Global Information Assurance Certification Paper

GCIA Certification

Practical Assignments

Steve Lukacs

Assignment 1 – Describe the State of Intrusion Detection

Introduction

Overview – The State of Intrusion Detection

Economics

Evolution

Intrusion Detection – The Future

Conclusion

Assignment 2 – Network Detects

Network Detect 1

Network Detect 2

Network Detect 3

Network Detect 4

Network Detect 5

Assignment 3 – "Analyze This" Scenario

Introduction

Scope

Word of Caution

Analysis Files

Data

Executive Summary

Defence recommendation

Analysis Process

SANS GIAC Assignment #1 - Describe the state of Intrusion Detection

Servants of INTRUSION DETECTION

Introduction

As the current generation of Intrusion Detection (ID) Systems attempt to incorporate all of the newest technologies, ideas and signatures, security analysts are faced with sorting and analysing the output of these systems.

Today's ID systems are complex, generate overwhelming numbers of logs and alerts with the expectation security analysts will have the training and time to sort it all out. ID systems employ varying types of technologies from traffic to content analysis but ID falls short when viewed from an enterprise perspective. The state of IDS is too complex and time intensive for the average business to dedicate funds to, thus only samples of alerts get attention, fewer systems are purchased and overall security suffers. This article is focused mainly from the perspective of the Snort IDS, an open source system at the leading edge of technology and competing successfully with the commercial world of Intrusion Detection.

Overview - The State of Intrusion Detection

From the complexities of setting up an Intrusion Detection System to the array of false alarms, users of Intrusion Detection Systems are faced with hundreds and even thousands of alerts. The task of determining whether alerts are real, false positives, malicious or normal network traffic is a time consuming task, which, means not only learning and understanding the intrusion detection system but also the intricacies of your network. Multiple tools are available to use with Snort and some are geared to help with determining what traffic is normal for one's network. For this type of analysis, Snort comes with a "plug in" called the Spade anomaly sensor, this "plug in" looks at all of the traffic on your network and attempts to learns what normal traffic looks like. Spade then attempts to report traffic that looks unusual or occurs infrequently, again adding to the massive number of alerts to be analysed, correlated and sorted.

Part of the problem with today's Intrusion Systems is that they only look at specific facets of the complete communication. Most ID systems are technology rich, contain multitudes of options and features but are far from user friendly and are inefficient in reducing the amount of time required to analyse network threats. Snort allows the Analyst to examine packets in detail to confirm alerts, an essential part of an ID system given the amounts of false alarms generated. Intrusion Detection Systems are merely the messenger delivering the package, which must be decrypted and interpreted. An analyst's job doesn't end at

finding the alert but digging deeper, looking into the packet and determining what is actually happening. This kind of technical forensics is difficult and takes excessive amounts of time, something that every IDS analyst must become adept at if they are to be successful in identifying real alarms.

Economics

From a business point of view Intrusion Detection can be financially prohibitive, since the cost of some ID systems and the support they require are out of the range of some businesses and potentially rule out using IDS as part of their security architecture. With the complexity of current Intrusion Detection Systems, there is a reliance on highly trained people to interpret the data emanating from these systems. Unfortunately, the number of trained people is relatively small. At present supply does not meet demand as indicated in the August issue of Information Security Magazine (Pg 44). This article reveals the increasing financial incentives designed to lure qualified IT professionals, particularly trained security analysts and especially GCIA certified Intrusion Analysts. With Intrusion Detection Systems such as Snort, there is not only a need for people who are trained in IDS administration and alert analysis but the need for people who will take an active role in the discovery and verification of new signatures, and open source development of the ID system itself.

Evolution

There is a race in Intrusion Detection Systems to offer the greatest features, highest performance, latest signatures and newest technologies in an effort to detect potential reconnaissance, attacks or infiltration of one's network. This leads to little stability in this market place and places greater strain on the job at hand -- detecting and mitigating security risks. If Analyst's are spending excessive amounts of time upgrading, patching, configuring and sorting through hundreds and thousands of alerts, the IDS is not contributing enough to the security of the network and in fact is potentially chewing up precious time that could be spent administering other security systems. The current generation of IDS logs and alerts are usually found in the form of text output that with some additional tools such as Snortsnarf, can be converted to html output. This output provides users with detected signatures, signature definitions, statistics, and other useful information formatted for easy navigation. However, the limitations of all text type output is the lack of view that an Analyst needs to see the big picture. Unfortunately there are few systems offering a clear comprehensive graphical view allowing the user to see exactly what's happening and what devices are affected. The type of view that could be used by less experienced security staff to help identify threats, take actions and allow those not specializing in Intrusion Detection to make a contribution to network security.

Intrusion Detection – The Future

IDS vendors, developers, and the Security Industry should endeavour to develop data correlation and dynamic event action into new systems. Of course, this exists today -- in part, with Snort additions such as Guardian, or SnortSam, which can dynamically change IP Chain's and Checkpoint Firewall-1 rules to a limited degree. The current state of "Active IDS" doesn't inspire confidence when one considers the amount of false alerts generated by these systems and the potential to cut off critical traffic entering and exiting one's network.

The current complement of network intrusion detection systems, host intrusion detection systems, routers, and firewalls, all handle the data gram as it makes its way through the network. All of these devices are capable of generating alerts, logs and taking action to various degrees. Using these devices in a centralized system would make Network Security much easier and require much less time from Analysts.

The next generation of Intrusion Detection Systems should use a comprehensive Security Management System or at least have the ability to interface into a traditional Network Management system. These systems would help to visually indicate where attacks are happening and how they are affecting devices and systems. They would document and archive the frequency of attacks and have the ability to change attributes of a device in real-time – thus limiting exposure and preventing attacks. The Security Management System would be based on comprehensive database containing representative models of the servers, firewalls, routers, switches, and other devices in one's network and potentially outside of one's network. Each device model in the database would contain information regarding operating system type, patch levels, applications, vulnerabilities, defence capabilities, and more. The database would contain information concerning what security measures the device itself can deploy, allowing the IDS system to call on that device to take action in the event of an alert.

The future of Intrusion Systems needs to be a combined system, which links all devices in a network such as routers, firewalls, NIDS and HIDS to allow real-time event correlation. This would help to eliminate false positives by providing information on how the packet affected each device on it's way through the network and whether there were any adverse reactions from the devices it traveled through. The Security Management System would learn of new threats and dynamically react to them in various ways. If a host within the protection zone was hit with an attack, the Host IDS, Virus Scanner or other host based monitors would provide information to the NIDS to help with attack recognition. Attributes such as attack signature, source address and hits would be compared to previous attack signatures. The NIDS would then be able to inform the Security Management System of the recognized signature and in turn instruct the firewall to form an instant defence. The firewall would block access to the host from the attacking IP address or block the signature on a wider scale. If the signature was not recognized, the Security Management System could provide the security administrator with real-time perimeter information and tactical options. Once a known signature was "mature" the

firewall or router would contain a table of known attacks and block these packets before they reached the host. This would eliminate the latency required by the Security Management System to learn and react to signatures.

The graphical based Security Management System would show each device with a security defence rating allowing analysts' to focus in on weak spots in their architecture. Signature based IDS would know which signatures apply to which hosts and greatly limit false positives and the work required by analyst's to review alerts. Traffic based IDS would be readily visible on the Security Management System and show origins of attacks and their history (if any). These would be correlated with the signature based IDS to show common attacks such as Denial of Service, IP address spoofing, fragmentation attacks and many others. The SMS would provide real-time solutions such as dynamically changing a router access list, shutting down a service on a system, or changing a firewall rule set. It could even go as far as to automatically run scripts or programs to check for things such as trojans, rootkits or binary file modifications when signatures indicate a system compromise. Alerts and actions would be displayed graphically on the Security Management System. They would include security level ratings for each object in the network including routers, switches, hosts and the applications they house. Each device/system would be displayed with their corresponding security rating. The security rating would be dynamically updated according to how each host or device responded to reconnaissance or attacks directed at it. Reports on the security ratings of hosts and devices could be exported and reports provided to the vendors. This would put the responsibility on them to provide more secure systems.

Conclusion

Today's systems place the focus of Intrusion Detection on the Security Analyst and their ability to read and decipher the generated alerts. The future of Intrusion Detection will further remove that dependency and place more of the analysis at the system level. Pioneering ID systems such as Snort are paving the road for the next generation of systems and with the support of organizations likes SANS and the open source community, the goal of self contained, proactive ID can become reality.

References

Information Security Magazine
Andy Briney, New Direction in Intrusion Detection,
http://www.infosecuritymag.com/articles/august01/cover.shtml
Information Security Magazine
Pete Loshin, "Meta Detection",
http://www.infosecuritymag.com/articles/august01/cover.shtml

Sys Admin Magazine

Jason Chan, Distributed Intrusion Detection with Open Source Tools
http://www.samag.com/documents/s=1147/sam0108b/

Network Magazine
Rik Farrow, Summer Dreams of IDS
http://networkmagazine.com/article/NMG20010718S0004

Sans Reading Room
James Kipp, Using Snort as an IDS and Network Monitor in Linux
http://www.sans.org/infosecFAQ/intrusion/monitor.htm

SANS GIAC Assignment #2 – Network Detects

Network Detect #1

[**] [1:221:1] DDOS TFN Probe [**]
[Classification: Attempted Information Leak] [Priority: 3]
09/28-06:46:03.857506 MY.NET.66.47 -> MY.NET.16.65
ICMP TTL:60 TOS:0x0 ID:678 IpLen:20 DgmLen:84
Type:8 Code:0 ID:6918 Seq:768 ECHO
[Xref => http://www.whitehats.com/info/IDS443]

(Payload Data)

[**] DDOS TFN Probe [**]
09/28-06:46:03.857506 MY.NET.66.47 -> MY.NET.16.65
ICMP TTL:60 TOS:0x0 ID:678 IpLen:20 DgmLen:84
Type:8 Code:0 ID:6918 Seq:768 ECHO
47 62 B4 3B 61 10 0E 00 08 09 0A 0B 0C 0D 0E 0F Gb.;a.....
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F .....
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F !"#$%&'()*+,-./
30 31 32 33 34 35 36 37 01234567

Source of Trace
My Network

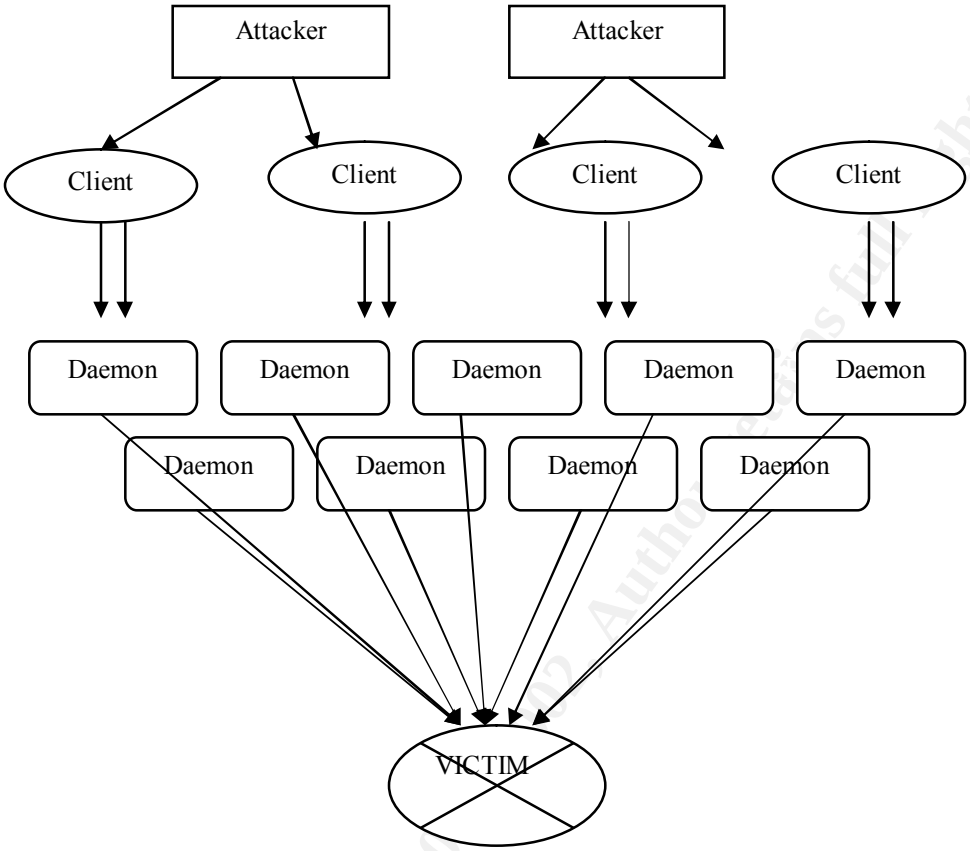
Detect Generated by:
Snort IDS 1.8 listening on Multiple VLAN Subnets.

Possibility the source address was spoofed

Low: The sender is attempting to find an active TFN (Tribal Flood Network) client or daemon, requiring a response from the target.

Description of Attack

- The DDOS TFN Probe is not an actual attack. The Probe as described will attempt to find Trojan installations of the Tribal Flood Network client or daemon. Once found the sender will attempt to connect to the Trojan and take control of it. The sender will then be able to launch Distributed Denial of Service attacks against targets with multiple daemons.
- Once a TFN Network has been established, the method of attack starts with the attackers sending commands to multiple clients who each control multiple daemons. The daemons are used to perform the actual attack on the victims.



Attack Mechanism

- The TFN probe scans for the TFN daemon utilizing ICMP as a communications channel. This type of communication is particularly unusual due to the nature of TCP/IP and ICMP connections. Generally, most applications use the Transmission Control Protocol or User Datagram Protocol to communicate on IP networks. ICMP (Internet Control Message Protocol) is used as a controlling protocol and is not used for direct communication.
- The TFN attack uses Denial of service attacks such as ICMP floods, SYN Floods, Smurf attacks, UDP Floods, ICMP floods to overwhelm the victim causing a denial of service.

Correlations

- SANS Practical, January 28, 2001 -- Miika Turkia Detected TFN Probe from his network. http://www.sans.org/giactc/gcia.htm
- David Dittrich's lab test of TFN - http://staff.washington.edu/dittrich/misc/tfn.analysis

Evidence of Active Targeting

Active targeting may be in play here because the destination host is a Unix system. However, there were no other attempts to connect to this machine from this IP address and no other scans were attempted.

Severity

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

Criticality = 5 (DNS Server)
Lethality = 1 (Probe for DDOS Clients, Daemons)
System countermeasure = 5 (TFN Not Installed, Unix machine no infiltrated)
Network countermeasure = 3 (DDOS attacks from TFN would have limited success due to egress filters, although outbound ICMP is permitted. IDS active)
Severity = (Criticality + Lethality) - (System + Network Countermeasures)

Severity (5 + 1) = 6 – (5 + 3) =8 (-2)

Defensive Recommendations

There are multiple ways in which an intruder can gain access to a Unix system to install and activate the TFN client or daemon.

Vulnerabilities CERT have seen exploited as a part of these attacks include:

- CA-99-08 - Buffer Overflow Vulnerability in rpc.cmsd

  http://www.cert.org/advisories/CA-99-08-cmsd.html

- CA-99-05 - Vulnerability in statd exposes vulnerability in automountd

  http://www.cert.org/advisories/CA-99-05-statd-automountd.html

- CA-98.11 - Vulnerability in ToolTalk RPC Service

  http://www.cert.org/advisories/CA-98.11.tooltalk.html

Steps you can take to mitigate the risk:

1. Apply latest service packs, and security patches.
2. Only run services that are required.
3. Remove services that are not required. This prevents someone from accidentally starting a service that may be vulnerable.
4. Block access to all ports that are not in use via your Filtering Router and Firewall.
5. Use egress filtering on your Router and firewall to block DDOS attacks that may originate from your network.

Multiple Choice test Question

Tribal Flood Network uses ICMP_____for communications?

1. Code 8, Type 0
2. Type 8, Code 0
3. Code 4, Type 1
4. Type 2, Code 2

Answer: Type 8, Code 0

Network Detect #2

[**] [1:338:1] FTP EXPLOIT format string [**]
[Classification: Attempted User Privilege Gain] [Priority: 8]
09/10-09:14:47.362622 207.158.33.203:3578 -> MY.NET.16.71:21
TCP TTL:39 TOS:0x0 ID:48418 IpLen:20 DgmLen:76 DF
AP Seq: 0xA44597DB Ack: 0xD1C63509 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 386175660 102742165
[Xref => http://www.whitehats.com/info/IDS453]

(Payload Data)

[**] FTP EXPLOIT format string [**]
09/10-09:14:47.362622 207.158.33.203:3578 -> MY.NET.16.71:21
TCP TTL:39 TOS:0x0 ID:48418 IpLen:20 DgmLen:76 DF
AP Seq: 0xA44597DB Ack: 0xD1C63509 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 386175660 102742165
53 49 54 45 20 45 58 45 43 20 25 30 32 30 64 7C SITE EXEC %020d|
25 2E 66 25 2E 66 7C 0A   %.f%.f|.

Source of Trace
My Network

Detect Generated by:
Snort IDS 1.8 listening on Multiple VLAN Subnets.

Possibility the source address was spoofed
Low: The attacker would attempt to exploit this vulnerability and gain a root access, thus requiring a response.

Description of Attack

The attacker attempts to fool the vulnerable ftp daemon into executing a root level command by constructing conversion characters with the printf() conversion characters. Multiple ftp daemons are vulnerable to this exploit

Attack Mechanism

Description taken from http://www.cert.org/advisories/CA-2000-13.html#vendors

The "site exec" vulnerability is the result of missing character-formatting argument in several function calls that implement the "site exec" command functionality. Normally if "site exec" is enabled, a user logged into an ftp server (including the 'ftp' or 'anonymous' user) may execute a restricted subset of quoted commands on the server itself. However, if a malicious user can pass character format strings consisting of carefully constructed *printf() conversion characters (%f, %p, %n, etc) while executing a "site exec" command, the ftp daemon may be tricked into executing arbitrary code as root.

Correlations

The "Site Exec" vulnerability was used by the Ramen worm as described on the SANS Web Site.

http://www.sans.org/y2k/ramen.htm

Evidence of Active Targeting

Active targeting is likely. This exploit was attempted on an ftp daemon running on the Unix host suggesting previous scans or connection attempts were made during reconnaissance phase. The FTP daemon running on this host is not vulnerable to this exploit.

Severity

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

Criticality = 3 (FTP Server)
Lethality = 5 (Could cause root compromise)

System countermeasure = 5 (Wu-FTP 2.6.0 was patched with recommended vendor patches as per cert advisory)
Network countermeasure = 3 (FTP Server – FTP connections permitted, egress filtering active, IDS active)
Severity = (Criticality + Lethality) - (System + Network Countermeasures)

Severity (3 + 5) = 8 – (5 + 3) =8 (0)

Defensive Recommendations

Apply source code change to Wu-FTP 2.6.0 as follows:

```
--- src/ftpcmd.y.orig           Wed Oct 13 11:15:28 1999
+++ src/ftpcmd.y   Fri Jun 30 11:42:40 2000
@@ -1926,13 +1926,13 @@
            }
            if (!maxfound)
               maxlines = defmaxlines;
-           lreply(200, cmd);
+           lreply(200, "%s", cmd);
            while (fgets(buf, sizeof buf, cmdf)) {
               size_t len = strlen(buf);

               if (len > 0 && buf[len - 1] == '\n')
                        buf[--len] = '\0';
-              lreply(200, buf);
+              lreply(200, "%s", buf);
               if (maxlines <= 0)
                        ++lines;
               else if (++lines >= maxlines) {
--- src/ftpd.c.orig   Thu Oct 14 10:41:47 1999
+++ src/ftpd.c       Fri Jun 30 11:42:40 2000
@@ -3156,7 +3156,7 @@
            reply(230, "User %s logged in.%s", pw->pw_name, guest ?
                "  Access restrictions apply." : "");
            sprintf(proctitle, "%s: %s", remotehost, pw->pw_name);
-           setproctitle(proctitle);
+           setproctitle("%s", proctitle);
            if (logging)
               syslog(LOG_INFO, "FTP LOGIN FROM %s, %s", remoteident, pw-
>pw_name);
 /* H* mod: if non-anonymous user, copy it to "authuser" so everyone can
@@ -5888,7 +5888,7 @@

    remotehost[sizeof(remotehost) - 1] = '\0';
    sprintf(proctitle, "%s: connected", remotehost);
```

```
-    setproctitle(proctitle);
+    setproctitle("%s", proctitle);

     wu_authenticate();
 /* Create a composite source identification string, to improve the logging
```

Multiple Choice test Question

Finding if WU-FTP has been patch for this exploit can be done by…

1. Typing in Wu-Ftp –v in a shell.
2. Checking ftpcmd.y and ftpd.c for the required changes.
3. FTP to the WU-FTP server and check the application version displayed in the banner.
4. Typing in wuftpd –V in a shell.

Answer: 2

Network Detect #3

```
[**] [1:160:1] BACKDOOR NetMetro Incoming Traffic [**]
09/26-15:20:25.976296 24.70.188.249:5031 -> MY.NET.16.114:25
TCP TTL:242 TOS:0x0 ID:22360 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x5B38141F  Ack: 0x68C75B67  Win: 0x4470  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS79]

[**] [1:160:1] BACKDOOR NetMetro Incoming Traffic [**]
09/26-15:20:26.438982 24.70.188.249:5031 -> MY.NET.16.114:25
TCP TTL:242 TOS:0x0 ID:22361 IpLen:20 DgmLen:89 DF
***AP*** Seq: 0x5B38141F  Ack: 0x68C75B67  Win: 0x4470  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS79]

[**] [1:160:1] BACKDOOR NetMetro Incoming Traffic [**]
09/26-15:20:29.785213 24.70.188.249:5031 -> MY.NET.16.114:25
TCP TTL:242 TOS:0x0 ID:22362 IpLen:20 DgmLen:73 DF
***AP*** Seq: 0x5B381450  Ack: 0x68C75BA5  Win: 0x4470  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS79]
```

(Payload Data)

```
[**] BACKDOOR NetMetro Incoming Traffic [**]
09/26-15:20:30.211781 24.70.188.249:5031 -> MY.NET.16.114:25
TCP TTL:242 TOS:0x0 ID:22364 IpLen:20 DgmLen:208 DF
***AP*** Seq: 0x5B381477  Ack: 0x68C75C0A  Win: 0x4470  TcpLen: 20
```

```
52 65 63 65 69 76 65 64 3A 20 66 72 6F 6D 20 31  Received: from 1
39 32 2E 31 36 38 2E 31 2E 34 20 28 5B 32 34 2E  92.168.1.4 ([24.
37 30 2E 31 38 38 2E 32 35 30 5D 29 20 62 79 20  70.188.250]) by
6D 61 69 6C 2E 72 61 65 62 65 72 67 72 61 70 68  mail.raebergraph
69 63 73 2E 63 6F 6D 20 28 41 70 70 6C 65 53 68  ics.com (AppleSh
61 72 65 20 49 50 20 4D 61 69 6C 20 53 65 72 76  are IP Mail Serv
65 72 20 36 2E 32 2E 31 29 20 69 64 20 33 33 38  er 6.2.1) id 338
33 37 32 20 76 69 61 20 54 43 50 20 77 69 74 68  372 via TCP with
20 53 4D 54 50 3B 20 57 65 64 2C 20 32 36 20 53   SMTP; Wed, 26 S
65 70 20 32 30 30 31 20 31 35 3A 32 39 3A 32 39  ep 2001 15:29:29
20 2D 30 36 30 30 0D 0A                          -0600..
```

Source of Trace
My Network

Detect Generated by:
Snort IDS 1.8 listening on Multiple VLAN Subnets.

Possibility the source address was spoofed
Low: NetMetro requires a response from the destination address for communication.

Description of Attack
This is client to server communication between the NetMetro Trojan and NetMetro user.

Attack Mechanism
NetMetro is a Trojan application that is used to take control of Windows Hosts. Once the Trojan is installed, the attacker can control the Windows host remotely and perform any task required. This is equivalent to a root level compromise on a Unix host. In general, inexperienced hackers do this type of attack. They may also use this type of Trojan to gain access to the host and use it as a Warez site or to attack other systems.

Correlations
None

Evidence of Active Targeting
At first glance this scan appears to be active targeting as the destination host is hit hundreds of times.

Further observations:

- An nslookup on the IP address of the source host resolves to mail.raebergraphics.com, which seems to be a mail server.
- The ttl value of each packet is 255, which points to the source host being Solaris 7 or lower.

- The packet payload contains mail data.

Synopsis: Snort has picked up on a false positive due to the signature of the packets. Source – 5031, Destination = 25. This is actually response traffic from a SMTP connection.

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

Criticality = 4 (Mail Server)
Lethality = 5 (Windows Trojan NetMetro, active installation)
System countermeasure = 5 (Unix machine, NetMetro cannot be installed)
Network countermeasure = 5 (Legitimate Traffic, IDS active)
Severity = (Criticality + Lethality) - (System + Network Countermeasures)

Severity (4 + 5) = 9 – (5 + 5) =10 (-1)

Defensive Recommendations
None: Legitimate SMTP Traffic

Multiple Choice test Question

TTL values help identify Operating Systems because…

1. Certain Operating Systems have no TTL
2. TTL only works on Unix hosts
3. Each Operating System has a default TTL
4. NetMetro uses TTL to probe hosts

Answer: 3

Network Detect #4

[**] [1:528:1] MISC loopback traffic [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
09/30-00:40:55.918352 MY.NET.16.88:35159 -> 127.4.2.1:25
TCP TTL:64 TOS:0x0 ID:13657 IpLen:20 DgmLen:48 DF
******S* Seq: 0x31B5B5A5 Ack: 0x0 Win: 0x60F4 TcpLen: 28
TCP Options (4) => NOP NOP SackOK MSS: 1460

(Mail Server Log)

Sep 30 00:40:55 smtp2 sendmail[27164]: [ID 801593 mail.info] f8PIHhu05769: to=<mennonitechick@fastmail.com>, delay=4+11:23:12, xdelay=00:22:28, mailer=esmtp, pri=17333727, relay=smtp03.fastmail.com. [127.4.2.1], dsn=4.0.0, stat=Deferred: Connection timed out with smtp03.fastmail.com.

Additional Data

```
; <<>> DiG 9.1.0 <<>> mx fastmail.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47204
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 3, ADDITIONAL: 7

;; QUESTION SECTION:
;fastmail.com.          IN    MX

;; ANSWER SECTION:
fastmail.com.       3600    IN    MX    50 smtp03.fastmail.com.
fastmail.com.       3600    IN    MX    50 smtp04.fastmail.com.
fastmail.com.       3600    IN    MX    10 smtp01.fastmail.com.
fastmail.com.       3600    IN    MX    20 smtp02.fastmail.com.

;; AUTHORITY SECTION:
fastmail.com.       3600    IN    NS    dns01.fastweb.com.
fastmail.com.       3600    IN    NS    dns02.fastweb.com.
fastmail.com.       3600    IN    NS    dns03.fastweb.com.

;; ADDITIONAL SECTION:
smtp03.fastmail.com.    3600    IN    A    127.4.2.1
smtp04.fastmail.com.    3600    IN    A    127.0.10.2
smtp01.fastmail.com.    3600    IN    A    127.0.0.1
smtp02.fastmail.com.    3600    IN    A    127.1.1.1
dns01.fastweb.com.    3600    IN    A    216.34.178.196
dns02.fastweb.com.    3600    IN    A    216.34.178.197
dns03.fastweb.com.    3600    IN    A    63.121.30.152

;; Query time: 264 msec
;; SERVER: MY.NET.16.65#53(MY.NET.16.65)
;; WHEN: Mon Oct  8 15:55:22 2001
;; MSG SIZE  rcvd: 305
```

Source of Trace
My Network

Detect Generated by:
Snort IDS 1.8 listening on Multiple VLAN Subnets.

Possibility the source address was spoofed
Low: Since this packet is a return email, the source address is from the local MY.NET mail server and is not spoofed.

Description of Attack
This attack is used to send SPAM mail and re-direct replies elsewhere.

Attack Mechanism
Assigning a loopback address for each of the mx records for fastmail.com's mail servers allows mailers to send SPAM mail and never have it returned. When the recipient mail server attempts to reply to fastmail.com it performs a lookup on the mx records for fastmail.com, that lookup resolves the smtp servers to a 127.x.x.x address as seen below. IANA assigns 127.x.x.x to local loopback. The reply mail would be send to the loopback address on the MY.NET mail server, potentially causing Denial Of Service. This type of attack is similar to a SYN flood in networking.

smtp01.fastmail.com – 127.0.0.1
smtp02.fastmail.com – 127.1.1.1
smtp03.fastmail.com – 127.4.2.1
smtp04.fastmail.com – 127.0.10.2

whois whois.arin.net 127.0.0.1:
IANA (LOOPBACK)
Internet Assigned Numbers Authority
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6695
US

Netname: LOOPBACK
Netblock: 127.0.0.0 - 127.255.255.255

Coordinator:
Internet Corporation for Assigned Names and Numbers (IANA-ARIN) res-ip@iana.org
(310) 823-9358

Record last updated on 02-Mar-1998.
Database last updated on 5-Oct-2001 23:18:41 EDT.

Correlations
None

Evidence of Active Targeting
Medium: The SPAM mailer likely scanned this server for an SMTP server. Once the attacker discovered this host was accessible, it began sending bulk SPAM.

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

Criticality = 5 (Mail Server)
Lethality = 3 (I have rated this as a 3 because SPAM mail can cause heavy loads on mail servers. Additionally, with the reply address resolving to a local loopback address this increases the load on the mail server as it has to wait for the connection to timeout)

System countermeasure = 4 (The source domain was block within the SMTP server. I only gave it a 4 since Spammers change their sending addresses frequently)
Network countermeasure = 4 (The source domain was blocked via the border router.)
Severity = (Criticality + Lethality) - (System + Network Countermeasures)

Severity (5 + 3) = 8 – (4 + 4) =8 (0)

Defensive Recommendations

- Block the DNS names of these addresses on your firewall or filtering router.
- Block connection attempts from these mail addresses in the sendmail configuration.

Multiple Choice test Question

Blocking SPAM can be accomplished by?

1. Filtering SPAM mailers IP addresses at your router
2. Filtering SPAM mailers IP addresses at your firewall
3. Filtering SPAM mailers IP addresses at your mail server
4. All of the above

Answer: 4

Network Detect #5

[**] [1:499:1] MISC Large ICMP Packet [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
09/29-17:52:10.103769 24.94.162.75 -> MY.NET.16.65
ICMP TTL:236 TOS:0x0 ID:32749 IpLen:20 DgmLen:1420 DF
Type:8 Code:0 ID:96 Seq:58546 ECHO
[Xref => http://www.whitehats.com/info/IDS246]

(Payload Data)

```
[**] MISC Large ICMP Packet [**]
09/29-17:52:10.103769 24.94.162.75 -> MY.NET.16.65
ICMP TTL:236 TOS:0x0 ID:32749 IpLen:20 DgmLen:1420 DF
Type:8  Code:0  ID:96   Seq:58546  ECHO
6D 61 69 6C 74 6F 3A 6F 70 73 40 64 69 67 69 73  mailto:ops@digis
6C 65 2E 63 6F 6D 20 66 6F 72 20 71 75 65 73 74  le.com for quest
69 6F 6E 73 20 20 20 20 54 68 69 73 20 49 43 4D  ions    This ICM
50 20 45 43 48 4F 20 52 45 51 55 45 53 54 2F 52  P ECHO REQUEST/R
45 50 4C 59 20 69 73 20 70 61 72 74 20 6F 66 20  EPLY is part of
74 68 65 20 72 65 61 6C 2D 74 69 6D 65 20 6E 65  the real-time ne
74 77 6F 72 6B 20 6D 6F 6E 69 74 6F 72 69 6E 67  twork monitoring
70 65 72 66 6F 72 6D 65 64 20 62 79 20 44 69 67  performed by Dig
69 74 61 6C 20 49 73 6C 61 6E 64 20 49 6E 63 2E  ital Island Inc.
20 20 49 74 20 69 73 20 6E 6F 74 20 61 6E 20 61    It is not an a
74 74 61 63 6B 2E 20 20 49 66 20 79 6F 75 20 68  ttack.  If you h
61 76 65 71 75 65 73 74 69 6F 6E 73 20 70 6C 65  avequestions ple
61 73 65 20 63 6F 6E 74 61 63 74 20 6F 70 73 40  ase contact ops@
64 69 67 69 73 6C 65 2E 63 6F 6D 00 00 00 00 00  digisle.com.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Source of Trace
My Network

Detect Generated by:
Snort IDS 1.8 listening on Multiple VLAN Subnets.

Possibility the source address was spoofed
Low: This ICMP Packet has embedded information from the senders and is meant to provide a service to the senders customers.

Description of Attack
ICMP Packets are sent to the recipient to map network or system response times.

Attack Mechanism
The ICMP packets have embedded messages meant for sites with Intrusion Detection Systems. The message is:
mailto:ops@digisle.com for questions. This ICMP ECHO REQUEST/REPLY is part of the real-time network monitoring performed by Digital Island Inc. It is not an attack. If you have questions please contact ops@digisle.com

Correlations
Erik Carus experience the same ICMP packets from Digital Island.
http://www.incidents.org/archives/y2k/072500-1200.htm

Evidence of Active Targeting
High: These packets are sent specifically to the DNS server to map response time.

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

Criticality = 4 (DNS Server)
Lethality = 1 (Response Time Mapping, could cause network flooding.)
System countermeasure = 0 (System Responds to ICMP echo requests)
Network countermeasure = 5 (Block large ICMP packets at firewall)
Severity = (Criticality + Lethality) - (System + Network Countermeasures)

Severity (4 + 1) = 5 – (0 + 5) =5 (0)

There is potential that these packets could cause some type of buffer overflow or denial of service if the host is under high load already.

Defensive Recommendations

- Send mail to the address provided in the ICMP echo requesting Digital Island to stop monitoring.
- Block the source addresses of the ICMP echo requests via a filtering router or firewall. **Note**: Blocking these packets is difficult due to the distributed nature of Digital Islands networks.
- Block large ICMP packets at firewall

Multiple Choice test Question

Embedded ICMP data can be used for…

1. Covert communication channels
2. Buffer overflow attacks
3. Application Control
4. All of the above

Answer: 4

SANS GIAC Assignment #3 – "Analyze This" Scenario

Security Audit – SANS University

Introduction

This audit has been conducted at the request of SANS University and is based on Intrusion Detection Logs provided by SANS. The Intrusion Detection System in use at SANS is Snort 1.x with a standard rulebase. Three types of logs were provided. Alert Logs – Logs containing possible signature matches made by the Snort IDS. Scan Logs – Logs containing network reconnaissance scans as identified by the Snort IDS. Lastly, the third log format is OOS logs – Log containing out of scope packet detail as captured by the Snort IDS. All log files were provided in Standard output (text).

Scope

The scope of the SANS audit is to provide a security assessment of the SANS University network with a snapshot spanning over a consecutive 5 day period. All analysis is based entirely from the provided logs. The analysis of the SANS network will contain specific recommendations to improve security, provide knowledge transfer, identify security breaches, assess vulnerabilities, and provide risk mitigation for the SANS University Network. Due to time limitations not all alerts will be individually assessed. Some alerts fall into general categories and general assumptions will be made. Alerts indicating likely exploits and attacks will be provided with a detailed analysis.

Word of Caution

Intrusion Detection Systems are known to generate false positives. When taking recommendations into account please note that not all signatures will actually be accurate and additional analysis will be required. A full network analysis will be required to monitor and track down the cause of certain alerts.

Analysis files:

Alert, OOS, Scan Sept 15 –19, 2001

Alert Signatures	Total	Percentage
WEB-MISC Attempt to execute cmd	323195	39%
ICMP Echo Request speedera	158656	19%
IDS552/web-iis_IIS ISAPI Overflow ida nosize	126277	15%
spp_http_decode: IIS Unicode attack detected	96023	12%
MISC Large UDP Packet	47282	6%
INFO MSN IM Chat data	7528	1%
ICMP Destination Unreachable (Communication Administratively Prohibited)	6309	1%
ICMP Echo Request Nmap or HPING2	6223	1%
WEB-MISC prefix-get //	4941	1%
MISC source port 53 to <1024	4658	1%
MISC traceroute	4029	0%
INFO Napster Client Data	2664	0%

CS WEBSERVER - external web traffic	2645	0%
Watchlist 000220 IL-ISDNNET-990517	2575	0%
ICMP Destination Unreachable (Network Unreachable)	2545	0%
TFTP - Internal TCP connection to external tftp server	2230	0%
ICMP Destination Unreachable (Host Unreachable)	1791	0%
INFO napster login	1779	0%
Possible trojan server activity	1139	0%
INFO Inbound GNUTella Connect accept	1045	0%
ICMP Fragment Reassembly Time Exceeded	1033	0%
TCP SRC and DST outside network	1010	0%
Incomplete Packet Fragments Discarded	932	0%
BACKDOOR NetMetro Incoming Traffic	928	0%
SMTP relaying denied	911	0%
Port 55850 tcp - Possible myserver activity - ref. 010313-1	903	0%
Null scan!	864	0%
ICMP traceroute	857	0%
UDP SRC and DST outside network	790	0%
FTP DoS ftpd globbing	656	0%
WEB-MISC 403 Forbidden	484	0%
ICMP Echo Request BSDtype	449	0%
ICMP Echo Request CyberKit 2.2 Windows	363	0%
INFO FTP anonymous FTP	338	0%
EXPLOIT x86 NOOP	336	0%
Tiny Fragments - Possible Hostile Activity	310	0%
INFO Possible IRC Access	280	0%
Watchlist 000222 NET-NCFC	254	0%
SMB Name Wildcard	246	0%
INFO Outbound GNUTella Connect accept	243	0%
ICMP Echo Request Windows	167	0%
ICMP Echo Request Sun Solaris	158	0%
beetle.ucs	151	0%
TFTP - Internal UDP connection to external tftp server	120	0%
BACKDOOR NetMetro File List	105	0%
High port 65535 tcp - possible Red Worm - traffic	100	0%
TELNET login incorrect	99	0%
SCAN Proxy attempt	99	0%
FTP CWD / - possible warez site	216	0%
WEB-IIS Unauthorized IP Access Attempt	85	0%
ICMP Source Quench	81	0%
ICMP Echo Request L3retriever Ping	75	0%
High port 65535 udp - possible Red Worm - traffic	72	0%
WEB-MISC http directory traversal	68	0%
WEB-IIS File permission canonicalization(Chinese charset)	61	0%
MISC Large ICMP Packet	61	0%
ICMP Destination Unreachable (Protocol Unreachable)	58	0%
WEB-IIS File permission canonicalization	46	0%

WEB-IIS File permission canonicalization	45	0%
Queso fingerprint	45	0%
ICMP Destination Unreachable (Fragmentation Needed and DF bit was set)	44	0%
x86 NOOP - unicode BUFFER OVERFLOW ATTACK	41	0%
ICMP Echo Request Delphi-Piette Windows	40	0%
EXPLOIT x86 setuid 0	38	0%
WEB-MISC count.cgi access	34	0%
connect to 515 from outside	34	0%
INFO napster upload request	33	0%
WinGate 1080 Attempt	31	0%
WEB-MISC compaq nsight directory traversal	27	0%
RPC tcp traffic contains bin_sh	27	0%
NMAP TCP ping!	25	0%
External RPC call	25	0%
EXPLOIT x86 setgid 0	25	0%
WEB-FRONTPAGE _vti_rpc access	23	0%
Port 55850 udp - Possible myserver activity - ref. 010313-1	20	0%
INFO - Web Cmd completed	19	0%
WEB-CGI redirect access	16	0%
SCAN FIN	16	0%
WEB-IIS _vti_inf access	15	0%
CS WEBSERVER - external ftp traffic	15	0%
Back Orifice	14	0%
WEB-CGI scriptalias access	13	0%
WEB-MISC L3retriever HTTP Probe	12	0%
SUNRPC highport access!	12	0%
SCAN Synscan Portscan ID 19104	11	0%
EXPLOIT x86 stealth noop	10	0%
WEB-FRONTPAGE shtml.dll	9	0%
WEB-CGI csh access	9	0%
connect to 515 from inside	9	0%
WEB-FRONTPAGE fpcount.exe access	8	0%
X11 outgoing	7	0%
WEB-CGI cvsweb.cgi access	7	0%
SMTP chameleon overflow	7	0%
WEB-FRONTPAGE fourdots request	6	0%
Virus - Possible pif Worm	6	0%
Russia Dynamo - SANS Flash 28-jul-00	6	0%
IDS50/trojan_trojan-active-subseven	6	0%
EXPLOIT x86 NOPS	6	0%
WEB-MISC guestbook.cgi access	5	0%
WEB-IIS view source via translate header	5	0%
WEB-CGI ksh access	5	0%
WEB-MISC Lotus Domino directory traversal	4	0%
WEB-CGI tsch access	4	0%

TCP SMTP Source Port traffic	4	0%
spp_http_decode: CGI Null Byte attack detected	4	0%
INFO – Possible Squid Scan	4	0%
ICMP SRC and DST outside network	4	0%
X11 xopen	3	0%
WEB-MISC whisker head	3	0%
WEB-FRONTPAGE shtml.exe	3	0%
WEB-CGI formmail access	3	0%
ICMP Redirect (Network)	3	0%
WEB-IIS encoding access	2	0%
WEB-CGI rsh access	2	0%
Virus – Possible scr Worm	2	0%
TFTP - External TCP connection to internal tftp server	2	0%
SYN-FIN scan!	2	0%
SNMP public access	2	0%
MISC PCAnywhere Startup	2	0%
DNS zone transfer	2	0%
WEB-MISC whisker splice attack	1	0%
WEB-IIS showcode access	1	0%
WEB-CGI phf access	1	0%
WEB-CGI glimpse access	1	0%
WEB-CGI calendar access	1	0%
Virus – Possible MyRomeo Worm	1	0%
TELNET access	1	0%
SCAN XMAS	1	0%
RFB - Possible WinVNC - 010708-1	1	0%
MISC Source Port 20 to <1024	1	0%
INFO Outbound GNUTella Connect request	1	0%
INFO napster new user login	1	0%
INFO Inbound GNUTella Connect request	1	0%
ICMP Destination Unreachable (Communication with Destination Network is Administratively Prohibited)	1	0%
DDOS shaft client to handler	1	0%
Total Alerts	**818437**	**100%**

****

Code Red / Nimda / Unicode Attack

66% or 545495 of the total alerts were related to the Code Red, Nimda and IIS 4/5 Unicode attacks against hosts within the Snort sensors scope. This represents an enormous level of traffic and should be top priority for the security and network administrators. These worms affect Microsoft NT/2000 Servers, IIS 4/5, Solaris, and Cisco Devices. Due to the sheer number of attacks, they can saturate networks and cause service degradation and outages. It is recommended these worms/attacks be blocked as

far up the network as possible such as the edge router or firewall. Most Network device vendors have provided workarounds to filter these worms.

The Top 10 source addresses detected propagating the Code Red, Nimda worm and IIS Unicode attacks are all similar in each top 10 list. These hosts are heavily infected and should be blocked entirely from this network. It should be noted that filtering is already in place as can been seen on the SANS University Graph showing no activity on Sept 19, 2001.

Alert	Total Count
Code Red Worm	126277
Nimda Worm	323195
Unicode	96023

Top 10 Alerts - Code Red Worm

Source	Total Count
211.90.176.59	7398
195.46.229.103	1978
130.39.100.139	1740
211.90.188.34	1616
211.90.88.43	1559
217.57.15.133	1530
211.96.99.59	1391
130.89.2.124	1336
196.28.50.220	1311
130.212.56.145	1295

Top 10 Alerts – Nimda Worm

Source	Total Count
211.90.176.59	8453
195.46.229.103	2377
130.39.100.139	2123
211.90.223.220	2059
211.90.188.34	1920
217.57.15.133	1795
211.90.88.43	1761
196.28.50.220	1742
130.212.56.145	1714
196.3.78.42	1679

Top 10 Alert – IIS Unicode

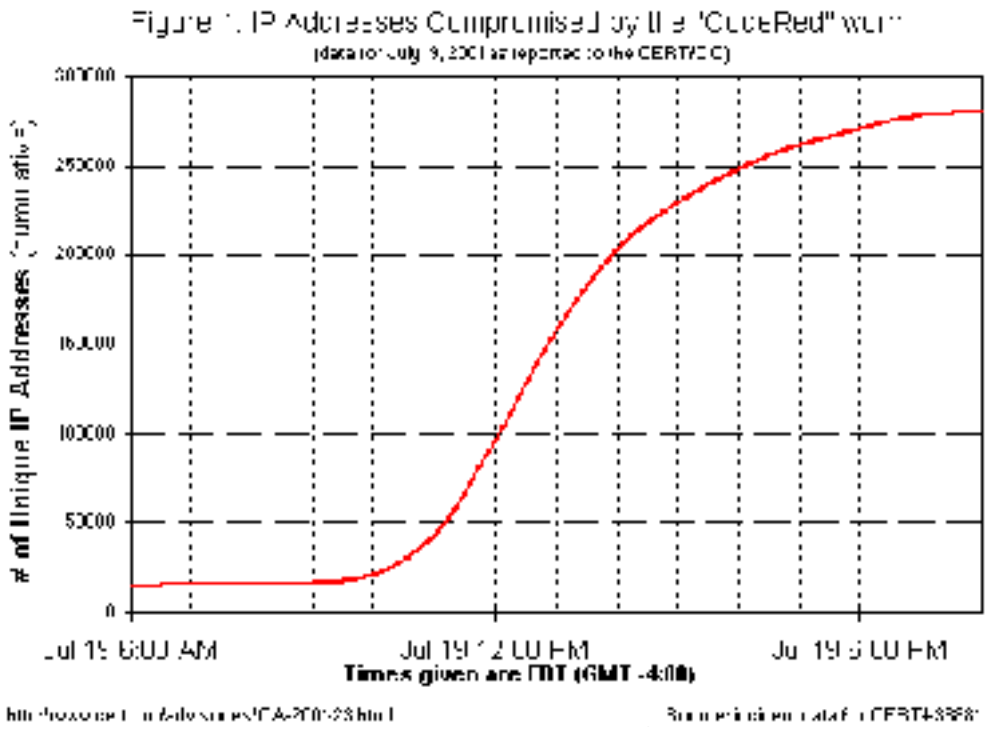
Source	Total Count
211.90.223.220	674
130.102.30.38	503
130.225.55.42	403
130.225.54.26	378
130.102.184.1	364
130.95.132.2	336
211.96.96.228	317
130.235.87.127	317
195.6.172.175	314
211.152.185.32	313

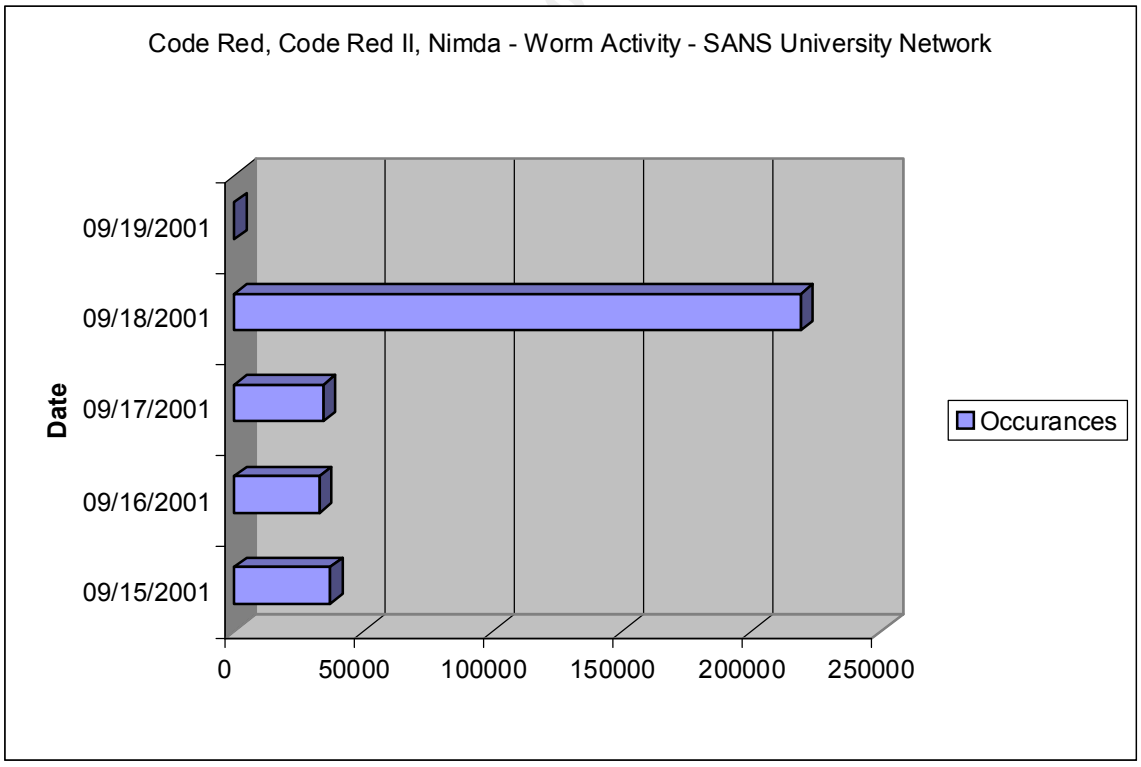
*** Please see the extended Code Red/Nimda/Unicode information at the bottom of this document to identify, patch and implement remedial actions ***

Observations

Code Red / Nimda:

The most significant alert is related to the size increase of log data starting on September 18, 2001. The log files show the number one signature to be "WEB-MISC Attempt to execute "cmd.exe". Although, this signature originally points to the Code Red Worm, it was discovered on September 18, 2001 to be a new and improved variant of the Code Red worms. This new strain has been given the designation Nimda and has proven to be more destructive than Code Red. Security sites including www.cert.org, www.sans.org, and www.security-focus.com reported significant increases in network bandwidth utilization and attacks to their systems. These attacks all point to the new worm Nimda. Nimda's ability to infiltrate targeted systems and replicate itself at record speeds has caused massive service degradation and outages. Nimda not only effects targeted systems but also has collateral effects on devices such as routers, firewalls and systems not typically affected by the Code Red variants. Below are descriptions of each of the Code Red, Code Red II and Nimda Worms taken from www.cert.org including a graph showing the original Code Red propagation throughout the Internet.





Nimda Worm Infection Types:

- Client to client via email
- Client to client via open network shares
- Web server to client via browsing of compromised web sites
- Client to web server via active scanning for and exploitation of various Microsoft IIS 4.0 / 5.0 directory traversal vulnerabilities (VU#111677 and CA-2001-12)
- Client to web server via scanning for the back doors left behind by the "Code Red II" (IN-2001-09), and "sadmind/IIS" (CA-2001-11) worms

Advisories

- CERT® Advisory CA-2001-26 Nimda Worm - http://www.cert.org/advisories/CA-2001-26.html
- CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL -
- CERT® Advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL - http://www.cert.org/advisories/CA-2001-13.html
- Cisco Security Advisory: "Code Red" Worm - Customer Impact - [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml
- CERT® Advisory CA-2001-11 sadmind/IIS Worm - http://www.cert.org/advisories/CA-2001-11.html

Infection Discovery & Code Red Symptoms

The Code Red and Nimda worms directly affect Microsoft Window but also have effects on Cisco devices. The steps below will help to find if your Windows Systems have been infected or your Cisco Routers are affected.

Windows

- A root.exe file (indicates a compromise by Code Red II or sadmind/IIS worms making the system vulnerable to the Nimda worm)
- An Admin.dll file in the root directory of c:\, d:\, or e:\ (Note that the file name Admin.dll may be legitimately installed by IIS in other directories.)
- Unexpected .eml or .nws files in numerous directories
- The presence of this string: /c+tftp%20-i%20x.x.x.x%20GET%20Admin.dll%20d:\Admin.dll 200 in the IIS logs, where "x.x.x.x" is the IP address of the attacking system. (Note that only the "200" result code indicates success of this command.)

See:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp for more information.

Cisco

- Large number of flows in NAT/PAT tables (if running NAT/PAT).
- Large number of ARPs/ARP storms in the network (caused by the IP address scan).
- Excessive memory use by IP Input, ARP Input, IP Cache Ager and CEF processes.
- High CPU utilization in ARP, IP Input, CEF and IPC.
- If running NAT, high CPU utilization at interrupt level at low traffic rates, or high CPU utilization at process level in IP Input.

See: http://www.cisco.com/warp/public/63/ts_codred_worm.shtml for additional information.

*Source: **www.cert.org**

Defence
Multiple defenses exist to mitigate the effects of the Code Red, Code Red II and Nimda worms as outlined in the cert advisories. Below is a summary taken from www.cert.org, www.microsoft.com, www.cisco.com, www.checkpoint.com.

- Install Virus Protection, update to the latest "Pattern File" and scan your entire computer including all hard disks, floppies.
- Apply vendor patches:http://www.microsoft.com/technet/security/bulletin/MS01-044.asp (This patch is a cumulative patch for the current Nimda worm and previous Code Red worms)
- How to Protect Your Network Against the Nimda Virus - http://www.cisco.com/warp/public/63/nimda.shtml

- Ingress filtering manages to prohibit externally initiated inbound connections to non-authorized services. With Nimda, ingress filtering of port 80/tcp could prevent instances of the worm outside of your network from scanning or infecting vulnerable IIS servers in the local network that are not explicitly authorized to provide public web services. Filtering of port 69/udp will also prevent the downloading of the worm to IIS via tftp.
- Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for machines providing public services to initiate outbound connections to the Internet. In the case of Nimda, employing egress filtering on port 69/udp at your network border will prevent certain aspects of the worm's propagation both to and from your network.
- Add rules on your Simple Mail Transfer Protocol (SMTP) server to block any email that has the following attachments:
    - readme.exe
    - Admin.dll

- If you want to use IE, disable Javascript, or get IE patched to SP II. If you want to use Netscape, no action is required.
- Use Cisco Network-based application recognition (NBAR) to filter readme.eml files from being downloaded. Here's an example for configuring NBAR.
- Use Checkpoint Firewall-1's HTTP Security Server to block:
    - readme.exe
    - cmd.exe

Recovery

- Steps for Recovering from a UNIX or NT System Compromise
- http://www.cert.org/tech_tips/win-UNIX-system_compromise.html
- Microsoft Security Bulletin MS01-044 - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp
- Microsoft Security Bulletin (MS01-020) - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

Top 10 Scans

Source Address	Total Count
MY.NET.206.114	248462
MY.NET.160.114	167685
MY.NET.222.158	69538
MY.NET.220.94	33548
MY.NET.235.234	24280
MY.NET.219.162	24277
MY.NET.234.154	24066
205.188.244.121	22142
205.188.233.153	20954
205.188.244.57	20923

Top 10 Scans (Destination)

Source	Total Count
MY.NET.160.114	45172
MY.NET.206.114	21228
MY.NET.235.234	6222
MY.NET.222.158	5524
205.188.244.57	5031

MY.NET.220.94	4774
205.188.233.153	4624
MY.NET.234.154	4360
205.188.233.185	4331
205.188.244.121	4217

****

MISC Large UDP Packet – 47282 Alerts

Top 10 Source addresses

13083 61.134.9.88:0
4600 61.150.5.19:0
3732 61.153.17.38:0
3714 61.153.17.244:0
2510 209.190.237.123:0
2098 61.153.19.95:0
997 61.150.5.18:0
771 63.250.214.68:0
721 61.153.17.243:0

Supporting data

5492 61.134.9.88:0->MY.NET.153.193:0
3728 61.153.17.38:0->MY.NET.111.221:0
3178 61.150.5.19:0->MY.NET.111.142:0
2662 61.134.9.88:0->MY.NET.153.149:0
2509 209.190.237.123:0->MY.NET.70.134:0
2374 61.134.9.88:0->MY.NET.153.185:0
1831 61.153.19.95:0->MY.NET.111.142:0
1422 61.153.17.244:0->MY.NET.111.221:0
1353 61.153.17.244:0->MY.NET.144.51:0
1115 61.134.9.88:0->MY.NET.112.244:0

inetnum	61.134.3.0 - 61.134.20.95
netname	SNXIAN
descr	XI'AN DATA BUREAU
country	CN
admin-c	WWN1-AP, inverse
tech-c	WWN1-AP, inverse
mnt-by	MAINT-CHINANET-SHAANXI, inverse

mnt-lower	MAINT-CN-SNXIAN, inverse
changed	ipadm@public.xa.sn.cn 20010427
source	APNIC

inetnum	61.150.0.0 - 61.150.31.255
netname	SNXIAN
descr	xi'an data branch,XIAN CITY SHAANXI PROVINCE
country	CN
admin-c	WWN1-AP, inverse
tech-c	WWN1-AP, inverse
mnt-by	MAINT-CHINANET-SHAANXI, inverse
mnt-lower	MAINT-CN-SNXIAN, inverse
changed	ipadm@public.xa.sn.cn 20010309
source	APNIC

The top talkers for this alert are from Net blocks originating in China. These packets are crafted as can be seen by the source and destination ports all being 0. The payload of these packets should be captured to better understand what is happening and these NetBlocks should be put on a Watchlist.

****

ICMP Echo Request speedera – 158656 Alerts

Top 10 Source addresses

MY.NET.205.234

Top 10 Destination addresses

64.219.131.70
66.33.117.144
172.132.106.38
172.143.129.222
24.186.127.170

This detect seems to be a false positive since the speedera icmp packets should be inbound to MY.NET. A close analysis of the host MY.NET.205.234 will reveal what types of ICMP packets are generating this signature. There is a gateway router (MY.NET.14.1) upstream from this device that is administratively prohibiting the ICMP echo packets from leaving the network so the destination addresses are likely not seeing these packets.

****

INFO MSN IM Chat data

Top 10 Source addresses

27 64.4.12.x:1863
29 MY.NET.98.144:1034
27 MY.NET.97.87:1755
27 64.4.12.x:1863
25 MY.NET.98.110:1037
24 MY.NET.98.115:2465
24 MY.NET.53.53:4051
24 MY.NET.53.128:3928
20 MY.NET.97.188:1129
19 MY.NET.98.232:1419

This traffic is from the internal network to multiple Microsoft Instant Messenger Servers. This traffic is normal if this type of external communication is permitted by your Security policy.

****

ICMP Destination Unreachable (Communication Administratively Prohibited)

Top 10 Source addresses

5875 MY.NET.14.1
77 216.158.21.226
76 192.80.53.46
70 216.158.21.42
38 131.118.255.18
30 128.192.166.2
28 192.5.89.62
28 152.61.1.10
15 141.161.184.45
12 MY.NET.14.2

Supporting data

2199 MY.NET.14.1->MY.NET.205.234
669 MY.NET.14.1->MY.NET.226.18
440 MY.NET.14.1->MY.NET.60.38
286 MY.NET.14.1->MY.NET.204.34
151 MY.NET.14.1->MY.NET.5.84
146 MY.NET.14.1->MY.NET.110.90
134 MY.NET.14.1->MY.NET.5.74
133 MY.NET.14.1->MY.NET.5.79
122 MY.NET.14.1->MY.NET.110.88
109 MY.NET.14.1->MY.NET.115.155

This is informational data usually from a router that is blocking outbound packets. These are normal messages but in the case of MY.NET.14.1 there are excessive hits and should be investigated. It is likely due to MY.NET.205.234 and the false speedera ICMP echo packets.

****

ICMP Echo Request Nmap or HPING2

Top 10 Source addresses

5141	MY.NET.226.18
292	MY.NET.212.230
66	MY.NET.215.146
46	MY.NET.212.214
28	MY.NET.88.152
26	MY.NET.203.134
25	MY.NET.98.188
25	MY.NET.153.200
23	MY.NET.181.82
19	MY.NET.152.216

Supporting data

1759	MY.NET.226.18->204.152.190.70
1729	MY.NET.226.18->204.71.200.75
1653	MY.NET.226.18->206.79.171.51
72	MY.NET.212.230->213.107.144.202
65	MY.NET.215.146->207.172.7.75
41	MY.NET.212.230->203.111.42.122
35	MY.NET.212.230->217.0.225.62
33	MY.NET.212.230->217.128.90.106
17	MY.NET.98.188->216.52.220.17
17	MY.NET.225.214->208.140.83.133

These alerts are all from internal hosts, possibly student residences, and could be using Nmap or HPING2 to probe systems, craft packets and attack systems inside and outside the University network. These tools should not be permitted due to the legal liabilities associated with them.

****

INFO Napster Client Data

Top 10 source addresses

794	MY.NET.223.126
547	24.5.78.96
342	62.250.14.6
133	151.189.12.24
66	MY.NET.97.196
54	24.154.71.222
51	MY.NET.235.202
41	MY.NET.201.246
40	MY.NET.98.125
34	MY.NET.234.118

Top 10 destination addresses

794	24.5.78.96
547	MY.NET.223.126
342	MY.NET.226.158
133	MY.NET.225.114
81	212.15.166.37
54	MY.NET.235.202
51	24.154.71.222
35	4.41.44.152
23	212.187.54.150
16	24.4.49.57
14	212.187.52.184
8	MY.NET.235.154

Supporting data

794	MY.NET.223.126:3233->24.5.78.96:6699
547	24.5.78.96:6699->MY.NET.223.126:3233
208	62.250.14.6:7777->MY.NET.226.158:62286
134	62.250.14.6:7777->MY.NET.226.158:33880
133	151.189.12.24:6666->MY.NET.225.114:3083
54	24.154.71.222:6666->MY.NET.235.202:3381
51	MY.NET.235.202:3381->24.154.71.222:6666
13	MY.NET.97.196:4859->212.15.166.37:7777
11	MY.NET.97.196:1162->212.15.166.37:7777
10	MY.NET.98.125:1581->4.41.44.152:7777

There is strong evidence of Napster use in the University network as the supporting data show connections to well known Napster ports. Napster is a peer-to-peer application used to exchange MP3 music. The risk factor for vulnerabilities in the Napster client is currently low-to-medium because there have been no known vulnerabilities. Napster does however give away IP address information of the host computer thus allowing attackers to target the host computer. Due to the size and number of MP3 files typically exchanged, Napster can also be a burden on your network. This issue should be addressed in the Universities security policy.

****

Watchlist 000220 IL-ISDNNET-990517

Top 10 Source addresses

1238	212.179.18.3
429	212.179.127.36
180	212.179.34.114
66	212.179.2.179
48	212.179.27.6
31	212.179.84.177
25	212.179.85.94
24	212.179.83.75
21	212.179.88.173
21	212.179.15.203

Top 10 Destination addresses

1238	MY.NET.209.242
424	MY.NET.210.34
176	MY.NET.213.2
66	MY.NET.204.74
46	MY.NET.226.46
31	MY.NET.70.101
28	MY.NET.205.94
27	MY.NET.220.166
24	MY.NET.214.222
21	MY.NET.233.54

Top 10 Ports

1238	MY.NET.209.242:1214
176	MY.NET.213.2:1214
77	MY.NET.210.34:3914
74	MY.NET.210.34:3950
72	MY.NET.210.34:3975
67	MY.NET.210.34:3876
66	MY.NET.204.74:2377
31	MY.NET.70.101:1214
27	MY.NET.220.166:1214
26	MY.NET.210.34:3744

Supporting data

516	212.179.18.3:62612->MY.NET.209.242:1214
316	212.179.18.3:62757->MY.NET.209.242:1214
179	212.179.18.3:63042->MY.NET.209.242:1214
165	212.179.18.3:62599->MY.NET.209.242:1214
160	212.179.34.114:22573->MY.NET.213.2:1214
77	212.179.127.36:1214->MY.NET.210.34:3914
74	212.179.127.36:1214->MY.NET.210.34:3950
72	212.179.127.36:1214->MY.NET.210.34:3975
67	212.179.127.36:1214->MY.NET.210.34:3876
66	212.179.2.179:6346->MY.NET.204.74:2377

There seems to be a lot of KAZAA file sharing from this network. The number of connections to specific hosts within the University network is proof that there is high activity. As with any of the file sharing applications, they pose a security risk and use high amounts of bandwidth. This issue should be addressed in the Universities security policy. The connections to ports 39xx should be captured in more detail but they are likely KAZAA clients re-configured to use these ports.

****

TFTP - Internal TCP connection to external tftp server

Top 10 Source addresses

791	204.191.124.229
221	MY.NET.215.198
197	MY.NET.215.146
147	MY.NET.204.114
135	MY.NET.212.222
70	64.12.25.191
60	64.12.29.4
46	MY.NET.212.118
42	MY.NET.215.150
37	64.12.28.246

Destination

791	MY.NET.215.146
197	204.191.124.229
159	64.12.25.191
137	64.12.29.4
83	MY.NET.215.198
74	64.12.28.246
73	64.12.27.225
71	64.12.28.245

59 64.12.27.227
56 MY.NET.204.114

Supporting data

2 MY.NET.157.8:4294->130.251.187.24:69
2 MY.NET.157.175:4924->130.205.102.188:69
2 MY.NET.157.175:3969->130.14.60.141:69
2 MY.NET.157.175:3481->130.126.43.50:69
2 MY.NET.157.175:1559->130.94.21.205:69
2 MY.NET.157.175:1244->130.235.82.230:69
2 MY.NET.136.2:1232->130.220.225.40:69
1 MY.NET.157.8:4999->130.205.122.243:69
1 MY.NET.157.8:4996->130.205.122.243:69
1 MY.NET.157.8:4762->130.127.9.44:69

These alerts are of concern. MY.NET addresses are using Trivial File Transport Protocol to send and receive data to and from addresses such as America Online, 229. corp.ottawa.psi.ca and others. Although this **may** be legitimate traffic, it is done in a clear (non-encrypted) method and with no authentication. Special attention should be given to these transfers. *Note, this applies to the UDP versions of this alert as well.
****

Possible Trojan server activity

Top 10 Source addresses

871 MY.NET.97.185
58 63.166.32.92
44 MY.NET.97.216
33 MY.NET.98.116
28 MY.NET.225.166
23 24.70.134.71
17 MY.NET.70.11
9 MY.NET.204.58
2 MY.NET.85.94
2 MY.NET.60.14

Top 10 Destination addresses

58 MY.NET.225.166:1214
28 63.166.32.92:27374
17 63.136.177.142:27374
9 63.226.24.207:27374

3 172.151.67.179:27374
3 172.142.69.2:27374
2 64.114.69.17:27374
2 61.128.109.228:27374
2 24.4.252.3:27374
2 216.145.66.226:27374

Supporting data

58 63.166.32.92:27374->MY.NET.225.166:1214
28 MY.NET.225.166:1214->63.166.32.92:27374
17 MY.NET.70.11:1214->63.136.177.142:27374
9 MY.NET.204.58:1214->63.226.24.207:27374
3 MY.NET.97.185:3275->172.142.69.2:27374
3 MY.NET.97.185:1093->172.151.67.179:27374
2 MY.NET.97.216:3192->207.195.210.149:27374
2 MY.NET.97.216:3165->207.195.210.121:27374
2 MY.NET.97.216:3149->207.195.210.104:27374
2 MY.NET.97.216:3083->207.195.210.36:27374

Port 1214 is a used by KAZAA servers to share media files such as music, video and images. The above are likely connections to those servers. Port 27374 is used by numerous Trojans such as Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader. Since some of the scans are originating from the internal network these hosts may be compromised and should be analysed for Trojans.

****

INFO Inbound GNUTella Connect accept

182 MY.NET.203.34:6346
95 MY.NET.98.188:6346
65 MY.NET.219.146:6346
53 MY.NET.233.54:6346
47 MY.NET.212.222:6346
43 MY.NET.229.10:6346
29 MY.NET.219.238:6346
21 MY.NET.211.46:6346
20 MY.NET.201.186:6346
19 MY.NET.98.213:6346

GNUTella is another application to share files on the Internet. Since GNUTella can connect on ports that are typically allowed through most packet filters and associated firewalls such as port 80 http, this makes GNUTella hard to stop and detect. This issue should be addressed in the Universities security policy.

****

TCP SRC and DST outside network

Top 10 Source addresses

98 169.254.101.152:80
39 172.148.203.171:80
29 172.170.247.173:80
26 172.143.24.219:6346
21 172.164.91.66:80
17 172.132.0.61:80
16 172.166.99.76:80
16 172.151.109.151:80
15 172.164.89.241:80
15 172.159.34.160:80

Top 10 Destination addresses

8 3.0.0.0:135
6 65.80.249.76:1214
6 206.45.180.130:1214
5 128.226.161.165:1214
4 150.135.185.221:1214
4 128.226.143.125:1214
3 65.80.49.133:1214
3 64.12.104.243:11523
3 38.213.22.2:1114
3 192.168.0.183:1209

Supporting data

2 169.254.101.152:80->213.25.51.4:36814
2 169.254.101.152:80->204.248.169.148:4258
2 169.254.101.152:80->200.52.84.131:5826
2 169.254.101.152:4292->205.188.48.154:5190
1 169.254.101.152:80->66.99.90.5:51623
1 169.254.101.152:80->66.136.75.131:61599
1 169.254.101.152:80->65.81.32.139:1337
1 169.254.101.152:80->65.45.74.10:2750
1 169.254.101.152:80->65.200.91.239:45327
1 169.254.101.152:80->64.64.94.194:11755

This alert may be a result of the Snort Sensor picking up traffic from networks outside the configured range. Most of the traffic looks like normal return trip HTTP requests. Possibly Snort is listening on a spanning port configured to multiple VLAN's.

****

Incomplete Packet Fragments Discarded

Top 10 Source addresses

174	61.159.225.33:0
161	210.76.63.49:0
126	63.210.47.88:0
84	64.232.206.141:0
82	63.210.47.80:0
58	63.210.47.81:0
38	63.210.47.89:0
33	64.232.139.174:0
29	211.117.63.154:0
28	64.12.33.11:0

Top 10 Destination addresses

220	MY.NET.211.238:0
174	MY.NET.111.146:0
117	MY.NET.110.8:0
88	MY.NET.209.194:0
84	MY.NET.223.166:0
72	MY.NET.213.218:0
44	MY.NET.162.194:0
29	MY.NET.211.78:0
28	MY.NET.201.218:0
17	MY.NET.153.151:0

This traffic is suspicious and should be analyzed in more detail. Payload data should be captured and analyzed. Source and destination port are both 0, which indicates crafted packets.

This could be MSN online gaming data that never made it back to the network?

Supporting data

http://www.incidents.org/detect/gaming.php

****

BACKDOOR NetMetro Incoming Traffic

Top 10 Source addresses

359	217.80.5.244:5031
134	217.229.89.40:5031

115 217.224.152.178:5031
100 217.82.137.46:5031
70 217.85.206.145:5031
68 217.82.197.128:5031
68 217.230.116.239:5031
13 217.82.204.134:5031
1 195.249.246.249:5031

Top 10 Destination addresses

927 MY.NET.104.104:20
1 MY.NET.150.204:1214

Supporting data

359 217.80.5.244:5031->MY.NET.104.104:20
134 217.229.89.40:5031->MY.NET.104.104:20
115 217.224.152.178:5031->MY.NET.104.104:20
100 217.82.137.46:5031->MY.NET.104.104:20
70 217.85.206.145:5031->MY.NET.104.104:20
68 217.82.197.128:5031->MY.NET.104.104:20
68 217.230.116.239:5031->MY.NET.104.104:20
13 217.82.204.134:5031->MY.NET.104.104:20
1 195.249.246.249:5031->MY.NET.150.204:1214

Supporting data – Snort Signature

alert tcp $EXTERNAL_NET 5031 -> $HOME_NET !53:80 (msg:"BACKDOOR NetMetro Incoming Traffic"; flags: A+; reference:arachnids,79; sid:160; rev:1;)

This alert looks like a false positive. The above Snort signature is a sample of Snorts newest signature for NetMetro new but the University may have been using an older signature looking for Source port 5031 and no specific destination port. The host MY.NET.104.104 is however highly suspected as being compromised and this alert may in fact be real. As previously mentioned, this host needs to be forensically analyzed.
****

EXPLOIT x86 NOOP

Top 10 Source addresses

244 129.128.5.191:20
15 216.136.171.202:2401
10 4.40.27.248:2068
9 24.20.206.187:1501

6	129.89.126.128:2062
4	152.3.142.12:27182
4	152.3.142.12:20
2	65.35.136.147:20
2	64.229.24.127:1800
2	24.31.221.159:3772
2	24.201.36.117:6699
2	216.52.220.11:20
2	216.164.24.178:17264

Top 10 Destination addresses

244	MY.NET.70.148
29	MY.NET.234.50
15	MY.NET.237.66
5	MY.NET.209.218
4	MY.NET.201.162
4	MY.NET.111.48
3	MY.NET.226.138
3	MY.NET.223.54
2	MY.NET.230.90
2	MY.NET.227.242
2	MY.NET.219.214

Supporting data -1

51	129.128.5.191:20->MY.NET.70.148:1638
45	129.128.5.191:20->MY.NET.70.148:1502
39	129.128.5.191:20->MY.NET.70.148:1639
39	129.128.5.191:20->MY.NET.70.148:1503
33	129.128.5.191:20->MY.NET.70.148:1763
28	129.128.5.191:20->MY.NET.70.148:1764
15	216.136.171.202:2401->MY.NET.237.66:40480
10	4.40.27.248:2068->MY.NET.234.50:412
9	24.20.206.187:1501->MY.NET.234.50:412
6	129.89.126.128:2062->MY.NET.234.50:412

Supporting data - 2

Snort Signature found in SANS Practical assignment from David Oborn.

http://www.sans.org/y2k/practical/David_Oborn_GCIA.html#detect4

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"EXPLOIT x86 NOOP"; content: "|90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90|"; flags: A+; reference:arachnids,181;)

alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"EXPLOIT x86 NOOP"; content:"|9090 9090 9090 9090 9090 9090 9090 9090|"; reference:arachnids,181;)

The Snort signature that generates these alerts looks inside payload contents and attempts to match specific strings. If these are in fact x86 hosts running a Unix variant, this alert may be a legitimate exploit to the MY.NET addresses and these hosts should be examined for suspicious activity. Further analysis should be done with payload captures.
****

Watchlist 000222 NET-NCFC

Top 10 Source addresses

92	159.226.41.166:23
9	159.226.228.1:1243
5	159.226.138.231:3137
2	159.226.8.113:1816
2	159.226.47.68:2965
2	159.226.45.29:1216
2	159.226.160.110:2444

Top 10 Destination addresses

47	MY.NET.163.100:1569
45	MY.NET.163.100:2564
17	MY.NET.253.114:80
10	MY.NET.253.42:25
6	MY.NET.254.0:80
5	MY.NET.99.39:6346
3	MY.NET.242.220:80
3	MY.NET.219.170:80
3	MY.NET.216.192:80
3	MY.NET.202.216:80

Supporting data

47	159.226.41.166:23->MY.NET.163.100:1569
45	159.226.41.166:23->MY.NET.163.100:2564
9	159.226.228.1:1243->MY.NET.253.42:25
5	159.226.138.231:3137->MY.NET.99.39:6346
2	159.226.8.113:1816->MY.NET.253.114:80
2	159.226.47.68:2965->MY.NET.203.242:80
2	159.226.45.29:1216->MY.NET.253.114:80
2	159.226.160.110:2444->MY.NET.215.185:80

Since this network is already under suspicion, more detailed packet capture should be performed to better understand what this data means. There are multiple Trojans that run or port 80 and GNUTella runs on 6346. This traffic is suspicious and these systems should be inspected.

****

x86 NOOP - unicode BUFFER OVERFLOW ATTACK

Top 10 Source addresses

21	24.94.14.213
9	4.40.27.248
3	24.181.80.101
3	172.146.122.183
2	129.89.126.128
1	64.225.153.49
1	64.224.109.6
1	24.20.206.187

Top 10 Destination addresses

33	MY.NET.234.50
3	MY.NET.53.40
3	MY.NET.222.158
2	MY.NET.130.86

Supporting data

21	24.94.14.213:4540->MY.NET.234.50:412
9	4.40.27.248:2068->MY.NET.234.50:412
3	24.181.80.101:6347->MY.NET.53.40:3068
3	172.146.122.183:1575->MY.NET.222.158:2346
2	129.89.126.128:2062->MY.NET.234.50:412
1	64.225.153.49:3023->MY.NET.130.86:1021
1	64.224.109.6:3137->MY.NET.130.86:1021
1	24.20.206.187:1501->MY.NET.234.50:412

The Snort signature that generates these alerts looks for payload content matching specific strings. It is similar to the Exploit x86 NOOP above. If these hosts are running Unicode susceptible to this attack they should be checked for compromise.

****

EXPLOIT x86 setuid 0

Top 10 Source addresses

2 128.205.220.17
1 66.71.4.146
1 66.66.30.232
1 65.67.28.25
1 65.198.105.229
1 64.231.110.64
1 63.198.235.150
1 4.42.51.15
1 24.45.193.16
1 24.248.130.45

Top 10 Destination addresses

4 MY.NET.217.98
2 MY.NET.203.230
1 MY.NET.70.72
1 MY.NET.53.197
1 MY.NET.238.42
1 MY.NET.235.102
1 MY.NET.233.234
1 MY.NET.230.90
1 MY.NET.227.106
1 MY.NET.225.158

Supporting data

1 152.17.121.130:1214->MY.NET.53.197:1128
1 128.61.67.192:1214->MY.NET.203.146:1386
1 128.253.108.26:4922->MY.NET.150.220:1234
1 128.205.32.51:20->MY.NET.209.218:1180
1 128.205.220.17:2031->MY.NET.217.98:14272
1 128.205.220.17:1925->MY.NET.217.98:61422
1 128.194.38.143:1509->MY.NET.208.98:1214

Again, this alert is similar to the x86 NOOP alerts above. The Snort signature alerts on specific payload strings looking for an attempted exploit of Unix running on X86 architecture. These signatures are known to set off false positives. If the destination addresses are running an x86 Unix flavor then they should be analyzed.
****

RPC tcp traffic contains bin_sh

Top 10 Source addresses

15 128.95.248.213
8 202.58.118.12

2 128.205.32.51
1 205.188.212.66
1 152.2.210.121

Top 10 Destination addresses

15 MY.NET.217.230
9 MY.NET.201.70
2 MY.NET.218.22
1 MY.NET.140.143

Supporting data

[**] 128.95.248.213:2201 -> MY.NET.217.230:49269
alert.010915:09/15-02:30:52.749850 [**] RPC tcp traffic contains bin_sh
[**] 128.95.248.213:2201 -> MY.NET.217.230:49269
alert.010915:09/15-02:35:00.636474 [**] EXPLOIT x86 NOOP [**]
128.95.248.213:2201 -> MY.NET.217.230:49269
alert.010915:09/15-02:37:36.708778 [**] RPC tcp traffic contains bin_sh
[**] 128.95.248.213:2201 -> MY.NET.217.230:49269

alert.010915:09/15-18:18:25.720682 [**] RPC tcp traffic contains bin_sh
[**] 128.205.32.51:29940 -> MY.NET.218.22:32887
alert.010915:09/15-18:18:25.748594 [**] RPC tcp traffic contains bin_sh
[**] 128.205.32.51:29940 -> MY.NET.218.22:32887
alert.010918:09/18-09:33:02.566771 [**] EXPLOIT x86 setuid 0 [**]
128.205.32.51:20 -> MY.NET.209.218:1180
alert.010918:09/18-09:41:06.984754 [**] EXPLOIT x86 NOOP [**]
128.205.32.51:20 -> MY.NET.209.218:1178

If the destination hosts MY.NET.217.230, MY.NET.218.22 run Unix then they should be checked for rootkits since there is an another signature indicating an attempted exploit from the same source address. A hacker may have compromised these systems and is executing shell commands.

The other 2 Destination Hosts MY.NET.201.70 and MY.NET.140.143 have no other exploit or attack against them by any of the source addresses so this **may** be legitimate traffic. It is worth noting that there are multiple RPC vulnerabilities and allowing RPC traffic outside the network and executing shell commands in unencrypted view is not recommended.
****

FTP CWD / - possible warez site

Top 10 Source addresses

58 217.0.238.93
13 217.80.101.153
5 217.84.27.185
5 217.229.92.146
5 217.0.93.236
4 194.122.136.7
3 62.158.171.147
3 217.80.159.71
3 217.229.166.127
2 62.158.26.16

Top 10 Destination addresses

213 MY.NET.104.104

Supporting data

3 217.80.159.71:3131->MY.NET.104.104:21
3 217.0.93.236:4099->MY.NET.104.104:21
2 62.155.235.122:3430->MY.NET.104.104:21
2 217.80.226.159:2444->MY.NET.104.104:21
2 217.80.101.153:18414->MY.NET.104.104:21
2 217.228.166.192:1057->MY.NET.104.104:21
2 217.225.253.53:3823->MY.NET.104.104:21
2 217.0.93.236:2661->MY.NET.104.104:21
1 62.2.78.110:2845->MY.NET.104.104:21
1 62.227.42.176:1124->MY.NET.104.104:21

This alert points to a compromise of the address MY.NET.104.104. Evidence suggests this host is infected by the Trojan, Subseven. See the section on questionable services for additional information. Connections are being made to the ftp port from multiple outside addresses supporting evidence that this host is compromised.
****

Back Orifice

Top 10 Source addresses

8 203.155.234.23
3 203.146.129.28
2 203.155.224.16
1 203.170.138.248

Top 10 Destination addresses

1 MY.NET.98.9
1 MY.NET.98.74

1 MY.NET.98.61
1 MY.NET.98.25
1 MY.NET.98.214
1 MY.NET.98.210
1 MY.NET.98.197
1 MY.NET.98.191
1 MY.NET.98.18
1 MY.NET.98.166

Supporting data

1 203.170.138.248:31338->MY.NET.98.74:31337
1 203.155.234.23:31338->MY.NET.98.61:31337
1 203.155.234.23:31338->MY.NET.98.25:31337
1 203.155.234.23:31338->MY.NET.98.214:31337
1 203.155.234.23:31338->MY.NET.98.18:31337
1 203.155.234.23:31338->MY.NET.98.14:31337
1 203.155.234.23:31338->MY.NET.98.13:31337
1 203.155.234.23:31338->MY.NET.98.126:31337
1 203.155.234.23:31338->MY.NET.98.124:31337
1 203.155.224.16:31338->MY.NET.98.9:31337
1 203.155.224.16:31338->MY.NET.98.166:31337
1 203.146.129.28:31338->MY.NET.98.210:31337
1 203.146.129.28:31338->MY.NET.98.197:31337
1 203.146.129.28:31338->MY.NET.98.191:31337

Back Orifice is a Trojan application used to control Windows systems. In some cases it is also used as an administrative tool. It appears there are multiple systems within the University network that are under the control of Back orifice and each of the above should be analyzed. The use of Trojan applications as administrative tools such as Back orifice is not recommended and should be addressed in the Universities security policy.
****

X11 outgoing

Top 10 Source addresses

2 24.37.107.206
2 203.164.187.47
1 200.65.126.72
1 156.56.208.96
1 131.118.1.26

Top 10 Destination addresses

2 MY.NET.220.182

1 MY.NET.60.39
1 MY.NET.60.38
1 MY.NET.209.22
1 MY.NET.201.202
1 MY.NET.15.193

Supporting data

1 24.37.107.206:6000->MY.NET.60.39:3830
1 24.37.107.206:6000->MY.NET.60.38:2716
1 203.164.187.47:6000->MY.NET.220.182:4335
1 203.164.187.47:6000->MY.NET.220.182:2099
1 200.65.126.72:6000->MY.NET.209.22:2183
1 156.56.208.96:6000->MY.NET.201.202:2993
1 131.118.1.26:6000->MY.NET.15.193:1817

X11 is a protocol used to send Unix graphical windows and applications across networks. This kind of traffic is not encrypted and is risky. X11 is also bandwidth intensive. If used, X11 should go across encrypted channels. Note: This will require additional bandwidth and resource.

****

SNMP public access

Top 10 Source addresses

MY.NET.111.188:1743 -> MY.NET.50.154:161

Top 10 Destination addresses

63.117.242.223:3639 -> MY.NET.135.0:161

Questionable Services- Inside Threats

This section outlines the questionable applications running inside the University Network. These applications place a high security risk and should be removed.

- INFO MSN IM Chat data: **Microsoft Chat Network.**
- ICMP Echo Request Nmap or HPING2: **OS fingerprinting, reconnaissance, packet crafting.**
- INFO Napster Client Data: **Music sharing.**
- TFTP - Internal TCP connection to external tftp server: **File Transfer Protocol with no authentication or encryption.**
- INFO napster login: **Music sharing.**
- INFO Inbound GNUTella Connect accept: **Internet File Sharing.**
- BACKDOOR NetMetro Incoming Traffic: **Windows Trojan.**

- TFTP - Internal UDP connection to external tftp server: **FTP with no authentication or encryption.**
- BACKDOOR NetMetro File List: **Windows Trojan.**
- FTP CWD / - possible warez site: **Hackers FTP site for file storage.**
- INFO napster upload request: **Music sharing**
- X11 outgoing: **Unix Graphical interface – Clear text.**
- IDS50/trojan_trojan-active-subseven: **Windows Trojan**
- X11 xopen: Unix Graphical interface: **Unix Graphical interface - Clear text.**
- SNMP public access: **Simple Network Management Protocol, which can view and control devices such as routers and switches.**
- MISC PCAnywhere Startup: **Windows Control Software.**
- INFO Outbound GNUTella Connect request: **Internet File Sharing.**
- INFO napster new user login: **Music sharing.**
- INFO Inbound GNUTella Connect request: **Internet File Sharing.**

MY.NET.104.104

Out of Spec Data

```
09/17-05:06:23.242086 217.80.112.127:2265 -> MY.NET.104.104:0
TCP TTL:54 TOS:0x0 ID:33844
21**R*** Seq: 0x1402C2   Ack: 0x784AF332   Win: 0x5010
00 14 02 C2 78 4A F3 32 1D C4 50 10 7F FF 66 57  ....xJ.2..P...fW
00 00 00 00 00 00                                ......
```

```
09/17-05:10:51.928942 217.80.112.127:2264 -> MY.NET.104.104:20
TCP TTL:54 TOS:0x0 ID:14708
21S**P** Seq: 0x2C20000   Ack: 0x75EBF33D   Win: 0x5010
08 D8 00 14 02 C2 00 00 75 EB F3 3D 0F CA 50 10  ........u..=..P.
7F FF 76 A6 00 00 00 00 00 00                    ..v.......
```

The Out of Spec data above looks like OS fingerprinting. The Reserved bits are set which is used to see how the IP stack responds to unusual settings in the TCP packet. This will give clues as to which operating system the host runs.

**This system has been compromised and should be removed from the network as soon as possible. MY.NET.104.104 is likely under control by the SubSeven Trojan and it being used as a Warez site. It should be noted that valuable forensics information could be on this system.

Many hosts inside the University network are communicating inside and outside the network with the above applications and protocols. This poses a high security risk and

potential legal liabilities. See recommendations at the bottom of this document to stop this traffic.

The top 10 scans show that most port scanning is coming from the internal network. This network seems to have high numbers of computers port scanning inside and outside the network. The addresses outside of the University network all resolve to Spinner.com which is an MP3 / Music Web Site. It seems that Snort picks up spinner traffic as port scans. This is a false positive. It may be that the MY.NET addresses placed in the top 10 port scans have spinner clients and are also generating port scan alerts. In any case these systems need to be checked to verify this is the case. A policy decision then needs to be made if this application can remain on these systems.

Top 10 Alert source addresses (excluding port scan) with registration information.

15983 61.134.9.88

inetnum: 61.134.3.0 - 61.134.20.95
netname: SNXIAN
descr: XI'AN DATA BUREAU
country: CN
admin-c: WWN1-AP
tech-c: WWN1-AP
mnt-by: MAINT-CHINANET-SHAANXI
mnt-lower: MAINT-CN-SNXIAN
changed: ipadm@public.xa.sn.cn 20010427
source: APNIC

person: WANG WEI NA
address: Xi Xin street 90# XIAN
country: CN
phone: +8629-724-1554
fax-no: +8629-324-4305
e-mail: xaipadm@public.xa.sn.cn
nic-hdl: WWN1-AP
mnt-by: MAINT-CN-SNXIAN
changed: wwn@public.xa.sn.cn 20001127
source: APNIC

15852 211.90.176.59

inetnum: 211.90.0.0 - 211.91.255.255
netname: UNICOM
descr: China United Telecommunications Corporation
country: CN
admin-c: XL31-AP

tech-c: XL31-AP
mnt-by: MAINT-CNNIC-AP
changed: xiaqing@cnnic.net.cn 20000414
source: APNIC

person: XiaoMing Li
address: 6F Office Tower 3, Henderson Centre, Beijing China
country: CN
phone: +86-10-65181800-291
fax-no: +86-10-65181800-777
e-mail: lxmlxm@public3.bta.net.cn
nic-hdl: XL31-AP
mnt-by: MAINT-CNNIC-AP
changed: wangch@cnnic.net.cn 20000331
source: APNIC

5438 61.150.5.19

inetnum: 61.150.0.0 - 61.150.31.255
netname: SNXIAN
descr: xi'an data branch,XIAN CITY SHAANXI PROVINCE
country: CN
admin-c: WWN1-AP
tech-c: WWN1-AP
mnt-by: MAINT-CHINANET-SHAANXI
mnt-lower: MAINT-CN-SNXIAN
changed: ipadm@public.xa.sn.cn 20010309
source: APNIC

person: WANG WEI NA
address: Xi Xin street 90# XIAN
country: CN
phone: +8629-724-1554
fax-no: +8629-324-4305
e-mail: xaipadm@public.xa.sn.cn
nic-hdl: WWN1-AP
mnt-by: MAINT-CN-SNXIAN
changed: wwn@public.xa.sn.cn 20001127
source: APNIC

4751 61.153.17.38

inetnum: 61.153.17.0 - 61.153.17.255
netname: NINGBO-ZHILAN-NET
descr: NINGBO TELECOMMUNICATION CORPORATION ,ZHILAN APPLICATION SERVICE PROVIDER

descr: Ningbo, Zhejiang Province
country: CN
admin-c: CZ61-AP
tech-c: CZ61-AP
mnt-by: MAINT-CHINANET-ZJ
changed: master@dcb.hz.zj.cn 20010512
source: APNIC

person: CHINANET ZJMASTER
address: no 378,yan an road,hangzhou,zhejiang
country: CN
phone: +86-571-7015441
fax-no: +86-571-7027816
e-mail: master@dcb.hz.zj.cn
nic-hdl: CZ61-AP
mnt-by: MAINT-CHINANET-ZJ
changed: master@dcb.hz.zj.cn 20001219
source: APNIC

4595 61.153.17.244

inetnum: 61.153.17.0 - 61.153.17.255
netname: NINGBO-ZHILAN-NET
descr: NINGBO TELECOMMUNICATION CORPORATION ,ZHILAN APPLICATION SERVICE PROVIDER
descr: Ningbo, Zhejiang Province
country: CN
admin-c: CZ61-AP
tech-c: CZ61-AP
mnt-by: MAINT-CHINANET-ZJ
changed: master@dcb.hz.zj.cn 20010512
source: APNIC

person: CHINANET ZJMASTER
address: no 378,yan an road,hangzhou,zhejiang
country: CN
phone: +86-571-7015441
fax-no: +86-571-7027816
e-mail: master@dcb.hz.zj.cn
nic-hdl: CZ61-AP
mnt-by: MAINT-CHINANET-ZJ
changed: master@dcb.hz.zj.cn 20001219
source: APNIC

4355 195.46.229.103

inetnum: 195.46.229.96 - 195.46.229.111
netname: VILLE-ESCH-LU
descr: Commune Esch-sur-Alzette
country: LU
admin-c: FR697-RIPE
tech-c: PM1628-RIPE
status: ASSIGNED PA
mnt-by: RIPE-NCC-NONE-MNT
changed: coutel@pt.lu 19980709
source: RIPE

3863 130.39.100.139

Louisiana State University (NET-TIGERLAN)
200 Computing Services Center
Baton Rouge, LA 70803
US

Netname: TIGERLAN
Netblock: 130.39.0.0 - 130.39.255.255

Coordinator:
Robbins, Sean (SR935-ARIN) sean@LSU.EDU
(504) 388-5204 (FAX) (504) 388-6400

Domain System inverse mapping provided by:

BIGDOG.LSU.EDU	130.39.198.8
OTC-DNS1.LSU.EDU	130.39.3.5
OTC-DNS2.LSU.EDU	130.39.244.30

Record last updated on 25-Jan-2001.
Database last updated on 5-Oct-2001 23:18:41 EDT.

3536 211.90.188.34

inetnum: 211.90.0.0 - 211.91.255.255
netname: UNICOM
descr: China United Telecommunications Corporation
country: CN
admin-c: XL31-AP
tech-c: XL31-AP
mnt-by: MAINT-CNNIC-AP
changed: xiaqing@cnnic.net.cn 20000414
source: APNIC

person: XiaoMing Li
address: 6F Office Tower 3, Henderson Centre, Beijing China
country: CN
phone: +86-10-65181800-291
fax-no: +86-10-65181800-777
e-mail: lxmlxm@public3.bta.net.cn
nic-hdl: XL31-AP
mnt-by: MAINT-CNNIC-AP
changed: wangch@cnnic.net.cn 20000331
source: APNIC

3466 211.90.223.220

inetnum: 211.90.0.0 - 211.91.255.255
netname: UNICOM
descr: China United Telecommunications Corporation
country: CN
admin-c: XL31-AP
tech-c: XL31-AP
mnt-by: MAINT-CNNIC-AP
changed: xiaqing@cnnic.net.cn 20000414
source: APNIC

person: XiaoMing Li
address: 6F Office Tower 3, Henderson Centre, Beijing China
country: CN
phone: +86-10-65181800-291
fax-no: +86-10-65181800-777
e-mail: lxmlxm@public3.bta.net.cn
nic-hdl: XL31-AP
mnt-by: MAINT-CNNIC-AP
changed: wangch@cnnic.net.cn 20000331
source: APNIC

3325 217.57.15.133

inetnum: 217.57.15.128 - 217.57.15.143
netname: SCP-CALCOLATORI-SRL
descr: S.C.P. CALCOLATORI SRL
country: IT
admin-c: AF834-RIPE
tech-c: LF2977-RIPE
status: ASSIGNED PA
notify: network@cgi.interbusiness.it
mnt-by: INTERB-MNT
changed: network@cgi.interbusiness.it 20010321

source: RIPE

It is interesting to note that 7 of the top 10 addresses found in the alert files originate from China. There is a growing number if Chinese hackers attacking Western systems as reported by numerous news agencies. Security Analyst's are saying Chinese hackers are becoming organized and coordinating attacks against American sites. The above data confirms this is reality and special attention should be paid to the Chinese networks involved in these attacks.

http://www.washtech.com/news/regulation/9392-1.html

http://asia.cnn.com/2001/TECH/internet/04/16/china.hacking/

Out of Spec Data

OOS – Top 10 Source IP's

9	217.80.112.127
9	199.183.24.194
6	24.0.154.106
5	158.75.57.4
4	66.24.124.237
2	66.24.232.76
2	65.27.86.23
2	65.164.16.45
2	213.123.120.241
2	198.186.202.147

OOS – Top 10 Destination IP's

9	MY.NET.104.104
6	MY.NET.218.254
5	MY.NET.253.41
5	MY.NET.213.242
3	MY.NET.70.80
3	MY.NET.253.43
3	MY.NET.224.238
3	MY.NET.178.86
3	MY.NET.100.165
2	MY.NET.99.39

09/16-23:17:17.554757 65.27.86.23:3295 -> MY.NET.99.39:6346

```
TCP TTL:15 TOS:0x0 ID:21516  DF
**SF*PA* Seq: 0x80004A   Ack: 0xE3720E72   Win: 0x5018
0C DF 18 CA 00 80 00 4A E3 72 0E 72 05 1B 50 18  .......J.r.r..P.
22 38 55 2C 00 00 68 37 3D 29 35 64 6E 6D FF 5C  "8U,..h7=)5dnm.\
51 5C                                            Q\
```

The above packet looks to be an OS fingerprinting attempt. By setting multiple TCP flags that don't make sense, the fingerprinting program will use the response of the destination hosts IP stack to make a guess at which operating system the host runs. GNUTella commonly uses the destination port of the MY.NET address, this may be used to disguise the real motivation, which is to fingerprint the OS.

The Out of Spec data shows TCP flags all over the map. It looks like this is the work of skilled attackers mapping out the Operating Systems of the MY.NET hosts to make exploiting these systems quicker.

Executive Summary

The Internal network allows access to multiple services outside the University network and has caused internal system compromises. There is evidence of Trojan activity and loose security policies, which, allow multiple insecure protocols including tftp, GNUTella, X11, Napster and others. If a Security policy does not exist this should be made a top priority. Cleaning up the infected internal hosts, closing up access and removing offending software will not work unless security can be enforced. The University has liability risks due to the probes, scans, and attacks originating from within the University network against outside systems. Much tighter access rules need to be applied both inside and outside the network to prevent further attacks. The top attack, Code Red/Nimda was successfully mitigated Sept 19, likely filtered by a firewall or router.

Although this is a University setting and latitude is given to students to promote a free learning environment, this network is very susceptible to a wide range of attacks. Student use of questionable tools and applications has opened the network to allow complete control from outside. Multiple hosts within the network have been compromised either maliciously or by students running control applications remotely. Outside networks such as the Chinese net blocks detailed above have taken curious interest in the University network. The data from these net blocks should be analyzed in detail and block from communication unless required. The amount of probes, scans, attacks and exploits against the University network can be partially attributed to the current level of security. With so many vulnerabilities, this network has become a haven for hackers both inside and out.

Defence Recommendation

Step 1. A comprehensive review of the Universities Security Policies should be completed. Consideration of legal liabilities should be reviewed. Access should be denied to all applications allowing remote access, insecure file transfers/protocols and file sharing. Acceptable use polices should be developed and communicated to each student.

Step 2. Firewall/Router audits, including rule sets. A security policy of "deny all, accept required" should be adopted. Rule sets should be used to protect the network from inbound and outbound traffic thus stopping the use of questionable applications such as GNUTella and Napster.

Step 3. Apply latest security patches to all servers, desktops and network devices. This will prevent the malicious attacks from inside and outside the network.

Step 4. Install Personal firewalls to local PC's to further prevent use of questionable applications such as Napster, GNUTella and others. This will stop the traffic before it hits the network, preserving network bandwidth and preventing this type of activity within the network.

Step 5. Train University administrators on Intrusion Detection.

Step 6. A campaign of use awareness should be started to inform students and staff of security issues. This is one of the most important aspects of security and should be made a priority.

Step 7. Update all Virus Protect Software

Step 8. Discontinue the use of the default SNMP community string (public).

Analysis Process

Snort logs were obtained via http://www.research.umbc.edu/~andy. Five consecutive days were downloaded and processed. Tools used to process the Snort logs included awk, sed, cat, grep, egrep, and uniq.

Step 1. Combine all of the alert, scan and oos files into one file for each of the respective areas.

Example:

```
# cat alert.1 alert.2 alert.3 alert.4 alert.5 > alert.combined
```

Step 2. Run a count on the alerts to find the total. This can be used to find percentages of unique alerts.

```
# cat alert.combined | wc
```

Step 3. Sort the files by source address and destination address and run a count on each unique address. This was used to provide the Top 10 Talkers.

Example:

cat alert.combined | awk –F] ‘print{ $2}’ | awk –F [‘{print $1}’ | sort | uniq –c | sort –rn > alert.src.sorted

cat alert.combined | awk –F] ‘print{ $4}’ | awk –F [‘{print $1}’ | sort | uniq –c | sort –rn > alert.src.sorted

Step 4. Sort by alert type and count these alerts.

Example:

grep –e “WEB-MISC Attempt to execute cmd” alert.combined > WEB-MISC.txt

awk ‘{print $9}’ WEB-MISC.txt | sed ‘s/ /: /g’ | awk –F : ‘{print $1}’ | sort | uniq –c | sort –rn > WEB-MISC.top.talkers

Many other variations of the commands above were used to extract date as required. A knowledge transfer and training in these standard Unix tools is essential to sorting through the large amounts of data provided.

References Assignment 2 & 3:

SANS
www.sans.org

CERT
www.cert.org

Washtech.com
http://www.washtech.com/news/regulation/9392-1.html

CNN
http://asia.cnn.com/2001/TECH/internet/04/16/china.hacking/

Microsoft
www.microsoft.com

Cisco
www.cisco.com

Incidents.org

www.incidents.org

University of Washington
http://staff.washington.edu/dittrich/misc/tfn.analysis

Security Focus
www.securityfocus.com

Whitehats.com
www.whitehats.com

Network-tools.com
www.network-tools.com