GIAC CERTIFICATIONS

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 permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

Glen F. Sharlun
Intrusion Detection Curriculum Practical Assignment
San Jose, CA 2000

1. SUB SEVEN SCAN, SERVER LOCATED(+ ? traffic), AND CONNECTED

```
Time             Delta Time   Srce IP        Srce Port    Dest IP     Dest Port      Size      Protocol
        Seq #, Ack #, Window size
SCAN
08:30:51.406308  00.000112    SUB7.MASTER  IP-2416 SCANNED1.SUB7        IP-27374          62       IP TCP
        S=    72264,L=    0,A=        0,W= 8192
08:30:51.406588  00.000280    SCANNED1.SUB7   IP-27374  SUB7.MASTER     IP-2416           64       IP TCP
        S=        0,L=    0,A=    72265,W=    0
….
CONNECT
08:30:51.425574  00.000935    SUB7.MASTER  IP-2421 SUB7.VICTIM   IP-27374          62       IP TCP
        S=    72305,L=    0,A=        0,W= 8192
08:30:51.425814  00.000240    SUB7.VICTIM  IP-27374          SUB7.MASTER IP-2421   64       IP TCP
        S= 752487162,L=    0,A=    72306,W= 8760
08:30:51.425967  00.000153    SUB7.MASTER  IP-2421 SUB7.VICTIM   IP-27374          58       IP TCP
        S=    72306,L=    0,A= 752487163,W= 8760
08:30:51.427497  00.001530    SUB7.VICTIM  IP-27374          SUB7.MASTER IP-2421   134      IP TCP
        S= 752487163,L=   76,A=    72306,W= 8760
08:30:51.538783  00.111286    SUB7.MASTER  IP-2421 SUB7.VICTIM   IP-27374          58       IP TCP
        S=    72306,L=    0,A= 752487239,W= 8684
RETURN TO SCAN
08:30:51.839278  00.300495    SUB7.MASTER  IP-2420 SCANNED3.SUB7        IP-27374          62       IP TCP
        S=    72293,L=    0,A=        0,W= 8192
08:30:51.839440  00.000162    SUB7.MASTER  IP-2419 SCANNED2.SUB7        IP-27374          62       IP TCP
        S=    72282,L=    0,A=        0,W= 8192
08:30:51.839506  00.000066    SUB7.MASTER  IP-2416 SCANNED1.SUB7        IP-27374          62       IP TCP
        S=    72264,L=    0,A=        0,W= 8192
08:30:51.839570  00.000064    SCANNED3.SUB7        IP-27374     SUB7.MASTER     IP-2420   64       IP TCP
        S=        0,L=    0,A=    72294,W=    0
08:30:51.839649  00.000079    SCANNED1.SUB7     IP-27374  SUB7.MASTER     IP-2416           64       IP TCP
        S=        0,L=    0,A=    72265,W=    0
08:30:51.839710  00.000061    SCANNED2.SUB7     IP-27374     SUB7.MASTER IP-2419           64       IP TCP
        S=        0,L=    0,A=    72283,W=    0
08:30:52.340048  00.500338    SUB7.MASTER  IP-2420 SCANNED3.SUB7        IP-27374          62       IP TCP
        S=    72293,L=    0,A=        0,W= 8192
08:30:52.340184  00.000136    SUB7.MASTER  IP-2419 SCANNED2.SUB7        IP-27374          62       IP TCP
        S=    72282,L=    0,A=        0,W= 8192
08:30:52.340254  00.000070    SUB7.MASTER  IP-2416 SCANNED1.SUB7        IP-27374          62       IP TCP
        S=    72264,L=    0,A=        0,W= 8192
08:30:52.340319  00.000065    SCANNED3.SUB7        IP-27374     SUB7.MASTER     IP-2420   64       IP TCP
        S=        0,L=    0,A=    72294,W=    0
08:30:52.340385  00.000066    SCANNED1.SUB7        IP-27374          SUB7.MASTER  IP-2416 64       IP TCP
        S=        0,L=    0,A=    72265,W=    0
08:30:52.340448  00.000063    SCANNED2.SUB7        IP-27374          SUB7.MASTER  IP-2419 64       IP TCP
        S=        0,L=    0,A=    72283,W=    0
08:30:52.718509  00.378061    SUB7.MASTER          IP-2421 SUB7.VICTIM     IP-27374          58       IP TCP
        S=    72306,L=    0,A= 752487239,W= 8684
08:30:52.718654  00.000145    SUB7.VICTIM          IP-27374          SUB7.MASTER  IP-2421 64       IP TCP
        S= 752487239,L=    0,A=    72307,W= 8760
08:30:52.720091  00.001437    SUB7.VICTIM          IP-27374          SUB7.MASTER  IP-2421 64       IP TCP
        S= 752487239,L=    0,A=    72307,W= 8760
```

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

© SANS Institute 2000 - 2002   As part of GIAC practical repository.   Author retains full rights.

```
08:30:52.720285   00.000194        SUB7.MASTER            IP-2421  SUB7.VICTIM    IP-27374            58         IP TCP
          S=    72307,L=    0,A= 752487240,W= 8684
????????
…    200 ARP REQUESTS FROM THE "MASTER" FOLLOWED BY 1 ARP RESPONSE FROM HERE.I.AM, THEN…

08:30:54.821725   02.101440        SUB7.MASTER            IP-2610  HERE.I.AM          IP-27374        62         IP TCP
          S=    73541,L=    0,A=        0,W= 8192
CONNECT
08:31:07.738280   12.916555        SUB7.MASTER  IP-2665  SUB7.VICTIM    IP-27374            62         IP TCP
          S=    73863,L=    0,A=        0,W= 8192
08:31:07.738463   00.000183        SUB7.VICTIM    IP-27374            SUB7.MASTER  IP-2665  64         IP TCP
          S= 752503477,L=    0,A=    73864,W= 8760
08:31:07.738624   00.000161        SUB7.MASTER  IP-2665  SUB7.VICTIM    IP-27374            58         IP TCP
          S=    73864,L=    0,A= 752503478,W= 8760
08:31:07.740106   00.001482        SUB7.VICTIM    IP-27374            SUB7.MASTER  IP-2665  134        IP TCP
          S= 752503478,L=   76,A=    73864,W= 8760
08:31:07.862265   00.122159        SUB7.MASTER  IP-2665  SUB7.VICTIM    IP-27374            58         IP TCP
          S=    73864,L=    0,A= 752503554,W= 8684
```

1. Source of trace:
    a. This trace was collected on a lab network.

2. Detect was generated by:
    a. It was collected with Etherpeek and saved into .txt format.

3. Probability the source address was spoofed:
    a. In this case I know that the address is not spoofed, but Sub 7 does have a GUI means of using a "victims" (Sub7 server running) computer to scan for more victims.

4. Description of attack:
    a. In this lab case I simply downloaded Sub7, created/edited the server with default setting (most notably the port #), saved the server to a disk, physically executed the server on the victim's machine and then just scanned for it from the client.

5. Attack mechanism
    a. The Sub7 client scans the range of addresses (IP or ICQ #'s) that are set by the user and with the results of the scan, allows the user to connect to any systems that responded to the scan
    b. The significance of this Trojan horse is that there is very little that you cannot do once you are connected, and that it is currently the most popular Trojan that I am scanned for. The author has taken great steps to make this Trojan very easy to use and very functional (lethal) as well as taking steps to change the signature of the server in an effort to stay ahead of the anti-virus companies.

6. Correlations:
    a. This is a very common Trojan horse scan. Around the new year (2000) Sub7 became the most popular Trojan to be scanned for. Remote scanning ability is a large part of that popularity.

7. Evidence of active targeting:

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

a. The first section of the trace (deleted all after the first host scanned) are just the client (Master) scanning for active servers (victims) on the default port 27374, and would not indicate any active targeting.
b. The second section is what you never what to see; the scanning client (Master), finding an active server (Victim)
c. The third section is the master returning to scan the addresses that were previously scanned (and that I cut out for space from the 1st section).
d. The fourth section has a time gap of 2 seconds where almost 200 ARP requests went out from the Master, with one ARP response from HERE.I.AM. Followed immediately with the scan of HERE.I.AM. I believe that HERE.I.AM is a router.
e. Finally, the last section is the client (Master) connecting to the server (Victim); definitely don't want to ever see this.
f. Honestly, there is more traffic here than is necessary for the job. I wouldn't run this test on your home system.

8. Severity: = (Criticality + lethality) - (System + Net Countermeasures)
   a. Criticality – 3; No specific machines were targeted
   b. Lethality – 5; Extremely lethal to a Win 95/98 machine, if exploited
   c. System – 3; Server executed on Win98 box; Server will not work on patched NT; client will
   d. Countermeasures – 1; Lab had no defenses for this (air-gapped for testing/security)
   e. Severity = 8 – 4 = 4

9. Defensive recommendations:
   a. Educating users on security (physical and executing attachments) is the first line of defense against Trojans. Screening for the default port 27374 at the firewall will keep the real Kiddies out (port is easily changed though). Monitor traffic leaving your system in response to a scan.

10. Multiple choice test question:
    a. Is there anything to be concerned about the second section of trace above?
       i. No, this is simply a standard TCP connection
       ii. Not really, this is a simple scan
       iii. Yes, assume that Victim is completely compromised and respond accordingly.
       iv. Be careful, this is a scan of a popular Trojan, but no emergency yet.

    Ans: iii

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

2. SOCKS SCAN

```
Date           Time               Delta Time      Srce IP               Srce Port
Dest IP            Dest Port        Size     Protocol      Seq #, Ack #, Window size

06/07/2000    18:41:50.143000                    IP-208.25.49.212      IP-1299        IP-
Sensor1.DSL   IP-1080         66    IP TCP       S=2605484196,L=    0,A=        0,W= 8760
06/07/2000    18:41:53.728000     03.585000      IP-208.25.49.212      IP-1299        IP-
Sensor1.DSL   IP-1080         66    IP TCP       S=2605484196,L=    0,A=        0,W= 8760
06/07/2000    18:41:53.754000     00.026000      IP-208.25.49.212      IP-1299        IP-
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Sensor1.DSL  IP-1080      66      IP TCP       S=2605484196,L=   0,A=       0,W= 8760
06/07/2000   18:41:53.754000      00.000000    IP-208.25.49.212    IP-1299       IP-
Sensor1.DSL  IP-1080      66      IP TCP       S=2605484196,L=   0,A=       0,W= 8760


06/07/2000   18:44:30.725000                   IP-208.25.49.212    IP-1408       IP-
Sensor2.DSL  IP-1080      66      IP TCP       S=2621329189,L=   0,A=       0,W= 8760
```

1. Source of trace:
    a. This was collected by two DSL connection, within the same providers address space.

2. Detect was generated by:
    a. BlackIce Defender and then analyzed with Etherpeek. Output is .txt format from Etherpeek.

3. Probability the source address was spoofed:
    a. Unlikely, though the SOCKS scan is generally looking for sites that they can bounce through, to hide their identity.

4. Description of attack:
    a. This is a scan for port 1080, the SOCKS port.

5. Attack mechanism:
    a. The scan is looking to establish a three-way-handshake, or at least get a Syn-Ack back so that it knows that port 1080 is open.
    b. WinGate is the most common application to have this vulnerability. It allows multiple systems to access the Internet from one IP address, but is not picky about allowing outside addresses in.
    c. The significance of this scan is that the SOCKS port and the application running on it are common bounce sites, and must be configured carefully.

6. Correlations:
    a. This scan was seen from two different sensors, within a few minutes of each other. It is likely that this is a large "search" for systems to use as a launching point for other attacks.
    b. IRC Chat Servers do scan for the SOCKS port open so that they can kick those people off of their service.

7. Evidence of active targeting:
    a. This looks like a general scan of the network.
        i. Though I was trace routed from this Sprint network space the following day; that was probably a wrong number; but still…

8. Severity: = (Criticality + lethality) - (System + Net Countermeasures)
    a. Criticality – 3; No specific machines were targeted
    b. Lethality – 3; Could be used as a launching site for hacking/cracking
    c. System – 4; Win98 box with updated patches
    d. Countermeasures – 5; Firewall/IDS and port 1080 is not used.
    e. Severity = 6 – 9 = -3

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

9. Defensive recommendations:
    a. None now.

10. Multiple choice test question:
    a. What is the vulnerability if this system responds to this scan?
        i. Possible Trojan horse.
        ii. There is no known vulnerability associated with this scan
        iii. System could be used as a bounce site for attackers
        iv. This is a simple host scan.

    Ans: iii

3. TCP OS FINGERPRINT SCAN

```
Date            Time                Srce IP             Srce Port  Dest IP            Dest Port
Size     Protocol     Seq #, Ack #, Window size

06/07/2000   08:39:22.524000     IP-24.1.104.76      IP-53   SENSOR3.DSL        IP-53
        64      TCP DNS     S=1249258219,L=    0,A=2125068537,W= 1028

06/07/2000   08:43:13.891000     IP-24.1.104.76      IP-53   SENSOR2.DSL                 IP-53
        64      TCP DNS     S= 893990728,L=    0,A=  28437962,W= 1028
```

1. Source of trace:
    a. This was collected on two DSL connections, within the same providers address space.

2. Detect was generated by:
    b. BlackIce Defender and then analyzed with Etherpeek. Output is .txt format from Etherpeek.

3. Probability the source address was spoofed:
    a. Unlikely that the address is spoofed

4. Description of attack:
    a. This scan is solely designed to get the host system to respond to an unusual packet. This response is then compared with a known database of responses to determine the OS and version that the host is running.
    b. Though I cannot show it in these traces, the Fin flag is set in both of these packets.
    c. This scan is looking for a DNS (port 53).

5. Attack mechanism:
    a. RFC 793 states that when an open port is hit with a Fin packet, there should be no response. There are OS/versions that will send back a Reset (i.e. MS win); this is what the sender of this scan is looking for.
    b. The significance of this is that if the attacker knows what OS/version the target system is, he can be much smarter on what tools/techniques he uses to exploit it.
    c. The fact that the target is a DNS (system listening on port 53) makes this a significant scan.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

6. Correlations:
    a. This is not a unique scan. Most systems that do OS fingerprinting will send Fin packets as one of the means of determining the OS.
    b. Though Nmap is far from the only OS fingerprinting scanner on the market (this scan is definitely not Nmap; too few packets) it has become the "Swiss Army Knife" of the scanning world due to its speed, stealth, and strong OS fingerprinting capabilities.

7. Evidence of active targeting:
    a. Again, this is likely a large-scale scan due to the fact that two different sensors picked it up within a few minutes of each other.

8. Severity: = (Criticality + lethality) - (System + Net Countermeasures)
    a. Criticality – 5; DNS targeted
    b. Lethality – 1; No DNS here
    c. System – 4; Win98 box with updated patches
    d. Countermeasures – 5; Firewall/IDS and port 1080 is not used.
    e. Severity = 6 – 9 = -3

9. Defensive recommendations:
    a. None at this time because I do not have a DNS running at this site. If there was a DNS running at this site, I would like to see how it would respond to a Fin scan.

10. Multiple choice test question:
    a. Is there any reason to be concerned about the above trace (Fin flags are set in both traces)?
        i. No, just the average scans
        ii. Yes, scan for OS fingerprinting of DNSs
        iii. Yes, buffer overflow attempt
        iv. No, mis-configured router trace

    Ans: ii

4. UDP TROJAN HORSE SCAN (HACK'A'TACK)

```
Date            Time                Srce IP          Srce Port      Dest IP             Dest Port
Size            Protocol

05/12/2000    22:21:22.756000  IP-200.53.160.182  IP-31790      CONNECTED.DSL   IP-31789
       64     IP UDP
```

1. Source of trace:
    a. This was collected on a DSL connection.

2. Detect was generated by:
    a. BlackIce Defender and then analyzed with Etherpeek. Output is .txt format from Etherpeek.

3. Probability the source address was spoofed:

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

   a. Unlikely that the address is spoofed, but the scanner may be bouncing through another system in order to stay anonymous.

4. Description of attack:
   a. Based on the UDP port number (Default for Hack'A'Tack Trojan), this is most likely the Hack'A'Tack client scanning for active Hack'A'Tack servers.
   b. Hack'A'Tack uses the following default scanning protocols/ports: TCP ports 31785, 31787 and UDP ports 31789, 31791

5. Attack mechanism:
   a. First the Attacker needs to get the Trojan server running on a target machine or attempt to steal someone else's victim.
   b. Then the Scanner looks to find the executed servers by scanning for the specific protocol/port that the server was set to (often times the default).
   c. UDP when scanned, if the port is open or blocked at the firewall, there will be no response from the port. If the port is closed the Scanner should get, "ICMP Destination Port Unreachable".
   d. The redundant response of open and blocked UDP ports is often why TCP scanning is done in conjunction with UDP scanning, though not apparently in this case. (TCP scans are often blocked at the firewall.).
   e. If the port is determined to be open, then the client will attempt to connect to it and if it is successful, the user of the client "owns" that machine.
   f. The significance of this scan is the same for all Trojan horses; if they are exploited on your machine, they "own" your machine!

6. Correlations:
   a. This is not a unique scan. Though Hack'A'Tack is not the most popular Trojan on the market, it is easy to find on the web.

7. Evidence of active targeting:
   a. There is no evidence of active targeting and it is likely that this was a random scan.

8. Severity: = (Criticality + lethality) – (System + Net Countermeasures)
   a. Criticality – 3; Random scan
   b. Lethality – 5; Extremely lethal to a Win 95/98 machine, if exploited
   c. System – 4; Server executed on Win98 box; Server will not work on a NT machine.
   d. Countermeasures – 5; Firewall/IDS and current anti-virus.
   e. Severity = 8 – 9 = -1

9. Defensive recommendations:
   a. None at this time, other than be careful about what software/executables are loaded on machine.

10. Multiple choice test question:
   a. What type of response will the source IP expect from this trace if the destination UDP port is open?
      i. "ICMP Destination Port Unreachable"
      ii. TCP Syn/Ack
      iii. No response at all

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

iv. TCP Reset

Ans: iii

5. SHIELDSUP.GRC.COM SCAN

```
Date          Time          Delta Time        Srce IP        Srce Port     Dest IP
      Dest Port       Size        Protocol          Seq #, Ack #, Window size

06/03/2000    21:26:51.110000                 IP-207.71.92.221    IP-1148        SENSOR1.DSL
      IP-139          64    TCP NetBIOS       S=1147831401,L=    0,A=        0,W= 8192
06/03/2000    21:26:54.015000    02.905000    IP-207.71.92.221    IP-1148        SENSOR1.DSL
      IP-139          64    TCP NetBIOS       S=1147831401,L=    0,A=        0,W= 8192
06/03/2000    21:27:00.615000    06.600000    IP-207.71.92.221    IP-1148        SENSOR1.DSL
      IP-139          64    TCP NetBIOS       S=1147831401,L=    0,A=        0,W= 8192
06/03/2000    21:27:12.720000    12.105000    IP-207.71.92.221    IP-1148        SENSOR1.DSL
      IP-139          64    TCP NetBIOS       S=1147831401,L=    0,A=        0,W= 8192
06/03/2000    21:31:37.300000    04:24.580000 IP-207.71.92.221    IP-1687        SENSOR1.DSL
      IP-21           64    TCP FTPCtl        S=1148117415,L=    0,A=        0,W= 8192
06/03/2000    21:31:47.435000    10.135000    IP-207.71.92.221    IP-1687        SENSOR1.DSL
      IP-21           64    TCP FTPCtl        S=1148117415,L=    0,A=        0,W= 8192
06/03/2000    21:31:47.435000    00.000000    IP-207.71.92.221    IP-1687        SENSOR1.DSL
      IP-21           64    TCP FTPCtl        S=1148117415,L=    0,A=        0,W= 8192
06/03/2000    21:31:58.079000    10.644000    IP-207.71.92.221    IP-1687        SENSOR1.DSL
      IP-21           64    TCP FTPCtl        S=1148117415,L=    0,A=        0,W= 8192
06/03/2000    21:32:23.739000    25.660000    IP-207.71.92.221    IP-1796        SENSOR1.DSL
      IP-23           64    TCP TELNET        S=1148162487,L=    0,A=        0,W= 8192
06/03/2000    21:32:25.619000    01.880000    IP-207.71.92.221    IP-1796        SENSOR1.DSL
      IP-23           64    TCP TELNET        S=1148162487,L=    0,A=        0,W= 8192
06/03/2000    21:32:31.140000    05.521000    IP-207.71.92.221    IP-1796        SENSOR1.DSL
      IP-23           64    TCP TELNET        S=1148162487,L=    0,A=        0,W= 8192
06/03/2000    21:32:43.235000    12.095000    IP-207.71.92.221    IP-1796        SENSOR1.DSL
      IP-23           64    TCP TELNET        S=1148162487,L=    0,A=        0,W= 8192
06/03/2000    21:33:07.255000    24.020000    IP-207.71.92.221    IP-1897        SENSOR1.DSL
      IP-25           64    TCP SMTP          S=1148207542,L=    0,A=        0,W= 8192
06/03/2000    21:33:10.525000    03.270000    IP-207.71.92.221    IP-1897        SENSOR1.DSL
      IP-25           64    TCP SMTP          S=1148207542,L=    0,A=        0,W= 8192
06/03/2000    21:33:17.230000    06.705000    IP-207.71.92.221    IP-1897        SENSOR1.DSL
      IP-25           64    TCP SMTP          S=1148207542,L=    0,A=        0,W= 8192
06/03/2000    21:33:28.310000    11.080000    IP-207.71.92.221    IP-1897        SENSOR1.DSL
      IP-25           64    TCP SMTP          S=1148207542,L=    0,A=        0,W= 8192
06/03/2000    21:33:52.261000    23.951000    IP-207.71.92.221    IP-1949        SENSOR1.DSL
      IP-79           64    TCP Finger        S=1148252687,L=    0,A=        0,W= 8192
06/03/2000    21:34:00.885000    08.624000    IP-207.71.92.221    IP-1949        SENSOR1.DSL
      IP-79           64    TCP Finger        S=1148252687,L=    0,A=        0,W= 8192
06/03/2000    21:34:01.260000    00.375000    IP-207.71.92.221    IP-1949        SENSOR1.DSL
      IP-79           64    TCP Finger        S=1148252687,L=    0,A=        0,W= 8192
06/03/2000    21:34:13.845000    12.585000    IP-207.71.92.221    IP-1949        SENSOR1.DSL
      IP-79           64    TCP Finger        S=1148252687,L=    0,A=        0,W= 8192
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
06/03/2000    21:36:07.495000     01:53.650000  IP-207.71.92.221    IP-2170      SENSOR1.DSL
        IP-113          64      IP TCP              S=1148387851,L=   0,A=       0,W= 8192
06/03/2000    21:36:09.095000     01.600000     IP-207.71.92.221    IP-2171      SENSOR1.DSL
        IP-139          64      TCP NetBIOS         S=1148389419,L=   0,A=       0,W= 8192
06/03/2000    21:36:12.055000     02.960000     IP-207.71.92.221    IP-2171      SENSOR1.DSL
        IP-139          64      TCP NetBIOS         S=1148389419,L=   0,A=       0,W= 8192
06/03/2000    21:36:17.985000     05.930000     IP-207.71.92.221    IP-2171      SENSOR1.DSL
        IP-139          64      TCP NetBIOS         S=1148389419,L=   0,A=       0,W= 8192
06/03/2000    21:36:30.410000     12.425000     IP-207.71.92.221    IP-2171      SENSOR1.DSL
        IP-139          64      TCP NetBIOS         S=1148389419,L=   0,A=       0,W= 8192
06/03/2000    21:37:40.365000     01:09.955000  IP-207.71.92.221    IP-2345      SENSOR1.DSL
        IP-443          64      TCP HTTPS           S=1148479419,L=   0,A=       0,W= 8192
06/03/2000    21:37:42.435000     02.070000     IP-207.71.92.221    IP-2345      SENSOR1.DSL
        IP-443          64      TCP HTTPS           S=1148479419,L=   0,A=       0,W= 8192
06/03/2000    21:37:48.165000     05.730000     IP-207.71.92.221    IP-2345      SENSOR1.DSL
        IP-443          64      TCP HTTPS           S=1148479419,L=   0,A=       0,W= 8192
06/03/2000    21:38:00.130000     11.965000     IP-207.71.92.221    IP-2345      SENSOR1.DSL
        IP-443          64      TCP HTTPS    S=1148479419,L=   0,A=       0,W= 8192
```

1. Source of trace:
    - b. This was collected on my home DSL connection.

2. Detect was generated by:
    - c. BlackIce Defender and then analyzed with Etherpeek. Output is .txt format from Etherpeek.

3. Probability the source address was spoofed:
    - a. Unlikely. I went to this web site and requested that it scan my system and test for vulnerabilities. (Not a recommended tactic, but I wanted to see what the trace would look like. I bet they collect quite a database of information.)

4. Description of attack:
    - a. This is a simple TCP scan of commonly used ports.

5. Attack mechanism:
    - a. This site will TCP port scan the requesting system and give the requesting system feedback on what the scan could "see".
    - b. The feedback it gives is based on the following:
        - i. "Stealthy" – if the TCP packet is dropped, and no reply is sent to GRC. They cannot tell if the host system exists.
        - ii. "Closed" – if TCP Reset is sent back they know that the process is not available, but that the host exists.
        - iii. "Open" – if a TCP Syn/Ack is sent back, they know the process and the host are present.
    - c. There is no difference between the two scans of the NetBIOS ports, other than the Srce Port and the Seq #. It must be GRC's assumption that a majority of the systems that will use this service would be windows machines and therefore pay particular attention to port 139.

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

d. I assume that the scan is slow to keep from Syn Flooding the requesting system.

6. Correlations:
   a. You should not see this very obvious signature unless you have requested it from the named web site.

7. Evidence of active targeting:
   a. Yes, I requested that it scan my address.

8. Severity: = (Criticality + lethality) – (System + Net Countermeasures)
   a. Criticality – 4; Targeted scan (though by request)
   f. Lethality – 3; Could have a list of processes available on a machine
   g. System – 4; Win98 box with patches
   h. Countermeasures – 5; Firewall and IDS. All ports were "stealthy", except 139 was "closed"
   i. Severity = 7 – 9 = -2

9. Defensive recommendations:
   a. None. Don't request this service unless you are willing to have the outcome possibly used against you.

10. Multiple choice test question:
    a. Why shouldn't you have an external system, that you have no control over, scan your system?
       i. The scanning system may be collecting a vulnerability database
       ii. The scanning system may tell you that your system is secure, so that they can exploit the vulnerabilities that they found
       iii. A sniffer placed just outside the scanning site, could collect all of the data that the scanning site collects.
       iv. All of the above

    Ans: iv

6. LINUXCONF PORT PROBE

```
Date           Time           Delta Time            Srce IP        Srce Port
Dest IP           Dest Port        Size        Protocol        Seq #, Ack #, Window size

05/17/2000    05:08:56.064000              IP-202.88.131.3         IP-2039         IP-
SENSOR1.DSL          IP-98           78        IP TCP         S=2902566021,L=    0,A=         0,W=32120
05/17/2000    05:08:56.953000        00.889000      IP-202.88.131.3         IP-2039         IP-
SENSOR1.DSL          IP-98           78        IP TCP         S=2902566021,L=    0,A=         0,W=32120
```

1. Source of trace:
   a. This trace was collected on a DSL connection to the Internet.

2. Detect was generated by:

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

    a. BlackIce Defender and then analyzed with Etherpeek. Output is .txt format from Etherpeek

3. Probability the source address was spoofed:
    a. It is unlikely that this is a spoofed address.

4. Description of attack:
    a. This is a scan for an open port 98. There is a rumored vulnerability in Linux 6.0-6.1in the LinuxConf to a buffer overflow through this port. There has been a significant rise in the scanning for his port in the past 6 months to a year.
    b. Notice the very large window size.

5. Attack mechanism
    a. LinuxConf is a configuration utility (A user interface to do configuration tasks) and an activator. It is rumored that with the appropriate script (easy to find on web), that you can cause LinuxConf to crash with a buffer overflow. Though I have not seen this for myself, there has been enough traffic scanning for this port to lead me to believe that something constructive (that is, destructive) can be done with it.

6. Correlations:
    a. This has become a common port to scan for in the past year or so (less).

7. Evidence of active targeting:
    a. Unlikely. I am not running Linux nor have port 98 open, on the destination machine.

8. Severity: = (Criticality + lethality) - (System + Net Countermeasures)
    a. Criticality – 2; No specific machines were targeted
    b. Lethality – 1; Will not work against Win machines
    c. System – 4; Win 98 with patches
    d. Countermeasures – 5; Firewall and IDS. Port 98 is closed.
    e. Severity = 3 – 9 = -6

9. Defensive recommendations:
    a. None necessary.

10. Multiple choice test question:
    a. The LinuxConf vulnerability takes advantage of:
        i. A buffer overflow vulnerability on Linux machines
        ii. A Trojan horse for Linux machines
        iii. A configuration error in LILO
        iv. None of the above

    Ans: i

7. BACK ORIFICE PING

Date Time Delta Time Srce IP Srce Port Dest IP
Dest Port Size Protocol

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
04/28/2000    23:11:13.309000                IP-209.138.20.128    IP-31338      SENSOR3.DSL
        IP-31337              65     IP UDP
04/28/2000    23:11:17.992000    04.683000   IP-209.138.20.128    IP-31338      SENSOR3.DSL
        IP-31337              65     IP UDP

05/02/2000    02:30:13.563000                IP-209.138.23.151    IP-31338      SENSOR3.DSL
        IP-31337              65     IP UDP
05/02/2000    02:30:13.975000    00.412000   IP-209.138.23.151    IP-31338      SENSOR3.DSL
        IP-31337              65     IP UDP
```

1. Source of trace:
    a. This trace was collected on a DSL connection.

2. Detect was generated by:
    a. BlackIce Defender and then analyzed with Etherpeek. Output is .txt format from Etherpeek.

3. Probability the source address was spoofed:
    a. Unlikely that the address is spoofed, but the scanner may be bouncing through another system in order to stay anonymous.

4. Description of attack:
    a. Based on the UDP port number (31337[ELITE] is the default for the BO Trojan), this is most likely the Back Orifice client scanning for active BO servers.

5. Attack mechanism:
    a. First the Attacker needs to get the Trojan server running on a target machine or attempt to steal someone else's victim.
    b. Then the Scanner (in the client) looks to find the executed servers by scanning for the specific protocol/port that the server was set to (often times the default, but can be set by the user).
    c. With UDP, if the port is open or blocked at the firewall, there will be no response from the port. If the port is closed the Scanner should get, "ICMP Destination Port Unreachable".
    d. If the port is determined to be open, then the client will attempt to connect to it and if it is successful, the user of the client "owns" that machine.

6. Correlations:
    a. This is not a unique scan. In this case, the same machine (evident from the MAC address (not in this trace)), with a different IP (DHCP) has repeated this scan twice, in a couple days.
    b. BO used to be the most popular Trojan but it seems to have given the title over to Sub7.
    c. Originally reported to Cert in Oct 98 (http://www.cert.org/vul_notes/VN-98.07.backorifice.html)

7. Evidence of active targeting:
    a. There is no evidence of active targeting and it is likely that this was a random scan.

8. Severity: = (Criticality + lethality) – (System + Net Countermeasures)

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

a. Criticality – 3; Random scan
j. Lethality – 5; Extremely lethal
k. System – 4; Server executed on Win98 box; Server will not work on a NT machine.
l. Countermeasures – 5; Firewall/IDS and current anti-virus.
m. Severity = 8 – 9 = -1

9. Defensive recommendations:
   a. None at this time, other than be careful about what software/executables are loaded on machine and keep anti-virus updated.

10. Multiple choice test question:
   a. If your machine is infected with the BO server, what can the controlling client do?
      i. Edit your registry
      ii. Shut down processes and/or the system (hard or soft)
      iii. Log keystrokes (including passwords)
      iv. All of the above

      Ans: iv

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

8. SYN FLOOD

```
Date              Time                 Delta Time        Srce IP                Srce Port  Dest IP
        Dest Port    Flag       Size      Protocol       Seq #, Ack #, Window size
                     (R=Runt:  <64 bytes long)
…
04/10/2000     21:40:31.128000        00.083000        IP-63.29.248.61        IP-1951           IP-Sensor2.DSL
         IP-133            R          62        IP TCP           S=   1066875,L=     0,A=          0,W= 8192
04/10/2000     21:40:31.155000        00.027000        IP-63.29.248.61        IP-1952           IP-Sensor2.DSL
         IP-134            R          62        IP TCP           S=   1066883,L=     0,A=          0,W= 8192
04/10/2000     21:40:31.183000        00.028000        IP-63.29.248.61        IP-1953           IP-Sensor2.DSL
         IP-135            R          62        IP TCP           S=   1066885,L=     0,A=          0,W= 8192
04/10/2000     21:40:31.238000        00.055000        IP-63.29.248.61        IP-1954           IP-Sensor2.DSL
         IP-136            R          62        IP TCP           S=   1066893,L=     0,A=          0,W= 8192
04/10/2000     21:40:31.650000        00.412000        IP-63.29.248.61        IP-1955           IP-Sensor2.DSL
         IP-137 R          62        TCP NB NamSvc       S=   1066902,L=     0,A=          0,W= 8192
04/10/2000     21:40:31.650000        00.000000        IP-63.29.248.61        IP-1956           IP-Sensor2.DSL
         IP-138            R          62        TCP NetBIOS S=   1066915,L=     0,A=          0,W= 8192
04/10/2000     21:40:31.732000        00.082000        IP-63.29.248.61        IP-1957           IP-Sensor2.DSL
         IP-139            R          62        TCP NetBIOS S=   1066928,L=     0,A=          0,W= 8192
04/10/2000     21:40:31.759000        00.027000        IP-63.29.248.61        IP-1958           IP-Sensor2.DSL
         IP-1080           R          62        IP TCP           S=   1066945,L=     0,A=          0,W= 8192
04/10/2000     21:40:31.842000        00.083000        IP-63.29.248.61        IP-1959           IP-Sensor2.DSL
         IP-3128           R          62        IP TCP           S=   1066962,L=     0,A=          0,W= 8192
04/10/2000     21:40:31.952000        00.110000        IP-63.29.248.61        IP-1960           IP-Sensor2.DSL
         IP-6667           R          62        IP TCP           S=   1066967,L=     0,A=          0,W= 8192
…
```

Averaged ~ 10 packets per second for 5 minutes

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Sometimes 80 per second, then a 15 second delay, then again.

1. Source of trace:
   a. This was collected on a DSL connection.

2. Detect was generated by:
   a. BlackIce Defender and then analyzed with Etherpeek. Output is .txt format from Etherpeek.

3. Probability the source address was spoofed:
   a. Highly likely. For this DoS to work, the source IP must be a spoofed address that no one will respond (Syn/Ack) to.

4. Description of attack:
   a. The attacker spoofs a non-responding IP address and sends a flood of Syn packets at the victim. For each Syn that is received by the victim, an allotment of memory is dedicated until the 3-way handshake is completed. The handshake is never completed and eventually all of the resources (tcp.maxsyn) that the victim has are used up, and it will not respond to any legitimate traffic, until the existing memory times-out.

5. Attack mechanism:
   a. This attack takes advantage of the connection-oriented communication of TCP and limited memory space to keep track of the state of connections. The significance of this attack is that legitimate traffic will be denied while the memory queue is full with connections waiting to be completed (that never will be) or to time-out.

6. Correlations:
   a. This is not that common of a detect today due to many current OS's can deny this DoS from being successful.

7. Evidence of active targeting:
   a. Yes, the victim needs to be actively targeted.

8. Severity: = (Criticality + lethality) – (System + Net Countermeasures)
   a. Criticality – 4; Targeted scan
   n. Lethality – 4; Could have complete DoS
   o. System – 4; Win98 box with patches
   p. Countermeasures – 4; Firewall and IDS. All ports were "stealthy", except 139 was "closed"
   q. Severity = 8 – 8 = 0

9. Defensive recommendations:
   a. Have updated and patched OS
   b. Increase value of tcp.maxsyn
   c. Decrease memory time-out value
   d. Run system that will auto kill syn flood connections

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

10. Multiple choice test question:
    a. Why is a syn flood DoS almost always from a spoofed address?
        i. So that the attackers identity is kept secret
        ii. So that there is no one to respond to the Syn/Acks coming from the victim
        iii. Because UDP is connectionless-oriented
        iv. So there is no echo response

    Ans: ii

9. RPC PORT PROBE

```
Date              Time                Delta Time         Srce IP              Srce Port
Dest IP            Dest Port           Size      Protocol          Seq #, Ack #, Window size

06/08/2000     11:25:59.817000                          IP-24.17.96.120        IP-1992          IP-
SENSOR1.DSL          IP-111           78        TCP RPC        S=3072953087,L=    0,A=        0,W=32120
06/08/2000     11:26:01.290000      01.473000     IP-24.17.96.120        IP-1992          IP-
SENSOR1.DSL          IP-111           78        TCP RPC        S=3072953087,L=    0,A=        0,W=32120


06/08/2000     11:30:46.560000                          IP-24.17.96.120        IP-4129          IP-
SENSOR2.DSL          IP-111           78        TCP RPC        S=3138043308,L=    0,A=        0,W=32120
06/08/2000     11:30:46.577000      00.017000     IP-24.17.96.120        IP-4129          IP-
SENSOR2.DSL          IP-111           78        TCP RPC        S=3138043308,L=    0,A=        0,W=32120
```

1. Source of trace:
    a. This was collected on two DSL connections, within the same providers address space.

2. Detect was generated by:
    a. BlackIce Defender and then analyzed with Etherpeek. Output is .txt format from Etherpeek.

3. Probability the source address was spoofed:
    a. Unlikely that the address is spoofed

4. Description of attack:
    a. The scanning system is likely scanning thousands of systems looking for Unix systems that are running the Remote Procedure Call (RPC) on port 111. RPC is developed by Sun and is a very popular way of building network applications.

5. Attack mechanism:
    a. Once identifying systems that are running RPC, that attacker would likely next attempt an RPC portmapper dump, which would list all the RPC programs on that machine and tell the intruder if there are any he/she can exploit.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

b. The significance of this is that if this port is not blocked behind a firewall or other means, and a RPC portmapper dump is allowed by outsiders, the “keys to the kingdom” are in the attackers hands, for all practical purposes.

6. Correlations:
   a. Since September 1999, there has been a dramatic rise in the number of scans for this port. This is due to the rpc.cmsd overflow exploit (Cert: CA-99-08-cmsd). Vulnerability has been discovered in this RPC service, so hackers are scouring the Internet looking for this service so they can exploit it to break into the system.

7. Evidence of active targeting:
   a. This is likely a large-scale scan due to the fact that two different sensors picked it up within a few minutes of each other.

8. Severity: = (Criticality + lethality) - (System + Net Countermeasures)
   a. Criticality – 3; Unix systems
   b. Lethality – 1; Not Unix
   c. System – 4; Win98 box with updated patches
   d. Countermeasures – 5; Firewall/IDS and port 111 is not used (not Unix)
   e. Severity = 4 – 9 = -5

9. Defensive recommendations:
   a. None; not running Unix

10. Multiple choice test question:
   a. If you are responsible for a NT/2000 network, does the above trace concern you?
      i. Yes, I need to be concerned about all traces
      ii. Yes, it is obviously targeting my network
      iii. No, my network in not vulnerable to the exploit this trace is looking for
      iv. No, my automated response system takes care of all my concerns

   Ans: iii

10. PROXY PORT PROBE (followed immediately by SOCKs and TCP port probe)

```
Date              Time              Delta Time        Srce IP           Srce Port     Dest IP
Dest Port             Protocol          Seq #, Ack #, Window size

04/27/2000     20:53:13.975000                  IP-193.232.248.11     IP-30007       IP-USA.DSL
        IP-8080        TCP HTTP Proxy     S=1580732156,L=    0,A=         0,W=  512
04/27/2000     20:53:16.982000     03.007000     IP-193.232.248.11     IP-30007       IP-USA.DSL
        IP-8080        TCP HTTP Proxy     S=1580732156,L=    0,A=         0,W=32120
04/27/2000     20:53:18.458000     01.476000     IP-193.232.248.11     IP-30007       IP-USA.DSL
        IP-8080        TCP HTTP Proxy     S=1580732156,L=    0,A=         0,W=  512
04/27/2000     20:53:18.458000     00.000000     IP-193.232.248.11     IP-30007       IP-USA.DSL
        IP-8080        TCP HTTP Proxy     S=1580732156,L=    0,A=         0,W=32120
04/27/2000     20:53:23.218000     04.760000     IP-193.232.248.11     IP-30007       IP-USA.DSL
        IP-8080        TCP HTTP Proxy     S=1580732156,L=    0,A=         0,W=32120
```

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

© SANS Institute 2000 - 2002   As part of GIAC practical repository.   Author retains full rights.

```
04/27/2000   20:53:23.224000    00.006000    IP-193.232.248.11    IP-30007    IP-USA.DSL
       IP-8080      TCP HTTP Proxy     S=1580732156,L=   0,A=       0,W=32120

04/27/2000   20:53:35.358000    12.134000    IP-193.232.248.11    IP-30009    IP-USA.DSL
       IP-3128      IP TCP             S=1146331294,L=   0,A=       0,W=  512
04/27/2000   20:53:35.358000    00.000000    IP-193.232.248.11    IP-30009    IP-USA.DSL
       IP-3128      IP TCP             S=1146331294,L=   0,A=       0,W=32120
04/27/2000   20:53:35.364000    00.006000    IP-193.232.248.11    IP-30009    IP-USA.DSL
       IP-3128      IP TCP             S=1146331294,L=   0,A=       0,W=  512
04/27/2000   20:53:35.364000    00.000000    IP-193.232.248.11    IP-30009    IP-USA.DSL
       IP-3128      IP TCP             S=1146331294,L=   0,A=       0,W=32120
04/27/2000   20:53:40.961000    05.597000    IP-193.232.248.11    IP-30009    IP-USA.DSL
       IP-3128      IP TCP             S=1146331294,L=   0,A=       0,W=32120
04/27/2000   20:53:47.004000    06.043000    IP-193.232.248.11    IP-30009    IP-USA.DSL
       IP-3128      IP TCP             S=1146331294,L=   0,A=       0,W=32120
04/27/2000   20:53:49.970000    02.966000    IP-193.232.248.11    IP-30193    IP-USA.DSL
       IP-1080      IP TCP             S=2956186160,L=   0,A=       0,W=  512
04/27/2000   20:53:50.069000    00.099000    IP-193.232.248.11    IP-30193    IP-USA.DSL
       IP-1080      IP TCPS=2956186160,L=   0,A=       0,W=  512
04/27/2000   20:53:52.964000    02.895000    IP-193.232.248.11    IP-30193    IP-USA.DSL
       IP-1080      IP TCP             S=2956186160,L=   0,A=       0,W=32120
04/27/2000   20:53:54.874000    01.910000    IP-193.232.248.11    IP-30193    IP-USA.DSL
       IP-1080      IP TCP             S=2956186160,L=   0,A=       0,W=32120
04/27/2000   20:53:58.965000    04.091000    IP-193.232.248.11    IP-30193    IP-USA.DSL
       IP-1080      IP TCP             S=2956186160,L=   0,A=       0,W=32120
04/27/2000   20:54:06.653000    07.688000    IP-193.232.248.11    IP-30193    IP-USA.DSL
       IP-1080      IP TCPS=2956186160,L=   0,A=       0,W=32120
04/27/2000   20:54:22.080000    15.427000    IP-193.232.248.11    IP-30549    IP-USA.DSL
       IP-81        IP TCP             S=2821575098,L=   0,A=       0,W=  512
04/27/2000   20:54:22.087000    00.007000    IP-193.232.248.11    IP-30549    IP-USA.DSL
       IP-81        IP TCP             S=2821575098,L=   0,A=       0,W=  512
04/27/2000   20:54:23.960000    01.873000    IP-193.232.248.11    IP-30549    IP-USA.DSL
       IP-81        IP TCP             S=2821575098,L=   0,A=       0,W=32120
04/27/2000   20:54:23.965000    00.005000    IP-193.232.248.11    IP-30549    IP-USA.DSL
       IP-81        IP TCPS=2821575098,L=   0,A=       0,W=32120
04/27/2000   20:54:29.962000    05.997000    IP-193.232.248.11    IP-30549    IP-USA.DSL
       IP-81        IP TCP             S=2821575098,L=   0,A=       0,W=32120
04/27/2000   20:54:49.203000    19.241000    IP-193.232.248.11    IP-30549    IP-USA.DSL
       IP-81        IP TCP             S=2821575098,L=   0,A=       0,W=32120
```

This analysis will only cover the 1st section of this trace, the Proxy port probe, but I thought this entire trace was interesting. It was of particular interest because it occurred on three different occasions, within a two-day period, from two different international locations.

1. Source of trace:
    a. This was collected on a DSL connection.

2. Detect was generated by:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

   a. BlackIce Defender and then analyzed with Etherpeek. Output is .txt format from Etherpeek.

3. Probability the source address was spoofed:
   a. Likely. If not spoofed, at least used a proxy to remain anonymous. Particularly because proxies are the target as well.

4. Description of attack:
   a. This scan (the 1st section) is simply a TCP scan to see if anything is listening on port 8080. This is a common port to have a proxy server on.

5. Attack mechanism:
   a. The reason for this attack would be to allow the scanner to find a proxy to use to make his exploits anonymous.
   b. The significance of this attack is that if the scanner detects a proxy, and can exploit it, he can remove his "source IP" address from all further exploits, once he goes through the proxy.
      i. The SOCKs scan could be used in a similar manner.
   c. This could also be a US citizen who is using a "Minsk" (whois lookup) proxy, in order to find a more local proxy, for performance or secrecy reasons.

6. Correlations:
   a. I have not seen this trace before, except that it occurred to me 3 times, in 2 days, by 2 different international addresses.

7. Evidence of active targeting:
   a. Unlikely. None of these processes are running in the target system.

8. Severity: = (Criticality + lethality) - (System + Net Countermeasures)
   a. Criticality – 3;
   b. Lethality – 1; Processes not available
   c. System – 4; Win98 box with updated patches
   d. Countermeasures – 5; Firewall/IDS and port 1080 is not used.
   e. Severity = 4 – 9 = -5

9. Defensive recommendations:
   a. None.

10. Multiple choice test question:
    a. What is the scanner looking for with this scan?
       i. An active Trojan horse server
       ii. A system with a buffer overflow vulnerability
       iii. A system to make himself anonymous with
       iv. A system that can synchronize time with

    Ans: iii

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.