Global Information Assurance Certification Paper

Intrusion Detection Practical v 2.8a
Capitol SANS
Jon-Michael C. Brook
June 30, 2001

Assignment 1 (30 pts)

Overview:

The logs analyzed came from a small Internet café. They have a Class C registration. Their site performs web design and hosting in addition to email services; it has no restrictions or safeguards on entry. In early December, their ISP phoned with news that attacks on adult entertainment web sites originated from their IP address. At that time, they chose Black Ice Defender for a host based firewall system.

Black Ice Defender:

The logs provided contain twelve columns, ten by Black Ice and two for additional information. In depth information on Black Ice Defender is available at http://www.networkice.com/support/documentation.html.

Column one – Rule set violated
Column two – Date and time of latest violation
Column three – Attack Number
Column four – Attack Detected
Column five – Attacker Address
Column six – Attacker Name Resolution
Column seven – IP Address of Attackee
Column eight – Description of port attacked
Column nine – Attack parameters
Column ten – Count of attacks executed several times in a row
Column eleven – Attack severity
Column twelve – Results of Port scan of Attacker

Log Information:

The logs provided by the café began on installation in early December of Black Ice and continued through the end of December. Excerpts from the logs are used for this analysis.

Scan Information:

Attackers of the café's web server were scanned quickly (and politely) for open ports and services. This helps differentiate which attacker IP addresses were actually victims of someone else's malicious actions. SuperScan 3.00 was used for all scans, returning valuable IP addresses, open ports, and banner messages.

The café's Class C was also scanned, bringing to light the overburdened administrator's attempt at maintaining working computers rather than keep up to date on patches. The following table lists information obtained from scanning their address space.

IP Address	Port	Banner
10.10.10.1	80	HTTP/1.0 200 OK…
10.10.10.2	21 25 80 110	Microsoft FTP v. 4.0 NTMail v. 5.05.0002 IIS 4.0 POP 3 Server
10.10.10.31	21	Microsoft FTP v. 3.0
10.10.10.34	21 80	Microsoft FTP v. 4.0 IIS 4.0
10.10.10.49	21 80	Microsoft FTP v. 4.0 IIS 4.0

A whisker scan on the café's web server provided several non-available attacks and forbidden file reads. There was one exploit available against their cgi-bin directory.

There were five captures performed for this project:

Capture 1:

Rule SetDate & Time	Rule #Rule Desc	Attacker Addr	Attack Name	Attacked IP	Port Desc	Params	#
39 2000-12-25 08:04:16	2003016 RPC port probe	153.91.122.152		10.10.10.2			
39 2000-12-25 08:04:23	2003016 RPC port probe	153.91.122.152		10.10.10.130			
39 2000-12-25 08:04:23	2003016 RPC port probe	153.91.122.152		10.10.10.131			
39 2000-12-25 08:04:23	2003016 RPC port probe	153.91.122.152		10.10.10.132			
39 2000-12-25 08:04:23	2003016 RPC port probe	153.91.122.152		10.10.10.138			
39 2000-12-25 08:04:24	2003016 RPC port probe	153.91.122.152		10.10.10.146			
39 2000-12-25 08:04:24	2003016 RPC port probe	153.91.122.152		10.10.10.147			
39 2000-12-25 08:04:24	2003016 RPC port probe	153.91.122.152		10.10.10.148			
39 2000-12-25 08:04:24	2003016 RPC port probe	153.91.122.152		10.10.10.149			
39 2000-12-25 08:04:24	2003016 RPC port probe	153.91.122.152		10.10.10.150			
39 2000-12-25 08:04:24	2003016 RPC port probe	153.91.122.152		10.10.10.151			

39	2000-12-25 08:04:24	2003016 RPC port probe	153.91.122.152		10.10.10.152		
……		……	…	…	…	…	…

Attacks Continued

1. Source of Trace.

The logs analyzed came from a small Internet café. They have a Class C registration. Their site performs web design and hosting in addition to email services; it has no restrictions or safeguards on entry. In early December, their ISP phoned with news that attacks on adult entertainment web sites originated from their IP address. At that time, they chose Black Ice Defender for a host based firewall system.

2. Detect was generated by:

Black Ice Defender:

The logs provided contain twelve columns, ten by Black Ice and two for additional information. In depth information on Black Ice Defender is available at http://www.networkice.com/support/documentation.html.

Column one – Rule set violated
Column two – Date and time of latest violation
Column three – Attack Number
Column four – Attack Detected
Column five – Attacker Address
Column six – Attacker Name Resolution
Column seven – IP Address of Attackee
Column eight – Description of port attacked
Column nine – Attack parameters
Column ten – Count of attacks executed several times in a row
Column eleven – Attack severity
Column twelve – Results of Port scan of Attacker

3. Probability the source address was spoofed:

The source port was most likely not spoofed. The address of the attack is probably compromised, sporting the accessible Apache 1.3.12 and Red Hat Linux. With several Red Hat Vulnerabilities, and Apache buffer overflows found each day, the attacking IP could easily be compromised. For scanning to work with a spoofed IP, the attacker must be on the local segment of the return address, or on the local segment of the Café's LAN. Since the Internet Café is a closed location, it is unlikely this is the case. Again, the address of the attack was likely compromised, hiding any attackers true identity.

4. Description of attack:

The listed attack scanned every responding machine in the café's address space. The

attacker's scan gives indication of machines that are up, and targets Unix RPC services. The entire scan took 16 seconds. The last address on a tracert of the attacker's IP address led through cmsufire-bo.cmsu.edu, suggesting maybe a college student who couldn't make it home for Christmas. Any IDS sensor would easily detect this attack, however, by the time the administrator examines the logs (unless monitored 24x7 including Holidays), the compromise would already have occurred. Luckily, in this particular instance, the café's shop is all Windows based computers, which aren't vulnerable to these Unix RPC attacks.

5. Attack mechanism:

The attacker targeted port 111, the port designated for Unix RPC services. Several vulnerabilities exist through RPC, and the information provided by the RPC server will provide additional ports which may be compromised. Unix RPC services are turned on by default, and many users are more concerned with getting the machine working and less with how to secure it.

Most RPC based attacks consist of buffer overflows. Buffer overflows work by placing more information into a buffer variable than memory allocated for that buffer. When this occurs, the operating system may respond unexpectedly. In some instances, a command can be executed with root level privileges. This root level command can give an attacker an open entryway into the rest of the computer.

6. Correlations:

Many Remote Procedure Call service attacks are well known and thoroughly documented. An evening seminar at Capitol SANS was solely dedicated to the RPC service.

IANA:

SUN Remote Procedure Call portmap (TCP/UDP)

Advisories

1. March 2001, CERT/CC, http://www.cert.org/advisories/CA-2001-05.html Exploitation of snmpXdmid
2. Jan 2001, CERT/CC, http://www.cert.org/incident_notes/IN-2001-01.html, Widespread compromises via "ramen" toolkit. (TCP)
3. Nov 2000 (July 200), SecurityFocus, http://www.securityfocus.com/bid/1480
4. Sep 2000, CERT/CC, http://www.cert.org/incident_notes/IN-2000-10.html Widespread Exploitation of rcp.statd and wu-ftpd Vulnerabilities (TCP)
5. Sep 2000 (Aug 2000), CERT/CC, http://www.cert.org/advisories/CA-2000-17.html Input Validation Problem in rpc.statd
6. March 2000 (Dec 1999), CERT/CC, http://www.cert.org/advisories/CA-1999-16.html Buffer Overflow In Sun Solstice AdminSuite Daemon sadmind

7. Jan 2000 (Jul 1999), CERT/CC, http://www.cert.org/advisories/CA-1999-08.html Buffer Overflow Vulnerability in Calendar Manager Service Daemon, rpc.cmsd
8. Nov 1999 (June 1999), CERT/CC, http://www.cert.org/advisories/CA-1999-05.html vulnerability in statd exposes vulnerability in automountd
9. Sep 1999, CERT/CC, http://www.cert.org/advisories/CA-1999-12.html Buffer Overflow in amd (the Berkley Automounter daemon)
10. Nov 1998 (Oct 1998), CERT/CC, http://www.cert.org/advisories/CA-1998-12.html Remotely Exploitable Buffer Overflow Vulnerability in mountd
11. Jul 1999 (Sep 1998), CERT/CC, http://www.cert.org/advisories/CA-1998-11.html Vulnerability in ToolTalk RPC Service

Additional Information

- June 1998, RFC1057, http://www.faqs.org/rfcs/rfc1057.html, RPC: Remote Procedure Call Specification
- Aug 1995, RFC1833, http://www.faqs.org/rfcs/rfc1833.html, Binding Protocols for ONC RPC Version 2
- April 26, 2001, www.incidents.org says that this port is the fifth most frequently probed port in the past 30 days
- April 26, 2001, www.incidents.org says that this port is the third most frequently probed port in the past 7 days
- January 1999, http://www.cert.org/incident_notes/IN-99-01.html The sscan tool probes for this port. The sscan "port" signature is as follows:
  1. TCP ACK packets with source and destination ports set to 23, 25, 110, 143, 80
  2. If step one receivs a positive response, then port 80, (23, 143, 110 - all or none), 111, 6000, 79, 53, 31337, 2766. Then ports 139, 25, 21, 22, 1114, 1

7. Evidence of active targeting:

This attacker had previously determined which IP addresses were responding, possibly through a ping sweep. The attacker's scan gives indication of machines that are up, and targets Unix RPC services. However, nmap will perform a ping sweep prior to performing a port scan by default. This coupled with a scan for RPC services on an NT based network would not suggest much prior planning occurred for this attack.

8. Severity:

Overall Severity

2 – Non-targeted ineffective exploit

Criticality of target

5 – a web server at a web hosting company is relatively critical

Lethality

1 – Unix RPC Services are not ever present on an NT Machine. Unix exploits do not typically work on an NT box.

System Countermeasures

3 - older OS (NT Server) some patches missing including IIS patches, FTP older version, Host based firewall

Network Countermeasures

1 – None – no ACLs on outer router, fixed local passwords on several machines, multiple machines on the local subnet with hub connections, multiple un-patched services on several machines

9. Defensive recommendation:

The attack was stopped by the Black Ice host based firewall. However, the previous determination of IP address through an apparent ping sweep makes an attackers job entirely too easy. Nmap automatically performs this ping scan by default. Possibly blocking echo requests on either the machines themselves, or at the outer router may contribute to a bit more difficulty in site attack.

10. Multiple choice test question:

Which of the following point to the above detection being an automated attack?

a) # attacks
b) Rule Description
c) Date & Time
d) .edu attacker's domain name

a & c

Capture 2:

Rule Set	Date & Time	Rule #	Rule Desc	Attacker Addr	Attack Name
59	2000-12-22 09:39:33	2003104	Proxy port probe	165.121.72.134	user-2inii46.dialup.mindspring.com
59	2000-12-23 07:07:04	2003104	Proxy port probe	165.121.74.6	user-2iniig6.dialup.mindspring.com
59	2000-12-24 06:31:33	2003104	Proxy port probe	165.121.64.208	user-2inig6g.dialup.mindspring.com
59	2000-12-24 06:58:46	2003104	Proxy port probe	165.121.64.208	user-2inig6g.dialup.mindspring.com
59	2000-12-24 07:23:12	2003104	Proxy port probe	165.121.64.208	user-2inig6g.dialup.mindspring.com
59	2000-12-24 18:40:48	2003104	Proxy port probe	165.247.61.230	user-2iveff6.dialup.mindspring.com

59 2000-12-24 19:00:34	2003104 Proxy port probe	165.247.61.230	user-2iveff6.dialup.mindspring.com
59 2000-12-24 22:33:13	2003104 Proxy port probe	165.247.61.230	user-2iveff6.dialup.mindspring.com
59 2000-12-25 04:44:00	2003104 Proxy port probe	165.247.60.106	user-2ivef3a.dsl.mindspring.com
59 2000-12-25 06:08:06	2003104 Proxy port probe	165.121.76.184	user-2inij5o.dialup.mindspring.com
59 2000-12-25 06:20:29	2003104 Proxy port probe	165.247.60.106	user-2ivef3a.dsl.mindspring.com
59 2000-12-25 06:20:57	2003104 Proxy port probe	165.121.76.184	user-2inij5o.dialup.mindspring.com
59 2000-12-25 09:14:00	2003104 Proxy port probe	165.121.76.184	user-2inij5o.dialup.mindspring.com
59 2000-12-26 05:25:37	2003104 Proxy port probe	165.247.60.233	user-2ivef79.dsl.mindspring.com
59 2000-12-26 14:48:53	2003104 Proxy port probe	165.121.69.89	user-2inihap.dialup.mindspring.com
59 2000-12-27 05:40:44	2003104 Proxy port probe	165.247.60.186	user-2ivef5q.dsl.mindspring.com

1. Source of Trace.

The logs analyzed came from a small Internet café. They have a Class C registration. Their site performs web design and hosting in addition to email services; it has no restrictions or safeguards on entry. In early December, their ISP phoned with news that attacks on adult entertainment web sites originated from their IP address. At that time, they chose Black Ice Defender for a host based firewall system.

2. Detect was generated by:

Black Ice Defender:

The logs provided contain twelve columns, ten by Black Ice and two for additional information. In depth information on Black Ice Defender is available at http://www.networkice.com/support/documentation.html.

Column one – Rule set violated
Column two – Date and time of latest violation
Column three – Attack Number
Column four – Attack Detected
Column five – Attacker Address
Column six – Attacker Name Resolution
Column seven – IP Address of Attacked
Column eight – Description of port attacked
Column nine – Attack parameters
Column ten – Count of attacks executed several times in a row
Column eleven – Attack severity
Column twelve – Results of Port scan of Attacker

3. Probability the source address was spoofed:

The source address was likely not spoofed. For scanning to work, the attacker must be on the local segment of the return address. In a switched network, as is

DSL, being on a local segment is difficult without being at the address. This all supports the idea that the address was not spoofed. Instead, the addresses of the attacks are likely compromised. The attacker may be a Mindspring dialup user. As stated in Foundstone's Ultimate Hacking course, many attackers utilize dialup connections during attacks to create difficulties in identifying the final attacker. If this attacker only has dialup access, he has compromised two dsl accounts. This is a common problem with high-speed home Internet access; most users do not know the implications of connecting to the Internet. I personally have left notepad README messages on cable modem user's desktops suggesting security problems in their current configurations. A quick scan of the dsl connections reveals open ports on each of the dsl boxes, yielding access for covering the attacker's tracks.

4. Description of attack:

Proxy port probe. This attacker looked for proxy software. Proxy software is used to speed up Internet access or as a Firewall. This proxy software can be compromised, allowing an attacker to cover their tracks. A Trojan could also have been previously planted, listening to port 8080.

5. Attack mechanism:

Proxy servers/ Firewalls are typically seen as a "set it and forget it" solution to Internet access for small users. Dependent on the results of the probe, the manufacturer of the firewall or proxy server is typically displayed, as is often times the version. This is demonstrated by telneting into the proxy port and waiting for a response. Many vulnerability assessment tools, such as Nessus, Saint, and NetRecon will grab these banners and make the recommendation of performing a hexedit on the executable to change the displayed version number and information. These countermeasures are suggested in Foundstone's Ultimate Hacking course, as well as Scambray, McClure and Kurtz's *Hacking Exposed: 2nd Edition*. These modifications can make an attackers job more difficult. If this is the case, vulnerabilities for that specific product and version can be used, leaving considerably less work for the attacker.

Another manner of determining version information is by induction. NTMail, an smtp mail product from the UK, can be configured to provide proxy services on port 8080. The Café's web server also hosts their NTMail smtp service (See Café's Scan Information:). . This probe may be an attempt to locate the proxy server associated with the mail service.

The reason for the proxy probe above is the attacks on proxy software. Most proxy attacks are accomplished through buffer overflows. Buffer overflows work by placing more information into a buffer variable than memory allocated for that buffer. When this occurs, the operating system may react unexpectedly. Instead of killing the process, a command can be executed with root level privileges. This command can give an attacker an open entryway into the rest of the computer.

Proxy servers sometimes require passwords, subjecting themselves to password attacks. Enumeration of users through IPC$ shares can provide user names. A dictionary attack can check for weak passwords, or a brute force attack can attempt every number, letter, and special character combination. Another possible source is sniffing ftp or mail usernames and passwords from the additional open services on the web server (See Café's Scan Information:).

If a Trojan such as Windows NT's RingZero is listening to port 8080, the implications of the machine's compromise need assessing. This port was not, however open in the scans performed. An at (NT's version of cron) scheduled command would allow a port to open and close at certain hours of the day. This would place at least two new entries onto the system, furthering the possibility of detection. See Understanding the Attackers Toolkit by Sunnie Hawkins, www.sans.org/infosecFAQ/linux/toolkit.htm for more information on trojans.

6. Correlations:

This attack initially was not seen as a single effort, it may, in fact, not be. The Black Ice software did not automatically resolve the attack names. Upon name lookups on each of the IPs, the hostnames all resolved back to mindspring.com. The attacker possibly spread attacks across several days and several IP addresses, a method of avoiding detection by IDS products. The Internet Café's mail server previously had a proxy port open that they have since closed.

IANA

HTTP Alternate (see port 80) (TCP/UDP)

Trojans

1. RingZero

Other Known Uses

- Virtual Places Voice Chat (8000-9000)

Advisories

- May 2001, http://advice.networkice.com/advice/exploits/ports/8080/default.htm "This is a common port that contains HTTP servers and proxies. An imbedded management HTTP server that usually runs at this port, through which any file on the system can be retrieved. Puts a proxy server on this port". Also, NTmail uses port 8080 for proxy service. See http://www.ntmail.co.uk/ for more information.
- May 2001, http://www.securityfocus.com/bid/691.html,
- 16 May 2000, http://xforce.iss.net/alerts/vol-5_num-5.php, Vulnerability: cproxy-http-dos, Platforms Affected: Cproxy 3.3, Risk Factor: Medium, Attack Type: Network/Host Based, CProxy version 3.3 SP2 is vulnerable to a denial of service attack caused by a buffer overflow. CProxy is a Windows based proxy server,

developed by Computalynx. A local or remote attacker can crash the Cproxy server by sending a large amount of data to the HTTP service port (8080). Reference: BugTraq Mailing List: "CProxy v3.3 SP 2 DoS" at: http://www.securityfocus.com/templates/archive.pike?list=1&msg=007d01bfbf48$e44f0e40$01dc11ac@peopletel.org

- 10 Nov 2000, (Aug 1998), Cisco Bug ID CSCdk39378, The Cisco PIX Firewall product is shipped with a management application known as PIX Firewall Manager, or PFM. PFM is a Worldwide-Web-based application, and includes a limited HTTP server. The PFM HTTP server runs on Windows NT computers. A vulnerability in the PFM HTTP server allows any attacker who can connect to the server to retrieve any file known in advance to exist on the Windows NT host. In almost all cases, this means that the host is vulnerable to attack by any user inside the firewall, but not by users outside the firewall.

7. Evidence of active targeting:

There is the possibility that each of these attacks was perpetrated by separate users, but it is unlikely multiple hackers from the same ISP are going to hit the same victim in the same short (relatively) time span. The attack may be targeted as the Internet Café had previously kept a proxy server running with their mail product. This had since been shut off. This sweep might be an effort of finding this closed port.

8. Severity:

Overall Severity

4 – Non-targeted ineffective exploit

Criticality of target

5 – a web server at a web hosting company is relatively critical

Lethality

3 – Proxy software for a buffer overrun is not present on the machine; ntmail is, which has an associated proxy port. A Trojan may be on the machine, but it is more likely the association with ntmail.

System Countermeasures

3 - older OS (NT Server) some patches missing including IIS patches, FTP older version, Host based firewall,

Network Countermeasures

1 – None – no ACLs on outer router, fixed local passwords on several machines, multiple machines on the local subnet with hub connections, multiple un-patched services

on several machines

9. Defensive recommendation:

The attack was blocked by the firewall.

10. Multiple choice test question:

Why would an attacker use a dialup connection?

a) attack tools are just as easily scripted in command shells
b) the dialup provider creates another step in forensic determination to find the hacker
c) faster connection speed than dsl or T1
d) you don't have to go through the complexities of setting up a modem
e) people can't call you and bug you

a & b

Capture 3:

Rule SetDate & Time	Rule #Rule Desc	Attacker Addr	Attack Name	Attacked IP
39 2000-12-22 19:16:04	2001602 HTTP login failed	164.138.85.48	tours-9-48.abo.wanadoo.fr	10.10.10.2
59 2000-12-22 21:49:16	2003104 Proxy port probe	164.138.85.48	tours-9-48.abo.wanadoo.fr	10.10.10.2
39 2000-12-22 22:57:58	2001602 HTTP login failed	164.138.85.48	tours-9-48.abo.wanadoo.fr	10.10.10.2
39 2000-12-23 09:08:04	2001602 HTTP login failed	164.138.23.193	orleans-13-193.abo.wanadoo.fr	10.10.10.2
39 2000-12-23 11:39:58	2001602 HTTP login failed	164.138.23.202	orleans-13-202.abo.wanadoo.fr	10.10.10.2
39 2000-12-25 15:07:50	2001602 HTTP login failed	164.138.85.23	tours-9-23.abo.wanadoo.fr	10.10.10.2
39 2000-12-25 18:38:28	2001602 HTTP login failed	164.138.23.5	orleans-13.5.abo.wanadoo.fr	10.10.10.2
59 2000-12-25 18:55:12	2003104 Proxy port probe	164.138.23.5	orleans-13.5.abo.wanadoo.fr	10.10.10.2
39 2000-12-25 21:52:24	2001602 HTTP login failed	164.138.23.5	orleans-13-5.abo.wanadoo.fr	10.10.10.2
59 2000-12-25 22:00:32	2003104 Proxy port probe	164.138.23.5	orleans-13.5.abo.wanadoo.fr	10.10.10.2
39 2000-12-27 18:10:23	2003102 TCP port probe	164.138.182.57	tours-10-57.abo.wanadoo.fr	10.10.10.2

1. Source of Trace.

The logs analyzed came from a small Internet café. They have a Class C registration. Their site performs web design and hosting in addition to email services; it has no restrictions or safeguards on entry. In early December, their ISP phoned with news that attacks on adult entertainment web sites originated from their IP address. At that time, they chose Black Ice Defender for a host based firewall system.

2. Detect was generated by:

Black Ice Defender:

The logs provided contain twelve columns, ten by Black Ice and two for additional information. In depth information on Black Ice Defender is available at http://www.networkice.com/support/documentation.html.

Column one – Rule set violated
Column two – Date and time of latest violation
Column three – Attack Number
Column four – Attack Detected
Column five – Attacker Address
Column six – Attacker Name Resolution
Column seven – IP Address of Attackee
Column eight – Description of port attacked
Column nine – Attack parameters
Column ten – Count of attacks executed several times in a row
Column eleven – Attack severity
Column twelve – Results of Port scan of Attacker

3. Probability the source address was spoofed:

This attacker's address is likely not spoofed. In order for port probes and password attacks to work easily, the attacker must be on the local segment of the return address. In a switched network, being on a local segment is difficult without being at the address. All of this is covered by the discussion in segmentation in Sybex's CCNA study guide, and general TCP/IP literature. This all supports the idea that the addresses were not spoofed.

4. Description of attack:

In this capture there are failed HTTP logon attempts and port scans from France. These attacks appear to be from dial-in accounts, as evidenced by the numbers after the names, tours-x-x and orleans-x-x. This nomenclature is typically due to the high-capacity dial-in or dsl aggregation hardware used.

Even with Black Ice monitoring failed logins, the attacks and attempts following these could still have been successful. Login attempts following these would look like a typical web login. Without a stateful firewall or IDS system monitoring the network, the web servers have to serve web pages requested without the knowledge of failed logins. Black Ice has an auto-shunning feature that would disallow the IP address to make any more connections after a user-settable number of possible attacks. This was not set at the Café, so if multiple failed logins are noted as above, the web logs must be checked manually to determine if

suspicious logins followed. And this is only if the IIS server is setup to log logins, which they are not at the Café.

There is another possibility. Each web site with end user customizable data relies on a backend cgi or asp type program to parse the data entered. Web sites are written by programmers, and have the possibility of containing errors in the customizable fields. Making sure the information an end user enters is proper is the responsibility of the programmers. The failed HTTP logins seen in this detect may be attempts at overrunning a programmer's buffer field. If an overrun occurs, the operating system may react unexpectedly, returning system administrator access. Additionally, the Café was running IIS 4.0, which unpatched, has several buffer overflow conditions. Some of these overflows consist of attempted logins.

Buffer overflows and weak passwords will always be potential points of entry. A Ziff-Davis news story (news.zdnet.co.uk/story/o,,s2090250,00.html) by Wendy McAuliffe on June 28, 2001 describes the password vulnerabilities of most computer users. Over 125 usernames and passwords were attempted in the three days cited above. The usernames and passwords could easily have been aquired through sniffing the ftp or mail connections (See Café's Scan Information:). The TCP Probe and Proxy Probe conditions, coupled with all the source addresses suggest that all of these attempts are malevolent.

5. Attack mechanism:

HTTP login failed's could be evidence of buffer overflows or password attempts on the server. If this were an attempt at a buffer overflow, Black Ice would likely display different information.

That said, web pages secured by passwords are susceptible to brute force attacks, and should follow the suggestions for strong passwords. These include increased length, increased complexity (numbers, upper & lower cased characters, symbols) and frequency of password changes.

6. Correlations:

HTTP password attempts are quite common, and are the reason the café installed Black Ice Defender in the first place. Someone was doing from their site (attacking web site passwords) what is above illustrated happening to their site.

IANA:

World Wide Web HTTP (TCP/UDP)

Aug 1998, RFC2396

http://www.faqs.org/rfcs/rfc2396.html, Uniform Resource Identifiers (URI): Generic Syntax

Advisories

1. 15 May 2001, CERT/CC, http://www.cert.org/advisories/CA-2001-12.html, CERT Advisory CA-2001-12 Superfluous Decoding Vulnerability in IIS, (references RFC2396). Like all web servers, Microsoft IIS decodes input URIs to a canonical format. Thus, the following encoded string: "A%20Filename%20With%20Spaces" will get decoded to "A Filename With Spaces". Unfortunately, IIS decodes some of the input twice. The second decoding is superfluous. Security checks are applied to the results of the first decoding, but IIS utilizes the results of the second decoding. If the results of the first decoding pass the security checks and the results of the second decoding refer to a valid file, access will be granted to the file even if it should not be.

Trojans

1. Executor (TCP)
2. RingZero

Additional Information

- 01 Jun 2001, http://www.cisco.com/warp/public/707/arrowpoint-webmgmt-vuln-pub.shtml, A user can gain access to the web management interface without being authenticated on the CSS 11000 series switch. This vulnerability can be minimized by restricting http access to the CSS 11000 series switch.
- 01 May 2001, http://www.microsoft.com/technet/security/bulletin/MS01-023.asp, Windows 2000 introduced native support for the Internet Printing Protocol (IPP), an industry-standard protocol for submitting and controlling print jobs over HTTP. The protocol is implemented in Windows 2000 via an ISAPI extension that is installed by default as part of Windows 2000 but which can only be accessed via IIS 5.0. A security vulnerability results because the ISAPI extension contains an unchecked buffer in a section of code that handles input parameters. This could enable a remote attacker to conduct a buffer overrun attack and cause code of her choice to run on the server. Such code would run in the Local System security context. This would give the attacker complete control of the server, and would enable her to take virtually any action she chose. The attacker could exploit the vulnerability against any server with which she could conduct a web session. No other services would need to be available, and only port 80 (HTTP) or 443 (HTTPS) would need to be open. Clearly, this is a very serious vulnerability, and Microsoft strongly recommends that all IIS 5.0 administrators install the patch immediately.
- 26 April 2001, www.incidents.org says that this port is the sixth most frequently probed port in the past 30 days
- January 1999, http://www.cert.org/incident_notes/IN-99-01.html The sscan tool probes for this port. The sscan "port" signature is as follows:
  1. TCP ACK packets with source and destination ports set to 23, 25, 110, 143, 80
  2. If step one receivs a positive response, then port 80, (23, 143, 110 - all or none), 111,

6000, 79, 53, 31337, 2766.
3. Then ports 139, 25, 21, 22, 1114, 1

7. Evidence of active targeting:

This attacker is attempting several methods to gain access to the café's server. A proxy port probe, HTTP logins, and TCP port probes all are directed at the cafe from wanadoo.fr. Multiple methods over multiple days from multiple addresses with multiple attempts may lend itself to active targeting.

8. Severity:

Overall Severity

6 - Recon Probe and Targeted Exploit

Criticality of target

5 – a web server at a web hosting company is relatively critical

Lethality

5 – Multiple methods of attack on the same server, some of which are valid points of entry for administrative access.

System Countermeasures

3 older OS (NT Server) some patches missing including IIS patches, FTP older version, Host based firewall,

Network Countermeasures

1 – None – no ACLs on outer router, fixed local passwords on several machines, multiple machines on the local subnet with hub connections, multiple un-patched services on several machines

9. Defensive recommendation:

In a properly secured network, many of these attacks, including the TCP and proxy port probes should not be reaching the end host. They should be blocked with outer router ACLs. Additionally, port blocking and/or TCP wrappers should be in place on any machines that are internally trustedsuch as the Café's DNS or database machines. Finally, the firewall policies that did finally block these requests should be reviewed periodically for updates to the network architecture.

10. Multiple choice test question:

After examining the café's network infrastructure in section 8 and the scan information: at the beginning of this document, what would likely be the remote source (i.e. if you were attacking from France) for usernames and passwords used in the HTTP login failures?

a) social engineering
b) sniffing mail usernames and passwords from within the café's publicly accessible storefront
c) Recovering a SAM emergency repair disk
d) IPC$/Null session enumeration techniques

b, d

Capture 4:

Rule SetDate & Time	Rule #Rule Desc	Attacker Addr	Attack Name	At
39 2000-12-26 17:35:51	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:52	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:52	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:53	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:53	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39 2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10

39	2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39	2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39	2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39	2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39	2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39	2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39	2000-12-26 17:35:55	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10
39	2000-12-26 17:35:56	2003004 FTP port probe	202.180.88.239	202-180-88-239.iff6.attica.net.nz	10

Attacks on 53 Continued…

1. Source of Trace.

The logs analyzed came from a small Internet café. They have a Class C registration. Their site performs web design and hosting in addition to email services; it has no restrictions or safeguards on entry. In early December, their ISP phoned with news that attacks on adult entertainment web sites originated from their IP address. At that time, they chose Black Ice Defender for a host based firewall system.

2. Detect was generated by:

Black Ice Defender:

The logs provided contain twelve columns, ten by Black Ice and two for additional information. In depth information on Black Ice Defender is available at http://www.networkice.com/support/documentation.html.

Column one – Rule set violated
Column two – Date and time of latest violation
Column three – Attack Number
Column four – Attack Detected
Column five – Attacker Address
Column six – Attacker Name Resolution
Column seven – IP Address of Attackee
Column eight – Description of port attacked
Column nine – Attack parameters
Column ten – Count of attacks executed several times in a row
Column eleven – Attack severity
Column twelve – Results of Port scan of Attacker

3. Probability the source address was spoofed:

The source port was likely not spoofed. For scanning to work, the attacker must be on the local segment of the return address.

4. Description of attack:

This capture could be a major concern. The attacker began with a quick port scan of the

café's IP redirects. Each of the IP addresses above is a separate .com site. They all are then translated through a multihomed Nic on the Café's web server at 10.10.10.2. In mapping the remapped addresses, the attacker may be in hopes that a configuration error exists. The attacker appears to use a dialup account or some other dynamically assigned IP address for harder tracking. The timing of the attacks (120 packets are sent within three seconds) and precise numbers of packets (four to almost every IP address) sent suggest the attacker used some port scanner.

5. Attack mechanism:

The ports chosen are well-documented attacks, including Novell server exploits and some easily compromised Domain Name Servers.

DNS exploits include buffer overflows and route poisoning. Buffer overflows work by placing more information into a buffer variable than memory allocated for that buffer. When this occurs, a command can be executed with root level privileges. This command can give an attacker an open entryway into the rest of the computer. Route poisoning is not evidenced in the above detects.

The Novell exploit's (port 524) for all communication between Netware 5 clients-servers and time synchronization between server-server running IP. I suppose that an NCP requestor (i.e, Novell client) on the public side of a firewall could compromise a Novell server on the private side, especially if NDS or Bindery authentication information were known. See Novell TID 10013531 at http://support.novell.com. It should allow Internet access to your Novell file servers if they have IP access enabled.

6. Correlations:

DNS attacks were very popular following the Bind fiasco. This appears to be some sort of automated attack, searching DNS and NCP. Port 44767 has shown up with frequency on IDS newsgroups, dating back to May of 2000, with no final wording as to what it is. The first appearance can be found at http://www.sans.org/y2k/052400-1300.htm.

Port 53

IANA:

Domain Name Server, dns (TCP/UDP)

Nov 1987, RFC1035

http://www.faqs.org/rfcs/rfc1035.html, DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

Advisories

1. Feb 2001 (Nov 2000), CERT/CC, http://www.cert.org/advisories/CA-2000-20.html Multiple Denial-of-Service Problems in Internet Software Consortium (ISC) BIND
2. Jan 2001 (April 2000), CERT/CC http://www.cert.org/incident_notes/IN-2000-04.html DOS attacks using nameservers (primarily using UDP)
3. Sep 2000, CERT/CC, http://www.cert.org/advisories/CA-2001-02.html Multiple

Vulnerabilities in BIND

4. April 2000, CERT/CC, http://www.cert.org/incident_notes/IN-2000-04.html Continuing compromises of DNS servers
5. April 2000 (Nov 1999), CERT/CC, http://www.cert.org/advisories/CA-1999-14.html Multiple Vulnerabilities inBIND
6. Nov 1998 (Apri 1998), CERT/CC, http://www.cert.org/advisories/CA-1998-05.html Multiple Vulnerabilities inBIND

Additional Information

- 25 May 2001, http://www.usatoday.com/dns.htm, "USAToday.com has web server farms and associated domain name servers in several major cities of the U.S. To best serve our readership, we attempt to provide our content from the web servers which are best suited for a particular requestor. When someone views http://www.usatoday.com, they are redirected to one of our name servers at random and serviced from the web servers at that location. Thereafter, our load-balancing systems perform checks to determine which of our topographically closest co-location facilities to which we should direct future traffic from the given address. The systems use pings, dns queries, and traceroutes to determine best round-trip times, reliability checks, etc. You should be able to relate the times of the packets in question with any logs you may have in order to verify the occurrences. If you log outbound DNS queries, you should see the correlation. If this does not answer you concerns, please email us at support@usatoday.com."
- Subject: SYN/ACK to port 53 – "OK, this is beginning to drive me nuts. Since about February of this year, our firewall has been periodically hit with what can only be a probe, attack, whatever to port 53. Every time the scan exhibits the same behavior and is from the same set of IP addresses. A SYN/ACK packet is sent to TCP port 53. No SYN was sent from our system. The SYN & ACK sequence numbers appear to be random, but the ACK is always 1 less than the SYN. Our system responds with a RST to the ACK."
- 26 April 2001, www.incidents.org says that this port was the most frequently probed port in the past 30 days
- 26 April 2001, www.incidents.org says that this port is the sixth most frequently probed port in the past 7 days
- January 1999, http://www.cert.org/incident_notes/IN-99-01.html The sscan tool probes for this port. The sscan "port" signature is as follows:
  1. TCP ACK packets with source and destination ports set to 23, 25, 110, 143, 80
  2. If step one receivs a positive response, then port 80, (23, 143, 110 - all or none), 111, 6000, 79, 53, 31337, 2766
  3. Then ports 139, 25, 21, 22, 1114, 1
- If it's coming from Exodus, they may be using F5's 3dns server which does a null socket connect to your local dns servers using tcp to get rtt and latency. They (f5 3dns) uses this information to get the best response time and will load balance their servers behind accordingly. In your logs you will see port connects to tcp 53. I believe your fault is in how you think MS DNS works. Port 53 is used for the initial connection/request, then (in the NT implementation) a dynamic port (greater than 1023) for the reply back to the client.

- You should be okay. Usually only zone transfers are done over TCP.
  Vanja Hrustic wrote:
  > I've heard various comments on this, so I want to double-check it. Is it ok if only UDP/53 is left open, to serve DNS requests? As much as I have understood, I can safely close TCP/53. The server in question is a 'small' one (meaning: not so many requests per day, and only requests for www/dns/mail will probably come there anyway).
  >It is not a Microsoft issue. The RFC does say that. See RFC1035, sections 4.2.1 and 4.2.2. The MX record that your SMTP server was trying to pull down was probably more than 512 bytes, thus it resorted to TCP.

Port 524

IANA:

NCP (TCP/UDP)

Netware Core Protocol (NCP)

uses port 524 for all communication between Netware 5 clients-servers and time synchronization between server-server running IP. See Novell TID 10013531 at http://support.novell.com.

Port 4970

IANA:

Unassigned

Port 8080

IANA:

HTTP Alternate (see port 80) (TCP/UDP)

Trojans

2. RingZero

Other Uses

- Virtual Places Voice Chat (8000-9000)

Additional Information

- May 2001, http://advice.networkice.com/advice/exploits/ports/8080/default.htm "This is a common port that contains HTTP servers and proxies. An imbedded management HTTP server that usually runs at this port, through which any file on the system can be retrieved. Puts a proxy server on this port". Also, NTmail is listed as a reference – not sure why. I guess it must use port 8080 for proxy service. See http://www.ntmail.co.uk/ for more information.
- May 2001, http://www.securityfocus.com/bid/691.html,
- 16 May 2000, http://xforce.iss.net/alerts/vol-5_num-5.php, Vulnerability: cproxy-http-dos, Platforms Affected: Cproxy 3.3, Risk Factor: Medium, Attack Type: Network/Host Based, CProxy version 3.3 SP2 is vulnerable to a denial of service attack caused by a buffer overflow. CProxy is a Windows based proxy server, developed by Computalynx. A local or remote attacker can crash the Cproxy server

by sending a large amount of data to the HTTP service port (8080). Reference: BugTraq Mailing List: "CProxy v3.3 SP 2 DoS" at: http://www.securityfocus.com/templates/archive.pike?list=1&msg=007d01bfbf48$e44f0e40$01dc11ac@peopletel.org

- 10 Nov 2000, (Aug 1998), Cisco Bug ID CSCdk39378, The Cisco PIX Firewall product is shipped with a management application known as PIX Firewall Manager, or PFM. PFM is a Worldwide-Web-based application, and includes a limited HTTP server. The PFM HTTP server runs on Windows NT computers. A vulnerability in the PFM HTTP server allows any attacker who can connect to the server to retrieve any file known in advance to exist on the Windows NT host. In almost all cases, this means that the host is vulnerable to attack by any user inside the firewall, but not by users outside the firewall.

Ports 49142 – 65535.

IANA:

The Dynamic and/or Private Ports are those from 49152 through 65535

7. Evidence of active targeting:

Within 20 seconds, the entire café's network was scanned. Additionally, the only machines that were scanned were IP addresses linked to the same NIC as the web server.

8. Severity:

Overall Severity

6 – Targeted, Possibly Ineffective Exploit

Criticality of target

5 – a web server at a web hosting company is relatively critical

Lethality

5 – FTP exploits on a server with FTP can give administrative access, as can previously installed Trojans

System Countermeasures

3 - older OS (NT Server) some patches missing including IIS patches, FTP older version, Host based firewall,

Network Countermeasures

1 – None – no ACLs on outer router, fixed local passwords on several machines,

multiple machines on the local subnet with hub connections, multiple un-patched services on several machines

9. Defensive recommendation:

This too appears was blocked by the firewall. Maybe a one minute shun on scanning attackers would minimize the effectiveness of scanning on a network resource. Hopefully, a time of one minute will keep intentional spoofing from becoming the next fad attack.

10. Multiple choice test question:

What advantage does attacking a remapped IP address hold?

a) An IDS system may not be tuned for the remapped IP address
b) The real IP address is unknown
c) Misconfiguration of the secondary services on the multihomed NIC may lead to easier compromise
d) different services may be open on each remapped IP address

a & c

Capture 5:

Rule SetDate & Time	Rule #Rule Desc	Attacker Addr	Attack Name	Attacked IP
39 2000-12-24 08:08:56	2001602 HTTP login failed	211.110.80.18	…thrunet.ne.kr	10.10.10.2
39 2000-12-24 13:08:13	2001602 HTTP login failed	211.110.80.18		10.10.10.2
59 2000-12-24 14:03:29	2000317 TCP SYN with URG flag	211.110.80.18		10.10.10.2
39 2000-12-24 14:05:52	2001602 HTTP login failed	211.110.80.18		10.10.10.2
59 2000-12-24 14:43:30	2003104 Proxy port probe	211.110.80.18		10.10.10.2
59 2000-12-24 18:53:59	2003104 Proxy port probe	211.110.80.18		10.10.10.2
59 2000-12-24 21:24:06	2000313 TCP OS fingerprint	211.110.80.18		10.10.10.2
39 2000-12-24 21:25:19	2001602 HTTP login failed	211.110.80.18		10.10.10.2
59 2000-12-25 03:42:59	2000318 TCP Invalid Urgent offset	211.110.80.18		10.10.10.2
59 2000-12-25 03:43:29	2000313 TCP OS fingerprint	211.110.80.18		10.10.10.2
39 2000-12-25 03:44:08	2001602 HTTP login failed	211.110.80.18		10.10.10.2
39 2000-12-27 05:12:35	2001602 HTTP login failed	211.110.80.18		10.10.10.2
59 2000-12-27 05:37:27	2003104 Proxy port probe	211.110.80.18		10.10.10.2
59 2000-12-27 18:20:41	2002561 .htaccess URL	211.110.80.18		10.10.10.2
59 2000-12-27 18:20:41	2000617 HTTP URL contains /...	211.110.80.18		10.10.10.2
59 2000-12-27 18:56:00	2000313 TCP OS fingerprint	211.110.80.18		10.10.10.2
39 2000-12-27 18:57:17	2001602 HTTP login failed	211.110.80.18		10.10.10.2

1. Source of Trace.

The logs analyzed came from a small Internet café. They have a Class C registration. Their site performs web design and hosting in addition to email services; it has no restrictions or safeguards on entry. In early December, their ISP phoned with news that attacks on adult entertainment web sites originated from their IP address. At that time, they chose Black Ice Defender for a host based firewall system.

2. Detect was generated by:

Black Ice Defender:

The logs provided contain twelve columns, ten by Black Ice and two for additional information. In depth information on Black Ice Defender is available at http://www.networkice.com/support/documentation.html.

Column one – Rule set violated
Column two – Date and time of latest violation
Column three – Attack Number
Column four – Attack Detected
Column five – Attacker Address
Column six – Attacker Name Resolution
Column seven – IP Address of Attackee
Column eight – Description of port attacked
Column nine – Attack parameters
Column ten – Count of attacks executed several times in a row
Column eleven – Attack severity
Column twelve – Results of Port scan of Attacker

3. Probability the source address was spoofed:

The source port was likely not spoofed. For scanning to work, the attacker must be on the local segment of the return address. Since the IP addresses do not change, the information is probably being sent back to the Korean address. Whether the Korean machine is compromised in an attempt to cover the attacker's tracks is another story. The attacking IP address resolved to thrunet.ne.kr, possibly lending towards the machine's raison d'etre.

4. Description of attack:

All of the packets seen in this detect are attempts to compromise the web server through the SQL port. In this capture there are failed HTTP logon attempts and port scans. An nslookup on this attacker has him located in Korea, but a tracert stops registration information six + hops before the IP address. This may be due to an outer router with appropriate ACLs which block tracert. HTTP login failed attempts may be attacks with sniffed ftp or mail account usernames and passwords (See Café's Scan Information:).

Even with Black Ice monitoring failed logins, the attacks and attempts following these could still have been successful. Login attempts following these would look like a typical web login. Without a stateful firewall or IDS system monitoring the network, the web servers have to serve web pages requested without the knowledge of failed logins. Black Ice has an auto-shunning feature that would disallow the IP address to make any more connections after a user-settable number of possible attacks. This was not set at the Café, so if multiple failed logins are noted as above, the web logs must be checked manually to determine if suspicious logins followed. And this is only if the IIS server is setup to log logins, which they are not at the Café.

There is another possibility. Each web site with end user customizable data relies on a backend cgi, asp, or vbscript type program to parse the data entered. This interfaces into the SQL database through port 1433. Web sites are written by programmers, and have the possibility of containing errors in the customizable fields. Making sure the information an end user enters is proper is the responsibility of the programmers. The failed HTTP logins seen in this detect may be attempts at overrunning a programmer's buffer field. The attacker may be attempting to determine if the information is parsed prior to the username password checked. If an overrun occurs, the operating system may react unexpectedly, returning system administrator access. Additionally, the Café was running IIS 4.0, which unpatched, has several buffer overflow conditions.

Buffer overflows and weak passwords will always be potential points of entry. A Ziff-Davis news story (news.zdnet.co.uk/story/o,,s2090250,00.html) by Wendy McAuliffe on June 28, 2001 describes the password vulnerabilities of most computer users. Over 235 usernames and passwords were attempted in the three days cited above. The usernames and passwords could easily have been acquired through sniffing the ftp or mail connections (See Café's Scan Information:). The TCP Probe and Proxy Probe conditions, coupled with all the source addresses suggest that all of these attempts are malevolent.

TCP Syn w/ Urg Flag

The TCP SYN w/ URG flag may be an attempt to create an overflow condition with the web server's IP stack. The web server's IP stack could wreak havoc and give elevated privileges or allow arbitrary code execution.

TCP OS fingerprint

TCP OS fingerprinting, is defined in Foundstone's *Ultimate Hacking* course as using "differences between vendor IP stack implementations" to guess the Operating System. The TCP OS Fingerprinting occurs three times after attempted logins fail. Typically, according to Scambray, McClure and Kurtz's *Hacking Exposed: 2nd Edition*, the potentially vulnerable services or "low-hanging fruit"

should be addressed first. TCP OS fingerprinting allows an attacker to quickly define which attacks may be successful against a given system, identifying which services are vulnerable on those systems.

.htaccess URL

The .htaccess files are one manner of securing an Apache web server. These files can be manipulated to allow ssl only connections, restrict access to hosted web pages only by certain IP addresses, or require authentication for web sites. All of these entries can be modified if write access to the .htaccess file is granted. If only read access is available, an attacker can examine what permissions are allowed on sites hosted, and possibly find a configuration error.

HTTP URL contains /...

A directory traversal mechanism can allow the attacker to access the SAM files stored in the repair directory. This can allow later access to the machine. Alternatively, the possibility of attempting to access a /… directory, instead of the /. or /.. directories gives a location for root kit files to be stored.

Conclusion

If these attacks were closer together in time (an hour rather than three days) these attacks could more easily be attributed to a whisker or nessus scan. There are timing options on these attack tools, but the attacks seen above exhibit a large amount of interest (detected attacks), followed by a couple of light days.

5. Attack mechanism:

HTTP login failed

The HTTP login failed attempts are looking for weak username and password combinations. Usernames and passwords can be sniffed from the Café's customers' mail account access, or from the ftp server hosted on the same machine.

HTTP URL contains /…

The HTTP URL contains /… can be a directory traversal mechanism. Web servers serve files through http traffic. These documents can be of any format, from html commonly seen in web pages, to java applets, to binary files. A directory traversal mechanism requires two things to occur in order for files of importance to be accessed. The web server that the traversal exploit is being attempted against must allow directory traversal. According to Scambray, McClure and Kurtz's *Hacking Exposed: Second Edition*, "When you choose to install sample ASP code during a default installation of IIS 4.0, a number of poorly programmed sample files allow attackers to download another file's source. The problem lies in the scripts inability to restrict the use of ".." in the file's

path." The showcode.asp and codebrws.asp were definitely part of the default installation originally performed at the Café. The directory traversal feature /.. can be useful, allowing usage similar to ftp sites. however, iff a directory structure does not have the proper directory permissions, the /.. and showcode or codebrws enable an html request to access the directory above its current position, even outside of the web server's designated directory. Files that may be of interest may include the bin.ini files or the SAM files stored in the repair directory.

On Unix machines, /… can easily be mistaken for /.. by a system administrator. After performing an ls, /., /.. always appear. After installing a rootkit, an easy hiding mechanism (and one used in Foundstone's *Ultimate Hacking* lab) is placing files into "/…".

.htaccess

The .htaccess files are one manner of securing an Apache web server. These files can be manipulated to allow ssl only connections, restrict access to hosted web pages only by certain IP addresses, or require authentication for web sites. All of these entries can be modified if write access to the .htaccess file is granted. If only read access is available, an attacker can examine what permissions are allowed on sites hosted, and possibly find a configuration error.

TCP OS fingerprint

TCP OS fingerprinting, is defined in Foundstone's Ultimate Hacking course as using "differences between vendor IP stack implementations" to guess the Operating System. These IP stack implementation differences included sending the first 64 bytes of a packet back as the data in an ICMP error message vs. sending all zeros. The TCP OS Fingerprinting occurs three times after attempted logins fail. Typically, according to Scambray, McClure and Kurtz's *Hacking Exposed: 2nd Edition*, the potentially vulnerable services or "low-hanging fruit" should be addressed first. TCP OS fingerprinting allows an attacker to quickly define which attacks may be successful against a given system, identifying which services are vulnerable on those systems.

TCP Invalid Urgent offset/ TCP SYN with URG flag

Along the lines of TCP OS fingerprinting are invalid packets. These packets are not expected in typical IP communication, and some IP Stacks have inadequate checking mechanisms. These invalid IP packets may have unexpected results due to the inadequate checking, crashing the IP stack, which in turn may allow arbitrary execution of code, or take down the server, effectively causing a DoS.

The attackers are actively targeting the web server. However, it would appear, if all these attacks are being individually executed (examine the times of attack), that it is an inexperienced attacker. The IIS 4.0 banner from the Café's server appears with a simple

telnet and HTTP GET command. This banner would limit the attacks attempted, or at least vary the order to attempt the Wintel/IIS hacks first.

6. Correlations:

IANA:

Microsoft-SQL-Server (TCP/UDP)

Additional Information

- Sometimes NT administrators will leave the SQL Server with the default admin account "sa" and no password Allows SQL Access using port 1526
- CVE 1999-0276 mSQL v2.0.1 buffer overflow = remote exe
- CVE 1999-0753 Allowance of viewing restricted directories
- CVE 1999-0999 Microsoft SQL 7.0 allows DoS w/ Malformed Packets
- CVE 2000-0161 Sample Web sites don't validate properly and allow remote SQL queries
- CVE 2000-0202 SQL 7.0 & MSOE Allow Privileges gained via malformed SQL queries

7. Evidence of active targeting:

Each of these attacks is specifically slated for the café's backend SQL server web interface. The OS fingerprinting attempts will better differentiate which version of Microsoft's SQL is used, better providing buffer overflows and administrator access to the attacker. Several of the attacks are web server attacks, which, when applied against the correct type of web server, may provide information or access unintended by the system's administrator.

8. Severity:

Overall Severity

6 – Targeted, Possibly Ineffective Exploit

Criticality of target

5 – a web server at a web hosting company is relatively critical

Lethality

5 – SQL buffer overflow conditions will provide administrative access across the network

System Countermeasures

3 - older OS (NT Server) some patches missing including IIS patches, FTP older version, Host based firewall,

Network Countermeasures –

1 – None – no ACLs on outer router, fixed local passwords on several machines, multiple machines on the local subnet with hub connections, multiple un-patched services on several machines

9. Defensive recommendation:

By knowing the location of the café's SQL port, defensively, the system has failed. Too much information has been leaked without obvious work done by the attacker. Many of these attacks should not be reaching the end host. They should be blocked with router ACLs, port blocking on any trusted machines, and the firewall policies that did finally block these requests.

10. Multiple choice test question:

Why should strings such as "/.." be searched for by IDS systems?

a) the location /… offers a hiding spot for root kits
b) A buffer overflow may result in web applications
c) the characters are unique passwords
d) Domain name servers proxy ports

a & b

Assignment 2 – Describe the State of Intrusion Detection (30 Points)

Intrusion Detection Management in an Enterprise Environment

As networks grow in size and complexity, the information they provide follows accordingly. Management of an enterprise network is reasonably well documented. The goal for all enterprise products is to control more information, more efficiently with an elegant, intuitive design. Most corporations have only recently begun deploying Commercial Off-The-Shelf (COTS) Intrusion Detection Systems (IDS) on an enterprise scale (greater than 200K nodes), with the largest current project, the Navy/Marine Corps' Intranet network, approaching 500 thousand users and over 750 thousand nodes. This document discusses the unique problems associated with the management of an enterprise-wide intrusion detection system.

Multiple Products

Several vendors offer intrusion detection products, with more entering the arena each day. NIST's Special Publication on Intrusion Detection Systems classifies these IDSs by how they detect intrusions, and where they are located. Intrusion Detection Systems look for misuse or anomalies, and are either network based, host based, or application based. For a more detailed discussion, please see the NIST IDS publication.

Advantages \Disadvantages of different products

Enterprise environments can be difficult to manage. Homogenous networks ease a considerable amount of these complications. Everything is designed and tested to work with itself proprietarily. NIST comments, "Different Commercial IDSs rarely interoperate with each other, so you may not be able to consolidate your IDSs across your enterprise if you use more than one vendor's IDS. However, in the event of a newly discovered attack applicable to that network, homogeneity presents a more vulnerable front.

The same can be said of IDS deployments. Having IDS sensors that detect through attack signatures will not detect the newest 0-Day Hacks. Likewise, anomaly detection may not catch well-known attacks that look like proper, legitimate traffic. What one product doesn't catch, the others may. With Intrusion Detection, missing one attack can constitute a compromise.

Console requirements

In an enterprise environment, relying on one product increases the possibility of compromise. Multiple products increase the overall cost. Multiple products require

multiple sensors with careful placement so that each product performs its specific job best. In the Security Operations Center (SOC), the neural control center for an enterprise network operation, each product will require some sort of console and operator to provide its view of the current network status and possible intrusions. As a cost saving feature, more and more of today's consoles are using web interfaces to decrease the total cost.

Scalability \ Hierarchical design

Enterprise environments require scalability. Each sensor collects information. Communicating this information up to the final operator using as few network resources is important. A general information flow sends data from the sensors to some sort of manager of the data (typically a database), and sends it upwards until it reaches the final console. The NIST Special Publication on Intrusion Detection Systems states, "…many IDSs are not able to scale to large or widely distributed enterprise network environments."

As most commercial IDS systems are still in their infancy (as compared to PCs or Operating Systems), scalability has been of minor concern. Companies thus far appear to be more concerned with getting the technology working, then concentrating on scalability. Regionalizing SOCs across the enterprise can ease commercial IDS deployment, but enterprise environments must scale.

Stick

Scalability issues can be exacerbated when IDS systems themselves are attacked. One of the popular attack tools listed on Packetstorm's website (packetstorm.securify.com) is the stick attack tool. This tool takes the current Snort signature database (www.snort.com) and generates packets based on the signatures. The IP address for attack can be specified, as can the IP source. By default the source IP addresses are randomly generated, as are the destination addresses. The tool is designed to generate a Denial of Service against an IDS system. Many of the packets are valid packets, so they won't be discarded by outside routers. The internal addresses can be dispersed across a class A, B, or C space, so they will appear on the IDS sensors as internal targets. The Snort database used for the attacks is a flat text file, and can be modified easily to eliminate attacks that will obviously not get through a network (traceroute when an attempted traceroute is blocked at the outside router).

Modular components

Examples of scalability problems with commercial IDS systems are numerous. Three well-known products in the IDS arena are Cisco's Secure IDS (formerly known as Net Ranger), Symantec's Net Prowler, and ISS's Real Secure.

Cisco Secure IDS

Cisco's Secure IDS, aka Net Ranger, was the first commercial IDS product available. Net Ranger sensors are appliances based on x86 Solaris, or switch blade modules that fit into Cisco's 6500 series switches. Cisco has released two separate products to control Net Ranger sensors. The first, Cisco's Secure Policy Manager, is a Windows based GUI that displays spreadsheet-formatted data for alarms. It provides a console for approximately 15 Net Ranger sensors before the spreadsheet information provided becomes overwhelming in large attacks. In an enterprise environment, Cisco itself has pushed CSPM out of the picture with its inability to control the switch blades.

The other console product for Net Ranger, Cisco's Secure Intrusion Detection System, relies on HP's OpenView for control. Each sensor is assigned a separate node on a graphical map. When an attack is detected, an alarm is displayed within the node.

As a control for Cisco's Net Ranger sensors, the Secure IDS system does have better enterprise capabilities. CSIDS can forward alarms with different severities up consoles in a hierarchical manner. This can alleviate the IDS analysts at a global SOC from being overwhelmed with regional SOC data. However, this information is also not available for examination by the global analyst if a large-scale attack occurs.

Using the aforementioned stick tool, only a few seconds of an attack on the OpenView product locks a Cisco console for upwards of 30 minutes while the sensor synchronizes alarm data on a dual processor Solaris Ultra 80. This is currently well above the minimum requirements for an HP OpenView console. HP Openview currently has an additional design problem arising out of the maximum 1024 alarms per graphical map representation. These 1024 alarms are difficult to read, as each alert is displayed as an icon, with the size of the icon growing increasingly small as the alerts per page increases. Upon completion of the 30-minute synchronization, the few seconds of a stick attack from one machine exceeds this 1K limit. Even without the stick tool, one thousand attacks can appear from an external Nessus scan or DoS attack originating from an Internet access point.

Net Prowler

Axent technologies developed the Net Prowler product for fast intrusion signature comparison. Net Prowler integrates seamlessly with Axent's Raptor Firewall, allowing automatic hardening and shunning of attacking IP addresses. In December 2000, Symantec Corporation purchased Axent, and thereby Net Prowler and Raptor. Net Prowler is designed somewhat hierarchically, with agents, managers and consoles. The agents collect information, process it against known attack signatures, and send alerts to the manager. The manager stores data in an SQL database, and when viewed by the

console, displays alerts to the end operator.

Net Prowler's best attribute is speed. Each Net Prowler agent is assigned a range of IP addresses to monitor. If a packet is not destined for that range, the sensor does not examine it. Net Prowler allocates memory on each sensor for every attack signature on each IP address that it is assigned to monitor. This allows incoming packets to quickly be compared against one row of a table in RAM, rather than traversing several relational databases.

The Net Prowler console is clean and easy to use. Net Prowler provides real-time alerts, and can capture and respond to sessions on the fly. It provides information on one manager at a time, equating to approximately 20 sensors. Each of these sensors is designed to accommodate one class C address space, or approximately 250 devices, but this is limited only by RAM and processor availability. Currently, a dual processor 1G Xeon processor machine with 2 GB of RAM can handle approximately 50 class C address spaces.

Unfortunately for scalability, the console's program cannot watch multiple managers simultaneously; instead, each manager can be watched in a separate window on the same desktop. Each manager handles about 20 sensors, limiting Net Prowler's deployment in a large, distributed enterprise environment. Additionally, the signature/IP table that each sensor loads into memory, grows exponentially, disallowing the deployment on anything larger than several class C segments without multiple gigabytes of RAM. Lastly, there is no option for console/analyst view only privileges. Anyone with access to the console has free reign over the entire deployment controlled by that manager.

Real Secure

ISS's Real Secure is generally deployed as an outsourced, managed intrusion detection operation. It is available for separate purchase, and therefore included here. However, in examining their implementation of Real Secure, the product relies on sensors and consoles. Any console with password access can access any sensor. This allows viewing privileges across the enterprise network. Only one console can be the "master" console, allowed to push policy and update attack signatures down to the sensors. Any console can take ownership of a sensor, allowing a mesh hierarchical design. Again, typically Real Secure appears as an outsourced intrusion detection service, so the scalability in an enterprise setting is of concern to ISS alone. However, each sensor can report to an unlimited number of consoles. Segmenting alerts into regions can be accomplished through this mesh hierarchy, but the actual deployment and management can become tiresome in larger, more complex networks.

Other Products

The aforementioned products effectively communicate with about 20 sensors. In an enterprise environment, hundreds to thousands of sensors must communicate efficiently, preferably without breaking the environment into 20 sensor chunks. These products have difficulty processing and storing data from sensors and displaying it in an understandable way. The enterprise wide solutions for Intrusion Detection event correlation are mainly from third party vendors. These vendors recognize the need for large event correlation from multiple sensors scattered across the enterprise network.

Management LAN vs. In Band

Most current network designs employ a layered approach for security. If an intruder does attempt penetration, a layered design requires the attacker to compromise several resources to reach sensitive information. Intrusion Detection systems send a great deal of sensitive data from all points of the network directly to a centralized NOC. This has the potential of bypassing the layered network design.

The first of two methods for sending sensor information back to the NOC is as out-of-band traffic. Out-of-band LANs are primarily used for network management. Out-of-band networks lend themselves well to intrusion detection data transfers. These networks are not available to outside viewers, and route easily to the servers in the central command. Information transferred does not interfere with data on the production network, and alerts sent to IDS consoles are direct and unseen.

Out Of Band

There are some drawbacks to out-of-band traffic. Typically, management networks are smaller in scale than production networks. The 10-base-t connection speed of general management LANs provides more than enough speed than network providers need to perform console configuration and TFTP transfers. However, transfers of large or frequent IDS data packets may clog the slower management LAN. Additionally, unless specified in Service Level Agreements, management networks are typically not fault tolerant. Without fault tolerance, SLAs for management LAN repair time may allow IDS data to sit unseen for hours.

In Band

In contrast, IDS information sent to the NOC can also be placed in-band. Fault tolerance and SLAs are requirements on enterprise networks. Normally outsourced in large organizations, network resources such as large bandwidth and quality of service allow enterprise environments to run smoothly. VPN designs and IPsec transfers keep prying eyes from snooping IDS data. As a result, intrusion detection information is quickly, easily, and securely transferred.

In-band IDS traffic does place heavy concerns on security analysts. If an attacker notices

traffic after each attack, they are privy to the fact that an Intrusion Detection System is in place. In fact, they may even be capable of discerning which product is implemented, fingerprinting information in the same manner used by Nmap for OS enumeration. Also, attacks that are not monitored will not garner traffic responses, aiding the hacker in eluding enterprise wide detection. If an attack does provide a traffic response, a Denial of Service can be launched on some network resource and the network itself simultaneously. Or news of the attack through IDS information may be denied Central Command by a second attack on a network resource in between the consoles and sensors.

Disaster Recovery

All IDS information is useless if it cannot be communicated. In the event of a problem, quick recovery, or automatic fail-over is key in preventing the loss of data. Otherwise, every attack would begin with a calculated disaster disrupting the reporting capabilities of the intrusion detection systems. Fail over in enterprise intrusion detection arenas requires adequate protections on each of the sensors, managers, and consoles.

Remote control of Sensors

Enterprise IDS components must be as hands off and effortless as possible. Each trained technician's service call costs an enterprise, and must be avoided. Remote control of IDS devices is attained through the product's console, serial access, or telnet type access. Some of these solutions are more secure than others, implementing transmission encryption and/or authentication.

Fail over

Fail over in enterprise environments takes possible situations from serious to when convenience. Scheduling a technician a day ahead for replacement of a failed device rather than on call for an hour gives enterprise managers options to remain within SLAs. Fail over techniques for agents and managers allow cold spare, one-to-one, or one-to-many replacement. Cold spares require fully configured boxes that are hand delivered and updated with the settings of the failed device. They are a very little improvement over the technicians on site troubleshooting.

One-to-one

If a machine fails in a one-to-one configuration, a mirrored hot spare lies in wait for the signal the other device is unreachable. All information is sent between the two machines, allowing the second to continue where the other left off. If a heartbeat between them is not received, the spare begins duty, sending alerts back to the consoles warning of intruders and network attacks.

One-to-many

A one-to-many configuration has all sensors and/or managers reporting hierarchically up to consoles. If the console does not receive a heartbeat from a device, a hot spare is instructed by the console to reconfigure itself for service. The console pushes down the policy and settings of the failed machine to the spare, and an alert is sent to the SOC operator for necessary repairs.

Load Balancing
One benefit of fail over in devices is the advancement of load balancing. If a machine in a one-to-one or one-to-many deployment has already been purchased, and it will not harm the disaster recovery plan, it would be better used in covering network traffic spikes by sending half of the traffic to each device. This requires shared memory between the two devices, or an update system to keep track of all traffic. Again, this is only useful if it does not interfere with the disaster recovery plans in place.

Management Consoles
All of the above techniques work equally as well for IDS software consoles, but many are moving away from specialized programs and moving to web based controls. Since multiple machines in a SOC can access the IDS web server, this has the same effect as a one-to-many fail over; if a computer fails, change to another. It also allows the enterprise policy and desktop software bundle to be placed on SOC machines, lowering the total development costs.

Storage Requirements

Once the enterprise architecture can assure information is collected and reported up through to the consoles, the next hurdle for an enterprise environment is IDS data. Enterprise deployments of IDS sensors gather large amounts of information. In an enterprise environment, data analysis requires a network infrastructure, mass storage, sheer processing power and IDS analysts.

As many COTS products only send alerts to the SOC operators, additional information may be necessary for enterprise wide correlation or forensic analysis. Data from Cisco's Net Ranger sensors contains granular packet payload information. Firewall log files may contain causal information for host based IDS device alerts, such as Symantec's Intruder Alert. Products that send all captured packets, such as the Shadow 2.6 software generates gzip files on the order of hundreds of megabytes per hour. All of this information may be useful in longer-term correlations, and in turn, determining weaknesses in IDS and network/architecture design. Additionally, Service Level Agreements may require this information stored for forensic evidence upwards of two years. These SLAs may be in line with the recent dawn of Information Warfare, aiming the goal of hacking your site as my profession. Network probing in such instances would allow intervals outside the limits of real time IDS sensors. Long-term storage of this data in an enterprise

environment requires planning. Storage Area Networks (SANs) from Sun, Dot Hill and others provide solutions for the petabytes of data produced in an enterprise over the two + year forensic time span requirement.

Data Analysis

Processing Power

The collection of enterprise data requires computing power to produce information. Recourse Technologies Man Hunt product suggests Sun Enterprise class, multiprocessor machines for deployment. eSecurity recommends the same. Net Forensics has three software platforms: Linux, Windows NT and Solaris, designed for increasing network size. The Solaris platform can be spread across multiple machines, utilizing a remote Oracle database to perform all database storage, even on a Storage Area Network. And the end console is based on a java enabled web browser. The manager collects information from several COTS network products, including Cisco's Net Ranger, PIX firewalls, and IOS routers, and is slated to receive data from Symantec's Net Prowler, Raptor Firewall and other network security products. The processing power is used to perform as many correlations and data manipulations as possible. Intrusion Detection is hampered by false positives. The more tests and checks performed on incoming data, the less likely the IDS designer or SOC analyst is to turn off the sensitivity of the sensors. The analysts must also be presented with enough pre-processed information to determine from their own experience if an attack is eminent.

Skilled Analysts

Intrusion detection has always relied on skilled analysts to verify incoming alerts. Skilled SOC operators can differentiate false positives from true attacks if given the relevant information to draw such a conclusion. Security professionals need the ability to receive more information on demand about an alert. Managing these data transfers has proven to be an enterprise task in itself. Another aspect of IDS development is the shortage of trained security specialists. Enterprise managers are training users to simply believe the software in absence of professionals. This places more burdens on the software designer, as more correlation and deduction is expected to replace the human inferences by untrained operators, and security professionals are demanding more capabilities from each product released.

Conclusion:

Commercial Intrusion Detection Services have been deployed mostly in smaller business environments, but are still relatively new to the larger enterprise environment. The explosion of the Internet, and the security risks associated with connecting to it is

accelerating the rate of development for the IDS market. As larger organizations attempt to streamline their costs, and information ages faster, enterprise networks will continue to face greater security challenges. Intrusion Detection will continue as a significant management hurdle, with larger security threats and more centrally controlled devices. As network attacks grow more complex, so too shall the IDS requirements in an enterprise environment.

References:

Stick, www.eurocompton.net/stick/projects8.html

Pomeranz, H., SANS Institute, Solaris Security - Step by Step v. 2.0, 2000

eSecurity product literature, www.esecurity.com

Shadow 2.6 documentation, www.nswc.navy.mil/ISSEC/index.html

NetForensics documentation, www.netforensics.com

Symantec Net Prowler 3.5.1 documentation, www.axent.com

Recourse Technologies Man Hunt product literature, www.recourse.com

ISS Real Secure documentation, www.iss.com

Matthews, James, "The Port Report", May 2001

Dot Hill product literature, www.dothill.com

Cisco Net Ranger 2.2.1 documentation, www.cisco.com

Bace, R. & P. Mell, "NIST Special Publication on Intrusion Detection Systems", Feb. 2001

Assignment 3 - "Analyze This" Scenario (30 Points)

Overview of Data

Files

- SnortA35,36,3,6,25
- OOScheck.txt
- OOSche24-34, 4-5
- SnortAle
- SnortS2,7,8,26,27,29,32,ca
- UMBCNI2,25-61,

Dates

- 1/21/01 through 3/12/01

Types of Files

- OOS Files
- Scan Files
- Alert Files

A list of detects, prioritized either by severity or number of occurrences, and a brief description of these.

Signature	# Alerts	# Sources	# Destinations	Description
UDP Scan	636401	14	109921	UDP is a connectionless protocol, and may yield false positives, especially if firewalls or routers are filtering traffic. With the recent release of Probe X, these UDP Scans are of larger concern. Probe X allows OS fingerprinting with four UDP packets or less. Most of the traffic in these UDP scans appears to be very noisy, with much more than four packets heading to each host.

UDP SRC & DST outside Network	140425	378	280	A good part of this traffic is destined for 224.0.0.0 - 239.255.255.255. This IP address range is reserved for multicast services, such as H.323 streaming video. The traffic that is not destined for these multicast addresses is discussed below. This is also the signature that DHCP client's default IP address will fall in, 169.254.x.x (See DHCP Server Unavailable).
TCP Syn scan	98217	334	48623	Considered a "stealth" scan by Fyodor and his nmap product, the Syn scans performed in these detects are anything but. Syn Scans begin the first portion of a TCP handshake, but, after reception of a Syn-Ack, never send an acknowledgement packet. This allows enumeration of which hosts are up, and which ports are listening.
NMAP TCP ping	6485	7	3183	A network exploration tool and security/port scanner, Nmap TCP pings reduce the amount of work necessary to map a network. The machines that do not respond to pings are not considered on and are skipped for the rest of the tests.
Watchlist 000220 IL-ISND70-990517	6833	25	24	Israeli High Speed Internet connections, this address range appears in incident.org as a frequent attacker.
Possible RAMEN server activity	5633	1267	2464	http://www.cert.org/incident_notes/IN-2001-01.html - cert advisory CERT Widespread Compromises via "ramen" Toolkit Vulnerability Note VU#382365, LPRng can pass user-supplied input as a format string parameter to syslog() calls
TCP FPU Scan	6227	5	5293	Method of performing a scan that some firewalls and routers will not block, typically due to poor planning or coding
External RPC Call	3024	2	1461	Remote Remote Procedure Call
TCP SRC & DST outside Network	844	10	12	224.0.0.0 - 239.255.255.255 Multicast traffic destined for the internal network.
TCP SynFin Scan	16001	1267	15133	Method of performing a scan that some firewalls and routers will not block, typically due to poor planning or coding

An Internal "top talkers" list.

Source	# Alerts	# as Dest	# As Source	# Signatures
10.70.98.176	6161	0	573	2
10.70.98.150	4324	0	3695	1
10.70.97.13	4578	0	129	1
10.70.228.50	5680	0	5680	1
10.70.228.206	4590	0	35	1
10.70.228.122	6024	0	693	1
10.70.225.198	6090	0	184	1
10.70.224.74	4833	0	656	1
10.70.223.34	8083	0	52	1
10.70.220.142	4074	0	1735	2
10.70.218.90	18487	1	1920	2
10.70.217.74	8524	0	221	3
10.70.217.58	6191	0	2551	2
10.70.217.142	7023	87	2213	2
10.70.210.250	9679	0	1	9679
10.70.210.190	8005	0	219	1
10.70.206.42	3728	0	3728	1
10.70.203.234	6255	1	749	1
10.70.202.50	6897	0	89	1
10.70.202.50	7106	1	84	1
10.70.150.225	9425	0	846	2
10.70.150.145	4523	0	521	2
10.70.150.143	6785	0	578	1
10.70.150.133	8759	0	887	2
10.70.100.230	3967	0	2070	2

An External "top talkers" list. A list of source addresses and registration information about these.

Source	# Alerts	# Dsts	Network Block	Registration Info
205.188.244.249	859	859	205.188.0.0 - 205.188.255.255	America Online, Inc (NETBLK-AOL-DTC) 22080 Pacific Blvd Sterling, VA 20166

155.101.21.38	26301	16344	155.101.0.0 - 155.101.255.255	University of Utah (NET-UTAH-OC-NET) 606 Black Hawk Way Salt Lake City, UT 84108
140.142.19.72	4715	1	140.142.0.0 - 140.142.255.255	NorthWestNet Network Operations Center (NET-UW-SEA) Academic Computing Center 3737 Brooklyn NE Seattle, WA 98105
132.235.177.123	4258	4258	132.235.0.0 - 132.235.255.255	Ohio University (NET-OHIOU-NET) Ohio University - Communications Network Services Athens, OH 45701-2979
195.127.111.251	2439	2336	195.127.110.0 - 195.127.111.255	AWIC AG Eschborner Landstrasse 41-51 D-60489 Frankfurt a.M. Postfach 94 01 81 D-60459 Frankfurt a.M. DE
24.67.186.244	2385	2378	24.64.0.0 - 24.71.255.255	Shaw Fiberlink ltd. (NETBLK-FIBERLINK-CABLE) 630 3rd Avenue SW, Suite 900 Calgary AB, 4L4 CA
64.224.193.144	2049	2049	64.224.193.144 - 64.224.193.159	WEBMICESTER DESIGN (NETBLK-DSTILESCOBALT) DSTILESCOBALT
63.89.128.4	1392	1392	63.89.128.0 - 63.89.129.255	TJR Enterprises via UUNet
213.224.161.89	1315	1315	213.224.128.0 - 213.224.223.255	netname: TELENET descr: Telenet Operaties N.V. , BE
169.226.202.234	12129	12110	169.226.0.0 - 169.226.255.255	University at Albany, State University of New York 1400 Washington Av Albany, NY 12222
206.112.192.106	9992	1	206.112.192.0 - 206.112.192.255	OneNet Communications, Inc. Server Network via UUNet

65.9.212.74	3322	1157	65.9.208.0 - 65.9.215.255	@Home Network Washington DC
24.141.226.62	8642	1	24.141.224.0 - 24.141.239.255	Cogeco Cable Solutions
199.108.40.107	847	840	199.108.40.0 - 199.108.41.255	Control Net
212.162.240.66	1935	4	212.162.240.0 - 212.162.255.255	SEGA Sega Europe Ltd. 266-270 Gunnersbury Avenue London W4 5QB GB

At least one link graph.

212.162.240.66 - Destination

Feb 6 00:53:35 10.70.221.206:2003 -> 212.162.240.66:38778 UDP
Feb 6 00:54:33 10.70.217.94:2003 -> 212.162.240.66:39778 UDP
Feb 6 01:24:10 10.70.209.238:2016 -> 212.162.240.66:39778 UDP
Feb 6 05:45:55 10.70.207.34:2003 -> 212.162.240.66:39778 UDP
Feb 6 05:46:17 10.70.207.34:2002 -> 212.162.240.66:38778 UDP
Feb 6 16:18:02 10.70.207.178:2004 -> 212.162.240.66:38778 UDP
Feb 6 20:27:45 10.70.209.238:2008 -> 212.162.240.66:38778 UDP
Feb 6 21:55:19 10.70.214.26:2006 -> 212.162.240.66:38778 UDP
Feb 6 23:23:47 10.70.202.174:2003 -> 212.162.240.66:38778 UDP
Feb 7 17:58:01 10.70.207.110:2004 -> 212.162.240.66:38778 UDP
Feb 7 23:44:47 10.70.217.94:2001 -> 212.162.240.66:38778 UDP

This appears as a disjointed probe for UDP port 38778. None of the times correlate closely to any of the other packets sent from this host. Port 38778 does not have any well known listeners associated with it.

212.162.240.66 - Source

Feb 6 01:40:14 212.162.240.66:39777 -> 10.70.219.154:3076 UDP
Feb 6 01:40:17 212.162.240.66:39777 -> 10.70.217.94:4282 UDP
Feb 6 01:40:18 212.162.240.66:39777 -> 10.70.211.118:1081 UDP
Feb 6 01:40:18 212.162.240.66:39777 -> 10.70.211.118:1075 UDP
Feb 6 01:40:18 212.162.240.66:39777 -> 10.70.207.178:2848 UDP
Feb 6 01:40:18 212.162.240.66:39777 -> 10.70.207.178:2847 UDP
Feb 6 01:40:18 212.162.240.66:39777 -> 10.70.219.154:3077 UDP
Feb 6 01:40:18 212.162.240.66:39777 -> 10.70.217.94:4276 UDP
Feb 6 01:40:20 212.162.240.66:39777 -> 10.70.217.94:4282 UDP
Feb 6 01:40:21 212.162.240.66:39777 -> 10.70.207.178:2847 UDP
Feb 6 01:40:21 212.162.240.66:39777 -> 10.70.207.178:2848 UDP
Feb 6 01:40:21 212.162.240.66:39777 -> 10.70.211.118:1081 UDP
Feb 6 01:40:21 212.162.240.66:39777 -> 10.70.211.118:1075 UDP
… (Continued for 1500 packets on Feb 6th)
Feb 6 01:56:49 212.162.240.66:39777 -> 10.70.217.94:4284 UDP
Feb 6 01:56:49 212.162.240.66:39777 -> 10.70.211.118:1087 UDP
Feb 6 01:56:49 212.162.240.66:39777 -> 10.70.207.178:2849 UDP
Feb 6 01:56:51 212.162.240.66:39777 -> 10.70.211.118:1087 UDP
Feb 6 01:56:52 212.162.240.66:39777 -> 10.70.207.178:2849 UDP

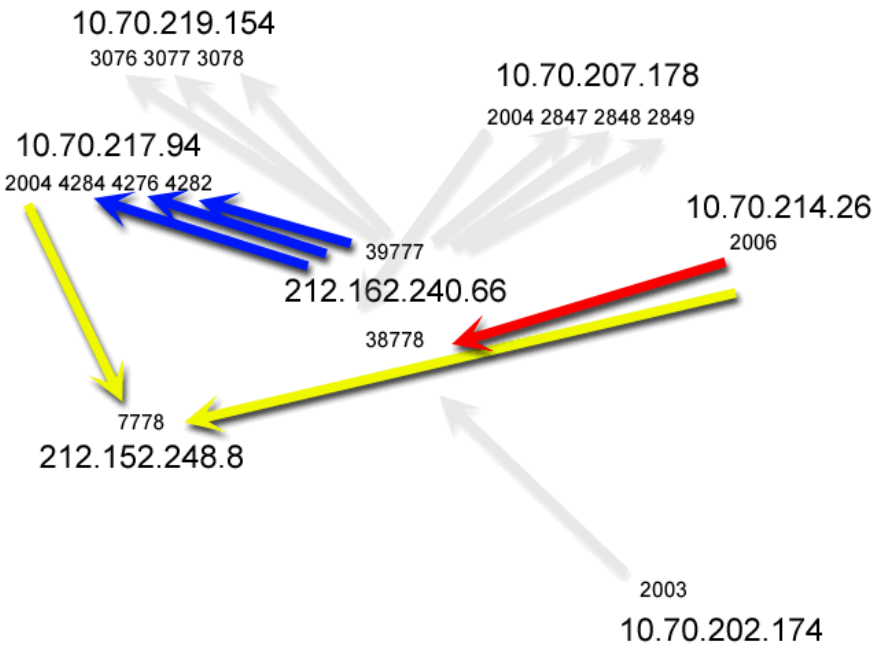
Feb 6 01:56:52 212.162.240.66:39777 -> 10.70.219.154:3078 UDP
Feb 6 01:56:52 212.162.240.66:39777 -> 10.70.217.94:4284 UDP
Feb 6 01:56:53 212.162.240.66:39777 -> 10.70.207.178:2848 UDP
Feb 6 01:56:54 212.162.240.66:39777 -> 10.70.219.154:3078 UDP
Feb 6 01:56:55 212.162.240.66:39777 -> 10.70.217.94:4282 UDP
Feb 6 01:56:55 212.162.240.66:39777 -> 10.70.217.94:4284 UDP
Feb 6 01:56:55 212.162.240.66:39777 -> 10.70.211.118:1087 UDP
Feb 6 01:56:55 212.162.240.66:39777 -> 10.70.219.154:3077 UDP
Feb 6 01:56:55 212.162.240.66:39777 -> 10.70.207.178:2849 UDP

The detected packets sent above all have a source port of 39777. This many packets in this short of a time period demonstrate some sort of communication. Again, none of these packets correlate with the destination packets seen above. There are no listings for any ports nearby 39777 with any well-known software listeners.

Feb 6 18:37:41 10.70.214.26:2004 -> 64.3.151.7:7778 UDP
Feb 6 18:37:42 10.70.214.26:2008 -> 24.113.79.65:7778 UDP
Feb 6 18:37:42 10.70.214.26:2001 -> 213.221.174.103:8031 UDP
Feb 6 18:37:42 10.70.214.26:2006 -> 212.122.148.84:7745 UDP
Feb 6 18:37:42 10.70.214.26:2007 -> 212.224.24.222:25001 UDP
Feb 6 18:37:42 10.70.214.26:2008 -> 128.186.178.164:7778 UDP
Feb 6 18:37:42 10.70.214.26:2007 -> 194.239.134.25:7821 UDP
Feb 6 18:37:42 10.70.214.26:2008 -> 195.88.134.245:7501 UDP
Feb 6 18:37:43 10.70.214.26:2000 -> 212.134.126.17:7778 UDP
Feb 6 18:37:43 10.70.214.26:2000 -> 195.88.134.215:7501 UDP
Feb 6 18:37:43 10.70.214.26:2005 -> 64.114.97.5:7798 UDP
Feb 6 18:37:43 10.70.214.26:2000 -> 194.251.102.150:7778 UDP
Feb 6 18:37:46 10.70.214.26:2001 -> 194.158.97.236:6667 UDP
Feb 6 18:37:46 10.70.214.26:2004 -> 62.226.30.73:7778 UDP
Feb 6 18:37:46 10.70.214.26:2006 -> 66.21.218.234:7778 UDP
Feb 6 18:37:46 10.70.214.26:2005 -> 65.33.187.120:7778 UDP
Feb 6 18:37:46 10.70.214.26:2006 -> 151.23.31.22:13701 UDP
Feb 6 18:37:46 10.70.214.26:2000 -> 212.113.80.152:7778 UDP
Feb 6 18:37:46 10.70.214.26:2008 -> 194.134.233.78:7778 UDP
Feb 6 18:37:47 10.70.214.26:2007 -> 207.151.157.250:7788 UDP
Feb 6 18:37:47 10.70.214.26:2008 -> 64.188.161.129:7778 UDP
Feb 6 18:37:47 10.70.214.26:2005 -> 193.11.10.186:7778 UDP
…
Feb 6 18:52:16 10.70.214.26:2014 -> 212.152.248.8:7778 UDP
…
Feb 7 23:55:20 10.70.214.26:2004 -> 24.14.232.250:7778 UDP
Feb 7 23:55:21 10.70.214.26:2006 -> 216.232.97.91:7778 UDP
Feb 7 23:55:21 10.70.214.26:2003 -> 209.233.190.86:7778 UDP

Feb 7 23:55:21 10.70.214.26:2000 -> 203.46.27.100:7778 UDP
Feb 7 23:55:21 10.70.214.26:2006 -> 216.233.110.42:7778 UDP
Feb 7 23:55:22 10.70.214.26:2005 -> 209.63.173.4:7778 UDP
Feb 7 23:55:22 10.70.214.26:2006 -> 203.7.198.11:8001 UDP
Feb 7 23:55:25 10.70.214.26:2009 -> 62.155.234.156:7778 UDP
Feb 7 23:55:25 10.70.214.26:2007 -> 64.123.165.98:7778 UDP
(765 Packets total)

Upon examining a partial link graph of the above data, the transfers become a bit more apparent. This link graph provided the information to begin delving into port 7778. Port 38**778** and port 39**777** both provided clues to their use without being readily apparent. Traffic on these ports may appear legitimate. Luckily, enough information was present to provide the Unreal Tournament ports below. The players also appear to generate IRC traffic on port 6667. This would be in line with expectations, as communication beyond simply fragging your playing opponents lends to the experience.



10.70.214.26

Port 7777

- IANA: cbt (TCP/UDP)
- May 2001, http://opennap.sourceforge.net/napster.txt, Napster, Napster uses TCP for client to server communication. Typically the servers run on ports 8888 and 7777. Note that this is different from the `metaserver' (or redirector) which runs on port 8875.

- May 2001, http://advice.networkice.com/advice/exploits/ports/7777/default.htm, Hacker can spoof UDP packets to this port in order to control the cable-modem.
- May 2001, http://www.securityfocus.com/bid/695.html, Hybrid Network's cable modems are vulnerable to several different types of attack due to a lack of authentication for the remote administration/configuration system. The cable modems use a protocol called HSMP, which uses UDP as its transport layer protocol. This makes it trivial to spoof packets and possible for hackers to compromise cable-modem subscribers anonymously. The possible consequences of this problem being exploited are very serious and range from denial of service attacks to running arbitrary code on the modem.

Port 7778

- IANA: Interwise (TCP/UDP)
- May 2001, http://advice.networkice.com/advice/exploits/ports/7778/default.htm, Unreal Tournament, an online multiplayer personal shooter
- Q: Have been noticing a HUGE pile of probes from one address to port 7778 on my firewall machine; all UDP packets.
  A: Unreal Tournament uses UDP packets on port 7778. Possibly there's a hole in the Unreal Tournament server? Or possibly somebody is trying to play through your firewall?

Port 6667

- IANA: IRCU (TCP/UDP), Internet Relay Chat
- Trojans
  1. WinSatan
  2. ScheduleAgent?
- May 1993, RFC1459, http://www.faqs.org/rfcs/rfc1459.html, Internet Relay Chat Protocol
- Apr 2001, RFC2810, http://www.faqs.org/rfcs/rfc2810.html, Internet Relay Chat: Architecture
- Apr 2001, RFC2811, http://www.faqs.org/rfcs/rfc2811.html, Internet Relay Chat: Channel Management
- Apr 2001, RFC2812, http://www.faqs.org/rfcs/rfc2812.html, Internet Relay Chat: Client Protocol
- Apr 2001, RFC2813, http://www.faqs.org/rfcs/rfc2813.html, Internet Relay Chat: Server Protocol
- At least the trojan WinSatan uses TCP port 6667 by default, possibly also the trojan ScheduleAgent. And not to forget some other 60 IRC trojans of various kinds. Many of uses IRC to broadcast passwords or logs captured by keyloggers, but there are also RATs and others as well.
- May 2001, http://advice.networkice.com/Advice/Exploits/Ports/groups/streaming/VocalTec_Internet_Phone/default.htm VocalTec Internet Phone, an alternate port other than 6670

used to connect to Vocaltec servers. Also, IRC clients can connect to IRC servers on this port.

Any insights into internal machines, such as compromise or possible dangerous or anomalous activity.

Older Broadcast Address Allowed on Network

Earliest such alert at **01:07:18**.988419 *on 02/20/2001*
Latest such alert at **21:29:18**.917755 *on 03/10/2001*

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total
0.0.0.0	7	7	2	2

0.0.0.0 should not be allowed on a network. It is used as a broadcast address by some older BSD routers, but it otherwise should not be assigned as an IP address. If these packets are not anticipated in poorly written router ACLs or firewall rulesets, these packets may slip through defensive layers.

Back Orifice Alerts

Earliest such alert at **17:04:09**.754841 *on 02/24/2001*
Latest such alert at **17:04:36**.800828 *on 02/24/2001*

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
63.10.224.59	9	9	9	9

Back Orifice Destinations

One interesting point that arises from the below destinations is the fact that there are only two subnets involved in these detects. A promiscuous listener connected to a subnet with all machines on a single segment can capture all traffic destined for a specific port on that segment. The destinations of these alerts should be examined further.

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
10.70.98.238	1	1	1	1
10.70.97.119	1	1	1	1
10.70.97.225	1	1	1	1
10.70.98.3	1	2	1	2
10.70.97.162	1	1	1	1
10.70.98.28	1	3	1	3
10.70.97.3	1	2	1	2
10.70.98.75	1	2	1	2
10.70.98.123	1	1	1	1

Further Snort Snarf Data Analysis

10.70.98.3

02/24-17:04:24.335687 [**] Back Orifice [**] 63.10.224.59:2382 -> 10.70.98.3:31337
Mar 5 00:15:12 24.3.9.225:1320 -> 10.70.98.3:12345 SYN **S*****

Port 12345

- IANA: Unassigned
- Advisories

1. Dec 1998, CERT/CC, http://www.cert.org/summaries/CS-98-08.html. In recent months, we have seen the spread of Windows-based Trojan horse programs. The most frequently reported incidents involving Windows-based Trojan horse programs involve the tools Back Orifice and NetBus. We receive occasional reports of compromised machines that have one of these tools installed; however, the majority of reports involving these tools are from sites noticing intruders scanning their networks for the presence of these tools. We receive daily reports indicating that intruders are actively scanning networks to find running instances

of these tools on already compromised machines. Look for the following symptoms to detect those scans:
NetBus - connection request (SYN) packets to TCP port 12345
Back Orifice - UDP packets to port 31337
Keep in mind that these tools can be configured to listen on different ports. Because of this, we encourage you to investigate any unexplained network traffic. Because these tools are Trojan horses, users must install them or be tricked into installing them. To impede the proliferation of this class of tools, we encourage system administrators to educate their users about safe computing practices (e.g., only install software from trusted sources, and use virus scanning software on any newly introduced software).

- Trojans

1. GrabanBus
2. NetBus (TCP)
3. Pie Bill Gates
4. X-bill

- 30 May 2001, The Trend Micro OfficeScan client tmlisten.exe allows remote attackers to cause a denial of service via malformed data to port 12345. Mitre CVE Candidate: CAN-2000-0203, URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0203, Phase: Proposed (20000322), Category: SF/CF/MP/SA/AN/unknown, Reference: BUGTRAQ:20000228 Re: TrendMicro OfficeScan tmlisten.exe DoS,Reference: http://www.securityfocus.com/templates/archive.pike?list=1&msg=412FC0AFD62ED31191B40008C7E9A11A0D481D@srvnt04.previnet.it, Reference: BUGTRAQ:20000315 Trend Micro release patch for "OfficeScan DoS & Message Replay" Vulnerabilities, Reference: URL:http://www.securityfocus.com/templates/archive.pike?list=1&msg=D129BBE1730AD2118A0300805FC1C2FE038AF28B@209-76-212-10.trendmicro.com, Reference: MISC: http://www.antivirus.com/download/ofce_patch_35.htm, Reference: http://www.securityfocus.com/bid/1013
- 23 May 2001, SecurityFocus Incidents List, Arthur Donkers wrote “Look what we found in our honeypot this morning: A new breed of the Linux w0rmkit that uses the adore module to hide itself. The backdoor listens on 12345 and is a 1.2.26 sshd with a preprogrammed password of h4ck3d! It is a more advanced version of the earlier w0rmkit since it uses the adore kernel based rootkit and chattr to make itself permanent on a system. It exploits the usual Linux vulnerabilities (the same scanner as w0rmkit) to gain access.”
- May 2001, http://advice.networkice.com/Advice/Exploits/Ports/12345/default.htm “Notice how this port is the sequence of numbers "1 2 3 4 5". This is common chosen whenever somebody is asked to configure a port number. It is likewise chosen by programmers when creating default port numbers for their products. One very famous such uses is with NetBus. (TCP) Trend Micro's OfficeScan products use this port. Sending random data to this port or opening too many connections can cause this service to crash. Affects version 3.5”

10.79.98.28

Feb 23 12:07:13 210.96.87.189:2666 -> 10.70.98.28:53 SYN **S*****
02/24-17:04:25.359418 [**] Back Orifice [**] 63.10.224.59:2382 -> 10.70.98.28:31337
Mar 10 19:04:49 64.224.193.144:21 -> 10.70.98.28:21 SYN **S*****
Jan 21 14:34:52 169.226.202.234:21 -> 10.70.98.28:21 SYNFIN **SF****

Port 53

- IANA: Domain Name Server, dns (TCP/UDP)
- Nov 1987, RFC1035, http://www.faqs.org/rfcs/rfc1035.html, DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
- Advisories

7. Feb 2001 (Nov 2000), CERT/CC, http://www.cert.org/advisories/CA-2000-20.html Multiple Denial-of-Service Problems in Internet Software Consortium (ISC) BIND
8. Jan 2001 (April 2000), CERT/CC http://www.cert.org/incident_notes/IN-2000-04.html DOS attacks using nameservers (primarily using UDP)
9. Sep 2000, CERT/CC, http://www.cert.org/advisories/CA-2001-02.html Multiple Vulnerabilities in BIND
10. April 2000, CERT/CC, http://www.cert.org/incident_notes/IN-2000-04.html Continuing compromises of DNS servers
11. April 2000 (Nov 1999), CERT/CC, http://www.cert.org/advisories/CA-1999-14.html Multiple Vulnerabilities inBIND
12. Nov 1998 (Apri 1998), CERT/CC, http://www.cert.org/advisories/CA-1998-05.html Multiple Vulnerabilities inBIND

- 26 April 2001, www.incidents.org says that this port was the most frequently probed port in the past 30 days
- 26 April 2001, www.incidents.org says that this port is the sixth most frequently probed port in the past 7 days
- January 1999, http://www.cert.org/incident_notes/IN-99-01.html The sscan tool probes for this port. The sscan "port" signature is as follows:

4. TCP ACK packets with source and destination ports set to 23, 25, 110, 143, 80
5. If step one receivs a positive response, then port 80, (23, 143, 110 - all or none), 111, 6000, 79, 53, 31337, 2766
6. Then ports 139, 25, 21, 22, 1114, 1

- If it's coming from Exodus, they may be using F5's 3dns server which does a null socket connect to your local dns servers using tcp to get rtt and latency. They (f5 3dns) uses this information to get the best response time and will load balance their servers behind accordingly. In your logs you will see port connects to tcp 53. I believe your fault is in how you think MS DNS works. Port 53 is used for the initial connection/request, then (in the NT implementation) a dynamic port (greater than 1023) for the reply back to the client.

Port 21

- IANA: File Transfer Protocol (control channel) (TCP/UDP)
- Avisories

1. Jan 2001, CERT/CC, http://www.cert.org/incident_notes/IN-2001-01.html, Widespread compromises via "ramen" toolkit. (TCP)
2. Nov 2000 (July 2000), http://www.cert.org/advisories/CA-2000-13.html Two Input Validation Problems In FTPD (TCP)
3. Sep 2000, CERT/CC, http://www.cert.org/incident_notes/IN-2000-10.html Widespread Exploitation of rcp.statd and wu-ftpd Vulnerabilities (TCP)
4. June 2000, AUSCERT, ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-2000.02 AusCERT description of wu-ftpd "site exec vulnerability (TCP)
5. Nov 1999 (Oct 1999), CERT/CC, http://www.cert.org/advisories/CA-1999-13.html Multiple vulnerabilities in wu-ftpd (TCP)
6. Mar 1999(Dec 1997), CERT/CC, http://www.cert.org/advisories/CA-1997-27.html FTP Bounce (TCP)

- Trojans

2. Back Construction
3. Blade Runner (TCP)
4. Doly Trojan (TCP)
5. Fore (TCP)
6. FTP Trojan
7. Invisible FTP (TCP)
8. Larva
9. WebEx (TCP)
10. WinCrash (TCP)
11. DarkFTP, http://advice.networkice.com/advice/Phauna/Trojan_Horse/FTP/DarkFTP/default.htm, http://www.dark-e.com/archive/trojans/darkftp/index.html

- May 2001, http://www.networkice.com/Advice/Exploits/Ports/groups/Midnight_Commander/default.htm
- April 26, 2001, www.incidents.org says that this port is the third most frequently probed port in the past 30 days
- April 26, 2001, www.incidents.org says that this port is the tenth most frequently probed port in the past 7 days
- January 1999, http://www.cert.org/incident_notes/IN-99-01.html The sscan tool probes for this port. The sscan "port" signature is as follows:

1. TCP ACK packets with source and destination ports set to 23, 25, 110, 143, 80
2. If step one receivs a positive response, then port 80, (23, 143, 110 - all or none), 111, 6000, 79, 53, 31337, 2766
3. Then ports 139, 25, 21, 22, 1114, 1

10.70.97.3

02/24-17:04:09.754841 [**] Back Orifice [**] 63.10.224.59:2382 -> 10.70.97.3:31337
Mar 9 02:17:52 195.127.111.251:2677 -> 10.70.97.3:53 SYN **S*****

Port 53 Again

10.70.98.75

Feb 24 05:44:05 132.235.177.123:2340 -> 10.70.98.75:53 SYN **S*****
02/24-17:04:27.815284 [**] Back Orifice [**] 63.10.224.59:2382 -> 10.70.98.75:31337

Port 53 Again

Conclusions

The above packets were the only associated detects for the Back Orifice alert destinations. All of these detects have scans for susceptible ports earlier or later in the data set. This suggests the possibility of these four machines having open services that may or may not have been exploited. However, because of the small amount of traffic for Back Orifice, it is more likely this is a mere probe for the previously installed program suite, as are the Syn packets scans for vulnerable services.

Compromised Host/Internal Threat

The below warnings are the only alerted communications to an internal host that, on February 20th, began, or continued (the logs were not present for immediate days prior to the 20th) an attack beginning with 10.70.96.32 and following through 10.70.255.246.

The 10.70.253.12 host appears to have RPC services (port 111) responding, allowing an attacker to attempt numerous buffer overflows on the service. This would be a completely separate issue, if not for the allowance of some understanding of the 10.70.x.x network.

02/20-19:50:24.855046 [**] External RPC call [**] 171.65.61.201:3453 -> 10.70.253.12:111
Feb 20 19:50:24 171.65.61.201:3453 -> 10.70.253.12:111 SYN **S*****
Jan 21 03:45:22 10.70.101.1:0 -> 10.70.253.12:40 INVALIDACK 2**FR*A* RESERVEDBITS

The 10.70.253.12 and 10.70.70.38 hosts are both sent packets from the same 10.70.101.1 address.

Jan 21 03:45:20 10.70.101.1:0 -> 10.70.253.12:40 INVALIDACK 2**FR*A* RESERVEDBITS
Jan 21 03:45:22 10.70.101.1:0 -> 10.70.253.12:40 INVALIDACK 2**FR*A* RESERVEDBITS
Feb 1 21:19:23 10.70.101.1:0 -> 10.70.70.38:40 INVALIDACK 2**FR*A* RESERVEDBITS

Hopefully, a System Administrator hoping to gain a better understanding of the current system architecture performed the following scans. Unfortunately, the Sys Admin would likely know which machines were DNS servers and not repeatedly scan port 53.

Feb 1 21:19:23 10.70.101.1:0 -> 10.70.70.38:40 INVALIDACK 2**FR*A* RESERVEDBITS
Mar 6 16:53:34 61.200.36.220:6346 -> 10.70.70.38:3828 INVALIDACK ***FR*A*
Feb 21 00:00:04 10.70.70.38:36338 -> 10.70.137.183:36063 SYN **S*****
Feb 21 00:00:02 10.70.70.38:36340 -> 10.70.137.183:36063 XMAS ***F*P*U
Feb 21 00:00:47 10.70.70.38:36340 -> 10.70.137.185:42634 XMAS ***F*P*U
Feb 21 00:01:15 10.70.70.38:36338 -> 10.70.137.187:43064 SYN **S*****
Feb 21 00:01:15 10.70.70.38:36340 -> 10.70.137.187:43064 XMAS ***F*P*U
Feb 21 00:01:15 10.70.70.38:36327 -> 10.70.137.187:43064 UDP
Feb 21 00:02:25 10.70.70.38:4267 -> 10.70.137.192:53 SYN **S*****
Feb 21 00:02:27 10.70.70.38:36338 -> 10.70.137.192:33243 SYN **S*****

```
Feb 21 00:02:27 10.70.70.38:36340 -> 10.70.137.192:33243 XMAS ***F*P*U
Feb 21 00:02:28 10.70.70.38:36327 -> 10.70.137.192:33243 UDP
Feb 21 00:02:38 10.70.70.38:36338 -> 10.70.137.192:40666 SYN **S*****
Feb 21 00:02:38 10.70.70.38:36340 -> 10.70.137.192:40666 XMAS ***F*P*U
Feb 21 00:02:38 10.70.70.38:36327 -> 10.70.137.192:40666 UDP
…
Feb 20 00:31:41 10.70.70.38:36338 -> 10.70.96.146:33044 SYN **S*****
Feb 20 00:31:41 10.70.70.38:36340 -> 10.70.96.146:33044 XMAS ***F*P*U
….
Feb 21 01:28:18 10.70.70.38:1800 -> 10.70.147.167:53 SYN **S*****
Feb 21 01:28:18 10.70.70.38:36338 -> 10.70.147.167:30059 SYN **S*****
Feb 21 01:28:18 10.70.70.38:36340 -> 10.70.147.167:30059 XMAS ***F*P*U
Feb 21 01:28:24 10.70.70.38:36338 -> 10.70.147.167:32974 SYN **S*****
Feb 21 01:28:24 10.70.70.38:36340 -> 10.70.147.167:32974 XMAS ***F*P*U
Feb 21 01:28:24 10.70.70.38:36327 -> 10.70.147.167:32974 UDP
….
Feb 21 01:42:45 10.70.70.38:36338 -> 10.70.147.221:41326 SYN **S*****
Feb 21 01:42:45 10.70.70.38:36340 -> 10.70.147.221:41326 XMAS ***F*P*U
Feb 21 01:42:45 10.70.70.38:36327 -> 10.70.147.221:41326 UDP
Feb 21 01:42:46 10.70.70.38:36338 -> 10.70.147.221:41326 SYN **S*****
Feb 21 01:42:46 10.70.70.38:36340 -> 10.70.147.221:41326 XMAS ***F*P*U
Feb 21 01:42:46 10.70.70.38:36327 -> 10.70.147.221:41326 UDP
…
Feb 21 03:49:07 10.70.70.38:4122 -> 10.70.149.192:53 SYN **S*****
Feb 21 03:49:08 10.70.70.38:4123 -> 10.70.149.192:53 SYN **S*****
Feb 21 03:49:08 10.70.70.38:36327 -> 10.70.149.192:36482 UDP
Feb 21 03:49:23 10.70.70.38:4124 -> 10.70.149.193:53 SYN **S*****
….
Feb 21 22:34:09 10.70.70.38:36327 -> 10.70.204.247:39717 UDP
Feb 21 22:34:23 10.70.70.38:36338 -> 10.70.204.248:34122 SYN **S*****
Feb 21 22:34:23 10.70.70.38:36340 -> 10.70.204.248:34122 XMAS ***F*P*U
…
```

Thankfully for the analyst, Snort outputs alerts for a few of the above traffic patterns.

```
02/20-00:31:41.027765  [**] NMAP TCP ping! [**] 10.70.70.38:36339 -> 10.70.96.146:33044
02/23-13:42:28.709120  [**] spp_portscan: PORTSCAN DETECTED from 10.70.70.38 (STEALTH) [**]
02/23-13:42:31.212658  [**] spp_portscan: portscan status from 10.70.70.38: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH [**]
02/23-13:42:33.829216  [**] spp_portscan: portscan status from 10.70.70.38: 3 connections across 1 hosts: TCP(2), UDP(1) STEALTH [**]
02/23-13:42:36.573834  [**] spp_portscan: End of portscan from 10.70.70.38 (TOTAL HOSTS:1 TCP:3 UDP:1) [**]
```

This traffic is obviously malicious, likely attempts to further enumerate the network. The NMAP TCP ping warnings explain the gaps in the destination IP addresses. Those hosts that did not respond were not sent the attack packets,

conserving network resources to examine more hosts per hour.

02/20-03:41:17.557159 [**] SUNRPC highport access! [**] 10.70.70.38:36338 -> 10.70.103.112:32771
02/20-03:41:17.557209 [**] NMAP TCP ping! [**] 10.70.70.38:36339 -> 10.70.103.112:32771
02/20-03:41:17.557209 [**] NMAP TCP ping! [**] 10.70.70.38:36339 -> 10.70.103.112:32771
02/20-03:41:17.557261 [**] SUNRPC highport access! [**] 10.70.70.38:36340 -> 10.70.103.112:32771
02/20-03:41:17.557261 [**] SUNRPC highport access! [**] 10.70.70.38:36340 -> 10.70.103.112:32771

The above packets are part of the same scan. The vulnerability assessment tool Nessus (www.nessus.org) will perform an Nmap scan, probe for open ports, and attempt compromises such as Sun RPC access. This was either performed by an internal user acting with less regard for the overall system, or the machine has been compromised.

Multicast Addresses

02/24-00:35:34.282042 [**] UDP SRC and DST outside network [**] 130.240.196.137:1036 -> 224.2.127.254:9875
02/24-01:10:34.817376 [**] UDP SRC and DST outside network [**] 130.240.196.137:1036 -> 224.2.127.254:9875
02/24-01:20:33.785110 [**] UDP SRC and DST outside network [**] 130.240.196.137:1036 -> 224.2.127.254:9875
02/24-01:20:33.788064 [**] UDP SRC and DST outside network [**] 130.240.196.137:1036 -> 224.2.127.254:9875
…
03/09-16:41:55.305436 [**] UDP SRC and DST outside network [**] 152.1.1.79:9875 -> 224.2.127.254:9875
03/09-16:41:55.306854 [**] UDP SRC and DST outside network [**] 152.1.1.79:9875 -> 224.2.127.254:9875
03/09-16:41:55.307376 [**] UDP SRC and DST outside network [**] 152.1.1.79:9875 -> 224.2.127.254:9875
03/09-16:41:55.308001 [**] UDP SRC and DST outside network [**] 152.1.1.79:9875 -> 224.2.127.254:9875
… (Continued for over 40,000 packets)

A large amount of traffic is destined for IP address 224.2.127.254 port 9875. This appears to be some sort of multicast device. Port 9875 appears with the following information:

- IANA: Unassigned
- Trojans: Portal of Doom v3.x (TCP)

The trojan is unlikely however, as there are approximately 40,000 packets in three days worth of detects. A Trojan with that much usage would significantly impair any machine. The entire idea behind multicasting is to limit the repetitive packets sent. High bandwidth usage on a multicast server is logical. The IP address of the internal server, xxx.127.254 is also in line with a server that is accessed easily for the internal networks usage; the IP address is reasonably easy to remember, without being obnoxiously apparent.

Bootstrap Protocol

02/24-00:02:53.750457 [**] UDP SRC and DST outside network [**] 10.0.0.1:68 -> 10.255.255.255:67
02/24-00:09:58.573039 [**] UDP SRC and DST outside network [**] 10.0.0.1:68 -> 10.255.255.255:67
02/24-01:55:37.209906 [**] UDP SRC and DST outside network [**] 10.0.0.1:68 -> 10.255.255.255:67
02/24-01:55:57.205649 [**] UDP SRC and DST outside network [**] 10.0.0.1:68 -> 10.255.255.255:67
02/24-02:01:27.135204 [**] UDP SRC and DST outside network [**] 10.0.0.1:68 -> 10.255.255.255:67
02/24-02:01:57.128595 [**] UDP SRC and DST outside network [**] 10.0.0.1:68 -> 10.255.255.255:67
02/24-02:03:22.513185 [**] UDP SRC and DST outside network [**] 10.0.0.1:68 -> 10.255.255.255:67
02/24-02:03:42.510365 [**] UDP SRC and DST outside network [**] 10.0.0.1:68 -> 10.255.255.255:67
… (For a over 3000 packets)

There are two possible explanations for this traffic. Port 67 and 68 are used for DHCP traffic. A quick run down on ports 67 & 68 follows:

- IANA: Bootstrap Protocol Server (TCP/UDP)
- Actually, according the dhcrelay man page for ISC dhcpd 2.0(beta), the relay listens on UDP port 67 for DHCP broadcast requests. The ISC dhcrelay agent can also be told to bind to particular interfaces, rather than all of them. This, plus whatever ipfwadm/ipfilter equivalent you have, ought to be enough to secure dhcrelay as well as any other service can be secured. Get ISC dhcpd v2.0(beta) at ftp://ftp.isc.org/isc/dhcp/.
- DHCP client to server uses 67 UDP
- DHCP server to client uses 68 UDP

If these are legitimate packets, the DHCP client makes a request for an IP address on a local segment. These packets are based on the client's MAC address. Since no one on the local segment is a DHCP server, the local router must be set up to forward DHCP requests. If this is the case, the local router relays the packets to the next relay agent, and the process continues until it reaches the final DHCP server. Each step on the journey to the final DHCP server is programmed into the router using helper addresses. The address 10.0.0.1, if a DHCP server, would respond to the broadcast packet sent in 10.255.255.255 by the router on the local segment of the bootstrapping PC and forwarded until received. This suggests that the packets these detects originated from may actually contain a 10.0.0.1 IP address. This DHCP server would respond to the port 67 10.255.255.255 broadcast address, with its own 10.0.0.1 port 68 packets. These packets would be marked as outside of the my.net network in this Snort Snarf diagnosis, leading to the alerts above.

The other possibility is that these packets are crafted, and an attacker sits on the route nearby the 10.0.0.1 node and the Snort device. The response of this broadcast will enumerate all DHCP devices on the network, and any other devices that are listening on port 67. This traffic is intended to look like DHCP traffic to hide its existence. This is unlikely, however, given the amount of packets sent, and the frequency with which they were deployed (one or more every eight to ten minutes).

DHCP Server Unavailable

02/20-12:41:26.559869 [**] UDP SRC and DST outside network [**] 169.254.194.113:137 -> 169.254.255.255:137
02/20-12:41:26.559869 [**] UDP SRC and DST outside network [**] 169.254.194.113:137 -> 169.254.255.255:137
02/20-12:41:33.886255 [**] UDP SRC and DST outside network [**] 169.254.194.113:137 -> 169.254.255.255:137
02/20-12:41:33.886255 [**] UDP SRC and DST outside network [**] 169.254.194.113:137 -> 169.254.255.255:137
02/20-12:41:38.386689 [**] UDP SRC and DST outside network [**] 169.254.194.113:137 -> 169.254.255.255:137
02/20-12:41:38.386689 [**] UDP SRC and DST outside network [**] 169.254.194.113:137 -> 169.254.255.255:137
02/20-12:41:39.136170 [**] UDP SRC and DST outside network [**] 169.254.194.113:137 -> 169.254.255.255:137

By design RFC 2151, DHCP clients request an IP address from a DHCP server on boot. If they cannot connect to a DHCP server, the machine assigns itself an IP address, with Windows machines assigning themselves an IP in the 169.254.x.x range. The above packets likely display a Windows based machine attempting to locate other clients on the local subnet. The connections are attempted on port 137, with port 137's uses listed below. A typical use of port 137, which would produce the above broadcast address of 169.254.255.255, includes opening the Network Neighborhood on a default Windows installation.

Port 137

- IANA: NETBIOS Name Service (TCP/UDP)
- Advisories
  1. (UDP) April 2000, CERT/CC, http://www.cert.org/incident_notes/IN-2000-03.html 911 Worm
  2. (UDP) April 2000 (March 2000), CERT/CC, http://www.cert.org/incident_notes/IN-2000-02.html Exploitation of Unprotected Windows Networking Shares
- April 26, 2001, www.incidents.org says that this port is the ninth most frequently probed port in the past 30 days
- April 26, 2001, www.incidents.org says that this port is the eighth most frequently probed port in the past 7 days
- In Windows->Settings->Network->TCP/IP Properties->NetBIOS, you can enable NetBIOS support which allows you to run NetBIOS applications over the TCP/IP protocols
- In most cases, queries against 139 are attacks. 139 is the netbios session port. You more typically see banging on 137 which is the netbios name query port. Win95 boxes and some NT boxes plugged into the net will always try to do netbios name queries for stuff. As far as NetLogon - logging in to a PDC - you don't necessarily need port 137 - if you have your LMHOSTS file configured completely and correctly. 137/udp is used for WINS. You will need 138/udp and 139/tcpfor sure. UDP 137 is a

port for NetBIOS name resolution. Microsoft realization for IP->name resolution includes both DNS and netbios resolution. Every time you connect to hosts running MS products (for example IIS) which resolves your IP - host tries to resolve your NetBIOS name by sending UDP packet to your 137 port. No one hacks you it's ok ;)

- May 2001, http://www.networkice.com/Advice/Exploits/Ports/137/default.htm "Firewall administrators will frequently see large numbers of incoming packets to port 137. This is due to the behavior of Windows servers that use NetBIOS (as well as DNS) to resolve IP addresses to names using the "gethostbyaddr()" function. As users behind the firewalls surf Windows-based web sites, those servers will frequently respond with NetBIOS lookups". Also, NetBIOS has been designed around a "broadcast" mechanism. The default Windows behavior is to simply broadcast information on the local network. Installing a WINS server (and configuring the clients to use it) will reduce broadcast traffic.
- May 2001, www.networkice.com "since broadcasts do not travel across subnets, WINS may be the only way that two distant machines can find each other." and "WINS is similar to DNS: both systems will resolve a name into an IP address. DNS solves the general Internet naming problem, WINS is designed only for NetBIOS names. It is only used in the cases where NetBIOS applications (such as Windows File and Print Services) need to talk to each other."
- May 2001, www.networkice.com, NetBIOS name service. This is how NetBIOS-based services find each other. On a NetBIOS network, these names uniquely identify the machine and services running on the machine (and the IP address doesn't matter). Machines find each other either using broadcasts or looking them up in a centralized NetBIOS naming server (called a WINS server).

02/20-09:19:13.334557 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 202.5.45.175:137
02/20-09:19:32.913506 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 202.5.45.177:137
02/20-09:19:32.913506 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 202.5.45.177:137
02/20-09:19:58.596319 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 202.5.45.180:137
02/20-09:19:58.596319 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 202.5.45.180:137
02/20-09:20:18.193240 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 202.5.45.182:137
02/20-09:20:18.193240 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 202.5.45.182:137
…
02/20-19:32:37.476009 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 214.178.34.113:137
02/20-19:32:37.476009 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 214.178.34.113:137
02/20-19:32:49.515992 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 214.178.34.114:137

02/20-19:32:49.515992 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 214.178.34.114:137
02/20-19:33:22.722371 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 214.178.34.118:137
02/20-19:33:22.722371 [**] UDP SRC and DST outside network [**] 169.254.67.123:137 -> 214.178.34.118:137
…(Continued for over 350 packets)

This doesn't appear to be any problem. Again, the DHCP client was unable to connect to a DHCP server, and assigned itself the address 169.254. Again communication is attempted on port 137. The anomaly begins with the incrementing external addresses. Five separate address spaces are defined in the full packet detects. The registration information of those five address spaces follows:

204.130.227.4
Holladay Park Medical Center (NET-HOLLADAYPARK)
1225 NE 2nd Ave.
Portland OR 97232

214.178.34.118
DoD Network Information Center (NETBLK-DDN-NIC15)
7990 Boeing Court M/S CV-50
Vienna, VA 22183

202.5.45.180
Asia Pacific Network Information Center, Pty. Ltd.
Regional Internet Registry for the Asia-Pacific Region
Level 1 - 33 Park Road.
PO Box 2131
Milton QLD 4064
Australia

203.210.217.13
Asia Pacific Network Information Center, Pty. Ltd.
Regional Internet Registry for the Asia-Pacific Region
Level 1 - 33 Park Road.
PO Box 2131
Milton QLD 4064
Australia

203.174.188.37
DAVNET
Davnet Telecommunications
Level 7, 209 Castlereagh Street
Sydney NSW 2000
Australia

Likely, this is a company guest that has hooked their laptop into the local network. The

lack of a DHCP server and not knowing the IP address scheme keeps this user from plugging directly into the network. In areas where physical network security is not as strict, such as non-government corporations, DHCP servers can give instant access to company sensitive or proprietary information. This user can see information on the local segment, and with products like MacOff, can even sniff the switched network traffic through to the local routers. If this were the intent, however, it is unlikely this much information would be present on the network analyzer. The existence of three Australian companies that "receive" broadcast attempts may hold extra significance in deciphering this information.

Local Loopback

02/20-03:22:47.334414 [**] TCP SRC and DST outside network [**] 127.0.0.1:207 -> 1.1.1.1:29406
02/20-03:22:47.334414 [**] TCP SRC and DST outside network [**] 127.0.0.1:207 -> 1.1.1.1:29406
02/20-03:22:47.334717 [**] TCP SRC and DST outside network [**] 127.0.0.1:209 -> 1.1.1.1:29408
02/20-03:22:47.334717 [**] TCP SRC and DST outside network [**] 127.0.0.1:209 -> 1.1.1.1:29408
02/20-03:22:47.336243 [**] TCP SRC and DST outside network [**] 127.0.0.1:214 -> 1.1.1.1:29413
02/20-03:22:47.336243 [**] TCP SRC and DST outside network [**] 127.0.0.1:214 -> 1.1.1.1:29413
02/20-03:22:47.336382 [**] TCP SRC and DST outside network [**] 127.0.0.1:215 -> 1.1.1.1:29414
… (For a total of 1406 alerts)

Both the 127.0.0.1 and the 1.1.1.1 IP addresses are reserved by the IANA. The 127.0.0.1 address is the local loopback. It can be a valid remote destination IP address for certain applications, and careful consideration should be given to security and the loopback address.

A bugtraq article titled "Pointcast and destination IP 1.1.1.1" was replied to by *pedward@WEBCOM.COM* on Tue Nov 03 1998 - 22:48:30 GMT.

> They are checking to see if they have net connectivity, because it can run in offline mode. If you try to send a packet to an unreachable host, you'll get an ICMP unreachable -> EXXXX socket error.

This is unlikely the case for 1406 attempts within less than 30 minutes. This is more likely a spoofed address sending DoS packets in an attempt to overwhelm a device's port resources. This packet will be forwarded to the default router, who may attempt to reply with an ICMP error. The reply address is the loopback port, which will send the packet response to the router itself, potentially tying up the port the packet was sent from.

Defensive recommendations.

A summary analysis of the aggregate data

The overall network is working. A large number of false positives were seen in the data provided. Tuning of the IDS's may yield better results from the end Intrusion analysts. The following suggestions may lead to a more secure infrastructure, and decrease the overall administration costs due to unknown problems. These problems may stem from users abusing their network privileges, successful hacks, or undefined/lax system policies. In a place of business, not everyone can be the system administrator without rampant anarchy.

Network Problems

Internal Network Problems

- Core routers should check IP address source listings so that IP spoofing is not allowed internally (internal IP's are allowed out and external IP's are allowed in)

- Microsoft machines appear to be on the network – TCP ports 135, 137, 139 should be blocked at the least at the external routers. Null sessions allow enumeration from anywhere. With minimal noise, an outside user can determine usernames, domain trusts, and shares offered on this network.

- DHCP Servers appear to be used on the internal network. This greatly eases administration of the network, not requiring volumes of IP address to name maps. However, any user can bring any machine onto the network from any open port simply by plugging in. Care should be taken that foreign PC's are not introduced onto the network. Locking unused switch ports will aid in disallowing just any user from plugging into the network without any policies in place on the machine.

- Switch ports on the network can be changed from an active machine to a foreign PC by removing a currently working machine's network connection. The switches should be locked to the MAC address of the card to greater enhance the network's security. This will avoid PC's set to DHCP without a DHCP server on the network being allowed to sniff the network.

- Reserved ports are allowed (eg Port 0) and should be blocked at all routers.

- Any services not actually offered should be blocked at firewalls and external routers.

- Flags improperly set should be blocked at the network boundaries

External Network Problems

Reserved IP Addresses

- 0.x.x.x is currently a valid ip address – it is a broadcast address and should be blocked at outer router

- 1.x.x.x is currently a valid ip address – it is reserved and should be blocked at outer router
- non-routable ip addresses (10.x.x.x, 172.16.x.x 192.168.x.x) – should not be allowed from the outside to the inside
- non-assigned address spaces should be blocked at the firewalls

Use a stateful firewall to prevent external to internal scans.

Shun several thousand attempts in succession for a minimal amount of time (1 minute?)

Education

Remind internal users that overall network security rests on their shoulders. Ask before attempting to set up an internal web server, rogue Half-Life games, or internal network scans with unclean software. Typically administrators will point users to tools necessary for their work, and offer space for a few html pages to avoid the potential of incorrect software installation or unpatched, unfit machines becoming servers.

Insure passwords are not available to outside users, such as those written on post-it notes stuck to monitors.

Prevention

Scan the internal network regularly for unknown services.

Enforce Password complexity requirements, aging, and minimum lengths. Run password cracking programs against current SAM and Passwd files to keep users aware of security problems.

Allow red teams to perform surprise audits of the network. This will guarantee the day-to-day responsibility of security.

Regularly peruse IDS and Firewall logs for possible breaches. Better, dependent on the size of the company, have a full time IDS analyst that constantly watches the IDS logs to quickly respond to any possible problems.

Deploy attractive hacking options, such as honeypots, to minimize losses if a breach occurs.

Look into tripwire-esque programs to insure integrity of deployed servers.