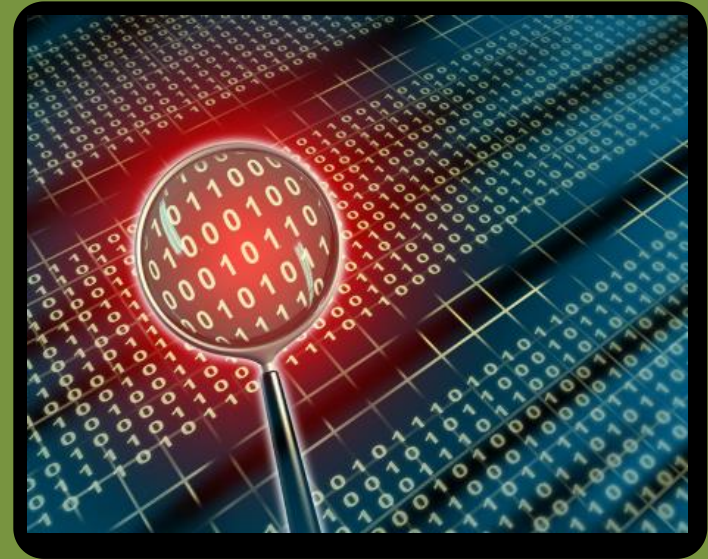


Advanced Network Forensics

- User/Password Crack.
- Port Scan.
- Signature Detection.
- Converted Formats.
- ARP Spoofing.
- DDoS Detection.





hping



Hydra



1.pcap

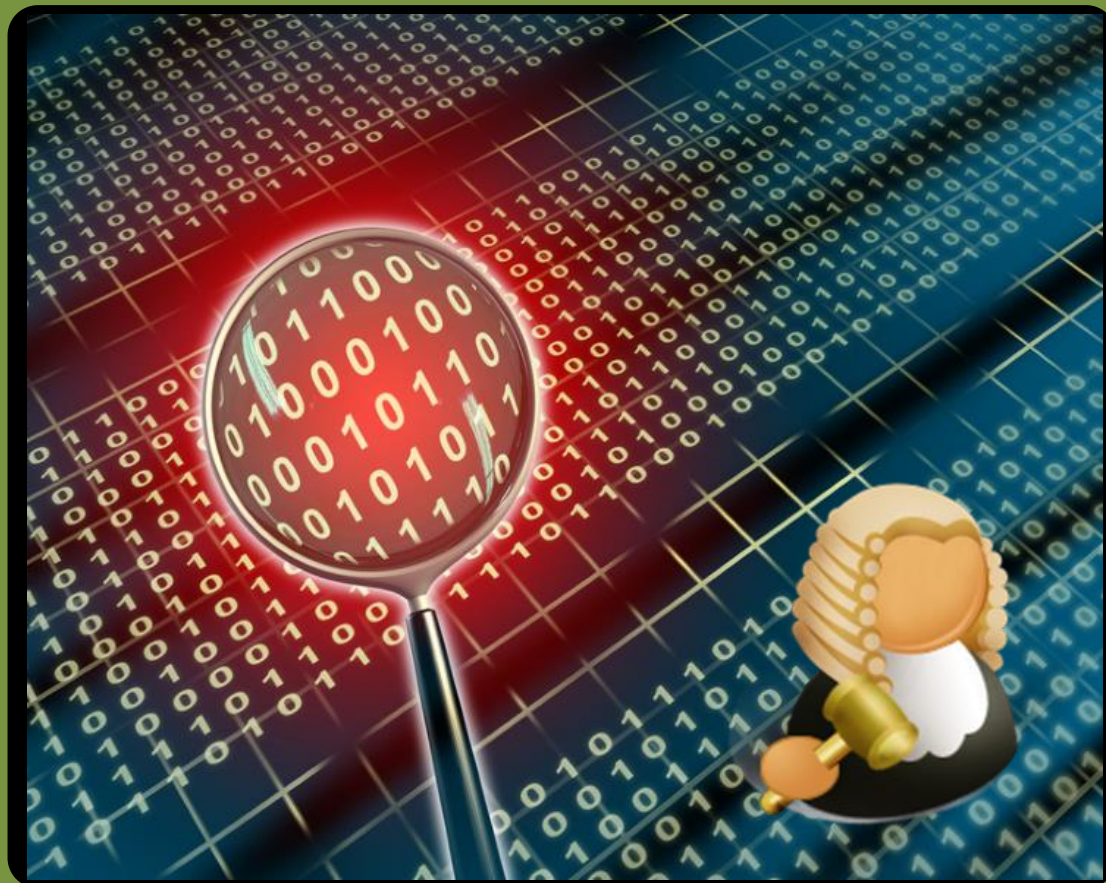
Snort -i 1 -c 1.rules



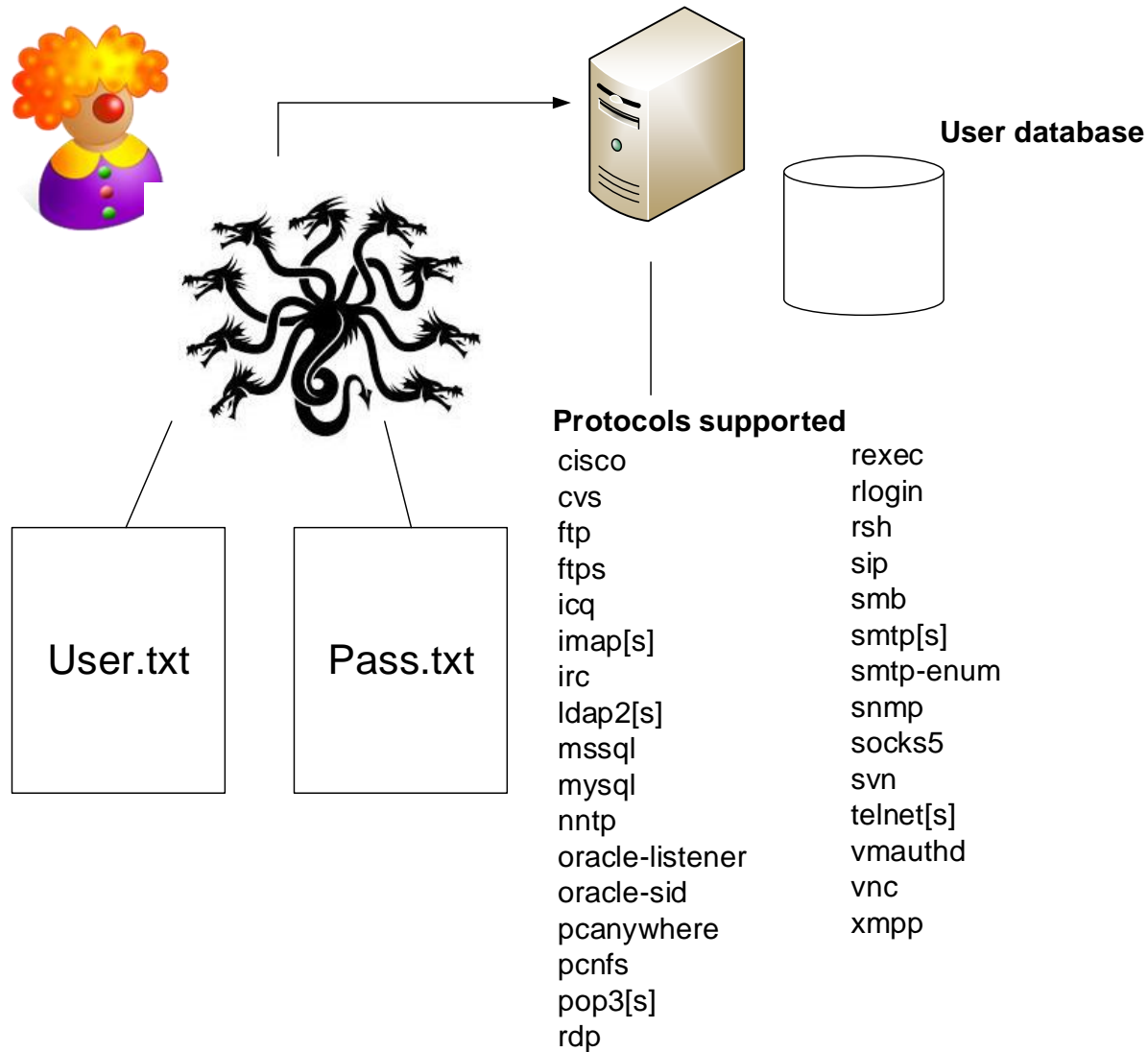
alert.ids

Snort -i 1 -r 1.pcap

Advanced Network Forensics



User/Password Crack





ftp.response.code

Correct login:

ftp.response.code==230

Incorrect login:

ftp.response.code==530

```

No.    Time    Source    Destination    Protocol    Length    Info
0. 0.47130.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 108 Response: 331 Password required for Administrator.
209 0.47156.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 108 Response: 331 Password required for Administrator.
213 0.47446.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 108 Response: 331 Password required for Administrator.
215 0.49207.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 96 Response: 530 User fred cannot log in.
218 0.49218.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 96 Response: 530 User fred cannot log in.
219 0.49912.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 108 Response: 331 Password required for Administrator.
220 0.49963.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 108 Response: 331 Password required for Administrator.
223 0.50570.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 96 Response: 530 User fred cannot log in.
228 0.51962.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 96 Response: 530 User fred cannot log in.
231 0.52736.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 96 Response: 530 User napier cannot log in.
246 0.54357.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 101 Response: 230 User Administrator logged in.
251 0.55028.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 96 Response: 530 User napier cannot log in.
252 0.55135.192.168.75.132 192.168.75.1 192.168.75.1 192.168.75.1 192.168.75.1 96 Response: 530 User napier cannot log in.

* Frame 246: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on 0
* Ethernet II, Src: VMware_0f:71:a3 (00:0c:29:0f:71:a3), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
* Internet Protocol Version 4, Src: 192.168.75.132 (192.168.75.132), Dst: 192.168.75.1 (192.168.75.1)
* Transmission Control Protocol, Src Port: ftp (21), Dst Port: 18164 (18164), Seq: 198, Ack: 84, Len: 35
* File Transfer Protocol (FTP)

0000 00 50 56 c0 00 08 00 29 0f 71 a3 08 00 45 00 ..P....}.q...E.
0010 00 57 0f 17 40 00 08 00 d0 b3 c0 a8 4b 01 c0 a8 ..W..0....K...
0020 4b 01 c0 a8 4b 01 c0 a8 4b 01 c0 a8 4b 01 c0 a8 ..K...F...K...
0030 fa 9d 0f a2 00 00 01 01 08 0a 00 71 c0 00 00 ..8...6...6...
0040 c0 a7 32 33 30 20 55 73 65 72 20 41 64 6d 69 6e ...230 Us er Admin
0050 69 73 74 72 61 74 6f 72 20 6f 6f 67 67 65 64 20 ..trator logged
0060 69 6e 2e 0d 0a ..in...

```

ftp contains "PASS"

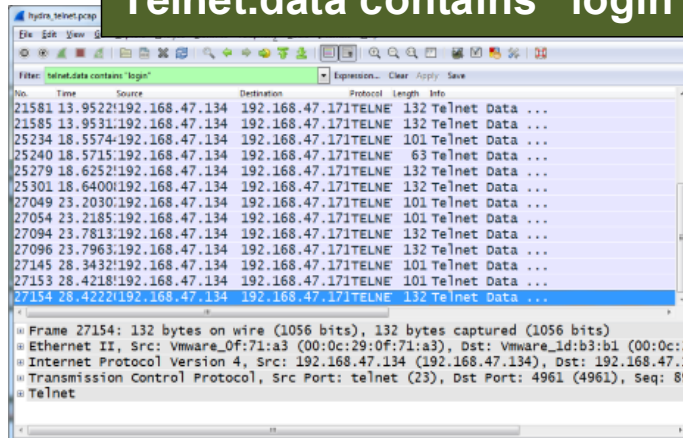
"Administrator" search:

ftp contains "Administrator"

Time	192.168.75.1	192.168.75.132	Comment
0.050571	18168 > ftp [SYN] S		TCP: 18168 > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1460
0.051163	18171 > ftp [SYN] S		TCP: 18171 > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1460
0.051412	ftp > 18168 [SYN] A		TCP: ftp > 18168 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
0.051502	18168 > ftp [ACK] S		TCP: 18168 > ftp [ACK] Seq=1 Ack=1 Win=66608 Len=0 TSv
0.051686	ftp > 18171 [SYN, ACK] S		TCP: ftp > 18171 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
0.051757	18171 > ftp [ACK] S		TCP: 18171 > ftp [ACK] Seq=1 Ack=1 Win=66608 Len=0 TSv
0.052312	Response: 220 Micro		FTP: Response: 220 Microsoft FTP Service
0.052670	Response: 220 Micro		FTP: Response: 220 Microsoft FTP Service
0.057815	18172 > ftp [SYN] S		TCP: 18172 > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1460
0.058506	ftp > 18172 [SYN] A		TCP: ftp > 18172 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
0.058603	18172 > ftp [ACK] S		TCP: 18172 > ftp [ACK] Seq=1 Ack=1 Win=66608 Len=0 TSv
0.059942	Response: 220 Micro		FTP: Response: 220 Microsoft FTP Service
0.190869	Request: USER test		FTP: Request: USER test
0.191066	Request: USER test		FTP: Request: USER test
0.191250	Request: USER admin		FTP: Request: USER admin
0.191424	Request: USER admin		FTP: Request: USER admin
0.191611	Request: USER admin		FTP: Request: USER admin
0.191792	Request: USER admin		FTP: Request: USER admin
0.191976	Request: USER test1		FTP: Request: USER test1
0.192166	Request: USER test1		FTP: Request: USER test1
0.197452	Response: 331 Passw		FTP: Response: 331 Password required for test.
0.197902	Response: 331 Passw		FTP: Response: 331 Password required for test.
0.198263	Response: 331 Passw		FTP: Response: 331 Password required for admin.
0.198875	Request: PASS passw		FTP: Request: PASS password
0.199015	Request: PASS none		FTP: Request: PASS none

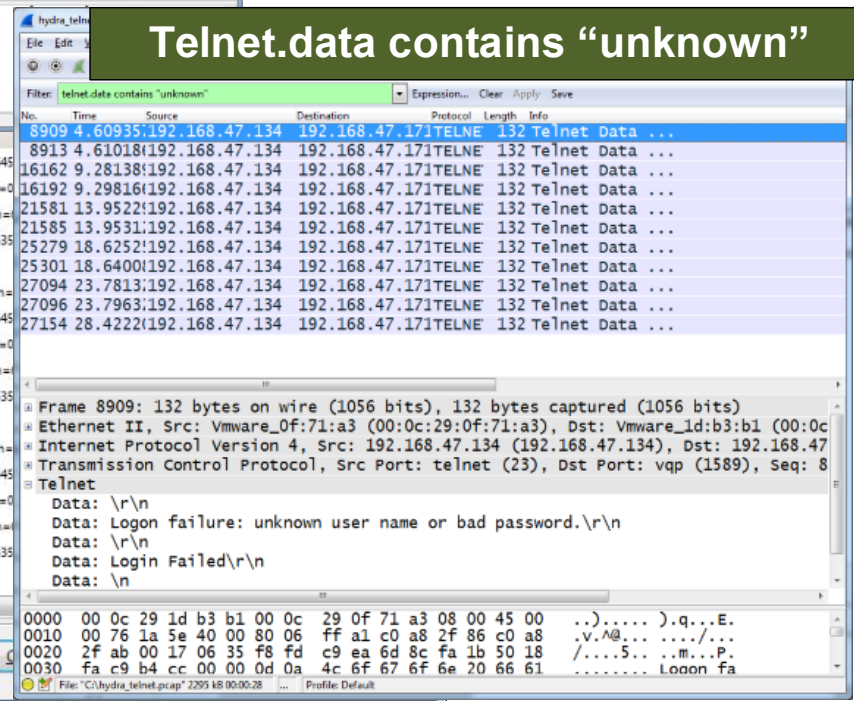
No.	Time	Source	Destination	Protocol	Length	Info
193	0.41634	192.168.75.1	192.168.75.132	FTP	86	Request: USER Administrator
195	0.41714	192.168.75.132	192.168.75.1	FTP	108	Response: 331 Password required for Administrator
196	0.41860	192.168.75.1	192.168.75.132	FTP	86	Request: USER Administrator
198	0.42000	192.168.75.132	192.168.75.1	FTP	108	Response: 331 Password required for Administrator
205	0.46854	192.168.75.1	192.168.75.132	FTP	86	Request: USER Administrator
206	0.46928	192.168.75.1	192.168.75.132	FTP	86	Request: USER Administrator
208	0.47130	192.168.75.132	192.168.75.1	FTP	108	Response: 331 Password required for Administrator
209	0.47156	192.168.75.132	192.168.75.1	FTP	108	Response: 331 Password required for Administrator
212	0.47377	192.168.75.1	192.168.75.132	FTP	86	Request: USER Administrator
213	0.47446	192.168.75.132	192.168.75.1	FTP	108	Response: 331 Password required for Administrator
217	0.49355	192.168.75.1	192.168.75.132	FTP	86	Request: USER Administrator
218	0.49764	192.168.75.1	192.168.75.132	FTP	86	Request: USER Administrator
219	0.49912	192.168.75.132	192.168.75.1	FTP	108	Response: 331 Password required for Administrator

Telnet.data contains "login"



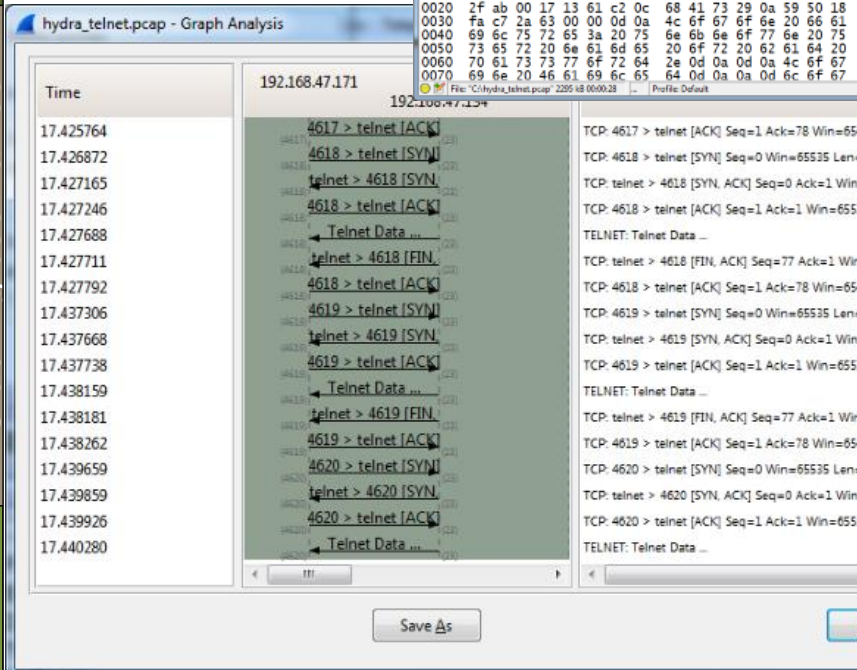
Bad Login:

Telnet.data contains "unknown"



Cracking usernames

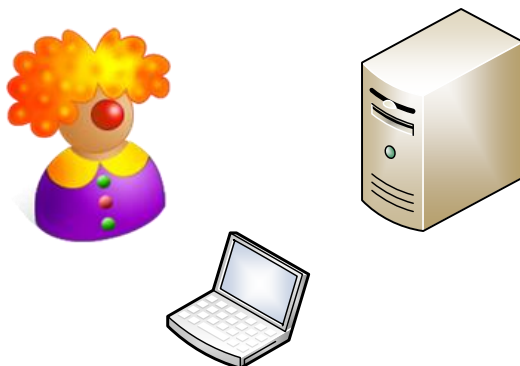
Adv Net For.



http://asecuritysite.com/log/hydra_telnet.zip

Author: Prof Bill Buchanan

Hydra (Telnet)



```
C:\Snort\bin> type 1.rules
```

```
alert tcp any 21 -> any any (msg:"FTP Bad login"; content:"530 User ";  
nocase; flow:from_server,established; sid:491; rev:5;)
```

```
C:\Snort\bin> snort -i 1 -c 1.rules -l log
```

```
C:\hydra>hydra -L user.txt -P pass.txt  
192.168.47.134 ftp
```

Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (<http://www.thc.org/thc-hydra>) starting at 2014-01-05 16:44:01

[DATA] 12 tasks, 1 server, 12 login tries (l:3/p:4), ~1 try per task

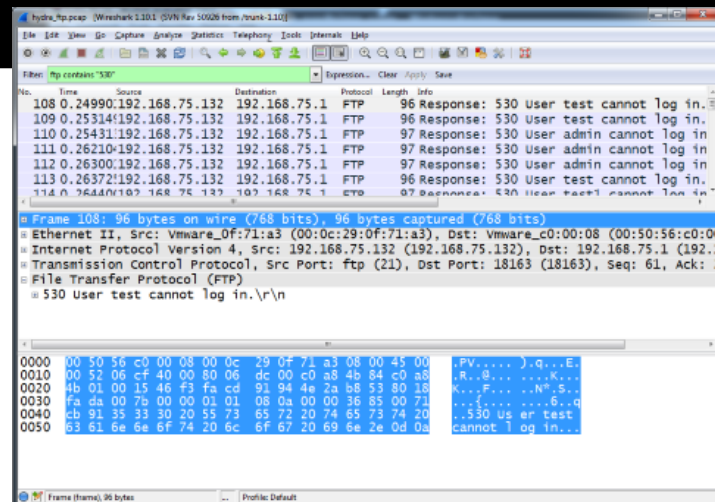
[DATA] attacking service ftp on port 21

[STATUS] attack finished for 192.168.47.134 (waiting for children to finish)

[21][ftp] host: 192.168.47.134 login:
administrator password: napier

1 of 1 target successfully completed, 1 valid password found

Hydra (<http://www.thc.org/thc-hydra>) finished at 2014-01-05 16:44:02



```
[**] [1:491:5] FTP Bad login [**]
```

```
[Priority: 0]
```

```
01/05-16:46:25.815069 192.168.47.134:21 -> 192.168.47.171:1230
```

```
TCP TTL:128 TOS:0x0 ID:26286 IpLen:20 DgmLen:79 DF
```

```
***AP*** Seq: 0x6852C889 Ack: 0x9F128FC0 Win: 0xFACF TcpLen: 20
```

```
[**] [1:491:5] FTP Bad login [**]
```

```
[Priority: 0]
```

```
01/05-16:46:25.815104 192.168.47.134:21 -> 192.168.47.171:1231
```

```
TCP TTL:128 TOS:0x0 ID:26287 IpLen:20 DgmLen:79 DF
```

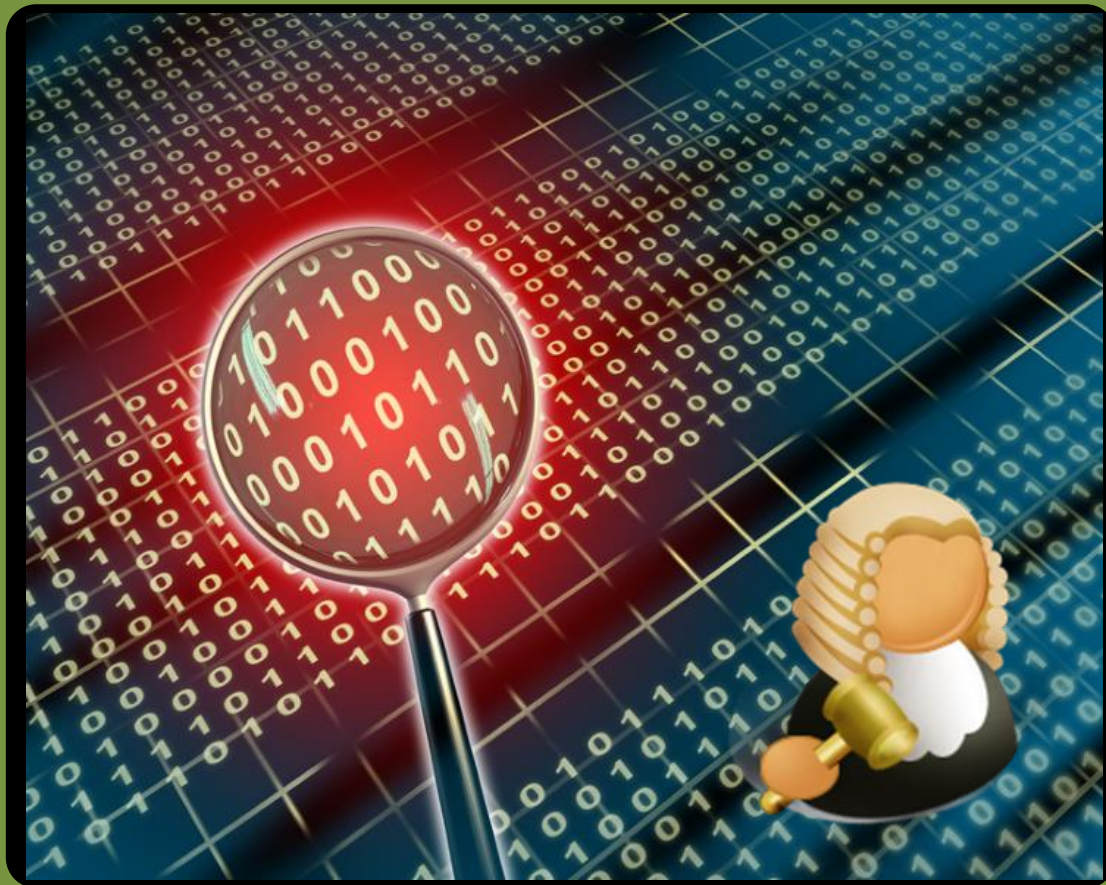
```
***AP*** Seq: 0x528728E2 Ack: 0x88B7039E Win: 0xFACD TcpLen: 20
```

http://asecuritysite.com/log/hydra_ftp.zip

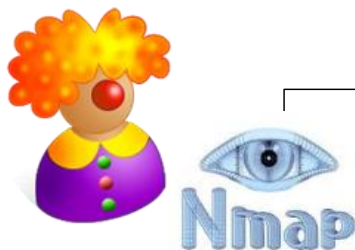
Author: Prof Bill Buchanan

Hydra (Snort detection)

Advanced Network Forensics



Port Scan



HOST DISCOVERY:

- sL: List Scan - simply list targets to scan
- sn: Ping Scan - disable port scan
- Pn: Treat all hosts as online -- skip host discovery
- PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports

- PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
- PO[protocol list]: IP Protocol Ping
- n/-R: Never do DNS resolution/Always resolve [default: sometimes]

SCAN TECHNIQUES:

- ss/st/sa/sw/sm: TCP SYN/Connect()/ACK/window/Maimon scans
- SU: UDP Scan
- SN/SF/SX: TCP Null, FIN, and Xmas scans

OS DETECTION:

- O: Enable OS detection

```
C:\Documents and Settings\Administrator> nmap -ss 192.168.47.134
```

```
Host is up (0.00088s latency).
```

```
Not shown: 973 closed ports
```

PORT	STATE	SERVICE
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
17/tcp	open	qotd
19/tcp	open	chargen
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet

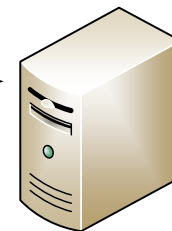
```
..
```

```
5900/tcp open  vnc
```

```
8099/tcp open  unknown
```

```
MAC Address: 00:0C:29:0F:71:A3 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds
```



[SYN], Port 1

Port
open

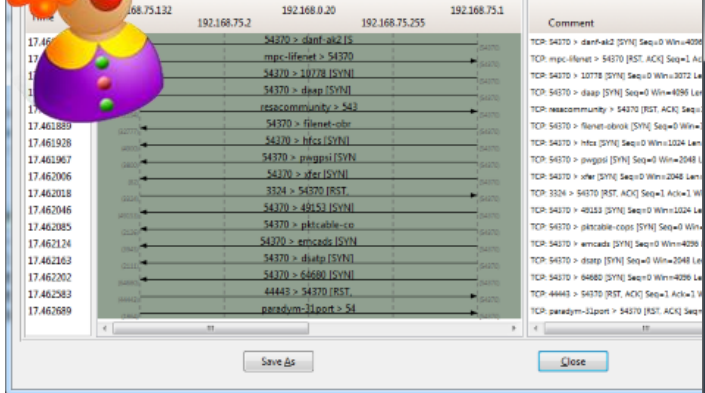
[SYN, ACK], Port 1

[ACK], Port 1

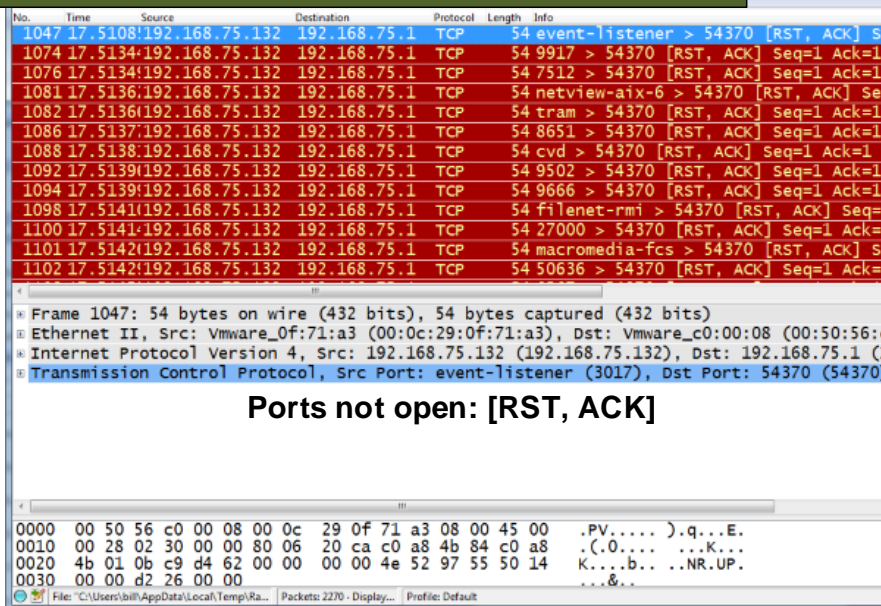
[SYN], Port 21

Port
closed

[RST, ACK], Port 21

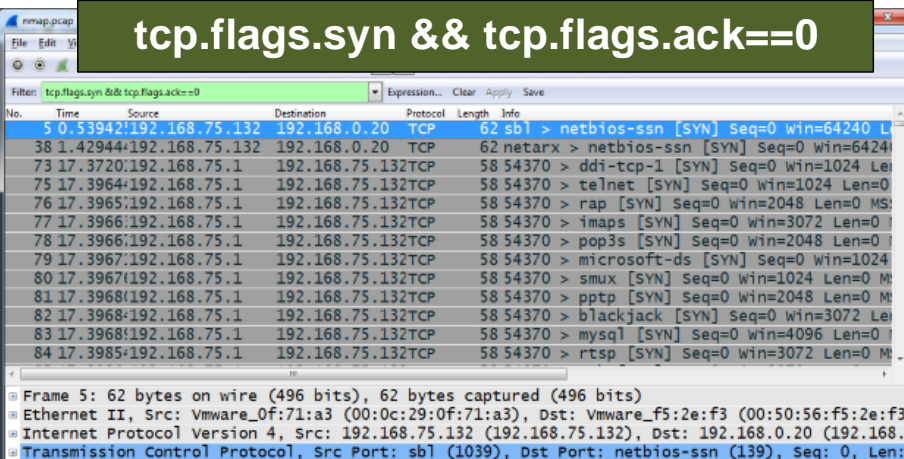


**ip.src==192.168.75.132 &&
tcp.flags.reset && tcp.flags.ack**

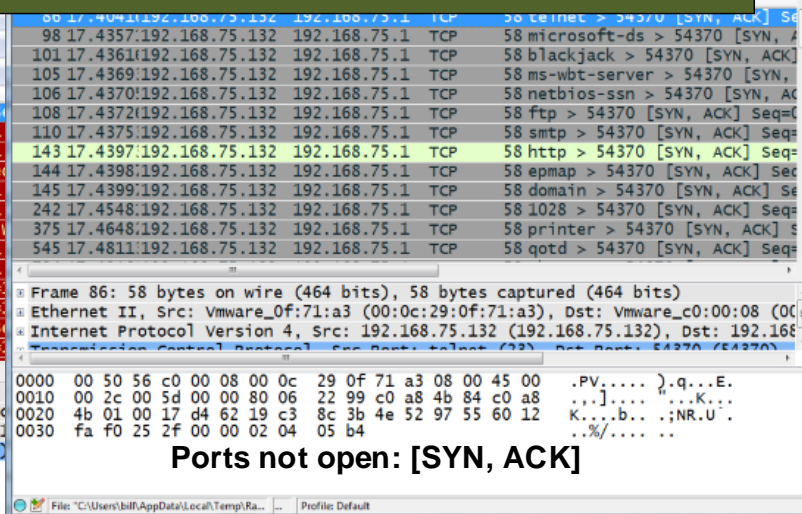


Ports not open: [RST, ACK]

tcp.flags.syn && tcp.flags.ack==0



**ip.src==192.168.75.132 &&
tcp.flags.syn==1 && tcp.flags.ack==1**



Ports not open: [SYN, ACK]



Xmas Tree [FIN,PSH,URG]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000	192.168.47.132	192.168.47.1	TCP	54	53004 > submission [FIN, PSH, URG] Seq=1 Win=1024
2	0.00000	192.168.47.132	192.168.47.1	TCP	54	53004 > domain [FIN, PSH, URG] Seq=1 Win=1024
3	0.00000	192.168.47.132	192.168.47.1	TCP	54	53004 > rfb [FIN, PSH, URG] Seq=1 Win=1024
4	0.00033	192.168.47.1	192.168.47.132	TCP	54	rfb > 53004 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
5	0.00378	192.168.47.132	192.168.47.1	TCP	54	53004 > telnet [FIN, PSH, URG] Seq=1 Win=1024
6	0.00378	192.168.47.132	192.168.47.1	TCP	54	53004 > smtp [FIN, PSH, URG] Seq=1 Win=1024
7	0.00381	192.168.47.1	192.168.47.132	TCP	54	telnet > 53004 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
8	0.00383	192.168.47.1	192.168.47.132	TCP	54	smtp > 53004 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
9	0.00745	192.168.47.132	192.168.47.1	TCP	54	53004 > blackjack [FIN, PSH, URG] Seq=1 Win=1024
10	0.00745	192.168.47.132	192.168.47.1	TCP	54	53004 > auth [FIN, PSH, URG] Seq=1 Win=1024
11	0.00745	192.168.47.132	192.168.47.1	TCP	54	53004 > http [FIN, PSH, URG] Seq=1 Win=1024
12	0.00745	192.168.47.132	192.168.47.1	TCP	54	53004 > microsoft-ds [FIN, PSH, URG] Seq=1 Win=1024
13	0.00748	192.168.47.1	192.168.47.132	TCP	54	blackjack > 53004 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
14	0.00751	192.168.47.1	192.168.47.132	TCP	54	auth > 53004 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
15	0.00752	192.168.47.1	192.168.47.132	TCP	54	http > 53004 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
16	0.00754	192.168.47.1	192.168.47.132	TCP	54	microsoft-ds > 53004 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

Frame 9: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Vmware_5e:b3:93 (00:0c:29:5e:b3:93), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.47.132 (192.168.47.132), Dst: 192.168.47.1 (192.168.47.1)
Transmission Control Protocol, Src Port: 53004 (53004), Dst Port: blackjack (1025), Seq: 1, Len: 0

0000 00 50 56 c0 00 08 00 29 5e b3 93 08 00 45 00 .PV....)^....E.
0010 00 28 95 85 00 25 06 20 75 c0 a8 2f 84 c0 a8 .(....% u./...
0020 2f 01 cf 04 01 a8 e8 17 42 00 00 00 00 50 29 /.....B.....P
0030 08 00 e2 cd 00 00

<http://asecuritysite.com/log/nmap.zip>

UDP Scan

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000	Vmware_5e:b3:93	Broadcast	ARP	42	who has 192.168.47.1? Tell 192.168.47.132
2	0.00002	Vmware_c0:00:08	Vmware_5e:b3:93	SARP	42	192.168.47.1 is at 00:50:56:c0:00:08
3	0.00059	192.168.47.132	192.168.47.2	DNS	85	standard query 0x5311 PTR 1.47.168.192.in-addr
4	0.02799	192.168.47.2	192.168.47.132	DNS	135	standard query response 0x5311 No such name
5	0.03123	Vmware_5e:b3:93	Broadcast	ARP	42	who has 192.168.47.1? Tell 192.168.47.132
6	0.03125	Vmware_c0:00:08	Vmware_5e:b3:93	SARP	42	192.168.47.1 is at 00:50:56:c0:00:08
7	0.03146	192.168.47.132	192.168.47.1	UDP	42	source port: 54890 Destination port: 1000
8	0.03146	192.168.47.132	192.168.47.1	UDP	42	source port: 54890 Destination port: 33717
9	0.03146	192.168.47.132	192.168.47.1	UDP	42	source port: 54890 Destination port: 30656
10	1.13173	192.168.47.132	192.168.47.1	UDP	42	source port: 54891 Destination port: 30656
11	1.13174	192.168.47.132	192.168.47.1	UDP	42	source port: 54891 Destination port: 33717
12	1.13174	192.168.47.132	192.168.47.1	UDP	42	source port: 54891 Destination port: 1000
13	1.13174	192.168.47.132	192.168.47.1	UDP	42	source port: 54891 Destination port: 62677
14	1.13174	192.168.47.132	192.168.47.1	UDP	42	source port: 54891 Destination port: 18250
15	1.13174	192.168.47.132	192.168.47.1	UDP	42	source port: 54891 Destination port: 53838
16	1.13174	192.168.47.132	192.168.47.1	UDP	42	source port: 54891 Destination port: 49396

Frame 7: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: Vmware_5e:b3:93 (00:0c:29:5e:b3:93), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.47.132 (192.168.47.132), Dst: 192.168.47.1 (192.168.47.1)
User Datagram Protocol, Src Port: 54890 (54890), Dst Port: 1000 (1000)

0000 00 50 56 c0 00 08 00 29 5e b3 93 08 00 45 00 .PV....)^....E.
0010 00 1c 12 a3 00 28 11 a0 58 c0 a8 2f 84 c0 a8 .(....X./...
0020 2f 01 de 6a 03 e8 00 08 45 b5

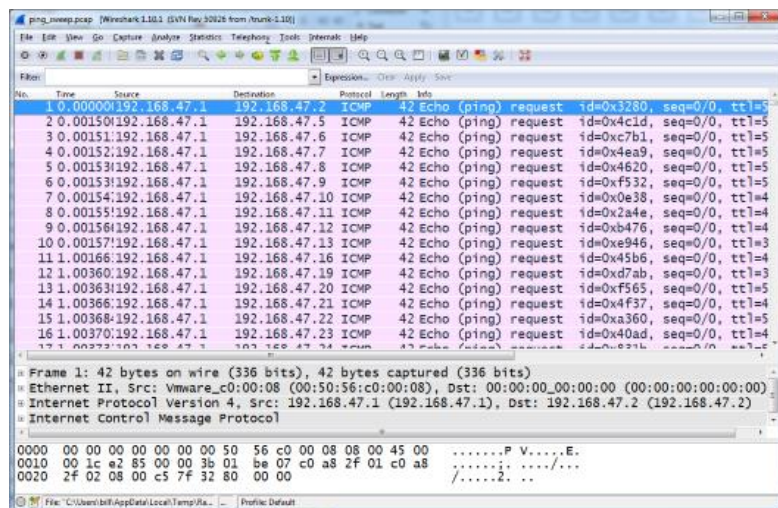
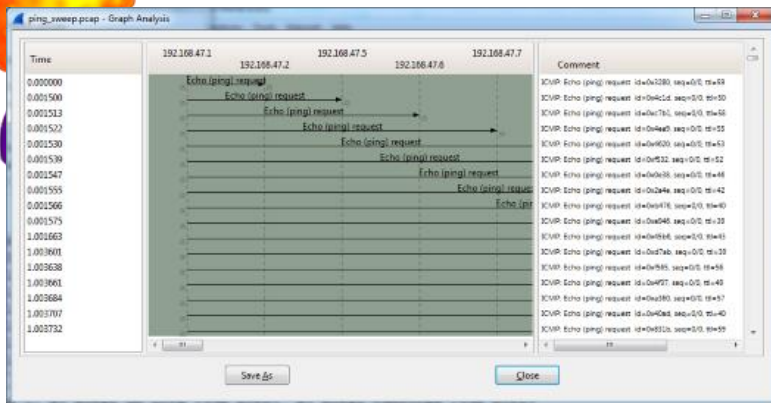
Null [...]

No.	Time	Source	Destination	Protocol	Length	Info
7	1.38659	192.168.47.171	192.168.47.134	TCP	54	51250 > mysql [None] Seq=1 win=1024 Len=0
8	1.38662	192.168.47.171	192.168.47.134	TCP	54	51250 > auth [None] Seq=1 win=1024 Len=0
9	1.38668	192.168.47.171	192.168.47.134	TCP	54	51250 > ms-wbt-server [None] Seq=1 win=1024 Len=0
10	1.38671	192.168.47.171	192.168.47.134	TCP	54	51250 > rfb [None] Seq=1 win=1024 Len=0
11	1.38674	192.168.47.171	192.168.47.134	TCP	54	51250 > submission [None] Seq=1 win=1024 Len=0
12	1.38677	192.168.47.171	192.168.47.134	TCP	54	51250 > auth [None] Seq=1 win=1024 Len=0
13	1.38682	192.168.47.171	192.168.47.134	TCP	54	51250 > rfb [None] Seq=1 win=1024 Len=0
14	1.38685	192.168.47.171	192.168.47.134	TCP	54	51250 > rap [None] Seq=1 win=1024 Len=0
15	1.38688	192.168.47.171	192.168.47.134	TCP	54	51250 > submission [None] Seq=1 win=1024 Len=0
16	1.38691	192.168.47.171	192.168.47.134	TCP	54	51250 > rap [None] Seq=1 win=1024 Len=0
17	1.38694	192.168.47.171	192.168.47.134	TCP	54	51250 > ddt-tcp-1 [None] Seq=1 win=1024 Len=0
18	1.38697	192.168.47.171	192.168.47.134	TCP	54	51250 > inaps [None] Seq=1 win=1024 Len=0
19	1.38700	192.168.47.171	192.168.47.134	TCP	54	51250 > ddt-tcp-1 [None] Seq=1 win=1024 Len=0
20	1.38703	192.168.47.171	192.168.47.134	TCP	54	51250 > pop3 [None] Seq=1 win=1024 Len=0
21	1.38706	192.168.47.171	192.168.47.134	TCP	54	51250 > inaps [None] Seq=1 win=1024 Len=0
22	1.38709	192.168.47.171	192.168.47.134	TCP	54	51250 > rtsp [None] Seq=1 win=1024 Len=0

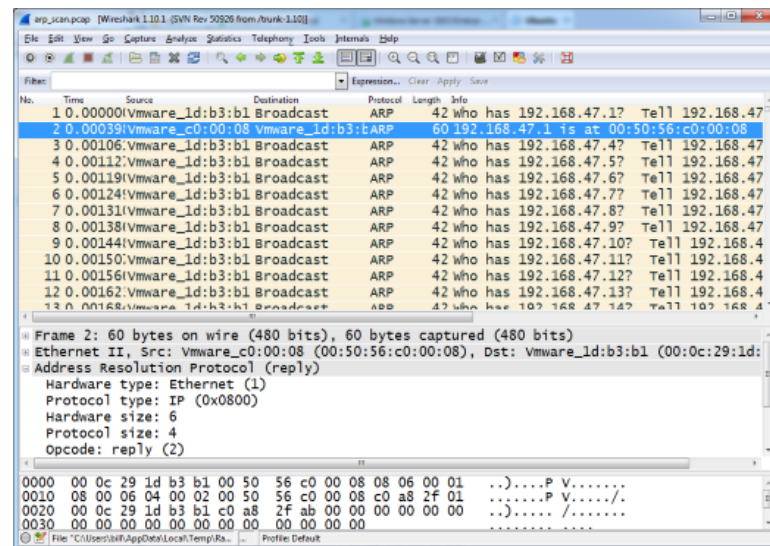
Frame 12: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Vmware_1d:b3:b1 (00:0c:29:1d:b3:b1), Dst: Vmware_0f:71:a3 (00:0c:29:0f:71:a3)
Internet Protocol Version 4, Src: 192.168.47.171 (192.168.47.171), Dst: 192.168.47.134 (192.168.47.134)
Transmission Control Protocol, Src Port: 51250 (51250), Dst Port: submission (387), Seq: 1, Len: 0

0000 00 0c 29 0f 71 a3 00 29 1d b3 b1 08 00 45 00 .-).q...)....E.
0010 00 28 64 4d 00 3a 06 3c 01 c0 a8 2f 84 c0 a8 .(dM... /..2.K...P.
0020 2f 86 c8 32 02 4b 03 88 e3 ab 00 00 00 50 00 /..2.K...P.
0030 04 00 19 b1 00 00

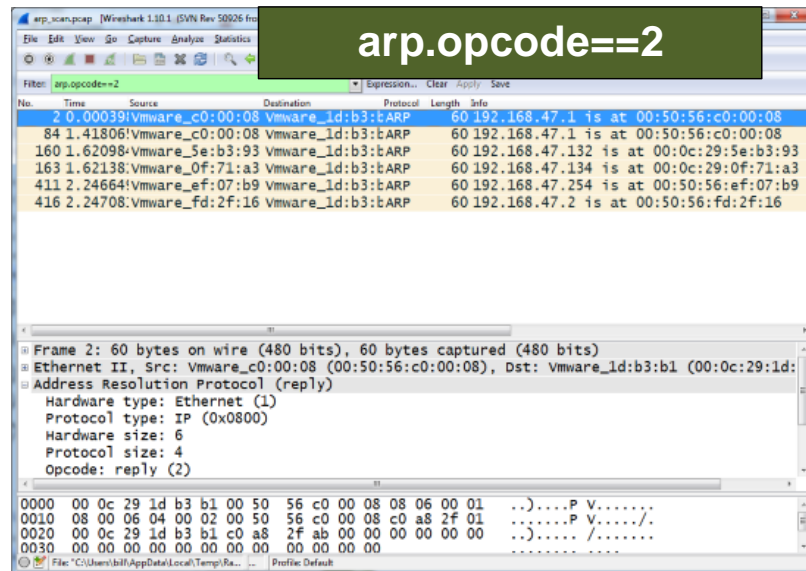
Author: Prof Bill Buchanan



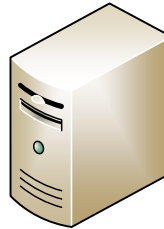
http://asecuritysite.com/log/ping_sweep.zip



arp.opcode==2



http://asecuritysite.com/log/arp_scan.zip



C:\Snort\bin>nmap 192.168.47.134

```
Starting Nmap 6.40 ( http://nmap.org ) at
2014-01-05 16:22 GMT Standard Time
Nmap scan report for 192.168.47.134
Host is up (0.000028s latency).
Not shown: 972 closed ports
PORT      STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
...
5900/tcp open  vnc
8099/tcp open  unknown
MAC Address: 00:0C:29:0F:71:A3
(VMware)

Nmap done: 1 IP address (1 host up)
scanned in 1.78 seconds
```

C:\snort\bin> type 1.rules

```
preprocessor sfportscan:\
  proto { all } \
  scan_type { all } \
  sense_level { high } \
  logfile { portscan.log }
```

C:\Snort\bin>snort -W

Index	Physical Address	IP Address	Device Name
1	00:0C:29:0F:71:A3	192.168.47.134	\Device\NPF_{BEB6E6E9-8D1A-463E-B650-4C388AEE925D}

Intel(R) PRO/1000 MT Network Connection

C:\Snort\bin>snort -i 1 -c 1.rules -l log



Time: 01/05-16:22:35.960159

event_ref: 0

192.168.47.171 -> 192.168.47.134 (portscan) TCP Filtered Portscan

Priority Count: 0

Connection Count: 200

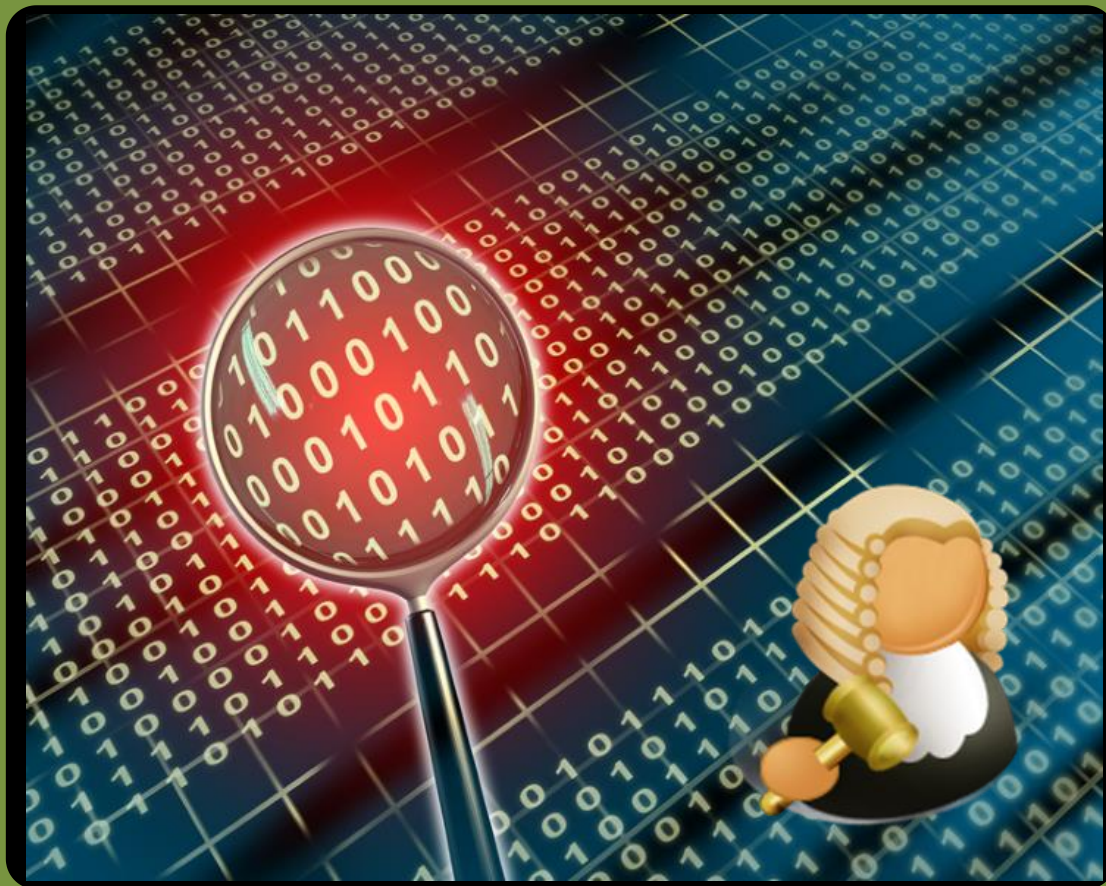
IP Count: 1

Scanner IP Range: 192.168.47.171:192.168.47.171

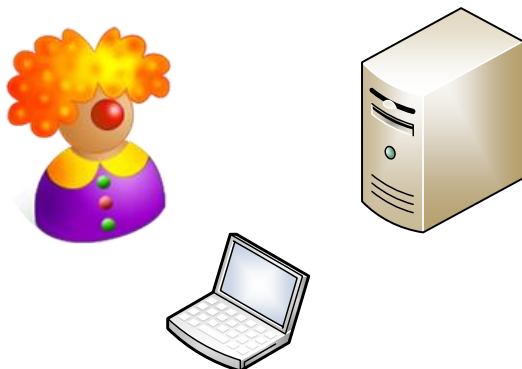
Port/Proto Count: 200

Port/Proto Range: 6:60443

Advanced Network Forensics



Signature Detection



http contains "\x25\x50\x44\x46"
http contains "%PDF"
http contains "GIF89a"

Follow TCP Stream

Stream Content

```
Referer: http://www.google.co.uk/ur1/  
sa=t&rc=j&q=&src=s&source=web&cd=1&ved=0CC8QfJAA&url=http%3A%2F%2Fwww.pdf995.com%  
2Fsamples%  
2Fpdf.pdf&ei=ja_JUuzzBexR7AbIKYCA&usg=AFQjCNFujjzA3W2DPPGoy7Fpbx0wEqSznA&bvm=bv.58187  
178,d.2gu  
Connection: keep-alive  
Range: bytes=0-65535  
  
HTTP/1.1 206 Partial Content  
Date: Sun, 05 Jan 2014 11:24:53 GMT  
P3P: policyref="http://info.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI  
PSA PSD IVA1 IVD1 CON1 TEL0 OTP1 OUR DEL1 SAM1 OTR1 UNR1 PUB1 IND PHY ONL UNI PUR FIN  
COM NAV INT DEM CNT STA POL HEA PRE LOC GOV"  
Last-Modified: Sat, 13 Dec 2003 01:36:20 GMT  
Accept-Ranges: bytes  
Content-Type: application/pdf  
Content-Range: bytes 0-65535/433994  
Content-Length: 65536  
Age: 28310  
Connection: keep-alive  
Server: YTS/1.20.28  
  
%PDF-1.3  
%....  
30 0 obj  
<</Length 31 0 R/Filter /FlateDecode>>  
stream  
x...  
[q].....+Kf+..%.../...=...{feY.T...  
2.7.7.0....7...{...<...?....C.%\ByL..K....!  
C.y>_r...<.K...<.!>..(.....m..]2.....0.  
...  
O.CN F."=AS N n
```

File Types

Adv Net For.

Filter: http contains "%PDF"

No.	Time	Source	Destination	Protocol	Length	Info
114	3.23636500	98.139.134.174	192.168.47.171	HTTP	391	HTTP/1.1 206 Partial

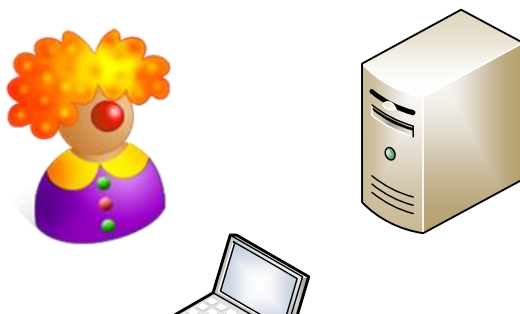
Frame 114: 391 bytes on wire (3128 bits), 391 bytes captured (3128 bits) on interface 0

Ethernet II, Src: Vmware_fd:2f:16 (00:50:56:fd:2f:16), Dst: Vmware_id:b3:b1 (00:0c:29:1d:b3:b1)

Internet Protocol Version 4, Src: 98.139.134.174 (98.139.134.174), Dst: 192.168.47.171

Transmission Control Protocol, Src Port: http (80), Dst Port: tcpdebugger (2576), Seq: 319, Ack: 83, Win: 0, Len: 0

[51 Reassembled TCP segments (66037 bytes): #41(501), #42(959), #44(1460), #45(1460), #46(1460), #47(1460), #48(1460), #49(1460), #50(1460), #51(1460), #52(1460), #53(1460), #54(1460), #55(1460), #56(1460), #57(1460), #58(1460), #59(1460), #60(1460), #61(1460), #62(1460), #63(1460), #64(1460), #65(1460), #66(1460), #67(1460), #68(1460), #69(1460), #70(1460), #71(1460), #72(1460), #73(1460), #74(1460), #75(1460), #76(1460), #77(1460), #78(1460), #79(1460), #80(1460), #81(1460), #82(1460), #83(1460), #84(1460), #85(1460), #86(1460), #87(1460), #88(1460), #89(1460), #90(1460), #91(1460), #92(1460), #93(1460), #94(1460), #95(1460), #96(1460), #97(1460), #98(1460), #99(1460), #100(1460), #101(1460), #102(1460), #103(1460), #104(1460), #105(1460), #106(1460), #107(1460), #108(1460), #109(1460), #110(1460), #111(1460), #112(1460), #113(1460), #114(1460), #115(1460), #116(1460), #117(1460), #118(1460), #119(1460), #120(1460), #121(1460), #122(1460), #123(1460), #124(1460), #125(1460), #126(1460), #127(1460), #128(1460), #129(1460), #130(1460), #131(1460), #132(1460), #133(1460), #134(1460), #135(1460), #136(1460), #137(1460), #138(1460), #139(1460), #140(1460), #141(1460), #142(1460), #143(1460), #144(1460), #145(1460), #146(1460), #147(1460), #148(1460), #149(1460), #150(1460), #151(1460), #152(1460), #153(1460), #154(1460), #155(1460), #156(1460), #157(1460), #158(1460), #159(1460), #160(1460), #161(1460), #162(1460), #163(1460), #164(1460), #165(1460), #166(1460), #167(1460), #168(1460), #169(1460), #170(1460), #171(1460), #172(1460), #173(1460), #174(1460), #175(1460), #176(1460), #177(1460), #178(1460), #179(1460), #180(1460), #181(1460), #182(1460), #183(1460), #184(1460), #185(1460), #186(1460), #187(1460), #188(1460), #189(1460), #190(1460), #191(1460), #192(1460), #193(1460), #194(1460), #195(1460), #196(1460), #197(1460), #198(1460), #199(1460), #200(1460), #201(1460), #202(1460), #203(1460), #204(1460), #205(1460), #206(1460), #207(1460), #208(1460), #209(1460), #210(1460), #211(1460), #212(1460), #213(1460), #214(1460), #215(1460), #216(1460), #217(1460), #218(1460), #219(1460), #220(1460), #221(1460), #222(1460), #223(1460), #224(1460), #225(1460), #226(1460), #227(1460), #228(1460), #229(1460), #230(1460), #231(1460), #232(1460), #233(1460), #234(1460), #235(1460), #236(1460), #237(1460), #238(1460), #239(1460), #240(1460), #241(1460), #242(1460), #243(1460), #244(1460), #245(1460), #246(1460), #247(1460), #248(1460), #249(1460), #250(1460), #251(1460), #252(1460), #253(1460), #254(1460), #255(1460), #256(1460), #257(1460), #258(1460), #259(1460), #260(1460), #261(1460), #262(1460), #263(1460), #264(1460), #265(1460), #266(1460), #267(1460), #268(1460), #269(1460), #270(1460), #271(1460), #272(1460), #273(1460), #274(1460), #275(1460), #276(1460), #277(1460), #278(1460), #279(1460), #280(1460), #281(1460), #282(1460), #283(1460), #284(1460), #285(1460), #286(1460), #287(1460), #288(1460), #289(1460), #290(1460), #291(1460), #292(1460), #293(1460), #294(1460), #295(1460), #296(1460), #297(1460), #298(1460), #299(1460), #300(1460), #301(1460), #302(1460), #303(1460), #304(1460), #305(1460), #306(1460), #307(1460), #308(1460), #309(1460), #310(1460), #311(1460), #312(1460), #313(1460), #314(1460), #315(1460), #316(1460), #317(1460), #318(1460), #319(1460), #320(1460), #321(1460), #322(1460), #323(1460), #324(1460), #325(1460), #326(1460), #327(1460), #328(1460), #329(1460), #330(1460), #331(1460), #332(1460), #333(1460), #334(1460), #335(1460), #336(1460), #337(1460), #338(1460), #339(1460), #340(1460), #341(1460), #342(1460), #343(1460), #344(1460), #345(1460), #346(1460), #347(1460), #348(1460), #349(1460), #350(1460), #351(1460), #352(1460), #353(1460), #354(1460), #355(1460), #356(1460), #357(1460), #358(1460), #359(1460), #360(1460), #361(1460), #362(1460), #363(1460), #364(1460), #365(1460), #366(1460), #367(1460), #368(1460), #369(1460), #370(1460), #371(1460), #372(1460), #373(1460), #374(1460), #375(1460), #376(1460), #377(1460), #378(1460), #379(1460), #380(1460), #381(1460), #382(1460), #383(1460), #384(1460), #385(1460), #386(1460), #387(1460), #388(1460), #389(1460), #390(1460), #391(1460), #392(1460), #393(1460), #394(1460), #395(1460), #396(1460), #397(1460), #398(1460), #399(1460), #400(1460), #401(1460), #402(1460), #403(1460), #404(1460), #405(1460), #406(1460), #407(1460), #408(1460), #409(1460), #410(1460), #411(1460), #412(1460), #413(1460), #414(1460), #415(1460), #416(1460), #417(1460), #418(1460), #419(1460), #420(1460), #421(1460), #422(1460), #423(1460), #424(1460), #425(1460), #426(1460), #427(1460), #428(1460), #429(1460), #430(1460), #431(1460), #432(1460), #433(1460), #434(1460), #435(1460), #436(1460), #437(1460), #438(1460), #439(1460), #440(1460), #441(1460), #442(1460), #443(1460), #444(1460), #445(1460), #446(1460), #447(1460), #448(1460), #449(1460), #450(1460), #451(1460), #452(1460), #453(1460), #454(1460), #455(1460), #456(1460), #457(1460), #458(1460), #459(1460), #460(1460), #461(1460), #462(1460), #463(1460), #464(1460), #465(1460), #466(1460), #467(1460), #468(1460), #469(1460), #470(1460), #471(1460), #472(1460), #473(1460), #474(1460), #475(1460), #476(1460), #477(1460), #478(1460), #479(1460), #480(1460), #481(1460), #482(1460), #483(1460), #484(1460), #485(1460), #486(1460), #487(1460), #488(1460), #489(1460), #490(1460), #491(1460), #492(1460), #493(1460), #494(1460), #495(1460), #496(1460), #497(1460), #498(1460), #499(1460), #500(1460), #501(1460), #502(1460), #503(1460), #504(1460), #505(1460), #506(1460), #507(1460), #508(1460), #509(1460), #510(1460), #511(1460), #512(1460), #513(1460), #514(1460), #515(1460), #516(1460), #517(1460), #518(1460), #519(1460), #520(1460), #521(1460), #522(1460), #523(1460), #524(1460), #525(1460), #526(1460), #527(1460), #528(1460), #529(1460), #530(1460), #531(1460), #532(1460), #533(1460), #534(1460), #535(1460), #536(1460), #537(1460), #538(1460), #539(1460), #540(1460), #541(1460), #542(1460), #543(1460), #544(1460), #545(1460), #546(1460), #547(1460), #548(1460), #549(1460), #550(1460), #551(1460), #552(1460), #553(1460), #554(1460), #555(1460), #556(1460), #557(1460), #558(1460), #559(1460), #560(1460), #561(1460), #562(1460), #563(1460), #564(1460), #565(1460), #566(1460), #567(1460), #568(1460), #569(1460), #570(1460), #571(1460), #572(1460), #573(1460), #574(1460), #575(1460), #576(1460), #577(1460), #578(1460), #579(1460), #580(1460), #581(1460), #582(1460), #583(1460), #584(1460), #585(1460), #586(1460), #587(1460), #588(1460), #589(1460), #590(1460), #591(1460), #592(1460), #593(1460), #594(1460), #595(1460), #596(1460), #597(1460), #598(1460), #599(1460), #600(1460), #601(1460), #602(1460), #603(1460), #604(1460), #605(1460), #606(1460), #607(1460), #608(1460), #609(1460), #610(1460), #611(1460), #612(1460), #613(1460), #614(1460), #615(1460), #616(1460), #617(1460), #618(1460), #619(1460), #620(1460), #621(1460), #622(1460), #623(1460), #624(1460), #625(1460), #626(1460), #627(1460), #628(1460), #629(1460), #630(1460), #631(1460), #632(1460), #633(1460), #634(1460), #635(1460), #636(1460), #637(1460), #638(1460), #639(1460), #640(1460), #641(1460), #642(1460), #643(1460), #644(1460), #645(1460), #646(1460), #647(1460), #648(1460), #649(1460), #650(1460), #651(1460), #652(1460), #653(1460), #654(1460), #655(1460), #656(1460), #657(1460), #658(1460), #659(1460), #660(1460), #661(1460), #662(1460), #663(1460), #664(1460), #665(1460), #666(1460), #667(1460), #668(1460), #669(1460), #670(1460), #671(1460), #672(1460), #673(1460), #674(1460), #675(1460), #676(1460), #677(1460), #678(1460), #679(1460), #680(1460), #681(1460), #682(1460), #683(1460), #684(1460), #685(1460), #686(1460), #687(1460), #688(1460), #689(1460), #690(1460), #691(1460), #692(1460), #693(1460), #694(1460), #695(1460), #696(1460), #697(1460), #698(1460), #699(1460), #700(1460), #701(1460), #702(1460), #703(1460), #704(1460), #705(1460), #706(1460), #707(1460), #708(1460), #709(1460), #710(1460), #711(1460), #712(1460), #713(1460), #714(1460), #715(1460), #716(1460), #717(1460), #718(1460), #719(1460), #720(1460), #721(1460), #722(1460), #723(1460), #724(1460), #725(1460), #726(1460), #727(1460), #728(1460), #729(1460), #730(1460), #731(1460), #732(1460), #733(1460), #734(1460), #735(1460), #736(1460), #737(1460), #738(1460), #739(1460), #740(1460), #741(1460), #742(1460), #743(1460), #744(1460), #745(1460), #746(1460), #747(1460), #748(1460), #749(1460), #750(1460), #751(1460), #752(1460), #753(1460), #754(1460), #755(1460), #756(1460), #757(1460), #758(1460), #759(1460), #760(1460), #761(1460), #762(1460), #763(1460), #764(1460), #765(1460), #766(1460), #767(1460), #768(1460), #769(1460), #770(1460), #771(1460), #772(1460), #773(1460), #774(1460), #775(1460), #776(1460), #777(1460), #778(1460), #779(1460), #780(1460), #781(1460), #782(1460), #783(1460), #784(1460), #785(1460), #786(1460), #787(1460), #788(1460), #789(1460), #790(1460), #791(1460), #792(1460), #793(1460), #794(1460), #795(1460), #796(1460), #797(1460), #798(1460), #799(1460), #800(1460), #801(1460), #802(1460), #803(1460), #804(1460), #805(1460), #806(1460), #807(1460), #808(1460), #809(1460), #810(1460), #811(1460), #812(1460), #813(1460), #814(1460), #815(1460), #816(1460), #817(1460), #818(1460), #819(1460), #820(1460), #821(1460), #822(1460), #823(1460), #824(1460), #825(1460), #826(1460), #827(1460), #828(1460), #829(1460), #830(1460), #831(1460), #832(1460), #833(1460), #834(1460), #835(1460), #836(1460), #837(1460), #838(1460), #839(1460), #840(1460), #841(1460), #842(1460), #843(1460), #844(1460), #845(1460), #846(1460), #847(1460), #848(1460), #849(1460), #850(1460), #851(1460), #852(1460), #853(1460), #854(1460), #855(1460), #856(1460), #857(1460), #858(1460), #859(1460), #860(1460), #861(1460), #862(1460), #863(1460), #864(1460), #865(1460), #866(1460), #867(1460), #868(1460), #869(1460), #870(1460), #871(1460), #872(1460), #873(1460), #874(1460), #875(1460), #876(1460), #877(1460), #878(1460), #879(1460), #880(1460), #881(1460), #882(1460), #883(1460), #884(1460), #885(1460), #886(1460), #887(1460), #888(1460), #889(1460), #890(1460), #891(1460), #892(1460), #893(1460), #894(1460), #895(1460), #896(1460), #897(1460), #898(1460), #899(1460), #900(1460), #901(1460), #902(1460), #903(1460), #904(1460), #905(1460), #906(1460), #907(1460), #908(1460), #909(1460), #910(1460), #911(1460), #912(1460), #913(1460), #914(1460), #915(1460), #916(1460), #917(1460), #918(1460), #919(1460), #920(1460), #921(1460), #922(1460), #923(1460), #924(1460), #925(1460), #926(1460), #927(1460), #928(1460), #929(1460), #930(1460), #931(1460), #932(1460), #933(1460), #934(1460), #935(1460), #936(1460), #937(1460), #938(1460), #939(1460), #940(1460), #941(1460), #942(1460), #943(1460), #944(1460), #945(1460), #946(1460), #947(1460), #948(1460), #949(1460), #950(1460), #951(1460), #952(1460), #953(1460), #954(1460), #955(1460), #956(1460), #957(1460), #958(1460), #959(1460), #960(1460), #961(1460), #962(1460), #963(1460), #964(1460), #965(1460), #966(1460), #967(1460), #968(1460), #969(1460), #970(1460), #971(1460), #972(1460), #973(1460), #974(1460), #975(1460), #976(1460), #977(1460), #978(1460), #979(1460), #980(1460), #981(1460), #982(1460), #983(1460), #984(1460), #985(1460), #986(1460), #987(1460), #988(1460), #989(1460), #990(1460), #991(1460), #992(1460), #993(1460), #994(1460), #995(1460), #996(1460), #997(1460), #998(1460), #999(1460), #1000(1460), #1001(1460), #1002(1460), #1003(1460), #1004(1460), #1005(1460), #1006(1460), #1007(1460), #1008(1460), #1009(1460), #1010(1460), #1011(1460), #1012(1460), #1013(1460), #1014(1460), #1015(1460), #1016(1460), #1017(1460), #1018(1460), #1019(1460), #1020(1460), #1021(1460), #1022(1460), #1023(1460), #1024(1460), #1025(1460), #1026(1460), #1027(1460), #1028(1460), #1029(1460), #1030(1460), #1031(1460), #1032(1460), #1033(1460), #1034(1460), #1035(1460), #1036(1460), #1037(1460), #1038(1460), #1039(1460), #1040(1460), #1041(1460), #1042(1460), #1043(1460), #1044(1460), #1045(1460), #1046(1460), #1047(1460), #1048(1460), #1049(1460), #1050(1460), #1051(1460), #1052(1460), #1053(1460), #1054(1460), #1055(1460), #1056(1460), #1057(1460), #1058(1460), #1059(1460), #1060(1460), #1061(1460), #1062(1460), #1063(1460), #1064(1460), #1065(1460), #1066(1460), #1067(1460), #1068(1460), #1069(1460), #1070(1460), #1071(1460), #1072(1460), #1073(1460), #1074(1460), #1075(1460), #1076(1460), #1077(1460), #1078(1460), #1079(1460), #1080(1460), #1081(1460), #1082(1460), #1083(1460), #1084(1460), #1085(1460), #1086(1460), #1087(1460), #1088(1460), #1089(1460), #1090(1460), #1091(1460), #1092(1460), #1093(1460), #1094(1460), #1095(1460), #1096(1460), #1097(1460), #1098(1460), #1099(1460), #1100(1460), #1101(1460), #1102(1460), #1103(1460), #1104(1460), #1105(1460), #1106(1460), #1107(1460), #1108(1460), #1109(1460), #1110(1460), #1111(1460), #1112(1460), #1113(1460), #1114(1460), #1115(1460), #1116(1460), #1117(1460), #1118(1460), #1119(1460), #1120(1460), #1121(1460), #1122(1460), #1123(1460), #1124(1460), #1125(1460), #1126(1460), #1127(1460), #1128(1460), #1129(1460), #1130(1460), #1131(1460), #1132(1460), #1133(1460), #1134(1460), #1135(1460), #1136(1460), #1137(1460), #1138(1460), #1139(1460), #1140(1460), #1141(1460), #1142(1460), #1143(1460), #1144(1460), #1145(1460), #1146(1460), #1147(1460), #1148(1460), #1149(1460), #1150(1

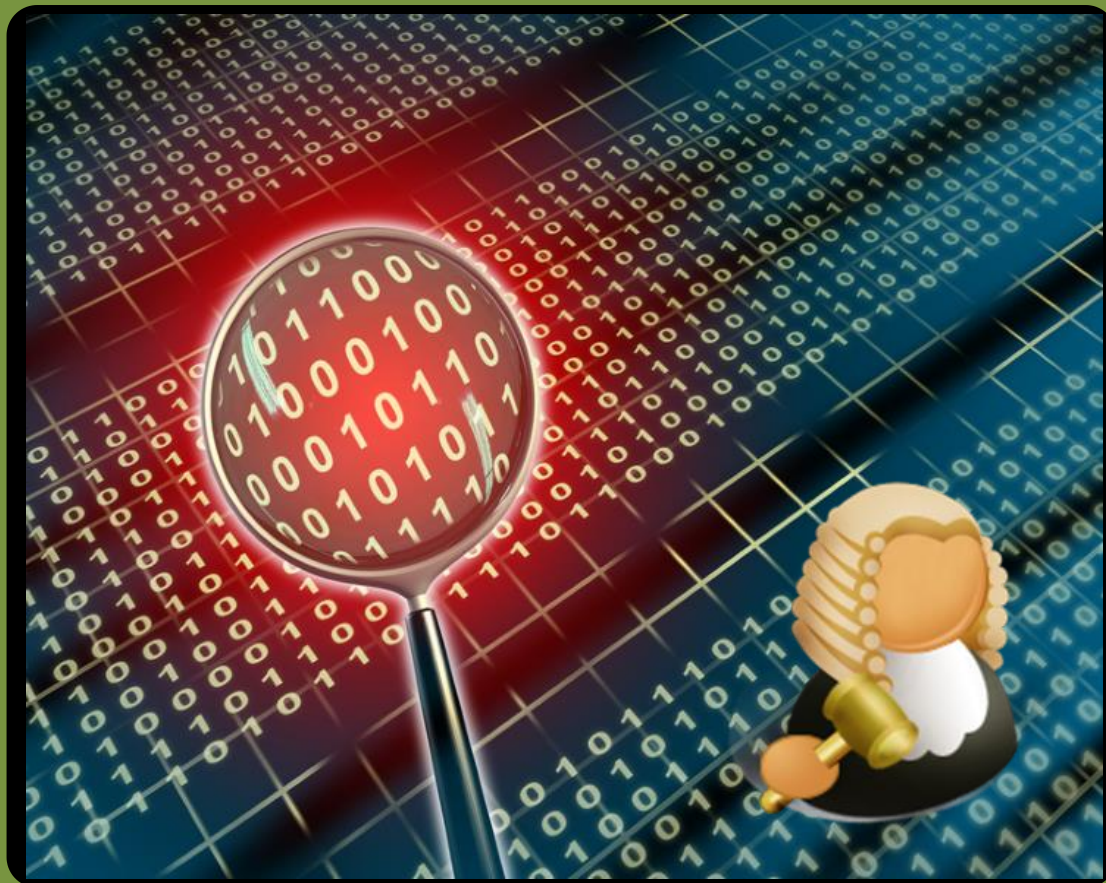


```
alert tcp any any -> any any (content:"GIF89a"; msg:"GIF";sid:10000)
alert tcp any any -> any any (content:"%PDF"; msg:"PDF";sid:10001)
alert tcp any any -> any any (content:"|89 50 4E 47|"; msg:"PNG";sid:10002)
alert tcp any any -> any any (content:"|50 4B 03 04|"; msg:"ZIP";sid:10003)
```



```
[**] [1:10001:0] PDF [**]
[Priority: 0]
01/05-20:08:06.177354 61.67.219.91:80 -> 192.168.47.171:2700
TCP TTL:128 TOS:0x0 ID:62294 IpLen:20 DgmLen:1238
***AP*** Seq: 0x6BFA2147 Ack: 0xC3534C66 Win: 0xFAF0 TcpLen: 20
```

Advanced Network Forensics



Converted Formats

MIME Encoding

```
alert tcp any any <> any 25 (pcre:"/[a-zA-Z0-9._%+-]+@[a-zA-Z0-9._%+-]"/; \
msg:"Email in message";sid:9000000;rev:1;)
```

```
[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.648260 192.168.47.171:2826 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:13590 IpLen:20 DgmLen:78 DF
***AP*** Seq: 0xB1484585 Ack: 0xFB0FDF97 Win: 0xFF71 TcpLen: 20

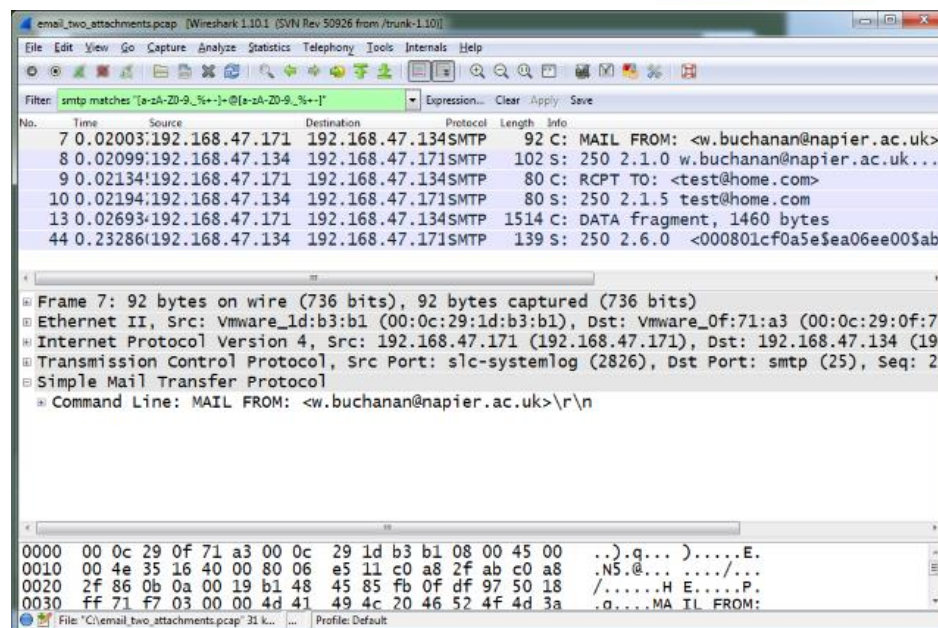
[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.649220 192.168.47.134:25 -> 192.168.47.171:2826
TCP TTL:128 TOS:0x0 ID:2017 IpLen:20 DgmLen:88 DF
***AP*** Seq: 0xFB0FDF97 Ack: 0xB14845AB Win: 0xFAB5 TcpLen: 20

[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.649568 192.168.47.171:2826 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:13591 IpLen:20 DgmLen:66 DF
***AP*** Seq: 0xB14845AB Ack: 0xFB0FDFC7 Win: 0xFF41 TcpLen: 20

[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.650165 192.168.47.134:25 -> 192.168.47.171:2826
TCP TTL:128 TOS:0x0 ID:2018 IpLen:20 DgmLen:66 DF
***AP*** Seq: 0xFB0FDFC7 Ack: 0xB14845C5 Win: 0xFA9B TcpLen: 20

[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.655157 192.168.47.171:2826 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:13593 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xB14845CB Ack: 0xFB0FE00F Win: 0xFE99 TcpLen: 20

[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.861083 192.168.47.134:25 -> 192.168.47.171:2826
TCP TTL:128 TOS:0x0 ID:2030 IpLen:20 DgmLen:125 DF
***AP*** Seq: 0xFB0FE00F Ack: 0xB148AE2E Win: 0xFAEB TcpLen: 20
```



```
smtp matches "[a-zA-Z0-9._%+-]+@[a-zA-Z0-9._%+-]"
```



```
alert tcp any any <> any any (pcre:"/5\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; \
  msg:"MasterCard number detected in clear \
  text";content:"number";nocase;sid:9000003;rev:1;)
```

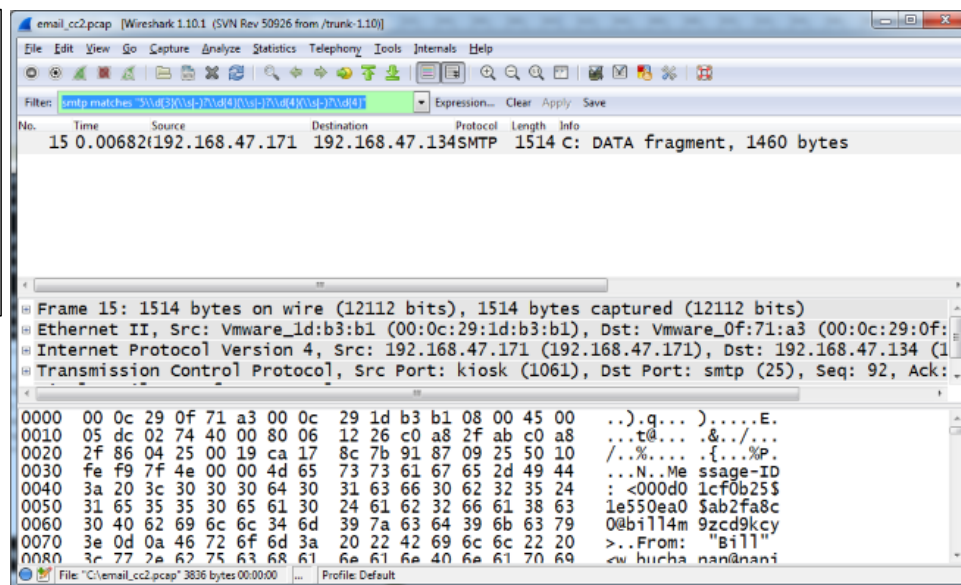


```
alert tcp any any <> any any (pcre:"/3\d{3}(\s|-)?\d{6}(\s|-)?\d{5}/"; \
  msg:"American Express number detected in clear \
  text";content:"number";nocase;sid:9000004;rev:1;)
```

```
alert tcp any any <> any any (pcre:"/4\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; \
  msg:"Visa number detected in clear \
  text";content:"number";nocase;sid:9000005;rev:1;)
```

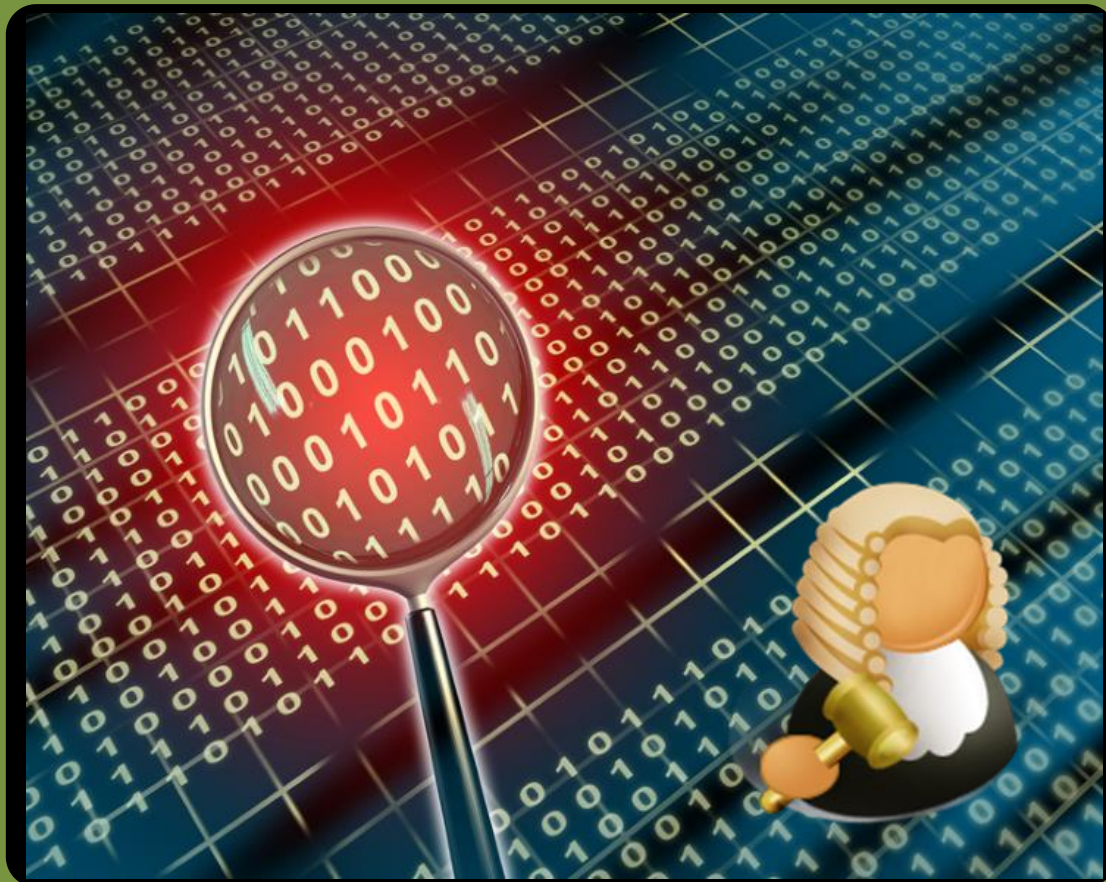
```
[**] [1:9000005:1] Visa number detected in clear text [**]
[Priority: 0]
01/06-21:20:26.755456 192.168.47.171:1061 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:628 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xCA178C7B Ack: 0x91870925 Win: 0xFEFE9 TcpLen: 20
```

```
[**] [1:9000003:1] MasterCard number detected in clear text [**]
[Priority: 0]
01/06-21:20:26.755456 192.168.47.171:1061 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:628 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xCA178C7B Ack: 0x91870925 Win: 0xFEFE9 TcpLen: 20
```



smtp matches "5\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}"

Advanced Network Forensics



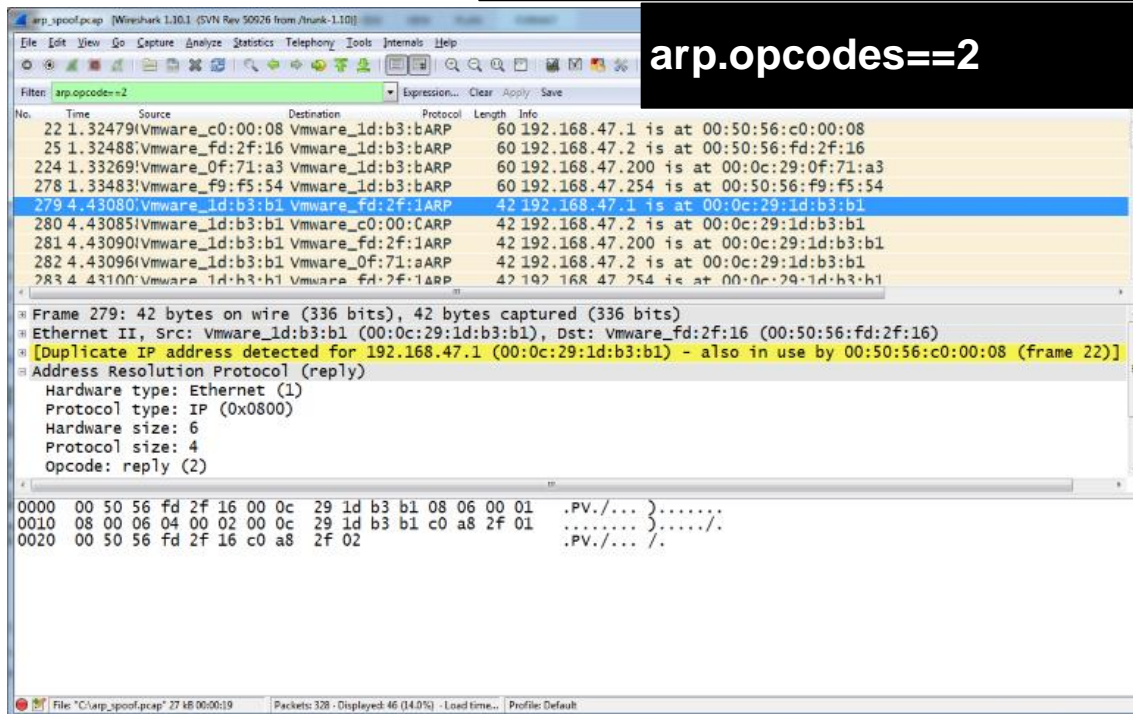
ARP Spoofing



preprocessor arpspoof

preprocessor arpspoof_detect_host: 192.168.47.200 00:0C:29:0F:71:A3

arp.opcodes==2



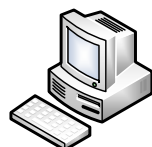
ARP Spoofing

Adv Net For.

Who has 192.168.47.1? Tell 192.168.47.171

192.168.47.1 is at 00:50:56:c0:00:08

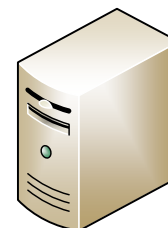
192.168.47.1 is at 00:0c:29:1d:b3:b1



192.168.47.171



192.168.47.x

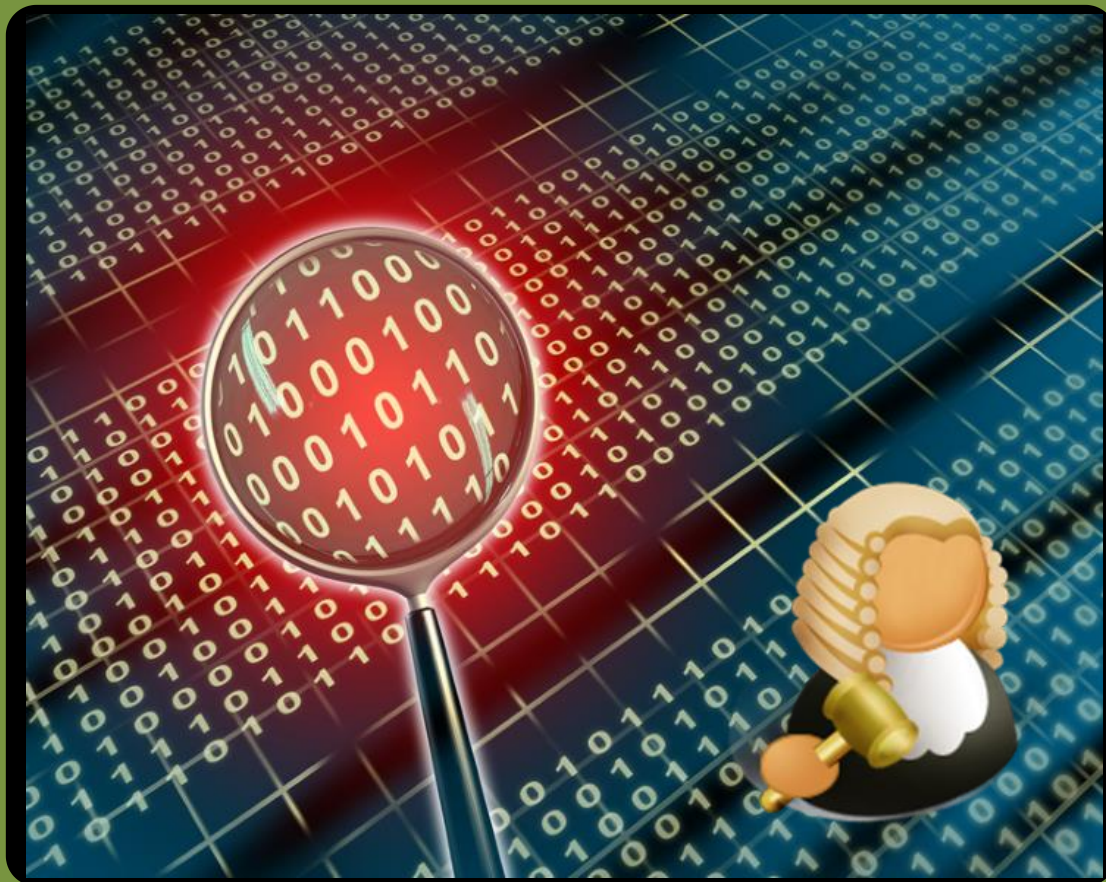


192.168.47.1

Author: Prof Bill Buchanan

ARP Spoofing

Advanced Network Forensics



DDoS Detection



hping_syn.pcap [Wireshark 1.10.1 (SVN Rev 50926 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools

Filter:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000	192.168.75.137	192.168.75.1	TCP	58	x9-icue > 0 [SYN] Seq=0 Win=512 Len=4
2	1.00363	192.168.75.137	192.168.75.1	TCP	58	audit-transfer > 0 [SYN] Seq=0 Win=512 Len=4
3	2.00671	192.168.75.137	192.168.75.1	TCP	58	capioverlan > 0 [SYN] Seq=0 Win=512 Len=4
4	3.00979	192.168.75.137	192.168.75.1	TCP	58	elfiq-repl > 0 [SYN] Seq=0 Win=512 Len=4
5	4.01281	192.168.75.137	192.168.75.1	TCP	58	bvtsonar > 0 [SYN] Seq=0 Win=512 Len=4
6	5.01588	192.168.75.137	192.168.75.1	TCP	58	blaze > 0 [SYN] Seq=0 Win=512 Len=4
7	6.01928	192.168.75.137	192.168.75.1	TCP	58	unizensus > 0 [SYN] Seq=0 Win=512 Len=4
8	7.03559	192.168.75.137	192.168.75.1	TCP	58	winpoplanmess > 0 [SYN] Seq=0 Win=512 Len=4
9	8.03900	192.168.75.137	192.168.75.1	TCP	58	[TCP segment of a reassembled PDU]
10	9.04210	192.168.75.137	192.168.75.1	TCP	58	resacommunity > 0 [SYN] Seq=0 Win=512 Len=4
11	10.0260	Vmware_6b:0e:96	Vmware_c0:00:08	CARP	42	who has 192.168.75.1? Tell 192.168.75.137
12	10.0260	Vmware_c0:00:08	Vmware_6b:0e:96	ARP	42	192.168.75.1 is at 00:50:56:c0:00:08
13	10.0451	192.168.75.137	192.168.75.1	TCP	58	nfa > 0 [SYN] Seq=0 Win=512 Len=4
14	11.0481	192.168.75.137	192.168.75.1	TCP	58	iascontrol-oms > 0 [SYN] Seq=0 Win=512 Len=4
15	12.0512	192.168.75.137	192.168.75.1	TCP	58	iascontrol > 0 [SYN] Seq=0 Win=512 Len=4
16	13.0543	192.168.75.137	192.168.75.1	TCP	58	dbcontrol-oms > 0 [SYN] Seq=0 Win=512 Len=4

Frame 1: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)

Ethernet II, Src: Vmware_6b:0e:96 (00:0c:29:6b:0e:96), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)

Internet Protocol Version 4, Src: 192.168.75.137 (192.168.75.137), Dst: 192.168.75.1 (192.168.75.1)

Transmission Control Protocol, Src Port: x9-icue (1145), Dst Port: 0 (0), Seq: 0, Len: 4

Data (4 bytes)

alert tcp any any -> any 80 (msg:"DOS flood denial of service attempt";flow:to_server;\ detection_filter:track by_dst, count 60, seconds 60;\ sid:25101; rev:1;)



hping



192.168.47.171



[SYN][SYN][SYN]



192.168.47.1

Advanced Network Forensics

- User/Password Crack.
- Port Scan.
- Signature Detection.
- Converted Formats.
- ARP Spoofing.
- DDoS Detection.

