

Lab 1: Sniff-then-spoof ARP

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. A display filter bar shows 'Apply a display filter ... <Ctrl-/>' and an 'Expression...' field.

No.	Time	Source	Destination	Protocol	Length	Info
5	2.000604023	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) request id=0x511a, seq=19/4864, ttl=6...
6	2.000839919	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) reply id=0x511a, seq=19/4864, ttl=6...
7	2.009670725	CadmusCo_86:a4:e5	CadmusCo_78:c8:72	ARP	60	Who has 192.168.56.102? Tell 192.168.56.103
8	2.009828718	CadmusCo_78:c8:72	CadmusCo_86:a4:e5	ARP	60	192.168.56.102 is at 08:00:27:78:c8:72
9	3.000577778	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) request id=0x511a, seq=20/5120, ttl=6...
10	3.000863884	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) reply id=0x511a, seq=20/5120, ttl=6...
11	4.000551892	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) request id=0x511a, seq=21/5376, ttl=6...
12	4.000675465	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) reply id=0x511a, seq=21/5376, ttl=6...

Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: CadmusCo_86:a4:e5 (08:00:27:86:a4:e5), Dst: CadmusCo_78:c8:72 (08:00:27:78:c8:72)
Address Resolution Protocol (request)

```
0000 08 00 27 78 c8 72 08 00 27 86 a4 e5 08 06 00 01 ..'x.r..'.....
0010 08 00 06 04 00 01 08 00 27 86 a4 e5 c0 a8 38 67 ..... '.....8g
0020 00 00 00 00 00 00 c0 a8 38 66 00 00 00 00 00 00 ..... 8f.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ..
```

SSH

Wireshark interface showing a network capture of an SSH session. The packet list displays several packets, with the selected packet (No. 2) being an SSH Server: Encrypted packet (len=36). The packet details pane shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and SSH Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.102	192.168.56.103	SSH	102	Client: Encrypted packet (len=36)
2	0.000570236	192.168.56.103	192.168.56.102	SSH	102	Server: Encrypted packet (len=36)
3	0.000803202	192.168.56.102	192.168.56.103	TCP	66	34404 → 22 [ACK] Seq=37 Ack=37 Win=305 Len=0 TSval=1
4	0.156416456	192.168.56.102	192.168.56.103	SSH	102	Client: Encrypted packet (len=36)
5	0.156797985	192.168.56.103	192.168.56.102	SSH	102	Server: Encrypted packet (len=36)
6	0.156926859	192.168.56.102	192.168.56.103	TCP	66	34404 → 22 [ACK] Seq=73 Ack=73 Win=305 Len=0 TSval=1
7	0.247697575	192.168.56.102	192.168.56.103	SSH	102	Client: Encrypted packet (len=36)

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0

- Ethernet II, Src: CadmusCo_86:a4:e5 (08:00:27:86:a4:e5), Dst: CadmusCo_78:c8:72 (08:00:27:78:c8:72)
- Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.102
- Transmission Control Protocol, Src Port: 22 (22), Dst Port: 34404 (34404), Seq: 1, Ack: 37, Len: 36
- SSH Protocol

```
0000  08 00 27 78 c8 72 08 00 27 86 a4 e5 08 00 45 10  ..'x.r.. '.....E.
0010  00 58 bf 14 40 00 40 06 89 5d c0 a8 38 67 c0 a8  .X..@. .]..8g..
0020  38 66 00 16 86 64 1b 5b 02 5b bc 7c 8e 6a 80 18  8f...d.[.[.].j..
0030  01 25 0b 05 00 00 01 01 08 0a 00 02 2f dc 00 02  .%. .... /...
0040  32 b3 dc 1e e7 ff 4b bf a1 c7 d5 0b 48 ae 65 9c  2....K. ....H.e.
0050  2f e5 29 58 4f 00 e9 df 8b 71 a5 e5 04 57 1d 76  /.)X0... .q...W.v
0060  4b cc bb f2 04 a1                                K.....
```

Data is encrypted

Telnet

Wireshark packet capture showing a Telnet session. The packet list shows a SYN, ACK, and data packets. The packet details show the Telnet data structure. The packet bytes show the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.102	192.168.56.103	TCP	74	53410 → 23 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SA...
2	0.000162027	192.168.56.103	192.168.56.102	TCP	74	23 → 53410 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 ...
3	0.000328680	192.168.56.102	192.168.56.103	TCP	66	53410 → 23 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval...
4	0.018463544	192.168.56.103	192.168.56.102	TELNET	78	Telnet Data ...
5	0.018649563	192.168.56.102	192.168.56.103	TCP	66	53410 → 23 [ACK] Seq=1 Ack=13 Win=29312 Len=0 TSva...
6	0.018831845	192.168.56.102	192.168.56.103	TELNET	78	Telnet Data ...
7	0.018834130	192.168.56.103	192.168.56.102	TCP	66	23 → 53410 [ACK] Seq=13 Ack=13 Win=29056 Len=0 TSv...

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: CadmusCo_78:c8:72 (08:00:27:78:c8:72), Dst: CadmusCo_86:a4:e5 (08:00:27:86:a4:e5)
Internet Protocol Version 4, Src: 192.168.56.102, Dst: 192.168.56.103
Transmission Control Protocol, Src Port: 53410 (53410), Dst Port: 23 (23), Seq: 0, Len: 0

0000 08 00 27 86 a4 e5 08 00 27 78 c8 72 08 00 45 10 ..'.....'x.r..E.
0010 00 3c 0e 84 40 00 40 06 3a 0a c0 a8 38 66 c0 a8 .<..@.@.8f..
0020 38 67 d0 a2 00 17 e5 8b 6d 8f 00 00 00 00 a0 02 8g.....m.....
0030 72 10 5c ec 00 00 02 04 05 b4 04 02 08 0a 00 05 r.\.....
0040 63 0b 00 00 00 00 01 03 03 07 c.....

enp0s8: <live capture in progress> Packets: 101 · Displayed: 101 (100.0%) Profile: Default

Data is not encrypted

It was possible to discover the password by looking at each message (each message sent one character)

<pre> 'x.r.. '.....E. .@f.@.@.8g.. 8f....NG ...tY\.. ..6..... ..'...Pass word: </pre>	<pre> .. '..... 'x.r..E. .5..@.@.8f.. 8g.....t Y\NG.... ...G..... ..d </pre>
<pre> .. '..... 'x.r..E. .5..@.@.8f.. 8g.....t Y]NG....Qi </pre>	<pre> '..... 'x.r..E. .5..@.@.8f.. 8g.....t Y^NG.... ...a..... .cg </pre>
<pre> .. '..... 'x.r..E. .5..@.@.8f.. 8g.....t Y_NG....i </pre>	<pre> .. '..... 'x.r..E. .5..@.@.8f.. 8g.....t Y`NG....1.. ..s </pre>
<pre> .. '..... 'x.r..E. .5..@.@.8f.. 8g.....t YaNG....K.. ..e </pre>	<pre> .. '..... 'x.r..E. .5..@.@.8f.. 8g.....t YbNG.... ...3..... ..c </pre>
<pre> .. '..... 'x.r..E. .6..@.@.8f.. 8g.....t YcNG....1.. </pre>	

ARP impersonation

The screenshot shows a Wireshark capture on interface enp0s8. The packet list displays several ICMP Echo (ping) requests and replies between 192.168.56.102 and 192.168.56.103. Packet 645 is selected, showing a ping reply from 192.168.56.103 to 192.168.56.102. The packet details pane shows the Ethernet II frame with source MAC 08:00:27:cd:cf:f6 and destination MAC 08:00:27:78:c8:72. The Internet Protocol Version 4 details show source 192.168.56.103 and destination 192.168.56.102. The Internet Control Message Protocol details show it's an Echo (ping) reply. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
640	3485.7228905...	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) request id=0x52c2, seq=1/256, ttl=64 ...
641	3485.7290681...	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) reply id=0x52c2, seq=1/256, ttl=128...
642	3486.7247216...	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) request id=0x52c2, seq=2/512, ttl=64 ...
643	3486.7692861...	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) reply id=0x52c2, seq=2/512, ttl=128...
644	3487.7261608...	192.168.56.102	192.168.56.103	ICMP	98	Echo (ping) request id=0x52c2, seq=3/768, ttl=64 ...
645	3487.7570793...	192.168.56.103	192.168.56.102	ICMP	98	Echo (ping) reply id=0x52c2, seq=3/768, ttl=128...
646	3502.7244562...	192.168.56.1	224.0.0.251	MDNS	462	Standard query 0x0000 PTR _airport._tcp.local, "QM...
647	3502.7525382...	192.168.56.1	192.168.56.255	DB-LSP...	208	Dropbox LAN sync Discovery Protocol

Frame 645: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: CadmusCo_cd:cf:f6 (08:00:27:cd:cf:f6), Dst: CadmusCo_78:c8:72 (08:00:27:78:c8:72)
Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.102
Internet Control Message Protocol

```
0000 08 00 27 78 c8 72 08 00 27 cd cf f6 08 00 45 00 ..'x.r.. '....E.
0010 00 54 aa 42 00 00 00 01 9e 48 c0 a8 38 67 c0 a8 .T.B.... .H...8g..
0020 38 66 00 00 ea 6f 52 c2 00 03 6d 8d 55 58 0a e2 8f...oR. ..m.UX..
0030 0a 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 .....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... !"#$$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060 36 37 67
```

08:00:27:cd:cf:f6 is 192.168.56.100 and is impersonating 192.168.56.103

Lab 2: Firewall

Blocked

```
digitalsec@digitalsec-VM: ~  
digitalsec@digitalsec-VM:~$ sudo iptables -A INPUT -p tcp --dport telnet -j DROP  
[sudo] password for digitalsec:  
Sorry, try again.  
[sudo] password for digitalsec:  
Sorry, try again.  
[sudo] password for digitalsec:  
digitalsec@digitalsec-VM:~$ sudo iptables -A INPUT -p tcp --dport telnet -j DROP  
digitalsec@digitalsec-VM:~$ sudo iptables -A OUTPUT -p tcp --dport telnet -j DROP  
digitalsec@digitalsec-VM:~$ telnet 192.168.56.102 23  
Trying 192.168.56.102...
```

Blocked

```
digitalsec@digitalsec-VM: ~  
digitalsec@digitalsec-VM:~$ telnet 192.168.56.101  
Trying 192.168.56.101...  
^C  
digitalsec@digitalsec-VM:~$ telnet 192.168.56.101 23  
Trying 192.168.56.101...
```


Not blocked

```
digitalsec@digitalsec-VM: ~  
[sudo] password for digitalsec:  
Sorry, try again.  
[sudo] password for digitalsec:  
digitalsec@digitalsec-VM:~$ sudo iptables -A INPUT -p tcp --dport telnet -j DROP  
digitalsec@digitalsec-VM:~$ sudo iptables -A OUTPUT -p tcp --dport telnet -j DROP  
digitalsec@digitalsec-VM:~$ telnet 192.168.56.102 23  
Trying 192.168.56.102...  
^C  
digitalsec@digitalsec-VM:~$ sudo iptables -D INPUT 1  
digitalsec@digitalsec-VM:~$ sudo iptables -D OUTPUT 1  
digitalsec@digitalsec-VM:~$ sudo iptables -A INPUT -p tcp --dport telnet -m state --state NEW,ESTABLISHED -j ACCEPT  
digitalsec@digitalsec-VM:~$ sudo iptables -A OUTPUT -p tcp --dport telnet -m state --state NEW,ESTABLISHED -j ACCEPT  
digitalsec@digitalsec-VM:~$ sudo iptables -A INPUT -p tcp --dport telnet -j DROP  
digitalsec@digitalsec-VM:~$ sudo iptables -A OUTPUT -p tcp --dport telnet -j DROP  
digitalsec@digitalsec-VM:~$ telnet 192.168.56.102 23  
Trying 192.168.56.102...  
Connected to 192.168.56.102.  
Escape character is '^]'.  
Ubuntu 16.04.1 LTS  
digitalsec-VM login: █
```

Blocked

```
digitalsec@digitalsec-VM: ~  
digitalsec@digitalsec-VM:~$ telnet 192.168.56.101  
Trying 192.168.56.101...  
^C  
digitalsec@digitalsec-VM:~$ telnet 192.168.56.101 23  
Trying 192.168.56.101...  
^[^C  
digitalsec@digitalsec-VM:~$ telnet 192.168.56.101 23  
Trying 192.168.56.101...
```

Tunneling

```
digitalsec@digitalsec-VM: ~  
digitalsec@digitalsec-VM:~$ ssh -L 4500:localhost:23 digitalsec@192.168.56.101  
digitalsec@192.168.56.101's password:  
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-53-generic i686)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
193 packages can be updated.  
4 updates are security updates.  
  
Last login: Sun Dec 18 20:26:38 2016 from 192.168.56.102  
digitalsec@digitalsec-VM:~$ channel 3: open failed: connect failed: Connection t  
imed out
```

```
digitalsec@digitalsec-VM: ~  
digitalsec@digitalsec-VM:~$ telnet localhost 4500  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
Ubuntu 16.04.1 LTS  
digitalsec-VM login: █
```


Lab 3: DoS

Ponging 103 from 102

The image shows a Wireshark packet capture window titled "Capturing from enp0s8". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons for packet capture and analysis. Below the toolbar is a display filter bar with the text "Apply a display filter ... <Ctrl-/>".

The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
6	14.508636471	192.168.56.1	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, ...
7	29.478339968	192.168.56.103	192.168.56.101	ICMP	60	Echo (ping) request id=0x0015, seq=39596/44186, t...
8	29.478406262	192.168.56.101	192.168.56.103	ICMP	54	Echo (ping) reply id=0x0015, seq=39596/44186, t...
9	30.068613029	192.168.56.1	192.168.56.255	DB-LSP...	208	Dropbox LAN sync Discovery Protocol
10	34.487733454	CadmusCo_b2:67:a8	CadmusCo_86:a4:e5	ARP	42	Who has 192.168.56.103? Tell 192.168.56.101
11	34.488071723	CadmusCo_86:a4:e5	CadmusCo_b2:67:a8	ARP	60	192.168.56.103 is at 08:00:27:86:a4:e5
12	41.566368132	192.168.56.1	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, ...

The packet details pane for the selected packet (No. 7) shows the following structure:

- Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: CadmusCo_86:a4:e5 (08:00:27:86:a4:e5), Dst: CadmusCo_b2:67:a8 (08:00:27:b2:67:a8)
- Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.101
- Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 08 00 27 b2 67 a8 08 00 27 86 a4 e5 08 00 45 00 ..'.g... '.....E.
0010 00 28 35 e3 00 00 80 01 12 d5 c0 a8 38 67 c0 a8 .(5.....8g..
0020 38 65 08 00 f6 d0 00 15 9a ac 61 62 63 64 65 66 8e.....abcdef
0030 67 68 69 6a 6b 6d 00 00 00 00 00 00          ghijklm.. ....
```

The status bar at the bottom indicates "enp0s8: <live capture in progress>", "Packets: 12 · Displayed: 12 (100.0%)", and "Profile: Default".

SYN flooding 103

Capturing from enp0s8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
579	20.522540068	199.253.94.130	192.168.56.103	TCP	60	1787 → 23 [SYN] Seq=0 Win=1500 Len=0
580	20.522726679	90.169.167.241	192.168.56.103	TCP	60	58141 → 23 [SYN] Seq=0 Win=1500 Len=0
581	20.522728815	218.175.86.247	192.168.56.103	TCP	60	34691 → 23 [SYN] Seq=0 Win=1500 Len=0
582	20.522729485	104.136.183.35	192.168.56.103	TCP	60	23277 → 23 [SYN] Seq=0 Win=1500 Len=0
583	20.522729971	68.4.171.14	192.168.56.103	TCP	60	33190 → 23 [SYN] Seq=0 Win=1500 Len=0
584	20.522859025	50.15.212.239	192.168.56.103	TCP	60	28762 → 23 [SYN] Seq=0 Win=1500 Len=0
585	20.522860875	187.151.29.6	192.168.56.103	TCP	60	16484 → 23 [SYN] Seq=0 Win=1500 Len=0
586	20.523000853	109.92.27.145	192.168.56.103	TCP	60	21656 → 23 [SYN] Seq=0 Win=1500 Len=0

▶ Frame 179: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: CadmusCo_86:a4:e5 (08:00:27:86:a4:e5)
▶ Internet Protocol Version 4, Src: 64.204.19.175, Dst: 192.168.56.103
▶ Transmission Control Protocol, Src Port: 58635 (58635), Dst Port: 23 (23), Seq: 0, Len: 0

0000 08 00 27 86 a4 e5 00 00 00 00 00 08 00 45 00 ..'. E.
0010 00 28 db 89 00 00 00 06 11 bc 40 cc 13 af c0 a8 .(.... .@....
0020 38 67 e5 0b 00 17 f1 88 00 46 00 00 00 50 02 8g F....P.
0030 05 dc 85 8a 00 00 00 00 00 00 00 00

enp0s8: <live capture in progress> Packets: 310237 · Displayed: 310237 (100.0%) Profile: Default