Global Information Assurance Certification Paper

GCIA Certification Practical

*** Northcutt, a neat twist are the detects that were created by ISS Security Scanner. Solid analysis process, you have to work to dig out some of the information, but some good stuff. 81 *

Stephen Zvacek

10 Detects with Analyses

April, 24, 2000

I&W Methodology used

Submitted as practical for SANS 2000 written exam (3/25/2000)

Severity calculated as follows;

(Critical + Lethal) - (System + Net Countermeasures) = Severity

Detect #1, DNS query

```
     1 M      [xxx.89.130.14]   [xxx.62.69.70]       78 0:00:00.000   0.000.000     04/10/2000 03:36:10 PM DNS: C
ID=54183 OP=QUERY NAME=raphost.os.xxx.com
     2        [xxx.62.69.70]    [xxx.89.130.14]     139 0:00:00.005   0.005.535     04/10/2000 03:36:10 PM DNS: R
ID=54183 STAT=Name error NAME=raphost.os.xxx.com
     3        [xxx.89.130.14]   [xxx.62.69.70]       75 0:00:00.008   0.003.274     04/10/2000 03:36:10 PM DNS: C
ID=61777 OP=QUERY NAME=raphost.xxx.com
     4        [xxx.62.69.70]    [xxx.89.130.14]     140 0:00:00.101   0.092.430     04/10/2000 03:36:10 PM DNS: R
ID=61777 STAT=Name error NAME=raphost.xxx.com
     5        [xxx.89.130.14]   [xxx.62.69.70]       67 0:00:00.104   0.003.333     04/10/2000 03:36:10 PM DNS: C
ID=48592 OP=QUERY NAME=raphost
     6        [xxx.62.69.70]    [xxx.89.130.14]     140 0:00:00.109   0.005.269     04/10/2000 03:36:10 PM DNS: R
ID=48592 STAT=Name error NAME=raphost
```

ANALYSIS

Evidence of Active Targeting?

No, This traffic was detected in our Intranet and does not appear to be hostile

Identify the Technique?

These are three pairs of DNS queries and responses. xxx.89.130.14 is making a QUERY NAME request to xxx..62.69.70. There is an error in the requesting as xxx.62.69.70 is returning “name error” responses. This query was from our internal DNS servers who are not allows to make queries outside our Intranet. NAME "raphost" was not in the DNS servers table.

Evidence of Intent?

There is no evidence of malicious intent in this trace.

Severity?

(5+1)-(3+4) = -1
Criticality - This machine is a DNS server
Lethality - There does not appear to be an attack
Countermeasures - Older Unix system with some patches missing
Net Countermeasures - Good firewall with some external connections

Detect #2, Get file

```
 1 M      [xxx.210.230.198] [xxx.89.130.193]     60 0:00:00.000   0.000.000     04/06/2000 10:05:31 AM TCP: D=80
S=1198 SYN SEQ=508304410 LEN=0 WIN=8192
     2        [xxx.89.130.193]  [xxx.210.230.198]    60 0:00:00.001   0.001.062     04/06/2000 10:05:31 AM TCP:
D=1198 S=80 SYN ACK=508304411 SEQ=3210260865 LEN=0 WIN=8760
     3        [xxx.210.230.198] [xxx.89.130.193]     60 0:00:00.063   0.062.786     04/06/2000 10:05:31 AM TCP: D=80
S=1198     ACK=3210260866 WIN=8760
     4        [xxx.210.230.198] [xxx.89.130.193]     83 0:00:00.065   0.001.531     04/06/2000 10:05:31 AM HTTP: C
Port=1198 GET /perl/files.pl HTTP/1.0
     5        [xxx.89.130.193]  [xxx.210.230.198]    60 0:00:00.066   0.001.198     04/06/2000 10:05:31 AM TCP:
D=1198 S=80     ACK=508304440 WIN=8760
     6        [xxx.210.230.198] [xxx.89.130.193]     60 0:00:00.123   0.056.584     04/06/2000 10:05:31 AM HTTP: C
Port=1198 HTML Data
     7        [xxx.89.130.193]  [xxx.210.230.198]   215 0:00:00.137   0.013.866     04/06/2000 10:05:31 AM HTTP: R
Port=1198 HTML Data
     8        [xxx.89.130.193]  [xxx.210.230.198]   261 0:00:00.137   0.000.498     04/06/2000 10:05:31 AM HTTP: R
Port=1198 HTML Data
     9        [xxx.89.130.193]  [xxx.210.230.198]    60 0:00:00.137   0.000.385     04/06/2000 10:05:31 AM TCP:
D=1198 S=80 FIN ACK=508304442 SEQ=3210261234 LEN=0 WIN=8760
    10        [xxx.210.230.198] [xxx.89.130.193]     60 0:00:00.191   0.053.966     04/06/2000 10:05:31 AM TCP: D=80
S=1198 FIN ACK=3210261027 SEQ=508304442 LEN=0 WIN=8599
    11        [xxx.89.130.193]  [xxx.210.230.198]    60 0:00:00.192   0.000.705     04/06/2000 10:05:31 AM TCP:
D=1198 S=80     ACK=508304443 WIN=8760
    12        [xxx.210.230.198] [xxx.89.130.193]     60 0:00:00.195   0.003.246     04/06/2000 10:05:31 AM TCP: D=80
S=1198 RST WIN=0
    13        [xxx.210.230.198] [xxx.89.130.193]     60 0:00:00.196   0.000.802     04/06/2000 10:05:31 AM TCP: D=80
S=1198 RST WIN=0
    14        [xxx.210.230.198] [xxx.89.130.193]     60 0:00:00.255   0.059.328     04/06/2000 10:05:31 AM TCP: D=80
S=1198 RST WIN=0
```

ANALYSIS

Evidence of Active Targeting? Yes. This appeared on our external Internet segment. This trace is one in a series of GET/POST actions initiated by this remote machine.
Identify the Technique? The remote machine has made a TCP connection with our webserver. It is attempting to retrieve (GET) the file "files.pl"from our webserver. Although the trace printout does lists packets 6 through 16 as HTML data, the server responded the file was not found. A problem in the 'files.pl' script distributed with the Novell WebServer Examples Toolkit v2 could allow a remote attacker to view the contents of any file or directory on vulnerable servers. The attacker would be limited to viewing files accessible to the user owning the server process. (This is from the ISS Security Scanner database on specific checks made by this program)
Evidence of Intent? There is clearly intent from this trace.
Identify Hostile Individuals and Groups It was later identified that we were being evaluated by our government contracting office. They tasked another contractor to evaluate the security of our external connections. It appeared from this and other traces they were using ISS Security scanner to perform the task.
Severity? (2+2)-(3+4) = -3 Criticality - This machine is a webserver Lethality - This could be a confidentiality issue Countermeasures - Older Unix system with some patches missing Net Countermeasures - Good firewall with some external connections

Detect #3, ICMP Echo

```
     4 PC9852            pc9854 74 0:00:15.673   0.993.022     04/17/2000 12:25:51 PM ICMP:
Echo
     5 pc9854.kcp.com    PC9852 74 0:00:15.673   0.000.296     04/17/2000 12:25:51 PM ICMP:
Echo reply
     6 PC9852            pc9854 74 0:00:16.673   0.999.822     04/17/2000 12:25:52 PM ICMP:
Echo
     7 pc9854.kcp.com    PC9852 74 0:00:16.673   0.000.290     04/17/2000 12:25:52 PM ICMP:
Echo reply
     8 PC9852            pc9854 74 0:00:17.673   0.999.881     04/17/2000 12:25:53 PM ICMP:
Echo
     9 pc9854.kcp.com    PC9852 74 0:00:17.673   0.000.264     04/17/2000 12:25:53 PM ICMP:
Echo reply
```

ANALYSIS

Evidence of Active Targeting?

No, This traffic was detected in our Intranet and does not appear to be hostile.

Identify the Technique?

This is a example of a standard ping done by pc9852 against pc9854. The echo and echo reply are paired together. They is approximately one second delay between echo requests from pc9852.

Evidence of Intent?

There is no evidence of malicious intent in this trace.

Severity?

(2+2)-(3+4) = -3
Criticality - These are internal workstations
Lethality - This could be a confidentiality issue
Countermeasures - Older system with some patches missing
Net Countermeasures - Good firewall with some external connections

Detect #4, POST file

```
     1 M      [xxx.210.230.198] [xxx.89.130.193]     60 0:00:00.000   0.000.000     04/06/2000 10:05:15 AM TCP: D=80
S=1181 SYN SEQ=508289247 LEN=0 WIN=8192
     2        [xxx.89.130.193]  [xxx.210.230.198]    60 0:00:00.001   0.001.321     04/06/2000 10:05:15 AM TCP:
D=1181 S=80 SYN ACK=508289248 SEQ=3208321885 LEN=0 WIN=8760
     3        [xxx.210.230.198] [xxx.89.130.193]     60 0:00:00.058   0.057.081     04/06/2000 10:05:16 AM TCP: D=80
S=1181     ACK=3208321886 WIN=8760
     4        [xxx.210.230.198] [xxx.89.130.193]    587 0:00:00.075   0.016.778     04/06/2000 10:05:16 AM HTTP: C
Port=1181 POST /msadc/msadcs.dll/RDSServer.DataFactory.Query HTTP/1.1
     5        [xxx.89.130.193]  [xxx.210.230.198]    60 0:00:00.076   0.001.254     04/06/2000 10:05:16 AM TCP:
D=1181 S=80     ACK=508289781 WIN=8760
     6        [xxx.89.130.193]  [xxx.210.230.198]   196 0:00:00.091   0.015.064     04/06/2000 10:05:16 AM HTTP: R
Port=1181 HTML Data
     7        [xxx.89.130.193]  [xxx.210.230.198]   261 0:00:00.092   0.000.536     04/06/2000 10:05:16 AM HTTP: R
Port=1181 HTML Data
     8        [xxx.210.230.198] [xxx.89.130.193]     60 0:00:00.153   0.061.690     04/06/2000 10:05:16 AM TCP: D=80
S=1181     ACK=3208322235 WIN=8411
     9        [xxx.210.230.198] [xxx.89.130.25]      60 0:00:07.438   7.284.563     04/06/2000 10:05:23 AM TCP: D=80
S=1171 FIN ACK=3207177883 SEQ=508280962 LEN=0 WIN=8760
    10        [xxx.89.130.25]   [xxx.210.230.198]    60 0:00:07.439   0.000.855     04/06/2000 10:05:23 AM TCP:
D=1171 S=80     ACK=508280963 WIN=8760
    11        [xxx.210.230.198] [xxx.89.130.193]     60 0:00:15.153   7.714.377     04/06/2000 10:05:31 AM TCP: D=80
S=1181 FIN ACK=3208322235 SEQ=508289781 LEN=0 WIN=8411
    12        [xxx.89.130.193]  [xxx.210.230.198]    60 0:00:15.154   0.000.726     04/06/2000 10:05:31 AM TCP:
D=1181 S=80     ACK=508289782 WIN=8760
    13        [xxx.89.130.193]  [xxx.210.230.198]    60 0:00:15.155   0.001.491     04/06/2000 10:05:31 AM TCP:
D=1181 S=80 FIN ACK=508289782 SEQ=3208322235 LEN=0 WIN=8760
```

ANALYSIS

Evidence of Active Targeting?

Yes. This appeared on our external webserver.

Identify the Technique?

The server xxx.210.230.198 has made a TCP connection and is attempting to POST the file msadcs.dll in the msadc directory on our webserver. Although the printout does not capture, the trace does show our webserver responded this file was not present.

Evidence of Intent?

This was determined to be a test conducted by ISS Security Scanner. This is part of a series of tests conducted by this machine as it runs tests against the target machine.

Severity?

(2+4)-(3+4) = -1
Criticality - This machine is a webserver
Lethality - This could be a DOS issue
Countermeasures - Older Unix system with some patches missing
Net Countermeasures - Good firewall with some external connections

Detect #5, Port Scan

```
    42        PC9852            POLEYN             132 0:01:40.356   0.247.088     04/17/2000 12:27:16 PM UDP: D=1
S=3584  LEN=98
    43        POLEYN            PC9852              70 0:01:40.356   0.000.267     04/17/2000 12:27:16 PM ICMP:
Destination unreachable (Port unreachable)
    44        PC9852            POLEYN              60 0:01:40.357   0.001.093     04/17/2000 12:27:16 PM TCP: D=2
S=3585 SYN SEQ=5114789 LEN=0 WIN=8192
    45        POLEYN            PC9852              60 0:01:40.357   0.000.132     04/17/2000 12:27:16 PM TCP:
D=3585 S=2 RST ACK=5114790 WIN=0
    46        PC9852            POLEYN             132 0:01:40.606   0.248.663     04/17/2000 12:27:16 PM UDP: D=2
S=3586  LEN=98
    47        POLEYN            PC9852              70 0:01:40.606   0.000.170     04/17/2000 12:27:16 PM ICMP:
Destination unreachable (Port unreachable)
    48        PC9852            POLEYN              60 0:01:40.607   0.001.065     04/17/2000 12:27:16 PM TCP: D=3
S=3587 SYN SEQ=5114800 LEN=0 WIN=8192
    49        POLEYN            PC9852              60 0:01:40.607   0.000.125     04/17/2000 12:27:16 PM TCP:
D=3587 S=3 RST ACK=5114801 WIN=0
    50        PC9852            POLEYN             132 0:01:40.856   0.248.517     04/17/2000 12:27:16 PM UDP: D=3
S=3588  LEN=98
    51        POLEYN            PC9852              70 0:01:40.856   0.000.145     04/17/2000 12:27:16 PM ICMP:
Destination unreachable (Port unreachable)
60        PC9852            POLEYN             60 0:01:41.357   0.001.043     04/17/2000 12:27:17 PM TCP: D=6
S=3593 SYN SEQ=5114835 LEN=0 WIN=8192
    61        POLEYN            PC9852              60 0:01:41.357   0.000.133     04/17/2000 12:27:17 PM TCP:
D=3593 S=6 RST ACK=5114836 WIN=0
    62        PC9852            POLEYN             132 0:01:41.606   0.248.621     04/17/2000 12:27:17 PM UDP: D=6
S=3594  LEN=98
    63        POLEYN            PC9852              70 0:01:41.606   0.000.156     04/17/2000 12:27:17 PM ICMP:
Destination unreachable (Port unreachable)
    64        PC9852            POLEYN              60 0:01:41.607   0.000.920     04/17/2000 12:27:17 PM TCP: D=7
S=3595 SYN SEQ=5114842 LEN=0 WIN=8192
    65        POLEYN            PC9852              60 0:01:41.607   0.000.124     04/17/2000 12:27:17 PM TCP:
D=3595 S=7 RST ACK=5114843 WIN=0
    66        PC9852            POLEYN             132 0:01:41.856   0.248.689     04/17/2000 12:27:17 PM UDP: D=7
S=3596  LEN=98
    67        POLEYN            PC9852              70 0:01:41.856   0.000.145     04/17/2000 12:27:17 PM ICMP:
Destination unreachable (Port unreachable)
    68        PC9852            POLEYN              60 0:01:41.857   0.001.039     04/17/2000 12:27:17 PM TCP: D=8
S=3597 SYN SEQ=5114852 LEN=0 WIN=8192
    69        POLEYN            PC9852              60 0:01:41.857   0.000.122     04/17/2000 12:27:17 PM TCP:
D=3597 S=8 RST ACK=5114853 WIN=0
    70        PC9852            POLEYN             132 0:01:42.106   0.249.006     04/17/2000 12:27:18 PM UDP: D=8
S=3598  LEN=98
    71        POLEYN            PC9852              70 0:01:42.106   0.000.146     04/17/2000 12:27:18 PM ICMP:
Destination unreachable (Port unreachable)
```

ANALYSIS
Evidence of Active Targeting? Yes, this scan is obviously a port scan from pc9852.
Identify the Technique? PC9852 has initiated a port scan of POLEYN. This scan is both a TCP and UDP scan with the port incrementing starting at port on. POLEYN responds with a "port unreachable" for the UDP scan. For the TCP scan, pc9852 sends a SYN packet and POLEYN responds with the a RST/ACK. Each port, starting with port 1 is incremented by one with both a TCP and UDP request. The source port is also incrementing by one each time.
Evidence of Intent? Intent is clearly a port scan. This trace when on through port 1024 for both TCP and UDP.
Severity? (2+2)-(3+4) = -3 Criticality - These machines are internal workstations Lethality - This could be a confidentiality issue Countermeasures - Older system with service packs installed but some patches missing Net Countermeasures - Good firewall with some external connections

Detect #6, SMTP data

```
     1 M      [xxx.210.230.198] [xxx.89.130.30]      60 0:00:00.000   0.000.000     04/06/2000 10:06:27 AM SMTP: C
PORT=25   Text Data
     2        [xxx.89.130.30]   [xxx.210.230.198]    71 0:00:00.000   0.000.750     04/06/2000 10:06:27 AM SMTP: R
PORT=25   250 Reset state
     3        [xxx.210.230.198] [xxx.89.130.30]      60 0:00:00.050   0.049.977     04/06/2000 10:06:28 AM SMTP: C
PORT=25   HELO
     4        [xxx.89.130.30]   [xxx.210.230.198]    60 0:00:00.147   0.096.715     04/06/2000 10:06:28 AM TCP:
D=4398 S=25     ACK=507691543 WIN=61440
     5        [xxx.210.230.198] [xxx.89.130.30]      60 0:00:00.205   0.057.967     04/06/2000 10:06:28 AM SMTP: C
PORT=25   Text Data
     6        [xxx.89.130.30]   [xxx.210.230.198]    88 0:00:01.198   0.992.779     04/06/2000 10:06:29 AM SMTP: R
PORT=25   501 HELO requires domain address
     7        [xxx.210.230.198] [xxx.89.130.30]      60 0:00:01.250   0.052.504     04/06/2000 10:06:29 AM SMTP: C
PORT=25   VRFY :
     8        [xxx.210.230.198] [xxx.89.130.30]      60 0:00:01.395   0.144.711     04/06/2000 10:06:29 AM SMTP: C
PORT=25   Text Data
     9        [xxx.89.130.30]   [xxx.210.230.198]    82 0:00:01.412   0.017.060     04/06/2000 10:06:29 AM SMTP: R
PORT=25   250 <xxxx@xxx.com>
    10        [xxx.210.230.198] [xxx.89.130.xxx]     60 0:00:01.432   0.019.921     04/06/2000 10:06:29 AM SMTP: C
PORT=25   RSET
```

ANALYSIS

Evidence of Active Targeting?

No, This traffic was detected in our Intranet and does not appear to be hostile

Identify the Technique?

This is a segment of SMTP traffic which a VERIFY function is taking place. xxx.210.230.198 is making a request to xxx.89.130.30 for verification of a mail address (xxx@xxx.com). Packet #3 is a HELO request from xxx.210.230.198 to xxx.89.130.30 which .130.30 sends and ACK. However, a properly formed HELO request must be accompanied by a FQDN. xxx.210.230.198 then requests a VRFY, which is a request to verify a mail address without actually sending mail to the address. Packet #8 represents the response that was not fully captured by the trace. Packet #10 is a RESET from xxx.210.230.198 which aborts both ends of transaction. All data about the sequence is lost.

Evidence of Intent?

There is no evidence of malicious intent in this trace.

Severity?

(4+1)-(3+4) = -2
Criticality - This machine is a e-mail server
Lethality - This attack is unlikely to succeed.
Countermeasures - Older Unix system with some patches missing
Net Countermeasures - Good firewall with some external connections

Detect #7, Scan for Webservers

20:38:47.050283 aaa.bbb.com.57932 > 11.0.0.255.80: . ack 0 win 1024
20:38:47.050291 aaa.bbb.com.57932 > 11.0.1.255.80: . ack 0 win 1024
20:38:47.052772 aaa.bbb.com.57932 > 11.0.2.255.80: . ack 0 win 1024
20:38:47.053498 aaa.bbb.com.57932 > 11.0.3.255.80: . ack 0 win 1024
20:38:47.053833 aaa.bbb.com.57932 > 11.0.4.255.80: . ack 0 win 1024
20:38:47.055802 aaa.bbb.com.57932 > 11.0.5.255.80: . ack 0 win 1024
20:38:47.057831 aaa.bbb.com.57932 > 11.0.6.255.80: . ack 0 win 1024
20:38:47.057846 aaa.bbb.com.57932 > 11.0.7.255.80: . ack 0 win 1024
20:38:47.079566 aaa.bbb.com.57932 > 11.0.9.255.80: . ack 0 win 1024
20:38:47.080023 aaa.bbb.com.57932 > 11.0.12.255.80: . ack 0 win 1024
20:38:47.080612 aaa.bbb.com.57932 > 11.0.13.255.80: . ack 0 win 1024
20:38:47.080619 aaa.bbb.com.57932 > 11.0.10.255.80: . ack 0 win 1024
20:38:47.082266 aaa.bbb.com.57932 > 11.0.8.255.80: . ack 0 win 1024
20:38:47.097504 aaa.bbb.com.57932 > 11.0.14.255.80: . ack 0 win 1024

ANALYSIS

Evidence of Active Targeting?

Yes

Identify the Technique?

Facts about this scan;

1. The timestamps are very close together. Might indicate this was a scripted operation.
2. The same port is being used from the source address; 57932 which is not impossible, but somewhat unusual.
3. The destination addresses are broadcast addresses on port. The attacker could be looking for webservers on these subnets.
4. There is no SYN packets. ACK packets, under normal conditions, must have a corresponding SYN packet. Without this combination, there is no TCP connection.
5. The sequence number is zero. Under normal conditions, ACK packets cannot have a sequence number of 0. A SYN packet always consumes one sequence number, so the ACK could not be zero.
6. Zero ACK sequence numbers are a indication of an NMAP scan. Ramdon sequence numbers have been introduced in version 2.3BETA9

Evidence of Intent?

This a scan trying to locate webservers by using the ACK packets. A RESET response would be returned .

Severity?

(2+1)-(3+4) = -4
Criticality - This machine is a webserver
Lethality - This attack is unlikely to succeed
Countermeasures - Older Unix system with some patches missing
Net Countermeasures - Good firewall with some external connections

Detect #8

```
     1 M      [xxx.210.230.198] [xxx.89.130.30]      90 0:00:00.000   0.000.000     04/06/2000 10:06:29 AM HTTP: C
Port=1293 GET /IISADMPWD/aexp.htr HTTP/1.0
     2        [xxx.89.130.30]   [xxx.210.230.198]    78 0:00:00.011   0.011.147     04/06/2000 10:06:29 AM HTTP: R
Port=1293 HTML Data
     3        [xxx.89.130.30]   [xxx.210.230.198]    91 0:00:00.011   0.000.399     04/06/2000 10:06:29 AM HTTP: R
Port=1293 HTML Data
     4        [xxx.89.130.30]   [xxx.210.230.198]    74 0:00:00.011   0.000.093     04/06/2000 10:06:29 AM HTTP: R
Port=1293 HTML Data
     5        [xxx.89.130.30]   [xxx.210.230.198]    79 0:00:00.011   0.000.143     04/06/2000 10:06:29 AM HTTP: R
Port=1293 HTML Data
     6        [xxx.89.130.30]   [xxx.210.230.198]    60 0:00:00.011   0.000.059     04/06/2000 10:06:29 AM HTTP: R
Port=1293 HTML Data
     7        [xxx.89.130.30]   [xxx.210.230.198]    96 0:00:00.012   0.000.208     04/06/2000 10:06:29 AM HTTP: R
Port=1293 HTML Data
     8        [xxx.89.130.30]   [xxx.210.230.198]    83 0:00:00.012   0.000.100     04/06/2000 10:06:29 AM HTTP: R
Port=1293 HTML Data
     9        [xxx.89.130.30]   [xxx.210.230.198]   122 0:00:00.012   0.000.144     04/06/2000 10:06:29 AM HTTP: R
Port=1293 HTML Data
    10        [xxx.89.130.30]   [xxx.210.230.198]    62 0:00:00.012   0.000.061     04/06/2000 10:06:29 AM HTTP: R
Port=1293 HTML Data
    11        [xxx.89.130.30]   [xxx.210.230.198]    60 0:00:00.012   0.000.554     04/06/2000 10:06:29 AM TCP:
D=1293 S=80 FIN ACK=508363034 SEQ=380480256 LEN=0 WIN=61440
    12        [xxx.89.130.xxx]  [xxx.210.230.198]    60 0:00:00.053   0.040.562     04/06/2000 10:06:29 AM TCP:
D=4401 S=25     ACK=507692560 WIN=49152
    13        [xxx.89.130.200]  [xxx.210.230.198]    60 0:00:00.053   0.000.031     04/06/2000 10:06:29 AM TCP:
D=1292 S=80     ACK=508362843 WIN=49152
    14        [xxx.210.230.198] [xxx.89.130.30]      60 0:00:00.062   0.009.168     04/06/2000 10:06:29 AM HTTP: C
Port=1293 HTML Data
    15        [xxx.89.130.30]   [xxx.210.230.198]    60 0:00:00.062   0.000.219     04/06/2000 10:06:29 AM TCP:
D=1293 S=80 RST WIN=0
    16        [xxx.210.230.198] [xxx.89.130.30]      60 0:00:00.064   0.001.319     04/06/2000 10:06:29 AM TCP: D=80
S=1293 FIN ACK=380480025 SEQ=508363036 LEN=0 WIN=8168
    17        [xxx.89.130.30]   [xxx.210.230.198]    60 0:00:00.064   0.000.174     04/06/2000 10:06:29 AM TCP:
D=1293 S=80 RST WIN=61440
    18        [xxx.210.230.198] [xxx.89.130.30]      60 0:00:00.066   0.002.378     04/06/2000 10:06:29 AM TCP: D=80
S=1294 SYN SEQ=508362973 LEN=0 WIN=8192
    19        [xxx.89.130.30]   [xxx.210.230.198]    60 0:00:00.066   0.000.238     04/06/2000 10:06:29 AM TCP:
D=1294 S=80 SYN ACK=508362974 SEQ=380608000 LEN=0 WIN=61440
    20        [xxx.210.230.198] [xxx.89.130.30]      60 0:00:00.068   0.001.904     04/06/2000 10:06:29 AM TCP: D=80
S=1293 RST WIN=0
```

ANALYSIS
Evidence of Active Targeting? Yes, This traffic was detected in our Intranet probing out webserver
Identify the Technique? xxx.210.230.198 had been making several probes to this machine all morning. This trace is one part of a very long sequence. It is attempting to get the fine "aexp.htr" from the IISADMPWD directory. The following is a taken from the X-Force database from www.iss.net. Internet Information Server 4.0 introduces the ability for remote web users to administer their passwords on the server machine and on other machines connected to the same network. This functionality is implemented through the /IISADMPWD/ virtual directory and various .HTR files.
Evidence of Intent? xxx.210.230.198 was attempting to determine if this file was present on our webserver.
Severity? (2+5)-(3+4) = 0 Criticality - This machine is a webserver Lethality - If successful, could lead to root access Countermeasures - Older Unix system with some patches missing Net Countermeasures - Good firewall with some external connections

Detect #9, Smurf attack

18:11:27.604944 attacker.COM > 10.0.1.0: icmp: echo request
18:11:27.604947 attacker.COM > 10.0.2.0: icmp: echo request
18:11:27.604962 attacker.COM > 10.0.1.255: icmp: echo request
18:11:27.604965 attacker.COM > 10.0.0.255: icmp: echo request
18:11:27.605924 attacker.COM > 10.0.2.255: icmp: echo request
18:11:27.619118 attacker.COM > 10.0.3.255: icmp: echo request
18:11:27.629025 attacker.COM > 10.0.3.0: icmp: echo request
18:11:27.633366 attacker.COM > 10.0.4.0: icmp: echo request
18:11:27.635618 attacker.COM > 10.0.4.255: icmp: echo request

ANALYSIS

Evidence of Active Targeting?

Yes

Identify the Technique?

This appears to be the classic Smurf attack. Several items indicated this possibility.

1. The time stamps for each packet. These packets are arriving very fast with time between each packet. These must be script generated.
2. The attacker is stepping through subnets starting with subnet "0". There may be some attempt at randomness as exhibited by 10.0.0.255 arriving after 10.0.1.255.
3. Both .0 and .255 broadcasts are used. Some implementations us .0 as a broadcast.
4. The protocol is ICMP

Evidence of Intent?

This is either a network map operation or if the destination address is spoofed, a DOS attack against attacker.com. One indication this may be a DOS attack is the speed in which the packets are being sent. If network mapping was the goal, more time would be allowed for responses.

Severity?

(2+4)-(3+4) = -1
Criticality - This machine is a workstation
Lethality - This could result in a DOS
Countermeasures - Older Unix system with some patches missing
Net Countermeasures - Good firewall with some external connections

Detect #10, Port Scanning
08:56:46.330769 aaa.bbb.com.13356 > 10.0.68.19.111: S 2105675008:2105675008 (0) win 512 08:56:46.330929 aaa.bbb.com.13329 > 10.0.68.10.111: S 1283255785:1283255785 (0) win 512 08:56:46.331419 aaa.bbb.com.13376 > 10.0.68.21.111: S 1093368475:1093368475 (0) win 512 08:56:46.331747 aaa.bbb.com.13051 > 10.0.68.1.111: S 3429678225:3429678225 (0) win 512 08:56:46.332607 aaa.bbb.com.13332 > 10.0.68.13.111: S 4149824266:4149824266 (0) win 512 08:56:46.333058 aaa.bbb.com.13378 > 10.0.68.23.111: S 3619956806:3619956806 (0) win 512 08:56:46.333222 aaa.bbb.com.13379 > 10.0.68.24.111: S 21823303:21823303 (0) win 512 08:56:46.333386 aaa.bbb.com.13190 > 10.0.68.5.111: S 2733884631:2733884631 (0) win 512
ANALYSIS
Evidence of Active Targeting? Yes
Identify the Technique? The following are items of interest for the analyst. 1. The timestamps indicate a very fast scan. 2. The ports for the attacking host are random but within a defined range in the 13000 range 3. The attacker is working through the 10.0.68 subnet looking for machines that will respond to the SYN packet. 4. The attacking machine is interested in port 111, portmapper.
Evidence of Intent? Port 111 is the Unix implementation of the Portmapper service. The remote-procedure call (RPC) *portmapper* program dynamically assignes the TCP and UDP ports for RPC services. It provides useful information to attackers by clearly reporting all RPC-based services that are available on the hosts. There are several know vulnerabilities associated with the RPC services that could be exploited by discovering a listening 111 port.
Severity? (2+5)-(3+4) = 0 Criticality - This machine is a Unix desktop system Lethality - This could lead to root access Countermeasures - Older Unix system with some patches missing Net Countermeasures - Good firewall with some external connections