# Intrusion Detection in Depth

*GIAC Certified Intrusion Analyst (GCIA) Practical Assignment*

GCIA Practical Version 3.0
SANS 2001 Washington DC

**Brian K. Sheffler**

# Table of Contents

# Assignment 1

# Network Detects

## Detect #1 – Battle.Net or CDE Subprocess Control Service?

### TCPDump Log:

```
20:48:47.022770 63.240.202.131.6112 > MY.NET.121.209.6112:  udp 8
  0000: 4500 0024 9c8e 0000 7311 e355 3ff0 ca83        E..$....s.ãU?ðÊ.
  0010: 0a01 79d1 17e0 17e0 0010 2061 0500 0000        C yÑ.à.à.. a....
  0020: 7465 6e62                                      tenb

20:48:47.023137 63.240.202.131.6112 > MY.NET.121.209.6112:  udp 8
  0000: 4500 0024 9c8f 0000 7311 e354 3ff0 ca83        E..$....s.ãT?ðÊ.
  0010: 0a01 79d1 17e0 17e0 0010 2061 0500 0000        C yÑ.à.à.. a....
  0020: 7465 6e62                                      tenb

21:16:43.482091 63.240.202.131.6112 > MY.NET.121.209.6112:  udp 8
  0000: 4500 0024 2d92 0000 7311 5252 3ff0 ca83        E..$-...s.RR?ðÊ.
  0010: 0a01 79d1 17e0 17e0 0010 2061 0500 0000        C yÑ.à.à.. a....
  0020: 7465 6e62                                      tenb

21:16:43.482615 63.240.202.131.6112 > MY.NET.121.209.6112:  udp 8
  0000: 4500 0024 2d93 0000 7311 5251 3ff0 ca83        E..$-...s.RQ?ðÊ.
  0010: 0a01 79d1 17e0 17e0 0010 2061 0500 0000        C yÑ.à.à.. a....
  0020: 7465 6e62                                      tenb

21:25:40.104547 63.240.202.139.6112 > MY.NET.121.209.6112:  udp 8
  0000: 4500 0024 6ac0 0000 7311 151c 3ff0 ca8b        E..$jÀ..s...?ðÊ.
  0010: 0a01 79d1 17e0 17e0 0010 2059 0500 0000        C yÑ.à.à.. Y....
  0020: 7465 6e62                                      tenb

21:25:40.104908 63.240.202.139.6112 > MY.NET.121.209.6112:  udp 8
  0000: 4500 0024 6ac1 0000 7311 151b 3ff0 ca8b        E..$jÁ..s...?ðÊ.
  0010: 0a01 79d1 17e0 17e0 0010 2059 0500 0000        C yÑ.à.à.. Y....
  0020: 7465 6e62                                      tenb

22:14:03.795018 63.240.202.131.6112 > MY.NET.121.209.6112:  udp 8
  0000: 4500 0024 5c6a 0000 7311 237a 3ff0 ca83        E..$\j..s.#z?ðÊ.
  0010: 0a01 79d1 17e0 17e0 0010 2061 0500 0000        C yÑ.à.à.. a....
  0020: 7465 6e62                                      tenb
```

```
22:14:03.795381 63.240.202.131.6112 > MY.NET.121.209.6112:  udp 8
 0000: 4500 0024 5c6c 0000 7311 2378 3ff0 ca83          E..$\l..s.#x?ðÊ.
 0010: 0a01 79d1 17e0 17e0 0010 2061 0500 0000          C yÑ.à.à.. a....
 0020: 7465 6e62                                        tenb
```

## SOURCE OF TRACE:

This capture came from a colleague’s private network.

## DETECT GENERATED BY:

Manual analysis using OpenBSD v3.0 and the included tcpdump (v3.4.0, libpcap 0.5) functionality.

## PROBABILITY THAT THE SOURCE ADDRESS WAS SPOOFED:

This source IP was most likely not spoofed. Although my first instinct was related to the Carnegie Mellon Software Engineering Institute CERT Coordination Center’s (CERT/CC) recently published CERT® Advisory CA-2001-31, Buffer Overflow in CDE Subprocess Control Service, that vulnerability operates over port 6112 using TCP. Because this traffic occurs on port 6112 UDP (Battle.Net), I looked for matches in various search engines against the data given in the payload sections and found excellent information at http://www.digivill.net/~minus/starhack.txt[1] and at http://archives.neohapsis.com/archives/incidents/2000-03/0169.html.[2] This indicated that the traffic appears to be valid Battle.Net traffic, and in conjunction with my colleague’s confirmation of playing Starcraft and Diablo, constitutes the low probability that the source IP was spoofed.

## DESCRIPTION OF THE ATTACK:

The information given at http://www.digivill.net/~minus/starhack.txt[1] clearly shows that the “tenb” statement in the payload of these packets, and by being associated with port 6112 UDP (Battle.Net), indicates valid Battle.Net traffic (Battle.Net is used for on-line gaming such as Diablo and Starcraft). There is the possibility that this traffic is reconnaissance due to the passing of system information that occurs during the authentication and response/challenge stages of connecting to the Battle.Net. However, knowing the applications that are running and that this system is used for playing games leads me to the conclusion that this is valid traffic.

## ATTACK MECHANISM:

Because this has been determined to be valid traffic, no attack mechanism is stated. However, it is important to note that a large amount of system information is passed in the clear when connecting to Battle.Net on this port and may be used for reconnaissance purposes.

## CORRELATIONS:

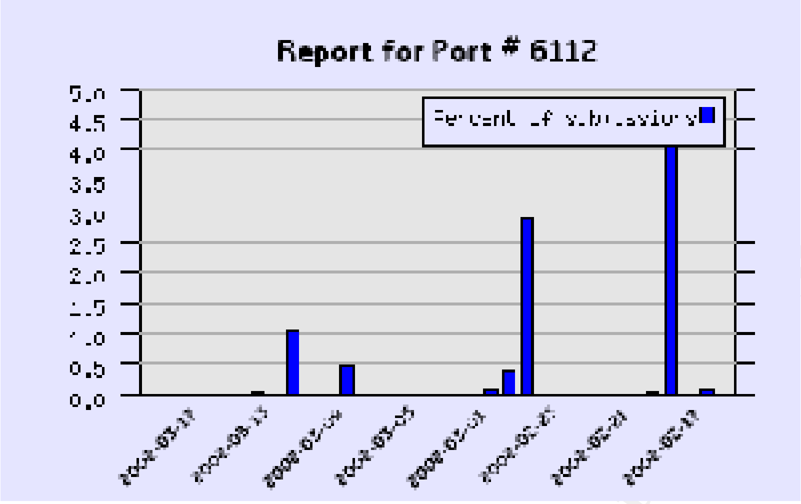
Port 6112 UDP and Battle.Net information can be found at the following sites:
http://www.digivill.net/~minus/starhack.txt[1]
http://archives.neohapsis.com/archives/incidents/2000-03/0169.html[2]
http://www.incidents.org/archives/intrusions/msg02922.html[3]
http://www.battle.net/[4]
http://advice.networkice.com/Advice/Exploits/Ports/6112/default.htm[5]

On 12 November 2001, CERT/CC published a CERT® Advisory CA-2001-31, Buffer Overflow in CDE Subprocess Control Service, and Vicki Irwin, in the "Handler's Diary" at Incidents.org, noted that there had been fairly low interest in port 6112 scanning for the previous month.
http://www.cert.org/advisories/CA-2001-31.html[6]
http://www.incidents.org/archives/intrusions/msg02922.html[3]

On 18 December 2001, in another Incidents.org "Handler's Diary" posting, interest was noted for TCP port 6112. That posting referenced a link to a separate submission from John Sage in which the traffic was attributed to people looking for on-line game servers.
http://www.incidents.org/diary.php?id=125[7]
http://www.incidents.org/archives/intrusions/msg02922.html[3]

The CDE Subprocess Control Service vulnerability has been assigned the identifier "CAN-2001-0803" by the Mitre Corporation's Common Vulnerabilities and Exposures (CVE) group: http://cve.mitre.org/cve.[8]

For further information on the CDE vulnerability see also:
http://www.kb.cert.org/vuls/id/172583[9]
http://xforce.iss.net/alerts/advise101.php[10]



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=6112)[11]

## EVIDENCE OF ACTIVE TARGETING:

This system is often used to play on-line games that commonly use port 6112. Therefore, there was no evidence of active targeting outside of the scope of those games.

## SEVERITY:

(Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity
* (Scale: 0-5)

Criticality – My basis for scoring criticality is determined by the operational or functional role a system plays in a given network. (Criticality = Impact + Contingency Capability)

The specific intent of this system is to capture Internet traffic as it occurs in the wild. Therefore, the operational impact of this machine has little bearing on the overall functionality of the network. Furthermore, the host performed as was expected. However, had this host been compromised, its posture as a non-trusted entity would have resulted in minimal impact to the internal network infrastructure.

Criticality = 1.

Lethality – I use this section to determine the lethality of the attack itself, thereby minimizing the subjective nature inherent when re-computing the score of each attack as it is applied to the varying roles of any given system within a network. I have done this to provide for a standardized baseline that, when combined with the other criteria, results in a more consistent and meaningful determination of the Severity, or impact, to that network. (Lethality = Probability of success + Potential for loss or damage)

My basis for scoring Lethality is to determine the level of access gained, or the loss of functionality that would result, from a successful attack. Also taken into consideration is the likelihood that this attack could or would be successful. By doing this, I allow for the Criticality of the system to counterbalance, or further support, the overall determination of its Severity. Hence, a high-level attack on a non-critical system becomes averaged out through the overall formula. I have found this to be an effective method when performing risk analysis.

In this case, the UDP traffic did not cause any damage, however, in the event that the traffic had been malicious, the effect would have been limited to reconnaissance, thus supporting a lower score.

Lethality = 0.

<u>System Countermeasures</u> – My basis for scoring System Countermeasures is to determine the actual configuration of the system at the time of the attack versus the most secure and up-to-date configuration that was available. This allows me to objectively compare and contrast any deficiencies within my defensive posture at the system level.
(System Countermeasures = |Actual Configuration – Most Secure Configuration |)

In this case the target system was actively used for on-line gaming and performed as was expected. However, because the objective of this machine was to attract and capture Internet traffic in an unsecured posture/environment, the only system countermeasures in place are those that are enabled by default. This results in a very low Actual Configuration when compared to the Most Secure Configuration. Also, no additional host-based firewall software was installed.

System Countermeasures = 0

<u>Network Countermeasures</u> – My basis for scoring Network Countermeasures is to determine the actual defensive measures that were in place, and their effectiveness, that existed on the network at the time of the attack versus those measures that might have prevented this traffic from reaching inside the infrastructure. This allows me to objectively compare and contrast any deficiencies within my defensive posture at the network level.
(Network Countermeasures = |[Actual Countermeasures + Actual Configuration] – [Available Countermeasures + High Security Configuration]|)

The objective of this machine was to attract and capture Internet traffic in an unsecured posture/environment, therefore, the existing network countermeasures provided no protection for the target machine. This intentionally resulted in a low score and did not allow for the evaluation of deficiencies within the network defenses.

Network Countermeasures = 0

<u>Overall Severity</u>:

(Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity

**(1 + 0) – (0 + 0) = 1**

## DEFENSIVE RECOMMENDATIONS:

The previously mentioned Overall Severity score indicates that, in this configuration, an attack would have had a high probability of success and, if successful, may have resulted in a high-level compromise for this particular machine. However, because this configuration is intentional and the system is not operationally critical, the lower Severity score is justified.

Security recommendations are as follows:

- Unauthorized software should be removed
- The latest vendor patches/fixes should be applied
- Unnecessary services should be disabled
- Logging/auditing should be enabled
- The system should be placed behind a perimeter firewall
- A host-based firewall should be installed
- Unused ports should be blocked
- A network IDS should be installed
- A strict security policy should be enforced

## MULTIPLE CHOICE TEST QUESTION:

Which of the following is commonly associated with UDP port 6112?

a) A CDE Subprocess Control Service Buffer Overflow vulnerability
b) A SSH/CRC32 Buffer Overflow vulnerability
c) MySQL
d) Diablo or Starcraft

Answer - The best answer is (d). UDP port 6112 is commonly associated with Battle.Net. Diablo and Starcraft are on-line games that use the Battle.Net service.

## Detect #2 – Sun RPC Portmapper

**TCPDump Log:**

```
03:48:26.461340 218.7.9.68.2661 > MY.NET.121.209.111: S 3317536456:3317536456(0)
win 32120 <mss 1460,sackOK,timestamp 92294684 0,nop,wscale 0> (DF)
 0000: 4500 003c 60a9 4000 2e06 4b56 da07 0944          E..<`©@...KVÚ..D
 0010: 0a01 79d1 0a65 006f c5bd 96c8 0000 0000          C yÑ.e.oÅ½.È....
 0020: a002 7d78 6edb 0000 0204 05b4 0402 080a          .}xnÛ.....´....
 0030: 0580 4e1c 0000 0000 0103 0300                    ..N.........

03:48:29.429346 218.7.9.68.2661 > MY.NET.121.209.111: S 3317536456:3317536456(0)
win 32120 <mss 1460,sackOK,timestamp 92294984 0,nop,wscale 0> (DF)
 0000: 4500 003c 6464 4000 2e06 479b da07 0944          E..<dd@...G.Ú..D
 0010: 0a01 79d1 0a65 006f c5bd 96c8 0000 0000          C yÑ.e.oÅ½.È....
 0020: a002 7d78 6daf 0000 0204 05b4 0402 080a          .}xm¯.....´....
 0030: 0580 4f48 0000 0000 0103 0300                    ..OH........

01:14:11.643593 195.188.190.142.57488 > MY.NET.121.209.111: S
1535749076:1535749076(0) win 8760 <mss 1460> (DF)
 0000: 4500 002c 11ad 4000 f706 3262 c3bc be8e          E..,.-@.÷.2bÃ¼¾.
 0010: 0a01 79d1 e090 006f 5b89 abd4 0000 0000          C yÑà..o[.«Ô....
 0020: 6002 2238 4dd4 0000 0204 05b4                    `."8MÔ.....´
```

**SOURCE OF TRACE:**

This capture came from a colleague's private network.

**DETECT GENERATED BY:**

Manual analysis using OpenBSD v3.0 and the included tcpdump (v3.4.0, libpcap 0.5) functionality.

**PROBABILITY THAT THE SOURCE ADDRESS WAS SPOOFED:**

These source IP addresses were probably not spoofed. This appears to be a SYN scan on port 111 that is probing for a system that is running Sun RPC services. Because of this, the scanning host is looking for response, thus requiring the ability to receive those replies.

## DESCRIPTION OF THE ATTACK:

From the Intrusion Detection FAQs posted on the SANS.org web site (http://www.sans.org/newlook/resources/IDFAQ/blocking.htm)[12] David P. Reece provides the following description of this type of activity: "When a client makes an RPC call to a given program number, it first connects to rpcbind on the target system to determine the address where the RPC request should be sent. Basically, the active port 111 is going to have a list of all active services, and tell the requesting client were to go to connect." There are multiple RPC vulnerabilities that are tied to this exploit. See the Correlation section of this analysis for examples.

Microsoft Windows based systems are not affected by this exploit. Reference the http://www.networkice.com/advice/Intrusions/2003016/default.htm[13] statement that "For Windows users, this is not serious at all. The hacker is just scanning computers looking for a UNIX system they can exploit."

## ATTACK MECHANISM:

This was most likely part of a much larger scan(s) for systems that have an active port 111. This type of mass scanning activity is usually accomplished by using a scripting tool that can perform scans of this magnitude in a relatively short period of time. Further information referencing this type of automated scanning can be found at CERT/CC's web site (http://www.cert.org/incident_notes/IN-98-06.html)[14] or by doing a search for port 111 from their home page (http://www.cert.org).[15]

## CORRELATIONS:

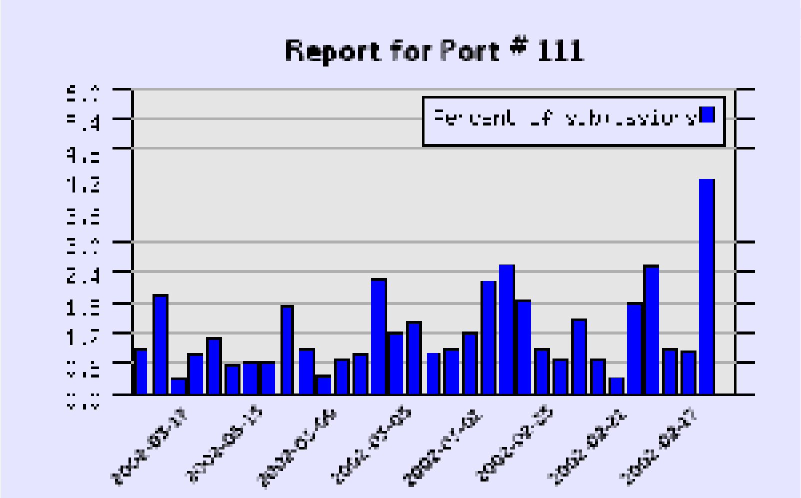
Logs posted by Laurie Zirkle at the SANS.org web site (http://www.incidents.org/archives/intrusions/msg03725.html)[16] on 06 February 2002 show similar types of port 111 scanning that occurred on 05 February 2002.

Network ICE (http://www.networkice.com/advice/Intrusions/2003016/default.htm)[13] noted in September 1999 that an increase in port 111 scanning had been observed. At that time, a significant rpc.cmsd overflow exploit had been identified and was credited as the cause of that traffic. However, this is only one of many exploits that exist for this port/service. Two such linked vulnerabilities can be found at CERT/CC's web site as VU#648304 (http://www.kb.cert.org/vuls/id/648304)[17] and VU#34043 (http://www.kb.cert.org/vuls/id/34043).[18]

David Reece's posting on SANS.org (http://www.sans.org/newlook/resources/IDFAQ/blocking.htm)[12] references security measures and, also, alternative ports that might allow some port blocking defenses to be subverted and rendered ineffective. The Internet Security Systems (ISS) web site (http://www.iss.net/security_center/static/330.php)[19] and the Mitre Corporation's Common

Vulnerabilities and Exposures (CVE-1999-0189) web site (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0189)[20] also reference these alternative port(s).

For further information RFCs for Port 111 (Sun RPC services) are posted here:
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1057.html[21]
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1833.html[22]



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=111)[23]

**EVIDENCE OF ACTIVE TARGETING:**

This is a TCP port 111 SYN scan for systems that are running Sun RPC services and is probably not targeted. Following the links through Network ICE's Port Knowledgebase (http://advice.networkice.com/Advice/Exploits/Ports/111/default.htm[24] and http://www.networkice.com/advice/Intrusions/2003016/default.htm)[13] lends more detail to this explanation: "An intruder has attempted to access the Sun RPC (rpcbind, portmapper) service on your system. This is probably during a sweep of millions of machines on the Internet, and is probably not targeting your computer in particular."

**SEVERITY:**

(Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity
* (Scale: 0-5)

Criticality – My basis for scoring criticality is determined by the operational or functional role a system plays in a given network. (Criticality = Impact + Contingency Capability)

The specific intent of this system is to capture Internet traffic as it occurs in the wild. Therefore, the operational impact of this machine has little bearing on the overall functionality of the network. Furthermore, the host performed as was expected. However, had this host been compromised, its posture as a non-trusted entity would have resulted in minimal impact to the internal network infrastructure.

Criticality = 1.

Lethality – I use this section to determine the lethality of the attack itself, thereby minimizing the subjective nature inherent when re-computing the score of each attack as it is applied to the varying roles of any given system within a network. I have done this to provide for a standardized baseline that, when combined with the other criteria, results in a more consistent and meaningful determination of the Severity, or impact, to that network. (Lethality = Probability of success + Potential for loss or damage)

My basis for scoring Lethality is to determine the level of access gained, or the loss of functionality that would result, from a successful attack. Also taken into consideration is the likelihood that this attack could or would be successful. By doing this, I allow for the Criticality of the system to counterbalance, or further support, the overall determination of its Severity. Hence, a high-level attack on a non-critical system becomes averaged out through the overall formula. I have found this to be an effective method when performing risk analysis.

In this case, the UDP traffic did not cause any damage, however, in the event that the traffic had been malicious, the effect would have been limited to reconnaissance, thus supporting a lower score.

Lethality = 0.

System Countermeasures – My basis for scoring System Countermeasures is to determine the actual configuration of the system at the time of the attack versus the most secure and up-to-date configuration that was available. This allows me to objectively compare and contrast any deficiencies within my defensive posture at the system level. (System Countermeasures = |Actual Configuration – Most Secure Configuration |)

In this case the target system was actively used for on-line gaming and performed as was expected. However, because the objective of this machine was to attract and capture Internet traffic in an unsecured posture/environment, the only system countermeasures in place are those that are enabled by default. This results in a very low Actual Configuration when compared to the Most Secure Configuration. Also, no additional host-based firewall software was installed.

System Countermeasures = 0

Network Countermeasures – My basis for scoring Network Countermeasures is to determine the actual defensive measures that were in place, and their effectiveness, that existed on the network at the time of the attack versus those measures that might have prevented this traffic from reaching inside the infrastructure. This allows me to objectively compare and contrast any deficiencies within my defensive posture at the network level. (Network Countermeasures = |[Actual Countermeasures + Actual Configuration] – [Available Countermeasures + High Security Configuration]|)

The objective of this machine was to attract and capture Internet traffic in an unsecured posture/environment, therefore, the existing network countermeasures provided no protection for the target machine. This intentionally resulted in a low score and did not allow for the evaluation of deficiencies within the network defenses.

Network Countermeasures = 0

Overall Severity:

(Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity

**(1 + 0) – (0 + 0) = 1**

## DEFENSIVE RECOMMENDATIONS:

The Overall Severity score indicates that, in this configuration, a scan for the purposes of reconnaissance would not have resulted in a high-level compromise for this particular machine.

Note that Microsoft Windows based systems are not affected. Reference the following statement on Network ICE's web site (http://www.networkice.com/advice/Intrusions/2003016/default.htm)[13] that "For Windows users, this is not serious at all. The hacker is just scanning computers looking for a UNIX system they can exploit."

CERT® Advisory CA-1994-15 NFS Vulnerabilities (http://www.cert.org/advisories/CA-1994-15.html)[25] recommends the following security measures:

- Filter packets at your firewall/router (in this case, port 111 UDP/TCP and possibly an alternative high port)
- Use a portmapper that disallows proxy access
- Check the configuration of the /etc/exports files on your hosts
- Ensure that your systems are current with patches and workarounds available from your vendor and identified in CERT advisories

Other security recommendations are as follows:

- Unauthorized software should be removed
- The latest vendor patches/fixes should be applied
- Unnecessary services should be disabled
- Logging/auditing should be enabled
- The system should be placed behind a perimeter firewall
- A host-based firewall should be installed
- Unused ports should be blocked
- A network IDS should be installed
- A strict security policy should be enforced

**MULTIPLE CHOICE TEST QUESTION:**

Why would an attacker probe for port 111, the Sun RPC service?

a) It is a backdoor into UNIX systems
b) To find potential connections for an exploit
c) It is a backdoor into Microsoft Windows based systems
d) To find web proxy servers

Answer - The best answer is (b). From the Intrusion Detection FAQs posted on the SANS.org web site (http://www.sans.org/newlook/resources/IDFAQ/blocking.htm)[12] David P. Reece provides the following description of this type of activity: "When a client makes an RPC call to a given program number, it first connects to rpcbind on the target system to determine the address where the RPC request should be sent. Basically, the active port 111 is going to have a list of all active services, and tell the requesting client were to go to connect."

## Detect #3 – Port 80 SYN Scan

**Log:**

The following log file was posted by Ken Connelly in the Incidents.Org archives (http://www.incidents.org/archives/intrusions/msg03828.html)[26] on 15 February 2002.

"The following extracts show the beginning and ending of scan activity was detected on my network. The number following each set is the total number of probes for that source. Timestamps are GMT-0600.

```
Feb 14 04:12:26 217.136.114.162:3408 -> xxx.yyy.0.0:80 SYN ******S*
Feb 14 04:12:29 217.136.114.162:3409 -> xxx.yyy.0.1:80 SYN ******S*
Feb 14 04:12:26 217.136.114.162:3410 -> xxx.yyy.0.2:80 SYN ******S*
Feb 14 04:12:26 217.136.114.162:3416 -> xxx.yyy.0.8:80 SYN ******S*
Feb 14 04:12:29 217.136.114.162:3417 -> xxx.yyy.0.9:80 SYN ******S*
Feb 14 04:12:26 217.136.114.162:3419 -> xxx.yyy.0.11:80 SYN ******S*
Feb 14 04:12:29 217.136.114.162:3420 -> xxx.yyy.0.12:80 SYN ******S*
Feb 14 04:12:29 217.136.114.162:3422 -> xxx.yyy.0.14:80 SYN ******S*
[...]
Feb 14 05:14:06 217.136.114.162:4404 -> xxx.yyy.67.100:80 SYN ******S*
Feb 14 05:14:10 217.136.114.162:4413 -> xxx.yyy.67.173:80 SYN ******S*
Feb 14 05:14:12 217.136.114.162:4419 -> xxx.yyy.67.173:80 SYN ******S*
Feb 14 05:14:17 217.136.114.162:4431 -> xxx.yyy.67.173:80 SYN ******S*
Feb 14 05:14:21 217.136.114.162:4442 -> xxx.yyy.67.173:80 SYN ******S*
Feb 14 05:14:22 217.136.114.162:4444 -> xxx.yyy.67.173:80 SYN ******S*
Feb 14 05:14:23 217.136.114.162:4446 -> xxx.yyy.67.184:80 SYN ******S*
Feb 14 05:14:25 217.136.114.162:4448 -> xxx.yyy.71.250:80 SYN ******S*
42975
--
- Ken
==================================================================
```

Ken Connelly (KC152) Systems and Operations Manager, ITS - Network Services University of Northern Iowa Cedar Falls, IA 50614-0121 email: Ken.Connelly@uni.edu phone: (319) 273-5850 fax: (319) 273-7373"

**SOURCE OF TRACE:**

This capture came from a posting by Ken Connelly in the Incidents.Org archives (http://www.incidents.org/archives/intrusions/msg03828.html)[26] on 15 February 2002. The source appears to be the University of Northern Iowa Cedar Falls.

## DETECT GENERATED BY:

Although not stated, this capture appears to be from SNORT.

## PROBABILITY THAT THE SOURCE ADDRESS WAS SPOOFED:

The source IP was most likely not spoofed. This appears to be a SYN scan on port 80 that is looking for a particular response from a system, thus indicating that it might be vulnerable. This requires the ability to receive those responses, hence the use of TCP and the assumed 3-way handshake, which supports the conclusion that that the source IP was not spoofed.

## DESCRIPTION OF THE ATTACK:

This appears to be a port 80 SYN scan. The incrementing source ports, and corresponding destination IPs, that contain SYN flags within a short amount of time support this assessment. Also, because this was posted as "scan" activity, and no SYN-ACK traffic was reported, I must assume that that 3-way handshake was not completed.

This activity was most likely carried out by a scanning tool such as the popular NMAP, of which, according to the NMAP.Org web site (http://www.nmap.org/nmap/index.html)[27], "was designed to rapidly scan large networks, although it works fine against single hosts." Port 80 scans are quite commonplace and multiple vulnerabilities/exploits exist for the different web servers and systems that may be listening on that port.

CERT/CC posted:

- CERT® Advisory CA-2001-23 Continued Threat of the "Code Red" Worm (http://www.cert.org/advisories/CA-2001-23.html)[28] "Systems not running IIS, but with an HTTP server listening on TCP port 80 will probably accept the HTTP request, return with an "HTTP 400 Bad Request" message, and potentially log this request in an access log." This is an example of a well-known exploit (Code Red) and, furthermore, this stated reply could be used for reconnaissance purposes.

- CERT® Advisory CA-2001-11 sadmind/IIS Worm (http://www.cert.org/advisories/CA-2001-11.html)[29] "Solaris systems compromised by this worm are being used to scan and compromise other Solaris and IIS systems. IIS systems compromised by this worm can suffer modified web content." Multiple vulnerabilities exist for both Solaris and Microsoft's Internet Information Server (IIS), however, recently IIS exploits/vulnerabilities have been the most common and prolific. See

- CERT® Incident Note IN-99-01 (http://www.cert.org/incident_notes/IN-99-01.html)[30] "The sscan tool performs probes against victim hosts to identify services which may potentially be vulnerable to exploitation. Though sscan itself does not attempt to exploit vulnerabilities, it can be configured to automatically execute scripts of commands that can be maliciously crafted to exploit vulnerabilities."

## ATTACK MECHANISM:

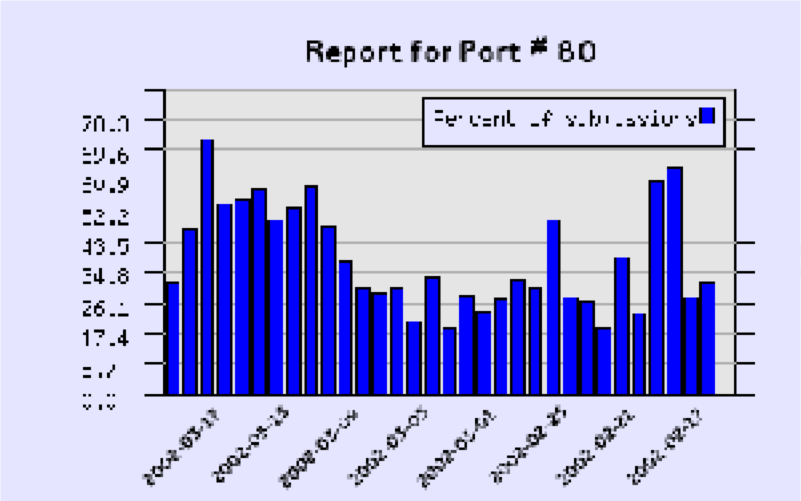
Nmap.Org's web site (http://www.nmap.org/nmap/index.html)[27] also gives the following description of its mechanics: "Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers, and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL." This same concept is used by many of the other scanning tools and appears to be in widespread use.

## CORRELATIONS:

- CERT/CC CERT® Incident Note IN-99-01 (http://www.cert.org/incident_notes/IN-99-01.html)[30] "The sscan tool performs probes against victim hosts to identify services which may potentially be vulnerable to exploitation. Though sscan itself does not attempt to exploit vulnerabilities, it can be configured to automatically execute scripts of commands that can be maliciously crafted to exploit vulnerabilities."

- At NMAP.Org (http://www.nmap.org/nmap/index.html)[27] "Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics."

- A Security Focus web site thread (http://www.securityfocus.com/cgi-bin/archive.pl?id=75&start=2002-02-17&end=2002-02-23&mid=256047&threads=1)[31], posted on 13 February 2002 by David Nesting, states that port 80 traffic had been observed. This thread goes on to explore the possibility of a SYN flood or "bounced" attack against a 3rd party by spoofing that 3rd party's IP as the source of the SYN traffic. A "reflected" DDoS is described in this part of the thread: http://www.securityfocus.com/cgi-bin/archive.pl?id=75&start=2002-02-17&end=2002-02-23&mid=256101&threads=1[32] by Dave Dittrich. However, in the detect that I posted here, some of the specifics mentioned in this thread are not met (a changing source IP, etc.) and thus, do not indicate this type of attack.



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=80)[33]

## EVIDENCE OF ACTIVE TARGETING:

This is a SYN scan that is looking for systems that are listening on port 80 and it is probably not targeted. An excerpt from Network ICE's web site (http://www.networkice.com/Advice/Intrusions/2003102/default.htm)[34] describes this type of traffic as "This means that if you see a TCP port probe for port 80, then a hacker is most likely testing your system to see if you've installed your own web server." The only IP in this detect that was singled out or was hit more often was "xxx.yyy.67.173" of which may require closer inspection. Otherwise, the intruder appears to be looking for targets of opportunity.

## SEVERITY:

(Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity
* (Scale: 0-5)

Criticality – My basis for scoring criticality is determined by the operational or functional role a system plays in a given network. (Criticality = Impact + Contingency Capability)

The specific role of this system is not stated, however, because it is located at a university, I am making my Severity determinations based on the concept that this system is used to perform captures in the wild. Therefore, the operational impact of this machine has little bearing on the overall functionality of the network. Had this host been compromised, its posture as a non-trusted entity would have resulted in minimal impact to the internal network infrastructure.

Criticality = 1.

Lethality – I use this section to determine the lethality of the attack itself, thereby minimizing the subjective nature inherent when re-computing the score of each attack as it is applied to the varying roles of any given system within a network. I have done this to provide for a standardized baseline that, when combined with the other criteria, results in a more consistent and meaningful determination of the Severity, or impact, to that network. (Lethality = Probability of success + Potential for loss or damage)

My basis for scoring Lethality is to determine the level of access gained, or the loss of functionality that would result, from a successful attack. Also taken into consideration is the likelihood that this attack could or would be successful. By doing this, I allow for the Criticality of the system to counterbalance, or further support, the overall determination of its Severity. Hence, a high-level attack on a non-critical system becomes averaged out through the overall formula. I have found this to be an effective method when performing risk analysis.

In this case, the TCP traffic did not cause any damage, however, in the event that the traffic had been malicious, the effect would have been limited to reconnaissance, thus supporting a lower score.

Lethality = 0.

System Countermeasures – My basis for scoring System Countermeasures is to determine the Actual Configuration of the system at the time of the attack versus the Most Secure and up-to-date configuration that was available. This allows me to objectively compare and contrast any deficiencies within my defensive posture at the system level.

In this case the countermeasures of the capture device are not stated. But because of the assumption that it is used to capture traffic in the wild, I am also assuming that the countermeasures are minimal. This results in a very low Actual Configuration when compared to the Most Secure Configuration. Also, no indication of additional host-based firewall software was installed.

System Countermeasures = 0

Network Countermeasures – My basis for scoring Network Countermeasures is to determine the actual defensive measures that were in place, and their effectiveness, that existed on the network at the time of the attack versus those measures that might have prevented this traffic from reaching inside the infrastructure. This allows me to objectively compare and contrast any deficiencies within my defensive posture at the network level.

Once again, assuming the objective of this machine was to attract and capture traffic in an unsecured posture/environment, the existing network countermeasures provided no protection for the target machine. This intentionally resulted in a low score and did not allow for the evaluation of deficiencies within the network defenses.

Network Countermeasures = 0

Overall Severity:

(Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity

**(1 + 0) – (0 + 0) = 1**

## DEFENSIVE RECOMMENDATIONS:

Security recommendations are as follows:

- Unauthorized software should be removed
- The latest vendor patches/fixes should be applied
- Unnecessary services should be disabled
- Logging/auditing should be enabled
- The system should be placed behind a perimeter firewall
- A host-based firewall should be installed
- Unused ports should be blocked
- A network IDS should be installed
- A strict security policy should be enforced

Also note the article on ITWorld.com, "Gartner recommends dropping IIS" (http://www.itworld.com/AppDev/3262/IDG010926IIS/)[35], in which both the Gartner Group's recommendation to "drop" IIS and Microsoft's defense of its IIS product are referenced.

## MULTIPLE CHOICE TEST QUESTION:

What type of activity is displayed in this capture?

a) Normal web type traffic
b) "Back-scatter" from a Denial of Service attack
c) Scanning for an open mail relay
d) Scanning for web servers

Answer - The best answer is (d). From an excerpt on Network ICE's web site (http://www.networkice.com/Advice/Intrusions/2003102/default.htm)[34] describing this traffic as "This means that if you see a TCP port probe for port 80, then a hacker is most likely testing your system to see if you've installed your own web server." Furthermore, note the incrementing source ports and destination IPs, which is also characteristic of a scan.

## Detect #4 – Port 21 SYN Scan

### Log:

The following log file was posted by Mike Poor in the Incidents.Org archives (http://www.incidents.org/archives/intrusions/msg03816.html)[36] on 14 February 2002.

“Seeing two distinct scanning characteristics: 1st ... 'normal' TCP/IP ephemeral to server port combinations with incrementing port numbers on the client side; and then (as in the second set of scan data, we have a few 'normal' mixed with reflexive port combinations. Any one see this lately? Strange, as you normally see either the scan come in all as 'normal' TCP/IP behavior for a scan, or all reflexive indicative of a scanning script. just curious, Mike Poor”

```
Feb 13 19:20:21 66.35.145.163:2963 -> MY.NET.WORK.4:21 SYN ******S*
Feb 13 19:20:21 66.35.145.163:2967 -> MY.NET.WORK.8:21 SYN ******S*
Feb 13 19:20:21 66.35.145.163:2966 -> MY.NET.WORK.7:21 SYN ******S*
Feb 13 19:20:21 66.35.145.163:2964 -> MY.NET.WORK.5:21 SYN ******S*
Feb 13 19:20:21 66.35.145.163:2965 -> MY.NET.WORK.6:21 SYN ******S*
Feb 13 19:20:21 66.35.145.163:2968 -> MY.NET.WORK.9:21 SYN ******S*
Feb 13 19:20:21 66.35.145.163:2969 -> MY.NET.WORK.10:21 SYN ******S*
Feb 13 19:20:22 66.35.145.163:2974 -> MY.NET.WORK.15:21 SYN ******S*
Feb 13 19:20:32 66.35.145.163:1038 -> MY.NET.WORK.10:21 SYN ******S*
Feb 13 20:38:49 66.24.199.54:21 -> MY.NET.WORK.4:21 SYN ******S*
Feb 13 20:38:50 66.24.199.54:3968 -> MY.NET.WORK.6:21 SYN ******S*
Feb 13 20:38:49 66.24.199.54:21 -> MY.NET.WORK.5:21 SYN ******S*
Feb 13 20:38:50 66.24.199.54:3969 -> MY.NET.WORK.7:21 SYN ******S*
Feb 13 20:38:50 66.24.199.54:3970 -> MY.NET.WORK.8:21 SYN ******S*
Feb 13 20:38:50 66.24.199.54:3971 -> MY.NET.WORK.10:21 SYN ******S*
Feb 13 20:38:49 66.24.199.54:21 -> MY.NET.WORK.9:21 SYN ******S*
Feb 13 20:38:49 66.24.199.54:21 -> MY.NET.WORK.16:21 SYN ******S*
Feb 13 20:38:49 66.24.199.54:21 -> MY.NET.WORK.15:21 SYN ******S*
```

### SOURCE OF TRACE:

This capture came from a posting by Mike Poor in the Incidents.Org archives (http://www.incidents.org/archives/intrusions/msg03816.html)[36] on 14 February 2002. The source appears to be from his employer’s network.

### DETECT GENERATED BY:

Although not stated, this capture appears to be from SNORT.

## PROBABILITY THAT THE SOURCE ADDRESS WAS SPOOFED:

The source IP was most likely not spoofed. This appears to be a SYN scan on port 21 that is looking for a particular response from a system, thus indicating that it might be vulnerable. This requires the ability to receive those responses, hence the use of TCP and the assumed 3-way handshake, which supports the conclusion that that the source IP was not spoofed.

## DESCRIPTION OF THE ATTACK:

This appears to be a port 21 SYN scan. The incrementing source ports, and corresponding destination IPs, that contain SYN flags within a short amount of time support this assessment. Also, because this was posted as "scan" activity, and no corresponding SYN-ACK traffic was noted, I must assume that a 3-way handshake was not completed. Of notable interest though is that at the end of this detect the originating (source) port changes for a limited number of SYN packets. Looking at the earlier capture, many of those destination IPs that are receiving the source port 21 packets had already received an ephemeral port packet. This would indicate that the originator received a response from the destination and thus altered its scan accordingly, or that the scanning mechanism has the ability to adjust its scanning techniques and can incorporate reflective port scans, as was stated by Mike Poor in his comments. Also, destination IP MY.NET.WORK.10 was hit 3 times in the capture that was posted. Assuming that the first three net blocks are the same, this may warrant further investigation by the owners of that system/network.

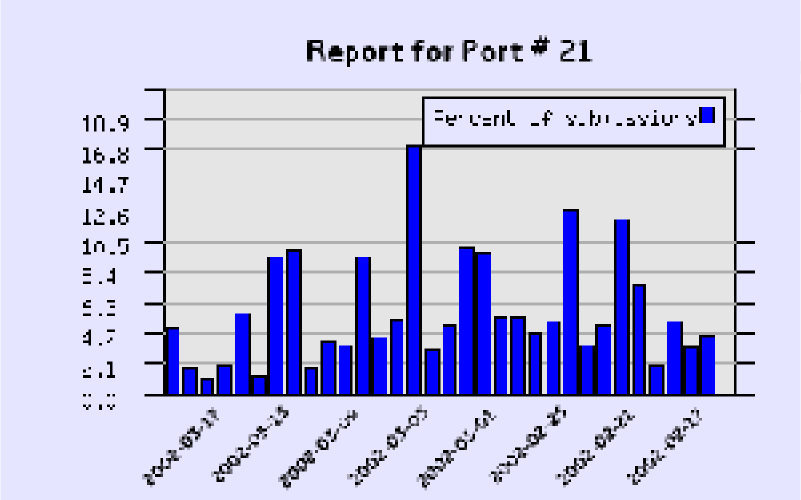
This activity was most likely carried out by a scanning tool such as the popular NMAP, of which, according to the Nmap.Org website (http://www.nmap.org/nmap/index.html)[27], "was designed to rapidly scan large networks, although it works fine against single hosts" or Grim's Ping (http://grimsping.cjb.net/).[37] An excerpt from ZDNet.com (http://www.zdnet.com/products/stories/reviews/0,4161,2651662,00.html)[38] lists a few of the free port scanners that are available and that require little user expertise.

## ATTACK MECHANISM:

Nmap.Org's website (http://www.nmap.org/nmap/index.html)[27] also gives the following description of its mechanics: "Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers, and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL." This same concept is used by many of the other scanning tools and appears to be in widespread use.

## CORRELATIONS:

A brief introduction to FTP and some of its related issues can be found at DSHIELD.Org (http://www1.dshield.org/ports/port21.html).[39]



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=21)[58]

See the "WU-FTP" Resource Center (http://www.landfield.com/wu-ftpd/)[40], by the Landfield Group, which offers a fairly robust set of resources for supporting WU-FTP implementations.

A listing of FTP related RFCs/hyper-links can be found at the WU-FTP.Org web site (http://www.wu-ftpd.org/rfc/).[41]

A few of the security concerns and issues associated with FTP can be found at the following web sites:

- http://advice.networkice.com/Advice/Intrusions/2001302/default.htm[42]
- http://advice.networkice.com/Advice/Services/FTP/PASV/default.htm[43]
- http://advice.networkice.com/Advice/Phauna/Trojan_Horse/FTP/DarkFTP/default.htm[44]
- http://advice.networkice.com/Advice/Exploits/Ports/21/default.htm[45]
- http://www.google.com/search?hl=en&q=port+21+scanners[46]
- http://www.davecentral.com/browse/188/[47]
- http://www.davecentral.com/projects/grimsping1/[48]
- http://www.incidents.org/archives/intrusions/msg03441.html[49]

There are also more than 110 instances of FTP related CVE links listed at Mitre Corporation's Common Vulnerabilities and Exposures web site: http://www.cve.mitre.org/cve/downloads/full-cve.html.[50]

## EVIDENCE OF ACTIVE TARGETING:

This is a SYN scan that is looking for systems that are listening on port 21 and it is probably not targeted. Port 21 scans are quite commonplace, but because port 21 is the command channel for FTP and port 20 is the data channel, and because no port 20 traffic was reported, I do not see evidence of a compromise from this detect.

## SEVERITY:

(Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity
* (Scale: 0-5)

<u>Criticality</u> – My basis for scoring criticality is determined by the operational or functional role a system plays in a given network. (Criticality = Impact + Contingency Capability)

The specific role of this system is not stated, however, because it is located in an assumed work environment, I am making my Severity determinations based on the concept that this system is a used to perform intrusion detection. Therefore, the operational impact of this machine has a moderate bearing on the overall functionality of the network. Had this host been compromised, its posture would not have necessarily resulted in an operational impact to the internal network infrastructure.

Criticality = 2.

<u>Lethality</u> – I use this section to determine the lethality of the attack itself, thereby minimizing the subjective nature inherent when re-computing the score of each attack as it is applied to the varying roles of any given system within a network. I have done this to provide for a standardized baseline that, when combined with the other criteria, results in a more consistent and meaningful determination of the Severity, or impact, to that network. (Lethality = Probability of success + Potential for loss or damage)

My basis for scoring Lethality is to determine the level of access gained, or the loss of functionality that would result, from a successful attack. Also taken into consideration is the likelihood that this attack could or would be successful. By doing this, I allow for the Criticality of the system to counterbalance, or further support, the overall determination of its Severity. Hence, a high-level attack on a non-critical system becomes averaged out through the overall formula. I have found this to be an effective method when performing risk analysis.

In this case, the FTP traffic did not cause any damage, however, in the event that a subsequent attack had been successful the effect may have been reconnaissance, file sharing, and possibly root access, thus supporting an elevated score.

Lethality = 3.

<u>System Countermeasures</u> – My basis for scoring System Countermeasures is to determine the Actual Configuration of the system at the time of the attack versus the Most Secure and up-to-date configuration that was available. This allows me to objectively compare and contrast any deficiencies within my defensive posture at the system level.

In this case the countermeasures of the capture device are not stated. But because of the assumption that it is used to perform intrusion detection, I am also assuming that the countermeasures are above average. This results in a reasonable Actual Configuration when compared to the Most Secure Configuration.

System Countermeasures = 3

Network Countermeasures – My basis for scoring Network Countermeasures is to determine the actual defensive measures that were in place, and their effectiveness, that existed on the network at the time of the attack versus those measures that might have prevented this traffic from reaching inside the infrastructure. This allows me to objectively compare and contrast any deficiencies within my defensive posture at the network level.

Once again, assuming the objective of this machine was to perform intrusion detection, in an unsecured posture/environment, the existing network countermeasures provided no protection for the target machine. This intentionally resulted in a low score and did not allow for the evaluation of deficiencies within the network defenses.

Network Countermeasures = 0

Overall Severity:

(Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity

**(2 + 3) – (3 + 0) = 2**

## DEFENSIVE RECOMMENDATIONS:

Defensive recommendations for intrusion detection devices tend to be varied depending on the placement, design, and role of the device within the network infrastructure. Therefore the following general guidelines would still apply, but may need to be modified depending on the organizations intent (e.g. Honey-Pot, etc.)

Security recommendations are as follows:

- Unauthorized software should be removed
- Do not allow anonymous logins or guest accounts
- The latest vendor patches/fixes should be applied
- Unnecessary services should be disabled
- Logging/auditing should be enabled
- The system should be placed behind a perimeter firewall
- A host-based firewall should be installed
- Unused ports should be blocked
- A network IDS should be installed
- A strict security policy should be enforced

**MULTIPLE CHOICE TEST QUESTION:**

What type of activity is displayed in this capture?

a) A probe for FTP services
b) Normal FTP type traffic
c) Scanning for open proxy servers
d) Scanning for DNS servers

Answer - The best answer is (a). Port 21 is the well known port for FTP and the incrementing ports/IPs, as well as the short time frame in which the traffic occurred, indicates scan activity that is looking for targets of opportunity.

## Detect #5 – Port 4400

### Log:

The following log file was posted by Simon Roper in the Incidents.Org archives (http://www.incidents.org/archives/intrusions/msg03824.html)[51] on 15 February 2002.

**"new at this... not sure what to make of this.**

- *Date*: Fri, 15 Feb 2002 09:53:33 -0000
- *From*: Simon Roper <Simon.Roper@xxxxxxxxxxxxx>
- *Subject*: new at this... not sure what to make of this.

```
Hi,

I have been checking our syslogs daily and have seen the
following entries
daily.  I have done some checks on the web for ports 4400 and
the other
ports, to no avail. Not sure what to make of it.. Any ideas?

Feb 14 12:46:38,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15912
Feb 14 12:47:10,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15942
Feb 14 12:47:38,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/80 dst outside:aa.bb.226.dd/15890
Feb 14 12:47:42,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15912
Feb 14 12:48:02,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15929
Feb 14 12:48:10,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15943

[output cut…]
```

```
[output cut…]

Feb 14 12:54:34,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15943
Feb 14 12:54:38,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15942
Feb 14 12:54:46,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/80 dst outside:aa.bb.226.dd/15890
Feb 14 12:55:10,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15912
Feb 14 12:55:30,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15929
Feb 14 12:55:38,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15943
Feb 14 12:55:42,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15942
Feb 14 12:56:34,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15929
Feb 14 12:56:42,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15943
Feb 14 12:56:46,  , 3, %PIX-3-106011: Deny inbound (No xlate)
tcp src
outside:168.167.25.2/4400 dst outside:aa.bb.226.dd/15942

Simon Roper”
```

**SOURCE OF TRACE:**

This capture came from a posting by Simon Roper in the Incidents.Org archives (http://www.incidents.org/archives/intrusions/msg03824.html)[51] on 15 February 2002.  The source appears to be from his employer’s network.

## DETECT GENERATED BY:

This capture appears to come from a Cisco PIX Firewall.

## PROBABILITY THAT THE SOURCE ADDRESS WAS SPOOFED:

The source IP was most likely not spoofed. This appears to be a scan from port 4400, and port 80, that is looking for a particular type of system. This requires the ability to receive those responses, hence the use of TCP and the assumed 3-way handshake, which supports the conclusion that that the source IP was not spoofed.

Alternately, this could be back-scatter from someone spoofing our IP address in an attack against the source IP, in which the source as seen here would still not be spoofed.

## DESCRIPTION OF THE ATTACK:

The traffic is originating on port 4400 and alternates to port 80 at just about every 5th packet. The incrementing source ports within a short amount of time indicates that this is scanning activity, of which was blocked at the firewall. Looking at the capture it is difficult to determine if the destination IP is remaining the same or alternating along with the destination port numbers, due to Simon's sanitizing of his IP addresses. If his IP is remaining constant, as is indicated by the continuous ".dd", then I would chalk this up to a scan. There does not appear to be enough traffic, within a given time frame, to support a denial of service (DoS) theory against Simon's network.

An alternative is that the traffic in this capture is actually back-scatter, in which we see the returned SYN-ACK from a source that has been sent a packet(s) with our spoofed IP address. I do not know if these are actually SYN-ACK packets or if egress filtering is being used on this network, so I can not investigate this possibility any further.

A third possibility could be that port 4400 has been associated with the Undernet IRC community and this may be a system that is looking for another Undernet IRC server with which to connect. However, the incrementing destination ports, alternating source ports, and unchanging destination IP leads me to believe that this is most likely someone scanning from a box which happens to be using (or has chosen to use) those particular source ports.

## ATTACK MECHANISM:

The Undernet Chat Network (http://www.undernet.org/show_news.php?main_n_id=12) [52] posted a virus alert on 01 March 2002 that a mIRC virus is being propagated throughout the Undernet. Their web site explains how you can infect yourself if you type a certain command, but, because of this method of propagation, this does not appear to be what was captured at Simon's firewall.

It is more likely that this is part of a scan than that of a discovery probe for IRC servers. This capture did not provide enough information for me to determine which tool might have been used, however, this type of scanning is often accomplished using common and freely available tools such as Nmap (http://www.nmap.org/nmap/index.html)[27] or Hping (http://www.hping.org/) [53]. Because the firewall blocked the traffic, and I assume that no other related traffic was observed, the responses that the originator received could be used for reconnaissance purposes, which is good reason to null route traffic if/when possible.

It is also possible that these are SYN-ACK responses to packets in which Simon's IP address had been spoofed. The information provided here does not prove nor disprove this possibility.

A third and less likely option is that of a Denial of Service (DoS) against Simon's network. This is not as probable because there are easier and more effective ways to accomplish a DoS, however, this possibility does exist.

**CORRELATIONS:**

ZDNet.com (http://www.zdnet.com/products/stories/reviews/0,4161,2651662,00.html) [38] lists a few of the free port scanners that are available and that require little user expertise.

An overview of both the Nmap and HPING scanning tools is provided below:

- **Nmap** (http://www.insecure.org/nmap/) [54]: "Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks… to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers, and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL."

- **HPING** (http://www.hping.org/) [53]: "hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.
  While hping was mainly used as a security tool in the past, it can be used in many ways by people that don't care about security to test networks and hosts. A subset of the stuff you can do using hping:
  - Firewall testing
  - Advanced port scanning
  - Network testing, using different protocols, TOS, fragmentation
  - Manual path MTU discovery

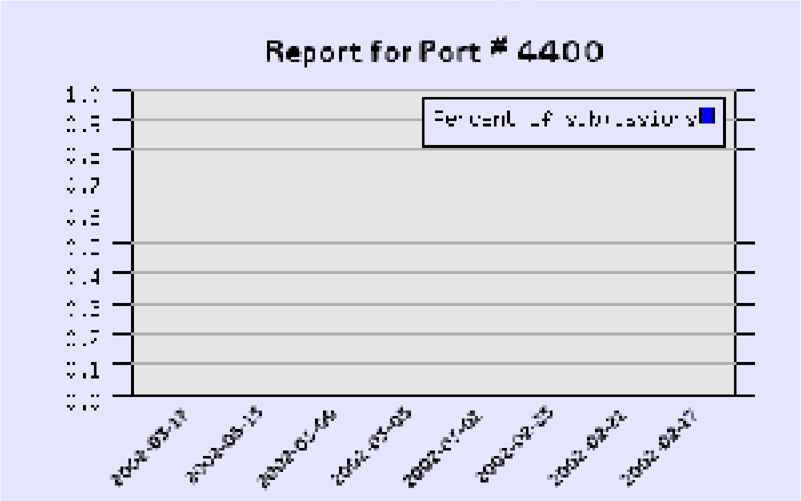
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

hping can also be useful to students that are learning TCP/IP.
Hping should work without problems on the following unix-like systems:

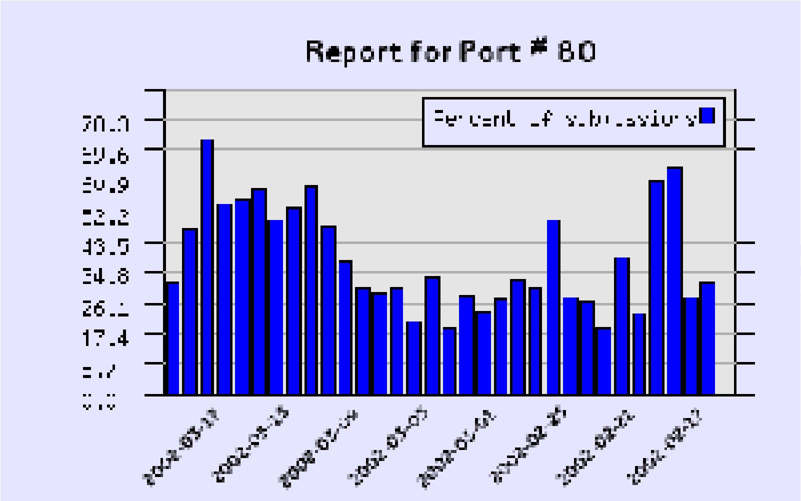
- Linux, FreeBSD, NetBSD, OpenBSD, Solaris

The next generation of hping is hping3, under development."

For more information on the Undernet, reference the Undernet User Committee web site http://www.user-com.undernet.org/[55] and the Undernet Chat Network web site http://www.undernet.org/.[56] These sites contain explanations and configuration examples that shed some light on what is expected from/within the Undernet community/servers. See also the mIRC virus alert on the Undernet Chat Network web site, posted at http://www.undernet.org/show_news.php?main_n_id=12.[52]



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=4400)[57]



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=80)[33]

## EVIDENCE OF ACTIVE TARGETING:

Although port/network scanning has become quite commonplace, if the destination IP address is indeed a constant then this would appear to be a targeted scan or possibly SYN-ACK response packets. This warrants investigation and some protective measures to ensure that the box is not "scanned today, gone tomorrow".

## SEVERITY:

(Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity
* (Scale: 0-5)

Criticality – My basis for scoring criticality is determined by the operational or functional role a system plays in a given network. (Criticality = Impact + Contingency Capability)

The specific role of this system is not stated, however, because it is located in an assumed work environment, I am making my Severity determinations based on the concept that this system was targeted because it was of value to the owner or to someone else. Therefore, the organizational impact of this machine may have a moderate/heavy bearing on the overall functionality of the network or organization. Had this host been compromised, its role may have had a significant operational impact.

Criticality = 5.

Lethality – I use this section to determine the lethality of the attack itself, thereby minimizing the subjective nature inherent when re-computing the score of each attack as it is applied to the varying roles of any given system within a network. I have done this to provide for a standardized baseline that, when combined with the other criteria, results in a more consistent and meaningful determination of the Severity, or impact, to that network. (Lethality = Probability of success + Potential for loss or damage)

My basis for scoring Lethality is to determine the level of access gained, or the loss of functionality that would result, from a successful attack. Also taken into consideration is the likelihood that this attack could or would be successful. By doing this, I allow for the Criticality of the system to counterbalance, or further support, the overall determination of its Severity. Hence, a high-level attack on a non-critical system becomes averaged out through the overall formula. I have found this to be an effective method when performing risk analysis.

In this case the scan did not cause any damage, however, because it may have been targeted traffic and the perimeter defenses may have been identified, this supports a low/moderate score.

Lethality = 2.

System Countermeasures – My basis for scoring System Countermeasures is to determine the Actual Configuration of the system at the time of the attack versus the Most Secure and up-to-date configuration that was available. This allows me to objectively compare and contrast any deficiencies within my defensive posture at the system level.

In this case the countermeasures of the targeted system had no bearing on the outcome of this activity and they were not stated. But because of the assumption that it is an operational system of some value, I am also assuming that the countermeasures are above average. This would result in a reasonable Actual Configuration when compared to the Most Secure Configuration.

System Countermeasures = 4

Network Countermeasures – My basis for scoring Network Countermeasures is to determine the actual defensive measures that were in place, and their effectiveness, that existed on the network at the time of the attack versus those measures that might have prevented this traffic from reaching inside the infrastructure. This allows me to objectively compare and contrast any deficiencies within my defensive posture at the network level.

Once again, assuming this machine was performing in an operational capacity, its position within the infrastructure and network defenses provided perfectly adequate protection in this scenario. It appears as though the firewall was configured to deny all traffic that wasn't explicitly permitted. This resulted in a high score, but did not allow for the evaluation of other deficiencies within the network's defenses. Egress filtering, if not already performed, is recommended.

Network Countermeasures = 5

Overall Severity:

(Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity

**(5 + 3) – (4 + 5) = -1**

## DEFENSIVE RECOMMENDATIONS:

The Overall Severity score indicates that, under this assumed configuration, an attack would have had a low probability of success. However, because this configuration is assumed and the system is deemed operationally valuable, the following security recommendations should be implemented.

Security recommendations are as follows:

- Unauthorized software should be removed
- Do not allow anonymous logins or guest accounts
- The latest vendor patches/fixes should be applied
- Unnecessary services should be disabled
- Logging/auditing should be enabled
- The system should be placed behind a perimeter firewall
- Perform egress filtering
- A host-based firewall should be installed
- Unused ports should be blocked and null routed
- A network IDS should be installed
- A strict security policy should be enforced

## MULTIPLE CHOICE TEST QUESTION:

What type of analysis can be inferred from this capture?

e) The source is vulnerable to port 4400 traffic
f) The source is vulnerable to port 80 traffic
g) The source is under a Denial of Service attack
h) The destination is being targeted

Answer - The best answer is (d). Because the destination IP address does not change, there is a strong possibility that it is being targeted. This detect alone is not enough to determine if the source is actually under a DoS attack.

# Appendix A

## References (Assignment 1)

[1] McGann, Seth. "Hacking Blizard's Starcraft." URL: http://www.digivill.net/~minus/starhack.txt (21 January 2002).

[2] Staniford-Chen, Stuart. "Re: Port 6112." 20 March 2000. URL: http://archives.neohapsis.com/archives/incidents/2000-03/0169.html (21 January 2002).

[3] Sage, John. "[Logs] tcp:23, tcp:6112 FSGS, udp:137, tcp:21 probes at FinchHaven for 12/16/2001." 17 December 2001. URL: http://www.incidents.org/archives/intrusions/msg02922.html (21 January 2002).

[4] Battle.Net. URL: http://www.battle.net/ (21 January 2002).

[5] NetworkICE.Com. "Port 6112 BattleNet." URL: http://advice.networkice.com/Advice/Exploits/Ports/6112/default.htm (20 January 2002).

[6] Manion, Art. "CERT® Advisory CA-2001-31 Buffer Overflow in CDE Subprocess Control Service." January 10, 2002. CERT Coordination Center URL: http://www.cert.org/advisories/CA-2001-31.html (21 January 2002).

[7] Incidents.Org, Handler's Diary. "Port 6112/tcp Activity Report." 18 December 2001. URL: http://www.incidents.org/diary.php?id=125 (21 January 2002).

[8] Mitre.Org. "Common Vulnerabilities and Exposures." URL: http://cve.mitre.org/cve (22 January 2002).

[9] Manion, Art. "Vulnerability Note VU#172583 Common Desktop Environment (CDE) Subprocess Control Service dtspcd contains buffer overflow." 15 February 2002. CERT Coordination Center. URL: http://www.kb.cert.org/vuls/id/172583 (22 January 2002).

[10] Spencer, Chris. "Multi-Vendor Buffer Overflow Vulnerability in CDE Subprocess Control Service." 12 November 2001. Internet Security Systems. URL: http://xforce.iss.net/alerts/advise101.php (22 January 2002).

[11] Dshield.Org. "Port Report for 6112 – DTSPC." URL: http://www.dshield.org/port_report.php?port=6112 (21 January 2002).

[12] Reece, David P. “Is blocking port 111 sufficient to protect your systems from RPC attacks? Information Security Paper: ‘Rpcbind and Portmapper’.” 26 February 2000. SANS.Org, Intrusion Detection FAQ. URL: http://www.sans.org/newlook/resources/IDFAQ/blocking.htm (23 January 2002).

[13] NetworkICE.Com. “RPC TCP port probe.” URL: http://www.networkice.com/advice/Intrusions/2003016/default.htm (23 January 2002).

[14] CERT Coordination Center. “CERT® Incident Note IN-98-06 Automated Scanning and Exploitation.” 09 December 1998. URL: http://www.cert.org/incident_notes/IN-98-06.html (24 January 2002).

[15] CERT Coordination Center. URL: http://www.cert.org (23 January 2002).

[16] Zirkle, Laurie. “[LOGS] February 5, 2002 probes.” 06 February 2002. Incidents.Org. URL: http://www.incidents.org/archives/intrusions/msg03725.html (23 January 2002).

[17] Cohen, Corey F. “Vulnerability Note VU#648304 Sun Solaris DMI to SNMP mapper daemon snmpXdmid contains buffer overflow.” 14 September 2001. CERT Coordination Center. URL: http://www.kb.cert.org/vuls/id/648304 (24 January 2002).

[18] Shafer, John. and King, Brian. “Vulnerability Note VU#34043 rpc.statd vulnerable to remote root compromise via format string stack overwrite.” 29 November 2000. CERT Coordination Center. URL: http://www.kb.cert.org/vuls/id/34043 (24 January 2002).

[19] Internet Security Systems. “RPC bind service on improper port.” 04 June 1997. ISS.Net. URL: http://www.iss.net/security_center/static/330.php (24 January 2002).

[20] Mitre.Org. “CVE-1999-0189.” 22 March 2000. URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0189 (24 January 2002).

[21] Ohio State University. “RPC: Remote Procedure Call Protocol Specification Version 2.” URL: http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1057.html (24 January 2002).

[22] Ohio State University. “Binding Protocols for ONC RPC Version 2.” URL: http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1833.html (24 January 2002).

[23] Dshield.Org. “Port Report for 111 – SUNRPC.” URL: http://www.dshield.org/port_report.php?port=111 (23 January 2002).

[24] NetworkICE.Com. “Port 111 Sun RPC Portmapper.” URL: http://advice.networkice.com/Advice/Exploits/Ports/111/default.htm (24 January 2002).

[25] CERT Coordination Center. “CERT® Advisory CA-1994-15 NFS Vulnerabilities.” 23 September 1997. URL: http://www.cert.org/advisories/CA-1994-15.html (24 January 2002).

[26] Connelly, Ken. “[LOGS] Summary of large-scale portscanning detects.” 15 February 2002. Incidents.Org. URL: http://www.incidents.org/archives/intrusions/msg03828.html (20 February 2002).

[27] Nmap.Org. “Nmap Free Security Scanner.” URL: http://www.nmap.org/nmap/index.html (20 February 2002).

[28] Danyliw, Roman. and Householder, Allen. “CERT® Advisory CA-2001-23 Continued Threat of the "Code Red" Worm.” 17 January 2002. CERT Coordination Center. URL: http://www.cert.org/advisories/CA-2001-23.html (20 February 2002).

[29] CERT Coordination Center. “CERT® Advisory CA-2001-11 sadmind/IIS Worm.” 10 May 2001. URL: http://www.cert.org/advisories/CA-2001-11.html (20 February 2002).

[30] CERT Coordination Center. “CERT® Incident Note IN-99-01 "sscan" Scanning Tool.” 28 January 1999. URL: http://www.cert.org/incident_notes/IN-99-01.html (20 February 2002).

[31] Nesting, David M. “Port 80 SYN flood-like behavior.” 13 February 2002. SecurtyFocus.Com. URL: http://www.securityfocus.com/cgi-bin/archive.pl?id=75&start=2002-02-17&end=2002-02-23&mid=256047&threads=1 (25 February 2002).

[32] Dittrich, Dave. “Re: Port 80 SYN flood-like behavior.” 13 February 2002. SecurityFocus.Com. URL: http://www.securityfocus.com/cgi-bin/archive.pl?id=75&start=2002-02-17&end=2002-02-23&mid=256101&threads=1 (25 February 2002).

[33] Dshield.Com. “Port Report for 80 – HTTP.” URL: http://www.dshield.org/port_report.php?port=80 (25 February 2002).

[34] NetworkICE.Com. “TCP port probe.” URL: http://www.networkice.com/Advice/Intrusions/2003102/default.htm (25 February 2002).

[35] ITWorld.Com. “Gartner Recommends Dropping IIS.” 26 September 2001. URL: http://www.itworld.com/AppDev/3262/IDG010926IIS/ (25 February 2002).

[36] Poor, Mike. “ftp scans.” 14 February 2002. Incidents.Org. URL: http://www.incidents.org/archives/intrusions/msg03816.html (27 February 2002).

[37] grimsping.cbj/net. “Grim’s Ping making the everyday pub scanning faster and more reliable.” URL: http://grimsping.cjb.net/ (27 February 2002).

[38] Randall, Niel. “Freeware Port Scanners: Plug the Holes.” 16 November 2000. ZDNet.Com. URL: http://www.zdnet.com/products/stories/reviews/0,4161,2651662,00.html (27 February 2002).

[39] Dshield.Org. “Port 21 – FTP.” 13 February 2002. URL: http://www1.dshield.org/ports/port21.html (27 February 2002).

[40] Landfield.Com. “WU-FTPD Resource Center.” Landfield Group. URL: http://www.landfield.com/wu-ftpd/ (27 February 2002).

[41] Wu-ftpd.Org. WU-FTPD Development Group. URL: http://www.wu-ftpd.org/rfc/ (27 February 2002).

[42] NetworkICE.Com. “FTP PORT bounce to other system.” URL: http://advice.networkice.com/Advice/Intrusions/2001302/default.htm (27 February 2002).

[43] NetworkICE.Com. “PASV.” URL: http://advice.networkice.com/Advice/Services/FTP/PASV/default.htm (27 February 2002).

[44] NetworkICE.Com. “DarkFTP.” URL: http://advice.networkice.com/Advice/Phauna/Trojan_Horse/FTP/DarkFTP/default.htm (27 February 2002).

[45] NetowrkICE.Com. “Port 21 ftp.” URL: http://advice.networkice.com/Advice/Exploits/Ports/21/default.htm (27 February 2002).

[46] Google.Com. “Searched the web for port 21 scanners.” URL: http://www.google.com/search?hl=en&q=port+21+scanners (27 February 2002).

[47] DaveCentral.Com. “Port Scanners.” URL: http://www.davecentral.com/browse/188/ (27 February 2002).

[48] DaveCentral.Com. “Connectivity – Port Scanners.” URL: http://www.davecentral.com/projects/grimsping1/ (27 February 2002).

[49] McKinlay, Ken. “RE: wanadoo ftp scan for upload area.” 21 January 2002. Incidents.Org. URL: http://www.incidents.org/archives/intrusions/msg03441.html (28 February 2002).

[50] Cve.Mitre.Org. “CVE (version 20020309).” URL: http://www.cve.mitre.org/cve/downloads/full-cve.html (28 February 2002).

[51] Roper, Simon. “new at this... not sure what to make of this.” 15 February 2002. Incidents.Org. URL: http://www.incidents.org/archives/intrusions/msg03824.html (05 March 2002).

[52] Simba. “*ALERT* mIRC virus spreading around the undernet.” 01 March 2002. Undernet.Org. URL: http://www.undernet.org/show_news.php?main_n_id=12 (05 March 2002).

[53] Hping.Org. “hping.” URL: http://www.hping.org/ (04 March 2002).

[54] Insecure.Org. “Nmap.” URL: http://www.insecure.org/nmap/ (04 March 2002).

[55] User-com.Undernet.Org. “Undernet User Community.” URL: http://www.user-com.undernet.org/ (04 March 2002).

[56] Undernet.Org. “Undernet Chat Network.” URL: http://www.undernet.org/ (05 March 2002).

[57] Dshield.Org. “Port Report for 4400 - ???.” URL: http://www.dshield.org/port_report.php?port=4400 (05 March 2002).

[58] Dshield.Org. “Port Report for 21 – FTP.” URL: http://www.dshield.org/port_report.php?port=21 (15 March 2002).

# Assignment 2

# An Approach to Intrusion Analysis

## *The Design and Theory of Data Visualization Tools and Techniques*

The purpose of this paper is to inform and educate security professionals about the analytical potential of using a tool or technique that renders visual representations of the data/traffic that traverses a given network. The emphasis is on the design and theory behind such tools. Included are examples of data visualization products that are commercially available.

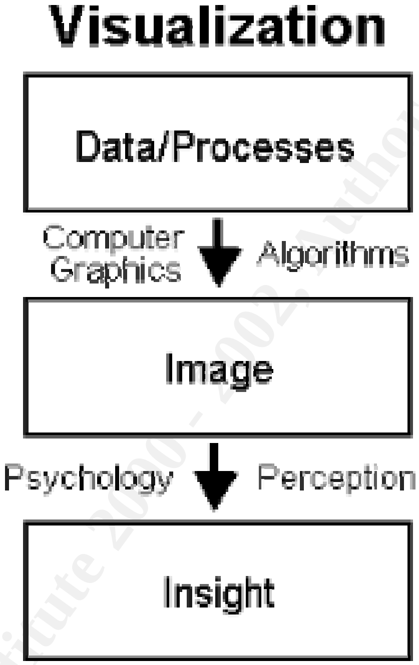
## Introduction

Networked enterprises have grown exponentially for more than a decade and have become quite unwieldy to manage and secure. These issues stem from the rapid development and implementation of technology over a short period of time. What we now have are massive heterogeneous environments that offer, and demand, more resources and bandwidth than ever before. Thus, many of our existing tools are no longer viable for managing these networks. However, there are many new tools, techniques, and approaches on the horizon that have the potential to scale to, and with, the enterprise. One such technique is that of rendering a visual representation of data for the use of inter-network traffic analysis. It is primarily my personal experience with the limitations of existing products that has prompted me to further explore the design potential of the data visualization approach.

Edward Tufte, a pioneer in the use of graphics as a means of representing information, argues that a major issue we deal with is that of presenting large amounts of information in a way that is compact, accurate, adequate for the purpose, and easy to understand. Specifically, to show cause and effect, to insure that the proper comparisons are made, and to achieve the (valid) goals that are desired. He further states that the solution is to develop a consistent approach to the display of graphics, which enhances its dissemination, accuracy, and ease of comprehension.[1] And although traffic analysis was not necessarily his intent, this approach can be applied to the data visualization techniques and tools that are being developed for this specific purpose.

## The Basis for Design and Use

To begin the design of a tool or technique you must first define the processes involved and the relationship between those processes. Khai Truong, Gregory Abowd, and Jason A. Brotherton, of the College of Computing & GVU Center at the Georgia Institute of Technology in Atlanta, Georgia defined the process of *capture and access* as “the task of preserving a record of some live experience that is then reviewed at some point in the future. Capture occurs when a tool generates an artifact that documents the history of what happened and access devices are the tools used to review the captured experiences.”[2] Furthermore, a true science of visualization must incorporate both a formal theory of computer graphics and a theory of human perception.[3a]



*From URL: http://www.ergogero.com/dataviz/dviz1.html[3a]

In intrusion analysis our capture devices are made up of intrusion detection devices (IDS) and the logs from other attached networked devices/applications. The collection and structuring of these captures is how we make the access to this stored data available for review and analysis. This is often done by collecting the captures in a database that is indexed for the timely retrieval of the stored data. The idea behind data visualization in traffic analysis is that the data may be presented to the user in a format that is optimized for ease of comprehension, and to make identifying anomalous traffic and patterns more easily recognizable. A prime benefit of being able to visualize these captures is that the new perspective often lends itself to revealing hidden patterns that may not be readily apparent from the context of a flat file or queried result. Also, the efficiency with which we can perform analysis on large amounts of data can be increased, thus maximizing those resources required when performing that analysis. Therefore, “designers constructing capture and access applications are faced with more than just issues related to different pieces of data. Beyond data, there are still the users, the devices, time and locations involved in the experience to take into consideration in the design."[2]

"These components form the minimal set of issues that need to be addressed when designing capture and access applications:

- *Who* are the users?
- *What* is captured and accessed?
- *When* does capture and access occur?
- *Where* does capture and access occur?
- *How* is capture and access performed?"[2]
- *Why* data visualization?

**The Who Dimension-**

"In understanding each person's part, designers can design systems to support specific roles in the capture and access of the experience."[2] For example, within the network and systems security arena, we have Administrators, Managers, Incident Handlers, and Intrusion Analysts, among others, who may all be a part of the "system" that is used to provide protection for a given network. Because these roles may somewhat overlap, but have different means and motivations, the design of a given tool or technique must be cognizant of those requirements that are levied by each of this supporting cast. Otherwise, the tool may be no more beneficial than those that are already in use and may just add overhead to an already time and resource intensive process.

"The issues in the *who* dimension that designers must consider are:

- The number of capturers
- The number of accessors
- The overlap between capturers and accessors
- The perspective of the capture (public, private, shared, etc.)"[2]

**The What Dimension-**

"Designers must also identify *what* to capture and make available for access; that is, determine what artifacts best document the experience. While the actual experience sets the ceiling for what is captured, the amount of information actually captured sets the ceiling for the access of the experience." "To increase the fidelity of the access experience, more streams can be captured and integrated; collectively, they can give a more accurate account of the experience."[2] The *what* portion of the design process tends to focus on the collection, or capture, of the data of which, from a data visualization standpoint, is often determined by the type of output that your particular IDS/log file uses. In network security, my experience is that we try to capture everything we possibly can, and that our greatest limitation for collecting data is either the monetary resources that have been committed to a security operation or the scale of the operation/enterprise that we are trying to protect. These issues will be discussed further in the Limitations section of this white paper.

What is of direct importance though, in visualization, is that the interface, or access, between the visualization tool and the stored captures is flexible enough to accept any format of data, to include data from multiple sources. It must also do this without seriously inhibiting the timeliness of the rendered output. If the tool is too cumbersome or resource intensive then you may limit the amount of manipulation that is possible with the rendered result. The capability of manipulating the data is the key to making a visualization technique an integral and useful part of an Intrusion Analysts repertoire.

"The issues in the *what* dimension that designers must consider are:
- The artifacts in the live experience
- The artifacts captured
- The artifacts accessed
- The fidelity of the access experience with respect to the live experience"[2]

**The When Dimension-**

"The *when* dimension deals with issues related to when capture occurs, when access occurs, and the time scale between the capture and access phases."[2] This is where we, as Intrusion Analysts and Incident Handlers, continue to demand that the capture and access devices we use provide that captured data in an environment that is as near to real-time as possible and archive that data for as long as possible. This is because the security of our networks and our approach when responding to a possible intrusion is directly related to the time and timeframe in which that traffic occurs.

"… Long-term applications store information as records for posterity. Information needs to persist for much longer periods of time than other types of applications and it may make sense to provide users with a synthesized summary of the experience with an interface that supports being able to drill down to the exact point that the user(s) want to review."[2] This "drill-down" feature would be extremely beneficial to those Handlers and Analysts that must support a large enterprise that passes enormous amounts of traffic, but may not have the manpower and resources available to perform a full, in-depth analysis of all traffic. This visual overview of network traffic can be an efficient and helpful way to identify those anomalous events that are of the highest criticality to your overall network security. But of note is that by generalizing, or aggregating, the data you may distort the fidelity and accuracy of the detail that often only exists in the more raw forms of the original data. Those details are often what are necessary in order to perform an accurate analysis of network events. That is why it is important to retain, and make available, as much detail as possible when drilling down into an event. However, most of the visualization tools I have dealt with perform their rendering based on how the data is presented to the visualization tool and any generalization, summarization, or aggregation that is performed on the original data is most often implemented by the collection or access device, not by the visual rendering tool itself. Therefore, the adverse affects of generalization are most likely to be symptoms of your collection/access devices and may be overcome through a well, thought out security strategy. However, due to the previously indicated requirement for long-term storage, some operations may be bound by the limitations of those collateral systems that support the underlying security infrastructure. This is to say that although data visualization is a most helpful tool for many varying circumstances, it is not a "silver bullet" and must be applied in the correct manner in order to be effective. A lesson learned from this is that you should never become reliant on any one tool when performing analysis. Correlation is a key ingredient in any analysis, and security is no exception. Just like any other tool, it should be one of many that aid the analyst in the performance of his or her duties.

"The issues in the *when* dimension that designers must consider are:

- The times when capture occurs
- The times when access occurs
- The frequency/periodicity of the capture and access occurrences
- The time scale difference between when capture and access happens"[2]

**The Where Dimension-**

"The *where* dimension addresses the physical locations involved in capture and access phases. Most capture and access applications handle experiences that occur in a single location. However, it is becoming more commonplace for people in many different places to collaborate and essentially share an experience remotely. Furthermore, capture and access applications must also take user mobility into consideration."[2]

Visualization of the *where* provides an excellent technique, by perspective and from a temporal display, for viewing the distribution and time-line of traffic and events that occur across an enterprise. Identifying where traffic and attempts occur can help inform the analyst of the magnitude or scope of an event, of potential distributed attacks, and of possible weaknesses in their security posture. These are some of the greatest advantages of using data visualization, versus that of a standard database or flat file, when performing intrusion detection and analysis.

"The issues in the *where* dimension designers must consider are:

- The locations of capture
- The locations of access
- The overlap of physical spaces
- The mobility of the users
- The multiplicity of locations"[2]

**The How Dimension-**

**"**The tools and methods for capturing and accessing information as well as the scale of devices form the last dimension: *how*. Capture and access applications are typically built as a confederation of tools. The number of devices that are used in a system defines the scale of devices for capture and access applications. At one end of the scale, only a single device is used in the application. A key question in the building of capture and access devices is whether the device that is doing the capture can also be used to provide the access." "In most cases, capture is often done using a number of devices and so a certain amount of effort must be devoted to coordinating these devices to work together."[2]

In this dimension the integration of the devices involved, along with the users, takes center stage. Here the numbers, locations, roles, and capabilities of the various devices must all be developed into a comprehensive and intuitive interface that is also robust and stable. The *how* of any security system may be the most complex stage of the technical design and its utility. Furthermore, when creating a visual representation of data the execution and sustainability of an application becomes that much more complex due to the additional overhead and resource requirements. This is important because the fidelity and integrity of one's resulting analysis will only be as accurate as the amount and timeliness of their data. For example, if you only capture 50% of your network traffic, or your systems are unavailable/unreliable 50% of the time, then so to will be the accuracy and timeliness of your analysis. Thus, the perceived usefulness, or trust, that the Analysts and Handlers place on the tool will be directly related to the successful implementation of these previously referenced dimensions.

"The issues in the *how* dimension designers must consider are:
- The method of capture
- The number of capture devices
- The number of access devices
- The role of the devices"[2]

**The Why Dimension-**

I have added this dimension to the design process because it is truly the driving force behind data visualization in traffic analysis. The Why is the justification and value-added portion for the practical application of this technique. The following statement summarizes the Why dimension of data visualization: Analysts need a tool that can aid them in determining whether something *counter-intuitive* is, or has, occurred. Hence, the Holy Grail of intrusion analysis. For it is not what we know, but what we don't know, that often concerns us the most.

The issues in the *why* dimensions include:
- Why develop data visualization tools/techniques
- The usefulness of the tool/technique
- The benefits of the tool/technique
- The practicality/feasibility of implementing the tool/technique

## Limitations of Existing Designs

From the dimensions and issues discussed this far, one can begin to grasp how the complexity of visualization has inherently led to many of the limitations that exist in today's commercial products. However, because these principles have progressed from a preset of initial concepts, their continuing evolution has provided a fairly thorough set of guidelines for structuring the next generation of visualization tools. Initially, many of the current products were developed as proofs-of-concept due to the stated complexity and under-perceived practical application in various fields. But, when, and where, open integration and the application of these sound design standards take focus those ensuing tools will begin to benefit many fields beyond that of the classroom and traffic analysis environments.

The first of the three greatest limitations that currently inhibit existing data visualization products is that of resources. Because data visualization products are fairly young in their development cycles, many are very resource intensive and inefficient. I have personally experienced this while running one such tool on a dual Pentium 4 Xeon processor server with 1 GB of memory, mostly when rendering medium-to-large quantities of data, or when rendering data in 3-D. This contributes to the high cost of such tools, as does the learning curve that is associated with any new application. Because this is a tangible limitation, it is also the most easily overcome. However, the money and expertise required at this stage are prohibitive to widespread implementations of these tools. The costs associated with these tools will recede over time, as will the learning curve, but until then, justifying the Why dimension's questions of feasibility and practicality will be based mostly on the potential and scalability of the tools usefulness in a given environment.

The second limitation to note is that of integration and interoperability. Herein lies the fabric that brings the concept to the desktop. Due to past experiences with different tools, the integration with the capture/access device is of extreme importance when choosing or designing a tool. Some of these tools are able to import data from a flat file, while others only accept data from a limited range of commercial vendor databases. Most of them can be ported or customized to the requirements of a given customer, however, this then leads you back to the first limitation of cost and feasibility. Those organizations with developers on staff may be able to overcome some of these issues internally, as has mine, but again, this will deter the adoption of visualization tools for many smaller enterprises. Besides the issue of accessing the data is that of defining and representing the data in a meaningful structure. Here I must give credit to those vendors whose tools I have used, because they all seem to be very flexible and with out many restrictions in this regard. However, most existing tools work with the assumption that an IDS or application has already performed some type of once over analysis that allows for the visualization of the pre-munged data. Because this scenario is probably true more often than not, I can not fault them for this decision, but security professionals should be aware that adapting raw or unaggregated data can be quite cumbersome and complex, once again degrading the feasibility in some environments.

The final and often most important limitation is that of the human factor. These are the limitations that will most affect the final design and capability of any visualization tool. These issues can only be addressed up to the point that we, as human beings, possess the ability to gain meaning from a visual stimulus. "For human beings, our potential is directly constrained by our attention, memory, and processing capabilities."[3b] From this perspective, we tend to have difficulty dealing with and processing information that exists visually in more than three-dimensions. Thus, many tools are governed by what is assumed to be the ability of the customer. This is not a limitation that necessarily has a solution or, if one does exist, will be easily overcome. Alas, we are our own weakest links… but, never underestimate human ingenuity.

## Tool and Theory Overview –

The most compelling reason for using data visualization in analysis is that of resources. Due to the scale of many enterprises, there are not enough intrusion analysts, nor is there enough time, available to cover all of the networks that are in existence today. And, at the rate the Internet and networks are expanding this trend is not likely to go away.

Although I originally started writing this paper because of my personal experiences in intrusion detection and my frustration with some of the tools that are available to analysts, my learning experience while performing the research for this paper has afforded me new insights about the challenges we face. For those of us working in large enterprises, the tools that we currently use are quickly becoming outdated and overburdened. Because the possibility of hiring more, highly qualified analysts is not always an option, new tools and techniques must be developed that allow us to maximize those resources we do have access to.

We must become conscious of the amounts of time we can allocate to analyzing traffic and detects. If we are able to investigate, or capture, 1 out of every 10 detects, then that means there are potentially 9 incidents that may go unresolved. Our goal should be to bring that number to 0, even though this may not be truly possible. In large or global enterprises, we need tools that can help us find patterns and perform correlation in a fast and effective manner. Currently I believe that a great amount of potential for doing just that exists by utilizing data visualization techniques. Postmortem analysis is a reactive process that does nothing to defend against ongoing and new/original attack methods. Through near real-time data visualization, the analysts can observe what is happening around them as the activities occur, and they can see this from different perspectives and at different levels. Databases queries and flat files are not currently capable of providing this level of hierarchical analysis form the top down. That is why I am a sincere advocate of developing technologies that allow for the near real-time visualization of network traffic for the purposes of security and management.

Currently most of the analysts I know of, that are using some sort of data visualization tool, are using it reactively to find patterns and anomalies from within sets of raw data. Herein lies another great strength of visualization. Because of the capability to view data on multiple axes, an analyst can see traffic as it occurred across time and locations, while at the same time having the data sorted by event categories and system/network roles, in conjunction with correlating between multiple source IPs.

Listed in the appendices of this assignment are examples of some data visualization tools that are commercially available. Once these tools and techniques mature, then near real-time analysis, along those lines indicated above, should become a reality. This is the direction in which, I feel, intrusion analysis/detection should be moving.

## Recommended Reading –

For further information on the origin, concepts, and design of general visualization techniques:

- "The Visual Display of Quantitative Information" by Edward R. Tufte (Graphics Press); ISBN: 096139210X.
- "Envisioning Information" by Edward R. Tufte (Graphics Press); ISBN: 0961392118.
- "Visual Explanations: Images and Quantities" by Edward R. Tufte (Graphics Press); ISBN: 0961392126.
- "Readings in Information Visualization : Using Vision to Think" by Stuart K. Card, Jock D. MacKinlay, and Ben Shneiderman (Morgan Kaufmann Publishers); ISBN: 1558605339.
- "Designing Visual Interfaces: Communication Oriented Techniques" by Kevin Mullet and Darrell Sano (Prentice Hall) ; ISBN: 0133033899.
- "Ultimate Visual Dictionary 2001" (DK Publishing); ISBN: 0789461110.
- "Toward a Perceptual Science of Multidimensional Data Visualization: Bertin and Beyond" by Marc Green, Ph.D.; URL: http://www.ergogero.com/dataviz/dviz0.html.[3]

# Appendix A

# Visual Insights' ADVIZOR™

The following is an excerpt from an informational document (.pdf) titled "ADVIZOR™: A Technical Overview" which was authored by Stephen G. Eicks, Ph.D., of Visual Insights, Incorporated (www.visualinsights.com). The document can be downloaded from the following web site:

http://www.visualinsights.com/pressroom/whitepapers/advisor_tech.pdf[4]

Although I downloaded the file on 21 January 2002, I was unable to determine when it was actually written/published. However, the information it contains is relevant and supports the objective of this practical.

## Overview –

"Visual Insights ADVIZOR is a flexible environment and platform for building interactive visual query and analysis applications. ADVIZOR consists of four parts: a rich set of flexible visual components, an in-memory data pool, data manipulation components, and container applications. Working together, ADVIZOR's architecture provides a powerful production platform for creating innovative visual query and analysis applications.

Visual Insights' ADVIZOR™ is a complete interactive environment for building visual applications. Analogous to a "visual spreadsheet," ADVIZOR enables companies to add visual query and analysis solutions to their existing decision support infrastructure. Systems now routinely collect fine-grain transaction data. By analyzing this data, i.e. understanding customer buying decisions, exploiting cross-sell opportunities, better managing brands, and leveraging limited shelf space, businesses can achieve significant advantage. The analysis tools, unfortunately, have not kept pace with ever increasing data volumes. The result is data overload and information drought, the inability to make effective business decisions because of too much data.

The idea embodied in ADVIZOR is that desktop PCs, including browser-based thin clients, have become fast enough to enable a new class of analysis and query tools that exploit interactive visualization. Previous approaches to making sense of data involved manipulating text displays such as crosstabs, running complex statistical packages, and assembling the results into reports using presentation graphics. Browsers and the web have popularized the idea that modern interfaces combine text and graphics. ADVIZOR takes this approach one step further by making the text and graphics interactive, applying color to encode information, and enabling the user to pose and resolve queries dynamically using the mouse. Broadly speaking, visual tasks may be divided into three classes.

1. *Presentation Graphics* such as is included with MS PowerPoint or even spreadsheet graphics. These generally consist of bars, pies, and line charts that are easily populated with static data and drop into printed reports or presentations. The next version of presentation graphics, exemplified by VRML-based browsers, enriches the static displays with a 3D information landscape. Users can then navigate through the landscape and animate it to display time-oriented information. This class of visualizations is generally useful for answering "what" questions and for conveying results.

2. *Visual Interfaces* for Information Access are focused on enabling users to navigate through complex spaces such as the web and find nuggets of information. Supported user tasks involve searching, back tracking, and history logging. User Interface techniques attempt to preserve user context and support smooth transitions between locations.

3. *Full Visual Query and Analysis* systems such as ADVIZOR that combine the excitement of presentation graphics with the ability to probe, drill-down, filter, and manipulate the display to answer the "why" questions.

The difference between answering a "what" and a "why" question involves an interactive operation. For example, in a set of sales data the answer to a "what happened" might be that sales went up. Answering the why question might involve an interactive operation such as drilling-down, drilling-across, hiding, or rescaling to discover that one product had an exceptional quarter. Both of these are "single table" questions since they can both be answered from a data table showing sales by product. Going further requires linking multiple data tables, e.g. relating the sales table to the transaction table. It might be that sales went up because of a single huge order. For a busy analyst it is important to provide fast and efficient techniques to navigate through the many varied possibilities."[4]

## Summary –

"There are three unique and compelling aspects to ADVIZOR's technology:

- Rich interactive Visual Components that are linked by selection, focus, data, and color

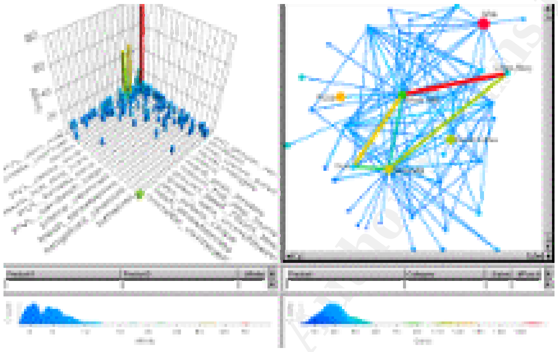
- Data Pool containing multiple, linkable tables for visualization

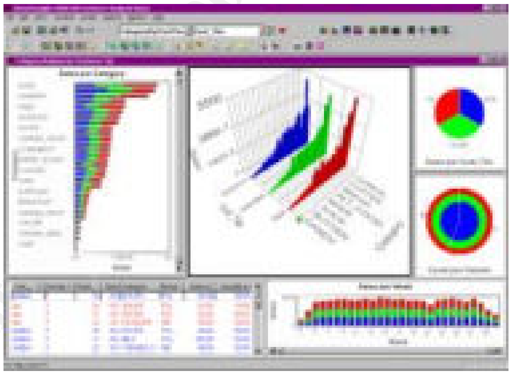
- ADVIZOR and ADVIZOR/2000 containers that host the components and function as visual workspaces.

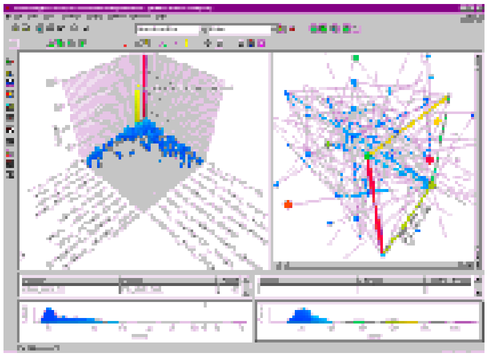
Together the different aspects of ADVIZOR function as a powerful environment for visual query and analysis."[4]

## Screen Captures –

The following screen captures can be found at the Visual Insights web site: http://www.visualinsights.com/base_pages/mainhtml.asp?level1=four&level2=three&level3=one&picked=4-1-1[5]







# Appendix B

## SecureScope™
## by Secure Decisions,
## a Division of Applied Visions Inc.

The following is an excerpt from a Power Point presentation titled "Visualization for Information Security Situational Awareness" which was posted on the Secure decisions web site (http://www.securedecisions.com/documents/SecureScopeOverview022602.ppt).[6]

## Overview –

"SecureScope visually correlates data from multiple sensors in an RDBMS. SecureScope interfaces with any common RDBMS.

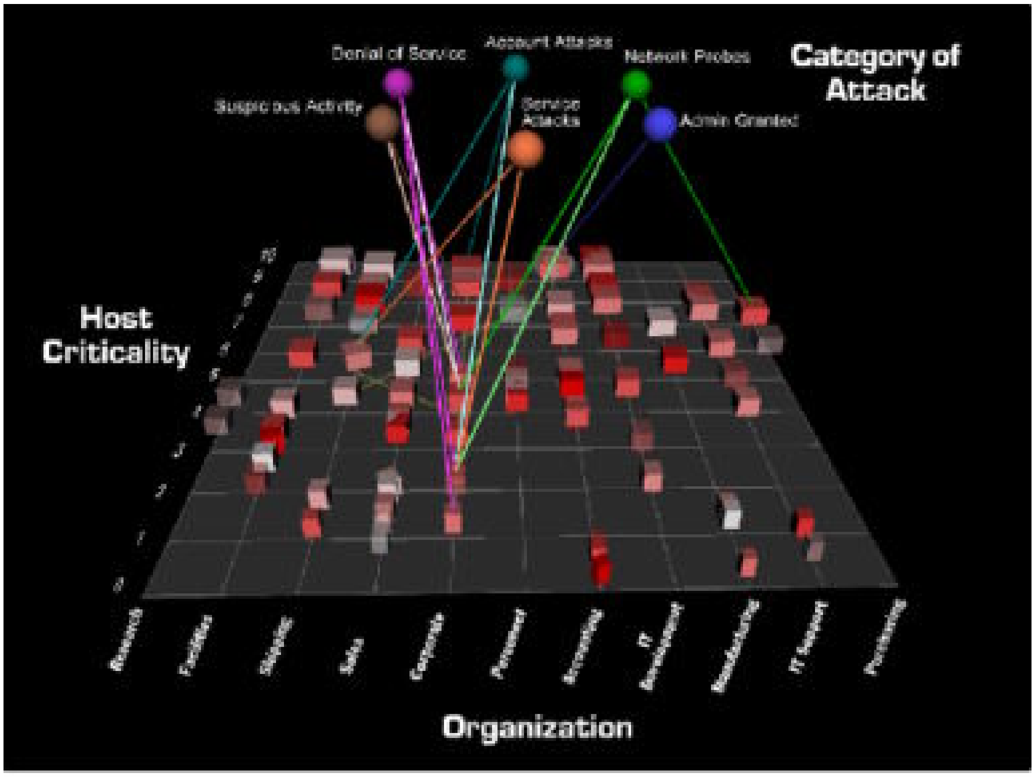
SecureScope Goals:

- Improve analysts situational awareness
  - Speed detection of patterns
  - Reduce mental workload
- Get more value from existing sensors (e.g. IDS, firewalls)
- Leverage people's innate ability to detect visual patterns
- Reside on an affordable platform
- Be easy to use"[6]

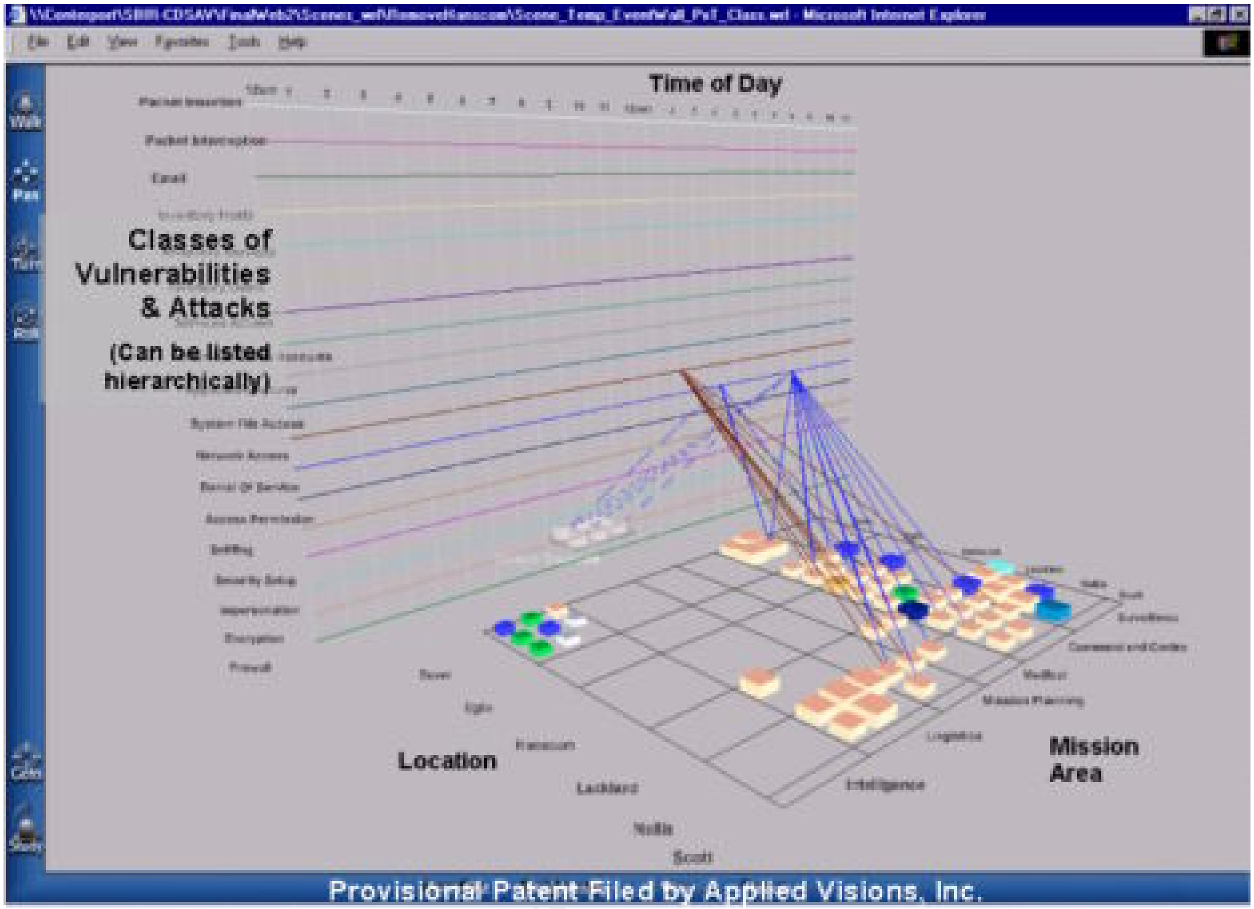
## Summary –

"Targeted users:

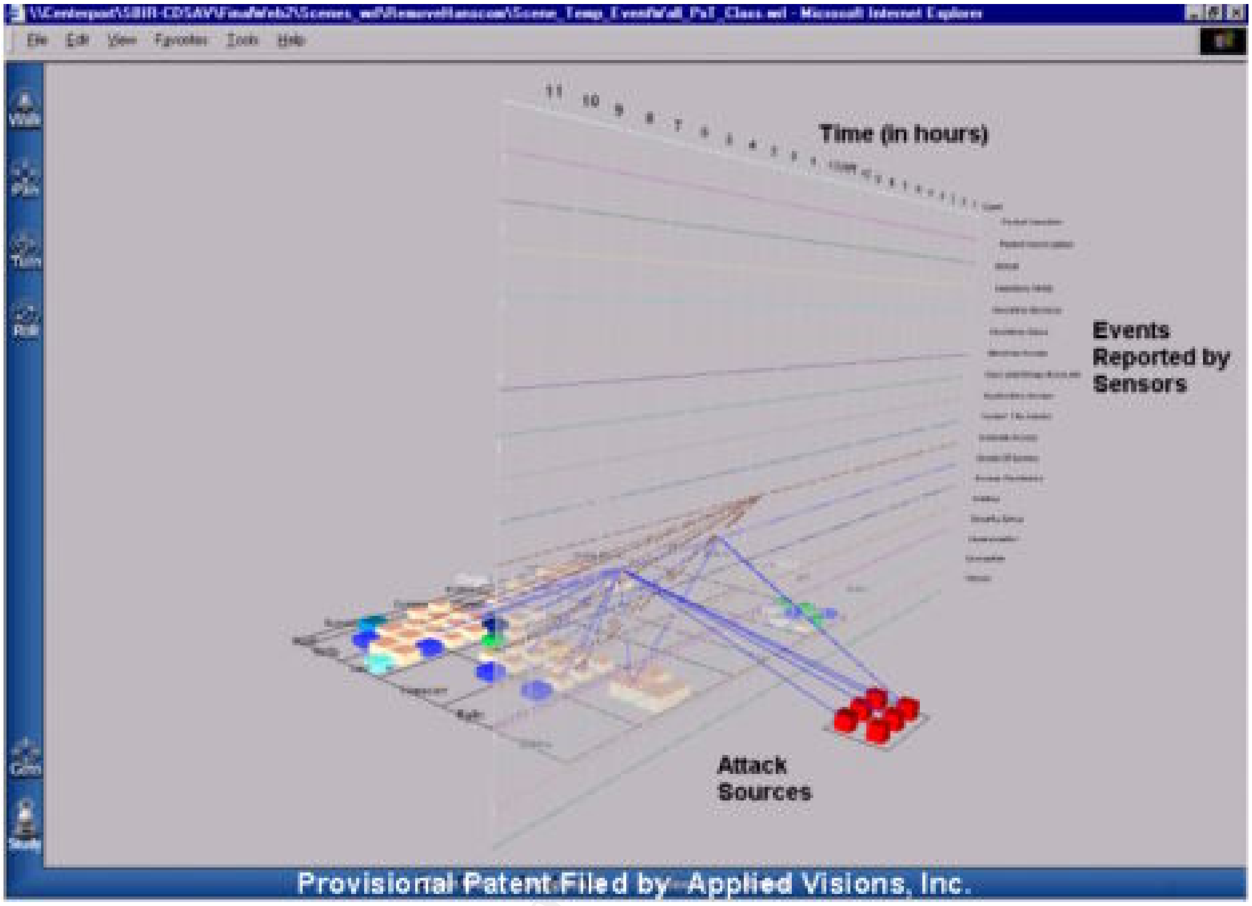
- Information Security Officers and Network Administrators
- Information Security Analysts and Consultants
- Network Operations Centers and Security Monitoring Centers"[6]



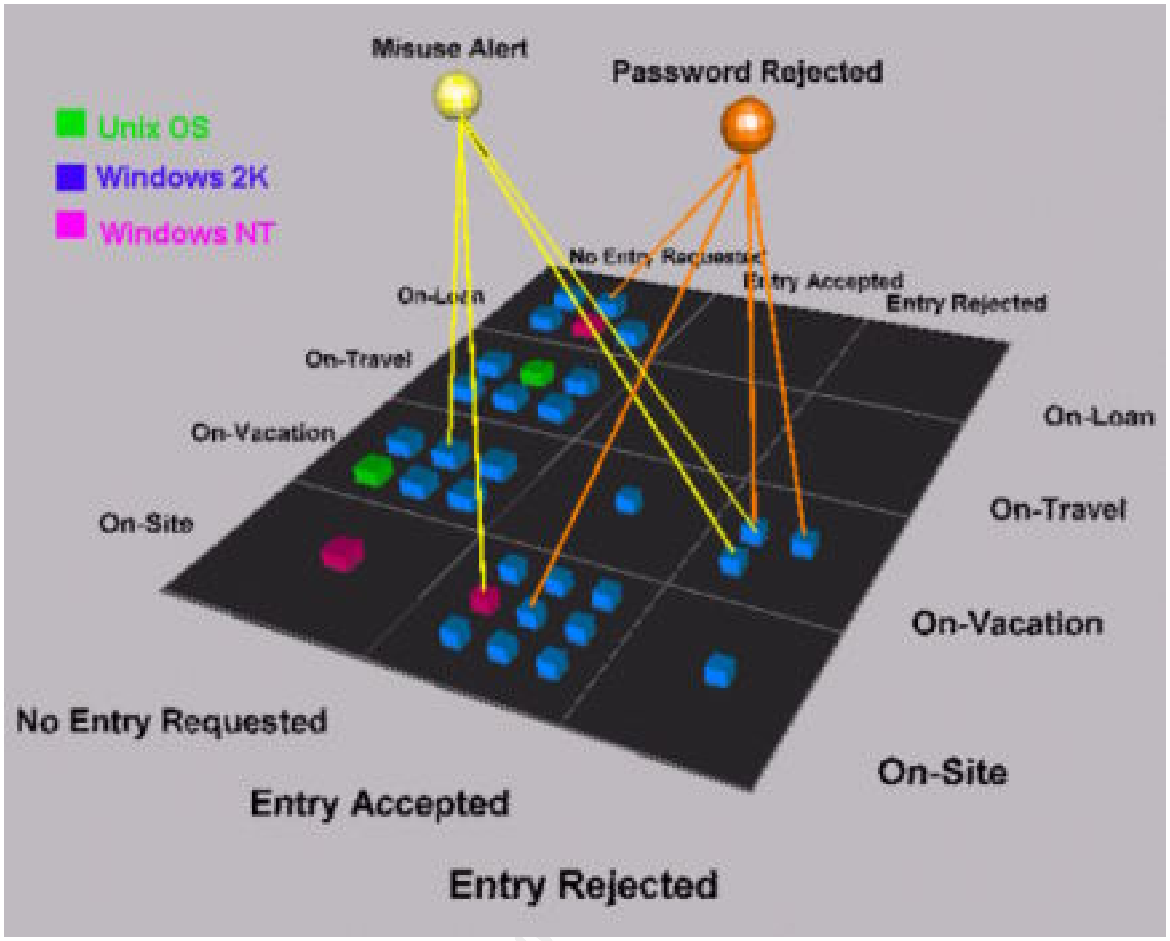
* 3-D visual correlation enhances discovery of patterns in security events.



*Temporal wall links security events with the targets of those events in time.[6]


\\Centerpoint\SBIR-CDSAV\FinalWeb2\Scenes_wrl\RemoveHanscom\Scene_Temp_EventWall_PsT_Class.wrl - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Walk
Pan
Turn
Roll
Goto
Study
11 10 9 8 7
Time (in hours)
Events Reported by Sensors
Attack Sources
Provisional Patent Filed by Applied Visions, Inc.

*Rear grid can show attacker characteristics or sensor sources.[6]



*Visualization of suspicious insider events.[6]

# Appendix C

## "Open e-Security Platform"
## (e-Security Incorporated)

as written by Winn Schwartau

Because I don't have personal experience with e-Security Incorporated's Open e-Security Platform, all of the following ideas and quotations are derived from a white paper titled "Solving 'Dumb Days' with Security visualization" which was written by Winn Schwartau and is posted on the Ebiz.Net web site:
http://e-serv.ebizq.net/shared/white_papers.jsp?ID=schwartau_1.pdf[7]

Note that in order to download this paper you must be a registered Ebiz.Net user with a login and password. Although I downloaded the white paper on 17 March 2002, I was unable to determine when it was actually written/published. However, the information it contains is relevant and supports the objective of this practical.

"Winn Schwartau is President of Interpact, Inc., a security awareness consulting firm, the founder of Infowar.Com (www.infowar.com), and the author of numerous books and articles about information security including "Time Based Security," and his latest, "CyberShock." He can be reached at winns@gte.net."[7]

## Overview –

Mr. Schwartau suggests that the two precepts of intrusion detection in "Time-Based Security" are:

> "1. Discover that the bad guy is doing bad guy things as quickly as we can. A door alarm will detect that the seal has been broken in less than a second. We need similar approaches in information security."[7]
>
> "2. Then we have to react to the online threat immediately to mitigate the potential for damage."[7]

He supports his "Time-Based Security" theory on the premise that "Time-Based Security invites network performance and diagnostic monitors to complement other detection methods in gathering a more complete picture of the network. Monitoring tools are effective at identifying software at nodes in the network and often are used for copyright/license compliance. However, the same mechanisms are applicable for identification of miscreant software at the user's workstation." "When protection products integrate detection, the overall state of network defense will rise significantly." "Nodal Detection should be added at more nodes in a network to improve security. Monitoring decentralized nodal system activity can provide massive amounts of information to establish norms, trends, and systemic errors when the sampling is sufficient."[7]

Thus, the same concept, when used in relation to traffic analysis, is further supported in this example: "Say a network usually operates its T-1 to the Internet at 30 percent utilization with bursts to 85 percent. Then one night, it sits at 72 percent for hours on end. If it were my company, I would like to know what the heck was going on. Wouldn't you? If Bob and Alice never talk to each other within the company network, yet over a one-week period they suddenly exchange 48 e-mails, something has changed. If John's profile says he rarely uses the Internet but he suddenly sends large amounts of data to SpiesRUs.com.cn (cn = china), as a manager I would quickly be suspicious. In all of these cases, the suspicion is raised by behavior detected through traffic analysis, not the actual contents of the communications. Traffic analysis tools make an ideal detection mechanism if the baseline profiles are reasonably set, and the reaction channel can be whatever management chooses it to be."[7]

At this point it is important to note that there are legal implications of monitoring certain types of communications, but because that is not the objective of this paper, it is only mentioned here to bring it to the attention of security professionals.[7]

Mr. Schwartau cites that the problem with collecting enormous amounts of raw data stems from the amount of time, versus the optimal time-frame for incident response that is required to process and analyze that data. The longer this process takes, the more time attackers have to do malicious things before an organization can respond. Hence, raw data alone provides little to no time relevant information, or knowledge, because it gets "stuffed in a drawer" until someone can take the time to manually analyze that data. And, "… that gargantuan task is a nightmare on the brain, the eyes, and an exercise in futility." Which brings us to the problem of "how do we handle the massive amounts of real-time data… and make decisions on what to do?"[7]

He argues that "pictures of dynamic events occurring in multiple spots across wide spans of network space are… infinitely easier than manual eye-to-brain diagnosis of network traffic patterns." And that "pictures of security-relevant events make decent network security administration feasible."[7]

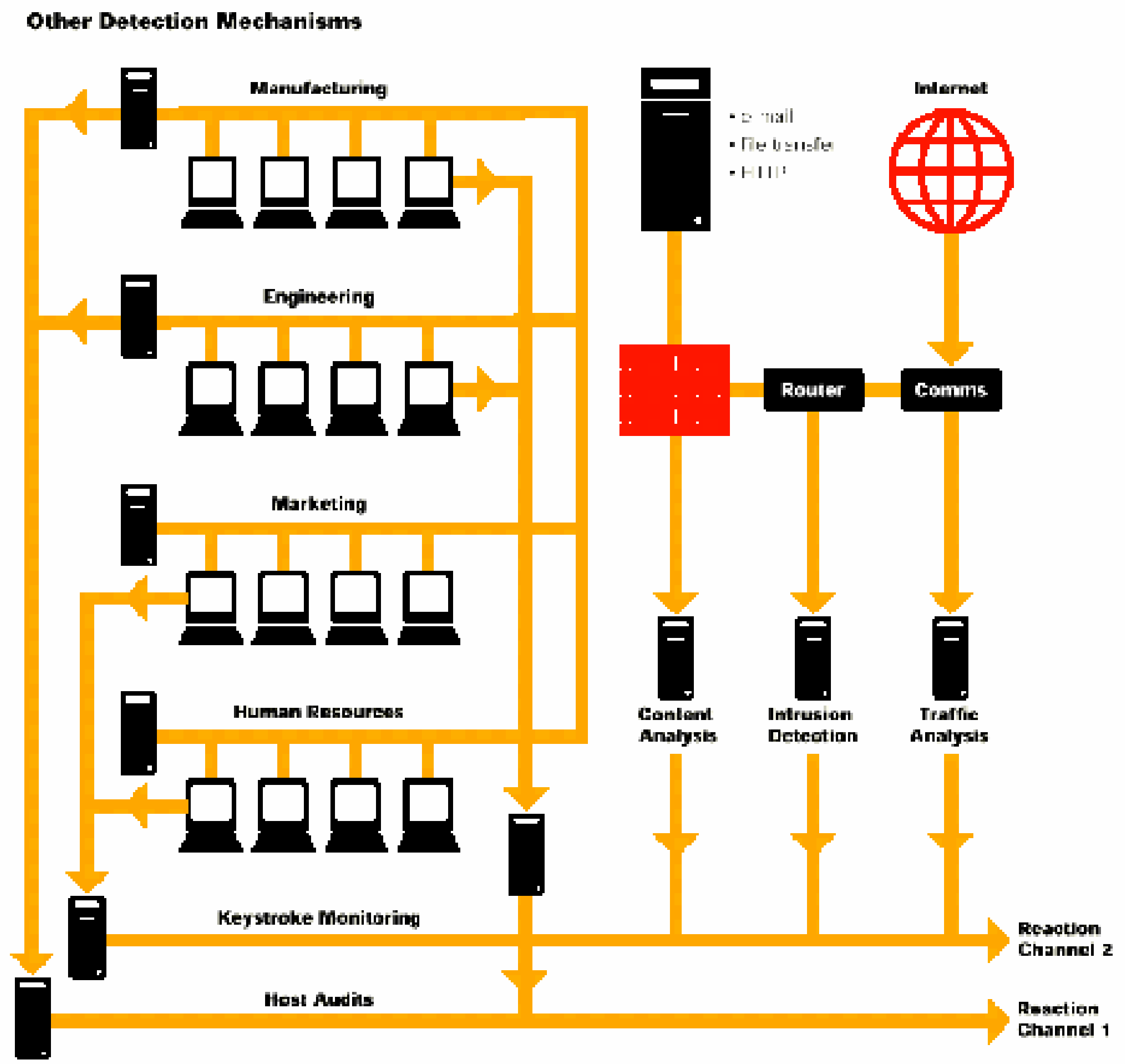
The product that he is keying on is the Open e-Security Platform (OEsP) by e-Security Incorporated. "Simply, OeSP is a security management platform that performs real-time visualization of security-relevant events across an entire enterprise. In fact, their tag line is right on target: "Enterprise security you can see." There are many segmented security products which do provide visualization tools of their own small piece of the network, like perimeter intrusion detection, bandwidth utilization and firewall performance. However, OeSP integrates these functions from the leading security devices into a single view of the enterprise, depending upon what view you take."[7]

The solution that this product tries to provide to security professionals is two-fold:

> "1. Rather than attempting to analyze several different viewpoints of the network, and then correlate them in your head or draw your own pictures and conclusions, OeSP provides a single image view of the entire network."[7]
>
> "2. You can achieve this all, in nearly real time (depending upon the speed of the host detection mechanisms), from a single console."[7]

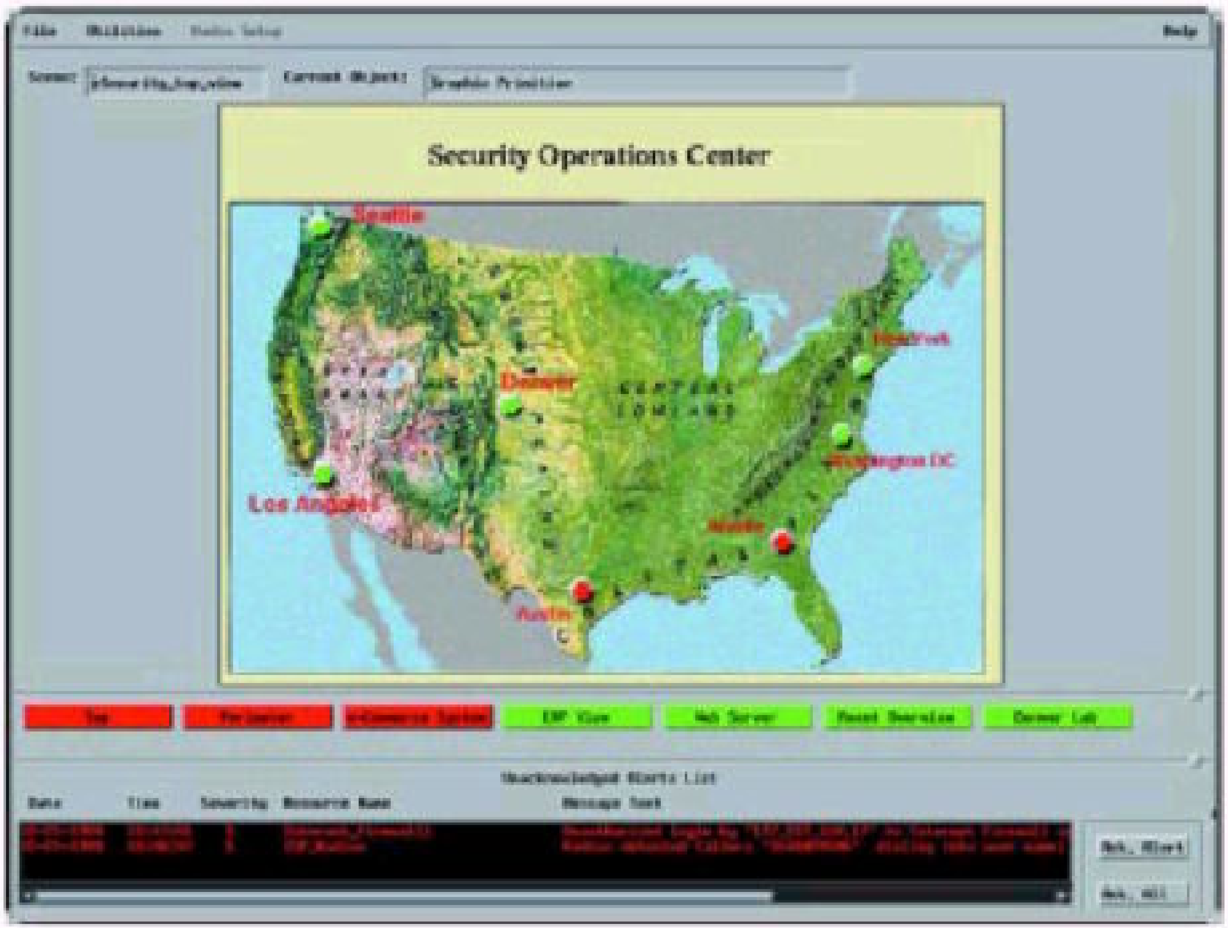
"This way, apparently unrelated events can be correlated so that informed decisions can be made on how to react."[7]

He then provides the following example: "… in your network, does a hacker knocking at the door of your Austin, Texas-based servers have any relevance to a web-graffiti assault on your California web server? Pictures tell the story one heck of a lot easier than separate reports, separate visualization or no analysis at all. But you probably also want a more drilled-down view to understand exactly what is going on – without having to sort through a thousand pages of text or 20 different detection products. e-Security's pictorial OeSP Perimeter View of the attack now tells the administrator that the attack is coming from outside the company (the Internet) and not from the modem pool. In an eCommerce view, the entire process can be viewed in a single picture regardless of the peripheral security detection products used."[7]

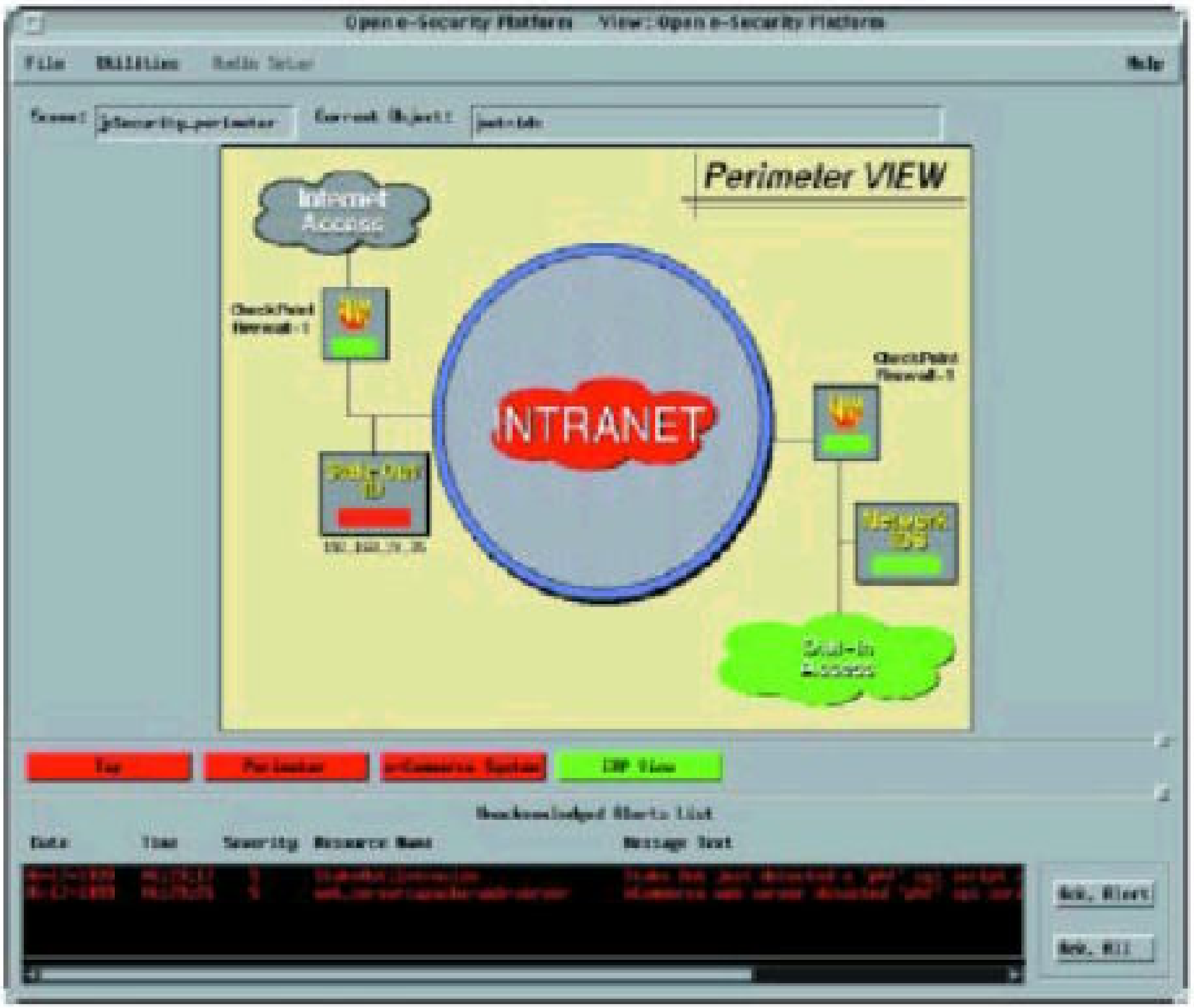


* "Detection means more than just perimeter defense, IP addresses, and hackers coming in from the Internet. Use the available data such as host audit information, traffic analysis from a NOC, and distributed IDS points throughout the enterprise network. This provides a more complete "picture" of threats to the system."[7]

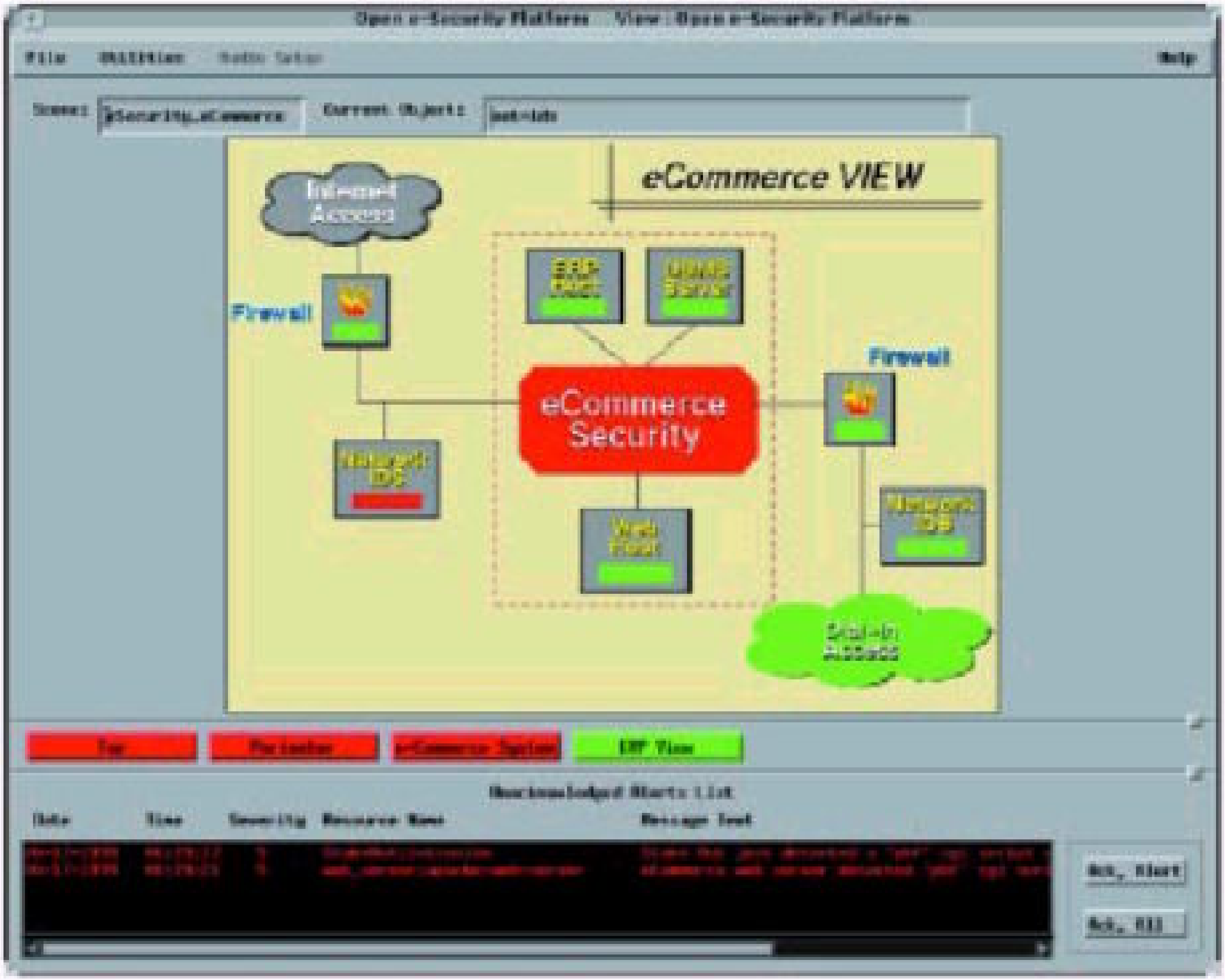
## Examples from the Open e-Security Platform:



* "The Open e-Security Platform console gives you a comprehensive picture to monitor all your enterprise security resources with the flexibility to customize specific views of your security system such as e-commerce or perimeter security.  Shown here is an example of a geographic view of network security across the enterprise."[7]



* “[This] is an example of an Open e-Security Platform perimeter view of intranet security that incorporates a variety of security point security products and resources. It illustrates the console perimeter view during an attack on the network via Internet access.”[7]



* “[This] is a more detailed view of the attack within the context of the enterprise’s e-commerce environment displayed in real time on the console.”[7]

# Appendix D

# References (Assignment 2)

[1] University of Washington. URL: http://www.washington.edu/computing/training/560/zz-tufte.html (15 March 2002).

[2] Troung, Khai N., Abowd, Gregory D., and Brotherton, Jason A. "Who, What, When, Where, How: Design Issues of Capture & Access Applications." College of Computing & GVU Center, Georgia Institute of Technology. URL: ftp://ftp.cc.gatech.edu/pub/gvu/tr/2001/01-02.pdf (20 January 2002).

[3] Green, Marc Ph.D. "Toward a Perceptual Science of Multidimensional Data Visualization: Bertin and Beyond." URL: http://www.ergogero.com/dataviz/dviz0.html. (21 January 2002).

[3a] Green, Marc Ph.D. "Toward a Perceptual Science of Multidimensional Data Visualization: Bertin and Beyond." URL: http://www.ergogero.com/dataviz/dviz1.html. (21 January 2002).

[3b] Green, Marc Ph.D. "Toward a Perceptual Science of Multidimensional Data Visualization: Bertin and Beyond." URL: http://www.ergogero.com/dataviz/dviz2.html. (21 January 2002).

[4] Eicks, Stephen G. Ph.D. "ADVIZOR™: A Technical Overview." Visual Insights, Inc. URL: http://www.visualinsights.com/pressroom/whitepapers/advisor_tech.pdf (21 January 2002).

[5] Visual Insights ADVISOR™. URL: http://www.visualinsights.com/base_pages/mainhtml.asp?level1=four&level2=three&level3=one&picked=4-1-1 (17 March 2002)

[6] Secure Decisions SecureScope™. "Visualization for Information Security Situational Awareness." Secure Decisions. URL: http://www.securedecisions.com/documents/SecureScopeOverview022602.ppt (17 March 2002).

[7] Schwartau, Winn. "Solving 'Dumb Days' With Security Visualization." Ebiz.Net. URL: http://e-serv.ebizq.net/shared/white_papers.jsp?ID=schwartau_1.pdf (17 March 2002).

# Assignment 3
# "Analyze This" Scenario

## OVERVIEW –

The following information has been provided per your request, and in cooperation with the University of Maryland, Baltimore County (UMBC), from the SANS.Org Global Information Assurance web site (see Assignment 3 at http://www.giac.org/GCIA_assign_29.php#7 )[1] as is stated here: "You have been asked to provide a security audit for a University. You have been provided with data from a Snort system with a fairly standard rulebase. This data is posted at http://www.research.umbc.edu/~andy."[8] As is referenced, the log files were found at the web site http://www.research.umbc.edu/~andy.[8]

The following analysis is from UMBC's web site postings and is represented by the SNORT alerts, scans, and OOS (out of spec) files provided there. These log files and the resulting analyses encompass the dates of 29 December 2002 through 02 January 2002.

| Alert Logs | OOS Logs | Scan Logs |
|---|---|---|
| alert.011229.gz | Oos_Dec.29.2001.gz | scans.011229.gz |
| alert.011230.gz | Oos_Dec.30.2001.gz | scans.011230.gz |
| alert.011231.gz | Oos_Dec.31.2001.gz | scans.011231.gz |
| alert.020101.gz | oos_Jan.01.2001.gz | scans.020101.gz |
| alert.020102.gz | oos_Jan.02.2002.gz | scans.020102.gz |

Any errors or gaps in the derived conclusions, or speculation, of specific events/incidents that is provided in this analysis was due to my lack of intimate knowledge and/or familiarity of the network infrastructure and its resulting defensive posture. As is it stated in the first paragraph, I do not know the "fairly standard rulebase" that SNORT used to generate these detects and may be required to make some assumptions about the traffic based upon my personal experience with SNORT (http://www.snort.org/ )[9] and Silicon Defense's SnortSnarf v020124.1 (http://www.silicondefense.com/software/snortsnarf/) [15]. I recommend that, for due diligence, UMBC establish a security team or procure the services of a 3rd party with the ability to perform an in depth and complete investigation, to include hands-on analysis and recommendations.

## Analysis Procedures –

In this paper I will begin by analyzing the Alerts, then the Scans, and finally the OOS events. This is to emphasize the priority and significance given to each type of event and also to provide as much correlation between the events as is possible.

I used a global search and replace command inside of vi editor to change the "MY.NET" to "10.1" for ease of analysis and use with SnortSnarf. Because using a private addressing scheme internally is a good security practice, along with saving the expense of an entire class B net block, I must assume that this is the situation at UMBC. From this point forward I will consider the "10.1" IP address range to represent UMBC's internal network addresses.

My method of analysis was to identify the relevant information and, in the process, to answer the following four questions:

1. What was the scope of the activity?
2. Was the activity targeted at or against the site?
3. Did any destination receive an anomalous amount/type of traffic?
4. Where there any indications of compromise?

While performing this analysis I tried to characterize traffic as it is understood under normal conditions and compared this to what I saw in these logs. I then evaluated the traffic that I observed, via the logs, to determine any targeted IPs, or IP ranges. In doing so, I primarily answer the first two questions and begin to filter that traffic which may require more scrutiny. When answering these questions, the obvious compromises begin to stand out and flags, or clues, begin to take form which may indicate the possible intent of the originating party. This is where the an Analyst's experience and mental filter become key, because the data that remains from the previous tests is the final clue that may reveal whether said traffic is truly malicious. Finally, and often the most difficult part of this process, is that of correlation and fusion. I used external tools such as D-Shield (http://www.dshield.org/) [16], Sam Spade (http://www.samspade.org/) [23], and other security related web sites (as is referenced in the following analysis) to look for trends and historical data/patterns in an effort to correlate past, or concurrent, events. I then take all of the relevant information that has resulted from this analysis and make a defensive recommendation so that UMBC may resolve and assess the threat as it applies to their respective situation.

## SNORT Alert Log Analysis –

I began my analysis by summarizing the alerts, by event signatures, using Silicon Defense's SnortSnarf v020124.1 (http://www.silicondefense.com/software/snortsnarf/) [15]:

Earliest alert at **00:05:46**.037713 *on 12/29/2001*
Latest alert at **23:54:08**.335080 *on 01/02/2002*

| Signature | # Alerts | # Sources | # Dests |
|---|---|---|---|
| **ICMP Echo Request Nmap or HPING2** | 1 | 1 | 1 |
| **ICMP Echo Request L3retriever Ping** | 2 | 1 | 1 |

| | | | |
|---|---|---|---|
| **SMB Name Wildcard** | 8 | 2 | 4 |
| **SYN-FIN scan!** | 26 | 1 | 26 |
| **TCP SRC and DST outside network** | 28 | 9 | 7 |
| **SCAN Proxy attempt** | 41 | 1 | 22 |
| **INFO – Possible Squid Scan** | 99 | 1 | 52 |
| **SNMP public access** | 226 | 9 | 16 |
| **ICMP Router Selection** | 1368 | 118 | 1 |

*As output by SnortSnarf, priority was not assigned to any of the above signatures

### 1st Alert – ICMP Echo Request Nmap or HPING2

- **All sources triggering this attack signature**

| Source | # Alerts (sig) | # Alerts (total) | # Dsts (sig) | # Dsts (total) |
|---|---|---|---|---|
| 10.1.150.86 | 1 | 3 | 1 | 1 |

- **All destinations receiving this attack signature**

| Destinations | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|
| 10.1.153.220 | 1 | 4 | 1 | 2 |

- **Brief description of the attack**

Earliest such alert at **18:26:12**.263785 *on 01/02/2002*
Latest such alert at **18:26:12**.263785 *on 01/02/2002*

The log data did not provide enough information to speculate about which tool, NMAP or HPING, may have been used in this instance and I was unable to find the specific rule in the SNORT web database (http://www.snort.org/snort-db/all.html)[10]. However, an ICMP Echo Request may be used to test for connectivity when troubleshooting network problems and to probe for live hosts on a given network by eliciting an ICMP Echo Reply. The later use provides a good reason to null route these requests at your perimeter via either a router or a firewall. That way the originator of the PING can not confirm or rule out the existence of any particular host within your network.

An overview of both the Nmap and HPING scanning tools is provided below:

- **Nmap** (http://www.insecure.org/nmap/) [24]: "Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks… to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers, and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL."

- **HPING** (http://www.hping.org/) [25]: "hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.
While hping was mainly used as a security tool in the past, it can be used in many ways

by people that don't care about security to test networks and hosts. A subset of the stuff you can do using hping:

- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

hping can also be useful to students that are learning TCP/IP.
Hping should work without problems on the following unix-like systems:

- Linux, FreeBSD, NetBSD, OpenBSD, Solaris

The next generation of hping is hping3, under development."

- **Defensive recommendation**

As I stated in the last section, null routing ICMP Echo Requests via a router or firewall at the perimeter should be part of every network's defense and only if it is absolutely necessary should exceptions be made. Furthermore, I recommend that your defensive posture is to deny anything that is not explicitly allowed. This will serve to limit your external exposure of those necessary vulnerabilities that may exist within your network and also help to protect you in the case that a device inside your network happens to be misconfigured, thus unintentionally vulnerable.

However, in this case the source and destination IPs appear to be from the same private IP addressing scheme, thus indicating either an internal compromise, a misconfigured system, or valid traffic. Although only one detect was captured as an Echo Request, two more detects were captured as ICMP Echo Request L3retriever Pings, of which will be discussed in the 2nd Alert analysis. At this point I will rule out a system compromise due to the fact that no other suspect activity has been recorded to or from this machine.

For defense in depth purposes I would also recommend using a host-based firewall to protect the systems/network in the event of a compromise or other malicious activity. In this case I suspect that an inside user may have caused this traffic, which further supports the need for a host-based firewall. Two such firewalls that I have experience with and recommend are ISS's BlackICE Defender (http://www.iss.net/products_services/hsoffice_protection/buy.php) [27] and Zone Lab's ZoneAlarm (http://www.zonelabs.com/products/za/freedownload2.html) [26].

- **Correlation**

1. What was the scope of the activity?
   The traffic went from one source IP to one destination IP.

2. Was the activity targeted at or against the site?
   The activity appears to be targeted, but could possibly be valid or a misconfiguration.

3. Did any destination receive an anomalous amount/type of traffic?
   The activity did match on a SNORT rule, but, at the resulting analysis does not fully support the conclusion that this was malicious. This likely could be someone testing the connectivity to the system, testing a network tool, or an erroneous entry while performing a PING.

4. Where there any indications of compromise?
   There are no indications of compromise or of malicious intent from this detect but, when correlated with the data in the 2nd Alert, there is an indication that the internal source IP/system should be investigated for the possibility that someone on the inside may intentionally have caused this type of traffic. Only a hands-on investigation can reveal whether or not these three Pings were malicious.

## 2nd Alert – ICMP Echo Request L3retriever Ping

### ➢ All sources triggering this attack signature

| Source | # Alerts (sig) | # Alerts (total) | # Dsts (sig) | # Dsts (total) |
|---|---|---|---|---|
| 10.1.150.86 | 2 | 3 | 1 | 1 |

### ➢ All destinations receiving this attack signature

| Destinations | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|
| 10.1.153.220 | 2 | 4 | 1 | 2 |

### ➢ Brief description of the attack

Earliest such alert at **07:37:05**.330264 *on 01/02/2002*
Latest such alert at **07:37:07**.332273 *on 01/02/2002*

An ICMP Echo Request may be used to test for connectivity when troubleshooting network problems and to probe for live hosts on a given network by eliciting an ICMP Echo Reply. The later use provides a good reason to null route these requests at your perimeter via either a router or a firewall. That way the originator of the PING can not confirm or rule out the existence of any particular host within your network.

Because I was able to find an entry in the SNORT web database (http://www.snort.org/snort-db/sid.html?id=466)[11] I could see that the payload for this type of activity was indeed abnormal. What is of interest is that the source and destination IPs are from the same private addressing scheme, thus indicating a compromised system, a misconfigured system, or valid traffic coming from an inside operator.

Information about the SNORT rule this traffic matched on came from the SNORT web database (http://www.snort.org/snort-db/sid.html?id=466)[11] as follows:

- "This signature is unfinished."
- "alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; **content: "ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"**; itype: 8; icode: 0; depth: 32; reference:arachnids,311; classtype:attempted-recon; sid:466; rev:1;)
- "Attempted Information Leak "
- "Latest Revision: 1"

### ➢ Defensive recommendation

As I stated before, null routing ICMP Echo Requests via a router or firewall at the perimeter should be part of every network's defense and, only if it is absolutely necessary, should exceptions be made. Furthermore, I recommend that your defensive posture is to deny anything that is not explicitly allowed and absolutely necessary. This will serve to limit your external exposure of those necessary vulnerabilities that may exist within your network and also help to protect you in the case that a device inside your network happens to be misconfigured, thus unintentionally vulnerable.

However, in this case the source and destination IPs appear to be from the same private IP addressing scheme, thus indicating either an internal compromise, a misconfigured system, or valid traffic. Although only two detects were captured as ICMP Echo Request L3retriever Pings, one more detect was captured as an ICMP Echo Request Nmap or HPING2, which was discussed under the 1st Alert section of this analysis. At this point I will rule out a system compromise due to the fact that no other detects were recorded for this source IP, however, because there are indications of an insider generating this type of traffic, system auditing and internal defenses will need to be scrutinized in addition to investigating the source IP/system and possible originators.

To provide defense in depth I would also recommend using a host-based firewall to protect the systems/network in the event of a compromise or other malicious activity. In this case I suspect that an inside user may have caused this traffic, which further supports the need for a host-based firewall. Two such firewalls that I have experience with and recommend are ISS's BlackICE Defender (http://www.iss.net/products_services/hsoffice_protection/buy.php) [27] and Zone Lab's ZoneAlarm (http://www.zonelabs.com/products/za/freedownload2.html) [26].

- **Correlation**

1. What was the scope of the activity?
   The traffic went from one source IP to one destination IP.

2. Was the activity targeted at or against the site?
   The activity appears to be targeted, but could possibly be valid or a misconfiguration.

3. Did any destination receive an anomalous amount/type of traffic?
   The activity did match on a SNORT rule in which the payload is abnormal, but the resulting analysis does not fully support the conclusion that this was malicious. This likely could be someone testing a network tool.

4. Where there any indications of compromise?
   There doesn't appear to be a system compromise, but there are indications of malicious intent due to the payload and correlation with the 1st Alert analysis. This activity warrants the investigation of the internal source IP/system and the possibility that someone on the inside may intentionally have caused this type of traffic. Only an investigation can reveal whether or not these three Pings were malicious.

### 3rd Alert – SMB Name Wildcard

- **All sources triggering this attack signature**

| Source | # Alerts (sig) | # Alerts (total) | # Dsts (sig) | # Dsts (total) |
|---|---|---|---|---|
| 10.1.221.174 | 4 | 4 | 2 | 2 |
| 10.1.111.188 | 4 | 4 | 2 | 2 |

- **All destinations receiving this attack signature**

| Destinations | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|
| 10.1.150.84 | 3 | 8 | 1 | 4 |
| 10.1.150.170 | 3 | 13 | 1 | 4 |
| 10.1.150.172 | 1 | 12 | 1 | 4 |
| 10.1.151.66 | 1 | 1 | 1 | 1 |

- **Brief description of the attack**

Earliest such alert at **00:05:46**.037713 *on 12/29/2001*
Latest such alert at **15:17:03**.072170 *on 01/02/2002*

A good, concise description of what characterizes normal port 137 traffic is provided at the Network ICE web sites http://advice.networkice.com/Advice/Exploits/Ports/137/default.htm [30] and http://advice.networkice.com/Advice/Exploits/Ports/groups/Microsoft/default.htm [31] respectively as “Firewall administrators will frequently see large numbers of incoming packets to port 137. This is due to the behavior of Windows servers that use NetBIOS (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 NetBIOS lookups.” and “This is how NetBIOS-based services find each other. On a NetBIOS network, these names uniquely identify the machine and services running on the machine (and the IP address doesn't matter). Machines find each other either using broadcasts or looking them up in a centralized NetBIOS naming server (called a WINS server).”

An attacker can probe port 137 to elicit a response that may reveal information about the local system’s domain, system ID, and other user and services information. This is often done in an effort to find open/unprotected shares on Microsoft Window’s machines. Yotam Rubin wrote an excellent post on the Incidents Mailing List at SecurityFocus.com (archived at http://archives.neohapsis.com/archives/incidents/2001-05/0034.html) [33] that further describes this type of activity.

Bryce Alexander posted a paper in the Intrusion Detection FAQ section of the SANS.Org web site (http://www.sans.org/newlook/resources/IDFAQ/port_137.htm)[2] that gives a detailed packet trace and a correlation of increased port 137 scanning attributed to the internet worm "network.vbs" that was propagating in the Spring of 2000. This is an interesting read and contains useful information about dissecting the raw packets if they are available to you. See also his post at the SANS.Org Global Incident Analysis Center web site at http://www.sans.org/y2k/honeypot_catch.htm [3] for an entire trace of this type of activity. An incident note has been posted at the CERT.Org web site (http://www.cert.org/incident_notes/IN-2000-02.html) [36] "CERT® Incident Note IN-2000-02" in relation to the "network.vbs" worm.

There are multiple vulnerabilities and exploits related to this port/service. Examples can be found at the following web sites or by performing an http://www.google.com [46] search on "NetBIOS name service":

- http://www.kb.cert.org/vuls/id/32650 [37]
- http://www.cert.org/vul_notes/VN-2000-03.html [38]
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0288 [47]
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0811 [48]
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0347 [49]
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0673 [50]
- http://www.winguides.com/search.php?guide=security&keywords=netbios+name+service [53]

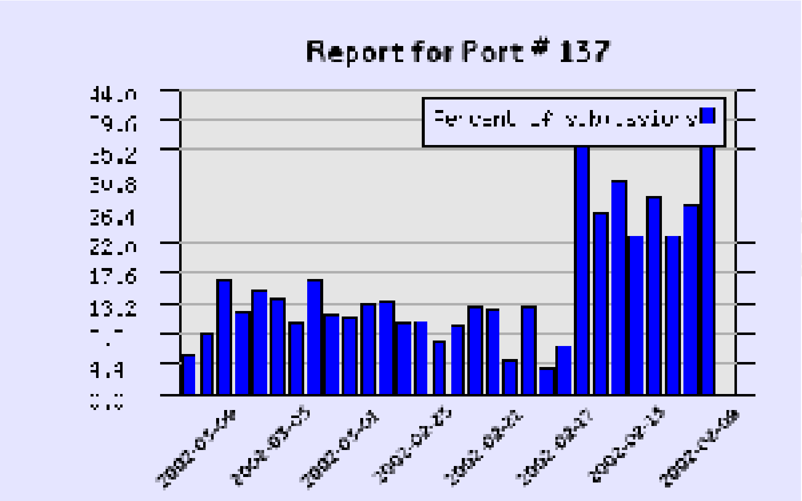
## ➢ Defensive recommendation

Once again, blocking all ports that are not specifically required should be the standard configuration of every network's perimeter defenses. Furthermore, using a host-based firewall and NAT with internal private addressing is also a best practices recommendation.

For this specific type of exploit, it would be prudent to also educate and train your users about the adverse affect of open shares, of any sort. Because this occurred at a university, sharing is to be expected, so training the users to protect and secure their shared files, systems, and networks would most likely afford an excellent return on investment for your organization.

## ➢ Correlation

1. What was the scope of the activity?
   The activity occurred between two sources and four destinations. Each source sent traffic to two different destinations.



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=137) [17]

2. Was the activity targeted at or against the site?
   Because there doesn't appear to be a scan that is related to this traffic, and because both the source and destination IP addresses came from within the same classful, private net block, this appears to be targeted. However, this service often operates by broadcasts and could be seen outside of its switched LAN if there are misconfigured devices present.

3. Did any destination receive an anomalous amount/type of traffic?
   The activity did match on a SNORT rule, but the resulting analysis and amount/type of traffic does not support the conclusion that this was malicious. This is likely to be a misconfiguration within the network.

4. Where there any indications of compromise?
   There were no indications of compromise or malicious intent. No additional activity was logged.

### 4th Alert – SYN-FIN scan!

- **All sources triggering this attack signature**

| Source | # Alerts (sig) | # Alerts (total) | # Dsts (sig) | # Dsts (total) |
|---|---|---|---|---|
| 129.71.215.240 | 26 | 26 | 26 | 26 |

- **All destinations receiving this attack signature**

| Destinations | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|
| 10.1.88.160 | 1 | 4 | 1 | 3 |
| 10.1.88.146 | 1 | 2 | 1 | 2 |
| 10.1.152.120 | 1 | 9 | 1 | 2 |
| 10.1.153.121 | 1 | 3 | 1 | 2 |
| 10.1.153.220 | 1 | 4 | 1 | 2 |
| 10.1.88.149 | 1 | 1 | 1 | 1 |
| 10.1.150.243 | 1 | 5 | 1 | 3 |
| 10.1.88.187 | 1 | 3 | 1 | 2 |
| 10.1.152.180 | 1 | 1 | 1 | 1 |
| 10.1.152.44 | 1 | 1 | 1 | 1 |
| 10.1.151.75 | 1 | 3 | 1 | 2 |
| 10.1.150.231 | 1 | 9 | 1 | 5 |
| 10.1.152.212 | 1 | 3 | 1 | 2 |
| 10.1.150.170 | 1 | 13 | 1 | 4 |
| 10.1.150.172 | 1 | 12 | 1 | 4 |
| 10.1.150.237 | 1 | 3 | 1 | 2 |
| 10.1.153.135 | 1 | 2 | 1 | 2 |
| 10.1.152.137 | 1 | 2 | 1 | 2 |
| 10.1.153.219 | 1 | 4 | 1 | 3 |
| 10.1.152.159 | 1 | 1 | 1 | 1 |
| 10.1.150.197 | 1 | 1 | 1 | 1 |
| 10.1.152.178 | 1 | 1 | 1 | 1 |
| 10.1.152.30 | 1 | 2 | 1 | 2 |
| 10.1.150.51 | 1 | 10 | 1 | 4 |
| 10.1.150.55 | 1 | 11 | 1 | 3 |
| 10.1.152.18 | 1 | 1 | 1 | 1 |

- **Brief description of the attack**

Earliest such alert at **05:57:22**.580991 *on 12/31/2001*
Latest such alert at **06:02:55**.377657 *on 12/31/2001*

A packet with the SYN and FIN flags set is never a valid packet and thus, it should always be a part of your IDS's rule set. These types of crafted packets are used to elicit responses that indicate what ports a system is listening on by scanning a range of hosts on a specific port, or by scanning on multiple ports. A SYN-FIN scan by itself is not necessarily malicious, but it is often the precursor to an attack of some sort.

In this case, the source is scanning on port 22 to several different hosts and is probably looking for the recently publicized Secure Shell vulnerability (SSH/CRC32). SSH/CRC32 is a critical vulnerability in the widely used Secure Shell application. Secure Shell allows users to remotely log into a computer from across a network and the entire login session, including transmission of the password, is encrypted. Vulnerabilities have been discovered in Secure Shell Protocol Version 1, whereby an intruder can modify data within an encrypted SSH session and gain root access to a system. The intruder can also use a compromised system to attack other networks.

The source's Arin.Net (http://www.arin.net/whois/index.html) [54] information is as follows:

```
West Virginia Network for Educational Telecomputing (NET-
WVNET)
   837 Chestnut Ridge Road
   Morgantown, WV 26505
   US

   Netname: WVNET
   Netblock: 129.71.0.0 - 129.71.255.255

   Coordinator:
      Lynch, Rich  (RL104-ARIN)  rich@WVNVM.WVNET.EDU
      (304) 293-5192

   Domain System inverse mapping provided by:

   NAMESERV.WVNET.EDU            129.71.1.1
   WVNVAXA.WVNET.EDU      129.71.2.1

   Record last updated on 27-Feb-1993.
   Database last updated on  9-Mar-2002 19:56:49 EDT.
```

Educational institutions, by nature, are widely open to exploits and are often used for malicious purposes. The one referenced here is apparently of a technical nature and determining whether the scan came from a compromised system or by an enterprising student can only be discovered by investigating the source machine and the users.

- **Defensive recommendation**

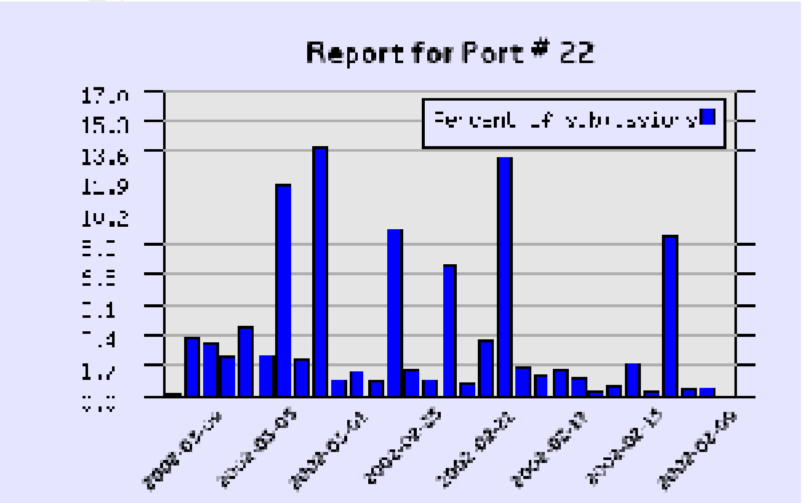
All implementations of Secure Shell Protocol Version 1 are vulnerable and all upgraded versions with Fallback to version 1 enabled are also vulnerable. Unix systems in particular are highly vulnerable and SSH is installed by default in many operating systems. Therefore, it is necessary that you ensure that all of your systems, (clients, servers, and other network devices) have been secured by completely removing any current implementations of Secure Shell Protocol Version 1, then upgrade by installing a non-vulnerable version as is recommended by the vendor.

See the following web sites for further information about SSH vulnerabilities:
- http://www.kb.cert.org/vuls/id/945216 [39]
- http://www.cert.org/advisories/CA-2001-35.html [40]
- http://www.cert.org/incident_notes/IN-2001-12.html [41]
- http://www.kb.cert.org/vuls/id/13877 [42]
- http://www.cert.org/summaries/CS-2001-04.html [43]
- http://www.cert.org/summaries/CS-2002-01.html [44]
- CVE-2001-0144: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0144 [51]
- CAN-2002-0083: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0083[52]
- http://www.ciac.org/ciac/techbull/CIACTech02-001.shtml [55]
- http://www.incidents.org/diary/diary.php?id=148][7]

Once again, blocking all ports that are not specifically required should be the standard configuration of every network's perimeter defenses. Furthermore, using a host-based firewall and NAT with internal private addressing is also a best practices recommendation.

- **Correlation**

1. What was the scope of the activity?
   The scan occurred between one source and twenty-six destinations on port 22. This source was also detected in the Scan Log Analysis section at the end of this paper.



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=22) [18]

2. Was the activity targeted at or against the site?
   Although this was not an overly large scan, it did not appear to be targeted and no host was scanned more than once.

3. Did any destination receive an anomalous amount/type of traffic?
   No host was scanned more than once or received an anomalous amount/type of traffic other than the original SYN-FIN packet.

4. Where there any indications of compromise?
   There were no indications of compromise, however, a SYN-FIN scan is often a precursor to an attack and the stated Defensive Recommendations should be executed immediately.

**5th Alert – TCP SRC and DST outside network**

- **All sources triggering this attack signature**

| Source | # Alerts (sig) | # Alerts (total) | # Dsts (sig) | # Dsts (total) |
|---|---|---|---|---|
| 169.254.51.158 | 5 | 5 | 2 | 2 |
| 169.254.208.44 | 4 | 4 | 1 | 1 |
| 169.254.16.197 | 4 | 4 | 1 | 1 |
| 169.254.134.147 | 4 | 4 | 1 | 1 |
| 169.254.20.219 | 3 | 3 | 1 | 1 |
| 169.254.185.204 | 3 | 3 | 1 | 1 |
| 169.254.193.161 | 3 | 3 | 1 | 1 |
| 169.254.61.161 | 1 | 1 | 1 | 1 |
| 169.254.58.121 | 1 | 1 | 1 | 1 |

- **All destinations receiving this attack signature**

| Destinations | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|
| 169.254.20.219 | 9 | 9 | 3 | 3 |
| 169.254.193.161 | 7 | 7 | 2 | 2 |
| 169.254.141.59 | 3 | 3 | 1 | 1 |
| 169.254.141.62 | 3 | 3 | 1 | 1 |
| 169.254.166.218 | 3 | 3 | 1 | 1 |
| 169.254.77.192 | 2 | 2 | 1 | 1 |
| 169.254.185.204 | 1 | 1 | 1 | 1 |

- **Brief description of the attack**

Earliest such alert at **10:15:07**.389362 *on 01/02/2002*
Latest such alert at **19:49:25**.445597 *on 01/02/2002*

There are three possibilities to explain this type of activity. The first possibility is that someone inside your network is spoofing IP addresses when sending traffic, but I saw two-way types of traffic that appeared to be valid, so I will not explore this option any further. If this were the case, then egress filtering could prevent this.

The second possibility is that because you are on an open network, you may have more than one path to the internet or someone has created one for you via an unauthorized back door. If this were true, then valid routed traffic could potentially traverse your network if it was deemed to be the best path to the destination. However, I observed what appeared to be valid two-way traffic using NetBIOS, all from the same class B net block, on what is a reserved address range, thus, unless the route between the sources and destinations is misconfigured to allow the routing of reserved addresses, then I would not consider a routing traversal as an option, as it is not very likely.

The third and most plausible option is that you are on an open switched LAN/MAN and what you are seeing is NetBIOS traffic between hosts that are using, whether intentionally or not, the reserved IP addresses (169.254.X.X) which allows them to communicate locally using broadcasts. They could either be misconfigured or a network problem with DHCP has caused them to default over to an internally assigned reserved IP address that is often used to maintain local communications in the event that DHCP services are not available. You should look for DHCP discover packets to confirm this scenario.

An http://www.google.com [46] search on "169.254.X.X" and following web sites discuss this last situation further:

- http://support.microsoft.com/default.aspx?scid=kb;EN-US;q220874 [56]
- http://www.sans.org/y2k/072500-1200.htm [4]
- http://archives.neohapsis.com/archives/incidents/2000-04/0002.html [34]
- http://archives.neohapsis.com/archives/incidents/2000-04/0013.html [35]
- http://lists.insecure.org/incidents/2000/Mar/0270.html [28]
- http://lists.insecure.org/incidents/2000/Mar/0308.html [29]
- ftp://ftp.rfc-editor.org/in-notes/rfc2563.txt [58]

### ➢ Defensive recommendation

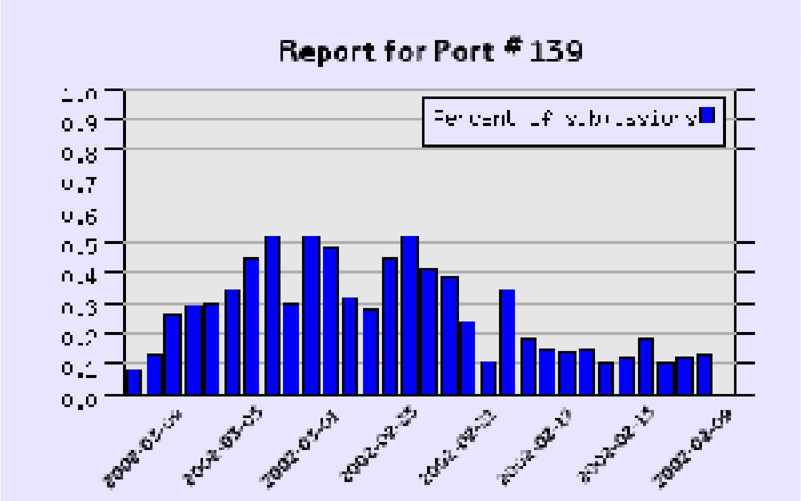
Make sure that your routers are configured correctly. They should typically not be forwarding or routing broadcasts or reserved/private IP addresses. You should also evaluate your infrastructure for design weaknesses and scalability. If you are seeing broadcast traffic from an entire class B network, then you may want to consider segmenting or VPNs as appropriate. Also look for back doors that may have been installed on your network. These are always a bad idea unless absolutely necessary. If they are required, then be sure to secure them just as you would the rest of your perimeter.

Blocking all ports that are not specifically required should be the standard configuration of every network's perimeter defenses. In this case, you should be blocking specifically NetBIOS ports. You may also want to implement egress filtering to ensure that IP addresses are not spoofed from within your network. Furthermore, using a host-based firewall and NAT with planned internal private addressing is also a best practices recommendation.

Finally, to be sure that your clients are not using automatic IP addressing unintentionally, you should look into configuration management and security policies that will help provide continuity across your enterprise. This may require user and administrator training. As indicated before, some network troubleshooting may be required to prove that this scenario is correct.

## ➢ Correlation

1. What was the scope of the activity?
   I observed traffic between 9 sources and 7 destinations. There appeared to be some two-way traffic that was probably valid.



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=139) [19]

2. Was the activity targeted at or against the site?
   This does not appear to be an attack, and as such, was not targeted at or against this network.

3. Did any destination receive an anomalous amount/type of traffic?
   The source and destination IP addresses were considered anomalous, but the most feasible scenario provided an explanation which indicated that this was not malicious activity. However, as was stated in the Defensive Recommendations, the network infrastructure and configuration management policies need to be evaluated to prove this hypothesis.

4. Where there any indications of compromise?
   There were no indications of compromise or malicious activity.

### 6th Alert – SCAN Proxy attempt

- **All sources triggering this attack signature**

| Source | # Alerts (sig) | # Alerts (total) | # Dsts (sig) | # Dsts (total) |
|---|---|---|---|---|
| 203.71.238.200 | 41 | 140 | 22 | 56 |

- **All destinations receiving this attack signature**

| Destinations | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|
| 10.1.152.125 | 5 | 10 | 1 | 1 |
| 10.1.150.14 | 5 | 40 | 1 | 3 |
| 10.1.152.120 | 4 | 9 | 1 | 2 |
| 10.1.152.127 | 3 | 9 | 1 | 1 |
| 10.1.150.170 | 3 | 13 | 1 | 4 |
| 10.1.153.71 | 2 | 5 | 1 | 1 |
| 10.1.150.172 | 2 | 12 | 1 | 4 |
| 10.1.150.147 | 2 | 11 | 1 | 4 |
| 10.1.150.55 | 2 | 11 | 1 | 3 |
| 10.1.153.109 | 1 | 3 | 1 | 1 |
| 10.1.150.84 | 1 | 8 | 1 | 4 |
| 10.1.153.110 | 1 | 2 | 1 | 1 |
| 10.1.150.231 | 1 | 9 | 1 | 5 |
| 10.1.88.146 | 1 | 2 | 1 | 2 |
| 10.1.152.214 | 1 | 1 | 1 | 1 |
| 10.1.153.120 | 1 | 2 | 1 | 1 |
| 10.1.150.237 | 1 | 3 | 1 | 2 |
| 10.1.153.137 | 1 | 1 | 1 | 1 |
| 10.1.153.121 | 1 | 3 | 1 | 2 |
| 10.1.150.51 | 1 | 10 | 1 | 4 |
| 10.1.150.52 | 1 | 4 | 1 | 2 |
| 10.1.152.244 | 1 | 1 | 1 | 1 |

- **Brief description of the attack**

Earliest such alert at **01:58:04**.361200 *on 12/29/2001*
Latest such alert at **05:47:47**.753046 *on 12/29/2001*

It appears that in this scan, and also in the 7th Alert, the originator is probing for proxy servers (WinGate has been a popular one). Proxy servers, if misconfigured, can allow attackers to anonymize themselves and thus become difficult, if not impossible to track down. This serves to obscure their true identities. The intent of this scan is most likely to gather information about available/vulnerable proxies that can be catalogued and used at a later date. One such tool that probes on both port 8080 and 3128 is Ring Zero. Further information about Ring Zero can be found on the SANS.Org web site in Intrusion Detection FAQ (http://www.sans.org/newlook/resources/IDFAQ/ring_zero.htm) [5].

Alternatively, if an attacker gains access to a proxy server, then they could also have access to the internal network behind that proxy, thus defeating your perimeter defenses.

A less likely option is that of a Denial of Service (DoS) against your network. This is not as probable because there are better and easier ways to accomplish a DoS, however, the possibility still exists.

Information about the SNORT rule this traffic matched on came from the SNORT.Org web database (http://www.snort.org/snort-db/sid.html?id=615) [12] as follows:

- "This signature is unfinished"
- "alert tcp $EXTERNAL_NET any -> $HOME_NET 8080 (msg:"SCAN Proxy attempt";flags:S; classtype:attempted-recon; sid:620; rev:1;) "
- "Attempted Information Leak "
- "Latest Revision: 1"

Information about the originator of this scan came from APNIC.Net (http://www.apnic.net) [60]:

**"Search results for '203.71.238.200'**

```
inetnum                  203.71.0.0 - 203.72.255.255
netname                  TANET
descr                    Taiwan Academic Network
country                  TW
admin-c                  CY1-TW, inverse
tech-c                   ZL1-TW, inverse
mnt-by                   MAINT-TWNIC-NS, inverse
changed                  snw@www.edu.tw 980908
source                   APNIC


person                   Ching-Hai Yin, inverse
address                  Taiwan Network Information Center
address                  Computer Center, Ministry of Education
address                  12th Fl, No. 106 Section 2, Hoping
East Rd.
address                  Taipei
address                  TW
phone                    +886-2-27377010 ext 213
fax-no                   +886-2-27377043
e-mail                   admin@twnmoe10.edu.tw, inverse
nic-hdl                  CY1-TW, inverse
mnt-by                   MAINT-TWNIC-NS, inverse
changed                  snw@ns.twnic.net 19980903
```

```
source                  APNIC

person                  Zi-Di Liu, inverse
address                 Taiwan Network Information Center
address                 Computer Center, Ministry of Education
address                 12th Fl, No. 106 Section 2, Hoping
East Rd.
address                 Taipei
address                 TW
phone                   +886-2-7377439
fax-no                  +886-2-7377043
e-mail                  color@twnmoe10.edu.tw, inverse
nic-hdl                 ZL1-TW, inverse
notify                  dbmon@apnic.net, inverse
mnt-by                  MAINT-NULL, inverse
changed                 hostmaster@apnic.net 19941214
source                  APNIC
```

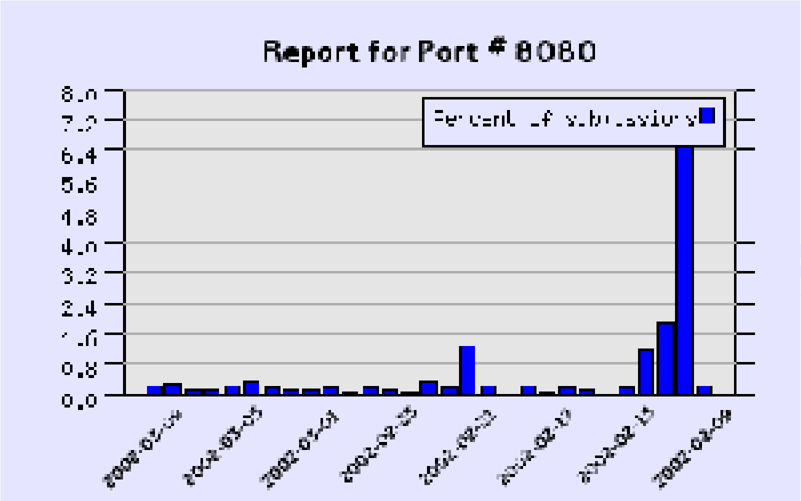
### ➢ Defensive recommendation

Any proxy servers you may have running should be restricted to responding to calls only from those systems inside of your network. Furthermore, you should keep your systems up to date with all upgrades and patches as they become available.

Once again, blocking all ports that are not specifically required and using NAT with a private IP addressing scheme should be the standard configuration of every network's perimeter defenses. I would also recommend using host-based firewalls to provide defense in depth in the event that an aggressor should gain access to your internal network.

### ➢ Correlation

1. What was the scope of the activity?
   This scan occurred between one source and 22 destinations on port 8080 (e.g. WinGate http://www.wingate.net/) [61]. The source was also part of the 7th Alert (Possible Squid Proxy Scan) and the Scan Log Analysis section at the end of this paper.



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=8080) [20]

2. Was the activity targeted at or against the site?
   Although the Top Listeners did receive more than one hit, this appears to be a scan that is looking for open proxy servers. The originator is, most likely, cataloguing targets of opportunity, not your specific network.

3. Did any destination receive an anomalous amount/type of traffic?
   Several destination IPs did receive more than one hit and may warrant investigation for possible proxy services and/or compromise.

4. Where there any indications of compromise?
   There were no obvious indications that a compromise occurred, but because several systems did receive more traffic than others, those systems should be assessed for the possibility of compromise, or at the very least to become aware of the services that they are running.

### 7th Alert – INFO - Possible Squid Scan

- **All sources triggering this attack signature**

| Source | # Alerts (sig) | # Alerts (total) | # Dsts (sig) | # Dsts (total) |
|---|---|---|---|---|
| 203.71.238.200 | 99 | 140 | 52 | 56 |

- **All destinations receiving this attack signature**

| Destinations | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|
| 10.1.152.127 | 6 | 9 | 1 | 1 |
| 10.1.150.14 | 5 | 40 | 1 | 3 |
| 10.1.152.125 | 5 | 10 | 1 | 1 |
| 10.1.152.120 | 4 | 9 | 1 | 2 |
| 10.1.150.55 | 3 | 11 | 1 | 3 |
| 10.1.150.172 | 3 | 12 | 1 | 4 |
| 10.1.150.170 | 3 | 13 | 1 | 4 |
| 10.1.153.71 | 3 | 5 | 1 | 1 |
| 10.1.153.134 | 2 | 2 | 1 | 1 |
| 10.1.153.117 | 2 | 2 | 1 | 1 |
| 10.1.153.136 | 2 | 2 | 1 | 1 |
| 10.1.150.106 | 2 | 2 | 1 | 1 |
| 10.1.153.119 | 2 | 2 | 1 | 1 |
| 10.1.150.195 | 2 | 129 | 1 | 4 |
| 10.1.153.123 | 2 | 2 | 1 | 1 |
| 10.1.150.51 | 2 | 10 | 1 | 4 |
| 10.1.153.106 | 2 | 2 | 1 | 1 |
| 10.1.153.124 | 2 | 2 | 1 | 1 |
| 10.1.153.107 | 2 | 2 | 1 | 1 |
| 10.1.153.125 | 2 | 2 | 1 | 1 |
| 10.1.150.147 | 2 | 11 | 1 | 4 |
| 10.1.153.108 | 2 | 2 | 1 | 1 |
| 10.1.153.126 | 2 | 2 | 1 | 1 |
| 10.1.153.109 | 2 | 3 | 1 | 1 |
| 10.1.153.127 | 2 | 2 | 1 | 1 |
| 10.1.150.84 | 2 | 8 | 1 | 4 |
| 10.1.151.75 | 2 | 3 | 1 | 2 |
| 10.1.153.111 | 2 | 2 | 1 | 1 |
| 10.1.152.212 | 2 | 3 | 1 | 2 |
| 10.1.153.113 | 2 | 2 | 1 | 1 |
| 10.1.153.116 | 2 | 2 | 1 | 1 |
| 10.1.88.160 | 1 | 4 | 1 | 3 |
| 10.1.153.120 | 1 | 2 | 1 | 1 |

| | | | | |
|---|---|---|---|---|
| 10.1.153.121 | 1 | 3 | 1 | 2 |
| 10.1.150.107 | 1 | 1 | 1 | 1 |
| 10.1.153.105 | 1 | 1 | 1 | 1 |
| 10.1.152.160 | 1 | 1 | 1 | 1 |
| 10.1.150.231 | 1 | 9 | 1 | 5 |
| 10.1.153.135 | 1 | 2 | 1 | 2 |
| 10.1.150.237 | 1 | 3 | 1 | 2 |
| 10.1.152.213 | 1 | 1 | 1 | 1 |
| 10.1.153.118 | 1 | 1 | 1 | 1 |
| 10.1.152.137 | 1 | 2 | 1 | 2 |
| 10.1.150.45 | 1 | 1 | 1 | 1 |
| 10.1.153.110 | 1 | 2 | 1 | 1 |
| 10.1.152.249 | 1 | 1 | 1 | 1 |
| 10.1.152.247 | 1 | 1 | 1 | 1 |
| 10.1.152.30 | 1 | 2 | 1 | 2 |
| 10.1.153.112 | 1 | 1 | 1 | 1 |
| 10.1.150.52 | 1 | 4 | 1 | 2 |
| 10.1.150.72 | 1 | 1 | 1 | 1 |
| 10.1.152.246 | 1 | 1 | 1 | 1 |

- **Brief description of the attack**

Earliest such alert at **01:58:10**.369412 *on 12/29/2001*
Latest such alert at **05:47:53**.679965 *on 12/29/2001*

My analysis for this activity is similar to that stated in the 6th Alert. It appears that in this scan the same originator is probing for proxy servers. Proxy servers, if misconfigured, can allow attackers to anonymize themselves and thus become difficult, if not impossible to track down. This serves to obscure their true identities. The intent of this scan is most likely to gather information about available/vulnerable proxies that can be catalogued and used at a later date. One such tool that probes on both port 8080 and 3128 is Ring Zero. Further information about Ring Zero can be found on the SANS.Org web site in Intrusion Detection FAQ (http://www.sans.org/newlook/resources/IDFAQ/ring_zero.htm) [5].

Alternatively, if an attacker gains access to a proxy server, then they could also have access to the internal network behind that proxy, thus defeating your perimeter defenses.

A less likely option is that of a Denial of Service (DoS) against your network. This is not as probable because there are better and easier ways to accomplish a DoS, however, the possibility still exists.

Information about the SNORT rule this traffic matched on came from the SNORT.Org web database (http://www.snort.org/snort-db/sid.html?id=618) [13] as follows:

- “alert tcp $EXTERNAL_NET any -> $HOME_NET 3128 (msg:"INFO - Possible Squid Scan"; flags:S; classtype:attempted-recon; sid:618; rev:1;) “
- “Attempted Information Leak “
- “Latest Revision: 1”
- “A external connection has been requested to the port squid runs on.”
- “This indicates someone looking for open web proxies on the $HOME_NET”
- “Squid is a caching web proxy server that runs on tcp/3128 by default.”
- “Attack Scenario: Banner ad hit couting External ips hiding web attacks behind web proxies”
- “Ease of Attack: Many automated scripts exist to increase banner ad revenue.”
- “False Positives: Legitimate external squid use.”
- “False Negatives: Squid can be configured to run on a port other than 3128.”
- “**Recommended Action**: From an $EXTERNAL_NET ip, telnet to 3128 on the $HOME_NET machine. If the connection is successful, try entering GET http://www.snort.org and press enter twice. If you see snort.org html, the proxy is open and this should be fixed.”

Information about the originator of this scan came from APNIC.net (http://www.apnic.net) [60]:

**“Search results for '203.71.238.200'**

```
inetnum                203.71.0.0 - 203.72.255.255
netname                TANET
descr                  Taiwan Academic Network
country                TW
admin-c                CY1-TW, inverse
tech-c                 ZL1-TW, inverse
mnt-by                 MAINT-TWNIC-NS, inverse
changed                snw@www.edu.tw 980908
source                 APNIC


person                 Ching-Hai Yin, inverse
address                Taiwan Network Information Center
address                Computer Center, Ministry of Education
address                12th Fl, No. 106 Section 2, Hoping
East Rd.
address                Taipei
address                TW
phone                  +886-2-27377010 ext 213
fax-no                 +886-2-27377043
e-mail                 admin@twnmoe10.edu.tw, inverse
```

```
nic-hdl                 CY1-TW, inverse
mnt-by                  MAINT-TWNIC-NS, inverse
changed                 snw@ns.twnic.net 19980903
source                  APNIC


person                  Zi-Di Liu, inverse
address                 Taiwan Network Information Center
address                 Computer Center, Ministry of Education
address                 12th Fl, No. 106 Section 2, Hoping
East Rd.
address                 Taipei
address                 TW
phone                   +886-2-7377439
fax-no                  +886-2-7377043
e-mail                  color@twnmoe10.edu.tw, inverse
nic-hdl                 ZL1-TW, inverse
notify                  dbmon@apnic.net, inverse
mnt-by                  MAINT-NULL, inverse
changed                 hostmaster@apnic.net 19941214
source                  APNIC
```

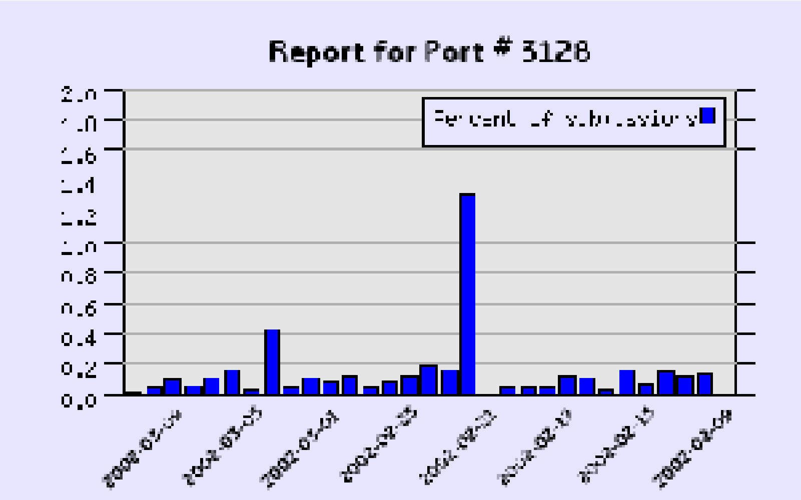
### ➢ Defensive recommendation

Any proxy servers you may have running should be restricted to responding to calls only from those systems inside of your network. Furthermore, you should keep your systems up to date with all upgrades and patches as they become available.

Once again, blocking all ports that are not specifically required and using NAT with a private IP addressing scheme should be the standard configuration of every network's perimeter defenses. I would also recommend using host-based firewalls to provide defense in depth in the event that an aggressor should gain access to your internal network.

### ➢ Correlation

1. What was the scope of the activity?
   This scan occurred between one source and 52 destinations on port 3128 (e.g. Squid http://www.squid-cache.org/) [62]. The source was also part of the 6th Alert (Scan Proxy Attempt) and the Scan Log Analysis section at the end of this paper.



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=3128) [21]

2. Was the activity targeted at or against the site?
   Although the Top Listeners did receive more than one hit, this appears to be a scan that is looking for open proxy servers. The originator is most likely cataloguing targets of opportunity, not your specific network.

3. Did any destination receive an anomalous amount/type of traffic?
   Several destination IPs did receive more than one hit and may warrant investigation for possible proxy services and/or compromise.

4. Where there any indications of compromise?
   There were no obvious indications that a compromise occurred, but because several systems did receive more traffic than others, those systems should be assessed for the possibility of compromise, or at the very least to become aware of the services that they are running. The SNORT.Org web site (http://www.snort.org/snort-db/sid.html?id=618) [13] recommends the following action: "From an $EXTERNAL_NET ip, telnet to 3128 on the $HOME_NET machine. If the connection is successful, try entering GET http://www.snort.org and press enter twice. If you see snort.org html, the proxy is open and this should be fixed."

### 8th Alert – SNMP public access

- **All sources triggering this attack signature**

| Source | # Alerts (sig) | # Alerts (total) | # Dsts (sig) | # Dsts (total) |
|---|---|---|---|---|
| 10.1.88.240 | 124 | 124 | 1 | 1 |
| 10.1.111.156 | 52 | 52 | 9 | 9 |
| 10.1.150.198 | 21 | 21 | 1 | 1 |
| 10.1.111.197 | 19 | 19 | 9 | 9 |
| 10.1.183.11 | 5 | 5 | 3 | 3 |
| 10.1.186.10 | 2 | 2 | 1 | 1 |
| 10.1.150.127 | 1 | 13 | 1 | 2 |
| 10.1.150.128 | 1 | 28 | 1 | 2 |
| 10.1.150.26 | 1 | 1 | 1 | 1 |

- **All destinations receiving this attack signature**

| Destinations | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|
| 10.1.150.195 | 127 | 129 | 3 | 4 |
| 10.1.150.14 | 30 | 40 | 2 | 3 |
| 10.1.151.114 | 21 | 21 | 1 | 1 |
| 10.1.150.147 | 7 | 11 | 3 | 4 |
| 10.1.150.51 | 6 | 10 | 2 | 4 |
| 10.1.150.231 | 6 | 9 | 3 | 5 |
| 10.1.150.55 | 5 | 11 | 1 | 3 |
| 10.1.150.172 | 5 | 12 | 1 | 4 |
| 10.1.150.243 | 4 | 5 | 2 | 3 |
| 10.1.153.219 | 3 | 4 | 2 | 3 |
| 10.1.150.170 | 3 | 13 | 1 | 4 |
| 10.1.88.187 | 2 | 3 | 1 | 2 |
| 10.1.88.160 | 2 | 4 | 1 | 3 |
| 10.1.150.52 | 2 | 4 | 1 | 2 |
| 10.1.150.84 | 2 | 8 | 2 | 4 |
| 10.1.150.178 | 1 | 1 | 1 | 1 |

- **Brief description of the attack**

Earliest such alert at **01:00:27**.327593 *on 12/29/2001*
Latest such alert at **23:51:28**.220230 *on 01/02/2002*

A significant amount of information and options can be accessed by sending SMNP queries to a given system. Some of the general information found in SNMP PDUs is listed at the

RAD Data Communication's web site (http://www.rad.com/networks/1995/snmp/snmp.htm) [63].

The SNORT.Org web database did not contain an entry that gave insight as to what triggered this detect, but my experience coincides with a posting by Bryce Alexander at the SANS.Org Global Incident Analysis Center web site (http://www.sans.org/y2k/051200.htm) [6] which indicates that this detect is triggered by an attacker who "tries to make a SNMP request using the password 'public'… May 5 17:45:52 myhost snort[290]: SNMP public access: 24-216-1-10.hsacorp.net:39343 -> my.ip.addr:161." It is important to note that many default passwords and community strings are readily available on the internet, but I won't give those links here.

Because the activity in this detect was a probe using the "public" password, I would rule out that this was related to the recent vulnerability in SNMP that was posted by CERT.Org as CERT® Advisory CA-2002-03 (http://www.cert.org//advisories/CA-2002-03.html) [45]. However, because the source and destination IP addresses are part of the same local private IP addressing scheme, as was discussed in an earlier detect, I would suspect either a compromised/misconfigured system or an internal user(s) had originated this traffic.

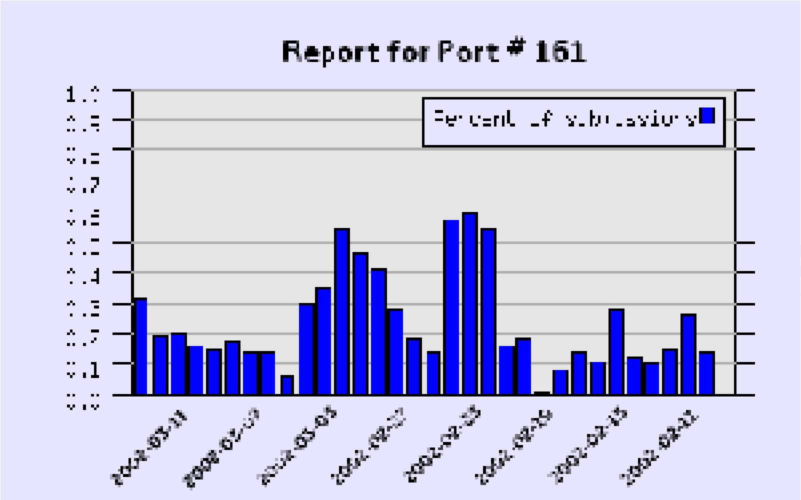
- **Defensive recommendation**

Make sure that no default passwords or community strings are being used or have been overlooked on the network. Disable/remove any unnecessary services and applications that are not part of your configuration management policy.

Again, blocking all ports that are not specifically required and using NAT with a private IP addressing scheme should be the standard configuration of every network's perimeter defenses. In this case, you should be blocking specifically SNMP related ports and following those recommendations listed in the CERT® Advisory CA-2002-03 (http://www.cert.org//advisories/CA-2002-03.html) [45]. I would also recommend using host-based firewalls to provide defense in depth in the event that an aggressor should gain access to your internal network. However, in this case the source and destination IPs appear to be from the same private IP addressing scheme, thus indicating either an internal compromise, a misconfigured system, or valid traffic. A hands-on investigation would be required to track down the exact cause of this traffic and also to determine if it is malicious or a simple misconfiguration.

- **Correlation**

1. What was the scope of the activity?
   The attempts occurred between 9 sources and 16 destinations, some of which will probably be misconfigured SNMP implementations.



*From the DSHIELD.Org web site (http://www.dshield.org/port_report.php?port=161) [22]

2. Was the activity targeted at or against the site?
   Besides matching a SNORT rule, the dispersion of traffic and the fact that it was internal to the network leads me to believe that at least some part of this activity was targeted and warrants further investigation.

3. Did any destination receive an anomalous amount/type of traffic?
   If indeed there was a compromised system, or insider, probing for default strings/passwords, then all such activity should be considered anomalous and scrutinized, beginning with the top talkers and listeners.

4. Where there any indications of compromise?
   There were no obvious compromises, but the type of traffic and the characteristics of the signature support the potential for a compromise and thus warrant an in depth investigation, if not just for the purpose of locking down the SNMP configuration and securing the network.

### 9th Alert – ICMP Router Selection

- **All sources triggering this attack signature**

| Source | # Alerts (sig) | # Alerts (total) | # Dsts (sig) | # Dsts (total) |
|---|---|---|---|---|
| 10.1.150.165 | 207 | 207 | 1 | 1 |
| 10.1.88.181 | 144 | 144 | 1 | 1 |
| 10.1.153.71 | 138 | 138 | 1 | 1 |
| 10.1.150.24 | 51 | 51 | 1 | 1 |
| 10.1.150.99 | 51 | 51 | 1 | 1 |
| 10.1.153.117 | 33 | 33 | 1 | 1 |
| 10.1.153.45 | 27 | 27 | 1 | 1 |
| 10.1.150.116 | 27 | 27 | 1 | 1 |
| 10.1.150.37 | 27 | 27 | 1 | 1 |
| 10.1.150.128 | 27 | 28 | 1 | 2 |
| 10.1.150.254 | 21 | 21 | 1 | 1 |
| 10.1.153.119 | 19 | 19 | 1 | 1 |
| 10.1.150.166 | 18 | 18 | 1 | 1 |
| 10.1.150.72 | 18 | 18 | 1 | 1 |
| 10.1.150.100 | 15 | 15 | 1 | 1 |
| 10.1.150.241 | 15 | 15 | 1 | 1 |
| 10.1.150.129 | 15 | 15 | 1 | 1 |
| 10.1.150.97 | 15 | 15 | 1 | 1 |
| 10.1.153.116 | 15 | 15 | 1 | 1 |
| 10.1.88.209 | 14 | 14 | 1 | 1 |
| 10.1.150.102 | 12 | 12 | 1 | 1 |
| 10.1.150.137 | 12 | 12 | 1 | 1 |
| 10.1.150.79 | 12 | 12 | 1 | 1 |
| 10.1.150.185 | 12 | 12 | 1 | 1 |
| 10.1.150.127 | 12 | 13 | 1 | 2 |
| 10.1.151.90 | 9 | 9 | 1 | 1 |
| 10.1.153.111 | 9 | 9 | 1 | 1 |
| 10.1.153.106 | 9 | 9 | 1 | 1 |
| 10.1.150.106 | 9 | 9 | 1 | 1 |
| 10.1.150.218 | 9 | 9 | 1 | 1 |
| 10.1.150.35 | 9 | 9 | 1 | 1 |
| 10.1.150.125 | 9 | 9 | 1 | 1 |
| 10.1.153.107 | 9 | 9 | 1 | 1 |
| 10.1.151.73 | 9 | 9 | 1 | 1 |
| 10.1.150.73 | 6 | 6 | 1 | 1 |
| 10.1.151.67 | 6 | 6 | 1 | 1 |
| 10.1.153.112 | 6 | 6 | 1 | 1 |
| 10.1.150.223 | 6 | 6 | 1 | 1 |
| 10.1.151.64 | 6 | 6 | 1 | 1 |

|  |  |  |  |  |
|---|---|---|---|---|
| 10.1.153.113 | 6 | 6 | 1 | 1 |
| 10.1.153.46 | 6 | 6 | 1 | 1 |
| 10.1.153.122 | 6 | 6 | 1 | 1 |
| 10.1.70.237 | 6 | 6 | 1 | 1 |
| 10.1.150.210 | 6 | 6 | 1 | 1 |
| 10.1.153.125 | 6 | 6 | 1 | 1 |
| 10.1.153.115 | 6 | 6 | 1 | 1 |
| 10.1.150.121 | 6 | 6 | 1 | 1 |
| 10.1.150.136 | 6 | 6 | 1 | 1 |
| 10.1.150.122 | 6 | 6 | 1 | 1 |
| 10.1.88.245 | 6 | 6 | 1 | 1 |
| 10.1.153.120 | 6 | 6 | 1 | 1 |
| 10.1.153.105 | 6 | 6 | 1 | 1 |
| 10.1.153.136 | 6 | 6 | 1 | 1 |
| 10.1.153.114 | 6 | 6 | 1 | 1 |
| 10.1.150.214 | 6 | 6 | 1 | 1 |
| 10.1.153.127 | 6 | 6 | 1 | 1 |
| 10.1.153.137 | 6 | 6 | 1 | 1 |
| 10.1.153.121 | 6 | 6 | 1 | 1 |
| 10.1.150.216 | 6 | 6 | 1 | 1 |
| 10.1.151.33 | 5 | 5 | 1 | 1 |
| 10.1.150.16 | 4 | 4 | 1 | 1 |
| 10.1.151.78 | 3 | 3 | 1 | 1 |
| 10.1.151.97 | 3 | 3 | 1 | 1 |
| 10.1.151.79 | 3 | 3 | 1 | 1 |
| 10.1.151.98 | 3 | 3 | 1 | 1 |
| 10.1.151.89 | 3 | 3 | 1 | 1 |
| 10.1.151.99 | 3 | 3 | 1 | 1 |
| 10.1.88.234 | 3 | 3 | 1 | 1 |
| 10.1.150.120 | 3 | 3 | 1 | 1 |
| 10.1.88.225 | 3 | 3 | 1 | 1 |
| 10.1.88.163 | 3 | 3 | 1 | 1 |
| 10.1.150.240 | 3 | 3 | 1 | 1 |
| 10.1.88.174 | 3 | 3 | 1 | 1 |
| 10.1.150.141 | 3 | 3 | 1 | 1 |
| 10.1.150.160 | 3 | 3 | 1 | 1 |
| 10.1.88.184 | 3 | 3 | 1 | 1 |
| 10.1.150.124 | 3 | 3 | 1 | 1 |
| 10.1.150.232 | 3 | 3 | 1 | 1 |
| 10.1.88.158 | 3 | 3 | 1 | 1 |
| 10.1.150.206 | 3 | 3 | 1 | 1 |
| 10.1.150.161 | 3 | 3 | 1 | 1 |
| 10.1.88.188 | 3 | 3 | 1 | 1 |
| 10.1.153.126 | 3 | 3 | 1 | 1 |

|  |  |  |  |  |
|---|---|---|---|---|
| 10.1.150.21 | 3 | 3 | 1 | 1 |
| 10.1.150.13 | 3 | 3 | 1 | 1 |
| 10.1.151.21 | 3 | 3 | 1 | 1 |
| 10.1.151.30 | 3 | 3 | 1 | 1 |
| 10.1.151.14 | 3 | 3 | 1 | 1 |
| 10.1.152.119 | 3 | 3 | 1 | 1 |
| 10.1.150.42 | 3 | 3 | 1 | 1 |
| 10.1.151.85 | 3 | 3 | 1 | 1 |
| 10.1.151.61 | 3 | 3 | 1 | 1 |
| 10.1.88.196 | 3 | 3 | 1 | 1 |
| 10.1.151.70 | 3 | 3 | 1 | 1 |
| 10.1.151.62 | 3 | 3 | 1 | 1 |
| 10.1.151.17 | 3 | 3 | 1 | 1 |
| 10.1.151.80 | 3 | 3 | 1 | 1 |
| 10.1.150.224 | 3 | 3 | 1 | 1 |
| 10.1.150.63 | 3 | 3 | 1 | 1 |
| 10.1.151.63 | 3 | 3 | 1 | 1 |
| 10.1.153.135 | 3 | 3 | 1 | 1 |
| 10.1.150.46 | 3 | 3 | 1 | 1 |
| 10.1.151.106 | 3 | 3 | 1 | 1 |
| 10.1.153.118 | 3 | 3 | 1 | 1 |
| 10.1.151.72 | 3 | 3 | 1 | 1 |
| 10.1.150.229 | 3 | 3 | 1 | 1 |
| 10.1.150.56 | 3 | 3 | 1 | 1 |
| 10.1.151.91 | 3 | 3 | 1 | 1 |
| 10.1.153.109 | 3 | 3 | 1 | 1 |
| 10.1.150.146 | 3 | 3 | 1 | 1 |
| 10.1.151.65 | 3 | 3 | 1 | 1 |
| 10.1.151.115 | 3 | 3 | 1 | 1 |
| 10.1.150.75 | 3 | 3 | 1 | 1 |
| 10.1.151.74 | 3 | 3 | 1 | 1 |
| 10.1.153.108 | 3 | 3 | 1 | 1 |
| 10.1.151.66 | 3 | 3 | 1 | 1 |
| 10.1.150.126 | 3 | 3 | 1 | 1 |
| 10.1.151.75 | 3 | 3 | 1 | 1 |

- **All destinations receiving this attack signature**

| Destinations | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total) |
|---|---|---|---|---|
| 224.0.0.2 | 1368 | 1368 | 118 | 118 |

### ➢ Brief description of the attack

Earliest such alert at **02:59:41**.402224 *on 12/29/2001*
Latest such alert at **23:54:08**.335080 *on 01/02/2002*

RFC1256 can be found at the web/ftp site ftp://ftp.rfc-editor.org/in-notes/rfc1256.txt [59] and specifies router-selection as "an extension of the Internet Control Message Protocol (ICMP) to enable hosts attached to multicast or broadcast networks to discover the IP addresses of their neighboring routers" or more simply, "Router Discovery Messages." This is used to communicate with all hosts on that subnet by allowing two-way communications with those multiple hosts, hence the destination's "multicast" IP address (224.0.0.2) from this detect.

Because there are relatively few hosts per subnet that are using this destination address, combined with the fact that they are internal private IP addresses, using a large address space, and executing the correct use of ICMP type 10 code 0 packets, I would have to assess this traffic as valid and contribute the detects to the wide distribution of the network across a LAN/MAN enterprise.

The only alternative to this scenario is that of reconnaissance for the purposes of "owning" the university's backbone. However, because of the diversity among the select IP addresses that were captured , this is not as strong of a possibility. Note that the IP addresses should still be correlated against the network topology to make sure that something anomalous has not happened, and that misconfigured of routing devices been implemented.

Information about the SNORT rule this traffic matched on came from the SNORT.Org web database (http://www.snort.org/snort-db/sid.html?id=443) [14] as follows and apparently triggers on Type/Code only:

- "This signature is unfinished"
- "alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Router Selection"; itype: 10; icode: 0; reference:arachnids,174; sid:443; classtype:misc-activity; rev:4;)"
- "Misc activity"
- "Latest Revision: 4"

### ➢ Defensive recommendation

I do not believe this to be a malicious attack, but still recommend the following defensive measures. Make sure that your routers are configured correctly. They should typically not be forwarding or routing broadcasts or reserved/private IP addresses. However, in this environment, they may perform this type of activity internally. You should also evaluate your infrastructure for design weaknesses and scalability. Also look for back doors that may have been installed on your network. These are always a bad idea unless absolutely necessary. If they are required, then be sure to secure them just as you would the rest of your perimeter.

Blocking all ports that are not specifically required should be the standard configuration of every network's perimeter defenses. You may also want to implement egress filtering to ensure that IP addresses are not spoofed from within your network. Furthermore, using a host-based firewall and NAT with planned internal private addressing is also a best practices recommendation.

Finally, you should look into configuration management and security policies that will help provide continuity across your enterprise. This may require user and administrator training. As indicated before, some network troubleshooting may be required to prove that this scenario is correct.

### ➢ Correlation

1. What was the scope of the activity?
   118 local hosts were sending Router Selection packets to a single multicast IP address. This is not necessarily anomalous activity.

2. Was the activity targeted at or against the site?
   No. The traffic was all sent to a multicast IP address. The only affect this may have had on the site was that of increase bandwidth consumption.

3. Did any destination receive an anomalous amount/type of traffic?
   No destinations received an anomalous amount/type of traffic.

4. Where there any indications of compromise?
   There were no indications of compromise or malicious activity.

## OOS Log Analysis –

The top 5 OOS Source and Destination ports were:

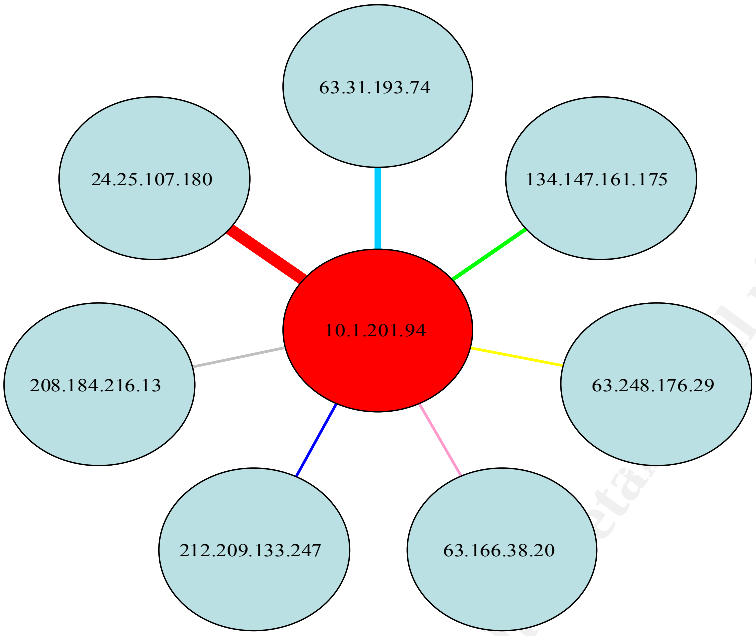
| Source Port | # Pkts | Destination Port | # Pkts |
|---|---|---|---|
| 18245 | 72 | 21536 | 72 |
| 5635 | 29 | 0 | 29 |
| 2728 | 21 | 3938 | 21 |
| 6688 | 9 | 6346 | 13 |
| 0 | 7 | 6688 | 11 |

Of the 220 OOS packets captured, all (220) had the TCP SYN flag set, 186 had at least one of the reserved bits set, 71 had TCP Options, 8 had all of the TCP flags set (Christmas Tree packets), 29 went to destination port 0, and 7 originated from source port 0. While a limited number of these packets may be attributed to general packet corruption or valid Explicit Congestion Notification (ECN: the TCP reserved bits), most of these are probably efforts to map or fingerprint your network and operating systems. Common OS fingerprinting tools include Nmap, Queso, and Hping.

The top 5 OOS Source and Destination IP addresses were:

| Top Sources | # of Pkts | Top Destinations | # of Pkts |
|---|---|---|---|
| 24.113.198.51 | 40 | 10.1.217.146 | 40 |
| 10.1.201.94 | 14 | 10.1.5.10 | 34 |
| 209.255.180.144 | 10 | 10.1.253.112 | 25 |
| 209.255.214.109 | 9 | 10.1.253.114 | 24 |
| 209.255.213.140 | 9 | 10.1.100.165 | 10 |

None of these OOS source IP addresses sent traffic that correlated to the Alert Log Analysis section of this paper. Also, only the 10.1.201.94 source IP sent OOS packets to more than one host:



*The width of the line corresponds with the number of packets received (5 - 1).

I would recommend investigating all of the IP addresses in these logs and would analyze more of the history associated with each IP.  Note that because 10.1.201.94 is one of UMBC's internal systems, and it appears to be generating OOS packets, you should place it at the top of your priority list.

## Scan Log Analysis –

The following are the source IP addresses and the destination ports of the top 10 scanners, none of these were part of the top 5 OOS sources:

| Source IP | Dest Port | # of Hits | Dates Active |
|---|---|---|---|
| 203.71.238.200 | 3128 / 8000 / 8080 | 163 | 29 Dec 01 |
| 80.11.22.201 | 21 | 69 | 02 Jan 02 |
| *10.1.6.45 | 7000 -> 7001 (UDP) | 53 | 29-30 Dec 01 & 02 Jan 02 |
| 194.224.200.103 | 22 | 49 | 29 Dec 01 |
| **129.71.215.240 | 22 | 26 | 31 Dec 01 |
| 128.239.3.11 | 22 | 24 | 29 Dec 01 |
| 217.11.104.51 | 11 | 21 | 01 Jan 02 |
| 164.15.131.4 | 22 | 21 | 30 Dec 01 |
| 62.144.114.48 | 53 | 20 | 29 Dec 01 |
| 193.253.230.174 | 21 | 18 | 31 Dec 01 |

*This was UDP traffic, all others were TCP
**This was a SYN-FIN scan; all others were SYN scans only

**203.71.238.200** – This was a SYN scan on ports 3128, 8000, and 8080 and was discussed earlier in the 6th and 7th Alerts.

**80.11.22.201 & 193.253.230.174** – These were SYN scans on port 21 in which a few hosts were hit twice. There were no indications of compromise.

**10.1.6.45** – This was UDP traffic from port 7000 to port 7001. There were only 3 sources and 46 destinations. The source port was 7000 (AFS File Server) and the destination port was 7001 (Cache Callback Manager Service). This indicates that this is probably an AFS file sharing application. I would recommend that, if this is authorized software, you ensure that the system is fully patched, running anti-virus, and running a host based firewall that is configured to only allow trusted machine through on these ports. These ports should also be blocked at the perimeter, because several trojans/backdoors are known to operate on this port or can be configured to listen on this port.

If this application is not authorized or the hosts involved are not "trusted," or you believe this to be suspicious activity, then investigate immediately and follow all of the previous defensive recommendations.

**194.224.200.103, 129.71.215.240, 128.239.3.11, & 164.15.131.4** – These were scans on port 22 where all of the sources only hit once per IP address with the exception of 128.239.3.11, who hit most of the targets twice, with approximately 2.5 minutes between the first and the second hit. There were no other indications of compromise.

The SYN-FIN scan by 129.71.215.240 was also discussed in the 4th Alert.

**217.11.104.51** – This was a SYN scan in which no IP addresses received more than one packet. Per the NetworkICE.com web site (http://advice.networkice.com/Advice/Exploits/Ports/11/default.htm) [32] "On some UNIX machines, creating a TCP connection to this port will dump the active processes and who launched them. The original intent for this was to make remote management of UNIX easier. However, intruders will query the `systat` information in order to map out the system."

**62.144.114.48** – This was a SYN scan on port 53 in which all of the host were hit only one time. There were no other indications of compromise.

## “Analyze This” Scenario – Conclusion

This is an open network that will require constant attention and enormous resources. Because of this environment, I will reiterate a few of my previous defensive recommendations, however, I feel strongly that a dedicated ensemble of equipment and personnel will be required to secure this enterprise appropriately. The Top 10 Talkers overall and Defensive Recommendations are listed below:

| Rank | Total # Alerts | **Source IP** | # Signatures triggered | Destinations involved |
|---|---|---|---|---|
| Rank #1 | 207 alerts | **10.1.150.165** | 1 signatures | 224.0.0.2 |
| Rank #2 | 144 alerts | **10.1.88.181** | 1 signatures | 224.0.0.2 |
| Rank #3 | 140 alerts | **203.71.238.200** | 2 signatures | (56 destination IPs) |
| Rank #4 | 138 alerts | **10.1.153.71** | 1 signatures | 224.0.0.2 |
| Rank #5 | 124 alerts | **10.1.88.240** | 1 signatures | 10.1.150.195 |
| Rank #6 | 52 alerts | **10.1.111.156** | 1 signatures | (9 destination IPs) |
| Rank #7 | 51 alerts | **10.1.150.24** | 1 signatures | 224.0.0.2 |
| | | **10.1.150.99** | 1 signatures | 224.0.0.2 |
| Rank #9 | 33 alerts | **10.1.153.117** | 1 signatures | 224.0.0.2 |
| rank #10 | 28 alerts | **10.1.150.128** | 2 signatures | 10.1.150.178, 224.0.0.2 |

*As output by SnortSnarf

**Defensive Recommendations:**

- Perform regular user/administrator training and security awareness
  - Work to eliminate all poor security practices

- Keep your personnel current with security training, trends, and tools
  - Stay in touch with what is happening in the “real world” (in the wild)
  - Subscribe to reputable security mailing lists

- Defensive posture should be to deny everything that is not explicitly allowed
  - Only if it is absolutely necessary should exceptions be made

- Perform egress filtering

- Null route sensitive ports/traffic (e.g. ICMP Echo Requests) via a router or firewall at the perimeter

- Create a screened subnet (DMZ) for those systems that require public access
  - Ensure you use a highly secure configuration

- Use NAT/PAT and a private internal IP addressing scheme

- Install Intrusion Detection Systems/Sensors
    - Hire dedicated security professionals to perform security related functions

- Consider developing a “Honey Pot” project

- Practice “Defense-in-Depth”
    - Use host-based firewalls to protect the systems/network
        - ISS’s BlackICE Defender (http://www.iss.net/products_services/hsoffice_protection/buy.php) [27]
        - Zone Lab’s ZoneAlarm (http://www.zonelabs.com/products/za/freedownload2.html) [26]
    - Keep up to date with all patches and upgrades for all systems
    - Disable/remove any unnecessary services/applications
    - Install anti-virus software and keep the engine/signatures up to date
    - Install an anti-virus email gateway that performs content filtering
    - Perform regular backups and store them off-site
    - Turn on auditing and logging where ever possible
    - Use encryption where ever possible
    - Develop and enforce a robust security and configuration management policy

- Perform risk analysis and risk management
    - Identify the critical parts of your infrastructure and prioritize
    - Develop contingency and emergency action plans

- Incorporate regular 3rd party security assessments and audits

- Become a member of the Security Community of Interest (COI)
    - Correlate your security experiences and findings with others

# Appendix A

## Analysis Tools –

**Tools Used during the Analysis Process:**

➢ Microsoft (MS) Office 2000 / XP

- http://www.microsoft.com/office/ork/xp/default.htm [57]

➢ Silicon Defense's SnortSnarf, v020124.1

- http://www.silicondefense.com/software/snortsnarf/ [15]

➢ Web Browser (MS-IE 6.0.2600.000) and various search engines

- www.google.com
- www.msn.com [64]
- www.yahoo.com [65]
- www.altavista.com [66]

➢ Generic Unix commands (this was quite cumbersome, especially with the OOS logs).

- more
- awk
- grep
- sort
- uniq
- vi editor

➢ I also used Perl (Comprehensive Perl Archive Network: http://www.cpan.org/) [67], but must give all credit to the invaluable assistance of Robert Nine, GCIA. The following code was provided and explained to me by Mr. Nine:

```
#!/usr/local/bin/perl
$/ = "";
while (<>) {
  if (/TCP Options /) {
    print;
  }
}
```

# Appendix B

# References (Assignment 3)

**Sources Cited in text (Assignment 3 – Analyze This):**

➢ SANS Institute Global Information Assurance Certification web site:
[1] SANS "Global Information Assurance Certification" 22 May 2001.
URL;http://www.giac.org/GCIA_assign_29.php#7 (04 March 2002).

➢ SANS Institute web sites:
[2] Alexander, Bryce. "Port 137 Scan" 10 May 2000.
URL:http://www.sans.org/newlook/resources/IDFAQ/port_137.htm (04 March 2002).

[3] Alexander, Bryce. "Followup on a Honeypot Catch"
URL:http://www.sans.org/y2k/honeypot_catch.htm (04 March 2002).

[4] Northcutt, Stephen. "Detects Analyzed 7/25/00" 25 July 2000.
URL:http://www.sans.org/y2k/072500-1200.htm (04 March 2002).

[5] Northcutt, Stephen ."Massive scanning for proxies/possible Trojan activity" 11 October 1999. URL:http://www.sans.org/newlook/resources/IDFAQ/ring_zero.htm (04 March 2002).

[6] Northcutt, Stephen. "Detects Analyzed 5/12/00" 12 May 2000.
URL:http://www.sans.org/y2k/051200.htm (04 March 2002).

➢ SANS Institute Incidents.Org web site:
[7] Incidents.org. "Handler's Comments" 7 March 2002.
URL:http://www.incidents.org/diary/diary.php?id=148 (07 March 2002).

➢ University of Maryland, Baltimore County web site:
[8] University of Maryland, Baltimore County "Index of /~Andy" 18 March 2002.
URL:http://www.research.umbc.edu/~andy (18 March 2002).

➢ Snort.Org:
[9] Snort.org. "The Open Source Network Intrusion Detection System"
URL:http://www.snort.org/ (04 March 2002).

[10] Snort.org. "Signatures Database" URL:http://www.snort.org/snort-db/all.html (04 March 2002).

[11] Snort.org. “Signatures Database” URL:http://www.snort.org/snort-db/sid.html?id=466 (04 March 2002).

[12] Snort.org. “Signatures Database” URL:http://www.snort.org/snort-db/sid.html?id=615 (04 March 2002).

[13] Snort.org. “Signatures Database” URL:http://www.snort.org/snort-db/sid.html?id=618 (04 March 2002).

[14] Snort.org. “Signatures Database” URL:http://www.snort.org/snort-db/sid.html?id=443 (04 March 2002).

- The Silicon Defense web site:
[15] Silicondefense.com “Snort Snarf” http://www.silicondefense.com/software/snortsnarf/ (04 March 2002).

- DShield.Org:
[16]Dshield.org. URL:http://www.dshield.org/ (04 March 2002).

[17] Dshield.org. “Port Report for 137-Netbios:NS” URL:http://www.dshield.org/port_report.php?port=137 (04 March 2002).

[18] Dshield.org. “Port Report for 22-SSH” URL:http://www.dshield.org/port_report.php?port=22 (04 March 2002).

[19] Dshield.org. “Port Report for 139-Netbios:SSN” URL:http://www.dshield.org/port_report.php?port=139 (04 March 2002).

[20] Dshield.org. “Port Report for 8080-HTTP-ALT” URL:http://www.dshield.org/port_report.php?port=8080 (04 March 2002).

[21] Dshield.org. “Port Report for 3128-Squid:HTTP” URL:http://www.dshield.org/port_report.php?port=3128 (04 March 2002).

[22] Dshield.org. “Port Report for 161-SNMP” URL:http://www.dshield.org/port_report.php?port=161 (04 March 2002).

- SamSpade.Org:
[23] Samspade.org. URL:http://www.samspade.org/ (04 March 2002).

- Insecure.Org:
[24]Insecure.org. “NMAP”. URL:http://www.insecure.org/nmap/ (04 March 2002).

- Hping.Org:
[25] Hping.org. URL:http://www.hping.org/ (04 March 2002).

- Zone Labs web site:
[26] Zonelabs.com "Downloads".
URL:http://www.zonelabs.com/products/za/freedownload2.html (04 March 2002).

- Internet Security Systems (ISS) web sites:
[27] ISS.net. "Purchase BlackICE Defender"
URL:http://www.iss.net/products_services/hsoffice_protection/buy.php (04 March 2002).

- Insecure.Org:
[28] Incidents.org. "137 NetBIOS Name Service Probe Activity"
URL:http://lists.insecure.org/incidents/2000/Mar/0270.html (04 March 2002).

[29] Incidents.org. "UDP 137 NetBIOS Name Service Probe Activity"
URL:http://lists.insecure.org/incidents/2000/Mar/0308.html (04 March 2002).

- NetworkICE web sites:
[30] Advice.networkice.com. "Port 137 Netbios-ns"
URL:http://advice.networkice.com/Advice/Exploits/Ports/137/default.htm (04 March 2002).

[31] Advice.networkice.com. "Port Microsoft"
URL:]http://advice.networkice.com/Advice/Exploits/Ports/groups/Microsoft/default.htm (04 March 2002).

[32] Advice.networkice.com. "Port 11 Systat"
URL:http://advice.networkice.com/Advice/Exploits/Ports/11/default.htm (04 March 2002).

- The Neohapsis web site archives for incidents@securityfocus.com:
[33] Neophasis.com "Neophasis Archives"
URL:http://archives.neohapsis.com/archives/incidents/2001-05/0034.html (04 March 2002).

[34] Neophasis.com "Neophasis Archives"
URL:http://archives.neohapsis.com/archives/incidents/2000-04/0002.html (04 March 2002).

[35] Neophasis.com "Neophasis Archives"
URL:http://archives.neohapsis.com/archives/incidents/2000-04/0013.html (04 March 2002).

➢ Carnegie Mellon Software Engineering Institute's CERT Coordination Center web sites:

[36] cert.org. "Exploitation of Unprotected Windows Networking Shares" 7 April 2000. URL:http://www.cert.org/incident_notes/IN-2000-02.html (04 March 2002).

[37] cert.org. "Denial of Service Attack in NetBIOS Services" 29 November 2000. URL:http://www.kb.cert.org/vuls/id/32650 (04 March 2002).

[38] cert.org. "Denial of Service Attack in NetBIOS Services" 10 August 2000. URL:http://www.cert.org/vul_notes/VN-2000-03.html (04 March 2002).

[39] cert.org. "SSH CRC32 attack detection code contains remote integer overflow" 05 March 2002. URL:http://www.kb.cert.org/vuls/id/945216 (04 March 2002).

[40] cert.org. "Recent Activity Against Secure Shell Daemons" 14 December 2001. URL:http://www.cert.org/advisories/CA-2001-35.html (04 March 2002).

[41] cert.org. "Exploitation of vulnerability in SSH1 CRC-32 compensation attack detector" 7 November 2001. URL:http://www.cert.org/incident_notes/IN-2001-12.html (04 March 2002).

[42] cert.org. "Weak CRC allows packet injection into SSH sessions encrypted with block ciphers" 7 November 2001. http://www.kb.cert.org/vuls/id/13877 (04 March 2002).

[43] cert.org. "CERT® Summary CS-2001-04" 20 November 2001. http://www.cert.org/summaries/CS-2001-04.html (04 March 2002).

[44] cert.org. "CERT® Summary CS-2002-01" URL:28 February 2002. URL:http://www.cert.org/summaries/CS-2002-01.html (04 March 2002).

[45] cert.org. "CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)" 18 March 2002 URL:http://www.cert.org//advisories/CA-2002-03.html (18 March 2002).

➢ Google.Com

[46] google.com http://www.google.com (04 March 2002).

➢ Mitre Corporation's Common Vulnerabilities and Exposures web sites:

[47] cve.mitre.org. "Denial of service in WINS with malformed data to port 137 (NETBIOS Name Service)." 25 August 1999. URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0288 (04 March 2002).

[48] cve.mitre.org. “Buffer overflow in Samba smbd program via a malformed message command.” 18 January 2000. URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0811 (04 March 2002).

[49] cve.mitre.org. “Windows 95 and Windows 98 allow a remote attacker to cause a denial of service via a NetBIOS session request packet with a NULL source name.” 13 January 2000. URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0347 (04 March 2002).

[50] cve.mitre.org. “The NetBIOS Name Server (NBNS) protocol does not perform authentication, which allows remote attackers to cause a denial of service by sending a spoofed Name Conflict or Name Release datagram, aka the "NetBIOS Name Server Protocol Spoofing" vulnerability.” 13 October 2000. URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0673 (04 March 2002).

[51] cve.mitre.org. “CORE SDI SSH1 CRC-32 compensation attack detector allows remote attackers to execute arbitrary commands on an SSH server or client via an integer overflow.” 7 May 2001. URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0144 (04 March 2002).

[52] cve.mitre.org. “CAN-2002-0083 (under review)” 6 March 2002. URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0083 (04 March 2002).

➢ Windows Guide Network’s WinGuide web site:
[53] Winguides.com. “Security Guide” URL:http://www.winguides.com/search.php?guide=security&keywords=netbios+name+service (04 March 2002).

➢ Arin.Net:
[54] Arin.net. URL:http://www.arin.net/whois/index.html (04 March 2002).

➢ U.S. Dept. of Energy’s Computer Incident Advisory Capability (CIAC) web site:
[55] ciac.org. 20 December 2001. “CIACTech02-001: Understanding the SSH CRC32 Exploit” URL:http://www.ciac.org/ciac/techbull/CIACTech02-001.shtml (04 March 2002).

➢ Microsoft web site:
[56] Microsoft.com. “Automatic Windows 98/Me TCP/IP Addressing Without a DHCP Server (Q220874)” 2 July 1999. URL:http://support.microsoft.com/default.aspx?scid=kb;EN-US;q220874 (04 March 2002).

[57] Microsoft.com. “Office XP Update: Service Pack 1 (SP-1)” 21 February 2002. URL:http://www.microsoft.com/office/ork/xp/default.htm (04 March 2002).

- Network Working Group's Request for Comments (RFC) web site:
  [58] ftp.rfc-editor.org. "DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients" May 1999. ftp://ftp.rfc-editor.org/in-notes/rfc2563.txt (04 March 2002).

  [59] ftp.rfc-editor.org. "ICMP Router Discovery Messages" September 1991. ftp://ftp.rfc-editor.org/in-notes/rfc1256.txt (04 March 2002).

- APNIC.Net:
  [60] Apnic.net. http://www.apnic.net (04 March 2002).

- WinGate.Net:
  [61] Wingate.net. http://www.wingate.net/ (04 March 2002).

- Squid-Cache.Org:
  [62] Squid-cache.org. http://www.squid-cache.org/ (04 March 2002).

- RAD Data Communications web site:
  [63]Cohen, Yoram. "SNMP - Simple Network Managment Protocol" URL:http://www.rad.com/networks/1995/snmp/snmp.htm (04 March 2002).

- The Microsoft Network web site:
  [64] MSN.com. www.msn.com (04 March 2002).

- Yahoo.Com:
  [65] Yahoo.com. www.yahoo.com (04 March 2002).

- Altavista.Com:
  [66] Altivista.com. www.altavista.com (04 March 2002).

- Comprehensive Perl Archive Network web site:
  [67] Cpan.org. http://www.cpan.org/ (04 March 2002).

## Acknowledgements –

I would like to acknowledge the following sources for ideas while performing this practical:

Nine, Robert. "SANS GIAC Certification, GCIA Practical Assignment V 2.9" 30 August 2001. URL: http://www.giac.org/practical/Robert_Nine_GCIA.doc (04 March 2002).

Leach, David. "SANS Intrusion Detection in Depth GCIA Practical Assignment Version 2.9" 29 October 2001. URL: http://www.giac.org/practical/David_Leach_GCIA.doc (04 March 2002).

Lukacs, Steve. "GCIA Certification Practical Assignments" 29 October 2001. URL: http://www.giac.org/practical/Steve_Lukacs_GCIA.doc (04 March 2002).

Stevens, W. Richard. TCP/IP Illustrated, Volume 1. Reading: Addison Wesley Longman, Inc, 1994.

Northcutt, Stephen and Novak, Judy. Network Intrusion Detection: An Analyst Handbook, 2 ed. New Riders Publishing. 2001.