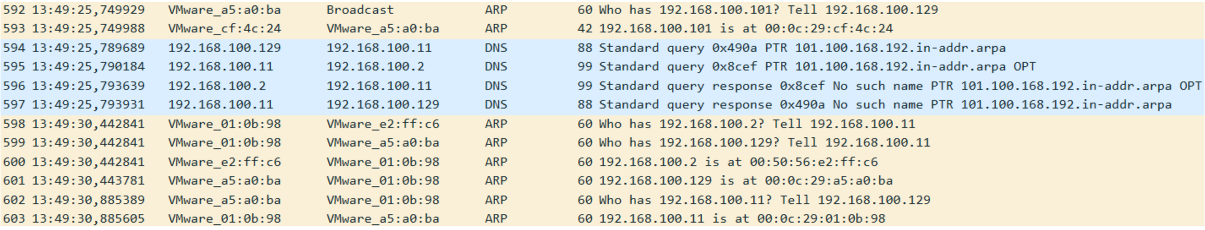
sudo nmap 192.168.100.101 -sn -oA host -PE --packet-trace

Eli tuloksena lähti kuitenkin taas vain ARP-ping:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 -sn -oA host -PE --packet-trace
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-27 06:49 EST
SENT (0.0182s) ARP who-has 192.168.100.101 tell 192.168.100.129
RCVD (0.0187s) ARP reply 192.168.100.101 is-at 00:0C:29:CF:4C:24
NSOCK INFO [0.0570s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0570s] nsock_connect_udp(): UDP connection requested to 192.168
.100.11:53 (IOD #1) EID 8
NSOCK INFO [0.0570s] nsock_read(): Read request from IOD #1 [192.168.100.11:5
3] (timeout: -1ms) EID 18
NSOCK INFO [0.0570s] nsock_write(): Write request for 46 bytes to IOD #1 EID
27 [192.168.100.11:53]
NSOCK INFO [0.0570s] nsock_trace_handler_callback(): Callback: CONNECT SUCCES
S for EID 8 [192.168.100.11:53]
NSOCK INFO [0.0570s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS
for EID 27 [192.168.100.11:53]
NSOCK INFO [0.0620s] nsock_trace_handler_callback(): Callback: READ SUCCESS f
or EID 18 [192.168.100.11:53] (46 bytes): I...........101.100.168.192.in-add
r.arpa.....
NSOCK INFO [0.0620s] nsock_read(): Read request from IOD #1 [192.168.100.11:5
3] (timeout: -1ms) EID 34
NSOCK INFO [0.0620s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.0620s] nevent_delete(): nevent_delete on event #34 (type READ)
Nmap scan report for 192.168.100.101
Host is up (0.00048s latency).
MAC Address: 00:0C:29:CF:4C:24 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Työaseman Wiresharkissa näkyivät vastaavasti ARP-pingit ja DNS-kyselyt:

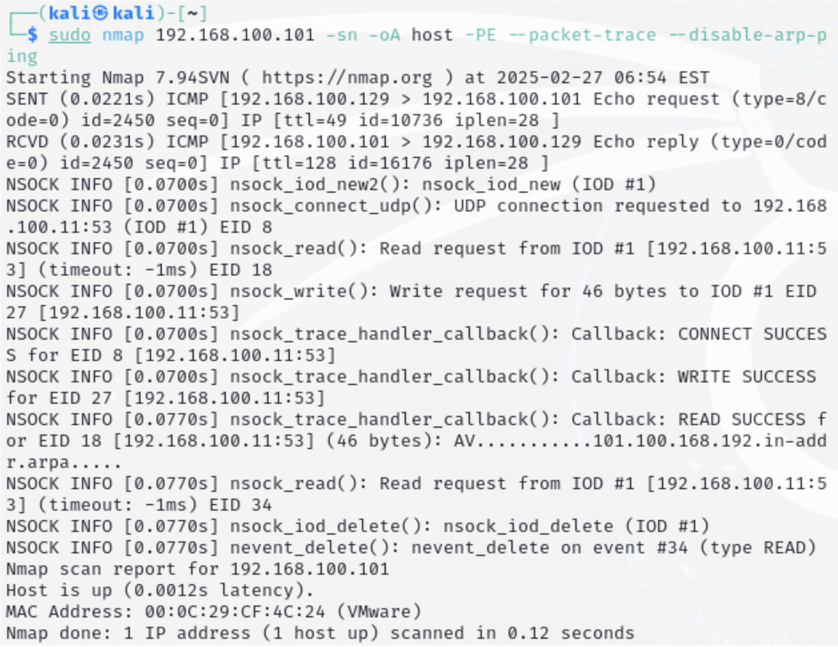


```
592 13:49:25,749929   VMware_a5:a0:ba     Broadcast           ARP          60 Who has 192.168.100.101? Tell 192.168.100.129
593 13:49:25,749988   VMware_cf:4c:24     VMware_a5:a0:ba     ARP          42 192.168.100.101 is at 00:0c:29:cf:4c:24
594 13:49:25,789689   192.168.100.129     192.168.100.11      DNS          88 Standard query 0x490a PTR 101.100.168.192.in-addr.arpa
595 13:49:25,790184   192.168.100.11      192.168.100.2       DNS          99 Standard query 0x8cef PTR 101.100.168.192.in-addr.arpa OPT
596 13:49:25,793639   192.168.100.2       192.168.100.11      DNS          99 Standard query response 0x8cef No such name PTR 101.100.168.192.in-addr.arpa OPT
597 13:49:25,793931   192.168.100.11      192.168.100.129     DNS          88 Standard query response 0x490a No such name PTR 101.100.168.192.in-addr.arpa
598 13:49:30,442841   VMware_01:0b:98     VMware_e2:ff:c6     ARP          60 Who has 192.168.100.2? Tell 192.168.100.11
599 13:49:30,442841   VMware_01:0b:98     VMware_a5:a0:ba     ARP          60 Who has 192.168.100.129? Tell 192.168.100.11
600 13:49:30,442841   VMware_e2:ff:c6     VMware_01:0b:98     ARP          60 192.168.100.2 is at 00:50:56:e2:ff:c6
601 13:49:30,443781   VMware_a5:a0:ba     VMware_01:0b:98     ARP          60 192.168.100.129 is at 00:0c:29:a5:a0:ba
602 13:49:30,885389   VMware_a5:a0:ba     VMware_01:0b:98     ARP          60 Who has 192.168.100.11? Tell 192.168.100.129
603 13:49:30,885605   VMware_01:0b:98     VMware_a5:a0:ba     ARP          60 192.168.100.11 is at 00:0c:29:01:0b:98
```

Lisättiin komentoon ARP-pingien estäminen (--disable-arp-ping) (20250227_1 klo 13.54):

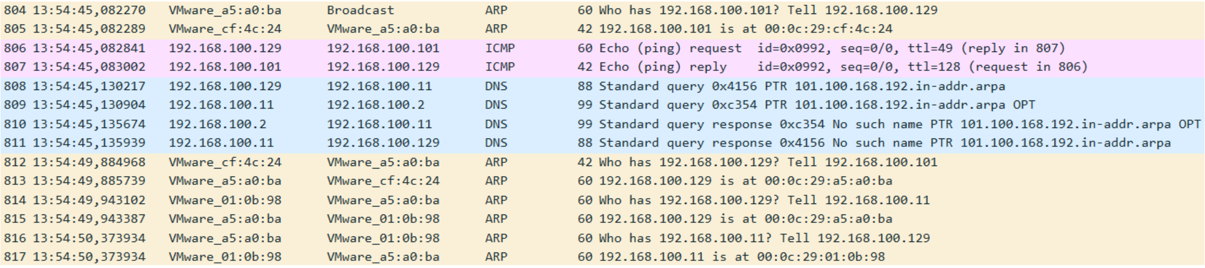
sudo nmap 192.168.100.101 -sn -oA host -PE --packet-trace --disable-arp-ping

Tällöin saatiin ICMP-pingit lähtemään, ja nähtiin vastauksen ttl-arvosta 128, että kyseessä on Windows-käyttöjärjestelmä:

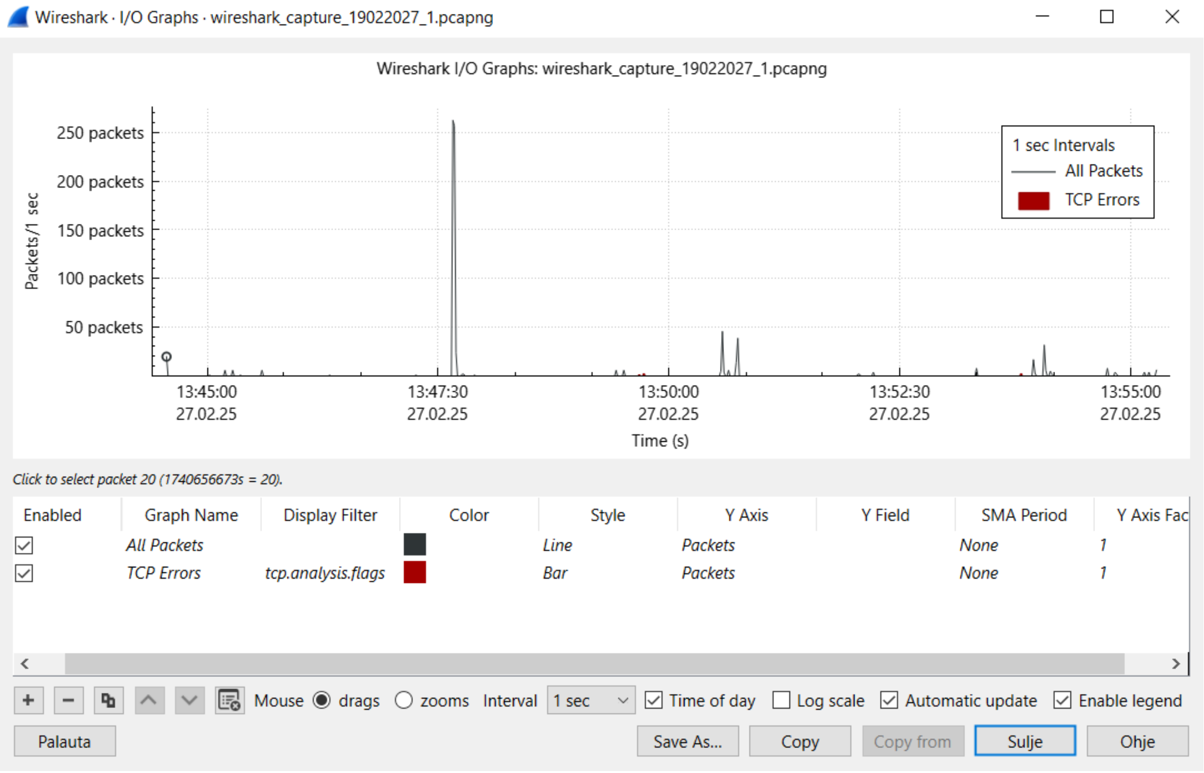


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 -sn -oA host -PE --packet-trace --disable-arp-p
ing
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-27 06:54 EST
SENT (0.0221s) ICMP [192.168.100.129 > 192.168.100.101 Echo request (type=8/c
ode=0) id=2450 seq=0] IP [ttl=49 id=10736 iplen=28 ]
RCVD (0.0231s) ICMP [192.168.100.101 > 192.168.100.129 Echo reply (type=0/cod
e=0) id=2450 seq=0] IP [ttl=128 id=16176 iplen=28 ]
NSOCK INFO [0.0700s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0700s] nsock_connect_udp(): UDP connection requested to 192.168
.100.11:53 (IOD #1) EID 8
NSOCK INFO [0.0700s] nsock_read(): Read request from IOD #1 [192.168.100.11:5
3] (timeout: -1ms) EID 18
NSOCK INFO [0.0700s] nsock_write(): Write request for 46 bytes to IOD #1 EID
27 [192.168.100.11:53]
NSOCK INFO [0.0700s] nsock_trace_handler_callback(): Callback: CONNECT SUCCES
S for EID 8 [192.168.100.11:53]
NSOCK INFO [0.0700s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS
for EID 27 [192.168.100.11:53]
NSOCK INFO [0.0770s] nsock_trace_handler_callback(): Callback: READ SUCCESS f
or EID 18 [192.168.100.11:53] (46 bytes): AV...........101.100.168.192.in-add
r.arpa.....
NSOCK INFO [0.0770s] nsock_read(): Read request from IOD #1 [192.168.100.11:5
3] (timeout: -1ms) EID 34
NSOCK INFO [0.0770s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.0770s] nevent_delete(): nevent_delete on event #34 (type READ)
Nmap scan report for 192.168.100.101
Host is up (0.0012s latency).
MAC Address: 00:0C:29:CF:4C:24 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Mutta jostain syystä työaseman Wiresharkissa näkyi ICMP-pingien (lila) ja DNS-kyselyn lisäksi edelleen myös ARP-pingit:



```
804 13:54:45,082270   VMware_a5:a0:ba     Broadcast           ARP          60 Who has 192.168.100.101? Tell 192.168.100.129
805 13:54:45,082289   VMware_cf:4c:24     VMware_a5:a0:ba     ARP          42 192.168.100.101 is at 00:0c:29:cf:4c:24
806 13:54:45,082841   192.168.100.129     192.168.100.101     ICMP         60 Echo (ping) request  id=0x0992, seq=0/0, ttl=49 (reply in 807)
807 13:54:45,083002   192.168.100.101     192.168.100.129     ICMP         42 Echo (ping) reply    id=0x0992, seq=0/0, ttl=128 (request in 806)
808 13:54:45,130217   192.168.100.129     192.168.100.11      DNS          88 Standard query 0x4156 PTR 101.100.168.192.in-addr.arpa
809 13:54:45,130904   192.168.100.11      192.168.100.2       DNS          99 Standard query 0xc354 PTR 101.100.168.192.in-addr.arpa OPT
810 13:54:45,135674   192.168.100.2       192.168.100.11      DNS          99 Standard query response 0xc354 No such name PTR 101.100.168.192.in-addr.arpa OPT
811 13:54:45,135939   192.168.100.11      192.168.100.129     DNS          88 Standard query response 0x4156 No such name PTR 101.100.168.192.in-addr.arpa
812 13:54:49,884968   VMware_cf:4c:24     VMware_a5:a0:ba     ARP          42 Who has 192.168.100.129? Tell 192.168.100.101
813 13:54:49,885739   VMware_a5:a0:ba     VMware_cf:4c:24     ARP          60 192.168.100.129 is at 00:0c:29:a5:a0:ba
814 13:54:49,943102   VMware_01:0b:98     VMware_a5:a0:ba     ARP          60 Who has 192.168.100.129? Tell 192.168.100.11
815 13:54:49,943387   VMware_a5:a0:ba     VMware_01:0b:98     ARP          60 192.168.100.129 is at 00:0c:29:a5:a0:ba
816 13:54:50,373934   VMware_a5:a0:ba     VMware_01:0b:98     ARP          60 Who has 192.168.100.11? Tell 192.168.100.129
817 13:54:50,373934   VMware_01:0b:98     VMware_a5:a0:ba     ARP          60 192.168.100.11 is at 00:0c:29:01:0b:98
```



Click to select packet 20 (1740656673s = 20).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Fac
☑	*All Packets*		■	*Line*	*Packets*		*None*	*1*
☑	*TCP Errors*	*tcp.analysis.flags*	🟥	*Bar*	*Packets*		*None*	*1*

Mouse ● drags ○ zooms Interval 1 sec ☑ Time of day ☐ Log scale ☑ Automatic update ☑ Enable legend

1.2 Kohteiden ja porttien skannaus

Tutkittiin työaseman avoimet portit ja sen palvelut. Skannatuille porteille voidaan saada kuusi erilaista tilaa:

- ”open”: yhteys muodostettu, yhteys voi olla TCP-yhteys, UDP-datagrammi tai SCTP-yhteys
- ”closed”: TCP-protokollan mukaisesti saatiin vastauksena RST-lipun sisältävä paketti
- “filtered”: Nmap ei pystynyt määrittämään, onko portti auki vai kiinni, koska vastausta ei saatu tai saatiin virheilmoitus
- “unfiltered”: saadaan vain TCP-ACK-skannauksesta ja tarkoittaa, että portti on saavutettavissa (auki tai kiinni)
- “open|filtered”: ei saada vastausta eli palomuuri tai pakettifiltteri saattaa suojata porttia
- “closed|filtered”: saadaan vain TCP-idle-skannauksella ja osoittaa, että oli mahdotonta määrittää, oliko portti kiinni vai palomuurin takana

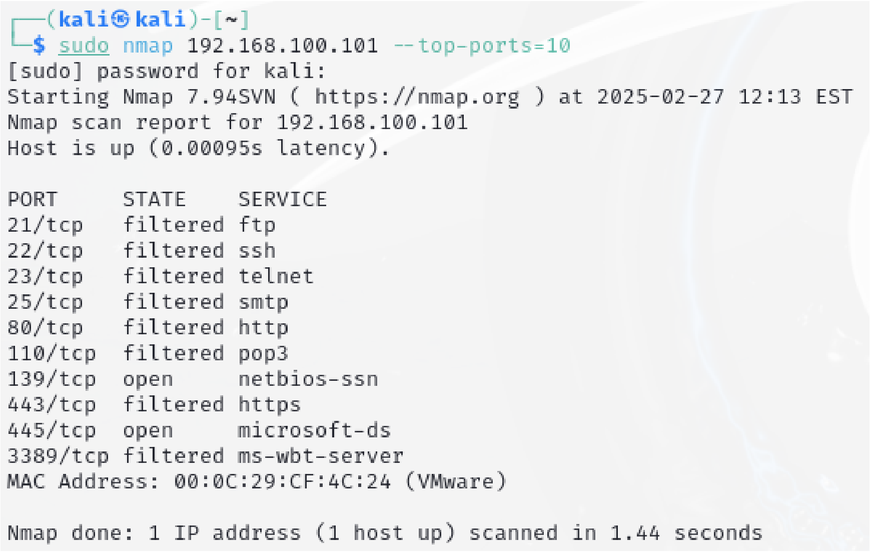
1.2.1 SYN-skannaus

Nmap skannaa oletuksena 1000 suosituinta porttia SYN-skannauksella (-sS), kun toimitaan pääkäyttäjänä. Muuten käytetään TCP-skannausta (-sT). SYN-skannaus ei suorita kokonaista kättelyä ja yhteys jää kesken. Tällöin skannauksen havaitseminen vaikeutuu, mutta edistyneet IDS/IPS-järjestelmät huomaavat myös ne.

Tehtiin kymmenen suosituimman TCP-portin SYN-skannaus (20250227_2 klo 19.13):

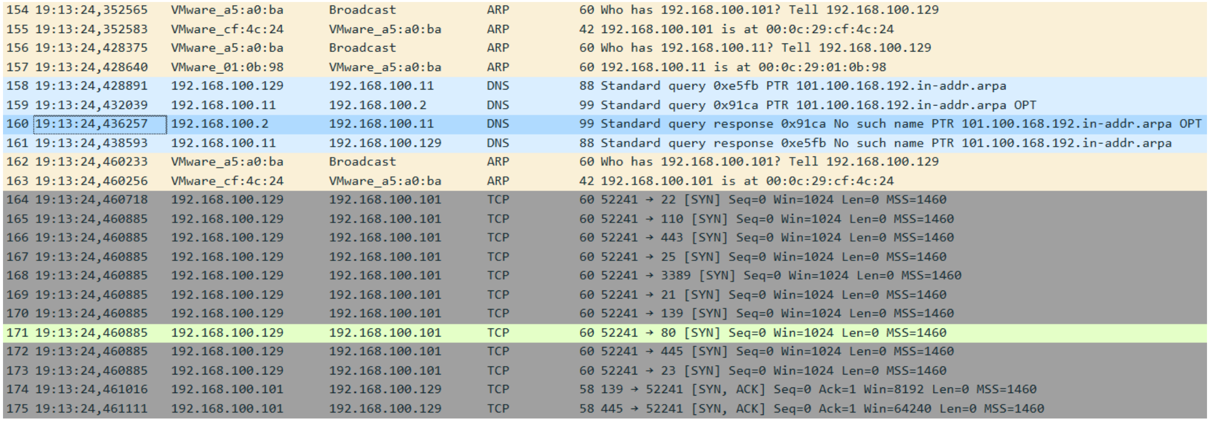
sudo nmap 192.168.100.101 --top-ports=10

Avoimia portteja löytyi kaksi: netbios-ssn ja microsoft-ds. Muut kymmenestä olivat ”filtered” eli Nmap ei pystynyt määrittämään, onko portti auki vai kiinni, koska vastausta ei saatu tai saatiin virheilmoitus:

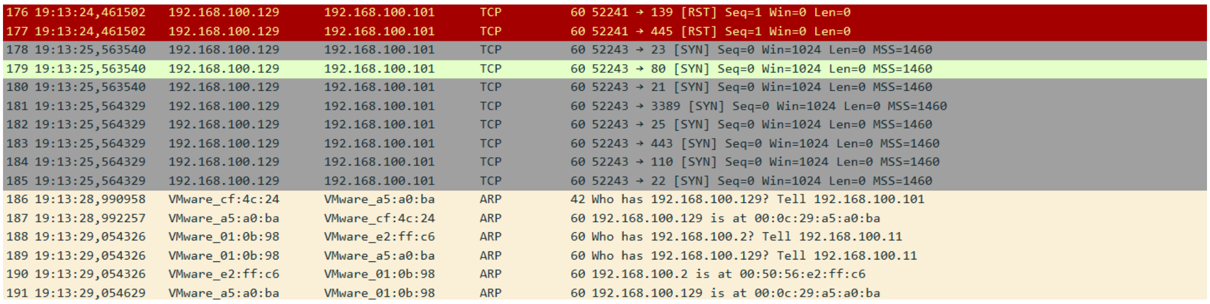


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 --top-ports=10
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-27 12:13 EST
Nmap scan report for 192.168.100.101
Host is up (0.00095s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  open     netbios-ssn
443/tcp  filtered https
445/tcp  open     microsoft-ds
3389/tcp filtered ms-wbt-server
MAC Address: 00:0C:29:CF:4C:24 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

Työaseman Wiresharkissa SYN-skannaukset näkyvät harmaalla ja http-portin SYN-skannaus vihreällä. Avointen porttien (139 ja 445) SYN, ACK-vastaukset näkyvät harmaalla ja Linux-koneen RST-vastaukset niihin punaisella.



```
154 19:13:24,352565   VMware_a5:a0:ba     Broadcast           ARP        60 Who has 192.168.100.101? Tell 192.168.100.129
155 19:13:24,352583   VMware_cf:4c:24     VMware_a5:a0:ba     ARP        42 192.168.100.101 is at 00:0c:29:cf:4c:24
156 19:13:24,428375   VMware_a5:a0:ba     Broadcast           ARP        60 Who has 192.168.100.11? Tell 192.168.100.129
157 19:13:24,428640   VMware_01:0b:98     VMware_a5:a0:ba     ARP        60 192.168.100.11 is at 00:0c:29:01:0b:98
158 19:13:24,428891   192.168.100.129     192.168.100.11      DNS        88 Standard query 0xe5fb PTR 101.100.168.192.in-addr.arpa
159 19:13:24,432039   192.168.100.11      192.168.100.2       DNS        99 Standard query 0x91ca PTR 101.100.168.192.in-addr.arpa OPT
160 19:13:24,436257   192.168.100.2       192.168.100.11      DNS        99 Standard query response 0x91ca No such name PTR 101.100.168.192.in-addr.arpa OPT
161 19:13:24,438593   192.168.100.11      192.168.100.129     DNS        88 Standard query response 0xe5fb No such name PTR 101.100.168.192.in-addr.arpa
162 19:13:24,460233   VMware_a5:a0:ba     Broadcast           ARP        60 Who has 192.168.100.101? Tell 192.168.100.129
163 19:13:24,460256   VMware_cf:4c:24     VMware_a5:a0:ba     ARP        42 192.168.100.101 is at 00:0c:29:cf:4c:24
164 19:13:24,460718   192.168.100.129     192.168.100.101     TCP        60 52241 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
165 19:13:24,460885   192.168.100.129     192.168.100.101     TCP        60 52241 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
166 19:13:24,460885   192.168.100.129     192.168.100.101     TCP        60 52241 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
167 19:13:24,460885   192.168.100.129     192.168.100.101     TCP        60 52241 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
168 19:13:24,460885   192.168.100.129     192.168.100.101     TCP        60 52241 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
169 19:13:24,460885   192.168.100.129     192.168.100.101     TCP        60 52241 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
170 19:13:24,460885   192.168.100.129     192.168.100.101     TCP        60 52241 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
171 19:13:24,460885   192.168.100.129     192.168.100.101     TCP        60 52241 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
172 19:13:24,460885   192.168.100.129     192.168.100.101     TCP        60 52241 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
173 19:13:24,460885   192.168.100.129     192.168.100.101     TCP        60 52241 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
174 19:13:24,461016   192.168.100.101     192.168.100.129     TCP        58 139 → 52241 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
175 19:13:24,461111   192.168.100.101     192.168.100.129     TCP        58 445 → 52241 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
```



```
176 19:13:24,461502   192.168.100.129     192.168.100.101     TCP        60 52241 → 139 [RST] Seq=1 Win=0 Len=0
177 19:13:24,461502   192.168.100.129     192.168.100.101     TCP        60 52241 → 445 [RST] Seq=1 Win=0 Len=0
178 19:13:25,563540   192.168.100.129     192.168.100.101     TCP        60 52243 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
179 19:13:25,563540   192.168.100.129     192.168.100.101     TCP        60 52243 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
180 19:13:25,563540   192.168.100.129     192.168.100.101     TCP        60 52243 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
181 19:13:25,564329   192.168.100.129     192.168.100.101     TCP        60 52243 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
182 19:13:25,564329   192.168.100.129     192.168.100.101     TCP        60 52243 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
183 19:13:25,564329   192.168.100.129     192.168.100.101     TCP        60 52243 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
184 19:13:25,564329   192.168.100.129     192.168.100.101     TCP        60 52243 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
185 19:13:25,564329   192.168.100.129     192.168.100.101     TCP        60 52243 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
186 19:13:28,990958   VMware_cf:4c:24     VMware_a5:a0:ba     ARP        42 Who has 192.168.100.129? Tell 192.168.100.101
187 19:13:28,992257   VMware_a5:a0:ba     VMware_cf:4c:24     ARP        60 192.168.100.129 is at 00:0c:29:a5:a0:ba
188 19:13:29,054326   VMware_01:0b:98     VMware_e2:ff:c6     ARP        60 Who has 192.168.100.2? Tell 192.168.100.11
189 19:13:29,054326   VMware_01:0b:98     VMware_a5:a0:ba     ARP        60 Who has 192.168.100.129? Tell 192.168.100.11
190 19:13:29,054326   VMware_e2:ff:c6     VMware_01:0b:98     ARP        60 192.168.100.2 is at 00:50:56:e2:ff:c6
191 19:13:29,054629   VMware_a5:a0:ba     VMware_01:0b:98     ARP        60 192.168.100.129 is at 00:0c:29:a5:a0:ba
```

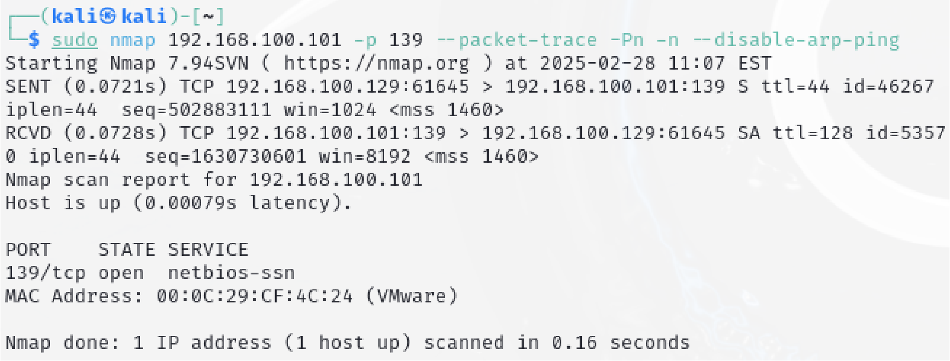
1.2.2 SYN-skannaus – avoin portti 139

Yksittäisen portin (139) SYN-skannauksesta saadaan enemmän tietoa komennolla (20250228_1 klo 18.07):

sudo nmap 192.168.100.101 -p 139 --packet-trace -Pn -n --disable-arp-ping

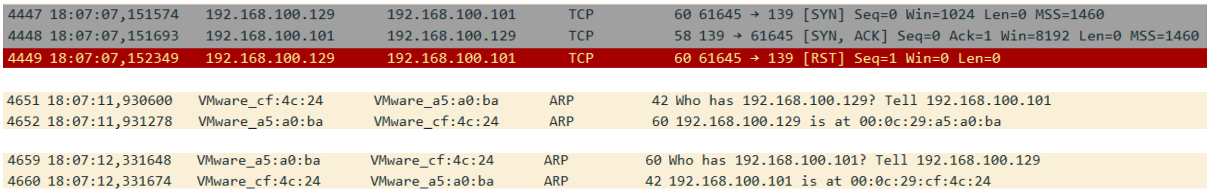
- -Pn: ICMP echo -kysely pois päältä
- -n: DNS-resoluutio pois päältä
- --disable-arp-ping: ARP-pingaus pois päältä

Nmapilla nähtiin nyt myös porttiin 139 tehty SYN-skannaus ja työasemalta vastauksena saatu SYN, ACK, muttei takaisin lähetettyä RST-vastausta:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 -p 139 --packet-trace -Pn -n --disable-arp-ping
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 11:07 EST
SENT (0.0721s) TCP 192.168.100.129:61645 > 192.168.100.101:139 S ttl=44 id=46267
iplen=44  seq=502883111 win=1024 <mss 1460>
RCVD (0.0728s) TCP 192.168.100.101:139 > 192.168.100.129:61645 SA ttl=128 id=5357
0 iplen=44  seq=1630730601 win=8192 <mss 1460>
Nmap scan report for 192.168.100.101
Host is up (0.00079s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:CF:4C:24 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Työaseman Wiresharkilla nähtiin TCP:t samoin kuin edellisellä komennolla:



```
4447 18:07:07,151574   192.168.100.129    192.168.100.101    TCP    60 61645 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4448 18:07:07,151693   192.168.100.101    192.168.100.129    TCP    58 139 → 61645 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
4449 18:07:07,152349   192.168.100.129    192.168.100.101    TCP    60 61645 → 139 [RST] Seq=1 Win=0 Len=0

4651 18:07:11,930600   VMware_cf:4c:24    VMware_a5:a0:ba    ARP    42 Who has 192.168.100.129? Tell 192.168.100.101
4652 18:07:11,931278   VMware_a5:a0:ba    VMware_cf:4c:24    ARP    60 192.168.100.129 is at 00:0c:29:a5:a0:ba

4659 18:07:12,331648   VMware_a5:a0:ba    VMware_cf:4c:24    ARP    60 Who has 192.168.100.101? Tell 192.168.100.129
4660 18:07:12,331674   VMware_cf:4c:24    VMware_a5:a0:ba    ARP    42 192.168.100.101 is at 00:0c:29:cf:4c:24
```

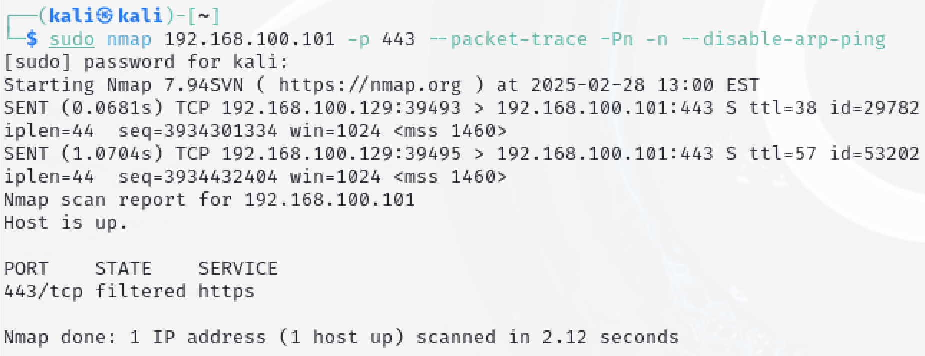
DNS-resoluutio jäi pois kuten pitikin mutta jostain syystä myös ARP:t näkyivät.

1.2.3 SYN-skannaus – ”filtered” portti 443

Yksittäisen portin (443) SYN-skannauksesta saadaan enemmän tietoa komennolla (20250228_3 klo 20.00):

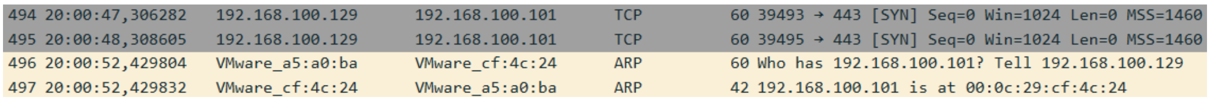
sudo nmap 192.168.100.101 -p 443 --packet-trace -Pn -n --disable-arp-ping

Nmapilla nähtiin nyt kaksi porttiin 443 tehtyä SYN-skannausta, muttei työasemalta vastauksena mitään eli portti käyttäytyy eri tavalla kuin avoin portti 139:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 -p 443 --packet-trace -Pn -n --disable-arp-ping
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 13:00 EST
SENT (0.0681s) TCP 192.168.100.129:39493 > 192.168.100.101:443 S ttl=38 id=29782
iplen=44  seq=3934301334 win=1024 <mss 1460>
SENT (1.0704s) TCP 192.168.100.129:39495 > 192.168.100.101:443 S ttl=57 id=53202
iplen=44  seq=3934432404 win=1024 <mss 1460>
Nmap scan report for 192.168.100.101
Host is up.

PORT    STATE    SERVICE
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
```

Työaseman Wiresharkilla nähtiin myös kaksi SYN-skannausta:



```
494 20:00:47,306282   192.168.100.129    192.168.100.101    TCP        60 39493 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
495 20:00:48,308605   192.168.100.129    192.168.100.101    TCP        60 39495 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
496 20:00:52,429804   VMware_a5:a0:ba    VMware_cf:4c:24    ARP        60 Who has 192.168.100.101? Tell 192.168.100.129
497 20:00:52,429832   VMware_cf:4c:24    VMware_a5:a0:ba    ARP        42 192.168.100.101 is at 00:0c:29:cf:4c:24
```

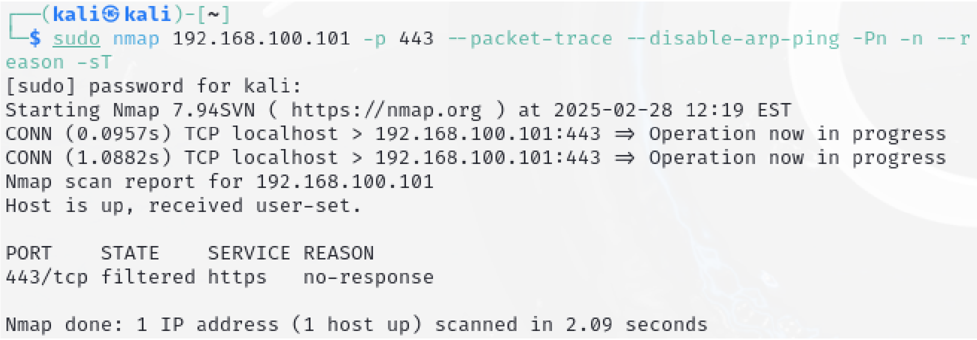
1.2.4 TCP-skannaus – ”filtered” portti 443

TCP connect -skannaus tekee kokonaisen kolmisuuntaisen kättelyn, joka on helposti havaittavissa nykyaikaisilla IDS/IPS-ratkaisuilla. Se on hidas ja sitä käytetään, kun tarkkuus on tärkeintä. Sillä ohitetaan palomuuri eikä sillä aiheuteta merkittävää haittaa palvelulle.

Tutkitaan ”filtered”-tilan saaneita portteja, kuten 443 (https) TCP-skannauksella (20250228_2 klo 19.19):

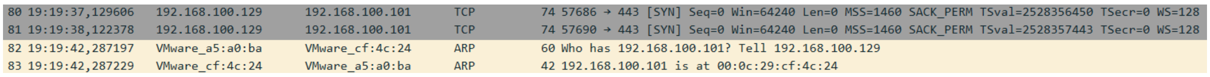
sudo nmap 192.168.100.101 -p 443 --packet-trace --disable-arp-ping -Pn -n --reason -sT

Nmapilla nähdään, että porttiin 443 tehdään kaksi TCP-skannausta, muttei saada vastausta:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 -p 443 --packet-trace --disable-arp-ping -Pn -n --r
eason -sT
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 12:19 EST
CONN (0.0957s) TCP localhost > 192.168.100.101:443 ⇒ Operation now in progress
CONN (1.0882s) TCP localhost > 192.168.100.101:443 ⇒ Operation now in progress
Nmap scan report for 192.168.100.101
Host is up, received user-set.

PORT    STATE    SERVICE REASON
443/tcp filtered https   no-response

Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```

Työaseman Wiresharkilla nähtiin yhä TCP:t ja ARP:t:



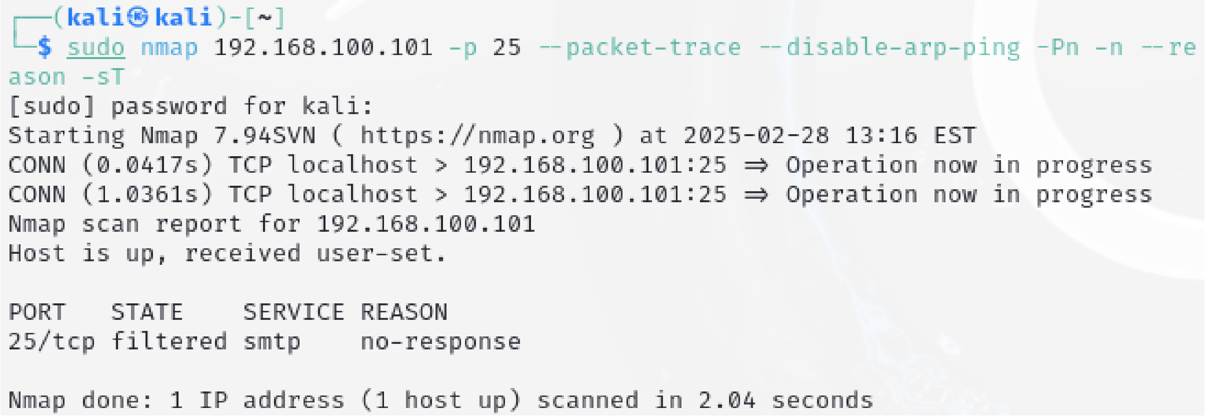
```
80 19:19:37,129606   192.168.100.129    192.168.100.101    TCP    74 57686 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2528356450 TSecr=0 WS=128
81 19:19:38,122378   192.168.100.129    192.168.100.101    TCP    74 57690 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2528357443 TSecr=0 WS=128
82 19:19:42,287197   VMware_a5:a0:ba    VMware_cf:4c:24    ARP    60 Who has 192.168.100.101? Tell 192.168.100.129
83 19:19:42,287229   VMware_cf:4c:24    VMware_a5:a0:ba    ARP    42 192.168.100.101 is at 00:0c:29:cf:4c:24
```

1.2.5 TCP-skannaus – ”filtered” portti 25

Tutkitaan ”filtered”-tilan saanutta porttia 25 (smtp) TCP-skannauksella (20250228_4 klo 20.16):

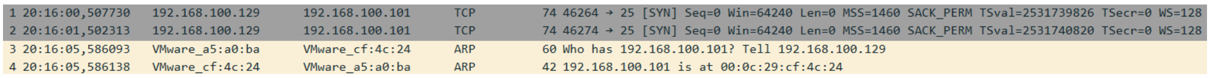
sudo nmap 192.168.100.101 -p 25 --packet-trace --disable-arp-ping -Pn -n --reason -sT

Nmapilla nähdään, että porttiin 25 tehdään kaksi TCP-skannausta, muttei saada vastausta:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 -p 25 --packet-trace --disable-arp-ping -Pn -n --re
ason -sT
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 13:16 EST
CONN (0.0417s) TCP localhost > 192.168.100.101:25 ⇒ Operation now in progress
CONN (1.0361s) TCP localhost > 192.168.100.101:25 ⇒ Operation now in progress
Nmap scan report for 192.168.100.101
Host is up, received user-set.

PORT   STATE    SERVICE REASON
25/tcp filtered smtp    no-response

Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
```

Työaseman Wiresharkilla nähtiin TCP:t ja ARP:t:



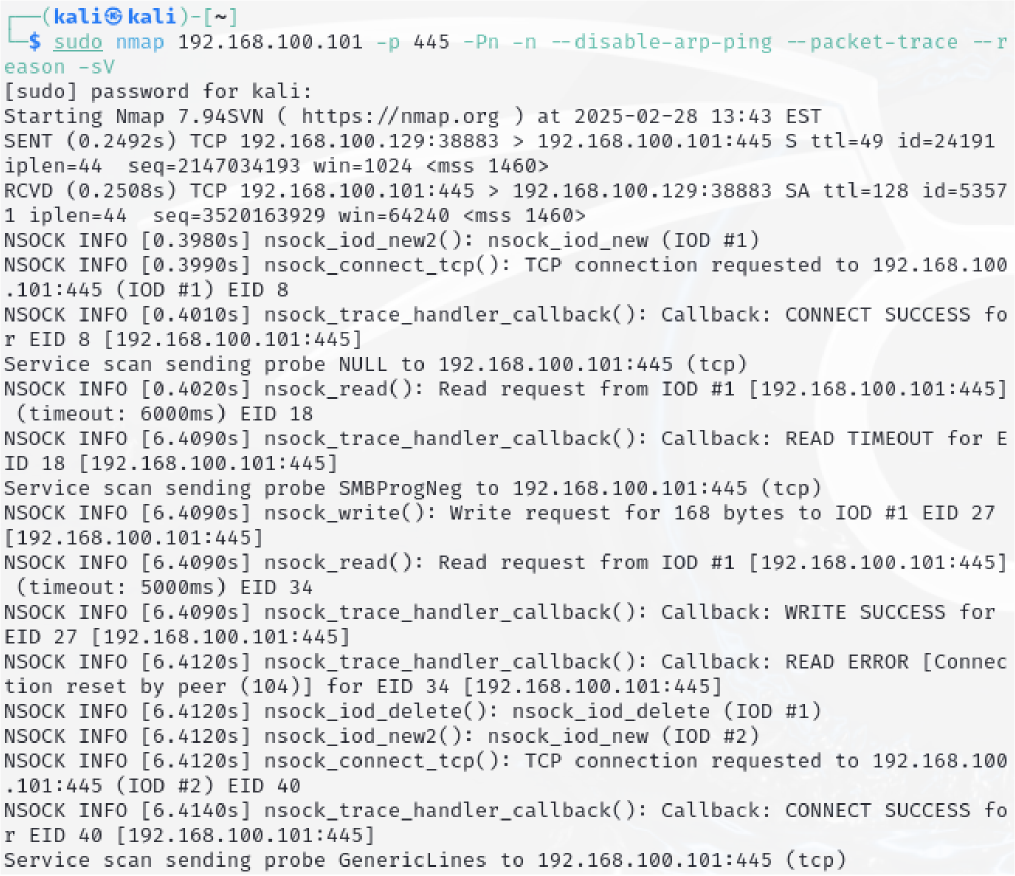
```
1 20:16:00,507730   192.168.100.129    192.168.100.101    TCP        74 46264 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2531739826 TSecr=0 WS=128
2 20:16:01,502313   192.168.100.129    192.168.100.101    TCP        74 46274 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2531740820 TSecr=0 WS=128
3 20:16:05,586093   VMware_a5:a0:ba    VMware_cf:4c:24    ARP        60 Who has 192.168.100.101? Tell 192.168.100.129
4 20:16:05,586138   VMware_cf:4c:24    VMware_a5:a0:ba    ARP        42 192.168.100.101 is at 00:0c:29:cf:4c:24
```

1.3 Palveluiden listaus

Lisätietoa avoimista porteista saadaan versioskannauksella (-sV), jolla voidaan määrittää versioita, palveluiden nimiä ja tietoja kohteesta.

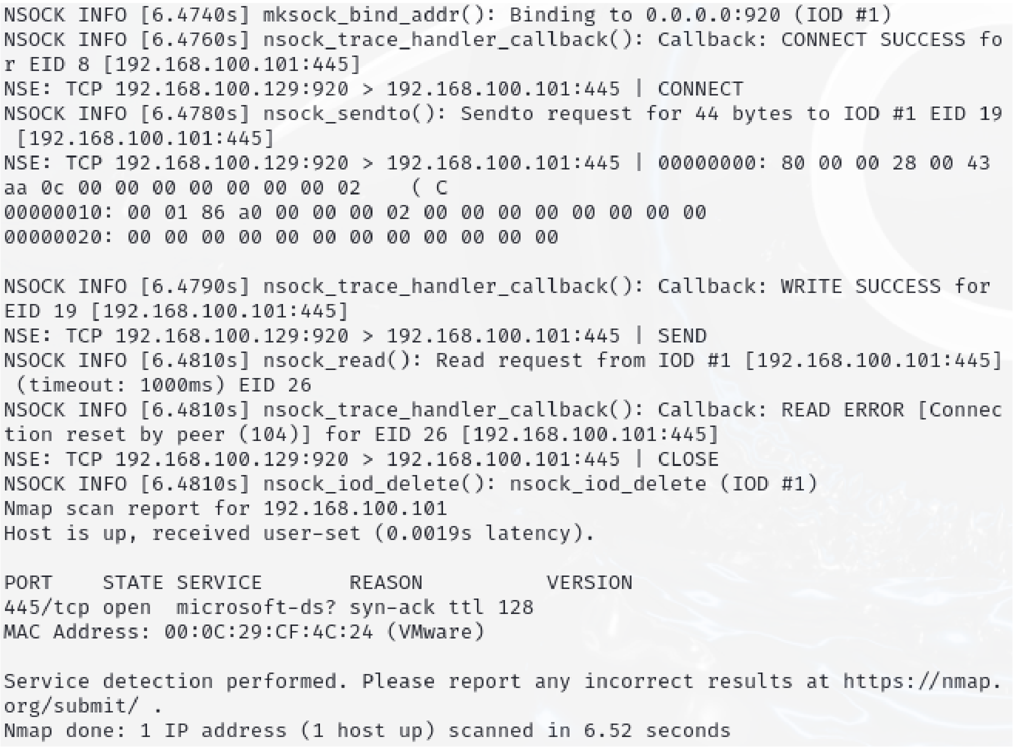
Kokeiltiin versioskannausta avoimeen porttiin 445 komennolla (20250228_5 klo 20.43):

sudo nmap 192.168.100.101 -p 445 -Pn -n --disable-arp-ping --packet-trace --reason -sV



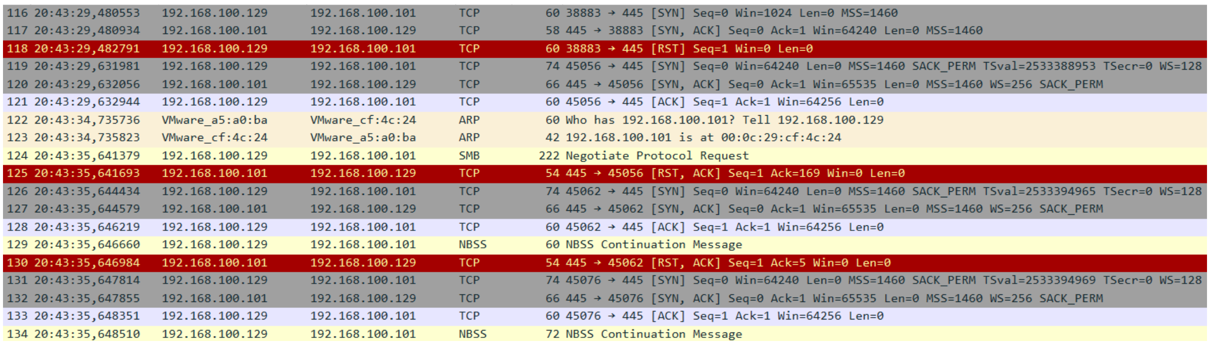
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.100.101 -p 445 -Pn -n --disable-arp-ping --packet-trace --r
eason -sV
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 13:43 EST
SENT (0.2492s) TCP 192.168.100.129:38883 > 192.168.100.101:445 S ttl=49 id=24191
iplen=44  seq=2147034193 win=1024 <mss 1460>
RCVD (0.2508s) TCP 192.168.100.101:445 > 192.168.100.129:38883 SA ttl=128 id=5357
1 iplen=44  seq=3520163929 win=64240 <mss 1460>
NSOCK INFO [0.3980s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.3990s] nsock_connect_tcp(): TCP connection requested to 192.168.100
.101:445 (IOD #1) EID 8
NSOCK INFO [0.4010s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS fo
r EID 8 [192.168.100.101:445]
Service scan sending probe NULL to 192.168.100.101:445 (tcp)
NSOCK INFO [0.4020s] nsock_read(): Read request from IOD #1 [192.168.100.101:445]
 (timeout: 6000ms) EID 18
NSOCK INFO [6.4090s] nsock_trace_handler_callback(): Callback: READ TIMEOUT for E
ID 18 [192.168.100.101:445]
Service scan sending probe SMBProgNeg to 192.168.100.101:445 (tcp)
NSOCK INFO [6.4090s] nsock_write(): Write request for 168 bytes to IOD #1 EID 27
[192.168.100.101:445]
NSOCK INFO [6.4090s] nsock_read(): Read request from IOD #1 [192.168.100.101:445]
 (timeout: 5000ms) EID 34
NSOCK INFO [6.4090s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for
EID 27 [192.168.100.101:445]
NSOCK INFO [6.4120s] nsock_trace_handler_callback(): Callback: READ ERROR [Connec
tion reset by peer (104)] for EID 34 [192.168.100.101:445]
NSOCK INFO [6.4120s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [6.4120s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [6.4120s] nsock_connect_tcp(): TCP connection requested to 192.168.100
.101:445 (IOD #2) EID 40
NSOCK INFO [6.4140s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS fo
r EID 40 [192.168.100.101:445]
Service scan sending probe GenericLines to 192.168.100.101:445 (tcp)
```

…



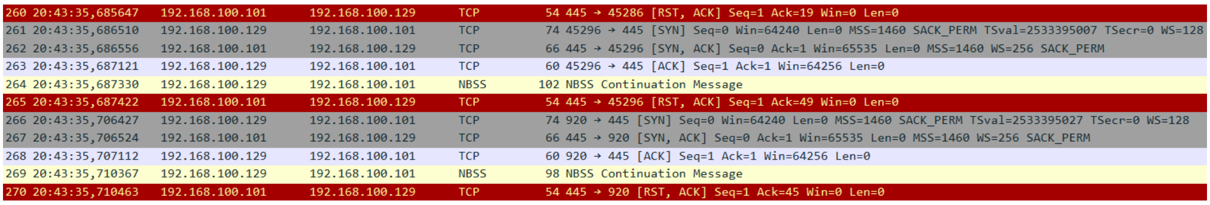
```
NSOCK INFO [6.4740s] mksock_bind_addr(): Binding to 0.0.0.0:920 (IOD #1)
NSOCK INFO [6.4760s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS fo
r EID 8 [192.168.100.101:445]
NSE: TCP 192.168.100.129:920 > 192.168.100.101:445 | CONNECT
NSOCK INFO [6.4780s] nsock_sendto(): Sendto request for 44 bytes to IOD #1 EID 19
 [192.168.100.101:445]
NSE: TCP 192.168.100.129:920 > 192.168.100.101:445 | 00000000: 80 00 00 28 00 43
aa 0c 00 00 00 00 00 00 00 02     ( C
00000010: 00 01 86 a0 00 00 00 02 00 00 00 00 00 00 00 00
00000020: 00 00 00 00 00 00 00 00 00 00 00 00

NSOCK INFO [6.4790s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for
EID 19 [192.168.100.101:445]
NSE: TCP 192.168.100.129:920 > 192.168.100.101:445 | SEND
NSOCK INFO [6.4810s] nsock_read(): Read request from IOD #1 [192.168.100.101:445]
 (timeout: 1000ms) EID 26
NSOCK INFO [6.4810s] nsock_trace_handler_callback(): Callback: READ ERROR [Connec
tion reset by peer (104)] for EID 26 [192.168.100.101:445]
NSE: TCP 192.168.100.129:920 > 192.168.100.101:445 | CLOSE
NSOCK INFO [6.4810s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
Nmap scan report for 192.168.100.101
Host is up, received user-set (0.0019s latency).

PORT    STATE SERVICE       REASON          VERSION
445/tcp open  microsoft-ds? syn-ack ttl 128
MAC Address: 00:0C:29:CF:4C:24 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.52 seconds
```

Työaseman Wireshark vastaavasti:



```
116 20:43:29,480553   192.168.100.129   192.168.100.101   TCP      60 38883 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
117 20:43:29,480934   192.168.100.101   192.168.100.129   TCP      58 445 → 38883 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
118 20:43:29,482791   192.168.100.129   192.168.100.101   TCP      60 38883 → 445 [RST] Seq=1 Win=0 Len=0
119 20:43:29,631981   192.168.100.129   192.168.100.101   TCP      74 45056 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2533388953 TSecr=0 WS=128
120 20:43:29,632056   192.168.100.101   192.168.100.129   TCP      66 445 → 45056 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
121 20:43:29,632944   192.168.100.129   192.168.100.101   TCP      60 45056 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0
122 20:43:34,735736   VMware_a5:a0:ba   VMware_cf:4c:24   ARP      60 Who has 192.168.100.101? Tell 192.168.100.129
123 20:43:34,735823   VMware_cf:4c:24   VMware_a5:a0:ba   ARP      42 192.168.100.101 is at 00:0c:29:cf:4c:24
124 20:43:35,641379   192.168.100.129   192.168.100.101   SMB     222 Negotiate Protocol Request
125 20:43:35,641693   192.168.100.101   192.168.100.129   TCP      54 445 → 45056 [RST, ACK] Seq=1 Ack=169 Win=0 Len=0
126 20:43:35,644434   192.168.100.129   192.168.100.101   TCP      74 45062 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2533394965 TSecr=0 WS=128
127 20:43:35,644579   192.168.100.101   192.168.100.129   TCP      66 445 → 45062 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
128 20:43:35,646219   192.168.100.129   192.168.100.101   TCP      60 45062 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0
129 20:43:35,646660   192.168.100.129   192.168.100.101   NBSS     60 NBSS Continuation Message
130 20:43:35,646984   192.168.100.101   192.168.100.129   TCP      54 445 → 45062 [RST, ACK] Seq=1 Ack=5 Win=0 Len=0
131 20:43:35,647814   192.168.100.129   192.168.100.101   TCP      74 45076 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2533394969 TSecr=0 WS=128
132 20:43:35,647855   192.168.100.101   192.168.100.129   TCP      66 445 → 45076 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
133 20:43:35,648351   192.168.100.129   192.168.100.101   TCP      60 45076 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0
134 20:43:35,648510   192.168.100.129   192.168.100.101   NBSS     72 NBSS Continuation Message
```

…



```
260 20:43:35,685647   192.168.100.101   192.168.100.129   TCP      54 445 → 45286 [RST, ACK] Seq=1 Ack=19 Win=0 Len=0
261 20:43:35,686510   192.168.100.129   192.168.100.101   TCP      74 45296 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2533395007 TSecr=0 WS=128
262 20:43:35,686556   192.168.100.101   192.168.100.129   TCP      66 445 → 45296 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
263 20:43:35,687121   192.168.100.129   192.168.100.101   TCP      60 45296 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0
264 20:43:35,687330   192.168.100.129   192.168.100.101   NBSS    102 NBSS Continuation Message
265 20:43:35,687422   192.168.100.101   192.168.100.129   TCP      54 445 → 45296 [RST, ACK] Seq=1 Ack=49 Win=0 Len=0
266 20:43:35,706427   192.168.100.129   192.168.100.101   TCP      74 920 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2533395027 TSecr=0 WS=128
267 20:43:35,706524   192.168.100.101   192.168.100.129   TCP      66 445 → 920 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
268 20:43:35,707112   192.168.100.129   192.168.100.101   TCP      60 920 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0
269 20:43:35,710367   192.168.100.129   192.168.100.101   NBSS     98 NBSS Continuation Message
270 20:43:35,710463   192.168.100.101   192.168.100.129   TCP      54 445 → 920 [RST, ACK] Seq=1 Ack=45 Win=0 Len=0
```

Lähdeluettelo

Hack the Box. (25. Helmikuu 2025). *Network Enumeration with Nmap*. Noudettu osoitteesta https://academy.hackthebox.com/module/details/19

OpenAI. (24. Helmikuu 2025). *ChatGPT*. Noudettu osoitteesta https://chatgpt.com/

Wireshark Foundation. (18. Helmikuu 2025). *Wireshark*. Noudettu osoitteesta https://www.wireshark.org/