



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Intrusion Detection In-Depth (Security 503)"
at <http://www.giac.org/registration/gcia>

Jason Elrod

SANS2000 San Jose – GIAC Intrusion Detection Curriculum Practical Assignment

DETECT #1

[**] Source Port traffic [**]
06/10-20:50:49.910317 63.69.63.2:53 -> X.X.102.161:53
TCP TTL:28 TOS:0x0 ID:39426
SF** Seq: 0x7B0B3E9D Ack: 0x6ED7538C Win: 0x404

[**] Source Port traffic [**]
06/10-20:50:49.942981 63.69.63.2:53 -> X.X.102.252:53
TCP TTL:28 TOS:0x0 ID:39426
SF** Seq: 0x7B0B3E9D Ack: 0x6ED7538C Win: 0x404

[**] Source Port traffic [**]
06/10-20:50:49.961420 63.69.63.2:53 -> X.X.102.42:53
TCP TTL:28 TOS:0x0 ID:39426
SF** Seq: 0x7B0B3E9D Ack: 0x6ED7538C Win: 0x404

[**] Source Port traffic [**]
06/10-20:50:50.006324 63.69.63.2:53 -> X.X.102.162:53
TCP TTL:28 TOS:0x0 ID:39426
SF** Seq: 0x7B0B3E9D Ack: 0x6ED7538C Win: 0x404

[**] Source Port traffic [**]
06/10-20:50:50.441195 63.69.63.2:53 -> X.X.102.106:53
TCP TTL:28 TOS:0x0 ID:39426
SF** Seq: 0x69566FEB Ack: 0x643B20A1 Win: 0x404

[**] Source Port traffic [**]
06/10-20:50:50.501309 63.69.63.2:53 -> X.X.102.129:53
TCP TTL:28 TOS:0x0 ID:39426
SF** Seq: 0x69566FEB Ack: 0x643B20A1 Win: 0x404

[**] spp_portscan: portscan status from 63.69.63.2: 6 connections across 6 hosts:
TCP(6),

UDP(0) STEALTH [**]
06/11-04:02:26.548331

1.1 Source of trace:
-Client internal network.

1.2 Detect was generated by:

-Snort IDS system on a Red Hat Linux system.

1.3 Probability the source address was spoofed:

-Low. IP address is from a range of IP's registered to Unus Corporation, a web-hosting service.

1.4 Description of attack:

-Attacker is scanning for active hosts on the network on the DNS service port (53).
-Stealth scan attempt using anomalous tcp flags set (both SYN and FIN).
-This is a reconnaissance attack.

1.5 Attack mechanism:

-Attacker sends a tcp packet bound for TCP port 53 on various systems in the network being scanned. Both the SYN and FIN flags are set in an attempt to be more 'stealthy' and / or bypass firewall rules. This is mainly a network mapping mechanism. However, if the system detected during this scan were an unprotected DNS server, it could provide host and zone information to the attacker. This was the case on one of the systems on the internal network.

1.6 Correlations:

-This reconnaissance attack is what is more commonly known as a 'SYN/FIN stealth scan'. And can be performed with widely available tools such as NMAP.

1.7 Evidence of active targeting:

-This attack appears to have been generated from the host '63.69.63.2' and actively scanning various targets within the DMV internal network range. The attacker is most likely compromised the host system and is using it to sweep through IP ranges to gather information.

1.8 Severity =

- (critical + lethal) – (system + net countermeasures)
- (5 + 2) – (1 + 2) = 4

1.9 Defensive recommendation:

-Defenses do not seem to be adequate. Current firewall is not blocking this type of attack. Firewall needs to be adjusted to stop this type of scan. DNS servers internal to the network need to be configured to limit zone transfers. Both action need to be taken immediately.

1.10 Multiple-choice test question (based on trace and analysis with the answer)

The intent of this attack is:

- a) Denial of Service
- b) Information Gathering
- c) Backdoor system access
- d) None of the above

Answer: b

DETECT 2

----- Frame 1 -----
Frame Source Address Dest. Address Size Abs. Time
1 [63.15.247.57] [X.X.17.73] 60 04/12/2000 03:19:49 AM

Summary

DLC: Ethertype=0800, size=60 bytes
IP: D=[X.X.17.73] S=[63.15.247.57] LEN=26 ID=31063
UDP: D=31337 S=3220 LEN=26

DLC: ----- DLC Header -----

DLC:

DLC: Frame 1 arrived at 03:19:49.0000; frame size is 60 (003C hex) bytes.

DLC: Destination = Station Intel 6E5005

DLC: Source = Station 00605CF39D99

DLC: Ethertype = 0800 (IP)

DLC:

IP: ----- IP Header -----

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

IP: Total length = 46 bytes

IP: Identification = 31063

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 118 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = B235 (correct)

IP: Source address = [63.15.247.57]

IP: Destination address = [X.X.17.73]

IP: No options

IP:

UDP: ----- UDP Header -----

UDP:

UDP: Source port = 3220

UDP: Destination port = 31337

UDP: Length = 26

UDP: Checksum = 0D30 (correct)

UDP: [18 byte(s) of data]

UDP:

2.1 Source of trace:

-My network.

2.2 Detect was generated by:

-Black ICE Defender

2.3 Probability the source address was spoofed:

-Low. A reverse DNS of the offending address revealed

1Cust57.tnt.sacramento2.ca.da.uu.net. This belongs to the block of addresses used for dial-in access from UUNET.

2.4 Description of attack:

-Somebody has pinged the system for the "Back Orifice" trojan.

2.5 Attack mechanism:

-This machine has been scanned, but not targeted. This most likely means the hacker is scanning thousands of machines hoping to find one that has been compromised by Back Orifice.

2.6 Correlations:

-Back Orifice pings are the one of the most frequent attacks seen on the Internet. Well known for its particular port usage (31337) and its ease of use.

2.7 Evidence of active targeting:

-Probability of active targeting is low. The attackers was probably sweeping through a large number of IP's in the hopes of locating a compromised system.

2.8 Severity

-(critical + lethal) – (system + net countermeasures)

-(2 + 5) – (5 + 4) = -2

2.9 Defensive recommendation:

-Defenses are fine. Black ICE blocked and alerted on this attempt. System is clean.

2.10 Multiple-choice test question (based on trace and analysis with the answer)

This trace shows an attempt to:

- a) Initiate a DNS zone transfer.
- b) Determine if the host has been compromised by a Trojan.
- c) Ping the host to see if it is up.
- d) Respond to an Echo Request.

Answer: b

Detect 3

```
----- Frame 1 -----  
Frame Source Address  Dest. Address  Size  Abs. Time  
1 [X.X.17.73] [216.6.3.200]  70  01/19/2000 04:58:08 AM
```

SUMMARY

Expert: ICMP Port Unreachable
DLC: Ethertype=0800, size=70 bytes
IP: D=[216.6.3.200] S=[X.X.17.73] LEN=36 ID=19957
ICMP: Destination unreachable (Port unreachable)

DLC: ----- DLC Header -----

DLC:
DLC: Frame 1 arrived at 04:58:08.0000; frame size is 70 (0046 hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, Broadcast
DLC: Source = Station Intel 6E5005
DLC: Ethertype = 0800 (IP)
DLC:

IP: ----- IP Header -----

IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP: Total length = 56 bytes
IP: Identification = 19957
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 128 seconds/hops
IP: Protocol = 1 (ICMP)
IP: Header checksum = 2E18 (correct)
IP: Source address = [X.X.17.73]
IP: Destination address = [216.6.3.200]
IP: No options
IP:

ICMP: ----- ICMP header -----

ICMP:
ICMP: Type = 3 (Destination unreachable)
ICMP: Code = 3 (Port unreachable)
ICMP: Checksum = DE97 (correct)
ICMP:
ICMP: [Normal end of "ICMP header".]
ICMP:
ICMP: IP header of originating message (description follows)
ICMP:
ICMP: ----- IP Header -----
ICMP:
ICMP: Version = 4, header length = 20 bytes
ICMP: Type of service = 00
ICMP: 000. = routine
ICMP: ...0 = normal delay
ICMP: 0... = normal throughput
ICMP:0.. = normal reliability
ICMP: Total length = 58 bytes
ICMP: Identification = 12291
ICMP: Flags = 0X
ICMP: .0.. = may fragment
ICMP: ..0. = last fragment
ICMP: Fragment offset = 0 bytes
ICMP: Time to live = 51 seconds/hops
ICMP: Protocol = 17 (UDP)
ICMP: Header checksum = 98F8 (correct)
ICMP: Source address = [216.6.3.200]
ICMP: Destination address = [X.X.17.73]
ICMP: No options
ICMP:
ICMP: [First 8 byte(s) of data of originating message]
ICMP:

```
----- Frame 2 -----  
Frame Source Address  Dest. Address  Size  Abs. Time
```

2 [X.X.17.73] [216.6.3.200] 70 01/19/2000 04:58:08 am

Summary

Expert: ICMP Port Unreachable

DLC: Ethertype=0800, size=70 bytes

IP: D=[216.6.3.200] S=[X.X.17.73] LEN=36 ID=20213

ICMP: Destination unreachable (Port unreachable)

DLC: ----- DLC Header -----

DLC:

DLC: Frame 2 arrived at 04:58:08.1550; frame size is 70 (0046 hex) bytes.

DLC: Destination = BROADCAST FFFFFFFF, Broadcast

DLC: Source = Station Intel 6E5005

DLC: Ethertype = 0800 (IP)

DLC:

IP: ----- IP Header -----

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000. = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

IP: Total length = 56 bytes

IP: Identification = 20213

IP: Flags = 0X

IP: .0.. = may fragment

IP: ..0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 128 seconds/hops

IP: Protocol = 1 (ICMP)

IP: Header checksum = 2D18 (correct)

IP: Source address = [X.X.17.73]

IP: Destination address = [216.6.3.200]

IP: No options

IP:

ICMP: ----- ICMP header -----

ICMP:

ICMP: Type = 3 (Destination unreachable)

ICMP: Code = 3 (Port unreachable)

ICMP: Checksum = DE97 (correct)

ICMP:

ICMP: [Normal end of "ICMP header".]

ICMP:

ICMP: IP header of originating message (description follows)

ICMP:

ICMP: ----- IP Header -----

ICMP:

ICMP: Version = 4, header length = 20 bytes

ICMP: Type of service = 00

ICMP: 000. = routine

ICMP: ...0 = normal delay

ICMP: 0... = normal throughput

ICMP:0.. = normal reliability

ICMP: Total length = 58 bytes

ICMP: Identification = 12296

ICMP: Flags = 0X

ICMP: .0.. = may fragment

ICMP: ..0. = last fragment

ICMP: Fragment offset = 0 bytes

ICMP: Time to live = 51 seconds/hops

ICMP: Protocol = 17 (UDP)

ICMP: Header checksum = 98F3 (correct)

ICMP: Source address = [216.6.3.200]

ICMP: Destination address = [X.X.17.73]

ICMP: No options

ICMP:

ICMP: [First 8 byte(s) of data of originating message]

ICMP:

----- Frame 3 -----
Frame Source Address Dest. Address Size Abs. Time
3 [216.6.3.200] [X.X.17.74] 72 01/19/2000 04:58:08 AM

Summary

DLC: Ethertype=0800, size=72 bytes

IP: D=[X.X.17.74] S=[216.6.3.200] LEN=38 ID=12299

UDP: D=53 S=1948 LEN=38

DNS: C ID=6 OP=QUERY NAME=version.bind

DLC: ----- DLC Header -----

DLC:

DLC: Frame 3 arrived at 04:58:08.3000; frame size is 72 (0048 hex) bytes.

DLC: Destination = Station 0008C7FA808D

DLC: Source = Station 00605CF39D99

DLC: Ethertype = 0800 (IP)

DLC:

IP: ----- IP Header -----

IP:

IP: Version = 4, header length = 20 bytes

IP: Type of service = 00

IP: 000 = routine

IP: ...0 = normal delay

IP: 0... = normal throughput

IP:0.. = normal reliability

IP: Total length = 58 bytes

IP: Identification = 12299

IP: Flags = 0X

IP: .0.. = may fragment

IP: .0. = last fragment

IP: Fragment offset = 0 bytes

IP: Time to live = 51 seconds/hops

IP: Protocol = 17 (UDP)

IP: Header checksum = 98EF (correct)

IP: Source address = [216.6.3.200]

IP: Destination address = [X.X.17.74]

IP: No options

IP:

UDP: ----- UDP Header -----

UDP:

UDP: Source port = 1948

UDP: Destination port = 53 (Domain)

UDP: Length = 38

UDP: Checksum = 166D (correct)

UDP: [30 byte(s) of data]

UDP:

DNS: ----- Internet Domain Name Service header -----

DNS:

DNS: ID = 6

DNS: Flags = 01

DNS: 0..... = Command

DNS: .000 0... = Query

DNS:0. = Not truncated

DNS:1 = Recursion desired

DNS: Flags = 0X

DNS: ...0 = Non Verified data NOT acceptable

DNS: Question count = 1, Answer count = 0

DNS: Authority count = 0, Additional record count = 0

DNS:

DNS: ZONE Section

DNS: Name = version.bind

DNS: Type = Text data (TXT,16)

DNS: Class = Chaos net (CH,3)

DNS:

----- Frame 4 -----

Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time
4 [216.6.3.200] [X.X.17.74] 72 000:01:05.045 64.745.000 01/19/2000 04:59:13 AM

Summary

DLC: Ethertype=0800, size=72 bytes

IP: D=[X.X.17.74] S=[216.6.3.200] LEN=38 ID=12369

UDP: D=53 S=1948 LEN=38

DNS: C ID=6 OP=QUERY NAME=version.bind

DLC: ----- DLC Header -----

DLC:

DLC: Frame 4 arrived at 04:59:13.0450; frame size is 72 (0048 hex) bytes.

DLC: Destination = Station 0008C7FA808D

DLC: Source = Station 00605CF39D99

DLC: Ethertype = 0800 (IP)

DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP:0 = normal delay
IP: 0... = normal throughput
IP:0.. = normal reliability
IP: Total length = 58 bytes
IP: Identification = 12369
IP: Flags = 0X
IP:0.. = may fragment
IP:0.. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 51 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 98A9 (correct)
IP: Source address = [216.6.3.200]
IP: Destination address = [X.X.17.74]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 1948
UDP: Destination port = 53 (Domain)
UDP: Length = 38
UDP: Checksum = 166D (correct)
UDP: [30 byte(s) of data]
UDP:
DNS: ----- Internet Domain Name Service header -----
DNS:
DNS: ID = 6
DNS: Flags = 01
DNS: 0... = Command
DNS: .000 0... = Query
DNS:0. = Not truncated
DNS:1 = Recursion desired
DNS: Flags = 0X
DNS: ...0 = Non Verified data NOT acceptable
DNS: Question count = 1, Answer count = 0
DNS: Authority count = 0, Additional record count = 0
DNS:
DNS: ZONE Section
DNS: Name = version.bind
DNS: Type = Text data (TXT,16)
DNS: Class = Chaos net (CH,3)
DNS:

3.1 Source of trace:

-My network.

3.2 Detect was generated by:

-Black ICE Defender

3.3 Probability the source address was spoofed:

-Low. There was no reverse DNS information available for this host. An ARIN lookup on the IP block revealed that it was registered to Gamma Entertainment.

3.4 Description of attack:

-Either a hacker is scanning this system looking for the "DNS" service, or somebody has mis-configured your machine as a DNS server. They are also looking for the version of BIND that we may be running.

3.5 Attack mechanism:

-The attacker sends a request on port 53 with a query as to which version of BIND that the receiving host is running. If the victim host responds, the attacker has two very valuable pieces of information. 1) That the host is alive and running DNS and 2) The actual version of BIND on that machine. This is valuable because there are known vulnerabilities in certain versions of BIND that will allow an attacker to get access to a system. Even if the current version on a system is free from bugs, a new exploit may surface and the hacker has a list already of hosts that are running that version. Thus making the box subject to future attacks.

3.6 Correlations:

Various BIND and DNS related vulnerabilities exist and are a common exploit used to gain access to remote systems.

3.7 Evidence of active targeting:

-Low. Other systems on the network received the same two packets. This was most likely just a probe for information and not a directed attack against the systems listed above.

3.8 Severity

-(critical + lethal) – (system + net countermeasures)

-(5 + 1) – (5 + 4) = -3

3.9 Defensive recommendation:

-Defenses are fine. No actions required as these systems are not running any instances of DNS.

3.10 Multiple-choice test question (based on trace and analysis with the answer)

The above trace shows the following:

- a) DNS zone transfer
- b) Inverse network mapping attempt
- c) DNS host mapping attempt
- d) None of the above

Answer: c

Detect 4

```
----- Frame 1 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time  Summary
1 [X.X.17.73] [199.236.213.1]  70 000:00:00.000 0.000.000  02/29/2000 07:40:12 PM Expert: ICMP Port Unreachable
                                DLC: Ethertype=0800, size=70 bytes
                                IP: D=[199.236.213.1] S=[X.X.17.73] LEN=36 ID=21780
                                ICMP: Destination unreachable (Port unreachable)
----- Frame 2 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time  Summary
2 [X.X.17.73] [199.236.213.1]  70 000:02:21.444 141.444.000  02/29/2000 07:42:33 PM Expert: ICMP Port Unreachable
                                DLC: Ethertype=0800, size=70 bytes
                                IP: D=[199.236.213.1] S=[X.X.17.73] LEN=36 ID=22292
                                ICMP: Destination unreachable (Port unreachable)
----- Frame 3 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time  Summary
3 [X.X.17.73] [199.236.213.1]  70 000:07:29.050 307.606.000  02/29/2000 07:47:41 PM Expert: ICMP Port Unreachable
                                DLC: Ethertype=0800, size=70 bytes
                                IP: D=[199.236.213.1] S=[X.X.17.73] LEN=36 ID=22548
                                ICMP: Destination unreachable (Port unreachable)
----- Frame 4 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time  Summary
4 [X.X.17.73] [199.236.213.1]  70 000:38:55.334 1886.284.000  02/29/2000 08:19:07 PM Expert: ICMP Port Unreachable
                                DLC: Ethertype=0800, size=70 bytes
                                IP: D=[199.236.213.1] S=[X.X.17.73] LEN=36 ID=23316
                                ICMP: Destination unreachable (Port unreachable)
----- Frame 5 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time  Summary
5 [X.X.17.73] [199.236.213.1]  70 000:56:22.389 1047.055.000  02/29/2000 08:36:34 PM Expert: ICMP Port Unreachable
                                DLC: Ethertype=0800, size=70 bytes
                                IP: D=[199.236.213.1] S=[X.X.17.73] LEN=36 ID=23828
                                ICMP: Destination unreachable (Port unreachable)
```

4.1 Source of trace:

-My network.

4.2 Detect was generated by:

-Black ICE Defender

4.3 Probability the source address was spoofed:

-High. We are seeing several responses that don't have corresponding requests. Doing a reverse DNS lookup we find that the address translates to 'lin-nat-213-001.linfiled.edu'. Most likely a host or user at that particular school.

4.4 Description of attack:

-Two possible:

- 1) Denial of service overload attempt. A large number of ICMP port-unreachable frames have been sent to a single IP address. The system and network may become unresponsive.
- 2) This may also occur as the result of a system or network mis-configuration. Sometimes, the system labeled as the intruder is trying to repetitively access a service which is unavailable.

4.5 Attack mechanism:

-Attack by a UDP-port scanner, which is scanning unsupported ports.
-This also may be a denial of service attack in which the source IP address is spoofed. The victim of this attack would be the destination address listed in the detect.

4.6 Correlations:

-I also saw a similar trace from the same system over the next two days. There has been no further traffic from this site leading me to believe that this is most likely a system that is misconfigured.

4.7 Evidence of active targeting:

-Low. This is a system that is not running the service requested and further leads me to believe that it was just a misconfiguration on the part of the remote systems admin.

4.8 Severity

-(critical + lethal) – (system + net countermeasures)

-(2+1) – (5+4) = -6

4.9 Defensive recommendation:

-Defenses are fine. No action required.

4.10 Multiple-choice test question (based on trace and analysis with the answer)

The above trace is an example of:

- a) PC Anywhere connection attempt.
- b) Inverse network mapping attempt
- c) A mis-configured system
- d) ICMP unreachable storm DOS attack

Answer: c

© SANS Institute 2000 - 2002. Author retains full rights.

Detect 5

```
----- Frame 1 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time      Summary
1 [63.202.81.195] [XX.17.74] 1468 000:00:00.000 0.000.000 06/10/2000 03:36:52 PM DLC: Ethertype=0800, size=1468 bytes
                                          P: D=[XX.17.74] S=[63.202.81.195] LEN=1434 ID=15329
                                          TCP: D=4699 S=6699 ACK=1408870595 SEQ=22388285 LEN=1414 WIN=8393

DLC: ---- DLC Header ----
DLC:
DLC: Frame 1 arrived at 15:36:52.1240; frame size is 1468 (05BC hex) bytes.
DLC: Destination = Station 0008C7FA808D
DLC: Source = Station 00605CF39D99
DLC: Ethertype = 0800 (IP)
DLC:

IP: ---- IP Header ----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0.. = normal throughput
IP: .... .0. = normal reliability
IP: Total length = 1454 bytes
IP: Identification = 15329
IP: Flags = 4X
IP: .1. .... = don't fragment
IP: .0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 116 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = 50F1 (correct)
IP: Source address = [63.202.81.195]
IP: Destination address = [XX.17.74]
IP: No options
IP:

TCP: ---- TCP header ----
TCP:
TCP: Source port = 6699
TCP: Destination port = 4699
TCP: Sequence number = 22388285
TCP: Next expected Seq number= 22389699
TCP: Acknowledgment number = 1408870595
TCP: Data offset = 20 bytes
TCP: Flags = 10
TCP: ..0. .... = (No urgent pointer)
TCP: ...1 .... = Acknowledgment
TCP: .... 0.. = (No push)
TCP: .... .0. = (No reset)
TCP: .... .0. = (No SYN)
TCP: .... .0. = (No FIN)
TCP: Window = 8393
TCP: Checksum = 61A2 (correct)
TCP: No TCP options
TCP: [1414 Bytes of data]
TCP:

----- Frame 2 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time      Summary
2 [208.184.216.220] [XX.17.74] 74 000:50:46.986 3046.986.000 06/10/2000 04:27:39 PM Expert: Idle Too Long
                                          DLC: Ethertype=0800, size=74 bytes
                                          IP: D=[XX.17.74] S=[208.184.216.220] LEN=40 ID=23017
                                          TCP: D=4697 S=8888 ACK=1407536257 SEQ=2420392442 LEN=20 WIN=16060

DLC: ---- DLC Header ----
DLC:
DLC: Frame 2 arrived at 16:27:39.1100; frame size is 74 (004A hex) bytes.
DLC: Destination = Station 0008C7FA808D
DLC: Source = Station 00605CF39D99
DLC: Ethertype = 0800 (IP)
DLC:

IP: ---- IP Header ----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0.. = normal throughput
IP: .... .0. = normal reliability
IP: Total length = 60 bytes
IP: Identification = 23017
IP: Flags = 4X
IP: .1. .... = don't fragment
IP: .0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 51 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = 6153 (correct)
IP: Source address = [208.184.216.220]
IP: Destination address = [XX.17.74]
IP: No options
```

```

IP:
TCP: ----- TCP header -----
TCP:
TCP: Source port      = 8888
TCP: Destination port = 4697
TCP: Sequence number  = 2420392442
TCP: Next expected Seq number= 2420392462
TCP: Acknowledgment number = 1407536257
TCP: Data offset      = 20 bytes
TCP: Flags            = 18
TCP:   ..0. .... = (No urgent pointer)
TCP:   ...1 .... = Acknowledgment
TCP:   .... 1... = Push
TCP:   .... 0.. = (No reset)
TCP:   .... .0. = (No SYN)
TCP:   .... ...0 = (No FIN)
TCP: Window          = 16060
TCP: Checksum        = CB2B (correct)
TCP: No TCP options
TCP: [20 Bytes of data]
TCP:

```

```

----- Frame 3 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time      Summary
3 [208.184.216.182] [X.X.17.74]  74 001:31:37.701 2450.715.000 06/10/2000 05:08:29 PM Expert Idle Too Long
DLC: Ethertype=0800, size=74 bytes
IP:  D=[X.X.17.74] S=[208.184.216.182] LEN=40 ID=54414
TCP:  D=4719 S=7777  ACK=1412587852 SEQ=32973252 LEN=20 WIN=16060

```

```

DLC: ----- DLC Header -----
DLC:
DLC: Frame 3 arrived at 17:08:29.8250; frame size is 74 (004A hex) bytes.
DLC: Destination = Station 0008C7FA808D
DLC: Source      = Station 00605CF39D99
DLC: Ethertype   = 0800 (IP)
DLC:

```

```

IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:   000. .... = routine
IP:   ...0 .... = normal delay
IP:   .... 0.. = normal throughput
IP:   .... .0. = normal reliability
IP: Total length = 60 bytes
IP: Identification = 54414
IP: Flags        = 4X
IP:   .1. .... = don't fragment
IP:   ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live  = 51 seconds/hops
IP: Protocol     = 6 (TCP)
IP: Header checksum = E6D3 (correct)
IP: Source address = [208.184.216.182]
IP: Destination address = [X.X.17.74]
IP: No options
IP:

```

```

TCP: ----- TCP header -----
TCP:
TCP: Source port      = 7777
TCP: Destination port = 4719
TCP: Sequence number  = 32973252
TCP: Next expected Seq number= 32973272
TCP: Acknowledgment number = 1412587852
TCP: Data offset      = 20 bytes
TCP: Flags            = 18
TCP:   ..0. .... = (No urgent pointer)
TCP:   ...1 .... = Acknowledgment
TCP:   .... 1... = Push
TCP:   .... 0.. = (No reset)
TCP:   .... .0. = (No SYN)
TCP:   .... ...0 = (No FIN)
TCP: Window          = 16060
TCP: Checksum        = 6EFC (correct)
TCP: No TCP options
TCP: [20 Bytes of data]
TCP:

```

```

----- Frame 4 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time      Summary
4 [208.184.216.182] [X.X.17.74]  74 001:51:42.296 1204.595.000 06/10/2000 05:28:34 PM Expert Idle Too Long
DLC: Ethertype=0800, size=74 bytes
IP:  D=[X.X.17.74] S=[208.184.216.182] LEN=40 ID=14126
TCP:  D=4719 S=7777  ACK=1412589359 SEQ=32993705 LEN=20 WIN=16060

```

```

DLC: ----- DLC Header -----
DLC:
DLC: Frame 4 arrived at 17:28:34.4200; frame size is 74 (004A hex) bytes.
DLC: Destination = Station 0008C7FA808D
DLC: Source      = Station 00605CF39D99
DLC: Ethertype   = 0800 (IP)
DLC:

```

```

IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes

```

```

IP: Type of service = 00
IP: 000 .... = routine
IP: ...0 .... = normal delay
IP: ....0.. = normal throughput
IP: ....0.. = normal reliability
IP: Total length = 60 bytes
IP: Identification = 14126
IP: Flags = 4X
IP: .1. .... = don't fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 51 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = 8434 (correct)
IP: Source address = [208.184.216.182]
IP: Destination address = [X.X.17.74]
IP: No options
IP:
TCP: ---- TCP header ----
TCP:
TCP: Source port = 7777
TCP: Destination port = 4719
TCP: Sequence number = 32993705
TCP: Next expected Seq number= 32993725
TCP: Acknowledgment number = 1412589359
TCP: Data offset = 20 bytes
TCP: Flags = 18
TCP: ..0. .... = (No urgent pointer)
TCP: ...1 .... = Acknowledgment
TCP: ....1... = Push
TCP: ....0.. = (No reset)
TCP: ....0.. = (No SYN)
TCP: ....0.. = (No FIN)
TCP: Window = 16060
TCP: Checksum = 0D3E (correct)
TCP: No TCP options
TCP: [20 Bytes of data]
TCP:

```

```

----- Frame 5 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time  Summary
5 [208.184.216.191] [X.X.17.74]  74 002:13:07.400 1285.104.000 06/10/2000 05:49:59 PM Expert: Idle Too Long
                                     DLC: Ethertype=0800, size=74 bytes
                                     IP: D=[X.X.17.74] S=[208.184.216.191] LEN=40 ID=198
                                     TCP: D=4771 S=8888 ACK=1417059045 SEQ=483306619 LEN=20 WIN=16060

```

```

DLC: ---- DLC Header ----
DLC:
DLC: Frame 5 arrived at 17:49:59.5240; frame size is 74 (004A hex) bytes.
DLC: Destination = Station 0008C7FA808D
DLC: Source = Station 00605CF39D99
DLC: Ethertype = 0800 (IP)
DLC:

```

```

IP: ---- IP Header ----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000 .... = routine
IP: ...0 .... = normal delay
IP: ....0.. = normal throughput
IP: ....0.. = normal reliability
IP: Total length = 60 bytes
IP: Identification = 198
IP: Flags = 4X
IP: .1. .... = don't fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 51 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = BA93 (correct)
IP: Source address = [208.184.216.191]
IP: Destination address = [X.X.17.74]
IP: No options
IP:

```

```

TCP: ---- TCP header ----
TCP:
TCP: Source port = 8888
TCP: Destination port = 4771
TCP: Sequence number = 483306619
TCP: Next expected Seq number= 483306639
TCP: Acknowledgment number = 1417059045
TCP: Data offset = 20 bytes
TCP: Flags = 18
TCP: ..0. .... = (No urgent pointer)
TCP: ...1 .... = Acknowledgment
TCP: ....1... = Push
TCP: ....0.. = (No reset)
TCP: ....0.. = (No SYN)
TCP: ....0.. = (No FIN)
TCP: Window = 16060
TCP: Checksum = 7504 (correct)
TCP: No TCP options
TCP: [20 Bytes of data]
TCP:

```

```

----- Frame 6 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time  Summary
6 [203.164.66.72] [XX.17.74] 1514 002:23:07.981 600.581.000 06/10/2000 06:00:00 PM Expert: Idle Too Long
DLC: Ethertype=0800, size=1514 bytes
IP: D=[XX.17.74] S=[203.164.66.72] LEN=1480 ID=5628
TCP: D=4785 S=6699 ACK=1417822968 SEQ=52770261 LEN=1460 WIN=8685

```

```

DLC: ---- DLC Header ----
DLC:
DLC: Frame 6 arrived at 18:00:00.1050; frame size is 1514 (05EA hex) bytes.
DLC: Destination = Station 0008C7FA808D
DLC: Source = Station 00605CF39D99
DLC: Ethertype = 0800 (IP)
DLC:

```

```

IP: ---- IP Header ----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0.. = normal throughput
IP: .... .0.. = normal reliability
IP: Total length = 1500 bytes
IP: Identification = 5628
IP: Flags = 4X
IP: .1. .... = don't fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 111 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = FF48 (correct)
IP: Source address = [203.164.66.72]
IP: Destination address = [XX.17.74]
IP: No options
IP:

```

```

TCP: ---- TCP header ----
TCP:
TCP: Source port = 6699
TCP: Destination port = 4785
TCP: Sequence number = 52770261
TCP: Next expected Seq number= 52771721
TCP: Acknowledgment number = 1417822968
TCP: Data offset = 20 bytes
TCP: Flags = 10
TCP: ..0. .... = (No urgent pointer)
TCP: ...1 .... = Acknowledgment
TCP: .... 0.. = (No push)
TCP: .... .0.. = (No reset)
TCP: .... .0.. = (No SYN)
TCP: .... .0.. = (No FIN)
TCP: Window = 8685
TCP: Checksum = DA8B (correct)
TCP: No TCP options
TCP: [1460 Bytes of data]
TCP:

```

```

----- Frame 7 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time  Summary
7 [208.184.216.191] [XX.17.74] 130 002:33:15.726 607.745.000 06/10/2000 06:10:07 PM Expert: Idle Too Long
DLC: Ethertype=0800, size=130 bytes
IP: D=[XX.17.74] S=[208.184.216.191] LEN=96 ID=53475
TCP: D=4771 S=8888 ACK=1417060778 SEQ=483315647 LEN=76 WIN=16060

```

```

DLC: ---- DLC Header ----
DLC:
DLC: Frame 7 arrived at 18:10:07.8500; frame size is 130 (0082 hex) bytes.
DLC: Destination = Station 0008C7FA808D
DLC: Source = Station 00605CF39D99
DLC: Ethertype = 0800 (IP)
DLC:

```

```

IP: ---- IP Header ----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0.. = normal throughput
IP: .... .0.. = normal reliability
IP: Total length = 116 bytes
IP: Identification = 53475
IP: Flags = 4X
IP: .1. .... = don't fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 51 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = EA3D (correct)
IP: Source address = [208.184.216.191]
IP: Destination address = [XX.17.74]
IP: No options
IP:

```

```

TCP: ---- TCP header ----
TCP:
TCP: Source port = 8888

```


TCP: Destination port = 4771
 TCP: Sequence number = 483315647
 TCP: Next expected Seq number= 483315723
 TCP: Acknowledgment number = 1417060778
 TCP: Data offset = 20 bytes
 TCP: Flags = 18
 TCP: .0. = (No urgent pointer)
 TCP:1 = Acknowledgment
 TCP: 1... = Push
 TCP:0.. = (No reset)
 TCP:0. = (No SYN)
 TCP:0 = (No FIN)
 TCP: Window = 16060
 TCP: Checksum = 3FB4 (correct)
 TCP: No TCP options
 TCP: [76 Bytes of data]
 TCP:

----- Frame 8 -----
 Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
 8 [63.202.81.51] [X.X 17.74] 642 004:44:25.971 7870.245.000 06/10/2000 08:21:18 PM Expert: Idle Too Long

DLC: Ethertype=0800, size=642 bytes
 IP: D=[X.X 17.74] S=[63.202.81.51] LEN=608 ID=42109
 TCP: D=4865 S=6688 ACK=1425991590 SEQ=37279096 LEN=588 WIN=8694

DLC: ---- DLC Header ----

DLC:
 DLC: Frame 8 arrived at 20:21:18.0950; frame size is 642 (0282 hex) bytes.
 DLC: Destination = Station 0008C7FA808D
 DLC: Source = Station 00605CF39D99
 DLC: Ethertype = 0800 (IP)
 DLC:

IP: ---- IP Header ----

IP:
 IP: Version = 4, header length = 20 bytes
 IP: Type of service = 00
 IP: 000. = routine
 IP: ...0 = normal delay
 IP: 0.. = normal throughput
 IP:0.. = normal reliability
 IP: Total length = 628 bytes
 IP: Identification = 42109
 IP: Flags = 4X
 IP: .1. = don't fragment
 IP: ..0. = last fragment
 IP: Fragment offset = 0 bytes
 IP: Time to live = 116 seconds/hops
 IP: Protocol = 6 (TCP)
 IP: Header checksum = EC1E (correct)
 IP: Source address = [63.202.81.51]
 IP: Destination address = [X.X 17.74]
 IP: No options
 IP:

TCP: ---- TCP header ----

TCP:
 TCP: Source port = 6688
 TCP: Destination port = 4865
 TCP: Sequence number = 37279096
 TCP: Next expected Seq number= 37279684
 TCP: Acknowledgment number = 1425991590
 TCP: Data offset = 20 bytes
 TCP: Flags = 18
 TCP: .0. = (No urgent pointer)
 TCP:1 = Acknowledgment
 TCP: 1... = Push
 TCP:0.. = (No reset)
 TCP:0. = (No SYN)
 TCP:0 = (No FIN)
 TCP: Window = 8694
 TCP: Checksum = 0E21 (correct)
 TCP: No TCP options
 TCP: [588 Bytes of data]
 TCP:

----- Frame 9 -----
 Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
 9 [167.206.203.122] [X.X 17.74] 1514 006:16:44.216 5538.245.000 06/10/2000 09:53:36 PM Expert: Idle Too Long

DLC: Ethertype=0800, size=1514 bytes
 IP: D=[X.X 17.74] S=[167.206.203.122] LEN=1480 ID=54620
 TCP: D=4899 S=6688 ACK=1431623350 SEQ=48842042 LEN=1460 WIN=8708

DLC: ---- DLC Header ----

DLC:
 DLC: Frame 9 arrived at 21:53:36.3400; frame size is 1514 (05EA hex) bytes.
 DLC: Destination = Station 0008C7FA808D
 DLC: Source = Station 00605CF39D99
 DLC: Ethertype = 0800 (IP)
 DLC:

IP: ---- IP Header ----

IP:
 IP: Version = 4, header length = 20 bytes
 IP: Type of service = 00
 IP: 000. = routine
 IP: ...0 = normal delay
 IP: 0.. = normal throughput

IP:0.. = normal reliability
 IP: Total length = 1500 bytes
 IP: Identification = 54620
 IP: Flags = 4X
 IP: .1. = don't fragment
 IP: ..0. = last fragment
 IP: Fragment offset = 0 bytes
 IP: Time to live = 113 seconds/hops
 IP: Protocol = 6 (TCP)
 IP: Header checksum = D88B (correct)
 IP: Source address = [167.206.203.122]
 IP: Destination address = [XX.17.74]
 IP: No options
 IP:
 TCP: ---- TCP header ----
 TCP:
 TCP: Source port = 6688
 TCP: Destination port = 4899
 TCP: Sequence number = 48842042
 TCP: Next expected Seq number= 48843502
 TCP: Acknowledgment number = 1431623350
 TCP: Data offset = 20 bytes
 TCP: Flags = 10
 TCP: ..0. = (No urgent pointer)
 TCP: ...1 = Acknowledgment
 TCP:0.. = (No push)
 TCP:0.. = (No reset)
 TCP:0.. = (No SYN)
 TCP:0.. = (No FIN)
 TCP: Window = 8708
 TCP: Checksum = FFFE (correct)
 TCP: No TCP options
 TCP: [1460 Bytes of data]
 TCP:

----- Frame 10 -----

Frame	Source Address	Dest. Address	Size	Rel. Time	Delta Time	Abs. Time	Summary
10	[206.170.161.231]	[XX.17.74]	60	006:26:47.456	603.240.000	06/10/2000 10:03:39 PM	Expert Idle Too Long DLC: Ethertype=0800, size=60 bytes IP: D=[XX.17.74] S=[206.170.161.231] LEN=8 ID=35360 ICMP: Echo

DLC: ---- DLC Header ----
 DLC:
 DLC: Frame 10 arrived at 22:03:39.5800; frame size is 60 (003C hex) bytes.
 DLC: Destination = Station 0008C7FA808D
 DLC: Source = Station 00605CF39D99
 DLC: Ethertype = 0800 (IP)
 DLC:

IP: ---- IP Header ----
 IP:
 IP: Version = 4, header length = 20 bytes
 IP: Type of service = 00
 IP: 000. = routine
 IP: ...0 = normal delay
 IP:0.. = normal throughput
 IP:0.. = normal reliability
 IP: Total length = 28 bytes
 IP: Identification = 35360
 IP: Flags = 0X
 IP: ..0. = may fragment
 IP: ..0. = last fragment
 IP: Fragment offset = 0 bytes
 IP: Time to live = 115 seconds/hops
 IP: Protocol = 1 (ICMP)
 IP: Header checksum = 6A44 (correct)
 IP: Source address = [206.170.161.231]
 IP: Destination address = [XX.17.74]
 IP: No options
 IP:

ICMP: ---- ICMP header ----
 ICMP:
 ICMP: Type = 8 (Echo)
 ICMP: Code = 0
 ICMP: Checksum = E8FF (correct)
 ICMP: Identifier = 512
 ICMP: Sequence number = 3328
 ICMP: [0 bytes of data]
 ICMP:
 ICMP: [Normal end of "ICMP header".]
 ICMP:

----- Frame 11 -----

Frame	Source Address	Dest. Address	Size	Rel. Time	Delta Time	Abs. Time	Summary
11	[208.184.216.214]	[XX.17.74]	184	006:36:52.011	604.555.000	06/10/2000 10:13:44 PM	DLC: Ethertype=0800, size=184 bytes IP: D=[XX.17.74] S=[208.184.216.214] LEN=150 ID=49377 TCP: D=4889 S=8888 ACK=1431457897 SEQ=536466955 LEN=130 WIN=16060

DLC: ---- DLC Header ----
 DLC:
 DLC: Frame 11 arrived at 22:13:44.1350; frame size is 184 (00B8 hex) bytes.
 DLC: Destination = Station 0008C7FA808D
 DLC: Source = Station 00605CF39D99
 DLC: Ethertype = 0800 (IP)
 DLC:

IP: ----- IP Header -----
 IP:
 IP: Version = 4, header length = 20 bytes
 IP: Type of service = 00
 IP: 000. = routine
 IP:0 = normal delay
 IP: 0... = normal throughput
 IP:0.. = normal reliability
 IP: Total length = 170 bytes
 IP: Identification = 49377
 IP: Flags = 4X
 IP: .1. = don't fragment
 IP: .0. = last fragment
 IP: Fragment offset = 0 bytes
 IP: Time to live = 51 seconds/hops
 IP: Protocol = 6 (TCP)
 IP: Header checksum = F9F2 (correct)
 IP: Source address = [208.184.216.214]
 IP: Destination address = [XX.17.74]
 IP: No options
 IP:

TCP: ----- TCP header -----
 TCP:
 TCP: Source port = 8888
 TCP: Destination port = 4889
 TCP: Sequence number = 536466955
 TCP: Next expected Seq number= 536467085
 TCP: Acknowledgment number = 1431457897
 TCP: Data offset = 20 bytes
 TCP: Flags = 18
 TCP: ..0. = (No urgent pointer)
 TCP: ...1 = Acknowledgment
 TCP: 1... = Push
 TCP:0.. = (No reset)
 TCP:0. = (No SYN)
 TCP:0. = (No FIN)
 TCP: Window = 16060
 TCP: Checksum = 9134 (correct)
 TCP: No TCP options
 TCP: [130 Bytes of data]
 TCP:

----- Frame 12 -----

Frame	Source Address	Dest. Address	Size	Rel. Time	Delta Time	Abs. Time	Summary
12	[204.210.25.10]	[XX.17.74]	1514	006:46:53.035	601.024.000	06/10/2000 10:23:45 PM	Expert: Idle Too Long DLC: Ethertype=0800, size=1514 bytes IP: D=[XX.17.74] S=[204.210.25.10] LEN=1480 ID=42163 TCP: D=4907 S=6699 ACK=1433149681 SEQ=46408556 LEN=1460 WIN=8719

DLC: ----- DLC Header -----
 DLC:
 DLC: Frame 12 arrived at 22:23:45.1590; frame size is 1514 (05EA hex) bytes.
 DLC: Destination = Station 0008C7FA808D
 DLC: Source = Station 00605CF39D99
 DLC: Ethertype = 0800 (IP)
 DLC:

IP: ----- IP Header -----
 IP:
 IP: Version = 4, header length = 20 bytes
 IP: Type of service = 00
 IP: 000. = routine
 IP:0 = normal delay
 IP: 0... = normal throughput
 IP:0.. = normal reliability
 IP: Total length = 1500 bytes
 IP: Identification = 42163
 IP: Flags = 4X
 IP: .1. = don't fragment
 IP: .0. = last fragment
 IP: Fragment offset = 0 bytes
 IP: Time to live = 111 seconds/hops
 IP: Protocol = 6 (TCP)
 IP: Header checksum = 98A1 (correct)
 IP: Source address = [204.210.25.10]
 IP: Destination address = [XX.17.74]
 IP: No options
 IP:

TCP: ----- TCP header -----
 TCP:
 TCP: Source port = 6699
 TCP: Destination port = 4907
 TCP: Sequence number = 46408556
 TCP: Next expected Seq number= 46410016
 TCP: Acknowledgment number = 1433149681
 TCP: Data offset = 20 bytes
 TCP: Flags = 10
 TCP: ..0. = (No urgent pointer)
 TCP: ...1 = Acknowledgment
 TCP: 0... = (No push)
 TCP:0.. = (No reset)
 TCP:0. = (No SYN)
 TCP:0. = (No FIN)
 TCP: Window = 8719
 TCP: Checksum = A0AD (correct)

TCP: No TCP options
TCP: [1460 Bytes of data]
TCP:

----- Frame 13 -----
Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
13 [24.3.1.158] [XX.17.74] 1514 020:26:41.706 49188.671.000 06/11/2000 12:03:33 PM Expert: Idle Too Long
DLC: Ethertype=0800, size=1514 bytes
IP: D=[XX.17.74] S=[24.3.1.158] LEN=1480 ID=21610
TCP: D=1164 S=6688 ACK=1482357213 SEQ=69725702 LEN=1460 WIN=8682

DLC: ---- DLC Header ----

DLC:
DLC: Frame 13 arrived at 12:03:33.8300; frame size is 1514 (05EA hex) bytes.
DLC: Destination = Station 0008C7FA808D
DLC: Source = Station 00605CF39D99
DLC: Ethertype = 0800 (IP)
DLC:

IP: ---- IP Header ----

IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0.. = normal throughput
IP:0.. = normal reliability
IP: Total length = 1500 bytes
IP: Identification = 21610
IP: Flags = 4X
IP: .1. = don't fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 113 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = B326 (correct)
IP: Source address = [24.3.1.158]
IP: Destination address = [XX.17.74]
IP: No options
IP:

TCP: ---- TCP header ----

TCP:
TCP: Source port = 6688
TCP: Destination port = 1164
TCP: Sequence number = 69725702
TCP: Next expected Seq number= 69727162
TCP: Acknowledgment number = 1482357213
TCP: Data offset = 20 bytes
TCP: Flags = 18
TCP: ..0. = (No urgent pointer)
TCP: ...1 = Acknowledgment
TCP: 1... = Push
TCP:0.. = (No reset)
TCP:0. = (No SYN)
TCP:0 = (No FIN)
TCP: Window = 8682
TCP: Checksum = 55A2 (correct)
TCP: No TCP options
TCP: [1460 Bytes of data]
TCP:

----- Frame 14 -----
Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
14 [24.3.1.158] [XX.17.74] 1514 020:36:42.331 600.625.000 06/11/2000 12:13:34 PM Expert: Idle Too Long
DLC: Ethertype=0800, size=1514 bytes
IP: D=[XX.17.74] S=[24.3.1.158] LEN=1480 ID=22687
TCP: D=1167 S=6688 ACK=1483122034 SEQ=70072192 LEN=1460 WIN=8674

DLC: ---- DLC Header ----

DLC:
DLC: Frame 14 arrived at 12:13:34.4550; frame size is 1514 (05EA hex) bytes.
DLC: Destination = Station 0008C7FA808D
DLC: Source = Station 00605CF39D99
DLC: Ethertype = 0800 (IP)
DLC:

IP: ---- IP Header ----

IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 = normal delay
IP: 0.. = normal throughput
IP:0.. = normal reliability
IP: Total length = 1500 bytes
IP: Identification = 22687
IP: Flags = 4X
IP: .1. = don't fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 113 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = AEF1 (correct)
IP: Source address = [24.3.1.158]
IP: Destination address = [XX.17.74]
IP: No options
IP:

```

TCP: ---- TCP header ----
TCP:
TCP: Source port      = 6688
TCP: Destination port = 1167
TCP: Sequence number  = 70072192
TCP: Next expected Seq number= 70073652
TCP: Acknowledgment number = 1483122034
TCP: Data offset      = 20 bytes
TCP: Flags            = 10
TCP:   ..0. .... = (No urgent pointer)
TCP:   ...1 .... = Acknowledgment
TCP:   .... 0... = (No push)
TCP:   .... .0.. = (No reset)
TCP:   .... .0. = (No SYN)
TCP:   .... ..0 = (No FIN)
TCP: Window          = 8674
TCP: Checksum        = 6E3F (correct)
TCP: No TCP options
TCP: [1460 Bytes of data]
TCP:

```

```

----- Frame 15 -----
Frame Source Address  Dest. Address  Size Rel. Time  Delta Time  Abs. Time  Summary
15 [204.186.1.103] [XX.17.74] 1514 021:17:01.155 2418.824.000 06/11/2000 12:53:53 PM Expert: Idle Too Long
DLC: Ethertype=0800, size=1514 bytes
IP: D=[XX.17.74] S=[204.186.1.103] LEN=1480 ID=42250
TCP: D=1183 S=6699 ACK=1485934619 SEQ=34817412 LEN=1460 WIN=8662

```

```

DLC: ---- DLC Header ----
DLC:
DLC: Frame 15 arrived at 12:53:53.2790; frame size is 1514 (05EA hex) bytes.
DLC: Destination = Station 0008C7FA808D
DLC: Source      = Station 00605CF39D99
DLC: Ethertype   = 0800 (IP)
DLC:

```

```

IP: ---- IP Header ----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:   000. .... = routine
IP:   ...0 .... = normal delay
IP:   .... 0... = normal throughput
IP:   .... .0.. = normal reliability
IP: Total length = 1500 bytes
IP: Identification = 42250
IP: Flags        = 4X
IP:   .1. .... = don't fragment
IP:   .0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live   = 18 seconds/hops
IP: Protocol      = 6 (TCP)
IP: Header checksum = 0D06 (correct)
IP: Source address = [204.186.1.103]
IP: Destination address = [XX.17.74]
IP: No options
IP:

```

```

TCP: ---- TCP header ----
TCP:
TCP: Source port      = 6699
TCP: Destination port = 1183
TCP: Sequence number  = 34817412
TCP: Next expected Seq number= 34818872
TCP: Acknowledgment number = 1485934619
TCP: Data offset      = 20 bytes
TCP: Flags            = 10
TCP:   ..0. .... = (No urgent pointer)
TCP:   ...1 .... = Acknowledgment
TCP:   .... 0... = (No push)
TCP:   .... .0.. = (No reset)
TCP:   .... .0. = (No SYN)
TCP:   .... ..0 = (No FIN)
TCP: Window          = 8662
TCP: Checksum        = 8AA7 (correct)
TCP: No TCP options
TCP: [1460 Bytes of data]
TCP:

```

5.1 Source of trace:
-My network.

5.2 Detect was generated by:
-Black ICE Defender.

5.3 Probability the source address was spoofed:
-Low. This traffic pattern was fairly prevalent on the network during this period.

5.4 Description of attack:

-This detect is a FALSE POSITIVE. The pattern match was on the port 7777 being used by Napster during these exchanges.

5.5 Attack mechanism:

-Normal usage of Napster will cause this type of traffic to appear on the network. High port (>1023) to high port connections and data transfer will kick off an alert when those ports happen to fall on commonly used 'hacker' ports (12345, 31337, etc). In this case it was port 7777 that triggered the alert. See the correlation below.

5.6 Correlations:

bugtraq id 695

class Design Error

cve GENERIC-MAP-NOMATCH

remote Yes

local No

published October 05, 1999

updated April 11, 2000

vulnerable Hybrid Networks Cable Broadband Access System 1.0 on port 7777

5.7 Evidence of active targeting:

-No evidence of active targeting unless you consider running the Napster client making yourself an active target ☺.

5.8 Severity

-(critical + lethal) – (system + net countermeasures)

-(2 + 1) – (5 +4) = -6

5.9 Defensive recommendation:

-None. This alert was a false positive due to the nature of the Napster product.

5.10 Multiple-choice test question (based on trace and analysis with the answer)

The above is an example of:

- a) Trojan horse probe.
- b) Covert channel communications.
- c) Copyright infringement in action.
- d) None of the above

Answer: c (most likely...)

Detect 6

Frame	Source Address	Dest. Address	Size	Rel. Time	Delta Time	Abs. Time	Summary
1	[X.X.17.76]	[X.X.17.201]	136	000:00:00:00.000	0.000.000	04/30/2000 10:07:27 PM	DLC: Ethertype=0800, size=136 bytes IP: D=[X.X.17.201] S=[X.X.17.76] LEN=102 ID=12229 TCP: D=139 S=1039 ACK=364421168 SEQ=975604891 LEN=82 WIN=16436 NETB: Data, 78 bytes (of 78) CIFS/SMB: C Open AndX Name=PIPEwinreg

6.1 Source of trace:

-My network.

6.2 Detect was generated by:

-Black ICE Defender.

6.3 Probability the source address was spoofed:

-Low. Both source and destination addresses are located on the same network and are both valid hosts.

6.4 Description of attack:

-Attempt for a local machine to access the registry of a host server remotely across the network.

6.5 Attack mechanism:

-The attacker is using either REGEDIT or REGEDT32 to attempt to access a secure servers registry over the network.

6.6 Correlations:

-This appears to be an attempt to gain access to a server that is normally not available to this user. If the registry can be accessed successfully, then the intruder may alter system policies or gain access to resources not normally allowed to them. This is a common means of both remote administration and exploit on NT networks.\

6.7 Evidence of active targeting:

-This appears to be very active in the targeting. This particular host maintains sensitive data and has both user and IP based restrictions on its usage. The source IP is from a portion of the network not allowed access to this system. Internally to the organization this host is known as a restricted one.

6.8 Severity

-(critical + lethal) – (system + net countermeasures)

-(5 + 4) – (5 + 4) = 0

6.9 Defensive recommendation:

-Defenses are fine. However, due to the nature of the data on this server and the source of the attack (internal to the network). Further investigation into the incident is warranted.

6.10 Multiple-choice test question (based on trace and analysis with the answer)

The above user is trying to do the following:

- a) Log onto the NT domain
- b) Log into the NDS tree
- c) Retrieve a file from a server
- d) None of the above.

Answer: d

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 7

[**] ICQ Trojan [**]
06/11-21:06:32.250874 X.X.16.1:53 -> X.X.17.74:4950
UDP TTL:125 TOS:0x0 ID:14211
Len: 122

7.1 Source of trace:

-My network.

7.2 Detect was generated by:

-SNORT IDS on a Win32 system

7.3 Probability the source address was spoofed:

-Low. Valid ip address that also belongs to the same organization.

7.4 Description of attack:

Two:

- 1) A connection attempt to the ICQ Trojan backdoor program.
- 2) Response to a DNS query – false positive due to the destination port.

7.5 Attack mechanism:

-The intruder is making an attempt to connect to the port commonly associated with the ICQ Trojan program. This would be a reconnaissance type attack if it were true...

-The offending system is one of the organizations DNS systems and is apparently responding to a request for information.

7.6 Correlations:

-After looking further at the packet contents I determined that this is a DNS query response. Correlation to the Trojan program port was purely coincidental.

7.7 Evidence of active targeting:

-None. This is a false positive. Interesting to note however, the destination address was running ICQ...

7.8 Severity

-(critical + lethal) – (system + net countermeasures)

-(2 + 3) – (5 +4) = -4

7.9 Defensive recommendation:

-Defenses are fine. No actions needed.

7.10 Multiple-choice test question (based on trace and analysis with the answer)

The trace above is an example of:

- a) Normal ICQ traffic
- b) Normal DNS traffic
- c) Abnormal ICQ traffic
- d) Abnormal DNS traffic

Answer: b

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 8

[**] SMB Name Wildcard [**]
06/10-14:01:14.253220 X.X.16.3:137 -> X.X.17.74:137
UDP TTL:125 TOS:0x0 ID:14953
Len: 58

[**] SMB Name Wildcard [**]
06/10-14:01:15.762628 X.X.16.3:137 -> X.X.17.74:137
UDP TTL:125 TOS:0x0 ID:23401
Len: 58

[**] SMB Name Wildcard [**]
06/10-14:01:17.241156 X.X.16.3:137 -> X.X.17.74:137
UDP TTL:125 TOS:0x0 ID:24425
Len: 58

[**] SMB Name Wildcard [**]
06/11-13:42:27.879790 X.X.16.3:137 -> X.X.17.74:137
UDP TTL:125 TOS:0x0 ID:56218
Len: 58

[**] SMB Name Wildcard [**]
06/11-13:42:29.378994 X.X.16.3:137 -> X.X.17.74:137
UDP TTL:125 TOS:0x0 ID:64922
Len: 58

[**] SMB Name Wildcard [**]
06/11-13:42:30.879192 X.X.16.3:137 -> X.X.17.74:137
UDP TTL:125 TOS:0x0 ID:65178
Len: 58

8.1 Source of trace:

-My network.

8.2 Detect was generated by:

-SNORT IDS on a Win32 system

8.3 Probability the source address was spoofed:

-Low. Real address on internal organization IP block.

8.4 Description of attack:

-Multiple logon attempts from one system on the network to another. This is a possible intrusion. The attacker is making several attempts to connect to a local service from a remote local. Possible 'password grinding' attempt using different name / password combinations.

8.5 Attack mechanism:

-Net BIOS SMB client being used to attempt access to SMB share. Remote system will attempt to access a list of available share over a network then try attempt to connect to those share(s) using various name / password combinations.

8.6 Correlations:

-VERY common type attack leveled against Microsoft operating systems from Window 9x through NT. Based on Microsoft file and Print sharing services and the public's common mistake of using either weak or no passwords on those shares.

8.7 Evidence of active targeting:

-Host is actively being targeted. There are repeated attempts to access this system throughout the day, that cease in the evening and pick back up the next day.

8.8 Severity

-(critical + lethal) – (system + net countermeasures)
-(2 + 3) – (5 + 1) = -1

8.9 Defensive recommendation:

-Defenses are fine. Offending workstation should be visited to determine the actual nature of the access being attempted. This could be a possible mis-configuration.

8.10 Multiple-choice test question (based on trace and analysis with the answer)

The trace shows the following:

- a) Mis-configured WINS server
- b) File sharing access attempt
- c) Net BIOS scan attempt
- d) None of the above.

Answer: b

Detect 9

[**] WinGate 8010 Attempt [**]
06/12-11:11:10.771471 202.235.50.12:65535 -> X.X.17.73:8010
TCP TTL:237 TOS:0x0 ID:49706
S*** Seq: 0xC22A0000 Ack: 0x0 Win: 0x200

9.1 Source of trace:
-My Network.

9.2 Detect was generated by:
-SNORT IDS on a Win32 system

9.3 Probability the source address was spoofed:
-Low.

9.4 Description of attack:
-Some versions of Wingate have a web server on port 8010 for the "Log File Service". If this port is open, then anyone can connect to WinGate in order to read not only the log files, but any other file on the drive WinGate was installed on. BugTraq ID 507

9.5 Attack mechanism:
-Intruder uses a scanner configured to connect to this port and log any systems that have this port open. At a later time, the intruder returns to the system and attempts the exploit listed above. This particular piece is just the target-acquisition phase of the attack.

9.6 Correlations:
Bugtraq ID: 507
Class: Unknown
Cve: none
Remote: YES
Local: YES
Published: February 22,1999

9.7 Evidence of active targeting:
-No real evidence of actively targeting this host. Probably just a IP block sweep looking for exploitable hosts.

9.8 Severity
-(critical + lethal) – (system + net countermeasures)
-(2 + 3) – (5 + 3) = -3

9.9 Defensive recommendation:
-Defenses are fine. No actions required.

9.10 Multiple-choice test question (based on trace and analysis with the answer)

The trace shows the following;

- a) A compromised system access
- b) A port probe for exploitable service
- c) A false reading on DNS activity
- d) None of the above.

Answer: b

© SANS Institute 2000 - 2002, Author retains full rights.

Detect 10

[**] Source Port traffic [**]
06/09-12:38:12.683322 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:10311
Len: 109

[**] Source Port traffic [**]
06/09-12:43:12.693363 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:42573
Len: 109

[**] Source Port traffic [**]
06/09-12:48:12.706306 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:29524
Len: 109

[**] Source Port traffic [**]
06/09-12:53:12.750049 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:22106
Len: 109

[**] Source Port traffic [**]
06/09-12:58:12.741123 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:43616
Len: 109

[**] Source Port traffic [**]
06/09-13:08:12.742498 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:23660
Len: 109

[**] Source Port traffic [**]
06/09-13:23:12.753812 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:5502
Len: 109

[**] Source Port traffic [**]
06/09-13:38:12.765620 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:26255
Len: 109

[**] Source Port traffic [**]
06/09-13:53:12.780849 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:53665
Len: 109

[**] Source Port traffic [**]
06/09-14:08:12.793534 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:15028

Len: 109

[**] Source Port traffic [**]
06/09-14:23:12.803576 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:13000
Len: 109

[**] Source Port traffic [**]
06/09-14:38:12.814251 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:63451
Len: 109

[**] Source Port traffic [**]
06/09-14:53:12.838832 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:54510
Len: 109

[**] Source Port traffic [**]
06/09-15:08:12.846216 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:56834
Len: 109

[**] Source Port traffic [**]
06/09-15:23:12.909755 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:25365
Len: 109

[**] Source Port traffic [**]
06/09-15:38:12.866332 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:61224
Len: 109

[**] Source Port traffic [**]
06/09-15:53:12.873498 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:10042
Len: 109

[**] Source Port traffic [**]
06/09-16:00:03.849761 X.X.16.1:53 -> X.X.17.73:137
UDP TTL:125 TOS:0x0 ID:40003
Len: 105

10.1 Source of trace:
-My Network

10.2 Detect was generated by:
-SNORT IDS on a Win32 system

10.3 Probability the source address was spoofed:
-Low. System is a known DNS server on the network.

10.4. Description of attack:

-This alert was triggered due to the source address of the packets. This is a FALSE POSITIVE.

10.5 Attack mechanism:

-Windows servers use Net BIOS (as well as DNS) to resolve IP addresses to names using the "gethostbyaddr()" function. As users behind the firewalls surf Windows-based web sites, those servers will frequently respond with Net BIOS lookups.

10.6 Correlations:

-The DNS server is also a Windows NT server. This is a common behavior with Microsoft based operating systems.

10.7 Evidence of active targeting:

-There is no real evidence of active targeting in this trace. There does appear to be some sort of mis-configuration at the DNS server however. No other hosts on the network received such traffic from the DNS system.

10.8 Severity

-(critical + lethal) – (system + net countermeasures)
-(2 + 1) – (5 + 2) = -4

10.9 Defensive recommendation:

-Defenses are fine. There is no need to adjust systems as this appears to be a false alert. Note: This traffic stopped after an upgrade to the DNS system was applied. It is possible that there was a mis-configuration on the DNS that caused this activity to occur and make the DNS respond in this manner.

10.10 Multiple-choice test question (based on trace and analysis with the answer)

The trace shows the following:

- a) DNS zone transfer in progress
- b) Covert channel communications
- c) Net BIOS file transfer.
- d) None of the above.

Answer: d

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced