

LAB 7

Name : ARAVINDHAN.K

ROLL NO : CH.EN.U4CYS22001

Scenario 2: FTP Server Attack Investigation

Scenario 2

Client network attack

Triggering Events:

- A denial of service (DoS) attack has been reported against FTP server 192.168.56.1
- FTP traffic spikes were seen prior to the FTP server being taken offline

What We Know:

- Captured traffic data that is narrowed down between an attacking host (192.168.56.101) and the FTP server (192.168.56.1)

Scenario 2

A little more abstract

- What caused the spike in FTP traffic
- What events took place prior to the FTP server being taken offline?
(E.g. Were any files transferred to/from the FTP server or were any user accounts compromised)

Objective

Investigate a potential Denial of Service (DoS) attack targeting an FTP server.

GOALS

```
=====
=== Goals ===
=====
1. What events led up to the attack on the FTP server?

2. What types of attacks did the attacker perform on the FTP
server?

3. What were the results of those attacks? (e.g. Did they
login, what did they find, were files stolen, etc.?)|
```

1. What events led to the attack on the FTP server?

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a list of 32 ARP requests (No. 1 to 32) originating from PCSSystemtec_b1:6f:: Broadcast and destined for 192.168.56.1. The bottom screenshot shows a detailed view of a packet capture starting at 537.12709941, displaying a series of TCP SYN packets (No. 21 to 218) from 192.168.56.1 to 192.168.56.101. The packet list on the right shows the sequence of SYN packets, and the packet details pane on the right shows the structure of a TCP packet (Seq=0, Win=8192, Len=0, MSS=1460).

File Machine View Input Devices Help

Apps Places

Scenario 2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
1	0.000000	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.1? Tell 192.168.56.101
2	0.000163	PCSSystemtec_00:d0:: Broadcast	192.168.56.1	ARP	60			192.168.56.1 is at 08:00:27:00:d0:24
3	0.000298	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.2? Tell 192.168.56.101
4	0.000447	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.3? Tell 192.168.56.101
5	0.000588	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.4? Tell 192.168.56.101
6	0.000781	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.5? Tell 192.168.56.101
7	0.001058	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.6? Tell 192.168.56.101
8	0.001295	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.7? Tell 192.168.56.101
9	0.001375	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.8? Tell 192.168.56.101
10	0.001512	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.9? Tell 192.168.56.101
11	0.001657	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.10? Tell 192.168.56.101
12	0.005247	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.13? Tell 192.168.56.101
13	0.005525	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.14? Tell 192.168.56.101
14	0.100715	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.2? Tell 192.168.56.101
15	0.100968	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.3? Tell 192.168.56.101
16	0.101178	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.4? Tell 192.168.56.101
17	0.103652	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.5? Tell 192.168.56.101
18	0.103808	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.6? Tell 192.168.56.101
19	0.103956	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.7? Tell 192.168.56.101
20	0.104099	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.8? Tell 192.168.56.101
21	0.104239	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.9? Tell 192.168.56.101
22	0.104379	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.10? Tell 192.168.56.101
23	0.106800	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.13? Tell 192.168.56.101
24	0.106975	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.14? Tell 192.168.56.101
25	0.201820	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.23? Tell 192.168.56.101
26	0.202175	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.2? Tell 192.168.56.101
27	0.202358	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.25? Tell 192.168.56.101
28	0.204789	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.28? Tell 192.168.56.101
29	0.204931	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.29? Tell 192.168.56.101
30	0.205116	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.30? Tell 192.168.56.101
31	0.205285	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.31? Tell 192.168.56.101
32	0.205444	PCSSystemtec_b1:6f:: Broadcast	192.168.56.1	ARP	42			Who has 192.168.56.32? Tell 192.168.56.101

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: PCSSystemtec_b1:6f::f9 (08:00:27:b1:6f:f9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

File Machine View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apps Places

Scenario 2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags==0x0012

No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
537	12.709941	192.168.56.1	192.168.56.101	TCP	21	60		21 - 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
540	12.712844	192.168.56.1	192.168.56.101	TCP	22	60		445 - 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
546	12.714714	192.168.56.1	192.168.56.101	TCP	25	60		139 - 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
564	12.716309	192.168.56.1	192.168.56.101	TCP	28	60		135 - 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
879	13.342184	192.168.56.1	192.168.56.101	TCP	352	60		48154 - 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
1580	14.173376	192.168.56.1	192.168.56.101	TCP	974	60		49152 - 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
1650	14.376811	192.168.56.1	192.168.56.101	TCP	1120	60		49156 - 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
1922	14.706248	192.168.56.1	192.168.56.101	TCP	1390	60		49153 - 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
2373	15.347860	192.168.56.1	192.168.56.101	TCP	1841	60		49155 - 37711 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
2541	16.947472	192.168.56.1	192.168.56.101	TCP	1991	74		21 - 51843 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2543	16.947564	192.168.56.1	192.168.56.101	TCP	1992	74		21 - 51844 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2545	16.947601	192.168.56.1	192.168.56.101	TCP	1993	74		21 - 51845 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2547	16.947639	192.168.56.1	192.168.56.101	TCP	1994	74		21 - 51846 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2549	16.947658	192.168.56.1	192.168.56.101	TCP	1995	74		21 - 51847 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2550	16.947671	192.168.56.1	192.168.56.101	TCP	1996	74		21 - 51848 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2551	16.947682	192.168.56.1	192.168.56.101	TCP	1997	74		21 - 51849 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2552	16.947694	192.168.56.1	192.168.56.101	TCP	1998	74		21 - 51850 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2553	16.947709	192.168.56.1	192.168.56.101	TCP	1999	74		21 - 51851 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2554	16.947724	192.168.56.1	192.168.56.101	TCP	2000	74		21 - 51852 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2555	16.947741	192.168.56.1	192.168.56.101	TCP	2001	74		21 - 51853 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2556	16.947757	192.168.56.1	192.168.56.101	TCP	2002	74		21 - 51854 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2557	16.947774	192.168.56.1	192.168.56.101	TCP	2003	74		21 - 51855 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2558	16.947785	192.168.56.1	192.168.56.101	TCP	2004	74		21 - 51856 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2559	16.947794	192.168.56.1	192.168.56.101	TCP	2005	74		21 - 51857 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2572	16.953587	192.168.56.1	192.168.56.101	TCP	2006	74		21 - 51858 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2764	19.004285	192.168.56.1	192.168.56.101	TCP	2007	74		21 - 51859 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2774	19.006910	192.168.56.1	192.168.56.101	TCP	2008	74		21 - 51860 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2810	19.015902	192.168.56.1	192.168.56.101	TCP	2009	74		21 - 51861 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2830	19.020929	192.168.56.1	192.168.56.101	TCP	2010	74		21 - 51862 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2839	19.020929	192.168.56.1	192.168.56.101	TCP	2011	74		21 - 51863 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2845	19.022651	192.168.56.1	192.168.56.101	TCP	2012	74		21 - 51864 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=
2849	19.023942	192.168.56.1	192.168.56.101	TCP	2013	74		21 - 51865 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=12157260 TSecr=

Frame 2545: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: PCSSystemtec_00:d0:24 (08:00:27:00:d0:24), Dst: PCSSystemtec_b1:6f::f9 (08:00:27:b1:6f:f9)
Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101
Transmission Control Protocol, Src Port: 21, Dst Port: 51845, Seq: 0, Ack: 1, Len: 0

Scenario 2.pcap

Packets: 174015 · Displayed: 5542 (3.2%)

Profile: Default

2. What types of attacks did the attacker perform the FTP server?

Wireshark · Follow TCP Stream (tcp.stream eq 2003) · Scenario 2.pcap

```
220 Hello, I'm freeFTPd 1.0
USER ""
331 Password required for ""
PASS monkey
530 Login incorrect
USER ""
331 Password required for ""
PASS liverpool
530 Login incorrect
USER ""
331 Password required for ""
PASS bubbles
530 Login incorrect
USER ""
```

7 client pkt(s), 7 server pkt(s), 13 turn(s).

Entire conversation (261 bytes) Show and save data as ASCII Stream 2003 Find Next

Scenario 2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp.response.code == 230 Expression...

Source	Destination	Protocol	Stream ID	Length
192.168.56.1	192.168.56.101	FTP	3640	
192.168.56.1	192.168.56.101	FTP	7356	

[Stream index: 3640]
[TCP Segment Len: 25]
Sequence number: 124 (relative sequence number)
[Next sequence number: 149 (relative sequence number)]
Acknowledgment number: 56 (relative ack number)
1000 = Header Length: 32 bytes (8)
> Flags: 0x018 (PSH, ACK)

Investigation Results

Attacker first initiated a ARP scan of the subnet
192.168.56.0/24

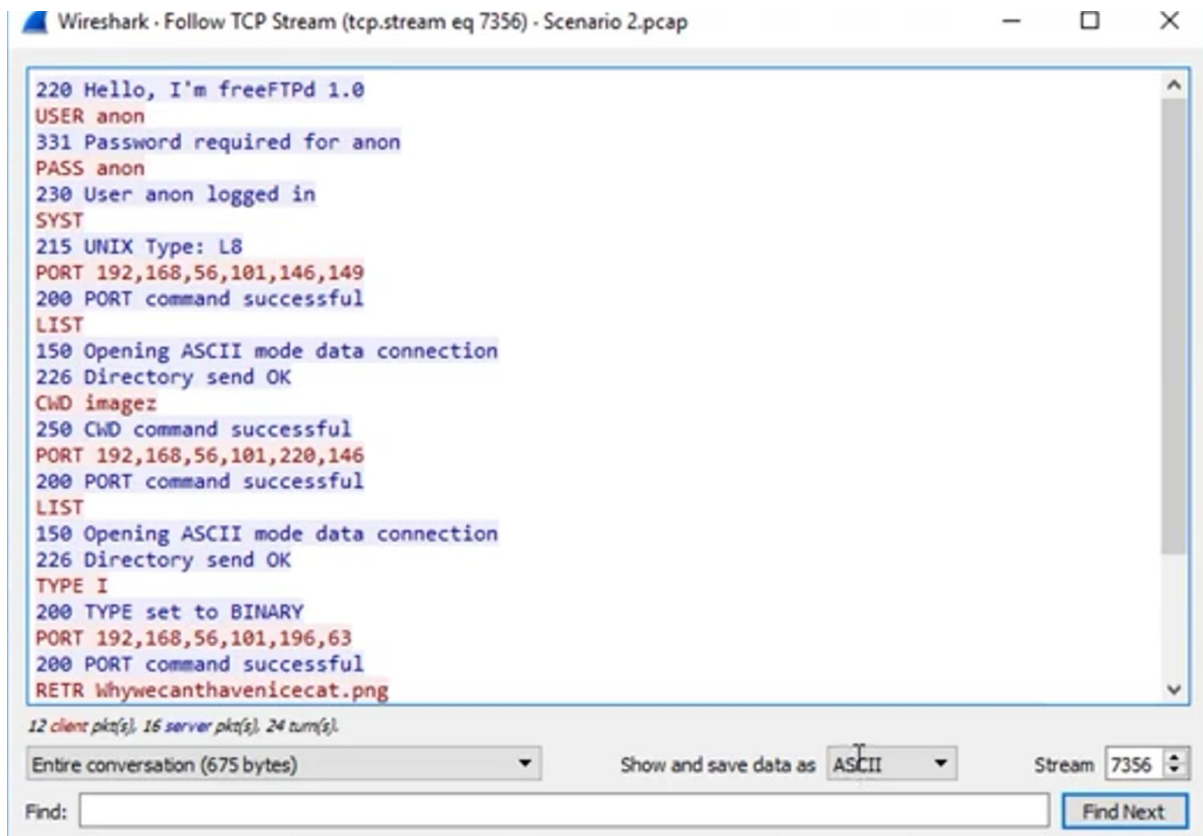
➤The following hosts were discovered: 192.168.56.1
and 192.168.56.100

Attacker then began a port scan of host 192.168.56.1

➤The following ports were found open: 21, 445, 139,
135, 49152, 49153, 49154, 49155, 49156

23

3. were the results of those attacks?
(e.g. Did they
login, did they find, files stolen, etc.



Wireshark · Follow TCP Stream (tcp.stream eq 7356) · Scenario 2.pcap

```
220 Hello, I'm freeFTPd 1.0
USER anon
331 Password required for anon
PASS anon
230 User anon logged in
SYST
215 UNIX Type: L8
PORT 192,168,56,101,146,149
200 PORT command successful
LIST
150 Opening ASCII mode data connection
226 Directory send OK
CWD imagez
250 CWD command successful
PORT 192,168,56,101,220,146
200 PORT command successful
LIST
150 Opening ASCII mode data connection
226 Directory send OK
TYPE I
200 TYPE set to BINARY
PORT 192,168,56,101,196,63
200 PORT command successful
RETR whywecanthavenicecat.png
```

12 client pkt(s), 16 server pkt(s), 24 turn(s).

Entire conversation (675 bytes) Show and save data as ASCII Stream 7356

Find: Find Next

Investigation Results

Attacker followed up with an FTP brute force attack against FTP server

- The credentials **anon/anon** were compromised

Attacker successfully logged in as user anon with stolen credentials

- File "**Whywecanthavenicecat.png**" was downloaded

- MD5 sum of the file:

12039fd05bc2fcd3902247124edcea06

CAT.PNG FOUND



1. What events led up to the attack on the FTP server?
 - ARP scan; devices located:
 - * 192.168.56.1
 - * 192.168.56.100
 - * 192.168.56.101
 - SYN scan:
 - * 21
 - * 445
 - * 139
 - * 135
 - * 49154
 - * 49152
 - * 49156
 - * 49153
 - * 49155
2. What types of attacks did the attacker perform on the FTP server?
3. What were the results of those attacks? (e.g. Did they login, what did they find, were files stolen, etc.?)
 - Attacker logged in with "Anon/anon"
 - They listed the directories and downloaded Whywecanthavenicecat.png (176510 bytes)
 - MD5SUM: 12039fd05bc2fcd3902247124edcea06 *cat.png

Conclusion

Network forensics requires systematic, methodical investigation combining technical skills, analytical thinking, and comprehensive documentation.