

ping 8.8.8.8

האם זה יתגלו כזיהה למשתמשים אחרים?

echo reply → יתגלו כזיהה למשתמשים אחרים, אך לא כמשתמש

בנוסף לכך, יוכל Sniff-Spoof את IP של המשתמש

לפיכך נסמן NSID → echo reply → יתגלו → יתגלו, אך לא כמשתמש.

האם זה יתגלו כמשתמש, echo reply → יתגלו 2 פעמיים על ידי אותו משתמש?

—> יתגלו 2 פעמיים → echo reply → יתגלו 2 פעמיים (seq number)

—> יתגלו 2 פעמיים על ידי המשתמש (UNION Ping)

Echo reply ->

```
[14]+ Stopped ping 8.8.8.8
root@9d56b5cb125d:/# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=110 time=53.8 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=64 time=70.7 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=2 ttl=64 time=24.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=110 time=57.1 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=3 ttl=64 time=19.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=110 time=52.4 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=4 ttl=64 time=27.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=110 time=52.2 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=5 ttl=64 time=26.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=110 time=51.9 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=6 ttl=64 time=35.8 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=110 time=53.0 ms (DUP!)
^Z
[15]+ Stopped ping 8.8.8.8
root@9d56b5cb125d:/#
```

:Duplicates

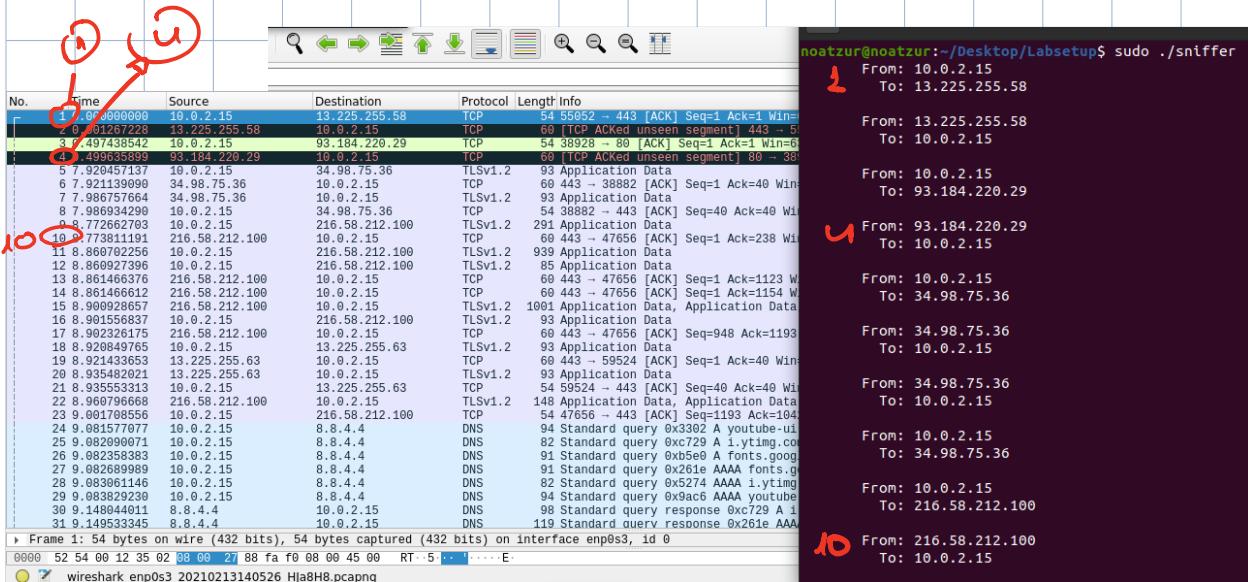
No.	Time	Source	Destination	Protocol	Length	Info
44	3.413707868	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x001d, seq=4/1024, ttl=110
45	4.364994725	10.9.0.5	8.8.8.8	ICMP	100	Echo (ping) request id=0x001d, seq=5/1280, ttl=64 (no response)
46	4.364994725	10.9.0.5	8.8.8.8	ICMP	100	Echo (ping) request id=0x001d, seq=5/1280, ttl=64 (reply in progress)
47	4.365058001	10.0.2.15	8.8.8.8	ICMP	100	Echo (ping) request id=0x001d, seq=5/1280, ttl=63 (reply in progress)
48	4.391090147	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x001d, seq=5/1280, ttl=64 (request)
49	4.391120115	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x001d, seq=5/1280, ttl=64
50	4.416788834	8.8.8.8	10.0.2.15	ICMP	100	Echo (ping) reply id=0x001d, seq=5/1280, ttl=111 (request)
51	4.416837214	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x001d, seq=5/1280, ttl=110
52	4.416877169	8.8.8.8	10.9.0.5	ICMP	100	Echo (ping) reply id=0x001d, seq=5/1280, ttl=110
53	5.365314196	10.9.0.5	8.8.8.8	ICMP	100	Echo (ping) request id=0x001d, seq=6/1536, ttl=64 (no response)
54	5.365314196	10.9.0.5	8.8.8.8	ICMP	100	Echo (ping) request id=0x001d, seq=6/1536, ttl=64 (reply in progress)
55	5.365392894	10.0.2.15	8.8.8.8	ICMP	100	Echo (ping) request id=0x001d, seq=6/1536, ttl=63 (reply in progress)
56	5.396058229	02:42:0a:09:00:05		ARP	44	Who has 10.9.0.1? Tell 10.9.0.5
57	5.396058229	02:42:0a:09:00:05		ARP	44	44 Who has 10.9.0.1? Tell 10.9.0.5
58	5.396297626	02:42:e4:1f:95:5a		ARP	44	44 10.9.0.1 is at 02:42:e4:1f:95:5a
59	5.396318647	02:42:e4:1f:95:5a		ARP	44	44 10.9.0.1 is at 02:42:e4:1f:95:5a
60	5.396318647	02:42:e4:1f:95:5a		TCP	100	Echo (ping) reply id=0x001d, seq=6/1536, ttl=64 (request)

Sniff - 92.1.C

תעלת אינטרנט

: 2.1A

. מילויים נטולים בפתקן כטבבן Sniffer יתבצע בסוף



Sniff - 92.1.C תעלת אינטרנט כטבבן Sniffer יתבצע WS-?

לפנינו מילויים נטולים בפתקן כטבבן Sniffer יתבצע WS-?

Sniff - 92.1.C !dst !src (Sniffer ?) ?ws- ?ws- ?ws- ?ws- ?ws-

Sniff - 92.1.C !dst !src (Sniffer ?) ?ws- ?ws- ?ws- ?ws- ?ws-

Sniff - 92.1.C !dst !src (Sniffer ?) ?ws- ?ws- ?ws- ?ws- ?ws-

: Question 1

① Pcap_lookupdev(errbuf);

הפעלת פונקציית הבדיקה (perror) על הdevice (כגון

פודט או היפר-בוקס) כמי שמצא (perror לא מופיע ככתוב).
שאנו מנסה לטעות בdevice.

כמי שמצא (perror לא מופיע ככתוב) בdevice.
הdevice (perror לא מופיע ככתוב).

② Pcap_open_live(myDEV, BUFSIZ, 1, 1000, errbuf);

פתיחת הdevice בmode "packet capture".

הdevice נקבע לdevice הקיים:

myDEV - Device (device name) בdevice - myDEV (Device)

BUFSIZ (buffer size) - BUFSIZ (snapshot size)

1 - promiscuous (promiscuous mode). (ctrl+alt+del)

errbuf - (promisc)

promiscuous - errbuf

0 - (time out)

1000 - (to_ms) (time out)

errbuf - errbuf (device name)

pcap_loop(handle, -1, got_Packet, NULL) -

② נסיגת ה-הפרוטון

(4) pcap_close (handle)-

מתקנים נייחים. ② Session ה-² בירור מושג ה-¹ Session ה-² ה-¹ ה-²

: Question 2

— ק promis mode כהו : Question 3

אנו מילאנו שיפר ב-
בכדי שיפר ימצא פולס הולא מילאנו שיפר

לפנינו. כהו שיפר מילאנו שיפר. כהו שיפר מילאנו שיפר.

— מילאנו שיפר מילאנו שיפר. כהו שיפר מילאנו שיפר.

ככה מילאנו שיפר מילאנו שיפר. כהו שיפר מילאנו שיפר.

IP (ה) — מילאנו שיפר מילאנו שיפר. כהו שיפר מילאנו שיפר.

. 8.8.8.8 ping (1-NNNN) (1-NNNN) (1-NNNN)

, מילאנו שיפר מילאנו שיפר. כהו שיפר מילאנו שיפר.

: מילאנו שיפר מילאנו שיפר. כהו שיפר מילאנו שיפר.

```
noa@noa-VirtualBox:~/Desktop$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=64 time=48.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=106 time=63.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=106 time=62.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=106 time=62.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=106 time=73.5 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=106 time=68.1 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=106 time=66.0 ms
^Z
[4]+ Stopped ping 8.8.8.8
noa@noa-VirtualBox:~/Desktop$
```

```
Activities Terminal Feb 23 17:31 en
noa@noa-VirtualBox:~/Desktop$ sudo ./sniff_2.1
noatzur@noatzur:~/Desktop/Labsetup$
```

promiscous mode

```
noa@noa-VirtualBox:~/Desktop$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=106 time=66.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=106 time=66.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=106 time=83.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=106 time=63.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=106 time=63.5 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=106 time=65.1 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=106 time=62.6 ms
^Z
[7]+ Stopped ping 8.8.8.8
noa@noa-VirtualBox:~/Desktop$
```

```
Activities Terminal Feb 23 17:36 en
noatzur@noatzur:~/Desktop/Labsetup$ sudo ./sniff_2.1
noatzur@noatzur:~/Desktop/Labsetup$ sudo password for noatzur:
noatzur@noatzur:~/Desktop/Labsetup$
```

promiscous mode

allow VM -> network ה-
allow VM -> network ה-
allow VM -> network ה-
allow VM -> network ה-

allow VM -> network ה-
allow VM -> network ה-
allow VM -> network ה-
allow VM -> network ה-

allow VM -> network ה-

Sniff_filter.c Sniff_filter2.c filters : 2.1B

ICMP sniff - Sniff_filter.c
Source ! destination - N
filter-exp filter -> C2' 8' 15' 16' 17' 18' 19' 20'

לע"ז בירכתי pcap-compile ו pcap-setfilter על מנת לרשום String הינו מערך של נוקדים (NN...NN) שיבואו כטבלה נורמה (normal) או לא-נורמל (abnormal). pcap-setfilter יאפשרfiltresession על מנת לרשום String הינו מערך של נוקדים (NN...NN) שיבואו כטבלה נורמל (normal) או לא-נורמל (abnormal).

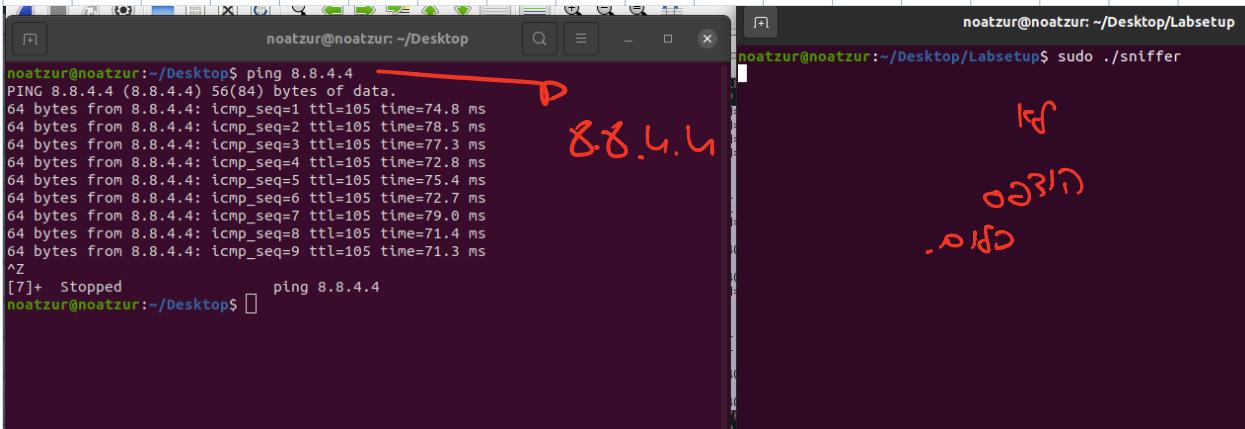
רשות רשת IP לא יכולה לשלוח IP לא נושא IP, כלומר לא יכול לשלוח IP לא נושא IP.

```
[+] noatzur@noatzur: ~/Desktop/Labsetup $ sudo ./sniffer
noatzur@noatzur:~/Desktop/Labsetup$ sudo ./sniffer
      From: 10.0.2.15
      To: 8.8.8.8
im an ICMP packet !!!
      From: 10.0.2.15
      To: 8.8.8.8
im an ICMP packet !!!
      From: 10.0.2.15
      To: 8.8.8.8
im an ICMP packet !!!
      From: 10.0.2.15
      To: 8.8.8.8
im an ICMP packet !!!
      From: 10.0.2.15
      To: 8.8.8.8
im an ICMP packet !!!
```

Sniffer ו Wireshark נורוּם 2 נורוּם 1 (טכניון) נורוּם 1 (טכניון) Sniffer ו Wireshark נורוּם 2 נורוּם 1 (טכניון) נורוּם 1 (טכניון)

No.	Time	Source	Destination	Protocol	Length	Info
31	0.570543984	192.114.46.176	10.0.2.15	TCP	60	443 - 38406 [FIN, ACK] Seq=1 Ack=26 Win=65535 Len=0
32	0.570742569	10.0.2.15	192.114.46.176	TCP	54	38406 - 443 [ACK] Seq=26 Ack=2 Win=63900 Len=0
33	0.570742569	10.0.2.15	192.114.46.176	TCP	60	443 - 38406 [ACK] Seq=26 Ack=26 Win=65535 Len=0
34	0.570814929	10.0.2.15	192.114.46.176	TCP	54	38404 - 443 [ACK] Seq=26 Ack=26 Win=63900 Len=0
35	1.372976530	10.0.2.15	65.9.109.34	TLSv1.2	93	Application Data
36	1.376565611	65.9.109.34	10.0.2.15	TCP	60	443 - 43760 [ACK] Seq=1 Ack=40 Win=65535 Len=0
37	1.392919336	65.9.109.34	10.0.2.15	TLSv1.2	93	Application Data
38	1.393383282	10.0.2.15	65.9.109.34	TCP	54	43760 - 443 [ACK] Seq=40 Ack=40 Win=63900 Len=0
39	2.376865568	10.0.2.15	91.228.74.198	TLSv1.2	100	Application Data
40	2.377197446	10.0.2.15	172.217.21.14	TLSv1.2	93	Application Data
41	2.379465778	91.228.74.198	10.0.2.15	TCP	60	443 - 55138 [ACK] Seq=1 Ack=47 Win=65535 Len=0
42	2.379466659	172.217.21.14	10.0.2.15	TCP	60	443 - 56094 [ACK] Seq=1 Ack=40 Win=65535 Len=0
43	2.445061257	172.217.21.14	10.0.2.15	TLSv1.2	93	Application Data
44	2.445174633	10.0.2.15	172.217.21.14	TCP	54	56094 - 443 [ACK] Seq=40 Ack=40 Win=63900 Len=0
45	2.445061861	91.228.74.198	10.0.2.15	TLSv1.2	100	Application Data
46	2.445391840	10.0.2.15	91.228.74.198	TCP	54	55138 - 443 [ACK] Seq=47 Ack=47 Win=63900 Len=0
47	2.550998145	10.0.2.15	192.114.43.110	TLSv1.2	78	[TCP Previous segment not captured] Application Data
48	2.551001779	10.0.2.15	192.114.43.110	TCP	54	4538 - 443 [FIN, ACK] Seq=26 Ack=2 Win=63900 Len=0
49	2.551001835	192.114.43.110	10.0.2.15	TCP	60	443 - ACKed unseen segment 443 - 4538 [ACK] Seq=1 Ack=2 Win=63900 Len=0
50	2.551001835	192.114.43.110	10.0.2.15	TCP	60	443 - 4538 [ACK] Seq=1 Ack=2 Win=65535 Len=0
51	2.567673281	192.114.43.110	10.0.2.15	TCP	60	443 - 4538 [FIN, ACK] Seq=27 Ack=2 Win=63900 Len=0
52	2.568165567	10.0.2.15	192.114.43.110	TCP	54	45538 - 443 [ACK] Seq=27 Ack=2 Win=63900 Len=0
53	2.804684091	10.0.2.15	192.114.43.110	TCP	54	45540 - 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
54	2.809774768	192.114.43.110	10.0.2.15	TCP	60	45540 - 443 [ACK] Seq=1 Ack=2 Win=65535 Len=0
55	3.283478198	10.0.2.15	8.8.8.8	ICMP	98	Echo (ping) request id=0x0010, seq=1/256, ttl=64 (reply in 5s)
56	3.350200167	8.8.8.8	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0010, seq=1/256, ttl=107 (request in 5s)
57	3.380886754	10.0.2.15	172.217.19.34	TLSv1.2	93	Application Data
58	3.381829778	10.0.2.15	172.217.19.34	TLSv1.2	93	Application Data
59	3.382173672	10.0.2.15	108.177.15.154	TLSv1.2	93	Application Data
60	3.382973604	172.217.19.34	10.0.2.15	TCP	60	443 - 45018 [ACK] Seq=40 Ack=40 Win=65535 Len=0
61	3.382973929	172.217.19.34	10.0.2.15	TCP	60	443 - 45020 [ACK] Seq=1 Ack=40 Win=65535 Len=0

הו נסחף ב-3 IP ה-10.0.2.15 מ-192.114.43.110 ל-10.0.2.15



Sniffer ה-10.0.2.15 מ-192.114.43.110 ל-10.0.2.15

Sniff_filter2.C

-TCP

10-100 מ-192.114.43.110 ל-10.0.2.15

ה-10.0.2.15 מ-192.114.43.110 ל-10-100

"top and dst portrange 10-100"

ה-10.0.2.15 מ-192.114.43.110 ל-10-100

8.8.8.8 מ-192.114.43.110 ל-10.0.2.15

23 מ-192.114.43.110 ל-10.0.2.15 - telnet

ה-10.0.2.15 מ-192.114.43.110 ל-10.0.2.15