GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

GIAC Practical – V2.9

Mark Maher

SANS Baltimore 2001

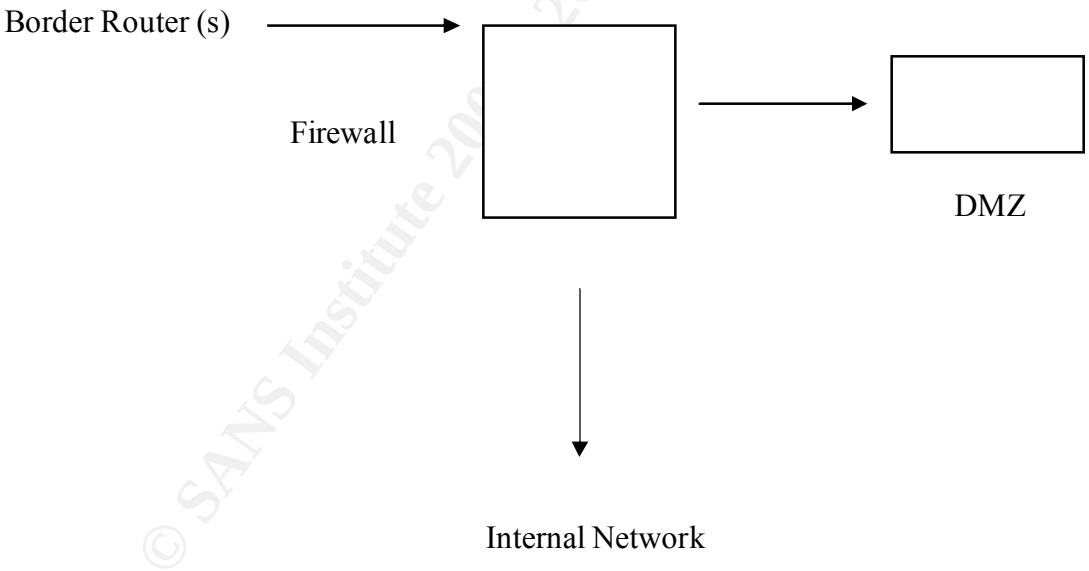
Assignment 1 – Network Detects

Detect # 1:

May 24 20:50:02 2001 FW s:attacker.net d:defender.net p:udp sp:23260 dp:111
May 24 20:50:02 2001 FW s:attacker.net d:defender.net p:udp sp:23260 dp:111
May 24 20:50:02 2001 FW s:attacker.net d:defender.net p:udp sp:23260 dp:111
May 24 20:50:02 2001 FW s:attacker.net d:defender.net p:udp sp:23260 dp:111
May 24 20:50:02 2001 FW s:attacker.net d:defender.net p:udp sp:23260 dp:111
May 24 20:50:02 2001 FW s:attacker.net d:defender.net p:tcp sp:23260 dp:111
May 24 20:50:02 2001 FW s:attacker.net d:defender.net p:tcp sp:23260 dp:111
May 24 20:50:02 2001 FW s:attacker.net d:defender.net p:tcp sp:23260 dp:111

1. Source of Trace:

My Company's network, specifically, a firewall configured as follows:



2. Detect was generated by:

Detect generated by an IBM SecureWay Firewall for AIX V4.1.

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

Description of SecureWay firewall logs:

May 24 20:50:02 2001 – Date, Time, and Year.
FW – The name of the firewall that logged this entry.
s:attacker.net – Source IP
d:defender.net – Destination IP
p:udp - Protocol
sp:23260 – Source Port
dp:111 – Destination Port

3. Probability the source address was spoofed:

Not likely or minimal. The person scanning, in this instance, is interested in the output from the portmapper request (tcp/udp 111). From the book Network Intrusion Detection, An Analyst's Handbook, 2nd edition, by Stephen Northcutt and Judy Novak: "Because the only purpose of the techniques (spoofing) is to write, it doesn't make sense to use the attacker's actual Internet address. The attacker is not establishing a connection; he is flooding a queue.." (p.110). Although UDP is connectionless (also note that TCP 111 was also scanned), which makes it vulnerable to spoofing, that does not appear the case in this scan.

Some helpful links that have provided explanations on spoofing for me are:

IP-spoofing Demystified (Trust-Relationship Exploitation) -by daemon9 / route / infinity for Phrack Magazine (http://www.networkcommand.com/docs/ipspoof.txt)

RFC2267 -This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point. (http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2267.html)

DoE: CIAC: Internet Address Spoofing and Hijacked Session Attacks- http://ciac.llnl.gov/ciac/bulletins/f-08.shtml

CERT: CA-95.01.IP.spoofing.attacks.and.hijacked.terminal.connections - http://www.cert.org/advisories/CA-1995-01.html

CERT: CA-96.21.tcp_syn_flooding - http://www.cert.org/advisories/CA-1996-21.html

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

Technical details of the attack described by Markoff in NYT- Tsutomu Shimomura describes how Kevin Mitnick used IP spoofing in order to break into his systems. (http://www.robertgraham.com/mirror/Shimomura-spoofing.html)

http://www.research.att.com/~smb/papers/ipext.pdf

http://www.nmrc.org/faqs/hackfaq/hackfaq-25.html#ss25.1

http://www.ryanspc.com/ipspoof.html

4. Description of attack:

It appears to be an intelligence gathering scan looking for Sun RPC's (TCP/UDP 111). This has the potential to be very serious, as noted in the SAN's Ten Most Critical Internet Security Threats (see http://www.sans.org/topten.htm), since these vulnerabilities, if exploited, can allow immediate root compromise. From the SANS Top Ten:

Systems Affected:
Multiple UNIX and Linux systems

CVE Entries:

rpc.ttdbserverd - CVE-1999-0687, CVE-1999-0003, CVE-1999-0693 (-0687 is newer than -0003, but both allow root from remote attackers and it's likely that -0003 is still around a LOT; -0693 is only locally exploitable, but does give root)

rpc.cmsd – CVE-1999-0696

rpc.statd - CVE-1999-0018, CVE-1999-0019.

Since Unix and Linux systems are used throughout the organization, some further investigation was done, namely running nmap and rcpinfo to determine if these services are running.

A quick nmap run against an IBM AIX V4.1 server revealed the following:

Interesting ports on defender.host.net (XXX.XXX.XXX.XXX):

Port	State	Protocol	Service
7	open	upd	echo
9	open	upd	discard

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

13	open	upd	daytime
19	open	upd	chargen
37	open	upd	time
111	open	upd	portmap/RPC
514	open	upd	syslog
872	open	upd	status (statd)
32769	open	upd	cmsd (Calendar Manager)
32771	open	upd	walld
32772	open	upd	sprayd
32773	open	upd	pcnfsd
32774	open	upd	mountd
32803	open	upd	nlockmgr

The Unix environment is 5 AIX and 4 Sun Solaris servers. Further investigation, using nmap on the other servers, revealed much the same as the above. As one can see, many of the active ports are vulnerable to the exploits rpc.ttdbserver (ToolTalk), rpc.cmsd (Calendar Manager), and rpc.statd as noted in the Top Ten documents. It can also be noted that the the nlock (CVE-2000-0508, securityfocus.com/bid/1372), pcnfsd (CVE-1999-0305/CAN-1999-0078, CA-1996-08), sprayd (CAN-1999-0613), and walld (CVE-1999-0181/CVE-2000-0428) services have noted vulnerabilities.

NOTE: CVE's are located at cve.mitre.org, and CA's relate to www.cert.org.

5. Attack mechanism:

The intent was to find open RPC services/ports behind our firewall, probably using the *rpcinfo* command. Example: *rpcinfo –p* would give the ports where these services reside.

6. Correlations:

As noted above, RPC scan are a favorite among the hacker community as reported in the SANS Top Ten document. It is also noted that that this attack can be correlated with exploits, as noted in the CVE, CA, and securityfocus entries.

Our firewall routinely gets RPC scans. The month of May (2001) alone had over 5 separate RPC scans. The source IP's were routinely checked against the GIAC Web site, as well as www.incidents.org.

7. Evidence of active targeting:

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

Most of the noted RPC scans show a general scan of an IP address range and not against a specific target (hosts, firewall, router, etc.). Thus, no discernable pattern can be established from the RPC scans, only a general range of IP's.

8. Severity:

Criticality:
Some of the IP's in the RPC scans are servers that are running DNS and other important applications. Thus, Criticality = 5.

Lethality:
Recon probes that are not at a specific target. Lethality = 2.

System Countermeasures:
Network: A firewall that has a restrictive policy: "Deny All." = 5
System: Host systems have vulnerable services running = 1
Total: 6

Calculation:
(Criticality + Lethality) – (Countermeasures) = Severity
(5 + 2) – 6 = 1

9. Defensive Recommendation:

A review of the firewall logs and alerts noted that the RPC scans were dropped at the firewall.

Further recommendations for host security:

- Periodically audit the Unix servers using nmap scanning, the *showmount* command, and the *rcpinfo* command.
- Remove (disable) the RPC services that are vulnerable.
- Run a secure portmapper and log using syslog.

10. Multiple Choice Question:

Which of the following are RPC Services:

a. IMAP, POP2, POP3, SMTP
b. NFS, rusers, ttdbserver, sadmind

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

c. Echo, chargen, daytime, discard
d. telnet, ftp, http, exec

Answer: b

Detect # 2:

May 22 16:33:17 2001 FW s:attacker.net d:defender.net p:tcp sp:4001 dp:109
May 22 16:33:17 2001 FW s:attacker.net d:defender.net p:tcp sp:4001 dp:109
May 22 16:33:17 2001 FW s:attacker.net d:defender.net p:tcp sp:4001 dp:109
May 22 16:35:22 2001 FW s:attacker.net d:defender.net p:tcp sp:4006 dp:110
May 22 16:35:22 2001 FW s:attacker.net d:defender.net p:tcp sp:110 dp:110
May 22 16:35:22 2001 FW s:attacker.net d:defender.net p:tcp sp:110 dp:110
May 22 17:03:35 2001 FW s:attacker.net d:defender.net p:tcp sp:23 dp:23
May 22 17:03:35 2001 FW s:attacker.net d:defender.net p:tcp sp:23 dp:110
May 22 17:03:35 2001 FW s:attacker.net d:defender.net p:tcp sp:23 dp:23

1. Source of Trace:

My Company's network, specifically, a firewall (see configuration above in Detect #1).

2. Detect was generated by:

Detect generated by an IBM SecureWay Firewall for AIX V4.1.

See the format of the firewall logs in Detect #1 above.

3. Probability the source address was spoofed:

Not likely or minimal. Since the attacker is doing reconnaissance (information gathering) and has not discovered a trusted port of an IP address, I believe these packets were not spoofed.

4. Description of attack:

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

It appears to be an intelligence gathering scan looking for the Post Office Protocol (POP), specifically, POP2 (109) and POP3 (110). Like the first detect (looking for RPC), this has the potential to be very serious, as noted in the SAN's Ten Most Critical Internet Security Threats (see http://www.sans.org/topten.htm), since these vulnerabilities, if exploited, can allow immediate root compromise. From the SANS Top Ten:

Systems Affected:
Multiple UNIX and Linux systems

CVE Entries:
CVE-1999-0005, CVE-1999-0006, CVE-1999-0042, CVE-1999-0920, CVE-2000-0091

Advice on correcting the problem:
A. Disable these services on machines that are not e-mail servers.

B. Use the latest patches and versions. Additional information may be found at:

http://www.cert.org/advisories/CA-98.09.imapd.html
http://www.cert.org/advisories/CA-98.08.qpopper_vul.html
http://www.cert.org/advisories/CA-97.09.imap_pop.html

Since the source and destination ports are the same on some of the packets, it can be assumed that these packets were "crafted", probably with nmap.

5. Attack mechanism:

The intent was to determine if POP2 and POP3 are vulnerable through reconnaissance to these ports. However, there are some troubling aspect of these scans. First, the source port in the scans for POP3 are the same as the destination port (110). Thus, it would appear that these packets were "crafted." Also, the attacker tried to telnet to the POP3 port (110), presumably, to glean critical information.

While the firewall logs noted that these request were denied, the security team tried to telnet to the IP that the attacker tried to see if we could "banner grab" information. The request was denied. TCPdump was running on the other side of the firewall and also verified that our packets did not make it through the firewall (phew!).

6. Correlations:

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

As noted above, POP scans are a favorite among the hacker community as reported in the SANS Top Ten document. It is also noted that that this attack can be correlated with exploits, as noted in the CVE, CA, CIAC and securityfocus entries.

Like the RPC scans mentioned above, our firewall gets routinely scanned for POP. The source IP's were routinely checked against the GIAC Web site, as well as www.incidents.org. However, unlike above, in this particular instance, the IP was listed on the www.incidents.org site. The logs are checked routinely, and fortunately, the attackers have not come back.

7. Evidence of active targeting:

I believe there is evidence of active targeting, since the attacker tried to telnet to port 110.

8. Severity:

Criticality:
Some of the IP's in the POP scans are servers that are running DNS and other important applications. Thus, Criticality = 5.

Lethality:
Recon probes, but active targeting, that is, telnetting to port 110. Lethality = 4.

System Countermeasures:
Network: A firewall that has a restrictive policy: "Deny All." = 5
System: Host systems have vulnerable services running = 1
Total: 6

Calculation:
(Criticality + Lethality) – (Countermeasures) = Severity
(5 + 4) – 6 = 3

9. Defensive Recommendation:

As noted above, using the latest patches and version. Some of the experts also recommend controlling access to these services using TCP wrappers and encrypted

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

channels such as SSH and SSL to protect passwords (taken from SANS Top Ten document).

10. Multiple Choice Question:

What other popular remote access mail protocol is mentioned with POP in the SANS Top Ten list (#9 on the list):

a. SNMP
b. IMAP
c. SMTP
d. Sendmail

Answer: b

Detect # 3:

Jun 21 2001 01:03:14: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.1/161
Jun 21 2001 01:03:15: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.1/161
Jun 21 2001 01:03:16: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.2/161
Jun 21 2001 01:03:18: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.2/161
Jun 21 2001 01:03:19: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.3/161
Jun 21 2001 01:03:20: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.3/161
Jun 21 2001 01:03:22: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.4/161
Jun 21 2001 01:03:23: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.4/161
Jun 21 2001 01:03:25: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.5/161
Jun 21 2001 01:03:26: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.6/161
-
-
-
Jun 21 2001 01:23:34: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.250/161
Jun 21 2001 01:23:35: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.250/161
Jun 21 2001 01:23:36: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.251/161
Jun 21 2001 01:23:38: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.251/161
Jun 21 2001 01:23:39: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.252/161
Jun 21 2001 01:23:41: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.252/161

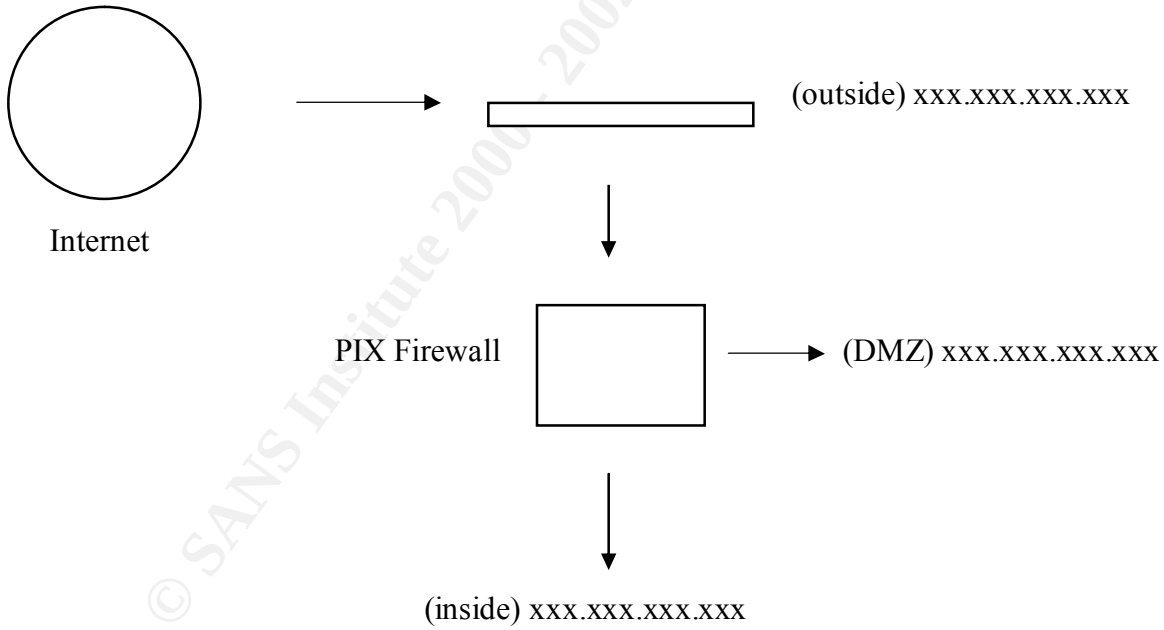
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Jun 21 2001 01:23:42: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.253/161
Jun 21 2001 01:23:43: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.253/161
Jun 21 2001 01:23:44: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.254/161
Jun 21 2001 01:23:48: %PIX-2-106006: Deny inbound UDP from attacker.net/3043 to defender.net.254/161

1. Source of Trace:

My Company's network, specifically, a PIX firewall. Note: the first two detects were a different firewall (IBM SecureWay) at a different location. This is another network operated by the company that employs me, and uses a different firewall.

The configuration is as follows:



2. Detect was generated by:

Detect generated by a Cisco PIX Firewall Model 515 running PIX firewall software version 5.02.

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

Explanation of the firewall log format (from the Cisco documentation):

`%PIX-2-106006: Deny inbound UDP from` *`faddr/fport`* `to` *`laddr/lport`* `on interface` *`int_name`*`.`

> **Explanation** This is a connection-related message. This message is logged if an inbound UDP packet is denied by your security policy.

The detect has been "scrubbed" to make it a little easier to read (the interface name has been eliminated).

3. Probability the source address was spoofed:

Not likely or minimal. Since the attacker is doing reconnaissance (information gathering for SNMP) and network mapping, and has not discovered a trusted port of an IP address, I believe these packets were not spoofed. The IP address of the attacker.net belongs to a range registered to the Asia Pacific Network Information Center.

4. Description of attack:

It appears to be an intelligence gathering and mapping scans looking for the Simple Network Management Protocol (SNMP). However, note that our entire Class "C" was scanned in about 20 minutes.

This is also a SANS Top Ten, thus there are CVE's:

Systems Affected:

All system and network devices.

CVE Entries:

default or blank SNMP community name (public) - CAN-1999-0517
guessable SNMP community name - CAN-1999-0516
hidden SNMP community strings - CAN-1999-0254, CAN-1999-0186

Many devices, such as routers, hubs, and printers have SNMP agents. From the SANS Top Ten: "The Simple Network Management Protocol (SNMP) is widely used by network administrators to monitor and administer all types of network-connected devices ranging from routers to printers to computers. SNMP uses an unencrypted "community string" as its only authentication mechanism. Lack of encryption is bad enough, but the default community string used by the vast majority of SNMP devices is "public", with a few "clever" network equipment vendors changing the string to "private". Attackers can

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

use this vulnerability in SNMP to reconfigure or shut down devices remotely. Sniffed SNMP traffic can reveal a great deal about the structure of your network, as well as the systems and devices attached to it. Intruders use such information to pick targets and plan attacks."

The excellent book (anything for a passing grade!) Network Intrusion Detection, 2nd edition, by Stephen Northcutt and Judy Novak, p.264, recommends: "The choice of private, internal, or the name of the organization for SNMP community strings are not advised. Pick something hard to guess."

SNMP is also discussed extensively in Hacking Exposed: Network Security Secrets and Solutions, 2nd edition by Joel Scambray, Stuart McClure, and George Kurtz (Osborne/McGraw-Hill): "SNMP is a protocol designed to help administrators manage their network devices simply. But the problem has always been that SNMPv1 (RFC 1157 – http://www.rfc-editor.org) is inherently insecure. The original version has only a single security mechanism: passwords, otherwise known as community names. In response, a greatly enhanced version quick came out (SNMPv2), as described in RFC 1146. SNMPv2 uses a hashing algorithm called message digest v5 (MD5) to authenticate transmissions between SNMP servers and agents. MD5 verifies the integrity of the communications and their origination. Also, SNMPv2 can encrypt your SNMP transmissions as well. Attackers sniffing your network connection would be blinded to the community names being used and therefore limited in their chaos-creating capabilities. But the encryption features in SNMPv2 did not restrict network administrators from choosing simple passwords for their routers.

SNMPv3, the current standard, goes a long way in helping to secure your devices, but its adoption will be slow. None of the SNMP versions, however, limits the fact that SNMP community names are being shipped from the vendor and set up by administrators with easily guessed passwords.

What's worse is that in many organizations, *SNMP is all but forgotten about during security reviews*. Perhaps it's because SNMP runs over UDP, or maybe few administrators know about its function. Either way, SNMP can be (and usually is) missed in security reviews, *leaving gaping holes for attack*." (pgs. 429 – 430)

5. Attack mechanism:

The scan was automated, probably using either IP Browser (http://www.solarwinds.net) or the *snmputil* utility from the NT Resource Kit.

6. Correlations:

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

As noted above, SNMP scans are a favorite among the hacker community as reported in the SANS Top Ten document. It is also noted that that this attack can be correlated with exploits, as noted in the CVE, CA, and securityfocus entries.

A Whois trace revealed that the IP address range of the attacker.net belongs to a range registered to the Asia Pacific Network Information Center. The GIAC and www.incidents.org web sites were also reviewed for further information about this IP range. We have since detected no further activity from this site.

7. Evidence of active targeting:

I believe there is evidence of active targeting, since the attacker scanned our entire Class "C" network.

8. Severity:

Criticality:
Some of the IP's in the SNMP scans are servers, routers, and hubs. Thus, Criticality = 5.

Lethality:
Recon probes, but active targeting, that is, scanning our entire Class "C". Lethality = 3.

System Countermeasures:
Network: A firewall that has a restrictive policy: "Deny All." = 5
System: Host systems as well as routers and hubs have vulnerable community strings (see #9 below) = 1
Total: 6

Calculation:
(Criticality + Lethality) – (Countermeasures) = Severity
(5 + 3) – 6 = 2

9. Defensive Recommendation:

Fortunately, the PIX firewall denied these scans and dropped them silently at the firewall.

Right after this scan, I ran IP Browser, which is an excellent graphical browser for enumerating SNMP information. It was noted that many of the network devices,

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

especially routers, as well as many of the Unix and NT servers, had community names of either public or private. I was thus able to extract a list of users (user names), ports and services running, shares, etc.

Axent NetRecon (a vulnerability scanning tool) noted that "read" access to the Management Information Base (MIB) was also possible on a few of the Unix servers.

To further enhance SNMP security (besides blocking UDP port 161 at the firewall), we changed the easily guessed passwords. For the Cisco routers, to change the community names to a difficult password:

snmp-server community <difficult password> RO

We also applied the following on our border routers, as suggested by Cisco:

access-list 101 deny udp any any eq 161 log ! Block SNMP traffic

10. Multiple Choice Question:

What version of SNMP uses a hashing algorith (MD5) and can also encrypt your SNMP transmission:

1. SNMP
2. SNMPv1
3. SNMPv3
4. SNMPv2

Answer: 4

Detect # 4:

May 5 06:20:12 2001 FW s:attacker.net d:defender.net p:tcp sp:29880 dp:80
May 5 06:20:12 2001 FW s:attacker.net d:defender.net p:tcp sp:29880 dp:80
May 5 06:20:12 2001 FW s:attacker.net d:defender.net p:tcp sp:29880 dp:80
May 5 06:20:12 2001 FW s:attacker.net d:defender.net p:tcp sp:29880 dp:80
May 5 06:20:12 2001 FW s:attacker.net d:defender.net p:tcp sp:29880 dp:80
May 5 06:20:12 2001 FW s:attacker.net d:defender.net p:tcp sp:29880 dp:80
May 5 06:20:12 2001 FW s:attacker.net d:defender.net p:tcp sp:29880 dp:80
May 5 06:20:12 2001 FW s:attacker.net d:defender.net p:tcp sp:29880 dp:80
May 5 06:20:12 2001 FW s:attacker.net d:defender.net p:tcp sp:29880 dp:80

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

-
-
-
May 5 06:24:30 2001 FW s:attacker.net d:defender.net p:tcp sp:137 dp:137
May 5 06:24:30 2001 FW s:attacker.net d:defender.net p:tcp sp:137 dp:137
May 5 06:24:30 2001 FW s:attacker.net d:defender.net p:tcp sp:137 dp:137
May 5 06:24:30 2001 FW s:attacker.net d:defender.net p:tcp sp:137 dp:137
May 5 06:24:30 2001 FW s:attacker.net d:defender.net p:tcp sp:137 dp:137

1. Source of Trace:

My Company's network, specifically, a firewall configured as shown in Detect # 1 above.

2. Detect was generated by:

Detect generated by an IBM SecureWay Firewall for AIX V4.1.

See the format of the firewall logs in Detect #1 above.

3. Probability the source address was spoofed:

Not likely. I do not believe that the source address was spoofed since the attacker is trying to do a scan for HTTP servers and other Windows information (port 137), with the hope of getting information back and possibly then trying to connect to these services (if open).

4. Description of attack:

It appears to be a network scan for HTTP servers and Windows NetBIOS information. The scan is very quick and many machines were scanned. The packets are probably crafted since the source ports are the same throughout the quick scans.

A Whois search revealed that the address space is registerd with Bellsouth.net INC (ISP). We have not detected any activity from this address space since this incident. The packets were dropped silently at the SecureWay firewall.

5. Attack mechanism:

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

The scan was automated, probably using either nmap or hping. With the identical source and destination ports for the port 137 scan, we can assume that this traffic has been "crafted." See "An ACK Scan" on page 32 of Network Intrusion Detection, which mentions this fact.

6. Correlations:

Attempts to connect to HTTP is often found in our firewall logs. There are also scans for SOCKS servers. With the vulnerabilities of Microsoft IIS, automated scripting (phfscan.c, cgiscan.c), automated applications (Grinder by Rhino9, SiteScan by Rhino9), input validation attacks, and buffer overflows, "web hacking" is a popular pastime.

7. Evidence of active targeting:

I believe there is no evidence of active targeting, since the attacker scanned a general range of addresses.

8. Severity:

Criticality:
Some of the IP's scanned do have HTTP running and are internal web servers. Some are in the process of being used for e-commerce platforms. Thus, Criticality = 5.

Lethality:
Recon probes against vulnerable services. Lethality = 4.

System Countermeasures:
Network: A firewall that has a restrictive policy: "Deny All." = 5
System: Host systems, NT (IIS) and Unix that have vulnerabilities = 1
Total: 6

Calculation:
(Criticality + Lethality) – (Countermeasures) = Severity
(5 + 4) – 6 = 3

9. Defensive Recommendation:

All HTTP request are proxied. The security team is in the process of strengthening web security on the various Windows NT machines running IIS.

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

10. Multiple Choice Question:

Most web attacks run over what ports – and why is this important:

1. 21, 25, and 53, and these ports are usually allowed into your internal network segment.
2. 7, 9, and 37, and these ports are usually allowed into your internal network segment.
3. 80, 443, and 8080 and these ports are usually allowed into your internal network segment.
4. 80, 81, and 4040, and these ports are usually allowed into your internal network segment.

Answer: 3

Detect # 5:

May 1 03:20:12 2001 FW s:attacker.net d:defender.net p:tcp sp:115 dp:1000
May 1 03:25:33 2001 FW s:attacker.net d:defender.net p:tcp sp:115 dp:9000
May 1 04:01:02 2001 FW s:attacker.net d:defender.net p:tcp sp:115 dp:1004
May 1 04:20:09 2001 FW s:attacker.net d:defender.net p:tcp sp:115 dp:1000
May 1 04:32:18 2001 FW s:attacker.net d:defender.net p:tcp sp:115 dp:2040
May 1 05:03:26 2001 FW s:attacker.net d:defender.net p:tcp sp:115 dp:2039
May 1 05:03:58 2001 FW s:attacker.net d:defender.net p:tcp sp:115 dp:2213
May 1 05:04:10 2001 FW s:attacker.net d:defender.net p:tcp sp:115 dp:2441
May 1 05:05:04 2001 FW s:attacker.net d:defender.net p:tcp sp:115 dp:2652

1. Source of Trace:

My Company's network, specifically, a firewall configured as shown in Detect # 1 above.

2. Detect was generated by:

Detect generated by an IBM SecureWay Firewall for AIX V4.1.

See the format of the firewall logs in Detect #1 above.

3. Probability the source address was spoofed:

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

Not likely. It appears to be a slow, stealthy host discovery using TCP.

4. Description of attack:

It appears to be a network host discovery, although before SANS Baltimore I was not sure of this type of traffic. From page 79 of Network Intrusion Detection: "the hacker might try to launch the scan using methods that may go undetected, known as stealth scans. These scans are considered more furtive because they use unconventional techniques that intrusion-detection systems are not likely to pick up. Some of these scanning techniques attempt to fingerprint the operating system. Many times a given exploit might plague a subset of operating systems. For the hacker to have a better chance of success for the exploit to work, reconnaissance must be done to find hosts running a particular operating system."

Something I learned at SANS Baltimore was very helpful in helping me understand this type of traffic. A network scan is usually recognized by SYN packets sent to the same service port on many different target machines. The target machines are queried in a systematic, orderly fashion and the probes are sent very rapidly. If a target host responds to the probe with a RESET, then the attacker knows that the target is not offering the desired service. On the other hand, if the target machine responds to the SYN with a SYN-ACK, then the attacker knows that the target host is indeed listening on the target port. This is referred to as a stealthy host discovery using TCP, and are usually slower probes. TCPDump was not used to glean this necessary information. Also, the crafting software, such as nmap, produces an impossible flag combination of SYN and FIN flags set simultaneously, which can elude IDS's and routers. (I hope my understanding is correct!).

A Whois search revealed that the address space is registered with Bellsouth.net INC (ISP). We have not detected any activity from this address space since this incident. The packets were dropped silently at the SecureWay firewall.

Since SANS Baltimore, TCP dump has been running in front of the SecureWay firewall to try to verify certain activity that is getting to our firewall. This activity has not been seen since this early May episode.

5. Attack mechanism:

The scan was automated, probably using nmap.

6. Correlations:

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

Per SANS Baltimore, this is referred to as a stealthy host discovery using TCP, probably with SYN-ACK packets. From page 278 of Network Intrusion Detection: "Recon probes should be taken seriously; if attackers can learn where your hosts are, they can make fairly short work of determining what services these hosts run. If they can't determine which of the hosts in your network address space are active, they have a very sparse matrix with which to work."

7. Evidence of active targeting:

I believe there is no evidence of active targeting, since the attacker scanned a general range of addresses.

8. Severity:

Criticality:
Some of the IP's scanned are servers with critical applications. As mentioned above, if attackers can learn where your hosts are, it fairly routine to determine the operating systems and services these hosts are running. Thus, Criticality = 5.

Lethality:
Host discovery using TCP. Lethality = 4.

System Countermeasures:
Network: A firewall that has a restrictive policy: "Deny All." = 5
System: Host systems "tucked" safely (?) behind the firewall = 2
Total:

Calculation:
(Criticality + Lethality) – (Countermeasures) = Severity
(5 + 4) – 7 = 2

9. Defensive Recommendation:

Firewall dropped these packets.

Consider an IDS (NIDS) to recognize these signatures.

10. Multiple Choice Question:

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

What combination of TCP flags results in a stealthy host discovery and often eludes IDS's:

1. SYN-ACK
2. SYN-FIN
3. SYN-SYN
4. RESET

Answer: 1

Summary of Detects:

The source of all the traces were my company's network and were generated by firewalls, either an IBM SecureWay or a PIX. Prior to SANS Baltimore, logs were not routinely reviewed by personnel. Since then, I have been reviewing the firewall logs. One of the great things of this assignment (besides learning a lot!) is that it has helped me "sell" security to management, because, as these scans show, there are some unusual activity. Management had been slow to react to most suggestions on strengthening hosts security. Most of these scans are on the SANS Top Ten Internet Threats list. The course mentioned the importance of intrusion detection as not a specific tool, but a capability, a blending of tools and techniques. The course also went on to mention that the most important IDS (usually) is the firewall, and as such, the logs must be reviewed.

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

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

Mark Maher

SANS Baltimore 2001

Assignment 2
Describe the State of Intrusion Detection

THE BUSINESS CASE FOR INTRUSION DETECTION

This paper will concentrate on the question "Is there a Business Case for Intrusion Detection?" as well as the overall state of intrusion detection as it relates to the business case. In my company's case, the answer to the question "Is there a Business Care for Intrusion Detection?" is unequivocally "YES!" and the reason is a governmental act known as the Health Insurance Portability and Accountability Act (HIPAA). Briefly, The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), also known as HIPAA, was enacted as part of a broad Congressional attempt at incremental healthcare reform. The "Administrative Simplification" aspect of that law requires the United States Department of Health and Human Services (DHHS) to develop standards and requirements for maintenance and transmission of health information that identifies individual patients.

These standards are designed to:

- Improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for specified administrative and financial transactions; and

- Protect the security and confidentiality of electronic health information.

The requirements outlined by the law and the regulations promulgated by DHHS are far-reaching--*all healthcare organizations that maintain or transmit electronic health information must comply*. This includes health plans, healthcare clearinghouses, and healthcare providers, from large integrated delivery networks to individual physician offices. The law provides for significant financial penalties for violations. Since I work for a hospital, as well as a health plan, the act applies to us.

A team has been assembled to help comply with HIPAA. The team consists of technical as well as business personnel. As I learned at SANS Baltimore, intrusion detection is more than a single-product, as is also more than a technical solution. HIPAA further

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

strengthens this, because the security of patient data also includes financial data, and therefore, goes beyond just the "bits and bytes."

Thus, this paper will discuss the aspects of understanding intrusion detection technology. The paper will also discuss the research that is going on in the field of intrusion detection.

CONCERNS

There is an unmistakable lack of adequate security over access to and the use of information, the computers, and the telecommunication network in which the hospital and health plan organizations (the one that employs me) depend. The term used in HIPAA is Information Assurance, and is the term used to identify the initiatives that are being offered to address this lack. HIPAA goes on to note that Information Assurance combines the protection of information with the need to secure the underlying technologies that support the processing, storage, and delivery of that information. In effect, Information Assurance is concerned with protecting and maintaining the value of information so that it can be trusted for use and with ensuring the availability to legitimate users and customers when it is needed to perform an authorized business activity (remember the integrity, confidentiality, and availability triad of computer security?).

Availability is a big issue with the advent of e-business and e-commerce. For example, denial-of-service attacks, are now being viewed as the greatest single threat to the highly automated and interconnected way of conducting business. Entire systems and networks are being shut down by these assaults for hours and even days. Several different surveys have indicated that the result of these incidents has been the loss of billions of dollars in revenue. The average loss has been identified as over $250,000 per responding organization. Other surveys have indicated that while the internal breaches of IT security continue to be of increasing concern, the external attacks were increasing at what was described as "an alarming rate." The responding organizations indicated that they had experienced an increase in penetration attacks of from 12 percent in 1998 to 23 percent in 1999. This increase in the growth of incidents reflects the growth of the Internet, and the planned increase in e-commerce can only intensify this upward trend. [1]

The sophistication of the attacks is also increasing. And they are becoming more stealthy. According to Alan Paller, the Director of Research for the SANS Institute: "There is a steadily increasing number of these attacks. And there are more of these that have three characteristics that set them apart. The first of these is that attacks are coming simultaneously from multiple, coordinated sites. The second is that the attacks are coming with more stealth, escaping the detection of intrusion monitoring systems by

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

limiting the number of "pings," or connections. These are coming in just under the detection threshold, at one every hour, or every three days. Third, they are coming from patient people, who are usually more professional than are children. Additionally, there is evidence that computer hackers are banding together across the globe to mount low-visibility attack in an effort to sneak under the radar of existing IDS's and other IT security controls." [2]

REQUIREMENTS

Like most organizations connected to the Internet, we employ a firewall security product to hinder attackers who are seeking to break into our network. The problem, and something that we must improve (because of HIPAA), is that if someone breached our firewall, it would be nearly impossible to determine what has occurred, and which systems were compromised. As Marcus Ranum, of Network Flight Recorder, says "once entry has been gained through the firewall, an attacker's traces vanish into thin air as systems logs are erased and the intruder exploits the break-in throughout the network." [3]

Since our firewall is basically a prevention device, we lack a detection, as well as a tracking and recording mechanism. Although our firewall has a recording mechanism, the logs are limited in what they record. Thus, our strategy for increasing security will have to satisfy the requirements of prevention, detection, and tracking and recording. Again, it is with the attempt to prevent incidents, and we are no exception, from occurring that most of the current generation of security technology is employed. Technologies such as vulnerability assessments, firewalls, passwords and access controls, encryption and the Public Key Infrastructure (PKI), biometrics, etc., are all useful in attempting to prevent security incidents from occurring.

CHARACTERISTICS OF A GOOD IDS

An intrusion detection system should address the following issues, regardless of what mechanism it is based on (taken from the COAST Intrusion Detection pages - http://www.cerias.purdue.edu/coast/intrusion-detection/welcome.html):

1. It must run continually without human supervision. The system must be reliable enough to allow it to run in the background of the system being observed. However, it should not be a "black box". That is, its internal workings should be examinable from outside.

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

2. It must be fault tolerant in the sense that it must survive a system crash and not have its knowledge-base rebuilt at restart.

3. On a similar note to above, it must resist subversion. The system can monitor itself to ensure that it has not been subverted.

4. It must impose minimal overhead on the system. A system that slows a computer to a crawl will simply not be used.

5. It must observe deviations from normal behavior.

6. It must be easily tailored to the system in question. Every system has a different usage pattern, and the defense mechanism should adapt easily to these patterns.

7. It must cope with changing system behavior over time as new applications are being added. The system profile will change over time, and the IDS must be able to adapt.

8. Finally, it must be difficult to fool.

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

The last point raises an issue about the type of errors likely to occur in the system. These can be neatly categorized as either false positive, false negative, or subversion errors. A false positive occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action. A false negative occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior. A subversion error occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.

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

False positive errors will lead users of the intrusion detection system to ignore its output, as it will classify legitimate actions as intrusions. The occurrences of this type of error should be minimized (it may not be possible to completely eliminate them) so as to provide useful information to the operators. If too many false positives are generated, the operators will come to ignore the output of the system over time, which may lead to an actual intrusion being detected but ignored by the users.

A false negative error occurs when an action proceeds even though it is an intrusion. False negative errors are more serious than false positive errors because they give a misleading sense of security. By allowing all actions to proceed, a suspicious action will not be brought to the attention of the operator. The intrusion detection system is now a liability as the security of the system is less than it was before the intrusion detector was installed.

Subversion errors are more complex and tie in with false negative errors. An intruder could use knowledge about the internals of an intrusion detection system to alter its operation, possibly allowing anomalous behavior to proceed. The intruder could then violate the system's operational security constraints. This may be discovered by a human operator examining the logs from the intrusion detector, but it would appear that the intrusion detection system still seems to be working correctly.

Another form of subversion error is fooling the system over time. As the detection system is observing behavior on the system over time, it may be possible to carry out operations each of which when taken individually pose no threat, but taken as an aggregate form a threat to system integrity. How would this happen? As mentioned previously, the detection system is continually updating its notion of normal system usage. As time goes by a change in system usage patterns is expected, and the detection system must cope with this. But if an intruder could perform actions over time which were just slightly outside of normal system usage, then it is possible that the actions could be accepted as legitimate where as they really form part of an intrusion attempt. The detection system would have come to accept each of the individual actions as slightly suspicious, but not a threat to the system. What it would not realize is that the combination of these actions would form a serious threat to the system.

CLASSIFICATION OF INTRUSION DETECTION SYSTEMS

Intrusions can be divided into 6 main types [4]

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

1. Attempted break-ins, which are detected by atypical behavior profiles or violations of security constraints.
2. Masquerade attacks, which are detected by atypical behavior profiles or violations of security constraints.
3. Penetration of the security control system, which are detected by monitoring for specific patterns of activity.
4. Leakage, which is detected by atypical use of system resources.
5. Denial of service, which is detected by atypical use of system resources.
6. Malicious use, which is detected by atypical behavior profiles, violations of security constraints, or use of special privileges.

However, we can divide the techniques of intrusion detection into two main types.

Anomaly Detection: Anomaly detection techniques assume that all intrusive activities are necessarily anomalous. This means that if we could establish a "normal activity profile" for a system, we could, in theory, flag all system states varying from the established profile by statistically significant amounts as intrusion attempts. However, if we consider that the set of intrusive activities only intersects the set of anomalous activities instead of being exactly the same, we find a couple of interesting possibilities: (1) Anomalous activities that are not intrusive are flagged as intrusive. (2) Intrusive activities that are not anomalous result in false negatives (events are not flagged intrusive, though they actually are). This is a dangerous problem, and is far more serious than the problem of false positives.

The main issues in anomaly detection systems thus become the selection of threshold levels so that neither of the above 2 problems is unreasonably magnified, and the selection of features to monitor. Anomaly detection systems are also computationally expensive because of the overhead of keeping track of, and possibly updating several system profile metrics. A block diagram of a typical anomaly detection system is shown at the following location:

http://www.acm.org/crossroads/xrds2-4/gfx/ifig1.gif

Misuse Detection: The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. This means that these systems are not unlike virus detection systems -- they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complement of "bad" behavior. Misuse detection

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

systems try to recognize known "bad" behavior. The main issues in misuse detection systems are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity. Several methods of misuse detection, including a new pattern matching model are discussed later. A block diagram of a typical misuse detection system is shown at the following location:

http://www.acm.org/crossroads/xrds2-4/gfx/ifig2.gif

THE STATE OF INTRUSION DETECTION SYSTEMS

What is the present state of IDS? This part of my paper is taken from the January 2000 Technical Report from the Carnegie Mellon University Software Engineering Institute. Its' report is entitled "State of the Practice of Intrusion Detection Technologies", and was sponsored jointly by the U.S. Air Force Computer Resources Support Improvement Program.

The body of that report defines an intrusion detection system as "a combination of hardware and software that monitors and collects system and network information and analyzes it to determine if an attack or an intrusion has occurred. Some IDS can automatically respond to an intrusion."

The report's Management Summary includes these useful observations: "Vendors make many claims for their IDS products in the commercial marketplace so separating hype from reality can be a major challenge. We are concerned that organizations are counting on these tools to solve a class of problems before they fully understand them. As a result, the solutions are likely to be inadequate or incorrect. Implementing intrusion detection systems on networks and hosts requires a broad understanding of computer security. The complexity of information technology infrastructures is increasing beyond any one person's ability to understand them, let alone administer them in a way that is operationally secure. Over-reliance on IDS technologies can create a false sense of confidence about the degree to which tools are detecting intrusions against an organization's critical assets. Evaluating IDS is non-trivial and there is a lack of credible, comprehensive product evaluation information. Hiring and retaining personnel to competently administer security in general and intrusion detection in particular are increasing challenges."

Although the Carnegie Mellon report is cautious in its tone, it concludes that IDS products are seen by users of computer and networked systems a s a viable tool to be included in their IT security arsenal. The Report observes that: "After reviewing the surveys cited in this Report, one could conclude that IDS technologies are becoming an

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

accepted part of many organization's information security tool suite. Thus, although IDS mechanisms are immature in their current state, it appears that an increasing number of IT executives see some innate benefit in their deployment and are including such mechanisms in their overall IT security strategy. Because of this interest, IDS products will continue to improve and their use can be expected to become commonplace in the years ahead."

SUMMARY AND CONCLUSION

Attacks against contemporary IT systems are occurring within the context of Internet time. Therefore, security prevention, detection, and response actions should strive to operate within a framework of Internet time.

When an IDS is designed, configured, and staffed properly, it forms a frontline defense against breaches of security because it operates within the framework of Internet time and provides the rapid response required by today's networked computing environments.

Successful IDS capabilities require the combination of sophisticated sensing and auditing tools and personnel experienced in the analysis of the outputs of those tools. Using such tool outputs and making preventive recommendations requires an even higher level of experience.

Intrusion Detection is still a fledgling field. However, it is beginning to assume enormous importance in today's computing environment. The combination of facts such as the unbridled growth of the Internet, the vast financial possibilities opening up in e-commerce, and the lack of truly secure systems make it an important and pertinent field of research. Future research trends seem to be converging towards a model that is a hybrid of the anomaly and misuse detection models; it is slowly acknowledged that neither of the models can detect all intrusion attempts on their own. This approach has been successfully adopted in NIDES (Next-Generation Intrusion Detection Expert System – see: http://www.sdl.sri.com/projects/nides/), and we can expect more such attempts in the future. Some schools doing research in this field include The COAST group at Purdue University, The University of California-Davis, and The University of California-Santa Barbara. The interested reader is encouraged to browse the provided links for more information.

So what is the decision of the HIPAA team? We now know the state of intrusion detection. We know we need a way of detecting internal and external threats to our medical records. The health plan part of the business relies heavily on the Internet. There is definitely a business case for intrusion detection. Preliminary assessments by our auditors, both internal and external, of the risks involved and how to reduce these risks,

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

have discussed the importance of intrusion detection and incidence response. Management is now willing to listen and spend money on computer security (thanks HIPAA!).

What's going to be the solution? We don't know that yet. We know the organization needs this technology in some form(s). We do know that intrusion detection is not a single, specific tool. To use a quote "intrusion detection is best thought of as a capability, not a single tool." [5] We need to further explore technical solutions, such as network-based and host-based tools, vulnerability scanners, and honeypots. We even discussed outsourcing the function of intrusion detection and response. Stay tuned!

BIBLIOGRAPHY

[1] Understanding Network Security Monitoring, Timothy Braithwaite. The EDP Audit, Control, and Security Newsletter, February 2001.

[2] Intrusion Detection Maintains An Unblinking Eye on Security, Marcus Ranum. The EDP Audit, Control, and Security Newsletter, May 2000.

[3] Ibid.

[4] Steven E Smaha. Haystack: An Intrusion Detection System. In Fourth Aerospace Computer Security Applications Conference, pages 37-44, Tracor Applied Science Inc., Austin, Texas, December 1998.

[5] Network Intrusion Detection: An Analyst's Handbook, 2nd edition. Stephen Northcutt and Judy Novak. New Riders Publishing, September 2000.

LINKS

COAST:
http://www.cerias.purdue.edu/coast/

UCSD:
http://seclab.cs.ucdavis.edu/Security.html

UCSB:
http://www.cs.ucsb.edu/Research/

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

State of the Practice of Intrusion Detection Technologies Report:
http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html

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

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

GIAC Practical – V2.9

Mark Maher

SANS Baltimore 2001

Assignment 3 - Analyze This

FILES ANALYZED

Alerts:

- Alert-01-Apr
- Alert-02-Apr
- Alert-03-Apr
- Alert-26-Mar
- Alert-27-Mar

Scans:

- SnortScan-01-Apr
- SnortScan-02-Apr
- SnortScan-03-Apr
- SnortScan-26-Mar
- SnortScan-27-Mar

OOS (Out of Specs):

- oos_Apr.2.2001
- oos_Apr.3.2001
- oos_Apr.4.2001
- oos_Apr.5.2001
- oos_Apr.6.2001

MANAGEMENT SUMMARY

Scope of the Analysis

In July of 2001, the Department of Security Administration performed a review of Snort alerts, Snort scans and Snort out-of-spec data. Five (5) days of each were reviewed.

The tool used to perform the bulk of the analysis was SnortSnarf by Silicon Defense.

Principal Observations

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

The following charts are taken from the SnortSnarf analysis. The first chart is for the Snort alerts, and the following five (5) charts are for the Snort scans. The information is in summary format. The alert summary:

22617 alerts found using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest alert at **00:02:37**.218486 *on 03/25/2001*
Latest alert at **23:48:12**.158179 *on 04/02/2001*

Signature (click for sig info)	# Alerts	# Sources	# Destinations	Detail link
ICMP SRC and DST outside network	6	3	3	Summary
Port 55850 tcp - Possible myserver activity - ref. 010313-1	7	5	5	Summary
SUNRPC highport access!	10	1	1	Summary
Tiny Fragments - Possible Hostile Activity	20	2	13	Summary
NMAP TCP ping!	21	8	12	Summary
Null scan!	22	16	13	Summary
Russia Dynamo - SANS Flash 28-jul-00	45	3	2	Summary
TCP SRC and DST outside network	57	20	31	Summary
Watchlist 000222 NET-NCFC	69	7	7	Summary
WinGate 1080 Attempt	79	35	44	Summary
Back Orifice	109	1	109	Summary
Queso fingerprint	116	6	13	Summary
connect to 515 from outside	119	6	109	Summary
SMB Name Wildcard	154	74	53	Summary
Possible RAMEN server activity	175	66	67	Summary

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

External RPC call	382	7	305	Summary
UDP SRC and DST outside network	571	41	259	Summary
SYN-FIN scan!	1924	1	1487	Summary
Watchlist 000220 IL-ISDNNET-990517	7898	21	20	Summary
Attempted Sun RPC high port access	10833	4	4	Summary

The Snort scans:

Scan File #1

SnortSnarf v052301.1

45738 alerts found using input module SnortFileInput, with sources:

- /root/perl/SnortScan-01-Apr

Earliest alert at **00:00:16** *on 3/31/2001*
Latest alert at **23:58:36** *on 3/31/2001*

Signature (click for sig info)	# Alerts	# Sources	# Destinations	
TCP *1SFR*AU scan	1	1	1	
TCP 21***PA* scan	1	1	1	
TCP **S*R**U scan	1	1	1	
TCP 2*S***AU scan	1	1	1	
TCP 21*FRPA* scan	1	1	1	
TCP 2**F*P** scan	1	1	1	

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

TCP 21*FR**U scan	1	1	1	
TCP 21S**P*U scan	1	1	1	
TCP *1SF**AU scan	1	1	1	
TCP 21S***A* scan	1	1	1	
TCP *1S***** scan	1	1	1	
TCP *1**R*AU scan	1	1	1	
TCP 2*SF*P*U scan	1	1	1	
TCP *1****AU scan	1	1	1	
TCP 21**RP*U scan	1	1	1	
TCP 21*FR*AU scan	1	1	1	
TCP **S*RPAU scan	1	1	1	
TCP 2****P*U scan	1	1	1	
TCP **SFRPAU scan	1	1	1	
TCP *1**R*** scan	1	1	1	
TCP 2***RPAU scan	1	1	1	
TCP 21****A* scan	1	1	1	
TCP 21*FR*** scan	1	1	1	
TCP 2****PAU scan	1	1	1	

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

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

TCP 2******* scan	1	1	1	
TCP 2**FR*** scan	1	1	1	
TCP *1SF*P** scan	1	1	1	
TCP 21*F*PAU scan	1	1	1	
TCP *1*F*PAU scan	1	1	1	
TCP *1S*R**U scan	1	1	1	
TCP *1***P** scan	1	1	1	
TCP 21SFR**U scan	1	1	1	
TCP 21*F*PA* scan	1	1	1	
TCP 2*SF**AU scan	1	1	1	
TCP 2******U scan	1	1	1	
TCP 2*SFR*** scan	1	1	1	
TCP *1S**PAU scan	1	1	1	
TCP 2*SFR*A* scan	1	1	1	
TCP *1S*RPA* scan	1	1	1	
TCP 21*F**A* scan	1	1	1	
TCP 2**F*PAU scan	1	1	1	
TCP *1SFR**U scan	1	1	1	

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

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

TCP *1*F*P** scan	1	1	1	
TCP 21S*RP*U scan	1	1	1	
TCP 21*FRP** scan	2	1	2	
TCP 2*SFRP*U scan	2	2	2	
TCP 21SFRP*U scan	2	2	2	
TCP *1*FR**U scan	2	2	2	
TCP **SFRP*U scan	2	1	2	
TCP *1S***A* scan	2	2	2	
TCP ***FR*AU scan	2	2	1	
TCP 21****AU scan	2	1	1	
TCP 21*FR*A* scan	2	2	2	
TCP ***FR*A* scan	2	2	2	
TCP *1*F*PA* scan	2	2	2	
TCP 2*SFR*AU scan	3	3	3	
TCP **SFRPA* scan	3	3	3	
TCP 21S**P** scan	3	1	1	
TCP 21S***** scan	6	2	4	
TCP ******** scan	17	10	12	

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

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

TCP **SF**** scan	2493	3	1951	
TCP **S***** scan	19726	30	14303	
UDP scan	23421	55	6961	

Scan File #2

SnortSnarf v052301.1

4082 alerts found using input module SnortFileInput, with sources:

- /root/perl/SnortScan-02-Apr

Earliest alert at **00:00:26**.627742 *on 04/01/2001*
Latest alert at **23:08:46**.418779 *on 04/01/2001*

Signature (click for sig info)	# Alerts	# Sources	# Destinations	
Tiny Fragments - Possible Hostile Activity	1	1	1	
NMAP TCP ping!	1	1	1	
ICMP SRC and DST outside network	2	1	1	
Watchlist 000222 NET-NCFC	4	2	2	
Null scan!	4	4	4	
Queso fingerprint	7	3	6	
TCP SRC and DST outside network	10	6	8	
WinGate 1080 Attempt	13	9	10	
SMB Name Wildcard	14	12	12	

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

Possible RAMEN server activity	84	12	69	
External RPC call	103	3	99	
UDP SRC and DST outside network	128	9	8	
Watchlist 000220 IL-ISDNNET-990517	1526	13	7	
SYN-FIN scan!	2185	1	1695	

Snort File #3

All Snort signatures

SnortSnarf v052301.1

30783 alerts found using input module SnortFileInput, with sources:

- /root/perl/SnortScan-03-Apr

Earliest alert at **00:00:09** *on 4/2/2001*
Latest alert at **23:56:58** *on 4/2/2001*

Signature (click for sig info)	# Alerts	# Sources	# Destinations	
TCP 21***PA* scan	1	1	1	
TCP 21*FRPA* scan	1	1	1	
TCP *1SF**AU scan	1	1	1	
TCP *1SFRP** scan	1	1	1	
TCP *1SFR*** scan	1	1	1	

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

TCP **SFRPAU scan	1	1	1	
TCP 2*S**P** scan	1	1	1	
TCP **SF**A* scan	1	1	1	
TCP 2**FRP*U scan	1	1	1	
TCP 21****A* scan	1	1	1	
TCP 21*FR*** scan	1	1	1	
TCP *1*FRPAU scan	1	1	1	
TCP 21*FR*A* scan	1	1	1	
TCP ***FR*A* scan	1	1	1	
TCP *1***P** scan	1	1	1	
TCP 21S***AU scan	1	1	1	
TCP 21SFR**U scan	1	1	1	
TCP 2**FR*AU scan	1	1	1	
TCP 21SF*PAU scan	1	1	1	
TCP *1*F***U scan	1	1	1	
TCP *1**RP*U scan	1	1	1	
TCP **SF*P*U scan	1	1	1	
TCP *1*F**AU scan	1	1	1	

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

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

TCP *1SF**A* scan	1	1	1	
TCP 21**RP** scan	1	1	1	
TCP 21**RPA* scan	1	1	1	
TCP 21SF***U scan	1	1	1	
TCP **SF**AU scan	1	1	1	
TCP 2*SF**** scan	1	1	1	
TCP 2*S*RP*U scan	2	2	1	
TCP 21*F***U scan	3	1	1	
TCP 21S***** scan	5	4	5	
TCP ******** scan	13	2	12	
TCP **S***** scan	1698	29	1161	
UDP scan	29033	72	7255	

Snort File #4

All Snort signatures

SnortSnarf v052301.1

61489 alerts found using input module SnortFileInput, with sources:

- /root/perl/SnortScan-26-Mar

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

Earliest alert at **00:00:30** *on 3/25/2001*
Latest alert at **23:56:16** *on 3/25/2001*

Signature (click for sig info)	# Alerts	# Sources	# Destinations	
TCP 2*S*R*A* scan	1	1	1	
TCP *1****AU scan	1	1	1	
TCP 2*SF*P*U scan	1	1	1	
TCP *1SFR*** scan	1	1	1	
TCP *1S***A* scan	1	1	1	
TCP 21**RPAU scan	1	1	1	
TCP *1*FR*AU scan	1	1	1	
TCP 2****PAU scan	1	1	1	
TCP 2***RP*U scan	1	1	1	
TCP 2**F**AU scan	1	1	1	
TCP 2******* scan	1	1	1	
TCP 2*****A* scan	1	1	1	
TCP 21SF*PA* scan	1	1	1	
TCP ****R*AU scan	1	1	1	
TCP 21SF*P*U scan	1	1	1	
TCP 2**F*PAU scan	1	1	1	

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

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

TCP ***F**** scan	1	1	1	
TCP 2*SF*PA* scan	1	1	1	
TCP 2*S*R*AU scan	1	1	1	
TCP 2****PA* scan	1	1	1	
TCP 21SF***U scan	1	1	1	
TCP 21*FR**U scan	1	1	1	
TCP 21S*RPAU scan	2	1	1	
TCP ***FR*A* scan	2	1	2	
TCP *******U scan	2	2	2	
TCP 21S*R*A* scan	2	2	2	
TCP 2*****AU scan	2	1	1	
TCP 2*SF**AU scan	3	3	3	
TCP ******** scan	4	4	4	
TCP 21S***** scan	98	2	3	
UDP scan	20176	57	7144	
TCP **S***** scan	41176	19	20158	

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

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

Snort File #5

All Snort signatures

SnortSnarf v052301.1

52593 alerts found using input module SnortFileInput, with sources:

- /root/perl/SnortScan-27-Mar

Earliest alert at **00:10:42** *on 3/26/2001*
Latest alert at **23:57:00** *on 3/26/2001*

Signature (click for sig info)	# Alerts	# Sources	# Destinations	
TCP *1*F**A* scan	1	1	1	
TCP 2*SF**A* scan	1	1	1	
TCP 2*SFR**U scan	1	1	1	
TCP 2**F*PA* scan	1	1	1	
TCP 21S**PAU scan	1	1	1	
TCP *1S***** scan	1	1	1	
TCP 21SF**** scan	1	1	1	
TCP *1*FR*AU scan	1	1	1	
TCP 21**RPAU scan	1	1	1	
TCP **SFRPAU scan	1	1	1	
TCP ***F***U scan	1	1	1	

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

TCP 2***RPAU scan	1	1	1	
TCP ****RPAU scan	1	1	1	
TCP 2*S*RPA* scan	1	1	1	
TCP 21*F*P*U scan	1	1	1	
TCP *1S**PA* scan	1	1	1	
TCP **S****U scan	1	1	1	
TCP *1*FRPA* scan	1	1	1	
TCP 21S*R*A* scan	1	1	1	
TCP *1*F**** scan	1	1	1	
TCP 21S*R**U scan	1	1	1	
TCP **S*R*A* scan	1	1	1	
TCP 21S**P** scan	1	1	1	
TCP *1SF**A* scan	1	1	1	
TCP *1*FR*A* scan	1	1	1	
TCP 21**RPA* scan	1	1	1	
TCP **SFRPA* scan	1	1	1	
TCP 2****P** scan	1	1	1	
TCP 21SF**AU scan	1	1	1	

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

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

TCP *1**R**U scan	1	1	1	
TCP 2*S**PAU scan	1	1	1	
TCP 21SFR*** scan	1	1	1	
TCP 21*FR*AU scan	1	1	1	
TCP 2**F***U scan	1	1	1	
TCP 2*SF**** scan	1	1	1	
TCP 2*S*RP** scan	1	1	1	
TCP 2*S****U scan	2	2	2	
TCP 21****A* scan	2	1	1	
TCP **SF**AU scan	2	2	2	
TCP ***FR*** scan	2	2	2	
TCP *1S*R**U scan	2	1	1	
TCP 2*S*RPAU scan	2	2	2	
TCP **SFR*AU scan	2	1	1	
TCP *1S*R*** scan	2	2	1	
TCP 21SF*P** scan	3	2	2	
TCP ***F**** scan	4	4	4	
TCP 21S***** scan	7	3	5	

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

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

TCP ******** scan	11	7	7	
TCP **S***** scan	7199	19	4742	
UDP scan	45317	71	7634	

Conclusion and Recommendation

Based upon the above summaries of Snort alerts and scans, it is obvious that MY.NET's network has been subjected to some very suspicious activity. Further analysis and recommendations are discussed in greater detail in the List of Detects with Explanations and Details section included in this report.

LIST OF DETECTS WITH EXPLANATIONS AND DETAILS

ICMP SRC and DST outside network

SnortSnarf v052301.1

ICMP is often used for purposes other than it was intended. ICMP can be used in denial-of-service attacks, and the SANS course used WinFreeze and Smurf as classic examples.

The CVE database at cve.mitre.org listed the following relating to ICMP:

- CVE-1999-0128
- CVE-1999-0214
- CVE-1999-0265
- CVE-1999-0513

6 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **13:21:04**.058485 *on 03/25/2001*
Latest such alert at **18:49:26**.972974 *on 04/02/2001*

ICMP SRC and DST outside network	3 sources	3 destinations

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

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
172.168.100.123	3	6	1	2
172.167.9.216	2	2	1	1
172.128.30.236	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
217.32.140.237	3	3	1	1
216.101.207.124	2	2	1	1
24.162.140.146	1	1	1	1

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

SnortSnarf v052301.1

See http://www.incidents.org/archives/y2k/082200.htm. Compromised Linux boxes were discovered to be "listening" on port 55850 (tcp) and these compromised boxes had rootkits installed.

7 alerts with this signature using input module SnortFileInput, with sources:

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

- /root/perl/allalerts.txt

Earliest such alert at **03:32:07**.497713 *on 03/26/2001*
Latest such alert at **16:47:04**.593439 *on 03/31/2001*

Port 55850 tcp - Possible myserver activity - ref. 010313-1	5 sources	5 destinations

---

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
198.81.129.194	3	3	1	1
212.158.113.194	1	1	1	1
255.254.60.38	1	1	1	1
193.63.177.1	1	1	1	1
204.68.24.61	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.253.112	6	6	4	4
63.97.226.2	1	1	1	1

SUNRPC highport access!

SnortSnarf v052301.1

As the SANS web site mentions in the Top Ten Internet Threats (www.sans.org/topten.htm), RPC are a common scan and if exploited, can allow root compromise. RPC (port 111) is routinely scanned for gathering information on RPC

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

services that may be running. Some good info: http://www.sans.org/y2k/trouble_RPCs.htm. A really good presentation on RPC's was given by David Hoelzer at SANS Baltimore titled "RPC's: Friend or Foe?"

A recent audit of one of our Solaris servers revealed the following RPC port problems (output from the Retina vulnerability scanner from www.eeye.com):

Rpc Services: RPC cmsd overflow	
Description:	The cmsd RPC service has been known to contain holes that would allow a remote attacker the ability to run code as root on the remote server due to an unchecked buffer condition.
Risk Level:	High
How To Fix:	Upgrade to the current version of cmsd from your vendor, or if this service is unnecessary, remove it following your vendor's directions.
CVE:	CVE-1999-0696
BugtraqID:	524

Rpc Services: RPC sadmind overflow	
Description:	The sadmind RPC service has been known to contain holes that would allow a remote attacker the ability to run code as root on the remote server due to an unchecked buffer condition.
Risk Level:	High
How To Fix:	Upgrade to the current version of cmsd from your vendor, or if this service is unnecessary, remove it following your vendor's directions.
CVE:	CVE-1999-0977
BugtraqID:	866

Rpc Services: RPC statd file deletion vuln	
Description:	The statd RPC service has been known to contain an error that could allow an attacker to create or delete files on the hard drive due to improper argument checking by the statd service.
Risk Level:	High
How To Fix:	Upgrade to the current version of statd from your vendor, or if this service is unnecessary, remove it following your vendor's directions.
CVE:	CVE-1999-0019

Rpc Services: RPC statd format string attack

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

Description:	The statd RPC service in numerous Linux distributions has been known to contain format string holes that would allow a remote attacker the ability to run code as root.
Risk Level:	High
How To Fix:	Upgrade to the current version of statd from your vendor, or if this service is unnecessary, remove it following your vendor's directions.
CVE:	CVE-2000-0666
BugtraqID:	1480

Rpc Services: RPC statd overflow	
Description:	The statd RPC service has been known to contain holes that would allow a remote attacker the ability to run code as root due to poor bounds checking.
Risk Level:	High
How To Fix:	Upgrade to the current version of statd from your vendor, or if this service is unnecessary, remove it following your vendor's directions.
CVE:	CVE-1999-0018
BugtraqID:	127

Rpc Services: RPC ttdbserver overflow	
Description:	The ttdbserver RPC service has been known to contain holes that would allow a remote attacker the ability to run code as root on the remote server due to an unchecked buffer condition.
Risk Level:	High
How To Fix:	Upgrade to the current version of ttdbserver from your vendor, or if this service is unnecessary, remove it following your vendor's directions.
CVE:	CVE-1999-0003
BugtraqID:	122

Rpc Services: RPC nlockd DoS	
Description:	The lockd RPC service has been known to contain holes that would allow a remote attacker the ability to deny service to normal NFS users.
Risk Level:	Medium
How To Fix:	Upgrade to the current version of nlockd from your vendor, or if this service is unnecessary, remove it following your vendor's directions.
CVE:	CVE-2000-0508

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

BugtraqID:	1372

Rpc Services: RPC rusersd username enumeration	
Description:	The rusers service can be used to gather information on your system that will help an attacker greatly. The information retrieved pertains to account names of users on your system and their access times. For example: rusers -l yourcomputer.com
Risk Level:	Medium
How To Fix:	We recommended that you disable this service if you are not currently using it.
CVE:	CVE-1999-0626

Rpc Services: RPC walld message spoofing	
Description:	The walld service can be used by attackers to trick local system users into carrying out various actions by spoofing messages to their consoles. Walld can also be used to carry out a Denial of Service attack by flooding user consoles with garbage.
Risk Level:	Medium
How To Fix:	It's recommended that you disable this service if you are not currently using it.
CVE:	CVE-1999-0181

10 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **14:58:28**.952796 *on 03/25/2001*
Latest such alert at **14:58:29**.585974 *on 03/25/2001*

SUNRPC highport access!	1 sources	1 destinations

Sources triggering this attack signature

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

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
216.136.171.195	10	10	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.100.225	10	10	1	1

Tiny Fragments - Possible Hostile Activity

SnortSnarf v052301.1

Fragmentation, the malicious kind, can be used in denial-of-service attacks. The course reviewed the most infamous associated with fragmentation: Ping of Death and Teardrop.

The scanning tool *nmap* (www.insecure.org/nmap) has an option (-f) that fragments the 20-byte TCP headers into multiple fragments. The purpose is to avoid detection by firewalls and intrusion detection systems that do not do packet re-assembly.

20 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **17:44:11**.884673 *on 03/25/2001*
Latest such alert at **16:48:11**.374219 *on 04/02/2001*

Tiny Fragments - Possible Hostile Activity	2 sources	13 destinations

---

Sources triggering this attack signature

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

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

202.39.78.125	18	18	11	11
202.39.78.124	2	2	2	2

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.203.150	4	5	1	2
255.254.208.30	2	2	1	1
255.254.230.42	2	2	1	1
255.254.208.142	2	2	1	1
255.254.203.50	2	2	1	1
255.254.210.26	1	1	1	1
255.254.205.18	1	1	1	1
255.254.202.166	1	1	1	1
255.254.204.218	1	1	1	1
255.254.220.62	1	1	1	1
255.254.207.254	1	1	1	1
255.254.218.178	1	1	1	1
255.254.228.2	1	1	1	1

NMAP TCP ping!

SnortSnarf v052301.1

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

This traffic was generated from *nmap* with the –sP option with the explicit purpose to determine active hosts. From the *nmap* manpage (www.insecure.com/nmap/nmap_manpage.html): "Ping scanning: Sometimes you only want to know which host on a network are up. Nmap can do this by sending ICMP echo request packets to every IP address on the network you specify. Hosts that respond are up. *Unfortunately, some sites such as Microsoft.com block echo request packets. Thus nmap can also send a TCP ack packet to (by default) port 80. If we get an RST back, that machine is up*."

Some CVE's relating to ping problems:

- CVE-1999-0053
- CVE-1999-0056
- CVE-1999-0074
- CVE-1999-0077

21 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **01:29:17**.800892 *on 03/25/2001*
Latest such alert at **20:32:54**.095143 *on 04/02/2001*

NMAP TCP ping!	8 sources	12 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
192.102.197.234	10	10	2	2
63.119.91.2	2	2	2	2
194.133.58.2	2	2	2	2
199.197.130.21	2	2	2	2
202.187.24.3	2	2	2	2
12.108.43.5	1	1	1	1

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

63.67.116.15	1	1	1	1
195.25.86.2	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.1.8	7	7	1	1
255.254.1.10	3	3	1	1
255.254.100.165	2	2	2	2
255.254.6.7	1	2	1	2
255.254.98.184	1	1	1	1
255.254.109.9	1	1	1	1
255.254.1.3	1	1	1	1
255.254.1.4	1	1	1	1
255.254.60.14	1	1	1	1
255.254.253.125	1	1	1	1
255.254.100.230	1	1	1	1
255.254.110.39	1	1	1	1

Null scan!

SnortSnarf v052301.1

The null scan traffic was generated with *nmap* using the –sN option (all TCP flags are set to a null [zero] value). From nmap manpages: "The null scan turns off all flags. Unfortunately, Microsoft (like usual) decided to completely ignore the standard and do

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

things their own way. *Thus this scan type will not work against systems running Windows 95/NT.*"

22 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **05:58:00**.774235 *on 03/25/2001*
Latest such alert at **04:38:08**.108174 *on 04/02/2001*

Null scan!	16 sources	13 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
24.43.241.223	4	4	1	1
24.17.64.12	2	2	1	1
24.141.54.29	2	2	1	1
24.201.95.135	2	2	1	1
213.89.88.29	1	1	1	1
209.221.200.17	1	1	1	1
24.200.182.116	1	1	1	1
212.199.104.98	1	1	1	1
194.109.233.100	1	1	1	1
212.4.217.243	1	1	1	1
24.108.146.141	1	1	1	1
63.91.227.152	1	1	1	1
62.254.145.163	1	1	1	1
213.65.8.178	1	1	1	1

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

129.93.83.7	1	1	1	1
202.77.194.196	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.209.30	9	9	4	4
255.254.178.42	1	42	1	3
255.254.226.82	1	2	1	2
255.254.222.154	1	6562	1	5
255.254.20.10	1	1	1	1

Russia Dynamo - SANS Flash 28-jul-00

SnortSnarf v052301.1

---

http://www.sans.org/y2k/072818.htm discussed this traffic. SANS recommended that traffic to and from this Russian IP range of 194.87.6.X be blocked. The recommendation mentioned a lot of unusual activity consisting of port scanning for proxies (proxy servers), with the information being returned to Russia.

45 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **17:26:58**.230744 *on 03/25/2001*
Latest such alert at **19:02:52**.309207 *on 04/02/2001*

Russia Dynamo - SANS Flash 28-jul-00	3 sources	2 destinations

---

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

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
194.87.6.189	40	40	1	1
255.254.178.42	4	4	1	1
194.87.6.21	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.178.42	41	42	2	3
194.87.6.21	4	4	1	1

TCP SRC and DST outside network

SnortSnarf v052301.1

The following traces have been pulled from several days of this traffic:

```
03/26-02:19:44.699718 [**] TCP SRC and DST outside network [**]
169.254.101.152:1898 -> 205.188.45.241:5190
 03/26-03:42:56.422299 [**] TCP SRC and DST outside network [**]
169.254.101.152:2137 -> 205.188.45.242:5190
 03/26-04:49:39.548821 [**] TCP SRC and DST outside network [**]
169.254.101.152:2652 -> 205.188.45.241:5190
 03/26-16:50:08.424602 [**] TCP SRC and DST outside network [**]
169.254.101.152:2824 -> 205.188.45.243:5190
 03/26-18:48:01.245286 [**] TCP SRC and DST outside network [**]
169.254.101.152:4583 -> 205.188.45.241:5190
 03/31-00:19:20.819341 [**] TCP SRC and DST outside network [**]
169.254.101.152:12345 -> 172.173.74.52:1049
```


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

```
 03/31-03:24:54.909527 [**] TCP SRC and DST outside network [**]
169.254.101.152:1983 -> 205.188.50.71:5190
 04/02-00:17:26.477013 [**] TCP SRC and DST outside network [**]
169.254.101.152:1156 -> 205.188.48.40:5190
 04/02-00:17:26.477013 [**] TCP SRC and DST outside network [**]
169.254.101.152:1156 -> 205.188.48.40:5190
 04/02-00:21:59.829935 [**] TCP SRC and DST outside network [**]
169.254.101.152:1302 -> 205.188.49.20:5190
 04/02-00:21:59.829935 [**] TCP SRC and DST outside network [**]
169.254.101.152:1302 -> 205.188.49.20:5190
 04/02-03:42:25.383238 [**] TCP SRC and DST outside network [**]
169.254.101.152:4098 -> 205.188.49.16:5190
 04/02-03:42:25.383238 [**] TCP SRC and DST outside network [**]
169.254.101.152:4098 -> 205.188.49.16:5190
 04/02-03:42:25.383283 [**] TCP SRC and DST outside network [**]
169.254.101.152:4098 -> 205.188.49.16:5190
```

A port search on port 5190 shows that it is America Online, ICQ2000 and Aimtalk. An IP search (whois) of 205.188.0.0 shows America Online (AOL's ICQ server?). It's hard to determine if this is a stimulus or response and whether this is a false positive or possibly some form of trojan.

Some CVE's relating to ICQ:

- CVE-1999-0474
- CVE-2000-0552
- There are 4 2000 Candidates

57 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **09:42:36**.137622 *on 03/25/2001*
Latest such alert at **22:24:19**.069127 *on 04/02/2001*

TCP SRC and DST outside network	20 sources	31 destinations

Sources triggering this attack signature

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

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
169.254.101.152	24	24	10	10
172.140.196.73	12	12	2	2
206.196.177.82	2	2	2	2
192.168.0.5	2	2	1	1
172.173.125.73	2	2	1	1
192.168.0.91	1	1	1	1
172.167.21.111	1	1	1	1
172.138.220.59	1	1	1	1
172.129.197.115	1	1	1	1
172.173.206.4	1	1	1	1
192.168.1.92	1	1	1	1
172.149.45.223	1	1	1	1
4.0.0.3	1	1	1	1
172.173.127.148	1	1	1	1
172.139.46.249	1	1	1	1
172.137.159.143	1	1	1	1
172.139.42.18	1	1	1	1
172.170.70.12	1	1	1	1
192.168.0.18	1	1	1	1
172.174.59.129	1	1	1	1

Destinations receiving this attack signature

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

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
12.77.186.67	10	10	1	1
205.188.49.16	6	6	1	1
205.188.49.19	5	5	1	1
205.188.45.241	3	3	1	1
204.71.202.119	2	2	1	1
64.4.13.39	2	2	1	1
205.188.48.40	2	2	1	1
205.188.49.20	2	2	1	1
205.188.50.71	2	2	1	1
212.111.5.91	2	2	1	1
208.209.196.171	1	1	1	1
64.224.121.81	1	1	1	1
203.202.10.26	1	1	1	1
24.183.165.163	1	1	1	1
64.228.196.108	1	1	1	1
200.59.34.137	1	1	1	1
208.146.124.44	1	1	1	1
216.234.174.8	1	1	1	1
205.188.48.42	1	1	1	1
198.142.218.72	1	1	1	1
152.163.241.120	1	1	1	1
205.188.45.242	1	1	1	1
205.188.45.243	1	1	1	1

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

134.155.40.9	1	1	1	1
205.188.39.163	1	1	1	1
208.232.153.67	1	1	1	1
64.4.13.218	1	1	1	1
172.173.74.52	1	1	1	1
4.0.0.3	1	1	1	1
65.64.30.3	1	1	1	1
163.18.152.2	1	1	1	1

Watchlist 000222 NET-NCFC

SnortSnarf v052301.1

Traffic from this range has resulted in a detect setup to alert on activity from the net NCFC (The Computer Network Center Chinese Academy of Sciences).

69 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **02:22:27**.634469 *on 03/26/2001*
Latest such alert at **21:37:37**.636498 *on 04/02/2001*

Watchlist 000222 NET-NCFC	7 sources	7 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
159.226.92.9	36	36	1	1

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

159.226.41.166	22	22	1	1
159.226.158.188	4	4	1	1
159.226.47.217	4	4	1	1
159.226.228.1	1	1	1	1
159.226.47.195	1	1	1	1
159.226.45.3	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.144.54	36	37	1	2
255.254.100.81	22	23	1	2
255.254.6.47	4	4	1	1
255.254.140.236	4	4	1	1
255.254.253.42	1	1	1	1
255.254.253.43	1	2	1	2
255.254.6.7	1	2	1	2

WinGate 1080 Attempt

SnortSnarf v052301.1

WinGate is a popular Windows 95/NT proxy firewall (wingate.deerfield.com) and has some known vulnerabilities reported over the years. From the CVE database:

- CVE-1999-0290

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

- CVE-1999-0291
- CVE-1999-0441
- CVE-1999-0494

A list of WinGate servers is maintained at Cyberarmy (www.cyberarmy.com/wingate).

79 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **00:19:58**.587588 *on 03/25/2001*
Latest such alert at **22:20:11**.600061 *on 04/02/2001*

WinGate 1080 Attempt	35 sources	44 destinations

NOTE:Due to the number of Sources and Destinations, for the sake of brevity, only the top number of sources and destinations will be included.

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
204.117.70.5	8	8	3	3
195.66.170.8	8	8	3	3
216.54.223.198	5	5	2	2
213.151.16.249	4	4	1	1
216.152.64.211	4	4	3	3
62.193.128.9	4	4	1	1
198.63.2.194	4	4	3	3

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

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.204.102	5	5	2	2
255.254.60.8	4	4	3	3
255.254.254.10	4	4	1	1
255.254.107.124	4	4	1	1
255.254.222.10	4	4	1	1

Back Orifice

SnortSnarf v052301.1

Back Orifice is a remote Windows administration tool, at least that is how it is portrayed by The Cult of the Dead Cow (http://www.cultdeadcow.com/tools/bo.html), the writers of this software. Unfortunately, it's used to gain administration of unsuspecting Windows machines, usually via port 31337.

CVE's to review:

- CAN-1999-0660
- CAN-2000-0562

109 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **14:37:58**.116356 *on 03/26/2001*
Latest such alert at **14:38:45**.807857 *on 03/26/2001*

Back Orifice	1 sources	109 destinations

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

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
24.162.245.198	109	109	109	109

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.0.0/24	1	1	1	1

Queso fingerprint

SnortSnarf v052301.1

This program probes a remote machine with a certain sequence of TCP packets. By analysing the response packets it can determine the type of operating system that runs on the remote machine, the version of that OS and sometimes it can even give information about the configuration of that machine.

For further information, see CAN-1999-0454 at cve.mitre.org

116 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **12:09:06**.016891 *on 03/25/2001*
Latest such alert at **15:30:33**.434439 *on 04/02/2001*

Queso fingerprint	6 sources	13 destinations

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

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
129.206.170.20	99	99	2	2
158.75.57.4	9	9	7	7
130.233.26.197	5	5	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.202.54	98	99	1	2
255.254.219.134	5	5	1	1

---

connect to 515 from outside

SnortSnarf v052301.1

This traffic can be a printer attack against HP printers, referred to as the HP JetDirect card attack. Port 515 is the print spooler port. See http://www.sans.org/newlook/alerts/port515.htm which discusses the Unix LPR service that runs on this port that has vulnerabilities. See:

- CVE-2000-0636
- CAN-2000-1062
- CAN-2000-1063
- CAN-2000-1064
- CAN-2000-1065

119 alerts with this signature using input module SnortFileInput, with sources:

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

- /root/perl/allalerts.txt

Earliest such alert at **13:35:45**.570696 *on 03/31/2001*
Latest such alert at **18:07:49**.638079 *on 04/02/2001*

connect to 515 from outside	6 sources	109 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
63.123.106.6	37	37	37	37
207.124.229.123	33	33	31	31
212.125.177.199	20	20	20	20
205.238.235.88	17	17	16	16
171.64.67.106	9	9	9	9
24.91.8.50	3	3	3	3

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.0.0/24	2	8	2	3

SMB Name Wildcard

SnortSnarf v052301.1

These are probes against NetBIOS port 137. http://www.sans.org/y2k/050300.htm has some interesting comments on this. www.robertgraham.com/pubs/firewall-seen.html

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

mentions the sscan tools, a popular scanning tool that attempts to find this vulnerability and then exploit it.

NetBIOS is used to enumerate information from Windows machines. www.securityfocus.com also mentioned that NetBIOS was used to propagate the Internet worm *network.vbs*.

See the following for further information:

- CVE-1999-0225
- CVE-1999-0391
- CAN-1999-0495

154 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **02:03:58**.634868 *on 03/25/2001*
Latest such alert at **23:35:23**.810694 *on 04/02/2001*

SMB Name Wildcard	74 sources	53 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
211.118.86.11	6	6	1	1
205.215.192.55	6	6	1	1
4.41.3.11	6	6	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.132.36	20	21	5	6

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

255.254.133.32	15	15	3	3
255.254.133.245	11	12	7	8
255.254.135.45	11	12	3	4

Possible RAMEN server activity

SnortSnarf v052301.1

See http://www.sans.org/y2k/ramen.htm for a detailed explanation of this worm and how to detect it. This worm seemed to propagate mostly on Linux machines and servers.

175 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **07:37:29**.387600 *on 03/25/2001*
Latest such alert at **19:57:08**.989338 *on 04/02/2001*

Possible RAMEN server activity	66 sources	67 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
63.10.42.245	15	15	1	1
255.254.209.86	13	13	1	1
255.254.221.26	10	10	4	4
255.254.98.171	9	9	1	1
24.180.160.210	6	6	2	2
255.254.98.166	6	6	1	1

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

255.254.219.178	5	5	3	3

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
63.10.40.155	17	17	2	2
255.254.210.2	15	15	1	1
24.180.160.210	15	15	2	2
255.254.221.26	9	9	6	6

External RPC call

SnortSnarf v052301.1

These alerts were triggered by scans to port 111, the portmapper service.

382 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **16:26:56**.292779 *on 03/25/2001*
Latest such alert at **23:18:23**.558962 *on 04/02/2001*

External RPC call	7 sources	305 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
209.217.53.190	81	81	81	81
61.129.39.161	81	81	65	65

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

24.91.102.156	69	69	69	69
209.189.124.214	52	52	52	52
209.70.72.22	44	44	44	44
38.162.57.27	29	29	29	29
63.109.70.97	26	26	23	23

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.0.0/24	3	3	2	2

UDP SRC and DST outside network

SnortSnarf v052301.1

A small (one day's) look at some of the traffic from the top IP generating this traffic (246 alerts):

```
03/25-19:09:10.936641 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.26:137
 03/25-19:10:14.146740 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.33:137
 03/25-19:10:23.176538 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.34:137
 03/25-19:11:18.844589 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.40:137
 03/25-19:11:54.980582 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.44:137
 03/25-19:14:08.940685 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.59:137
 03/25-19:14:10.445860 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.59:137
 03/25-19:14:25.511720 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.61:137
```


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

```
 03/25-19:14:28.505396 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.61:137
 03/25-19:14:46.565707 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.63:137
 03/25-19:14:54.106902 [**] UDP SRC and DST outside network [**]
169.254.67.123:137 -> 199.219.133.64:137
```

Note the same source and destination ports.

A review of the other top IP (101 alerts) showed that the source port was 137 while the destination port was 53.

From page 265 of Network Intrusion Detection by Northcutt and Novak mentions the following: "One of the characteristics of NetBIOS is that traffic to destination port 137 is often caused by something a site initiates. If you send email to a site running Microsoft Exchange, for example, they will often send a port 137 attempt back." The page goes on to mention "If your site doesn't use Network Address Translation (NAT), the Web server will have your IP address."

571 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **00:02:37**.218486 *on 03/25/2001*
Latest such alert at **23:48:12**.158179 *on 04/02/2001*

UDP SRC and DST outside network	41 sources	259 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
169.254.67.123	246	246	212	212
192.168.0.13	101	101	2	2
204.62.41.254	35	35	1	1
169.254.26.24	35	35	17	17
134.192.134.112	22	22	1	1

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

18.236.0.28	12	12	2	2
128.210.150.221	10	10	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
235.80.68.83	66	66	17	17
199.45.32.38	55	55	1	1
199.45.32.43	46	46	1	1
204.62.32.194	35	35	1	1
134.192.148.14	27	27	2	2

SYN-FIN scan!

SnortSnarf v052301.1

These are crafted packets designed to evade firewalls and IDS's. They are a "stealthy" fingerprinting method designed to help map a network. The stealth scan uses both the SYN and FIN TCP flags. This is an invalid flag combination with the purpose of evading firewalls and IDS's.

1924 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

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

Earliest such alert at **00:00:52**.899361 *on 03/31/2001*
Latest such alert at **18:22:46**.102902 *on 03/31/2001*

SYN-FIN scan!	1 sources	1487 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
211.178.63.4	1924	1924	1487	1487

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.2554.0.0/24	4	4	1	1

Watchlist 000220 IL-ISDNNET-990517

SnortSnarf v052301.1

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

Detect setup to alert on activity from the European Regional Internet Registry/RIPE NCC (NET-RIPE-NCC-).

7898 alerts with this signature using input module SnortFileInput, with sources:

/root/perl/allalerts.txt

Earliest such alert at **02:26:45**.860208 *on 03/25/2001*
Latest such alert at **23:07:48**.661953 *on 04/02/2001*

Watchlist 000220 IL-ISDNNET-990517	21 sources	20 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
212.179.4.50	6473	6473	1	1
212.179.72.226	1082	1082	1	1
212.179.27.6	84	84	3	3
212.179.5.87	73	73	1	1
212.179.83.143	69	69	1	1
212.179.95.5	26	26	2	2
212.179.7.182	22	22	1	1
212.179.79.2	17	17	2	2

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

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.222.154	6561	6562	4	5
255.254.201.238	1082	1082	1	1
255.254.219.38	90	90	4	4
255.254.219.18	69	69	1	1
255.254.207.210	24	24	1	1
255.254.202.10	22	22	1	1
255.254.221.102	14	14	1	1
255.254.253.41	1	1	1	1

Attempted Sun RPC high port access

SnortSnarf v052301.1

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

See "SunRPC highport access" above.

10833 alerts with this signature using input module SnortFileInput, with sources:

- /root/perl/allalerts.txt

Earliest such alert at **19:42:24**.114048 *on 03/26/2001*
Latest such alert at **22:40:51**.585106 *on 04/02/2001*

Attempted Sun RPC high port access	4 sources	4 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
63.121.232.185	10379	10379	2	2
209.150.227.153	452	452	1	1
205.188.153.101	1	1	1	1
205.188.153.97	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
255.254.221.198	8926	8926	1	1
255.254.224.2	1905	1905	2	2

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

255.254.228.90	1	1	1	1
255.254.224.58	1	1	1	1

INTERNAL NETWORK (MY.NET): MY.NET was changed to 255.254 in order to process the files through SnortSnarf.

TCP SCANS

The type of scans noted in the Snort logs involved various TCP scans designed to map MY.NET's network. Some of the scans were of a "stealthy" variety, such as the FIN and SYN-FIN scans, but some were also very "noisy", such as the XMAS scan.

Total number of TCP scans: 194,685 (derived from the 5 SnortSnarf summaries above).

Types of Scans noted:

- SYNFIN scans have been used on the Internet for many years now. Originally designed to bypass firewalls by setting the FIN bit. Many routers, at the time, saw the FIN bit set and assumed this packet was closing an already open connection.

- The NOACK scans are scans with no ACK bit set. These scans are used since only a single type of packet should have no ACK bit set and that is an initial SYN packet to start a session. Crafted packets of this sort with other bits set instead are designed to bypass filtering and solicit a response from a host. Similarly, the INVALIDACK scan sets the ACK bit, but with unusual combinations of other bits. These scans are designed to help "fingerprint" a system by soliciting unique responses to the invalid bits being set. Fingerprinting systems is done by sending invalid combinations of flags in the packet, which many operating systems will respond to in unique manner thus allowing the intruder to guess at the type of system being used. This is useful to discover the correct exploit to use on the machine at a later date.

- The UNKNOWN scans are scans with unusual combinations of bits set, also to fingerprint systems.

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

- The FIN scan was developed to work in the manner as described by the SYNFIN scans above. It is considered a "stealthy" scan.
- The VECNA scan is a unique set of flags set, U, P, U&P, P&F, or F&U.
- The FULLXMAS scan has all bits set.
- The XMAS scans has the F&P&U bits set.
- The SPAU scan has the S&P&A&U bits set.
- The NMAPID scan is the unique S&F&P&U bit setting.

TOP TALKERS

Alerts:

- 63.121.232.185
- 212.179.4.50
- 212.179.72.226
- 129.206.170.20
- 192.168.0.13
- 194.87.6.189
- 159.226.92.9
- 204.62.41.254
- 63.123.106.6
- 212.179.95.5
- 159.226.92.9

Scans:

- 212.144.16.169
- 200.51.8.209
- 255.254.221.198 (MY.NET)
- MY.NET.218.86
- MY.NET.2124.30

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

- 202.112.209.30
- 195.41.102.2
- 212.87.232.136
- 211.178.63.4
- 217.85.227.219
- 195.22.0.154

EXTERNAL SOURCE ADDRESSES AND REGISTRATION INFORMATION

1. Exodus Communications Inc.SantaClara-5 (NETBLK-EC20-2)
   2831 Mission College Blvd.
   Santa Clara, CA 95112
   US

   Netname: EC20-2
   Netblock: 216.136.128.0 - 216.136.255.255
   Maintainer: EC20

   Coordinator:
   Center, Network Control (NOC44-ARIN) CompServ@Exodus.net
   (888) 239-6387 (FAX) (888) 239-6387

   Domain System inverse mapping provided by:

   NS.EXODUS.NET 206.79.230.10
   NS2.EXODUS.NET 207.82.198.150

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
   * Rwhois reassignment information for this block is available at:
   * rwhois.exodus.net 4321

   Record last updated on 23-Mar-2001.
   Database last updated on 21-Jul-2001 23:13:10 EDT.

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

216.136.171.195 – This was chosen because it corresponds to the SunRPC Highport Access alert reported on the Snort Alerts. This attempt would make one believe that a host may have been compromised since the attacker specifically targeted a RPC port (32771):

```
03/25-14:58:28.952796 [**] SUNRPC highport access! [**]
216.136.171.195:3778 -> 255.254.100.225:32771
 03/25-14:58:28.953834 [**] SUNRPC highport access! [**]
216.136.171.195:3778 -> 255.254.100.225:32771
 03/25-14:58:28.955052 [**] SUNRPC highport access! [**]
216.136.171.195:3778 -> 255.254.100.225:32771
 03/25-14:58:28.956351 [**] SUNRPC highport access! [**]
216.136.171.195:3778 -> 255.254.100.225:32771
 03/25-14:58:28.957660 [**] SUNRPC highport access! [**]
216.136.171.195:3778 -> 255.254.100.225:32771
 03/25-14:58:28.958912 [**] SUNRPC highport access! [**]
216.136.171.195:3778 -> 255.254.100.225:32771
 03/25-14:58:29.278921 [**] SUNRPC highport access! [**]
216.136.171.195:3778 -> 255.254.100.225:32771
 03/25-14:58:29.508244 [**] SUNRPC highport access! [**]
216.136.171.195:3778 -> 255.254.100.225:32771
 03/25-14:58:29.509697 [**] SUNRPC highport access! [**]
216.136.171.195:3778 -> 255.254.100.225:32771
 03/25-14:58:29.585974 [**] SUNRPC highport access! [**]
216.136.171.195:3778 -> 255.254.100.225:32771
```

2. UUNET Technologies, Inc. (NETBLK-UUNET63) UUNET63 63.64.0.0 - 63.127.255.255
Sigecom (NETBLK-UU-63-121-232) UU-63-121-232 63.121.232.0 - 63.121.239.255

63.121.232.185 - This one was chosen because it was the "top talker" on the alerts list. It relates to the "Attempted Sun RPC highport access" on the Snort alert logs. Example:

```
03/26-19:42:24.114048 [**] Attempted Sun RPC high port access [**]
63.121.232.185:32768 ->
 255.254.221.198:32771
 03/26-19:42:27.178486 [**] Attempted Sun RPC high port access [**]
63.121.232.185:32768 ->
 255.254.221.198:32771
 03/26-19:42:27.602308 [**] Attempted Sun RPC high port access [**]
63.121.232.185:32768 ->
 255.254.221.198:32771
 03/26-19:42:27.671284 [**] Attempted Sun RPC high port access [**]
63.121.232.185:32768 ->
```


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

```
255.254.221.198:32771
```

3. 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
   CN

   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
   GINGKO.ICT.AC.CN 159.226.40.1

   Record last updated on 25-Jul-1994.
   Database last updated on 21-Jul-2001 23:13:10 EDT.

159.226.92.9 - This one corresponds to the "Watchlist 000222NET – NCFC" alert.

4. UUNET Technologies, Inc. (NETBLK-NETBLK-UUNET97DU)
   3060 Williams Drive, Suite 601
   Fairfax, va 22031
   US

   Netname: NETBLK-UUNET97DU
   Netblock: 63.0.0.0 - 63.63.255.255
   Maintainer: UUDA

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

Coordinator:
UUNET, Technical Support (OA12-ARIN) help@uu.net
(800) 900-0241

Domain System inverse mapping provided by:

DIALDNS1.UU.NET	153.39.194.10
DIALDNS2.UU.NET	153.39.194.26
DIALDNS200.NS.UU.NET	195.129.111.3
DIALDNS210.NS.UU.NET	195.129.111.4

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 20-Jun-2001.
Database last updated on 21-Jul-2001 23:13:10 EDT.

63.10.42.245 - This one corresponds to the "Ramen" worm alert. It's the only source destination that is external for this alert.

5. Asia Pacific Network Information Center (NETBLK-APNIC-CIDR-BLK)
These addresses have been further assigned to Asia-Pacific users.
Contact info can be found in the APNIC database,
at WHOIS.APNIC.NET or http://www.apnic.net/
Please do not send spam complaints to APNIC.
AU

Netname: APNIC-CIDR-BLK2
Netblock: 210.0.0.0 - 211.255.255.255

Coordinator:
Administrator, System (SA90-ARIN) [No mailbox]
+61-7-3367-0490

Domain System inverse mapping provided by:

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

NS.APNIC.NET	203.37.255.97
SVC00.APNIC.NET	202.12.28.131
NS.TELSTRA.NET	203.50.0.137
NS.RIPE.NET	193.0.0.193

Regional Internet Registry for the Asia-Pacific Region.

*** Use whois -h whois.apnic.net *** *** or see http://www.apnic.net/db/ for database assistance *** Record last updated on 03-May-2000. Database last updated on 21-Jul-2001 23:13:10 EDT.

211.178.63.4 – This one is the source for the SYN-FIN scans. This address generated 1924 alerts against 1487 destinations. Example:

```
03/31-00:00:52.899361 [**] SYN-FIN scan! [**] 211.178.63.4:53 ->
255.254.71.34:53
 03/31-00:05:54.315017 [**] SYN-FIN scan! [**] 211.178.63.4:21 ->
255.254.132.34:21
 03/31-00:06:07.092696 [**] SYN-FIN scan! [**] 211.178.63.4:8080 ->
255.254.130.34:8080
 03/31-00:06:50.406591 [**] SYN-FIN scan! [**] 211.178.63.4:21 ->
255.254.143.34:21
 03/31-00:08:42.688190 [**] SYN-FIN scan! [**] 211.178.63.4:21 ->
255.254.165.34:21
 03/31-00:08:58.954461 [**] SYN-FIN scan! [**] 211.178.63.4:109 ->
255.254.170.34:109
 03/31-00:10:09.383795 [**] SYN-FIN scan! [**] 211.178.63.4:21 ->
255.254.182.34:21
 03/31-00:11:47.248064 [**] SYN-FIN scan! [**] 211.178.63.4:109 ->
255.254.203.34:109
 03/31-00:12:41.866006 [**] SYN-FIN scan! [**] 211.178.63.4:53 ->
255.254.210.34:53
 03/31-00:14:34.061334 [**] SYN-FIN scan! [**] 211.178.63.4:53 ->
255.254.232.34:53
 03/31-00:21:27.679965 [**] SYN-FIN scan! [**] 211.178.63.4:21 ->
255.254.60.35:21
 03/31-00:27:44.343457 [**] SYN-FIN scan! [**] 211.178.63.4:111 ->
255.254.133.35:111
 03/31-00:29:42.394534 [**] SYN-FIN scan! [**] 211.178.63.4:21 ->
255.254.157.35:21
 03/31-00:30:25.818653 [**] SYN-FIN scan! [**] 211.178.63.4:8080 ->
255.254.161.35:8080
 03/31-00:30:28.337573 [**] SYN-FIN scan! [**] 211.178.63.4:21 ->
255.254.166.35:21
```


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

```
 03/31-00:30:44.639456 [**] SYN-FIN scan! [**] 211.178.63.4:109 ->
255.254.171.35:109
 03/31-00:31:29.532714 [**] SYN-FIN scan! [**] 211.178.63.4:21 ->
255.254.178.35:21
 03/31-00:31:52.517534 [**] SYN-FIN scan! [**] 211.178.63.4:8080 ->
255.254.178.35:8080
 03/31-00:34:42.847433 [**] SYN-FIN scan! [**] 211.178.63.4:53 ->
255.254.214.35:53
 03/31-00:35:03.248701 [**] SYN-FIN scan! [**] 211.178.63.4:53 ->
255.254.218.35:53
 03/31-00:38:18.585412 [**] SYN-FIN scan! [**] 211.178.63.4:109 ->
255.254.5.36:109
 03/31-00:38:27.761874 [**] SYN-FIN scan! [**] 211.178.63.4:21 ->
255.254.5.36:21
 03/31-00:39:11.146689 [**] SYN-FIN scan! [**] 211.178.63.4:8080 ->
255.254.9.36:8080
 03/31-00:39:53.953239 [**] SYN-FIN scan! [**] 211.178.63.4:53 ->
255.254.20.36:53
 03/31-00:42:23.401521 [**] SYN-FIN scan! [**] 211.178.63.4:109 ->
255.254.53.36:109
```

6. European Regional Internet Registry/RIPE NCC (NET-RIPE-NCC-)

These addresses have been further assigned to European users.

Contact info can be found in the RIPE database, via the

WHOIS and TELNET servers at whois.ripe.net, and at

http://www.ripe.net/db/whois.html

NL

Netname: RIPE-NCC-212

Netblock: 212.0.0.0 - 212.255.255.255

Maintainer: RIPE

Coordinator:

Reseaux IP European Network Co-ordination Centre Singel 258 (RIPE-NCC-ARIN)

nicdb@RIPE.NET

+31 20 535 4444

Domain System inverse mapping provided by:

NS.RIPE.NET 193.0.0.193

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

NS.EU.NET	192.16.202.11
AUTH03.NS.UU.NET	198.6.1.83
NS2.NIC.FR	192.93.0.4
SUNIC.SUNET.SE	192.36.125.2
MUNNARI.OZ.AU	128.250.1.21
NS.APNIC.NET	203.37.255.97

To search on arbitrary strings, see the Database page on
the RIPE NCC web-site at http://www.ripe.net/db/

Record last updated on 16-Oct-1998.
Database last updated on 21-Jul-2001 23:13:10 EDT.

212.179.4.50 - This one was number two on the alerts "top talkers." It generated 6473 alerts against one destination and is on the "Watchlist IL-ISDNNET-6473" alert.

7. Clarity Connect Inc (NETBLK-CCI-NETWORK)
   200 Pleasant Grove Road
   Ithaca, NY 14850
   US

   Netname: CCI-NETWORK
   Netblock: 209.150.224.0 - 209.150.255.255
   Maintainer: CLCO

   Coordinator:
   Lalley, Joseph (JL583-ARIN) lalley@CLARITYCONNECT.COM
   607-257-8596

   Domain System inverse mapping provided by:

NS1.CLARITYCONNECT.COM	206.64.143.2
NS2.CLARITYCONNECT.COM	206.64.143.10

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

Record last updated on 04-May-2001.

Database last updated on 21-Jul-2001 23:13:10 EDT.

209.150.227.153 - This IP relates to the "Attempted Sun RPC highport access" alert. It generated 452 alerts against MY.NET's network.

8. ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-5)
   13241 Woodland Park Road
   Herndon, VA 20171
   US

   Netname: ROAD-RUNNER-5
   Netblock: 24.160.0.0 - 24.170.127.255
   Maintainer: SCRR

   Coordinator:
   ServiceCo LLC (ZS30-ARIN) abuse@rr.com
   1-703-345-3416

   Domain System inverse mapping provided by:

DNS1.RR.COM	24.30.200.3
DNS2.RR.COM	24.30.201.3
DNS3.RR.COM	24.30.199.7
DNS4.RR.COM	65.24.0.172

   Record last updated on 14-Jun-2001.
   Database last updated on 21-Jul-2001 23:13:10 EDT.

24.162.245.198 – This IP is the sole source of 109 "Back Orifice" alerts against 109 MY.NET destinations. Example:

```
03/26-14:37:58.116356 [**] Back Orifice [**] 24.162.245.198:1112 ->
255.254.1.113:31337
 03/26-14:37:58.245299 [**] Back Orifice [**] 24.162.245.198:1112 ->
255.254.1.127:31337
```


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

```
 03/26-14:37:58.476692 [**] Back Orifice [**] 24.162.245.198:1112 ->
255.254.1.161:31337
 03/26-14:37:58.513510 [**] Back Orifice [**] 24.162.245.198:1112 ->
255.254.1.167:31337
 03/26-14:38:00.336602 [**] Back Orifice [**] 24.162.245.198:1112 ->
255.254.2.76:31337
```

9. US Sprint (NETBLK-SPRINT-BLKB) SPRINT-BLKB 204.117.0.0 - 204.120.255.255

TELE-TECH COMPANY (NETBLK-FON-343023769634089) FON-343023769634089 204.117.70.0 - 204.117.70.255

204.117.70.5 came up on the "WinGate 1080" snort alerts. Example:

```
03/25-15:35:47.172891 [**] WinGate 1080 Attempt [**] 204.117.70.5:2630
-> 255.254.224.98:1080
 03/25-15:35:47.618701 [**] WinGate 1080 Attempt [**] 204.117.70.5:2630
-> 255.254.224.98:1080
 03/25-16:53:07.523742 [**] WinGate 1080 Attempt [**] 204.117.70.5:2671
-> 255.254.202.6:1080
 03/26-00:14:30.009645 [**] WinGate 1080 Attempt [**] 204.117.70.5:1709
-> 255.254.202.58:1080
```

10. Ethos Communications (NETBLK-ETHOS-NET001)

6404 International Pwky Ste 2200

Plano, TX 75093

US

Netname: ETHOS-NET001

Netblock: 209.217.0.0 - 209.217.63.255

Maintainer: ETHO

Coordinator:

Miller, Bill (BM378-ARIN) bcmiller@dallas.net

972-380-2202 (FAX) 972-380-0911

Domain System inverse mapping provided by:

NS1.CATALOG.COM 209.217.1.2

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

NS2.CATALOG.COM	207.240.40.2
NS3.CATALOG.COM	209.217.16.2

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 04-May-2000.
Database last updated on 21-Jul-2001 23:13:10 EDT.

209.217.53.190 – is the top dog for "External RPC calls" on the Snort alert logs, generating 81 alerts against 81 MY.NET destinations.

CORRELATIONS

http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc

http://www.sans.org/y2k/practical/David_Singer_GCIA.doc

http://www.sans.org/y2k/practical/Byron_Thatcher_GCIA.doc

http://www.sans.org/y2k/practical/Chris_Kuethe_GCIA.doc

http://www.sans.org/y2k/practical/Marc_Bayerkohler_GCIA.doc

http://www.sans.org/y2k/practical/Roland_GerlachGCIA.doc

http://www.sans.org/y2k/practical/David_Oborn_GCIA.doc

LINK GRAPH AND ANALYSIS OF OOS FILES

There are 3588 entries in the OOS files (This was determines by combining all the OOS files (using the *cat* command) and then doing the *grep* command: grep - -'->' alloos.txt | wc -l).

All the OOS files were TCP (100%).

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

Top Talkers:

- 211.178.63.4
- 24.169.230.194
- 217.3.182.110
- 24.10.199.253
- 158.75.57.4
- 128.186.112.90
- 193.11.231.49
- 24.108.146.141
- 24.22.21.90
- 213.76.185.130

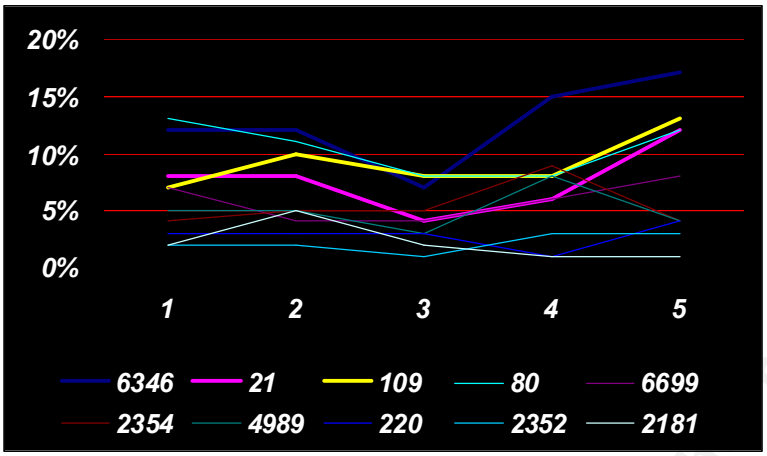
58% of the entries had the same source and destination ports.

The top ten probed ports:

- 6346 (12%)
- 21 (8%)
- 109 (7%)
- 80 (7%)
- 6699 (6%)
- 2354 (4%)
- 4989 (4%)
- 220 (4%
- 2352 (3%)
- 2181 (2%)

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

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



The above line graph represents the top ten ports that are accessed broken down by each day (April 2 – 6).

POSSIBLE COMPROMISED MACHINES

The following should be further investigated for possible compromise:

1. MY.NET.100.225 – Traffic from 216.136.171.195 targeted port 32771 and was reported as a "SunRPC highport access" alert.
2. The Back Orifice scans from 24.162.245.198 to MY.NET.21.0/24 and MY.NET.0.0/16. There were 109 alerts. It would be necessary to determine if anyone from MY.NET responded back.
3. The RAMEN server activity. Various MY.NET machines (MY.NET.209.86, MY.NET.221.26 and 28 others) responded back to external machines.

For the possible RAMEN worm infection, the machine should be reviewed for possible compromise. Since RAMEN usually infects Linux boxes, some of the commands that can be used include *netstat* and *lsof*. Both of these will help identify any active connections. If infected, the system will have to be rebuilt.

The same principles apply to the possible SunRPC highport access to port 32771.

Furthermore, the following is suggested in the Linux/Unix world:

- Review all pertinent logs
- Perform keyword searches
- Review relevant files
- Identify unauthorized user accounts or groups

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

- Identify rogue processes
- Check for unauthorized access points
- Analyze trust relationships

For Windows machines (Back Orifice) the following is suggested:

- Look for application logs not managed by the Windows Operating System.
- Look at the Event Viewer logs.
- Review the log files for each IIS service.
- Get a good file viewer, such as Quickview Plus (by JASC Software), to rapidly peruse suspect files.
- Review proprietary e-mail files, such as Outlook, Netscape Messenger, and AOL.
- Recover any deleted files and data throughout the system (Recycle Bin), including hidden files.
- Review the Registry files for the four major files: SAM, SECURITY, SOFTWARE and SYSTEM.
- Review the Swap file.
- Review Web Browser files
- Review Dial-Up networking

These suggestions, both Unix and Windows, were taken from Incident Response by Kevin Mandia and Chris Prosise (Osborne/McGraw Hill, 2001).

DEFENSIVE RECOMMENDATIONS

- Develop detailed security policies (see www.sans.org/newlook/resources/policies/policies.htm).
- Verify that computer equipment is *physically* secured.
- Implement an organizational Anti-viral policy that includes scanning at the server and desktop. Also consideration should be given to scan incoming e-mail and documents to prevent infection.
- Verify that no modems allow dial-in access to the network.
- Implement a firewall with a "deny all" policy. Periodically audit the firewall to ensure compliance with firewall rules.
- Implement an IDS such as Snort within MY.NET's network. Train (or outsource) someone to monitor these facilities on an on-going basis.
- Implement the suggested procedures, especially on border routers, in "Improving Security on Cisco Routers" available from www.cisco.com.
- Disable unnecessary services on key internal servers, especially RPC's.

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

- Verify that key e-commerce servers (if applicable), especially the Windows IIS servers, have the most current security patches.
- Consider access controls on key servers, such as Tripwire, TCPWrappers, SSH, etc.
- Obtain a vulnerability scanner, such as Nessus, and periodically run reviews to obtain a security "baseline." Make sure that any noted vulnerabilities are not exploitable outside of MY.NET.

ANALYSIS PROCESS

The Snort alert, scan, and OOS files were downloaded onto a Linux machine. This was done in order to use vi, awk, and perl. The particular files were then concatenated using the *cat* command. The result was three files: allalerts.txt, allscans.txt, and alloos.txt.

At first, the only Linux machine available had 64 mg. of RAM. Therefore, SnortSnarf (www.silicondefense.com) was not used (at first). I was able to run the perl program snort_sort.pl available from the www.snort.org page. To run:

./snort_sort.pl –r –w –h allalerts.txt

This program produced a nice HTML page summarizing (and detailing) the alerts. So at this point, I knew I had at least something to work with in case I would not be able to run SnortSnarf.

I was able to obtain a Linux machine with enough power to run SnortSnarf (a Sony Vaio with 192 mg. of RAM). This turned out to be one of the keys, at least for me, to completing this part of the assignment. Without this tool, I don't know how one could have completed the assignment since close to 20 mg. of data needed to be analyzed.

I followed the advice of others, in order to run SnortSnarf, and changed MY.NET to 255.254 by doing a global substitution using vi: s/MY.NET/255.254/g allscans.txt

SnortSnarf was run as follows: # ./snortsnarf.pl allscans.txt.

This was a mistake! This "hung" the computer and after about 5 hours, I rebooted. Actually, I was not able to reboot (CTRL-ALT-DEL) since the machine was totally unresponsive. I had to use the Magic SysRq keys: [Alt] [SysRq] [s][u][b]

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

The other option, and the one that worked, was to run each scan file separately. That is why in the Management Summary there are 5 scan files included instead of one. Once these ran, it was then fairly easy to analyze the scan data.

For the top talkers (alerts and scans) I used the perl code from **http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc** (with some slight modification) **,** specifically the top_talkers.pl.

For the OOS files, I also used a perl script (top_talkers_oos.pl) from **http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc .**

I modified the perl code to produce the top ports (OOS) and then did various *greps, awks*, *uniq*, and *sort –rn* to determine the percentages for the 5 April days. This resulted in the line graph. One thing I learned, I need to improve my perl skills to help manage the analysis process for Snort logs!

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

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