GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

SANS/GIAC
Intrusion Detection in Depth
GCIA Practical Assignment
Version 3.0 (revised Aug. 13, 2001)

SANS Network Security
San Diego CA
October 15 - 22, 2001

Prepared by Tomas Alex

December 27, 2001

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

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

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

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

Assignment 1 – Implementation Considerations of Intrusion Detection Systems

Introduction

Mounting security threats and the number of attacks on network systems is growing prompting security professionals to implement a variety of devices to stop and detect these intrusions. As part of an organisation's defence in-depth implementation, Intrusion Detection Systems (IDS) have become an integral part to detect and alert any unwanted network and host activity. Firewalls and border routers are the network security policy enforcement points at the perimeter. IDSes can let you know when these perimeter defences have been breached or if there is any unwanted activity launched from within the corporate network. There are three broad categories of IDSes:

- Host IDS (HIDS)

  Host based ID involves loading a software agent on the system to be monitored. The agent will scrutinize event logs, system and application files, and other auditable resources looking for any unauthorized changes or suspicious patterns of activity. Upon detection, an alert or SNMP trap can automatically raised.

- Network IDS (NIDS)

  Monitors network traffic on a network segment examining and matching packets against a known database of attacks, or performing protocol decodes to detect anomalies, or both. When suspicious activity is detected, an alert can be raised or the offending connection can be terminated. The NIDS sensor (hardware with IDS software) functions in promiscuous mode allowing all packets to be examined. Like a HIDS, alerts and SNMP traps can automatically be raised.

- Network Node IDS (NNIDS)

  Monitors network traffic on a network segment destined for the network node (i.e. system) on which the software agent resides. This agent functions in a similar manner to a NIDS but since it does not examine every packet in the network segment, it takes less system resources. NNIDS are particularly suitable in VPN implementations with encrypted traffic as the traffic can be examined after it is decrypted. Alerts can be raised similar to a HIDS and NIDS.

IDSes primarily provide:

- A greater level of detail not achieved by perimeter devices (i.e. routers and firewalls). This also allows for a tighter watch to be kept on the corporate network and critical machines that were accessed.

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

- Recorded historical traffic logs to determine anomalous activities and produce legal documentation as required.

- The ability to detect, identify, and stop an intruder. They support investigations to find out how the intruder got in and stop the exploit from use by future intruders.

- The ability to troubleshoot misconfigured systems on the network. Common problems detected are often in the form of the broadcasting of local loopback address, 127.0.0.1, incorrect subnet masks, and misconfigured DNS files.

IDSes can provide these benefits only if successfully deployed, managed, and monitored. The intent of this paper is to provide a set of implementation considerations to effectively utilize an IDS in the enterprise.

Planning

It is important to understand that the deployment of a corporate IDS requires careful thought and planning and should be proportional to the value of the assets being secured. What kinds of resources need to be protected? Are you worried about intruders breaking through the firewall and comprising your Internet web servers? Are you worried about suspicious internal network activity destined out to the Internet or to critical servers? All of this must be defined prior to deploying any IDS.

The type of sensors deployed will be dependent on the resources to be protected and may be a combination of network and host-based intrusion detection mechanisms. Also, prior to loading the IDS on the sensor, the OS on the host that the IDS resides on must be made secure.

Deployment

Although each network architecture may vary, IDS deployment should follow the guidelines to secure high valued resources as illustrated below in figure 1.

© SANS Institute 2000 - 2002 Author retains full rights.

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

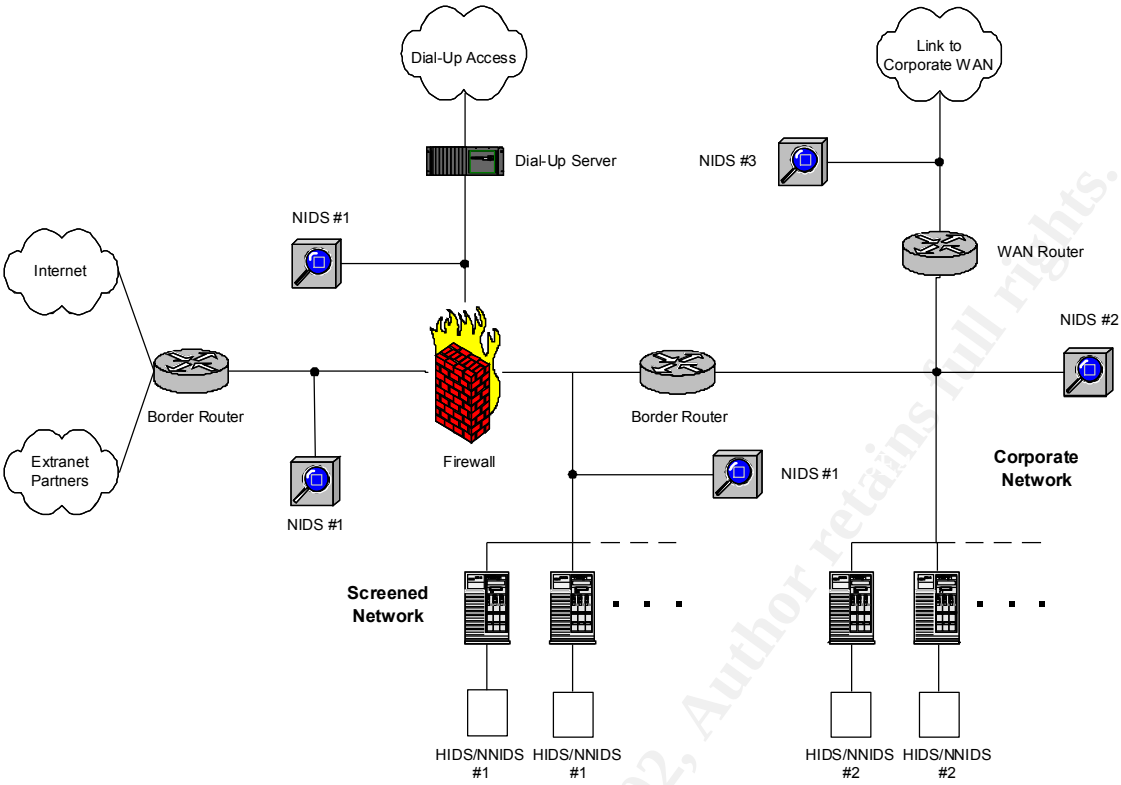


Figure 1 IDS sensor placement logical diagram.

Network Perimeter

An effective placement of IDS sensor is in the network perimeter at all untrusted access points to the corporate network (NIDS #1). Untrusted access points include both sides of the firewall, near the dial-up server, on extranet partner links, and on the screened network. Placement of sensors on the links outside the firewall allows the kinds of attacks to be shown which the site and firewall are exposed. The sensor placed behind the firewall will detect any intrusions that pass through the firewall that are destined for nodes on the screened network. It is exposed to less noise and will generate fewer false-positives since it should be configured for IDS signatures for these nodes (i.e. if the hosts are UNIX-based web servers, then disable all signatures to do with Windows NT, IIS web servers, etc.). IDS agents (HIDS/NNIDS #1) can also be loaded on the hosts to detect any suspicious patterns of activity. As stated in the book *Network Intrusion Detection An Analyst's Handbook* by Stephen Northcutt and Judy Novak, "Outside the firewall is *attack* detection, and inside it is *intrusion* detection."

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

Server Network Segments

Sensor placement (NIDS #2) in production server farm networks and (HIDS/NNIDS #2) on critical production servers would detect any suspicious activity from insiders. The sensors would be tuned to detect the data they are protecting and the traffic they are watching. In order not to overload the sensor due to the Gigabit speeds on many LAN backbone, care made be taken in the selection of an IDS solution as few of them today are Gigabit capable.

WAN Access Points

Another high-value location for an IDS is at any WAN access point (NIDS #3). Sensor placement here will look for suspicious traffic from outlying areas (i.e. field offices) coming to the corporate LAN backbone and vice-versa.

Centralized Management and Logging

In order to effectively manage all IDS sensors and collect their data, provision must be made for a centralized IDS management and logging console. One dedicated management console will allow the administrator(s) to update signature files, software, and tune the signature management filters at all sensor locations. Communication between the management console and all sensors should be encrypted.

Each IDS sensor will also push events to the centralized console where the data can be vulnerability correlated which can be extremely useful for identifying security problems quickly.

Effective management all IDS sensors must be done securely so each sensor should be deployed with two network interfaces and one IP stack. The first interface is used to monitor the network segment in promiscuous mode (listening to all packets). The second interface is placed on a separate network segment used for communication with the IDS management console only.

Managing and integrating the IDS logs with other network and system logs is also critical. Care must be taken in providing sufficient disk space to store the potentially gigabytes of data. Strong consideration should be given to integrating network and host based IDS logs with firewall and host based system logs (e.g. UNIX SYSLOG) where possible. This will allow the IDS analyst to perform vulnerability correlation across the enterprise. That being said, one will undoubtedly have integration issues with the variety of vendor products in use. This must be planned carefully.

Administration and Operation

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

Once the IDS has been made operational, the monitor, assess, and modify cycle commences which is repeated over and over. It is not an install and forget technology.

The person responsible for implementation and monitoring of the IDS needs to be a competent security administrator who is familiar with the network access points, host machines, applications and databases installed, and the user community and their habits. This individual also needs sound understanding of the IP protocol. The book *TCP/IP Illustrated Volume 1: The Protocols*, by Richard Stevens should lay the basis of this understanding. Obtaining training (and certification) in intrusion detection analysis from recognized reputable institution, such as the SANS & GIAC (http://www.giac.org/subject_certs.php#GCIA), should also be strongly considered.

Differing levels of importance must be assigned to different types of intrusion attempts with the alerts and responses scaled appropriately. An IDS can offer near-real-time detection and response capability if implemented correctly but it is not real time. By the time a sensor pushes the detail regarding the intrusion to the console ID and the administrator is alerted, the event has passed.

There are three obstacles that must be overcome when defining these alerts:

- False positives (false alerts) most commonly occur when the IDS sensor misinterprets benign packets as an attack. Assessing and modifying these alerts (i.e. reducing the level of importance or disabling) will be required.

- False negatives will occur when the IDS sensor does not detect malign packets and report them. Alert signatures must be continually updated from the IDS vendor as new exploits and vulnerabilities are discovered.

- False interpretations occur when packets are interpreted as benign when they are really malign (or vice versa). The analyst believes they know the traffic but they do not.

An IDS analyst with appropriate skill set can help mitigate these three obstacles.

Security is not static. As mentioned above, the IDS must be continually modified and refined to reflect the latest vulnerabilities being discovered and exploited all the time. Regularly monitoring and subscribe to the following mailing lists (there are more) to keep informed about the latest exploits and security vulnerabilities:

SANS	http://www.sans.org
CERT	http://www.cert.org
SecurityFocus	http://www.securityfocus.com
FIRST	http://www.first.org

Integration Issues

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

Completing the IDS implementation means integrating it into the other aspects of IT and HR. It must be integrated into the existing IT security incident response procedures. What happens when an apparent successful attack is detected? Who investigates the incident? How long are the IDS logs kept and preserved? Tracking and logging IDS signatures that capture day trading and job searching activities may also violate privacy laws and HR policies. Discussion with the legal department should be considered.

In House vs. Outsource

The management, administration, and operation of an IDS across the corporation can be difficult. The manpower required to complete the monitor, assess, and modify cycle of an IDS implementation may exceed a corporation IT staff headcount and available expertise. The IDS software too will have to be upgraded as the vendor produces a new version with a fix or new features. If effective IDS management poses a challenge, consideration should be given to an MSSP (Managed Security Service Provider) such as Counterpane Internet Security, Internet Security Systems, NetSolve, and Riptech. They can bring a high quality security to their customers than you may be able to do in house at much less cost. However, care must be taken in their selection as many MSSPs have filed for bankruptcy over the last year.

Conclusion

An IDS is a valuable component in a corporation's defence in-depth security plan. It is paramount to take the right steps in planning, deploying, and administering IDS technology. Failure to do so will cause an ineffective implementation. Ensure that IDS sensors are placed in high-value locations for your site. Also follow industry IDS technology trends and directions since these may mean changes that will need to be made at your site. Like any security device, an IDS can work well if it is implemented maintained by competent administrators and analysts. They are the key to making an IDS implementation successful.

References

1. Stephen Northcutt, Judy Novak, Network Intrusion Detection An Analyst's Handbook, Second Edition, New Rider's Publishing, September 2000

2. Intrusion Detection Systems Group Test (Edition 2), An NSS Group Report, December 2001
   http://www.nss.co.uk/ids/index.htm

3. Robert Graham, FAQ: Network Intrusion Detection Systems
   http://robertgraham.com/pubs/network-intrusion-detection.html

4. Dan Chandler, Planning Concerns Considerations, and Tips for IDS in Federal IT Systems, March 30, 2001, http://www.sans.org/infosecFAQ/intrusion/fed_IT.htm

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

5. To Catch a Thief, Network Magazine, August 20, 2001
http://www.networkcomputing.com/1217/1217f1.html

6. Danny Rozenblum, Understanding Intrusion Detection Systems, August 9, 2001
http://www.sans.org/infosecFAQ/intrusion/understand.htm

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

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

Assignment 2 – Network Detects

Detect 1 – LPD Service Scans

Nov 23 04:43:38 211.220.193.241:3879 -> a.b.c.18:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:3881 -> a.b.c.20:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:3899 -> a.b.c.38:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:3888 -> a.b.c.27:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:3932 -> a.b.c.71:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:3969 -> a.b.c.108:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:3912 -> a.b.c.51:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:3923 -> a.b.c.62:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:3943 -> a.b.c.82:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:3962 -> a.b.c.101:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4044 -> a.b.c.183:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4043 -> a.b.c.182:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4056 -> a.b.c.195:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4073 -> a.b.c.212:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4235 -> a.b.d.72:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4236 -> a.b.d.73:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4354 -> a.b.d.191:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4366 -> a.b.d.203:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4378 -> a.b.d.215:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4406 -> a.b.d.239:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4412 -> a.b.d.245:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4419 -> a.b.d.252:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4458 -> a.b.e.36:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4408 -> a.b.d.241:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4418 -> a.b.d.251:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4482 -> a.b.e.60:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4501 -> a.b.e.79:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4510 -> a.b.e.88:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4452 -> a.b.e.30:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4598 -> a.b.e.176:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4648 -> a.b.e.225:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4664 -> a.b.e.241:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4490 -> a.b.e.68:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4905 -> a.b.f.190:515 SYN ******S*
Nov 23 04:43:38 211.220.193.241:4552 -> a.b.e.130:515 SYN ******S*

Nov 23 04:43:43 hostka portsentry[247]: [ID 702911 daemon.notice] attackalert: Connect from host: 211.220.193.241/211.220.193.241 to TCP port: 513
Nov 23 04:45:32 hosthu /kernel: Connection attempt to TCP a.b.c.62:23 from 211.220.193.241:2668

1) Source of Trace

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

http://www.incidents.org/archives/intrusions/msg02581.html - November 23, 2001 probes (part 1) from Laurie Zirkle.

2) Detect was generated by:

Based on the output and reviewing several of Laurie's postings to at http://www.incidents.org, the first part was generated by Snort (version?) portscan module. The second last line appears to have been generated by Portsentry (version?) and the last line was probably generated by the SYSLOG utility on a UNIX host.

3) Probability the source address was spoofed:

Low. The attacker is attempting to gain reconnaissance so if the source address was spoofed, they will not get the information that is being probed for.

Registration Information:

```
inetnum         211.216.0.0 - 211.225.255.255
netname          KORNET
descr           KOREA TELECOM
descr           KOREA TELECOM Internet Operating Center
country          KR
admin-c          DL276-AP, inverse
tech-c          WK81-AP, inverse
remarks          ****************************************
remarks          Allocated to KRNIC Member.
remarks          If you would like to find assignment
remarks          information in detail please refer to
remarks          the KRNIC Whois Database at:
remarks          http://whois.nic.or.kr/english/index.html
remarks          ****************************************
mnt-by          MNT-KRNIC-AP, inverse
mnt-lower        MNT-KRNIC-AP, inverse
changed          hostmaster@apnic.net 20000901
changed          hostmaster@apnic.net 20000912
changed          hostmaster@apnic.net 20010627
source          APNIC
```

4) Description of attack:

The SYN packets are sent to elicit a SYN/ACK response from a node that has a service (typically lpd) running on port 515. Exploits with LPD on many versions of OS exist that enable the attacker to either cause a denial of service (DOS) or gain root access. Scanning on port 515 with LPD running can also apparently cause the

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

side effect of emptying paper trays with garbage printing (http://mm.isu.edu/pipermail/islug/2001-June/000876.html).

References:

- CAN-2000-0839 (under review) http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0839 - WinCOM LPD 1.00.90 allows remote attackers to cause a denial of service by sending a large number of LPD options to the LPD port (515).

- CERT® Advisory CA-2001-30 http://www.cert.org/advisories/CA-2001-30.html - Multiple Vulnerabilities in lpd

- CERT® Advisory CA-2001-32 http://www.cert.org/advisories/CA-2001-32.html - The HP-UX line printer daemon (rlpdaemon) enables various clients to share printers over a network. A remotely exploitable directory traversal vulnerability exists in the rlpdaemon.

5) Attack mechanism:

The attacker sent TCP SYN packets to port 515 to 4 (d – f) class C networks in the span of 1 second on November 23, 2001 with no apparent pattern in the destination addresses. These packets are almost certainly crafted and tools such as Synscan (http://www.psychoid.lam3rz.de/) by psychiod or a variant, masslpd (http://security.alldas.de/analysis/?aid=3) by overkill, were probably used. As mentioned in the link, Masslpd can scan destination IP addresses on port 515 from an input file or A, B, and C network class blocks based on the command-line options. The user can also specify the delay for each scanned host.

The Portsentry detect indicates the attacker made a connection to port 513/tcp (login) on host “hostka”. We’re not told the IP address of “hostka” or if anything else happened. And finally, a connection attempt to port 23/tcp (telnet) on a host which also received a port 515 probe was made. The last two packets (513/tcp and 23/tcp) may have been attempts to fingerprint the OS on those hosts.

6) Correlations:

This detect from the same attacker source IP can also be correlated here:

http://www.incidents.org/archives/intrusions/msg02546.html - November 19, 2001 from John Sage

The captured alerts:

+=+

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

Nov 19 05:35:45 - snort [1:0:0] TCP to 515 lpr
Source IP: 211.220.193.241 Source port: 4101
Source host: 211.220.193.241
Target IP: 12.82.137.190 Target port: 515 Proto: TCP
Target host: 190.seattle-23-24rs.wa.dial-access.att.net

[**] [1:0:0] TCP to 515 lpr [**]
11/19-05:35:45.556134 211.220.193.241:4101 -> 12.82.137.190:515
TCP TTL:49 TOS:0x0 ID:63295 IpLen:20 DgmLen:60 DF
******S* Seq: 0x16D4DD37 Ack: 0x0 Win: 0x7D78 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1813958191 0 NOP WS: 0

The same attacker also tried more attempts to connect to port 515 three days after this network detect:

http://www.incidents.org/archives/intrusions/msg02599.html - November 26, 2001 from Laurie Zirkle

The captured alerts:

Nov 26 20:29:24 211.220.193.241:4547 -> a.b.c.128:515 SYN ******S*
Nov 26 20:29:24 211.220.193.241:4747 -> a.b.d.73:515 SYN ******S*
Nov 26 20:29:24 211.220.193.241:4920 -> a.b.d.245:515 SYN ******S*
Nov 26 20:29:24 211.220.193.241:4955 -> a.b.e.25:515 SYN ******S*
Nov 26 20:29:24 211.220.193.241:4964 -> a.b.e.34:515 SYN ******S*
Nov 26 20:29:26 211.220.193.241:1466 -> a.b.f.251:515 SYN ******S*

This IP address also appears in the Contacting Host Owners URLs produced by Laurie Zirkle:

Contacting Host Owners, October Summary (part 2)
http://www.incidents.org/archives/intrusions/msg02524.html

01/10/22 211.220.193.241 PUSAN NODE Automated response

Contacting Host Owners (November) part 2
http://www.incidents.org/archives/intrusions/msg02990.html

01/11/26 211.220.193.241 PUSAN NODE [again; Oct. 20]

Based on reviewing other the responses from other organizations, the contact attempts have failed.

7) Evidence of active targeting:

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

There is no evidence of specific targeting. This was a general scan of random hosts (including printers) listening on port 515/tcp across 4 C class networks.

8) Severity:

(Critical + Lethal) – (System + Network Countermeasures) = Severity

(3 + 5) – (5 + 4) = -1

Critical – Because many hosts were scanned and we do not know which of them (if any) are critical servers, a 3 will be assigned. This is an appropriate score for a recon probe of a class C network networks.

Lethal – Even though this is a recon probe, a system vulnerable to this attack could be subject to a DOS attack or root access.

System – The last 2 lines of this probe indicate that one host is running Portsentry and another has SYSLOG configured to detect connections, both forms of host intrusion detection systems (HIDS).

Network Countermeasures – Sufficient network countermeasures are probably in place since this detect demonstrated signs of a NIDS and HIDS.

9) Defensive recommendation:

It appears to be the case but double-check that the firewall is blocking port 515/tcp to all hosts unless explicitly required. Ensure that any host running the LPD service have the OS locked down (i.e. hardened and patched) and that the LPD service is the latest set of binaries with the latest patches.

10) Multiple choice test question:

What does the above network detect best describe?

a) Reconnaissance activity
b) Normal printing activity via the LPD service
c) Specific attacks against print servers
d) Legitimate end user trying to find a network printer

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

Answer: a. This is reconnaissance activity looking for listening LPD print servers by an attacker. These are not specific attacks or exploit traffic, nor is it normal printing activity, or even a legitimate end user looking a print server. Someone is clearly looking for a listening LPD print server to possibly follow-up with a specific attack exploit.

Detect 2 – t0rnscan Scan for Backdoor SSH Server

12/03-11:07:24.340930 209.27.245.128:39999 -> www.xxx.yyy.5:39999
TCP TTL:240 TOS:0x0 ID:1795 IpLen:20 DgmLen:40
******S* Seq: 0x7AE80725 Ack: 0x4E25A69B Win: 0x28 TcpLen: 20

=+
=+=+=+

12/03-11:07:24.342227 209.27.245.128:39999 -> www.xxx.yyy.4:39999
TCP TTL:242 TOS:0x0 ID:1795 IpLen:20 DgmLen:40
******S* Seq: 0x7AE80725 Ack: 0x4E25A69B Win: 0x28 TcpLen: 20

=+
=+=+=+

12/03-11:07:24.343129 209.27.245.128:39999 -> www.xxx.yyy.12:39999
TCP TTL:242 TOS:0x0 ID:1795 IpLen:20 DgmLen:40
******S* Seq: 0x7AE80725 Ack: 0x4E25A69B Win: 0x28 TcpLen: 20

=+
=+=+=+

1) **Source of Trace**

http://www.incidents.org/archives/intrusions/msg02733.html - Monday, 3 Dec 2001 from Mike Manco

2) **Detect was generated by:**

Based on the output and reviewing several of Laurie's postings to at http://www.incidents.org, this detect was generated by Snort (version?).

3) **Probability the source address was spoofed:**

Low. The attacker's network probe is trying to elicit a response that will not be received if the source IP address is spoofed.

Registration Information:

Internet Business Services (NETBLK-CW-209-27-244)
300 S Harbor Blvd
Anaheim, CA 98706

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

US

Netname: CW-209-27-244
Netblock: 209.27.244.0 - 209.27.245.255
Maintainer: IBS

Coordinator:
Reeves, Lee (LR54-ARIN) lee@4IBS.COM
+1-714-635-9777 (FAX) 714.635.9779

4) Description of attack:

This combination of these packet characteristics is normally associated with the tool t0rnscan installed by the t0rn rootkit (see http://www.sans.org/y2k/011701-1500.htm - Chris Kuethe). The attacker is using t0rnscan to possibly probe for a backdoor SSH server running on port 39999 that has been previously installed on a compromised system. The systems may have been compromised by what is known as the SSH crc32 compensation attack detector exploit. Any hosts running the SSH1 protocol that have not been patched can be subject to this attack.

References:

- CVE-2001-0144 http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2001-0144+++ - 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

- CERT Vulnerability Note VU#945216 http://www.kb.cert.org/vuls/id/945216 - SSH CRC32 attack detection code contains remote integer overflow

5) Attack mechanism:

The t0rnscan attack works by sending the following sending packets with the following characteristics:

Source Port = Destination Port
TTL < 255
ID is the same
ACK is the same
Window size is 1024
Datagram length is the same

The ID and ACK sequence number, and window size will randomly change every second since t0rnscan has apparently been built with the rand function. The t0rnscan tool is probably a copy of synscan 1.7 or later (see

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

http://www.incidents.org/archives/intrusions/msg02736.html). Synscan is the product of psychoid (see http://www.psychoid.lam3rz.de/).

Since the attacker is using t0rnscan (installed by the t0rn rootkit), it is possible that the source IP address may be a compromised host.

6) Correlations:

Very similar detects were also noted on November 25, 2001 at http://www.incidents.org/diary.php?id=86.

A sample:

NOV 23 02:33:47 PROTO=6 24.156.53.180:39999 293.115.169.18:39999 L=40 S=0X00 I=15729 F=0X0000 T=242 SYN
NOV 23 02:33:47 PROTO=6 24.156.53.180:39999 293.115.169.23:39999 L=40 S=0X00 I=15729 F=0X0000 T=242 SYN
NOV 23 02:33:47 PROTO=6 24.156.53.180:39999 293.115.169.22:39999 L=40 S=0X00 I=15729 F=0X0000 T=242 SYN
NOV 23 02:33:47 PROTO=6 24.156.53.180:39999 293.115.169.21:39999 L=40 S=0X00 I=15729 F=0X0000 T=242 SYN
NOV 23 02:33:47 PROTO=6 24.156.53.180:39999 293.115.169.20:39999 L=40 S=0X00 I=15729 F=0X0000 T=242 SYN
NOV 23 02:33:47 PROTO=6 24.156.53.180:39999 293.115.169.19:39999 L=40 S=0X00 I=15729 F=0X0000 T=242 SYN
NOV 23 02:33:47 PROTO=6 24.156.53.180:39999 293.115.169.12:39999 L=40 S=0X00 I=15729 F=0X0000 T=242 SYN
NOV 23 02:33:47 PROTO=6 24.156.53.180:39999 293.115.169.17:39999 L=40 S=0X00 I=15729 F=0X0000 T=242 SYN
NOV 23 02:33:47 PROTO=6 24.156.53.180:39999 293.115.169.16:39999 L=40 S=0X00 I=15729 F=0X0000 T=242 SYN

The Handler's comments:

"Note of the typical synscan characteristics where SYN packets, source port = destination port, IP ID all held constant. Overall, 34 distinct targets were probed in this scan. Port 39999/tcp has occasionally been used to provide a rogue SSH server, and can be linked to the t0rn rootkit. It is unclear whether the attackers are looking for one of these servers, or something else."

7) Evidence of active targeting:

This recon probe was sent to 3 specific hosts implying that they have probably been actively targeted.

8) Severity:

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

(Critical + Lethal) – (System + Network Countermeasures) = Severity

(3 + 5) – (5 + 4) = -1

Critical – This is a recon probe against 3 hosts but one cannot tell if they are critical servers.

Lethal – The scan was looking for a backdoor SSH1 protocol trojan installed which could be extremely lethal if found.

System – No host systems responded to the probe implying that the hosts have not been compromised.

Network Countermeasures – Sufficient network countermeasures are probably in place since this detect demonstrated signs of a NIDS.

9) Defensive recommendation:

Block any access to all hosts on port 39999 assuming it is not used by a known application. Review current versions of any SSH1 protocol running on hosts and any check all hosts for an active service running on port 39999. Ensure any hosts running SSH (any version) have the latest security patches applied.

10) Multiple choice test question:

In the above trace, which field(s) show evidence of packet crafting?

a) Source port or destination port
b) Sequence number
c) Ack
d) All of the above

Answer: d. The above trace shows crafted source and destination ports, sequence number, and ack.

Detect 3 – Port 443 scan

```
Oct 24 00:28:03 130.233.44.98:2351 -> AA.BB.CC.50:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2356 -> AA.BB.CC.55:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2358 -> AA.BB.CC.57:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2360 -> AA.BB.CC.59:443 SYN ******S*
```


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

```
Oct 24 00:28:03 130.233.44.98:2363 -> AA.BB.CC.62:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2375 -> AA.BB.CC.74:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2381 -> AA.BB.CC.80:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2384 -> AA.BB.CC.83:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2393 -> AA.BB.CC.92:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2396 -> AA.BB.CC.95:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2407 -> AA.BB.CC.106:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2353 -> AA.BB.CC.52:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2431 -> AA.BB.CC.130:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2352 -> AA.BB.CC.51:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2354 -> AA.BB.CC.53:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2357 -> AA.BB.CC.56:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2359 -> AA.BB.CC.58:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2361 -> AA.BB.CC.60:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2371 -> AA.BB.CC.70:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2373 -> AA.BB.CC.72:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2372 -> AA.BB.CC.71:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2374 -> AA.BB.CC.73:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2379 -> AA.BB.CC.78:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2382 -> AA.BB.CC.81:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2385 -> AA.BB.CC.84:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2386 -> AA.BB.CC.85:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2388 -> AA.BB.CC.87:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2387 -> AA.BB.CC.86:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2390 -> AA.BB.CC.89:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2391 -> AA.BB.CC.90:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2394 -> AA.BB.CC.93:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2397 -> AA.BB.CC.96:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2399 -> AA.BB.CC.98:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2400 -> AA.BB.CC.99:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2403 -> AA.BB.CC.102:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2404 -> AA.BB.CC.103:443 SYN ******S*
Oct 24 00:28:03 130.233.44.98:2406 -> AA.BB.CC.105:443 SYN ******S*
Oct 24 00:28:04 130.233.44.98:2486 -> AA.BB.CC.185:443 SYN ******S*
Oct 24 00:28:04 130.233.44.98:2487 -> AA.BB.CC.186:443 SYN ******S*
Oct 24 00:28:04 130.233.44.98:2488 -> AA.BB.CC.187:443 SYN ******S*
```

1) Source of Trace

http://www.incidents.org/archives/intrusions/msg02252.html - Friday, 26 October 2001 from Arlen Fletcher.

2) Detect was generated by:

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

Based on the output and reviewing several of Laurie's postings to at http://www.incidents.org, this detect was generated by Snort (version?) portscan module.

3) Probability the source address was spoofed:

Low. The attacker's network probe is a reconnaissance trying to elicit a response that will not be received if the source IP address is spoofed.

Registration Information:

Helsinki University of Technology (NET-HUTNET)
Otakaari 1
FI 02150 Espoo
FI

Netname: HUTNET
Netblock: 130.233.0.0 - 130.233.255.255

Coordinator:
Laaksonen, Kimmo (KL66-ARIN) Kimmo.Laaksonen@HUT.FI
+358 9 451 4308 (FAX) +358 9 464 788

Domain System inverse mapping provided by:

NS1.HUT.FI	130.233.224.1
NS2.HUT.FI	130.233.224.13
NS-SECONDARY.FUNET.FI	128.214.248.132

4) Description of attack:

The attacker sent TCP SYN packets (i.e. a stimulus) to a class C network and port 443 in the span of 2 seconds on October 26, 2001 with no apparent pattern in the destination addresses. The source ports appear to be in sequence for the most part (a few exceptions possibly due to the speed of their arrival and the data was logged on the Snort host). As is well known, port 443 typically runs a secure sockets layer (SSL) service, usually a web server, for encrypted communications. If the attacker found a web server accepting connections and chose to follow-up, there are no shortage of web server vulnerabilities list in the CVE list for MS IIS, iPlanet Netscape, and Apache web servers.

References:

MS IIS Web Servers (84 CVE and CAN entries). Latest CAN below:

- CAN-2001-0709 (under review) - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0709 - Microsoft IIS 4.0 and before,

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

when installed on a FAT partition, allows a remote attacker to obtain source code of ASP files via a URL encoded with Unicode.

IPlanet Netscape Servers (62 CVE and CAN entries). Latest CAN below:

- CAN-2001-0747 (under review) http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0747 - Buffer overflow in iPlanet Web Server (iWS) Enterprise Edition 4.1, service packs 3 through 7, allows remote attackers to cause a denial of sevice and possibly execute arbitrary code via a long method name in an HTTP request.

Apache Web Servers (31 CVE and CAN entries). Latest CAN below:

- CAN-2001-0829 (under review) http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0829 - A cross-site scripting vulnerability in Apache Tomcat 3.2.1 allows a malicious webmaster to embed Javascript in a request for a .JSP file, which causes the Javascript to be inserted into an error message.

5) Attack mechanism:

Since the attacker sent a TCP probe with the SYN flag set, they are looking for machines with a web server running (i.e. machine would reply with SYN/ACK back) on port 443 for either site reconnaissance and/or possible follow-up with another set of tools. Nmap (http://www.nmap.org/) and Hping2 (http://www.hping.org/) allow you to generate characteristics of this nature and could be wrapped in a shell/perl script to be used as a scanner. Follow-up tools could include whisker, by Rain Forest Puppy at http://www.wiretrip.net/rfp/, a web scanner that also employs anti-IDS detection measures.

The attacker may have also elected to scan for https web servers on port 443 with the intent of using the encrypted communications via SSL. Most intrusion detection systems will not (network node IDS will) detect any signature alerts since the communications are encrypted. Thus the attacker may be looking to do some secure hacking.

6) Correlations:

No recent evidence of a similar scan was found after searching Incidents.org, Google.com, and Neohapsis.com. However, several recent detects were found that included port 443 among others:

http://www.incidents.org/archives/intrusions/msg02799.html - December 7, 2001 from Laurie Zirkle

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

http://www.incidents.org/archives/intrusions/msg00413.html - Wednesday, May 23, 2001 from Brent Erickson

Dshield.org provides some unusual statistics regarding port 443 activity from November 11 – 15, 2001 where the count reached as high as 1910 versus the normal count of between 1 – 100. Interestingly enough, Incidents.org failed to turn up any port 443 activity during the mid to late October 2001 timeframe where this detect occurred.

Note that the attacker source IP address does not appear in any of Laurie Zirkle's Contacting Host Owners URLs.

7) Evidence of active targeting:

There is no evidence of specific targeting. This was a general scan of machines listening on port 443/tcp across a C class network.

8) Severity:

(Critical + Lethal) – (System + Network Countermeasures) = Severity

(3 + 5) – (4 + 4) = 0

Critical – Because many hosts were scanned and we do not know which of them (if any) are critical servers, a 3 will be assigned. This is an appropriate score for a recon probe of a class C network.

Lethal – There are numerous known exploits and even though many of them have been known for quite some time, a system vulnerable to one of these could be subject to a root compromise.

System – No host systems responded to the probe implying that the hosts are not accepting connection requests.

Network Countermeasures – Sufficient network countermeasures are probably in place since this detect demonstrated signs of a NIDS.

9) Defensive recommendation:

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

Block all port 443 access to machines from the Internet unless a particular machine is running an SSL web server. For any hosts running a SSL web server, ensure that they are placed in a DMZ, have the OS locked down (i.e. secured and patched), and the web server has the latest patches applied to it.

10) Multiple choice test question:

If the attacker successfully found a destination IP with an SSL web server listening in the above detect and chose to embark on some encrypted hacking, how could the attacker's activity be best be tracked?

a) It could not be tracked properly because it is encrypted.
b) Network based IDS
c) Network node IDS
d) Host based IDS

Answer: c. Network node IDSes (NNIDS) are best suited today dealing with encrypted traffic. NNIDS can look at the network traffic directly on the server after it is decrypted to perform the signature analysis. Other IDSes cannot.

Detect 4 – MS SQL Server Scans

Nov 22 19:25:38 hostmau snort: [1:474:1] ICMP superscan echo [Classification: Attempted Information Leak] [Priority: 3]: {ICMP} 213.51.204.55 -> z.y.w.12
Nov 22 19:25:39 hostmau Connection attempt to TCP z.y.w.12:1433 from 213.51.204.55:1656
Nov 22 19:25:40 hostmau Connection attempt to TCP z.y.w.12:1433 from 213.51.204.55:1656
Nov 22 19:25:40 hostmau Connection attempt to TCP z.y.w.12:1433 from 213.51.204.55:1656

1) Source of Trace

http://www.incidents.org/archives/intrusions/msg02580.html – November 22, 2001 probes (part 2) from Laurie Zirkle.

2) Detect was generated by:

Based on the output, the first line was generated by Snort (version?). The last three lines appear to have been generated by the SYSLOG utility on a UNIX host.

3) Probability the source address was spoofed:

Very Low. The attacker's network probe is a reconnaissance trying to elicit a response that will not be received if the source IP address is spoofed.

Registration Information:

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

```
inetnum:      213.51.200.0 - 213.51.207.255
netname:      BENELUX-1
descr:        @Home Benelux Enschede Headend block
descr:        BENELUX-CASTEL-ENSCHEDE-2
country:      NL
admin-c:      ABNO1-RIPE
tech-c:       ABIM3-RIPE
remarks:      For abuse issues, please email abuse@corp.nl.home.com
status:       ASSIGNED PA
mnt-by:       BENELUX-MNT
mnt-lower:    BENELUX-MNT
changed:      judithh@excitehome.net 20010521
source:       RIPE

route:        213.51.0.0/16
descr:        @Home Benelux
origin:       AS9143
remarks:      For abuse issues, please email abuse@corp.nl.home.com
mnt-by:       BENELUX-MNT
changed:      judithh@excitehome.net 20010521
source:       RIPE

role:         AtHome Benelux Network Operations Centre
address:      Gyroscoopweg 90-92
address:      1042 AX Amsterdam
address:      The Netherlands
phone:        +31 20 885 5544
fax-no:       +31 20 885 5525
e-mail:       noc@corp.nl.home.com
trouble:      reports of network abuse, pls. contact
trouble:      abuse@corp.nl.home.com
admin-c:      JVV19-RIPE
tech-c:       JH4485-RIPE
tech-c:       RCE3-RIPE
nic-hdl:      ABNO1-RIPE
notify:       ipmgmt@corp.nl.home.com
changed:      judithh@excitehome.net 20010503
source:       RIPE

role:         AtHome Benelux IP Mgmt
address:      Gyroscoopweg 90-92
address:      1042 AX Amsterdam
address:      The Netherlands
phone:        +31 20 885 5544
fax-no:       +31 20 885 5525
e-mail:       ipmgmt@excitehome.net
```

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

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

trouble: reports of network abuse, pls. contact
trouble: abuse@corp.nl.home.com
admin-c: JH4485-RIPE
tech-c: JH4485-RIPE
tech-c: RCE3-RIPE
nic-hdl: ABIM3-RIPE
notify: judithh@excitehome.net
changed: judithh@excitehome.net 20010503
source: RIPE

4) Description of attack:

This is a stimulus to see if the host, z.y.w.12, will respond with an ICMP echo-reply. The last three lines are further connection attempts from 213.51.204.55 port 1656 to z.y.w.12 port 1433/tcp are captured by the host IDS (SYSLOG). They are probably TCP SYN packets sent as a stimulus looking for a SYN/ACK response. It is interesting to note that the Snort IDS did not generate an alert for these TCP connections. All traffic logged in this detect is against the host hostmau. The MS SQLServer application typically runs on port 1433. Any hosts running SQLServer are susceptible to two attack possibilities:

I. A recent vulnerability in SQL Server allows an attacker to send data that can cause a DoS (Denial of Service).

Reference:

- CAN-2001-0509 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0509 - Vulnerabilities in RPC servers in (1) Microsoft Exchange Server 2000 and earlier, (2) Microsoft SQL Server 2000 and earlier, (3) Windows NT 4.0, and (4) Windows 2000 allow remote attackers to cause a denial of service via malformed inputs.

II. On November 20, 2001, Douglas Brown discovered a new worm that targets insecure versions of MS SQLServer 7.0 installations where the System Administrator account has an empty password (see http://www.incidents.org/archives/intrusions/msg02536.html).

Reference: N/A

5) Attack mechanism:

The attacker appears to have used SuperScan (http://www.foundstone.com), a freeware TCP port scanner developed by Robin Keir, based on the Snort alert from the first line. When it sends an echo-request, the dsize or payload size is 8 bytes and the data is padded with only 0 (zeros).

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

The last three lines show three TCP SYN connection attempts within 2 seconds. Characteristics of the packets show the destination port is 1433/tcp and the source port is 1656/tcp. TCP scanning tests conducted with Superscan showed the source port increasing by 1. The attacker's source port remained at 1656/tcp. Thus, it appears that the attacker may not have used the SuperScan to send the TCP packets.

Further investigation regarding Superscan discovered the command-line tool, SendIP (http://freshmeat.net/projects/sendip/homepage/), that can craft and send arbitrary IP packets (TCP, UDP, ICMP, and RIP). One can specify the content of every header and even the wrong checksums can be sent. In order to generate the characteristics of this detect, SendIP commands could be wrapped in a shell/perl script to be used as a scanner.

6) Correlations:

These network detects have also been seen in the past:

http://www.incidents.org/archives/intrusions/msg01695.html - September 12, 2001 from Laurie Zirkle

http://www.incidents.org/diary/october01/100401.php#043 - October 4, 2001 from Vicki Irwin (Handler on Duty)

This IP address also appears in the Contacting Host Owners (November) part 2 URL produced by Laurie Zirkle at http://www.incidents.org/archives/intrusions/msg02990.html:

01/11/26 213.51.204.55 @Home Benelux Enschede Headend block Automated response

Based on reviewing other the responses from other organizations and another attempt at contacting the @Home Benelux Enschede Headend, the contact attempts have failed.

7) Evidence of active targeting:

This was a direct scan of z.y.w.12 determine is it was alive and running MS SQLServer on port 1433/tcp. Thus, since one host was targeted, this is evidence of active targeting.

8) Severity:

(Critical + Lethal) – (System + Network Countermeasures) = Severity

(3 + 5) – (5 + 4) = -1

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

Critical – This is a recon probe against 1 host but one cannot tell if they are critical servers.

Lethal – The scan was looking for a listening a misconfigured or unpatched MS SQLServer that could be susceptible to a DoS or possible root access (i.e. ability to run a command shell as administrator)

System – No host systems responded to the probe implying that the hosts have not been compromised. There appears to be a host IDS, SYSLOG, running.

Network Countermeasures – Sufficient network countermeasures are probably in place since this detect demonstrated signs of a NIDS.

9) Defensive recommendation:

Since this host is apparently accessible from the Internet, ensure that this machine has a firewall in front of it that will allow access to only the services required. Check other machines that are running MS SQLServer instances to ensure they configured correctly and that the latest patches have been applied.

10) Multiple choice test question:

How would you best describe the above network detect?

a) Shows crafted packets for OS fingerprinting
b) This is normal traffic from an legitimate user looking to connect to their MS SQLServer
c) An indication that a specific exploit may be released on port 1433.
d) Both a and c.

Answer: c. These are crafted packets but the attacker is clearly looking for an active connection on port 1433, probably for a listening MS SQLServer to take advantage of the latest exploit, and not OS fingerprinting.

Detect 5 – Port 227 Scans

Nov 30 02:28:37 203.251.80.48:2569 -> www.xxx.yyy.2:227 SYN ******S*
Nov 30 02:28:34 203.251.80.48:2579 -> www.xxx.yyy.12:227 SYN ******S*
Nov 30 02:28:34 203.251.80.48:2577 -> www.xxx.yyy.10:227 SYN ******S*

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

```
Nov 30 02:28:34 203.251.80.48:2583 -> www.xxx.yyy.16:227 SYN ******S*
Nov 30 02:28:34 203.251.80.48:2581 -> www.xxx.yyy.14:227 SYN ******S*
Nov 30 02:28:34 203.251.80.48:2572 -> www.xxx.yyy.5:227 SYN ******S*
Nov 30 02:28:34 203.251.80.48:2576 -> www.xxx.yyy.9:227 SYN ******S*
Nov 30 02:28:34 203.251.80.48:2571 -> www.xxx.yyy.4:227 SYN ******S*
Nov 30 02:28:34 203.251.80.48:2573 -> www.xxx.yyy.6:227 SYN ******S*
Nov 30 02:28:34 203.251.80.48:2575 -> www.xxx.yyy.8:227 SYN ******S*
```

1) Source of Trace

http://www.incidents.org/archives/intrusions/msg02735.html - November 30, 2001 from Mike Manco

2) Detect was generated by:

Based on the output and reviewing several of Laurie's postings to at http://www.incidents.org, this detect was generated by Snort (version?) portscan module.

3) Probability the source address was spoofed:

Low. The attacker's network probe is a reconnaissance trying to elicit a response that will not be received if the source IP address is spoofed.

Registration Information:

```
inetnum         203.248.0.0 - 203.255.255.255
netname          KRNIC-KR
descr           KRNIC
descr           Korea Network Information Center
country          KR
admin-c          HM127-AP, inverse
tech-c          HM127-AP, inverse
remarks          ****************************************
remarks          KRNIC is the National Internet Registry
remarks          in Korea under APNIC. If you would like to
remarks          find assignment information in detail
remarks          please refer to the KRNIC Whois DB
remarks          http://whois.nic.or.kr/english/index.html
remarks          ****************************************
mnt-by          APNIC-HM, inverse
mnt-lower        MNT-KRNIC-AP, inverse
changed          hostmast@rs.krnic.net 19981015
changed          hostmaster@apnic.net 20010606
source          APNIC
```

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

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

person Host Master, inverse
address Korea Network Information Center
address Narajongkeum B/D 14F, 1328-3, Seocho-dong, Seocho-ku, Seoul, 137-070, Republic of Korea
country KR
phone +82-2-2186-4500
fax-no +82-2-2186-4496
e-mail hostmaster@nic.or.kr, inverse
nic-hdl HM127-AP, inverse
mnt-by MNT-KRNIC-AP, inverse
changed hostmaster@nic.or.kr 20010514
source APNIC

4) Description of attack:

Port 227 is defined as a reserved port (see http://www.iana.org/assignments/port-numbers). Further analysis of this attacker source IP and the correlated detect below reveal that they may be attempting exploit a recent WU-FTP vulnerability (see http://www.incidents.org/archives/intrusions/msg02706.html). What does port 227 have to do with FTP when it normally runs on port 20 (data) and port 21 (control)? As stated in the aforementioned URL, Snort may have failed to detect or incorrectly log the attempt to get a port with the FTP reply code (PASV) of 227 (i.e. this command requests the server to listen on the data port and wait for a connection). See FTP RFC specification at http://www.ietf.org/rfc/rfc0959.txt. Dshield.org provides shows 224 scans of port 227 on November 28, 2001 but little activity since then.

References:

CAN-2001-0550 - wu-ftpd 2.6.1 allows remote attackers to execute arbitrary commands via a "~{" argument to commands such as CWD, which is not properly handled by the glob function (ftpglob). See http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0550.

CA-2001-33 (released November 29, 2001) - Multiple Vulnerabilities in WU-FTPD. See http://www.cert.org/advisories/CA-2001-33.html.

5) Attack mechanism:

The attacker sent TCP SYN packets (i.e. a stimulus) to port 227 to a Class C network in the span of 4 seconds with no apparent pattern in the destination addresses. There are two possibilities for an attack mechanism:

I. A shell/perl script was used in this attack that would have included the code to set an FTP server into passive mode and take advantage of the latest WU-FTP exploit.

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

II. The attacker made a mistake and was scanning (using Nmap or Hping2) for port 227 because they surmised it was an ftp connection port. No one said that attackers have to be bright.

6) Correlations:

A very similar detect from the same attacker source IP was also noted on November 28, 2001 by Stephen Shepherd at http://www.incidents.org/archives/intrusions/msg02662.html.

A sample:

Nov 28 22:40:31 203.251.80.48:1072 -> xxx.xxx.xxx.9:227 SYN ******S*
Nov 28 22:40:31 203.251.80.48:1069 -> xxx.xxx.xxx.6:227 SYN ******S*
Nov 28 22:40:31 203.251.80.48:1075 -> xxx.xxx.xxx.12:227 SYN ******S*
Nov 28 22:40:31 203.251.80.48:1077 -> xxx.xxx.xxx.14:227 SYN ******S*
Nov 28 22:40:31 203.251.80.48:1079 -> xxx.xxx.xxx.16:227 SYN ******S*
Nov 28 22:40:31 203.251.80.48:1088 -> xxx.xxx.xxx.25:227 SYN ******S*
Nov 28 22:40:31 203.251.80.48:1083 -> xxx.xxx.xxx.20:227 SYN ******S*
Nov 28 22:40:34 203.251.80.48:1065 -> xxx.xxx.xxx.2:227 SYN ******S*
Nov 28 22:40:31 203.251.80.48:1085 -> xxx.xxx.xxx.22:227 SYN ******S*
Nov 28 22:40:31 203.251.80.48:1093 -> xxx.xxx.xxx.30:227 SYN ******S*

To date, the attacker source IP address does not appear in any of Laurie Zirkle's Contacting Host Owners URLs.

7) Evidence of active targeting:

There is no evidence of specific targeting. This was a general scan of machines listening on port 227/tcp across on two C class networks.

8) Severity:

(Critical + Lethal) – (System + Network Countermeasures) = Severity

(3 + 5) – (4 + 4) = 0

Critical – Because many hosts were scanned and we do not know which of them (if any) are critical servers, a 3 will be assigned. This is an appropriate score for a recon probe of a class C network.

Lethal – Even though this is a recon probe, a system vulnerable to this attack could be subject to a root compromise.

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

System – No host systems responded to the probe implying that the hosts have not been compromised.

Network Countermeasures – Sufficient network countermeasures are probably in place since this detect demonstrated signs of a NIDS.

9) Defensive recommendation:

Inbound and outbound access to port 227 should be blocked at the firewall since it is a reserved port and no service should be associated with it. Any existing machines running an ftp server should be checked to ensure they are running the FTP latest binaries and the latest security patches.

10) Multiple choice test question:

One possible motive for a probe to port 227?

a) ftp data port
b) ftp control port
c) ftp PASV command
d) none of the above

Answer: d. Port 227 is a reserved port, port 20 is the ftp data port, and port 21 is the ftp command port. 227 is the ftp PASV command and has nothing to do with port 227.

© SANS Institute 2000 - 2002 Author retains full rights.

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

Assignment 3 – "Analyze This" Scenario

Executive Summary

The University has engaged us to provide a security audit based on data selected from five consecutive days, November 21, 2001 to November 25, 2001, provided from a Snort system with a fairly standard rulebase. As part of the security audit, we have been asked to look for signs of compromised systems or network problems.

Since we have been only provided raw output data from a Snort system, it is difficult to ascertain the network topology (i.e. network fabric and perimeter design) and what security architecture (i.e. what mechanisms serve to enforce the University's security policy) is in place. Some conclusions from the analysis drawn in this security audit may reflect this.

The following three types of data files have been provided:

- Snort Alert Logs – Alert signatures.
- Snort Scan Logs – Port scanning activity.
- Snort Out-Of-Spec (OOS) Logs – TCP packets with illegal TCP flag combinations.

A combination of Snortsnarf (http://www.silicondefense.com/software/snortsnarf/index.htm) and various UNIX scripts were used to process the alert, scan and OOS logs. The top 20 alerts were analysed based on the number of occurrences. The top 10 scans and OOS traces from the IP sources and destination were also analysed based on the number of occurrences. The analysis process is also discussed in detail at the end of this document. Appendix A lists the primary reference sites used for the analysis.

Correlations from previous GCIA student practicals (numbered 209 and above) and/or from other sources have been made throughout this security audit.

Internal machine insights from University machines were identified that appeared compromised or exhibited unusual signs of the highest levels of compromise or possible dangerous or anomalous activity.

The top five external source addresses were selected for further investigation based on various levels of compromise or possible dangerous or anomalous activity.

After conducting the security audit, the following defensive recommendations are suggested:

Short Term (immediate)

- Take action to deal with potentially the compromised machine, MY.NET.70.148.

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

- Take measures to conduct a security audit of the machines, MY.NET.16.42, MY.NET.11.4, MY.NET.6.7, MY.NET.253.114, MY.NET.60.14, and MY.NET.60.125 exhibiting highly suspicious signature activity.

- Review the scanning and telnet activity from the University machine, MY.NET.253.10, to other various University machines.

Long Term (3 months)

- Review the University's security policy to see if the network traffic activity shown in the security audit complies with it.

- Consider performing a Vulnerability Analysis (VA) against all University network access points.

- Consider reviewing the ingress and egress rulesets at the University network security enforcement points (i.e. border routers and firewalls).

- Review all host based security mechanisms in place, especially machines that face the Internet.

- Review the current placement of all Snort network IDSes.

- Ensure that appropriate personnel, system and security administrators are continually on the alert for new vulnerabilities to services used in the University's network.

Finally, it is important to note that during the course of this security audit, the very useful IDS resource site, http://www.whitehats.com, was unavailable. The following text was on their web site:

"Whitehats is currently experiencing some technical difficulties. Some hardware and other problems have caused us to move the systems, and so while they are being moved to a more stable place, whitehats will be unable to serve your IDS needs."

Files Analyzed

The following five consecutive days, November 21, 2001 to November 25, 2001, worth of files (http://www.research.umbc.edu/~andy/) from the University's Snort system were used in this analysis:

Alerts:

alert.011121.gz
alert.011122.gz
alert.011123.gz
alert.011124.gz

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

alert.011125.gz

OOS (Out Of Spec):

oos_Nov.21.2001.gz
oos_Nov.22.2001.gz
oos_Nov.23.2001.gz
oos_Nov.24.2001.gz
oos_Nov.25.2001.gz

Scans:

scans.011121.gz
scans.011122.gz
scans.011123.gz
scans.011124.gz
scans.011125.gz

Selected Detects – Snort Alerts

The following is a breakdown of the top 20 (there were 142 signatures generated in total) most significant Snort alerts (below), complete with analysis, that were matched based on number of occurrences. Appendix A lists the most commonly searched sites for port info, trojans, etc. used in the following analysis.

176348 Alerts	**# Alerts**	**# Sources**	**# Destinations**	**Detail link**
EXPLOIT x86 NOOP	1253	15	20	Summary
SCAN Proxy attempt	2139	84	62	Summary
NMAP TCP ping!	2363	31	867	Summary
ICMP Fragment Reassembly Time Exceeded	2366	30	29	Summary
Watchlist 000222 NET-NCFC	2401	12	10	Summary
ICMP Destination Unreachable (Communication Administratively Prohibited)	2407	171	50	Summary
ICMP Echo Request Nmap or HPING2	3675	38	720	Summary

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

connect to 515 from outside	4127	3	441	Summary
Watchlist 000220 IL-ISDNNET-990517	6123	173	36	Summary
Incomplete Packet Fragments Discarded	7206	10	13	Summary
SMB Name Wildcard	7951	268	3443	Summary
ICMP Destination Unreachable (Host Unreachable)	9428	1297	61	Summary
MISC Large UDP Packet	11658	9	13	Summary
INFO MSN IM Chat data	23922	249	367	Summary
ICMP Echo Request BSDtype	27896	19	21	Summary
CS WEBSERVER - external web traffic	30202	4194	1	Summary
WEB-MISC prefix-get //	31321	1140	5	Summary
MISC source port 53 to <1024	32770	6800	10	Summary
ICMP Echo Request Windows	40745	173	103	Summary
MISC traceroute	46539	98	25	Summary

- **EXPLOIT x86 NOOP**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
163.17.157.130	660	4305	2	36
129.128.5.191	288	302	1	1
128.183.105.216	280	280	1	1
194.18.30.208	8	8	3	3
205.138.230.234	3	3	3	3

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.190.51	343	1991	1	1

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

MY.NET.190.13	317	2291	1	3
MY.NET.70.148	288	29551	1	126
MY.NET.163.70	280	281	1	2
MY.NET.97.229	4	122	1	11

The Exploit x86 NOOP signature is triggered when a large sequence of contiguous bytes x86 NOOP instructions are embedded in the payload of a datagram. NOOPs are often used to pad out buffer overflow attacks. You also need to consider any additional details surrounding this alert such as what port is receiving this packet and are there other probes from the same source IP that preceded this alert? This is illustrated in a sample of the data:

11/25-23:40:15.906423 [**] connect to 515 from outside [**] 163.17.157.130:2625 -> MY.NET.190.51:515
11/25-23:40:16.219631 [**] EXPLOIT x86 NOOP [**] 163.17.157.130:2624 -> MY.NET.190.13:515
11/25-23:40:16.264754 [**] EXPLOIT x86 NOOP [**] 163.17.157.130:2625 -> MY.NET.190.51:515
11/25-23:40:16.517181 [**] connect to 515 from outside [**] 163.17.157.130:2624 -> MY.NET.190.13:515

It appears that 163.17.157.130 may well be attempting a buffer overflow attack on the LPD service (515/tcp) on MY.NET.190.13. See CVE-2001-0353, CAN-2001-0668 , and CAN-2001-0670. The alerts were generated from 23:37:40 till 23:51:39 on November 25, 2001.

Correlations

This detect (with both EXPLOIT x86 NOOP connect to 515 from outside alerts) can be correlated at http://www.sans.org/y2k/040401-1145.htm.

- **SCAN Proxy attempt**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
24.180.167.185	880	1032	1	2
24.6.129.165	290	291	1	2
136.160.5.145	127	127	1	1
172.166.51.191	106	106	1	1
134.192.89.86	95	95	1	1

Top 5 Destination Hosts

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

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.253.105	1988	2114	30	104
MY.NET.84.216	31	43	1	1
MY.NET.20.10	15	94	3	7
MY.NET.152.19	5	8	3	3
MY.NET.191.5	5	5	1	1

The attacker is performing reconnaissance and is scanning for misconfigured Wingate, Socks, Squid, and Proxy servers. Traffic sent to a misconfigured proxy server can be relayed anywhere (i.e. the Internet or the University's network). Most of the proxy scan attempts are being sent to MY.NET.253.105 to port 8080. HTTP Proxies typically listen on ports 3128, 5865, 8080, and even port 80. See CVE-1999-0291,CVE-1999-0471.

Correlations

This detect has also be seen by Laurie Zirkle at http://www.incidents.org/archives/intrusions/msg01422.html.

- **NMAP TCP ping!**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.253.10	2290	2582	845	857
64.152.70.68	18	18	1	1
64.119.138.2	6	6	3	3
193.144.127.9	5	5	1	1
64.210.77.125	5	5	2	2

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.1.8	22	23	4	5
MY.NET.1.3	7	11261	4	3468
MY.NET.23.38	6	6	1	1
MY.NET.25.65	6	6	1	1
MY.NET.24.69	6	7	1	1

The attacker is using Nmap (http://www.nmap.org) to perform network reconnaissance. Nmap has an option to scan networks with TCP instead of ICMP.

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

The most prevalent attacker is MY.NET.253.10 from source port 41161 to a variety of MY.NET class C networks.

Correlations

This detect been seen by Paul Asadoorian (practical number 337) at http://www.giac.org/Paul_Asadoorian_GCIA.zip.

- **ICMP Fragment Reassembly Time Exceeded**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.223.182	1376	1376	1	1
MY.NET.153.210	286	286	2	2
MY.NET.84.218	117	117	2	2
MY.NET.111.221	109	125	1	9
MY.NET.98.215	86	92	1	4

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.6.52	1376	1376	1	1
61.150.5.19	390	390	3	3
61.150.5.18	117	117	2	2
211.110.15.221	86	86	1	1
211.171.255.246	79	79	1	1

As stated in RFC-792 (http://www.faqs.org/rfcs/rfc792.html), "If a host reassembling a fragmented datagram cannot complete the reassembly due to missing fragments within its time limit it discards the datagram, and it may send a time exceeded message." An attacker can send a stimulus packet to cause a system to respond with an ICMP Fragment Reassembly Time Exceeded packet that may allow them to identify the OS.

Correlations

This detect has also been seen by Antony Riley at http://www.incidents.org/archives/intrusions/msg01590.html.

- **Watchlist 000222 NET-NCFC**

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

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
159.226.240.107	1213	1256	2	2
159.226.165.60	434	439	1	1
159.226.165.70	266	266	1	1
159.226.42.56	244	249	2	2
159.226.117.1	80	80	1	1

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.253.114	2159	33114	5	1124
MY.NET.100.230	85	92	2	4
MY.NET.253.41	52	64	1	6
MY.NET.100.165	45	31031	1	4288
MY.NET.110.32	25	25	1	1

The Watchlist 000222 NET-NCFC alert activated anytime packets belonging to the Computer Network Center Chinese Academy of Sciences are seen. Most of the top five sources alerts have been generated on traffic sent to MY.NET.253.114 and MY.NET.100.165 on port 80. They are more than likely running web servers. Also note that both MY.NET.253.114 and MY.NET.100.165 have an exceedingly high number of total alerts that need to be investigated further (see CS WEBSERVER - external web traffic alert and Internal Machine Insights below).

Registration Information for 156.226.0.0:

The Computer Network Center Chinese Academy of Sciences (NET-NCFC)

P.O. Box 2704-10,
Institute of Computing Technology Chinese Academy of Sciences
Beijing 100080, China

Netname: NCFC
Netblock: 159.226.0.0 - 159.226.255.255

Coordinator:
Qian, Haulin (QH3-ARIN) hlqian@NS.CNC.AC.CN
+86 1 2569960

Domain System inverse mapping provided by:

NS.CNC.AC.CN 159.226.1.1

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

GINGKO.ICT.AC.CN 159.226.40.1

Correlations

N/A. All the traffic from 159.226.0.0 appears to have generated alerts that are probably standard with a web based application.

- **ICMP Destination Unreachable (Communication Administratively Prohibited)**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
192.80.43.21	575	575	1	1
141.161.184.45	479	479	1	1
209.251.128.254	173	173	1	1
64.200.158.10	116	116	1	1
MY.NET.16.13	114	114	21	21

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.140.9	1232	49071	4	68
MY.NET.70.11	599	1657	92	124
MY.NET.70.192	116	122	1	5
207.46.197.100	112	256	2	6
MY.NET.70.146	109	3099	28	629

A router generates this alert if it cannot forward a packet due to administrative filtering. This is ICMP Type 3 - Destination unreachable, Code 13 - Communication with destination host is administratively prohibited. The top 3 source addresses are attempting to communicate with MY.NET.140.9 that has a total of 49,071 alerts.

Correlations

This detect has also been logged by Laurie Zirkle at http://www.incidents.org/archives/intrusions/msg02798.html.

- **ICMP Echo Request Nmap or HPING2**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)

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

MY.NET.98.172	893	927	1	6
MY.NET.98.180	814	824	2	6
MY.NET.98.120	362	812	3	23
200.241.247.36	361	390	361	361
MY.NET.253.10	292	2582	292	857

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
149.1.1.1	2023	2023	8	8
64.58.76.223	330	331	1	2
207.46.131.30	292	292	1	1
206.251.6.192	56	56	8	8
64.58.76.225	49	49	2	2

Nmap (http://www.nmap.org) and HPING2 (http://www.hping.org/) send an ICMP Echo request with no data at all. (Normal *BSD pings will send 64 bytes of data). These tools are being used by the sources (mainly University machines) for network recon probes.

Correlations

A similar detect has also been seen by John Copeland at http://people.atl.mediaone.net/jacopeland/probe4_5.html.

- **connect to 515 from outside**

All Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
163.17.157.130	3645	4305	36	36
211.198.225.65	480	480	414	414
255.255.255.255	2	2	2	2

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.190.13	1961	2291	1	3
MY.NET.190.51	1648	1991	1	1
MY.NET.137.106	3	4	2	3
MY.NET.190.3	3	4	2	3
MY.NET.132.6	3	3	2	2

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

This alert detects attempted external access to port 515/tcp (UNIX LPD) on any University internal MY.NET hosts. Exploits with LPD on many versions of OS exist that enable the attacker to either cause a denial of service (DOS) or gain root access. 163.17.157.130 attempts were intermixed with x86 NOOP alerts as well (see EXPLOIT x86 NOOP above) and focused primarily on MY.NET.190.13 and MY.NET.190.51. 211.198.225.65 launched a port 515/tcp recon probe across several class C networks. The attacker, 255.255.255.255, is a spoofed address and this particular attack has been seen before (see http://www.securityfocus.com/archive/19/187958). The SecurityFocus URL describes a similar attack with a destination port 515 (LPD) and source port of 31337 in scanning attempts.

Correlations

This detect can also be correlated with at http://www.sans.org/y2k/122100-1200.htm.

- **Watchlist 000220 IL-ISDNNET-990517**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
212.179.41.144	3623	3623	1	1
212.179.112.100	641	641	9	9
212.179.48.2	588	588	2	2
212.179.35.8	199	199	1	1
212.179.3.218	67	67	1	1

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.70.70	3705	5536	11	537
MY.NET.70.146	692	3099	27	629
MY.NET.152.173	229	285	42	65
MY.NET.98.159	199	243	1	5
MY.NET.98.109	117	121	1	3

These Snort rules alert on any connections from Israel (212.179.0.0). The traffic from 212.179.41.144, source port 2732, appears to be mainly to MY.NET.70.70, destination port 1214 over a 2-hour period on November 23, 2001. 212.179.48.2 is also communicating on to port 1214 on MY.NET.70.146 for approximately 3 hours. Port 1214 is associated with file sharing software called KAZAA (see

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

http://www.kazaa.com). Both MY.NET.70.70 and MY.NET.70.146 together have a very high percentage of the alerts need to be further investigated.

Registration Information for 212.179.0.0:

inetnum: 212.179.0.0 - 212.179.1.255
netname: AREL-NET
descr: arel-net
country: IL
admin-c: TP1233-RIPE
tech-c: TP1233-RIPE
status: ASSIGNED PA
notify: hostmaster@isdn.net.il
mnt-by: RIPE-NCC-NONE-MNT
changed: hostmaster@isdn.net.il 19990624
source: RIPE

route: 212.179.0.0/17
descr: ISDN Net Ltd.
origin: AS8551
notify: hostmaster@isdn.net.il
mnt-by: AS8551-MNT
changed: hostmaster@isdn.net.il 19990610
source: RIPE

person: Tomer Peer
address: Bezeq International
address: 40 Hashakham St.
address: Petakh Tiqwah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
nic-hdl: TP1233-RIPE
changed: registrar@ns.il 19991113
source: RIPE

Correlations

John Sage (http://www.incidents.org/archives/intrusions/msg02917.html) and Victor Maseda (http://www.giac.org//practical/Victor_Maseda_GCIA.doc) see traffic from the alert group.

- **Incomplete Packet Fragments Discarded**

Top 5 Source Hosts

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

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
61.150.5.18	2538	7636	4	5
61.150.5.19	2530	3842	2	2
61.134.9.88	1813	5882	2	3
211.40.179.122	235	745	2	2
216.106.172.149	84	556	1	1

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.53.36	2447	3314	1	1
MY.NET.53.148	1789	2090	2	3
MY.NET.53.33	1517	5087	3	5
MY.NET.153.153	834	1865	1	1
MY.NET.153.145	294	526	1	1

This alert detects when fragmented packets are received and subsequently discarded because the all of the packet fragments did not arrive within the specified time (set by a watchdog timer). All five alert sources have the same traits in the logs their communication with the destination is on both source and destination port 0.

11/21-18:51:25.748307 [**] MISC Large UDP Packet [**] 61.150.5.18:4549 -> MY.NET.53.148:1616
11/21-18:51:30.048778 [**] Incomplete Packet Fragments Discarded [**] 61.150.5.18:0 -> MY.NET.53.148:0
11/21-18:51:31.155551 [**] Incomplete Packet Fragments Discarded [**] 61.150.5.18:0 -> MY.NET.53.148:0

This often happens with corrupted or crafted data.

Correlations

Ralf Hildebrandt has detected these packets that were probably caused by corruption (http://www.geocrawler.com/archives/3/4890/2001/4/0/5645448/).

- **SMB Name Wildcard**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.163.53	2105	2105	1202	1202
169.254.101.152	1485	1488	1	3

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

MY.NET.217.42	823	823	487	487
MY.NET.85.111	572	572	223	223
MY.NET.218.66	323	323	184	184

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.5.118	1485	2010	1	2
MY.NET.133.59	20	20	1	1
MY.NET.132.10	16	26	4	9
MY.NET.16.14	13	175	6	86
MY.NET.217.42	13	16	13	15

The SMB Name Wildcard alert refers to UDP traffic from port 137 to port 137 made associated with NetBIOS name queries. A host doing name queries or an end user running the nbstat –a <IP Address> command looking for available shares, may activate this. Most of this activity appears to be contained within the University network except for one case when 169.254.101.152 is querying MY.NET.5.118 for the five consecutive days. It is unclear why 169.254.101.152 trying solely for this host. It is good practice not to make these services to the Internet community unavailable due to their vulnerability: CAN-1999-0520 - A system-critical NETBIOS/SMB share has inappropriate access control.

Correlations

The following detects have been seen by Robert Sorensen at http://www.giac.org/practical/Robert_Sorensen_GCIA.htm).

- **ICMP Destination Unreachable (Host Unreachable)**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
63.146.1.33	3368	3374	21	25
160.36.56.17	1412	1412	1	1
198.124.254.166	805	805	1	1
151.202.4.90	98	98	1	1
209.115.223.170	86	86	1	1

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)

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

MY.NET.140.9	2220	49071	5	68
MY.NET.70.146	2034	3099	451	629
MY.NET.70.70	1562	5536	411	537
MY.NET.70.97	1244	2020	448	594
MY.NET.70.11	1030	1657	18	124

These ICMP packets are probably being generated by the sources to perform a recon probe of particular hosts. The ICMP Destination Unreachable (Host Unreachable) message will be sent by a router in response to a packet that it cannot forward because the destination is not there or cannot be reached. Most of the activity is directed to MY.NET.70.70, MY.NET.70.97, MY.NET.70.11, MY.NET.137.7, and MY.NET.70.146.

Correlations

These detects can be correlated by Allan Powell at http://www.sans.org/y2k/092900.htm.

- **MISC Large UDP Packet**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
61.150.5.18	5098	7636	5	5
61.134.9.88	4068	5882	3	3
61.150.5.19	1311	3842	2	2
211.40.179.122	510	745	2	2
216.106.172.149	472	556	1	1

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.53.33	3554	5087	3	5
MY.NET.111.221	2589	2600	2	6
MY.NET.88.148	1936	1936	1	1
MY.NET.153.153	1031	1865	1	1
MY.NET.53.36	866	3314	1	1

This Snort alert was triggered because the UDP datagram length is greater than 1200 bytes. There appear to be lengthy communication sessions between the source and destination where the source port and destination port remain the same. Unfortunately, we do not have the data that shows the initiating connections so it is difficult to tell what is going on. There are new Internet services constantly starting

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

that use some new set of poorly documented and unregistered ports. A search for these ports (primarily 1610, 1629, 1739, 1873, and 2263) on the Trojan and Port List sites (see Appendix A) did not find them listed as possible trojans. These connections are quite possibly on-line gaming sites, chat sessions, or other Internet based conferencing/communication software. These ports were not currently listed on the SANS "What are some of the signs of Internet Gaming?" site at http://www.sans.org/y2k/gaming.htm. A good likelihood is that these are MS NetMeeting connections (secondary UDP connections on dynamically assigned ports, 1024-65535 (see http://support.microsoft.com/default.aspx?scid=kb;EN-US;q158623).

Correlations

This detect can be correlated at http://www.netarc.jp/doc/snfout.snort_portscan.log/193/251/174/src193.251.174.58.html.

- **INFO MSN IM Chat data**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
64.4.12.156	625	625	18	18
64.4.12.153	483	483	27	27
MY.NET.98.120	441	812	16	23
MY.NET.97.238	430	441	11	17
MY.NET.98.245	411	414	9	11

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
64.4.12.151	580	580	37	37
64.4.12.172	564	564	21	21
64.4.12.156	524	524	20	20
64.4.12.160	524	524	20	20
64.4.12.174	501	501	25	25

This Snort alert looks for traffic that is related to the MS MSN Messenger service (see http://support.microsoft.com/default.aspx?scid=kb;EN-US;q278887). This will look for activity on source and destination port 1863. MSN Messenger is a heavily used service within the University (249 sources and 367 destinations in total).

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

Correlations

N/A. All the traffic appears to have generated alerts that are probably standard with a MSN Messenger.

- **ICMP Echo Request BSDtype**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
128.16.64.81	4759	4973	1	1
141.213.11.120	4393	4533	1	1
147.46.59.144	4317	4480	1	1
129.79.245.106	4086	4238	1	1
129.132.66.28	3922	4093	1	1

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.70.148	27789	29551	9	126
195.94.94.111	17	17	1	1
24.18.175.188	10	10	1	1
165.247.84.143	8	8	1	1
172.25.5.63	6	6	1	1

This alert is an attempt is typically a recon probe where the source OS is BSD characteristics of the ICMP packet. All source alerts were ICMP BSD echo requests sent to MY.NET.70.148! Closer examination of MY.NET.70.148 show that there is other that malicious traffic from and to it generated alerts (see Internal Machine Insights).

Correlations

This detect can also seen by Jason Hunt at http://archives.neohapsis.com/archives/snort/2001-02/0529.html.

- **CS WEBSERVER - external web traffic**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
209.73.162.12	1489	1503	1	2

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

24.157.233.180	757	757	1	1
140.239.251.224	495	499	1	1
202.38.124.248	431	447	1	3
204.166.111.29	373	375	1	3

All Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.100.165	30202	31031	4194	4288

This alert refers all external http access to the CS WEBSERVER. A search on google.com found the following link, http://www.cs.ucla.edu/wwwmaster/about.html, which indicates this server is the UCLA Computer Science Department Web Server, http://www.cs.ucla.edu.

Since this is an Internet facing web server, one should expect to see this kind of traffic and alerts of this kind being triggered. Further examination reveals that all alerts seem to be the result of normal web browsing. Knowing which machines on the University network are high traffic web servers will help separate attacks from normal traffic.

25 different signatures are present for *MY.NET.100.165* as a destination

- 1 instances of *SCAN Proxy attempt*
- 1 instances of *spp_http_decode: CGI Null Byte attack detected*
- 1 instances of *WEB-CGI w3-msql access*
- 2 instances of *WEB-FRONTPAGE _vti_rpc access*
- 2 instances of *WEB-CGI finger access*
- 2 instances of *CS WEBSERVER - external ssh traffic*
- 2 instances of *High port 65535 tcp - possible Red Worm - traffic*
- 3 instances of *WEB-CGI ksh access*
- 4 instances of *WEB-CGI tsch access*
- 5 instances of *WEB-MISC Attempt to execute cmd*
- 8 instances of *spp_http_decode: IIS Unicode attack detected*
- 9 instances of *WEB-IIS view source via translate header*
- 9 instances of *WEB-IIS _vti_inf access*
- 11 instances of *INFO FTP anonymous FTP*
- 12 instances of *WEB-MISC prefix-get //*
- 15 instances of *Port 55850 tcp - Possible myserver activity - ref. 010313-1*
- 17 instances of *WEB-MISC Lotus Domino directory traversal*
- 18 instances of *WEB-CGI redirect access*
- 20 instances of *WEB-CGI csh access*
- 38 instances of *Queso fingerprint*
- 45 instances of *Watchlist 000222 NET-NCFC*

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

- 134 instances of *WEB-CGI scriptalias access*
- 203 instances of *CS WEBSERVER - external ftp traffic*
- 267 instances of *WEB-MISC http directory traversal*
- 30202 instances of *CS WEBSERVER - external web traffic*

Due to the nature of these alerts, a review of the OS and web server software security should be conducted.

Correlations

N/A. This Snort alert appears to track all traffic destined to the CS Web Server machine

- **WEB-MISC prefix-get //**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
67.201.13.219	420	420	1	1
208.148.191.201	348	350	1	2
206.196.188.55	346	346	1	1
24.4.252.20	259	259	1	1
207.19.126.2	246	246	1	1

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.253.114	30865	33114	1096	1124
MY.NET.253.115	439	442	43	44
MY.NET.100.165	12	31031	4	4288
MY.NET.179.77	3	71	3	27
MY.NET.5.76	2	12	2	5

This alert is triggered when two slashes are entered after the URL. This could be due to legitimate traffic (i.e. the web application) or someone attempting to manipulate of the HTTP request headers in order to gain access to parts of the web server not normally visible. This may also be an attempt by an attacker to evade the Snort system. As described in Rain Forest Puppy's whisker anti-IDS web scan tool URL at http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html:

"In an effort to break up a string, the classic double slash method replaced every single '/' with '//'. This resulted in checks for "/cgi-bin/some.cgi" not matching "//cgi-bin//some.cgi". However, most ID systems are aware of this trick."

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

The traffic should be examined closer to determine what is being accessed.

Correlations

N/A. All the traffic appears to have generated alerts that are probably normal traffic associated with a web based application.

- **MISC source port 53 to <1024**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
194.90.1.5	2382	2382	3	3
199.203.1.20	374	374	3	3
195.9.105.242	263	263	3	3
192.88.193.144	252	252	1	1
207.69.200.240	160	160	2	2

All Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.1.3	11227	11261	3462	3468
MY.NET.1.4	8999	9001	2690	2691
MY.NET.1.5	8881	8882	2588	2589
MY.NET.88.88	2675	2677	4	5
MY.NET.1.2	683	686	173	175
MY.NET.137.7	266	1211	152	157
MY.NET.1.10	18	29	2	7
MY.NET.1.9	16	28	1	10
MY.NET.130.122	4	4	3	3
MY.NET.98.215	1	33	1	3

These alerts were triggered DNS name lookups from source port 53 and are more than likely legitimate traffic. There does appear to be, however, a lot of incessant ICMP Destination Unreachable (Host Unreachable) traffic to MY.NET.137.7 that should be further investigated.

Correlations

N/A. All the traffic appears to have generated alerts that is probably normal DNS traffic.

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

- **ICMP Echo Request Windows**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
24.39.174.239	32744	32744	1	1
MY.NET.98.169	1969	1970	4	5
MY.NET.98.122	1444	1445	2	3
MY.NET.97.178	1368	1368	1	1
MY.NET.98.142	854	856	5	6

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.70.225	32744	32744	1	1
152.163.15.15	1956	1956	1	1
152.163.15.43	1368	1368	1	1
205.188.70.34	822	822	1	1
205.188.66.15	622	622	1	1

This alert is typically a recon probe where the source OS has MS Windows characteristics in the ICMP packet (i.e. TTL = 128). Of primary interest is the source, 24.39.174.239, which sent 32744 instances of ICMP echo requests to MY.NET.70.225 during the entire day of November 25, 2001. No other alerts were detected on MY.NET.70.225 so it is unknown what other information 24.139.174.239 was after. What other services are running MY.NET.70.225?

Correlations

This detect is seen and analyzed by Ofir Arkin at http://archives.indenial.com/hypermail/bugtraq/2001/May2001/0026.html.

- **MISC traceroute**

Top 5 Source Hosts

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
152.2.254.247	886	886	1	1
134.75.30.5	855	855	1	1
128.182.61.50	855	855	1	1
134.121.2.2	852	852	1	1

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

128.113.39.54	848	848	1	1

Top 5 Destination Hosts

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.140.9	45618	49071	58	68
MY.NET.70.148	837	29551	9	126
MY.NET.70.70	11	5536	1	537
MY.NET.1.10	9	29	4	7
MY.NET.115.115	8	124	3	43

This alert is generated from the sources who are trying to map the path (i.e. discover the routers through which a datagram would travel) to a destination, primarily MY.NET.140.9. A wide range of "traceroute" capable tools exist (such as Trout, TracerX, MTR) that may use a combination of ICMP and UDP packets to do their discovery.

As sample of the Misc traceroute signature traffic contains:

11/22-08:04:57.972327 MY.NET.140.9:33468	[**]	MISC	traceroute	[**]	128.182.61.50:54072	->
11/22-08:05:02.977320 MY.NET.140.9:33469	[**]	MISC	traceroute	[**]	128.182.61.50:54072	->
11/22-08:05:07.983734 MY.NET.140.9:33470	[**]	MISC	traceroute	[**]	128.182.61.50:54072	->

This small sample shows traffic to the same three destination ports, 33468, 33469, and 33470 with the pattern repeating itself for most of November 22, 2001. In fact, the entire list of source IPs above had similar traffic destined to MY.NET.140.9 on ports 33434 to 33470. This pattern is the standard range of ports used by the traceroute program (MS tracert only uses ICMP). These traceroutes could also be from the multitude of traceroute servers located in the Internet (see http://www.slac.stanford.edu/comp/net/wan-mon/traceroute-srv.html).

Correlations

This detect can be correlated at http://www.silicondefense.com/software/snortsnarf/example/src240.226.156.151.html.

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

Top Ten Talkers – Snort Scans

The top 10 talkers were determined by analysing the five days worth of Snort scan log files focusing on the number of scans by source and destination and categorising the traffic based on the most common ports used. The total number of Snort scan entries from November 21, 2001 to November 25, 2001 amounted to 1,467,666 packets.

Top 10 Sources of Scans

# of Scans	Source	Traffic Categorization (Most Common Ports)
680863	MY.NET.5.75	Source port 67, destination port 68 to internal many destinations
277421	MY.NET.87.50	Source port 888 & 999 to mainly port 27500, 27005, 2705, and 2213 on many external destinations
239618	MY.NET.5.76	Source port 67, destination port 67 & 68 to internal many destinations
9483	205.188.233.153	Destination port 6970, many different internal hosts.
8960	205.188.246.121	Destination port 6970, many different internal hosts.
8635	217.136.7.67	Destination port 21, many different internal hosts.
6544	209.235.8.118	Destination port 53, many different internal hosts.
6486	205.188.233.185	Destination port 6970, many different internal hosts.
6321	MY.NET.253.10	Source port 41162, many different internal hosts.
5923	MY.NET.97.212	Destination port 110, many different external hosts.

Analysis

The activity on MY.NET.5.75 appears to be DHCP related which uses the BOOTP protocol (BOOTP server is port 67/udp & BOOTP client is 68/udp). Since the source port is 67 and the destination port is 68, MY.NET.5.75 is probably a DHCP server.

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

MY.NET.87.50's activity is related to on-line gaming with port 27500 being associated with Quake V3.0 and port 27005 being associated with Half-Life. See the papers at Incidents.org (http://www.incidents.org/detect/gaming.php) and SANS (http://www.sans.org/y2k/gaming.htm) for references on on-lien gaming ports.

Destination port 6970/udp on 205.188.233.185 (g2lb5.spinner.com), 205.188.233.185 (g2lb3.spinner.com), and 205.188.233.185 (g2lb6.spinner.com) is associated with RealAudio from RealNetworks (http://www.real.com) that allows end users to download and play music on their machines.

217.136.7.67 scanned a variety of internal hosts looking for listening FTP servers (port 21). The attacker may be looking for an active FTP server to take advantage of the many exploits the various implementations of FTP have had. WU-FTP has had one recently. See CAN-2001-0550 at http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0550.

209.235.8.118 scanned a variety of internal hosts looking for DNS servers (port 53). Like FTP, implementations of DNS (BIND) have had their share of vulnerabilities. Searching for DNS CVE entries (http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=dns) produces a lengthy list of vulnerabilities.

MY.NET.253.10 initiated a Nmap XMAS scan at many internal hosts to perform reconnaissance. The fact that this internal machine probed other internal machines needs to be investigated. Is the attacker a curious employee or is this a compromised host?

MY.NET.97.212 scanned a variety of external hosts looking for POP3 (110/tcp) servers. Due to the thousands of hosts scanned, MY.NET.97.212 may be looking for POP3 servers to exploit. There are plenty of CVE numbers such as CVE-1999-0006 and CVE-1999-0042 (see http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=pop) associated with POP.

Top 10 Destinations Scanned

# of Scans	Destination	Traffic
19845	24.164.45.163	Many connections from MY.NET.87.50, source ports 888 & 999 to mainly port 27500
14245	24.254.241.95	Many connections from MY.NET.87.50, source ports 888 & 999 to mainly port 27005
9662	199.174.183.196	Many connections from MY.NET.87.50 on mainly port 2213
8370	24.180.10.152	Many connections from MY.NET.87.50 on mainly ports 2705 & 2213
5984	65.164.16.157	Many connections from MY.NET.87.50, source ports 888 & 999 to mainly port

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

		27005
5519	65.10.130.34	Many connections from MY.NET.87.50, source ports 888 & 999 to mainly port 27005
5038	24.4.97.225	Many connections from MY.NET.87.50, source ports 888 & 999 to mainly port 27005
4440	24.4.159.115	Many connections from MY.NET.87.50, source ports 888 & 999 to mainly port 27005
4435	211.245.73.153	Many connections from MY.NET.97.173 on a wide range of source and destination ports
4240	24.178.16.42	Many connections from MY.NET.87.50, source ports 888 & 999 to mainly port 27005

Analysis

The top scanned destination is 24.164.45.163 that is a Quake V3.0 on-line game server (port 27500/tcp) that MY.NET.87.50 is connecting to.

The activity to 24.254.241.95, 65.164.16.157, 65.10.130.34, 24.4.97.225, 24.4.159.115, and 24.178.16.42 appears to be Half-Life servers (port 27005/tcp) that MY.NET.87.50 is connecting to.

199.174.183.196 was scanned by MY.NET.87.50 that is activity related to Kali online gaming (see http://www.kali.net).

The scans to 211.245.73.153 are all from MY.NET.97.173 may be Microsoft's NetMeeting, video-conferencing style software, related since there are scans to ports 1503, 29322, 29323, 49606, 49607, 49608, and 49609. This activity can be correlated at http://www.avolio.com/columns/wishlist.html (see "The Bad and the Ugly: NetMeeting"). All of the scanning activity occurred in a 3.5-hour window from Nov. 22, 20:12:12 to Nov. 22, 23:44:58. The Snort alert logs also show MS MSN Messenger (see the "INFO MSN IM Chat data" alert described above) activity from MY.NET.97.173.

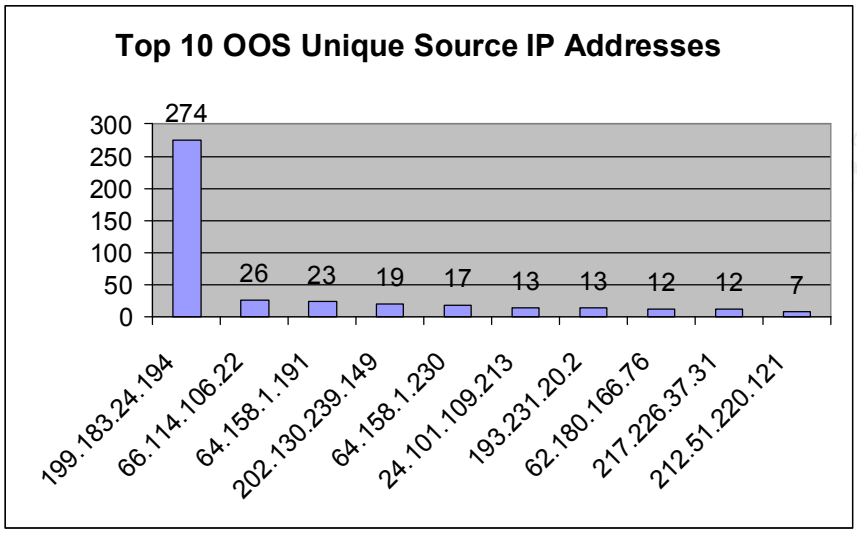
Out-of-Specification Files Analysis

Out-of-Specification (referred to Out-of-Spec or OOS) are TCP packets that are not normally seen by the TCP stack and may have invalid TCP flags set. They should not been seen under normal circumstances. However, attackers often craft packets of this type (using Nmap, Hping2, or Queso) in order to evade intrusion detection systems or

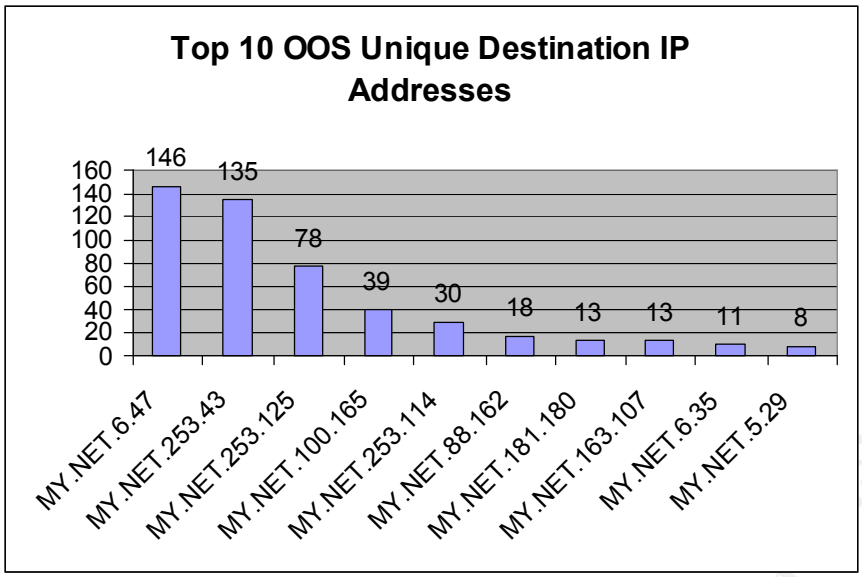
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

firewalls. They can also be caused by hardware problems or misconfigured devices such as routers.

During the five consecutive days, the total number of OSS entries amounted to 584 TCP packets. The following two link graphs, Top 10 Source IP Addresses and Top 10 Destination IP Addresses and the Top 10 Source/Destination IP Addresses Pairs table illustrate some interesting activity.



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



Top 10 Source/Destination IP Address Pairs Table

# of Occurrences	Source IP	Destination IP
142	199.183.24.194	MY.NET.6.47
131	199.183.24.194	MY.NET.253.43
23	64.158.1.191	MY.NET.253.125
18	202.130.239.149	MY.NET.253.114
17	64.158.1.230	MY.NET.253.125
13	24.101.109.213	MY.NET.88.162
13	193.231.20.2	MY.NET.100.165
12	62.180.166.76	MY.NET.253.125
12	217.226.37.31	MY.NET.181.180
10	66.114.106.22	MY.NET.6.35
7	212.51.220.121	MY.NET.163.107

As can be seen from the two link graphs and table, the source IP 199.183.24.194 has the majority share of OOS traffic to both MY.NET.6.47 and MY.NET.253.43. Upon

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

closer examination of activity between 199.183.24.194 and MY.NET.6.47 in the log files (Alerts, Scans, and OOS), we can see that the OOS packets have a Queso program signature on destination port 25 (SMTP). Activity between 199.183.24.194 and MY.NET.253.43 is identical.

Alerts log:

11/21-01:23:30.801720 [**] Queso fingerprint [**] 199.183.24.194:60006 -> MY.NET.6.47:25

Scans log:

Nov 21 01:23:30 199.183.24.194:60006 -> MY.NET.6.47:25 SYN 12****S* RESERVEDBITS

OOS log:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-01:23:39.672356 199.183.24.194:60006 -> MY.NET.6.47:25
TCP TTL:52 TOS:0x0 ID:26176  DF
21S***** Seq: 0x31B6D4E9   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 882946729 0 EOL EOL EOL EOL
```

Queso is a program similar to Nmap, although not as robust or popular, that is used for OS fingerprinting (see http://www1.securityfocus.com/frames/?focus=ids&content=/focus/ids/articles/portscan.html). It is a CVE Candidate, CAN-1999-0454, http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=queso.

Note that attempted communication between 199.183.24.194 with both MY.NET.6.47 and MY.NET.253.43 lasted for the five consecutive days.

ODD OOS Entries

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

Not shown in the above graphs and table, the following three source and destination pairs were found that contained corrupted headers:

# of Occurrences	Source IP	Destination IP
5	66.125.110.88	MY.NET.70.70
5	66.122.133.242	MY.NET.82.131
3	64.108.76.200	MY.NET.115.115

The following is an example of a 66.125.110.88 -> MY.NET.70.70 packet:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/21-01:58:48.868749 66.125.110.88 -> MY.NET.70.70
TCP TTL:109 TOS:0x0 ID:60754  DF MF
Frag Offset: 0x0   Frag Size: 0x22
68 F1 AF D0 4C C5 F7 7B 2D C8 5B C8 4D F2 CB F0  h...L..{-.[.M...
2C 0C 39 DC 2A AA 75 56 19 47 3F CC 5F BF 68 8A  ,.9.*.uV.G?._.h.
FA C4                                            ..
```

The most obvious problem with this packet is that it's missing port numbers! This cannot be the case in normal TCP communications. What happened? This packet and the others it definitely shows signs of being crafted. Perhaps the attacker is trying to evade the Snort system. Perhaps there is an issue with the event generator's, Snort, TCP port filtering and matching mechanism? Or, perhaps this packet corruption is the result of a hardware problem. More information is required.

Internal Machine Insights

The University Snort logs (alerts, scans, and OOS) showed unusual signs of benign, exploit, and reconnaissance activity from a variety of external and University sources. In addition to the University machines mentioned thus far, the following selected University machines show signs of the highest levels of compromise or possible dangerous or anomalous activity:

Compromised

MY.NET.70.148 had 29551 alerts (16 different signatures) were detected from 126 distinct source IPs from 00:06:54 on November 21, 2001 to 23:44:27 on November 25, 2001.

- 1 instances of FTP DoS ftpd globbing
- 1 instances of EXPLOIT x86 stealth noop
- 1 instances of ICMP traceroute
- 1 instances of MISC Source Port 20 to <1024
- 2 instances of ICMP Destination Unreachable (Communication Administratively Prohibited)

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

- 3 instances of INFO - Possible Squid Scan
- 3 instances of SCAN Proxy attempt
- 3 instances of EXPLOIT x86 setuid 0
- 5 instances of ICMP Echo Request Windows
- 6 instances of High port 65535 tcp - possible Red Worm - traffic
- 7 instances of x86 NOOP - unicode BUFFER OVERFLOW ATTACK
- 10 instances of ICMP Echo Request Nmap or HPING2
- 288 instances of EXPLOIT x86 NOOP
- 594 instances of INFO FTP anonymous FTP
- 837 instances of MISC traceroute
- 27789 instances of ICMP Echo Request BSDtype

10 alerts (2 signatures) were detected from this source to 1 distinct IP, 204.152.184.75, from 02:29:54 on November 21, 2001 to 23:26:02 on November 25, 2001:

- 5 instances of IDS50/trojan_trojan-active-subseven
- 5 instances of High port 65535 tcp - possible Red Worm - traffic

A sample of the traffic containing the IDS50/trojan_trojan-active-subseven activity:

11/21-02:29:54.452396	[**]	IDS50/trojan_trojan-active-subseven	[**]
MY.NET.70.148:1243 -> 204.152.184.75:53066			
11/21-22:13:31.879289	[**]	IDS50/trojan_trojan-active-subseven	[**]
MY.NET.70.148:1243 -> 204.152.184.75:64731			
11/21-23:16:14.985366	[**]	IDS50/trojan_trojan-active-subseven	[**]
MY.NET.70.148:1243 -> 204.152.184.75:60202			
11/24-09:44:05.038449	[**]	IDS50/trojan_trojan-active-subseven	[**]
MY.NET.70.148:1243 -> 204.152.184.75:52038			
11/25-23:26:02.477591	[**]	IDS50/trojan_trojan-active-subseven	[**]
MY.NET.70.148:1243 -> 204.152.184.75:63364			

It is clear from the multiple suspicious signatures (various scans, possible buffer overflow attacks, ICMP recon probes, and anonymous FTP activity) and the magnitude of alerts that MY.NET.70.148 is in trouble during the entire five consecutive days of files analysed. As seen by the sample of SubSeven (also known as BackDoor-G, Pinkorm, SubStealth, etc.) alert on the outbound traffic, there is clear indication that MY.NET.70.148 is a trojaned host and required immediate attention. SubSeven is a trojan designed for the MS Windows platform and is comprised of a client and server. The attacker uses the client to connect to the victim's machine to install the server agent. And, once the server agent is installed, the attacker has full access to the victim's machine that can then itself be used as an attack machine.

The following sources provide an excellent description (and removal process) of the SubSeven type trojans:

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

http://www.sans.org/infosecFAQ/malicious/subseven2.htm
http://www.sans.org/newlook/resources/IDFAQ/subseven.htm

Highly Dangerous or Anomalous Activity

MY.NET.16.42 and MY.NET.11.4 generated the following highly suspicious signatures in communication between themselves:

- Port 55850 tcp - Possible myserver activity - ref. 010313-1
  Myserver is a Distributed Denial of Service (DDOS) agent with DOS and scanning capabilities that use port 55850. The source IP is often spoofed. Even though Myserver is normally UDP, this TCP signature should still be investigated. See http://www-net.cs.umass.edu/~brian/cs515/lecture22.ppt.

- Possible trojan server activity
  This alert looks activity to port 27374/tcp which is normally associated with the SubSeven trojans (see MY.NET.70.148 above).

- High port 65535 tcp - possible Red Worm – traffic
  This alert has detected datagram payload containing a possible Code Red worm signature with a destination port of 65535/tcp. Code Red is a self-propagating worm the makes use of a MS IIS server vulnerability. See SANS link at http://www.sans.org/infosecFAQ/malicious/dragons.htm and the CERT link at http://www.cert.org/advisories/CA-2001-19.html for complete details.

- SUNRPC highport access!
  The attacker is may be attempting to access the Sun Solaris portmapper, requesting port information for the RPC services. The daemon ypbind is typically associated on port 32771/tcp.

MY.NET.6.7, MY.NET.253.114, MY.NET.60.14, MY.NET.60.125 exhibited the following highly suspicious signature activity as alert sources and as destinations from a variety of sources:

- Port 55850 tcp - Possible myserver activity - ref. 010313-1
  See above.

- Possible trojan server activity
  See above.

- High port 65535 tcp - possible Red Worm - traffic
  See above.

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

MY.NET.253.10 is using Nmap or Hping2 to scan several University machines during the full five days worth of logs and should be investigated. Two different signatures are present for MY.NET.253.10 as a source:

- 292 instances of ICMP Echo Request Nmap or HPING2
  See Selected Detects – Snort Alerts above.

- 2290 instances of NMAP TCP ping!
  See Selected Detects – Snort Alerts above.

Selected External Source Addresses

The following five external source addresses are selected for further investigation. This investigation should include the necessary steps to contact the host owners. A document produced by Donald Mclachlan and the GIAC Community that discusses these methods is available at http://www.incidents.org/react/contacting.php and should be reviewed.

1. 204.152.184.75

The identified IDS50/trojan_trojan-active-subseven and High port 65535 tcp - possible Red Worm - traffic Snort alerts from the apparent compromised University machine, MY.NET.70.148, is destined for 204.152.184.75. See Internal Machine Insights for further information above.

Registration Information:

M.I.B.H., LLC (NETBLK-MIBH-2BLK)
Star Route Box 159A
Woodside, CA 94062
US

Netname: MIBH-2BLK
Netblock: 204.152.184.0 - 204.152.191.255
Maintainer: VIX

Coordinator:
Vixie, Paul (PV15-ARIN) paul@VIX.COM
+1 415 747 0204

Domain System inverse mapping provided by:

NS-EXT.VIX.COM 204.152.184.64
NS1.GNAC.COM 209.182.195.77

Record last updated on 27-Apr-1999.

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

Database last updated on 21-Dec-2001 19:55:28 EDT.

2. 128.16.64.81

The largest number of Snort alert occurrences were generated by this attacker against the compromised machine, MY.NET.70.148, for the full five consecutive days:

- 62 instances of INFO FTP anonymous FTP
- 152 instances of MISC traceroute
- 4759 instances of ICMP Echo Request BSDtype

See Internal Machine Insights for further information above.

Registration Information:

University College London (NET-UCLNET)
Department of Computer Science Gower Street
London, WC1E 6BT
GB

Netname: UCL-CS-ETHER
Netblock: 128.16.0.0 - 128.16.255.255

Coordinator:
Andrews, John (JA168-ARIN) J.Andrews@cs.ucl.ac.uk
+44 71 387 7050 ext. 3691

Domain System inverse mapping provided by:

NS1.CS.UCL.AC.UK 128.16.5.32
MHS-RELAY.AC.UK 128.86.8.25

Record last updated on 01-Dec-2000.
Database last updated on 21-Dec-2001 19:55:28 EDT.

3. 24.39.174.239

This external source generated all 32744 instances of ICMP Echo Requests Windows Snort alerts to MY.NET.70.225 during the span from 10:47:38 on November 24, 2001 to 11:16:34 on November 25, 2001. 24.39.174.239 generated no other activity. What was it after? See Selected Detects – Snort Alerts above for additional information.

Registration Information:

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

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

@Home Network (NETBLK-HOME-5BLK)HOME-5BLK 24.36.0.0 - 24.39.255.255
@Home Network (NETBLK-BLTMMD1-MD-14) BLTMMD1-MD-14 24.39.160.0 - 24.39.175.255

4. 163.17.157.130

This attacker may be attempting a buffer overflow attack on MY.NET.190.13 LPD service (see EXPLOIT x86 NOOP alert described above). 660 instances of EXPLOIT x86 NOOP and 3645 instances of connect to 515 from outside alerts were detected. See Selected Detects – Snort Alerts above for additional information.

Registration Information:

Ministry of Education Computer Center (NET-TANET-B-5)
12th Fl, 106, Hoping E. Road, Sec 2.
Taiwan Republic of China, R.O.C
TW

Netname: TANET-B-5
Netblock: 163.17.0.0 - 163.17.255.255

Coordinator:
TANet, Administrator (AT122-ARIN) tanetadm@moe.edu.tw
886-2-27377010-295

Domain System inverse mapping provided by:

NCHUD1.NCHU.EDU.TW 140.120.1.2
MOEVAX.EDU.TW 140.111.1.2

Record last updated on 30-Apr-1999.
Database last updated on 21-Dec-2001 19:55:28 EDT.

5. 199.183.24.194

This external source generated the most OOS traffic to MY.NET.6.7 and MY.NET.253.114 for the full five consecutive days. These two machines also received a large amount of suspicious signatures from a variety of other external sources and which are noted in the Internal Machine Insights section.

Registration Information:

Red Hat Software (NET-REDHAT)
P.O. Box 4325
Chapel Hill, NC 27515
US

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

Netname: REDHAT
Netblock: 199.183.24.0 - 199.183.24.255

Coordinator:
Taylor, Stacy (ST452-ARIN) abuse@icgcom.com
408-579-5000

Record last updated on 01-Mar-2001.
Database last updated on 21-Dec-2001 19:55:28 EDT.

Defensive Recommendations

Based on the preceding analysis, the following actions are recommended to improve the security architecture at the University:

- Take immediate action to deal with potentially the compromised machine, MY.NET.70.148. Disconnect it from the network and conduct a full system audit. Preserve any system and application logs for a forensics review. Consider rebuilding the machine (i.e. reload all software starting with the OS) from scratch since the level of compromise (i.e. potentially many files) is unknown.

- Take immediate measures to conduct a security audit of the machines, MY.NET.16.42, MY.NET.11.4, MY.NET.6.7, MY.NET.253.114, MY.NET.60.14, and MY.NET.60.125 exhibiting highly suspicious signature activity. If necessary, follow the steps mentioned in the previous point.

- Review the scanning and telnet activity from the University machine, MY.NET.253.10, to other various University machines. Determine who may be involved and why this activity is being conducted.

- Review the University's security policy to see if the network traffic activity shown in the security audit complies with it. Identify the University machines which do not comply. Identify what services end users are allowed (or not) to run (i.e. RealAudio, Kazaa, on-line gaming, Napster, Gnotella, etc.).

- Consider performing a Vulnerability Analysis (VA) against all University network access points. This can be accomplished by hiring a reputable security firm to conduct it or this can be completed in-house. There are many excellent open source tools that can be used: Nmap at http://www.nmap.org, Nessus at http://www.nessus.org. Commercial scanners such as The ISS Internet scanner (http://www.iss.net) are also available to do this.

- Consider reviewing the ingress and egress rulesets at the University network security enforcement points (i.e. border routers and firewalls). Ensure that they are configured to only allow explicitly defined inbound and outbound traffic as per the security policy. Strong consideration should be given to completely block the

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

highly vulnerable services such as MS File and Print Sharing (port 135-139), telnet, LPD, etc.

- Review all host based security mechanisms in place, especially machines that face the Internet. Ensure that machine OS has been armoured (i.e. all non-essential services have been disabled, security patches have been applied, etc.).

- Review the current placement of all Snort network IDSes. Network IDSes are typically placed in front of or behind network security enforcement points (i.e. in front of or behind a firewall). They are also strategically placed in production server network segments to detect any activity destined to and from the site's critical server. Consideration should also be given to installed host based IDSes on all production servers (especially those that have and Internet facing network). Ensure that all IDS logs are routinely reviewed and correlated.

- Ensure that appropriate personnel, system and security administrators are on the alert for new vulnerabilities to services used in the University's network. Regularly monitor and subscribe to the following mailing lists to keep informed about the latest exploits and security vulnerabilities:

SANS	http://www.sans.org
CERT	http://www.cert.org
SecurityFocus	http://www.securityfocus.com
FIRST	http://www.first.org

Analysis Process

In order to process the five consecutive days' worth of Snort data files that were produced, a SUN Microsystems Sun-Fire-880 (2 x 750 MHz, 4Gb RAM, Solaris 2.8) was used. They were initially processed on a Sun Sparc5 (75 MHz, 96Mb RAM, Solaris 2.7) which proved to be woefully inadequate due to swapping issues. Below is the detail describing the process to prepare the data for analysis:

Snort Alerts Logs

SnortSnarf (http://www.silicondefense.com/software/snortsnarf/index.htm), version 010821.1, developed by James Hoagland, Stuart Staniford, and Joe McAlerney, which converts Snort alert logs to produce html was used. The processing of the 65 MB of Snort alert logs using SnortSnarf took to approximately 20 minutes to complete on the Sun-Fire-880.

1. First, combine the five alerts files into one:

```
for file in `ls alert*`
do
cat $file >> pre_main.alert
done
```


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

This created a 65Mb Snort alert file.

2. Second, convert all of the "MY.NET" references to an IP range not already used (192.173) in the alert file in order to allow SnortSnarf to process it:

   cat pre_main.alert | sed 's/MY.NET/192.173/g' > main.alert

3. Third, SnortSnarf was run:

   Snort.pl –d snortalerts main.alert

   After 20 minutes of processing, the 856Mb worth of SnortSnarf html structure was created in the snotralerts directory.

Snort OSS Logs

Various UNIX ksh (korn shell) scripts were used to process the OOS logs. Insights in building these scripts were gathered from Mike Bell's practical, http://www.giac.org/practical/Mike_Bell_GCIA.doc.

1. Combine the five OOS files into one:

   ```
   for $file in `ls oos_*`
   do
   cat $file >> main.oos
   done
   ```

   This created a 167Kb Snort OOS file.

2. To get total number of entries in oos files:

   grep -- '->' main.oos | wc –l

3. To obtain the top 10 source and destination IP address pairs:

   cat main.oos | grep -- '->' | awk '{print $2,$4}' | sed s/\:[0-9]*//g | head –10

4. To obtain the top 10 unique source IP addresses:

   cat main.oos | grep -- '->' | awk '{print $2,$4}' | sed s/\:[0-9]*//g | awk '{print $1}' | sort | uniq -c | sort -r -n -k 1 | head –10

5. To obtain the top 10 unique destination IP addresses:

   cat main.oos | grep -- '->' | awk '{print $2,$4}' | sed s/\:[0-9]*//g | awk '{print $2}' | sort | uniq -c | sort -r -n -k 1 | head –10

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

6. Taking the output from steps 4 and 5 into MS Excel created the graphs.

Snort Scan Logs

Various UNIX ksh (korn shell) scripts were used to process the Snort scan logs.

1. Combine the five scan files into one:

   ```
   for $file in `ls scans.*`
   do
   cat $file >> main.scans
   done
   ```

   This created an 88Mb Snort scan file.

2. To get total number of entries in scan files:

   ```
   $ grep -- '->' main.scans | wc –l
   ```

3. To obtain the top 10 unique source IP addresses that initiated scans:

   ```
   cat main.scans | grep -- '->' | awk '{print $4,$6}' | sed s/\:[0-9]*//g | awk '{print $1}' | sort | uniq –c | sort -r -n -k 1
   ```

4. To obtain the 10 top destination IP addresses that were scanned:

   ```
   cat main.scans | grep -- '->' | awk '{print $4,$6}' | sed s/\:[0-9]*//g | awk '{print $2}' | sort | uniq –c | sort -r -n -k 1
   ```

Appendix A – Reference Sites

http://www.sans.org/infosecFAQ/casestudies/univ_sec.htm - University Security, Douglas P. Brown, July 11, 2001
http://www.chebucto.ns.ca/~rakerman/port-table.html - Ports for Internet Services
http://www.wittys.com/files/all-ip-numbers.txt - All IP protocols and TCP/UDP ports (including. Trojans)
http://www.sys-security.com/html/papers/trojan_list.html - Trojan Port lists
http://www.robertgraham.com/pubs/firewall-seen.html - Port lists, trojans, and common seen occurrences.
http://www.simovits.com/nyheter9902.html - Another Trojan port list

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

Last Updated: May 28th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Boston SEC503	Boston, MA	Oct 09, 2017 - Oct 14, 2017	Community SANS
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced