Global Information Assurance Certification Paper

SANS Intrusion Detection in Depth

GCIA Practical v3.2

Name: Edmond Chiu

Assignment 1: Describe the State of Intrusion Detection

What is Intrusion Detection Message Exchange Format and Intrusion Detection Exchange Protocol?

Introduction

The intrusion detection(hereafter abbreviated as ID) technology is relatively new. Its importance in a layered approach and defense-in-depth to security has become more apparent as the complexity of network grows and more intrusions are successful. Vendors in the security industry has recognized the potentials in the ID market and are actively researching and marketing for more product offerings. This has contributed to many different proprietary systems in the current security marketplace.

Having numerous intrusion detection systems are important in the market place. This will promote research and ensure competition amongst different vendors. Business enterprises can benefit from competition as they now have different vendors to choose from. According to the article "New Directions in Intrusion Detection" from Information Security Magazine, (http://www.infosecuritymag.com/articles/august01/cover.shtml), "all enterprises should have at least one intrusion detection system on each network and critical server to detect attacks." In practice, rarely does an enterprise that employs an ID system had just one ID system implemented.

A layered approach security architecture often incorporates a network based ID system and host based ID system. Since incidents are often distributed over multiple locations within a network or enterprise, it is likely that different aspects of a single incident will be visible to different ID systems. As a result, it would be beneficial for diverse ID systems to be able to share data on attacks in progress. In order to do that, an interoperable Internet ID system protocols and structures must be created to enable ID system component communication.

Currently, the Internet Engineering Task Force (IETF), Intrusion Detection Exchange Working Group (IDWG) and Common Intrusion Detection Framework (CIDF) are putting together standards that include all facets of intrusion detection. Amongst the standards that have been completed was the Intrusion Detection Exchange Format requirements and data model, Intrusion Detection Message Exchange Format XML with Request For Comments (RFC) with these standards being recently issued. For the purpose of this paper, we will discuss these standards

and requirements.

Intrusion Detection Message Exchange

In order to define the Intrusion Detection Message Exchange Format (IDMEF), IDWG was formed. Its mandate was to "define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to the management systems that may need to interact with them." (www.silicondefense.com/idwg/draft-ietf-idwg-requirements-07.txt)

The rationale for such standard format is that users usually deploy different and more than one ID systems within their organizations. Those ID systems deployed may consist of host based ID systems, network based ID systems and application based ID systems that can either be commercial or free-ware. Because different products will generate different outputs, having a standard format for all the ID systems will ease the difficulty of interpreting these outputs. In addition, intrusions often involve multiple organizations or sites within an organization as victims. It is very likely that these organizations and sites would use different ID systems. In order to correlate and interpret these intrusions, it may be useful to have a common format. As well, this common format will also assist in commercial acceptance and justify further investment in research. The IDWG standards, if universally adopted, provide the following main advantages:

- Best-of-breed ID systems deployments. This will enable organizations to use different products in order to suit their specific needs and yet able to yield a common report.
- Correlation. As more devices, such as, routers, firewalls and IDS sensors, report IDMEF alerts, correlating events or intrusions among various sources will become easier.
- Interoperability. This will enable sensors, proxies and consoles from different vendors to communicate with each other.

In order to achieve the desired results, IDWG set out certain requirements and criteria for IDMEF. Some of the more pertinent requirements according to the Intrusion Detection Message Exchange Requirements draft –ietf-idwg-requirements-07 (www.silicondefense.com/idwg/draft-ietf-idwg-requirements-07.txt) include:

- The IDMEF specification should be able to operate in environments that contain IPv4 and IPv6 implementations. Since IPv4, hybrid IPv6/IPv4 and pure IPv6 environments are expected to exist within the time frame of IDMEF implementations, the IDMEF specification must support IPv6 and IPv4 environments.
- IDMEF message formats to support full internationalization and location. This requirement is important since network security and intrusion detection often cross many diverse boundaries i.e. geographic, political etc. Therefore, the IDMEF messages must be able to be presented and understood by a diverse group of operators.
- The format of IDMEF messages must support filtering and/or aggregation of data. Since

there will be filtering and aggregation performed on the IDMEF messages, this requirement must be satisfied.

- The IDMEF Communication Protocol (IDP) must support reliable transmission of messages.
- The IDP must support transmission of messages between ID components across firewall boundaries securely. Setting up communication between ID components should not require changes to the intervening firewalls that might weaken the security of the protected network.
- The IDP must support mutual authentication. As well, application layer authentication is required irrespective of the underlying transport layer. Since the messages will be transmitted across the network, it is critical that the receiver of these messages have confidence in the identity of the sender and that the sender have confidence in the identity of the receiver.
- The IDP must support confidentiality of the messages content during message exchange. This includes supporting the capability of supporting different encryption algorithms and adaptable to a wide variety of environments. It is crucial that the messages transmitted across the unsecured network be encrypted and shielded from prying eyes.
- The IDP must ensure the integrity of the message content. It must be able to support a variety of integrity mechanisms and adaptable to a wide variety of environments. Since non-repudiation of the origin of the IDMEF must be ensured, this requirement becomes important.
- The IDP should be able to resist protocol-related denial of service attacks. The IDP should also resist malicious duplication of messages. Availability and integrity of the ID systems that generate the messages is of paramount important. Therefore, IDP must be able to resist attacks that may impair its performance and resources.
- The IDMEF message must contain the identity of the source of the event and target component identifier if it is known. If it is a network-based event, this will be the source and destination IP address of the session used to launch the event.
- The IDMEF message must support the representation of different types of device addresses. This is useful as devices involved in an intrusion might use addresses that are not IP centric. i.e. MAC etc.

Intrusion Detection Exchange Protocol

Beside IDMEF as described above, IDWG also worked to define a standard for the Intrusion Detection Exchange Protocol (IDXP). Detailed IDXP standard and message elements can be found in (www.silicondefense.com/idwg/draft-ietf-idwg-beep-idxp-04.txt). IDXP, which specifies the data format and exchange procedures, and IDMEF will essentially allow different IDS components to communicate with one another.

To describe an intrusion attempt, IDMEF messages are generated. The format used for the IDMEF is Extensible Markup Language (XML). The IDMEF messages encapsulate the alert data

that is captured by the ID sensor and passed to the management console. One of the benefits of using XML is that XML is an extensible format and it will let vendors specify additional types of data that go beyond what is specified by the IDMEF Document Type Definition (DTD).

IDMEF alert messages are passed from the sensor to the management console using IDXP. IDXP supports confidentiality, integrity, and authentication over a connection-oriented protocol through the use of Blocks Extensible Exchange Protocol (BEEP) profiles. BEEP allows new connection-orientated application protocols to be developed quickly and many aspects of IDXP are provided within the BEEP framework.

BEEP has several profiles. They are the IDXP Profile, Tunnel Profile, Simple Authentication and Security Layer (SASL) Family of Profiles and the Transport Layer Security Profile.

According to the Intrusion Detection Exchange Protocol draft –ietf-idwg-beep-idxp-04 (www.silicondefense.com/idwg/draft-ietf-idwg-beep-idxp-04.txt). IDXP profile provides a mechanism for exchanging information between intrusion detection entities. The Tunnel profile is used to create an application layer tunnel that transparently forwards data over a chain of proxies. As well, the Tunnel profile will offer some kind of SASL authentication. With the TLS profile, it provides a combination of mutual confidentiality, integrity and mutual authentication for the IDXP profile.

As in the IDMEF, IDWG also set out certain requirements and criteria for IDXP. The following is some of the more pertinent requirements:

- IDXP must support reliable transmission of messages. Since IDXP operates over BEEP, this requirement is satirised by default as BEEP only operates over reliable connection-oriented transport protocols i.e. TCP etc..
- The IDXP must support transmission of messages between ID components across firewall boundaries securely. It is suggested that the Tunnel profile be used as an option to create application-layer tunnels to allow operation across firewalls. If the Tunnel profile is used, SASL should then be used as a mechanism to authenticate hosts.
- IDXP must support mutual authentication between the analyzer and the manager. It is suggested that the TLS be used to provide mutual authentication within the BEEP security profile.
- IDXP must support confidentiality of the messages content during message exchange. This includes supporting the capability of supporting different encryption algorithms and adaptable to a wide variety of environments. It is recommended that TLS profile be used as it provide TLS_DHE_DSS with 3DES_EDE_CBC_SHA cipher suite for confidentiality.
- IDXP must ensure the integrity of the message content. It must also be able to support a variety of integrity mechanisms and adaptable to a wide variety of environments. The TLS profile and SASL profile are encouraged to be used to ensure message integrity.
- IDXP should be able to ensure non-repudiation of the origin of the IDMEF messages. TLS through the authentication of public-key certificates can be used as the security profile to provide non-repudiation.

- The IDP should be able to resist protocol related denial of service attacks. The IDP should also resist malicious duplication of messages. Through the use of the TLS profile with the TLS_DHE_DSS with 3DES_EDE_CBC_SHA cipher suite, denial of service attacks and replay attacks can be prevented.

At the moment, the IDWG standards have still not conformed by the ID System vendors. However, it should be noted that Motorola www.Motorola.com/intrusionvision, has come out with a pure-play meta-ID system tool named Intrusion Vision (IV) in the past year. IV is configured to monitor all supported IDS sensor transmissions, collecting them all in one location, which is the console and form consolidated reporting of intrusion alerts. IV supports a wide range of sensors, for example, ISS Real Secure, NFR, Shadow, Kane Secure Enterprise, Cisco Secure and Snort etc.

The IDWG standards when fully developed and accepted will enable future ID systems to accept security alerts from all deployed security devices, interpret and format the raw data, extract information in a useful and manageable format. However, the major challenge remains to be whether the specifications within the standard can provide the kind of security and performance required as well as universal commercial vendor acceptance.

References:

www.silicondefense.com/idwg/draft-ietf-idwg-beep-idxp-04.txt

www.silicondefense.com/idwg/draft-ietf-idwg-requirements-07.txt

http://www.infosecuritymag.com/articles/august01/cover.shtml

http://www.sans.org/newlook/resources/IDFAQ/ID_standards.htm

http://www.ietf.org/html.charters/idwg-charter.html

http://www.incident.org/thesis/technology.html

www.Motorola.com/intrusionvision

Assignment 2 – Network Detects

Details on Corporate Network: The corporate network where the wild attack signatures are set-up were detected with a Snort sensor in front of a firewall. The corporate network has a Linux-based firewall with a screened subnet supporting Web, Mail and DNS servers. The corporate network exists on a commercial DSL high speed Internet provider. As well Internal addresses are protected using the RFC 1918 range of 192.168.1.0/24 address space. This information is useful when reviewing the following analysis of the detects presented below. Corporate network Internet registered IP's have been sanitized to a.b.c.d to hide true addressing.

Detect 1 – SCAN SOCKS Proxy Attempt

```
[**] SCAN SOCKS Proxy attempt [**]
06/08-18:46:57.783938 172.16.1.2:1080 -> a.b.c.d:1080
TCP TTL:63 TOS:0x0 ID:534 IpLen:20 DgmLen:60 DF
******S* Seq: 0xCF691FD1  Ack: 0x0  Win: 0x3EBC  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 493877 0 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] SCAN SOCKS Proxy attempt [**]
06/08-18:46:58.173230 172.16.1.2:1081 -> a.b.c.d:1080
TCP TTL:63 TOS:0x0 ID:541 IpLen:20 DgmLen:60 DF
******S* Seq: 0xCF772333  Ack: 0x0  Win: 0x3EBC  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 493915 0 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
[**] SCAN SOCKS Proxy attempt [**]
06/08-18:46:58.186854 172.16.1.2:1082 -> a.b.c.d:1080
TCP TTL:63 TOS:0x0 ID:543 IpLen:20 DgmLen:60 DF
******S* Seq: 0xCF3AFA03  Ack: 0x0  Win: 0x3EBC  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 493917 0 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
increments up to source port
[**] SCAN SOCKS Proxy attempt [**]
06/08-19:01:35.255092 172.16.1.2:1370 -> a.b.c.d:1080
```

TCP TTL:63 TOS:0x0 ID:2449 IpLen:20 DgmLen:60 DF

******S* Seq: 0x6D862FB Ack: 0x0 Win: 0x3EBC TcpLen: 40

TCP Options (5) => MSS: 1460 SackOK TS: 581624 0 NOP WS: 0

=+

1. Source of Trace

Corporate network

2. Detect Generated By

TCPDump 3.6.2 and Snort 1.8.

The detect was also generated by the Snort IDS rule under the scan.rules section: “alert tcp $EXTERNAL_NET any -> $HOME_NET 1080 (msg:"SCAN Proxy attempt"; flags:S; reference:url,help.undernet.org/proxyscan/; classtype:attempted-recon; sid:615; rev:2;)”

The detect rule is simplistic in nature, any external IP’s that target the home network at destination port 1080 with the syn flag set will be altered in the Snort alerts database.

3. Probability The Source Address Was Spoofed

The probability that the source address was spoofed is high as the 172.16.0.0 – 172.31.255.255 is an IANA reserved block of addresses not intended to be routable on the Internet. It is a possibility that the private address was used to obfuscate a legitimate address that was used during the same timeframe. Attackers that target systems sometimes use this method to drown out their source by using legitimate and illegitimate IP sources. In addition, the TTL value of the address was noted to be at a value of 63, or one hop away from its default TTL 64. Operating systems with TTL 64 and Window sizes of around 0X3ebc HEX or 16060 Decimal typically refer to a host that is probably Open BSD or AIX 4.3 according to http://www.incidents.org/archives/intrusions/msg01705.html . However because the sensor is Internet facing and does not normally see traffic with non-routable sources, it is very suspicious and is probably spoofed.

4. Description of The Attack

The attack is definitely a reconnaissance in nature. The attack is aimed at identifying hosts with

port 1080 open. Port 1080 is significant as there is an abundance of improperly configured wingate and Socks version 4 or 5 proxy servers on the Internet. My guess is that the attackers are not looking for security holes, but rather open socks `relays' to be used like open WinGates and mask the packet trails. The purpose would be to try to use it to gain access to an IRC server, making it look like the target machine was the packet source. However the only way an attacker would be able to receive the results of such a scan with spoofed IP source addresses would be to sniff on the local segment. There is no other way that the attacker would be able to see the results of the scan. The fact that the TTL value as described above is 63, (one hop from the target network) it is possible that an attacker could potentially be using the sniffer to collect this information. This is my best guest from the evidence collected.

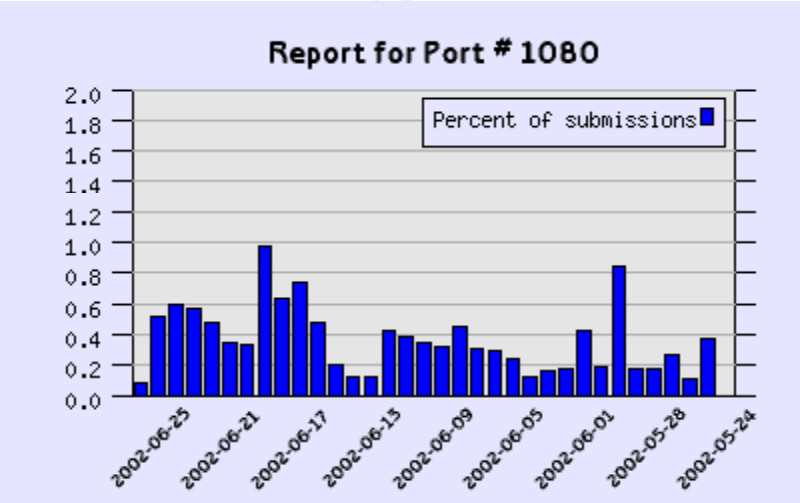
5. Attack Mechanism

As stated in Section 1, the attack works just to profile systems that have port 1080 open to the Internet. An attacker simply sends a packet with destination port 1080 set with a syn packet set to attempt to negotiate a connection on the said port. If the service is active, the server will send a Syn/Ack to the source identifying to the host that the service is running. A Syn/Ack from our target server would indicate a response from server with the proxy service listening. If an attacker is successful at identifying proxy servers, the next step will be to determine if these proxy servers are configured correctly. If not the attacker will take advantage of any vulnerabilities and traverse into the network via the proxy service port.

6. Correlations

a) As reported by Dshield, lies a graphic representation of scans on port 1080 in the past month.

(www.dshield.org)



b) http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0290 Wingate

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0291 Wingate

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-1435 Socks

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0471 Wingate

c) Evidence that this phenomena has occurred in the past can be found on http://www.dshield.org/pipermail/list/2001-July/000708.html

7. Evidence of Active Targeting

There is no direct evidence that suggests active targeting:

- Observing the time intervals from the source IP in the attack signatures tend to show that this is a targeted attack. Times between proxy scans are very close together. There is no evidence to suggest that this is a wide subnet attack as there are no proxy scans for other hosts on the corporate subnet or no other use of private IP ranges (i.e. as listed in RFC 1918).

However saying that the source IP is a private IANA address space, I lean on the theory that the attacker is hiding his traces behind scans that clutter the logs to make the true source less obvious.

8. Severity

Severity is determined by using the following formula:

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

Each metric is graded on a five points scale, with five being the highest and one being the lowest. The severity in this case is:

Criticality: 5 (This is a firewall and by virtue of its function is critical.)

Lethality: 3 (This is medium as the scan could be a result of an attacker using a sniffer off a local subnet thereby receiving results from a spoofed attack)

System Countermeasures: 4 (Modern OS is fully patched and is not running Proxy services)

Network Countermeasures: 5 (One choke into Firewalled environment, IDS acting as detective

control)

Severity: -1

Defensive Recommendation

One defensive recommendation would be to ensure that border routers and firewalls have rules that ensure that private IP addresses blocked. If proxy services are utilized on the network ensure that you have configured it with the latest patches available from the vendor and visit http://help.undernet.org/proxyscan.htm for a list of hyperlinks on how to secure wingate/socks 4 and 5 and Microsoft proxy services. In addition firewall policies should explicitly state that any service that is not explicitly permitted is denied and all new services must be supported by a business case.

Multiple Choice Test Question

One reason an attacker would scan for open socks proxy is to:

A) Attempt to see if the software its running is vulnerable

B) Attempt to use the proxy to gain access to a IRC server from the target host

C) Determine what OS version it is running

D) Use it to scan for other socks proxy servers on the Internet

Answer: A and B

Detect 2 – Web-IIS cmd.exe access Nimda

[**] WEB-IIS cmd.exe access [**]

06/12-05:05:28.159542 216.36.73.163:1318 -> a.b.c.d:80

TCP TTL:106 TOS:0x0 ID:18102 IpLen:20 DgmLen:120 DF

AP Seq: 0xD67E9F5 Ack: 0xA68D1672 Win: 0xFF00 TcpLen: 20

=+=

[**] WEB-IIS cmd.exe access [**]

06/12-05:05:28.400565 216.36.73.163:1325 -> a.b.c.d:80

TCP TTL:106 TOS:0x0 ID:18140 IpLen:20 DgmLen:120 DF

AP Seq: 0xD6D48BD Ack: 0xC86B271F Win: 0xFF00 TcpLen: 20

=+=

[**] WEB-IIS cmd.exe access [**]

06/12-05:05:28.654830 216.36.73.163:1332 -> a.b.c.d:80

TCP TTL:106 TOS:0x0 ID:18192 IpLen:20 DgmLen:136 DF

AP Seq: 0xD72867E Ack: 0xDA642472 Win: 0xFF00 TcpLen: 20

=+=

[**] WEB-IIS cmd.exe access [**]

06/12-05:05:28.899497 216.36.73.163:1342 -> a.b.c.d:80

TCP TTL:106 TOS:0x0 ID:18251 IpLen:20 DgmLen:157 DF

AP Seq: 0xD7AB348 Ack: 0xFEFB56FE Win: 0xFF00 TcpLen: 20

=+=

[**] WEB-IIS cmd.exe access [**]

06/12-05:05:29.146494 216.36.73.163:1393 -> a.b.c.d:80

TCP TTL:106 TOS:0x0 ID:18366 IpLen:20 DgmLen:157 DF

AP Seq: 0xD94B82E Ack: 0xD13F4162 Win: 0xFF00 TcpLen: 20

=+=

TCP Dump: **Selected Logs using tcpdump –vX –w dumpfile.date**

```
05:05:24.750542 216.36.73.163.4595 > a.b.c.d.80: P 1:73(72) ack 1 win 65280
(DF) (ttl 106, id 17464, len 112)
0x0000       4500 0070 4438 4000 6a06 dd90 d824 49a3 E..pD8@.j....$I.
0x0010       XXXX XXXX11f3 0050 0c20 011b c89f 4a9a  ...l...P......J.
0x0020       5018 ff00 b238 0000 4745 5420 2f73 6372 P....8..GET./scr
0x0030       6970 7473 2f72 6f6f 742e 6578 653f 2f63 ipts/root.exe?/c
0x0040       2b64 6972 2048 5454 502f 312e 300d 0a48 +dir.HTTP/1.0..H
0x0050       6f73                                    os
05:05:27.905769 216.36.73.163.1038 > a.b.c.d.80: P 1:71(70) ack 1 win 65280
(DF) (ttl 106, id 18079, len 110)
0x0000       4500 006e 469f 4000 6a06 db2b d824 49a3 E..nF.@.j..+.$I.
0x0010       XXXX XXXX040e 0050 0ccb 1372 c501 681e  ...l...P...r..h.
0x0020       5018 ff00 3d2f 0000 4745 5420 2f4d 5341 P...=/..GET./MSA
0x0030       4443 2f72 6f6f 742e 6578 653f 2f63 2b64 DC/root.exe?/c+d
0x0040       6972 2048 5454 502f 312e 300d 0a48 6f73 ir.HTTP/1.0..Hos
0x0050       743a                                    t:
05:05:28.147343 216.36.73.163.1318 > a.b.c.d.80: P 1:81(80) ack 1 win 65280
(DF) (ttl 106, id 18102, len 120)
```

```
0x0000      4500 0078 46b6 4000 6a06 db0a d824 49a3 E..xF.@.j....$I.
0x0010      XXXX XXXX0526 0050 0d67 e9f5 a68d 1672  ...l.&.P.g.....r
0x0020      5018 ff00 f3e7 0000 4745 5420 2f63 2f77 P.......GET./c/w
0x0030      696e 6e74 2f73 7973 7465 6d33 322f 636d innt/system32/cm
0x0040      642e 6578 653f 2f63 2b64 6972 2048 5454 d.exe?/c+dir.HTT
0x0050      502f                                    P/
05:05:28.388365 216.36.73.163.1325 > a.b.c.d.80: P 1:81(80) ack 1 win 65280
(DF) (ttl 106, id 18140, len 120)
0x0000      4500 0078 46dc 4000 6a06 dae4 d824 49a3 E..xF.@.j....$I.
0x0010      XXXX XXXX052d 0050 0d6d 48bd c86b 271f  ...l.-.P.mH..k'.
0x0020      5018 ff00 6287 0000 4745 5420 2f64 2f77 P...b...GET./d/w
0x0030      696e 6e74 2f73 7973 7465 6d33 322f 636d innt/system32/cm
0x0040      642e 6578 653f 2f63 2b64 6972 2048 5454 d.exe?/c+dir.HTT
0x0050      502f                                    P/
05:05:28.642631 216.36.73.163.1332 > a.b.c.d.80: P 1:97(96) ack 1 win 65280
(DF) (ttl 106, id 18192, len 136)
0x0000      4500 0088 4710 4000 6a06 daa0 d824 49a3 E...G.@.j....$I.
0x0010      XXXX XXXX0534 0050 0d72 867e da64 2472  ...l.4.P.r.~.d$r
0x0020      5018 ff00 e0de 0000 4745 5420 2f73 6372 P.......GET./scr
0x0030      6970 7473 2f2e 2e25 3235 3563 2e2e 2f77 ipts/..%255c../w
0x0040      696e 6e74 2f73 7973 7465 6d33 322f 636d innt/system32/cm
0x0050      642e                                    d.
05:05:28.887298 216.36.73.163.1342 > a.b.c.d.80: P 1:118(117) ack 1 win
65280 (DF) (ttl 106, id 18251, len 157)
0x0000      4500 009d 474b 4000 6a06 da50 d824 49a3 E...GK@.j..P.$I.
0x0010      XXXX XXXX053e 0050 0d7a b348 fefb 56fe  ...l.>.P.z.H..V.
0x0020      5018 ff00 a327 0000 4745 5420 2f5f 7674 P....'..GET./_vt
0x0030      695f 6269 6e2f 2e2e 2532 3535 632e 2e2f i_bin/..%255c../
0x0040      2e2e 2532 3535 632e 2e2f 2e2e 2532 3535 ..%255c../..%255
0x0050      632e 0x0000      4500 009d 474b 4000 6a06 da50 d824 49a3
      E...GK@.j..P.$I.
0x0010      XXXX XXXX053e 0050 0d7a b348 fefb 56fe  ...l.>.P.z.H..V.
0x0020      5018 ff00 a327 0000 4745 5420 2f5f 7674 P....'..GET./_vt
0x0030      695f 6269 6e2f 2e2e 2532 3535 632e 2e2f i_bin/..%255c../
0x0040      2e2e 2532 3535 632e 2e2f 2e2e 2532 3535 ..%255c../..%255
0x0050      632e                                    c.
                                    c.
05:05:29.134295 216.36.73.163.1393 > a.b.c.d.80: P 1:118(117) ack 1 win
65280 (DF) (ttl 106, id 18366, len 157)
```

```
0x0000      4500 009d 47be 4000 6a06 d9dd d824 49a3 E...G.@.j....$I.
0x0010      XXXX XXXX0571 0050 0d94 b82e d13f 4162  ...l.q.P.....?Ab
0x0020      5018 ff00 e65b 0000 4745 5420 2f5f 6d65 P....[..GET./_me
0x0030      6d5f 6269 6e2f 2e2e 2532 3535 632e 2e2f m_bin/..%255c../
0x0040      2e2e 2532 3535 632e 2e2f 2e2e 2532 3535 ..%255c../..%255
0x0050      632e                                    c.
```

Note: XXXX XXXX denotes intentional masking of corporate network IP address

1. Source of Trace

Corporate Network

2. Detect Generated By

TCPDump 3.6.2 and Snort 1.8.

The detect was also generated by the Snort IDS rule under the web-iis.rules section:

"alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS cmd.exe access"; flags:A+; content:"cmd.exe"; nocase; classtype:web-application-attack; sid:1002; rev:5;)"

The following Snort rule functions by doing a packet grep for the key ascii content "cmd.exe" from any host and port to destination web server ports.

3. Probability The Source Address Was Spoofed

It is not probable that the source was spoofed for the following reasons:

- Nature of attack requires 3 way TCP handshake to be successful
- Nature of signature is not a DoS, typically used with spoofed sessions
- Nature of how source sequence number packets and IP ID numbers are generated appear to have not been packet crafted as they are not identical or have low source port numbers.
- This attack signature is a worm and by its nature and characteristics is not from a spoofed source.

4. Description of The Attack

This is a known worm against Microsoft IIS web servers as well as servers running any version of Windows that have been infected with the Nimda Worm. Nimda began its propagation across the Internet September 18 2001. Nine months later Microsoft web servers across the Internet are still propagating the worm. The attack exploits inherent buffer overflow vulnerabilities in IIS including (i.e. the Unicode exploit, idq extension exploit and index server exploits) . Correlations and CVE references can be viewed by Section 6. Specifically nimda is known to target 4 discrete methods (discussed below). Nimda was so damaging and successful when initially released that it caused denial of service effects by large networks. Nimda is capable of compromising the entire security of a Windows machine by providing an attacker with full access of administration and system files.

5. Attack Mechanism

The worm propagates in the following 4 manners:

1. The worm scans for Microsoft servers and attempts to exploit numerous different Windows/IIS exploits, including the IIS/Personal web server extended Unicode directory traversal vulnerability, IIS/Personal web server escaped character decoding command execution vulnerability, and potential backdoors left by previous Code Red II and Sadmind infections. After successful infection of a compromised host, the worm uses the hosts tftp client to transfer code from the attacking host to the compromised host. The file tftp'ed is named Admin.dll.

2. The worm also collects e-mail addresses from the Windows address book and users mail boxes and mails itself to all addresses as an attachment named README.exe. The most common mail program used for this exploit happens to be Outlook or Outlook Express.

3. The worm also, if successfully infected by a web server, is capable of using the HTTP transport protocol to propagate itself to clients that visit the infected servers web page. If someone who has an unpatched Windows machine, the infected web server creates a MIME-encoded copy ofr itself named README.eml and searches the directory for web based extensions. The worm then attaches a piece of javascript to these web extention files. The javascript forces a download of README.eml to any client that reads the file with a browser. This would infect IE browsers especially if javascript in the browser is enabled.

4. The fourth discrete method that the worm can infect Windows machines is with open files shares. The worm will copy itself to open file shares for which the user has write permissions enabled. The worm is also capable of attaching itself to .exe files (executable binary files) that it finds in these permissive shares. Then the worm is manually exploited when someone loads one of these files that is infected.

Note: the following explanation has been taken from
http://www.securityspace.com/smysecure/w32_nmda_amm.html

6. Correlations

a) As reported by Dshield, lies a graphic representation of scans from Nimda in the past month. (www.dshield.org)

b) Bugtraq ID: 2524 / CVE ID: CAN-2001-0154

Microsoft Security Bulletin MS01-020

http://www.Microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

VulDB: http://www.securityfocus.com/bid/2524

Bugtraq ID: 2708 / CVE ID: CAN-2001-0333

Microsoft Security Bulletin MS01-026

http://www.Microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-026.asp

VulDB: http://www.securityfocus.com/bid/2708

Bugtraq ID: 1806 / CVE ID: CVE-2000-0884

Microsoft Security Bulletin MS00-078

http://www.Microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp

http://www.securityfocus.com/bid/1806

CVE ID: CVE-2001-26

http://www.cert.org/advisories/CA-2001-26.html

7. Evidence of Active Targeting

No evidence that this is active targeting. The following attack signature and order of automation of specific http get sequences from Nimda worm measure up. This is definitely not a case of active targeting but the worm looking for a vulnerable host to propagate to.

8. Severity

Severity is determined by using the following formula:

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

Each metric is graded on a five point scale, with five being the highest and one being the lowest. The severity in this case is:

Criticality: 4 (the server is directed at a web server and is critical by default)

Lethality: 3 (the exploits lethal to unpatched and unhardened web servers running IIS)

System Countermeasures: 5 (the web server is not running Microsoft IIS)

Network Countermeasures: 5 (the environment is protected by a firewall and has IDS detection running. All servers are patched up-to-date)

Severity: -3

9. Defensive Recommendation

Defences are appropriate for this scenario, as the corporate network does not have any Windows machines. However, it may be prudent to reinforce corporate policies and hardening guidelines to suggest that all machines/hosts shall be hardened according to industry standards. This means that all unnecessary services removed, file and folder shares with appropriate access controls, antivirus software installed with the latest definitions, and security/system patches that are regularly implemented from the vendor. Specifically for Windows machines, it is recommended that Administrator to visit www.Microsoft.com/security and utilize the "tools and services section" to harden and check the security of Windows machines. In addition, if Microsoft web servers are required, administrators may recommend to install reverse proxy servers to protect web server requests from the Internet and use it as a measure of "Defence In Depth".

10. Multiple Choice Test Question

Which is not a method by which the Nimda worm can propagate

A) Open Windows file shares with user write permissions on directories set

B) Visiting a web server already infected by Nimda

C) Opening an README.EXE from an email attachment from a server infected by nimda

D) Running a default install of Apache web server with RedHat Linux 7.1 on the Internet.

Answer: D) Nimda is a worm coded primarily for Windows.

Detect 3 – Shellcode x86 inc ebx NOOP

Snort Alert.ids Log

[**] SHELLCODE x86 inc ebx NOOP [**]

05/14-15:56:34.414488 216.33.75.21:80 -> 78.37.212.28:64569

TCP TTL:49 TOS:0x0 ID:2602 IpLen:20 DgmLen:1500 DF

AP Seq: 0x18A469FB Ack: 0x1B2A85E Win: 0x7D78 TcpLen: 20

=+=TCPDump Log using tcpdump –Xv –s 1500 –w dump.date (Default snap length is only 68 bytes too short to see all details therefore increased to 1500 bytes)

```
15:56:34.414488 216.33.75.21.80 > 78.37.212.28.64569: P [bad tcp cksum
b7ba!] 413428219:413429679(1460) ack 28485726 win 32120 (DF) (ttl 49, id
2602, len 1500, bad cksum 39c2!)
0x0000       4500 05dc 0a2a 4000 3106 39c2 d821 4b15 E....*@.1.9..!K.
0x0010       4e25 d41c 0050 fc39 18a4 69fb 01b2 a85e N%...P.9..i....^
0x0020       5018 7d78 df82 0000 4854 5450 2f31 2e30 P.}x....HTTP/1.0
0x0030       2032 3030 204f 4b0d 0a43 6f6e 7465 6e74 .200.OK..Content
0x0040       2d54 7970 653a 2061 7070 6c69 6361 7469 -Type:.applicati
0x0050       6f6e 2f78 2d73 686f 636b 7761 7665 2d66 on/x-shockwave-f
0x0060       6c61 7368 0d0a 436f 6e74 656e 742d 4c65 lash..Content-Le
0x0070       6e67 7468 3a20 3230 3237 340d 0a4c 6173 ngth:.20274..Las
0x0080       742d 4d6f 6469 6669 6564 3a20 4672 692c t-Modified:.Fri,
0x0090       2031 3520 4170 7220 3139 3934 2030 303a .15.Apr.1994.00:
0x00a0       3030 3a30 3020 474d 540d 0a44 6174 653a 00:00.GMT..Date:
0x00b0       2054 7565 2c20 3134 204d 6179 2032 3030 .Tue,.14.May.200
0x00c0       3220 3230 3a35 363a 3033 2047 4d54 0d0a 2.20:56:03.GMT..
```

```
0x00d0      436f 6e6e 6563 7469 6f6e 3a20 6b65 6570 Connection:.keep
0x00e0      2d61 6c69 7665 0d0a 4578 7069 7265 733a -alive..Expires:
0x00f0      2054 6875 2c20 3135 2041 7072 2032 3031 .Thu,.15.Apr.201
0x0100      3020 3230 3a30 303a 3030 2047 4d54 0d0a 0.20:00:00.GMT..
0x0110      0d0a 4657 5305 324f 0000 7000 0bb8 0000 ..FWS.2O..p.....
0x0120      9c40 000c 0100 4302 ffff ff7f 05bd 1700 .@....C.........
0x0130      0001 00ff d9ff d8ff d8ff e000 104a 4649 .............JFI
0x0140      4600 0102 0000 6400 6400 00ff ec00 1144 F.....d.d......D
0x0150      7563 6b79 0001 0004 0000 000f 0000 ffee ucky............
0x0160      000e 4164 6f62 6500 64c0 0000 0001 ffdb ..Adobe.d.......
0x0170      0084 0013 0f0f 1711 1725 1616 252f 241d .........%..%/$.
0x0180      242f 2c24 2323 242c 3a32 3232 3232 3a43 $/,$##$,:22222:C
0x0190      3d3d 3d3d 3d3d 4343 4343 4343 4343 4343 ======CCCCCCCCCC
0x01a0      4343 4343 4343 4343 4343 4343 4343 4343 CCCCCCCCCCCCCCCC
0x01b0      4343 4301 1417 171e 1a1e 2418 1824 3324 CCC.......$..$3$
0x01c0      1e24 3342 3329 2933 4243 423e 323e 4243 .$3B3))3BCB>2>BC
0x01d0      4343 4343 4343 4343 4343 4343 4343 4343 CCCCCCCCCCCCCCCC
0x01e0      4343 4343 4343 4343 4343 4343 4343 4343 CCCCCCCCCCCCCCCC
0x01f0      4343 4343 ffc0 0011 0800 f701 2c03 0122 CCCC........,.."
0x0200      0002 1101 0311 01ff c400 7e00 0002 0301 ..........~.....
0x0210      0100 0000 0000 0000 0000 0000 0004 0203 ................
0x0220      0501 0601 0101 0101 0100 0000 0000 0000 ................
0x0230      0000 0000 0001 0203 0410 0002 0102 0405 ................
0x0240      0302 0404 0603 0000 0000 0102 0011 0321 ...............!
0x0250      3112 0441 5171 1305 6181 2291 32a1 4223 1..AQq..a.".2.B#
0x0260      14f0 b1c1 72f1 5262 3315 06d1 e182 1101 ....r.Rb3.......
0x0270      0101 0003 0101 0000 0000 0000 0000 0000 ................
0x0280      0111 3102 1241 21ff da00 0c03 0100 0211 ..1..A!.........
0x0290      0311 003f 0057 ae72 4581 e143 2d5d 95c2 ...?.W.rE..C-]..
0x02a0      3543 f677 470a cf43 8a56 77f7 6c9c ea39 5C.wG..C.Vw.l..9
0x02b0      34d5 daef 5773 80c1 8709 8ad6 5866 2563 4...Ws......Xf%c
0x02c0      529a ae04 4962 ebd3 d635 67e5 6587 2332 R...Ib...5g.e.#2
0x02d0      b65b 86bf 6eaf f703 4334 f646 a597 989c .[..n...C4.F....
0x02e0      eb51 5561 50a2 a721 3991 a4a3 78fa 6dd3 .QUaP..!9...x.m.
0x02f0      8b4a 33ef dd2e 4bb6 517b 2e2b 5339 b86c .J3...K.Q{.+S9.l
0x0300      97de 5db3 d99b e6a7 29d3 8610 7d27 1ce5 ..].....)...}'..
0x0310      9676 ae41 a8a4 d54d 85b5 e11a 16c2 ccde .v.A...M........
```

```
0x0320      cd63 cd5e b0ca 7194 0254 d467 3d26 e36e .c.^..q..T.g=&.n
0x0330      2e0c b198 7bad b9b4 6bc2 5975 2cc3 3b6d ....{...k.Yu,.;m
0x0340      c953 5197 1134 ea18 5464 679d b6f4 349a .SQ..4..Tdg...4.
0x0350      bb2b f5f8 1c8e 5258 4ad8 3fa9 b6e9 fd26 .+....RXJ.?....&
0x0360      7dd6 a231 f48f ecfe 48e9 fc63 336f ff00 }..1....H..c3o..
0x0370      b6dd 2663 5581 7306 a729 a9e3 deab 4e53 ..&cU.s..)....NS
0x0380      2eef de66 bec6 de9b 608c ccdd 6634 1582 ...f....`...f4..
0x0390      e24d 2316 f709 9ae3 33ee 1b56 b1b8 3537 .M#.....3..V..57
0x03a0      296d a7d6 bab4 e9f4 98b1 ad31 7999 f006 )m.........1y...
0x03b0      9122 f62d 369c 59be b1bd 7a85 6445 a5ad ."-6.Y...z.dE..
0x03c0      6910 5684 38a8 0475 98bb fdb9 4b95 5c8e i.V.8..u....K.\.
0x03d0      33d0 9184 4b76 9aa9 ee25 9529 7d93 d548 3...Kv...%.)}..H
0x03e0      e936 89ee 6d41 e5fd 279a d85c d373 4f39 .6..mA..'..\.sO9
0x03f0      e8f6 27b9 65ed ff00 18c7 6585 4193 0650 ..'.e.....e.A..P
0x0400      0c90 6905 c46a 1d24 ad9a ca83 4921 a180 ..i..j.$....I!..
0x0410      c3d0 2caa d50a 904c 93be 9153 9482 b07c ..,....L...S...|
0x0420      4293 22bb 6aa0 7a49 354e 12bb a5a9 89d3 B."j.zI5N......
0x0430      5c84 95bf 8a53 8f18 0b3e 121a a76e 3549 \....S...>...n5I
0x0440      95d6 6993 ab6c 5241 d692 fac8 1159 149d ..i..lRA.....Y..
0x0450      c407 84cd dcd9 d06a 26a5 dbaa 8699 9943 .......j&......C
0x0460      2ade 5204 d44a e78c ff00 6dba cd2d b369 *.R..J....m..-.i
0x0470      ba3d 7099 fe3c 5159 7886 8d86 d241 e464 .=p..<QYx....A.d
0x0480      a45f 7c69 b8c3 d666 efde b702 7213 5b78 ._|i...f....r.[x
0x0490      3e61 b989 e7b7 772b 7c9e 51d4 aa2f 62e2 >a....w+|.Q../b.
0x04a0      6dec 6de8 498c 46a6 53ce 6bda ee91 5042 m.m.I.F.S.k...PB
0x04b0      afac b523 4945 44ef 589d a76a d758 6118 ...#IED.X..j.Xa.
0x04c0      26ab 598c 6d55 ddc2 83a5 46a6 e422 d76c &.Y.mU....F.."l
0x04d0      dcbc a438 143f 5125 7352 29ed 0f94 2cad ...8.?Q%sR)...,.
0x04e0      d342 ff00 fd4a 8c2b f61a c3e9 6f69 6edd .B...J.+....oin.
0x04f0      e83a 18e7 96b5 50ac 33ca 67a8 2831 e737 .:....P.3.g.(1.7
0x0500      3f59 af4b b0b9 a9c1 ff00 30fe 515d e2e9 ?Y.K......0.Q]..
0x0510      3717 acab c6df a5c5 53cf 08df 935a 39ff 7.......S....Z9.
0x0520      0052 cc71 5af8 f305 7535 26b7 8d63 a349 .R.qZ...u5&..c.I
0x0530      cc4c f7b7 f986 6268 d97d 605d 1d1a 6eb3 .L....bh.}`]..n.
0x0540      1a0b 6d49 d5c6 4cae 1e92 bb6d 2e72 1b0e ..mI..L....m.r..
0x0550      139b 6a6d 82d5 9247 20d0 6322 171c 4ce9 ..jm...G..c"..L.
0x0560      745c 04a8 b198 1896 f2e1 b76c bae6 32f7 t\.........l..2.
```

```
0x0570       8cab ebc7 8447 c9b8 5b24 7124 442b 22c3 .....G..[$q$D+".
0x0580       69b8 a7d6 7a6f 18f4 b857 98fe 53ca 5693 i...zo...W..S.V.
0x0590       d0ec 6e52 ea37 3c3e b35d b848 ede1 a2e3 ..nR.7<>.].H....
0x05a0       2f23 221a 5fe4 574d e279 8ac5 2b24 16ea /#"._.WM.y..+$..
0x05b0       920f 4946 a9dd 501e 5bb8 5240 ab0f b090 ..IF..P.[.R@....
0x05c0       0f09 1b2a 1d68 6581 1d3d 6450 9689 ce4e ...*.he..=dP...N
0x05d0       e7c1 4ce8 d7ca 44a9 26ad c245           ..L...D.&..E
```

1. Source of Trace

Source of Trace is http://www.incidents.org/logs/Raw/2002.4.14

2. Detect Generated By

Detect was generated by Snort 1.8 and tcpdump 3.6.2. The Snort rule that this detect was generated from is alert: “alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE x86 inc ebx NOOP"; content:"|43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43|"; classtype:shellcode-detect; sid:1390; rev:2;)”

3. Probability The Source Address Was Spoofed

The probability that this source was spoofed is unfounded for the following:

- Source of detect is not Denial of Service in Nature. The packet that causes this type of event is also normally a part of an established TCP session
- Packet fields do not appear to be crafted with low TTL or low source port ranges
- The packet in questions seems to be a response to stimulus from the 78.37.212.28 home network

4. Description of The Attack

As stated by Stephen Northcutt from “Intrusion Signatures and Analysis” (New Riders Publishing:2001) “ Buffer overflows are the top of the lethality food chain.” A buffer is an area of memory that stores information in a variable for a program. When programmers do not check or validate the input into these variables, it is possible to insert more information than the buffer was designed to hold. A basic buffer overflow attack can occur when buffers are overflowed with machine shellcode that intentionally overwrite a buffer and attempt to insert malicious code

to be executed than what the code was originally designed to do. Upon closer interrogation of the alert, the "Shellcode x86 inc ebx NOOP" attack is not suspicious. It is not a true buffer overflow attack from port 80 to the homenet port of 64569 (Excerpt from http://archives.neohapsis.com/archives/sf/ids/2002-q2/0029.html) "The key thing to remember is that just because these things trigger alerts doesn't mean that somebody is attacking you. These signatures are not triggering on the attack, but some (hopefully unique) fingerprint related to the attack. You can't just throw shellcode blindly at a machine and hope it will work, the real vulnerability will be something specific to the victim machine, shellcode is just one mechanism for exploiting that vulnerability. "

5. Attack Mechanism

The intent of the alert was to flag attempts whereby the IDS (Snort) flagged repeated content of the Hex Value 0x43 which is represented as the capital letter C in ASCII. In the context of a real buffer overflow attack the exploits would send a series of these No-Opperatrion (NOOP) bytes to pad the buffer and try and successfully append their exploit like /bin/sh as a common example. From our alert selected, the signature was too vague and from further interrogation is a false positive as it appears to be a response to a web server request with embedded shockwave content extensions.

6. Correlations

http://archives.neohapsis.com/archives/sf/ids/2002-q2/0029.html

Site has an article demonstrating the false positive nature of the Shellcode x86 inc ebx NOOP Snort rule.

7. Evidence of Active Targeting

The following example is not a true attack and thus is not actively targeted. As well the source IP address has not been found in any other instance of the log files that we examined that indicated that address was used in any reconnaissance or attack.

8. Severity

Severity is determined by using the following formula:

Severity = (Criticality + Lethality) - (System + Network Countermeasures)
Each metric is graded on a five point scale, with five being the highest and one being the lowest. The severity in this case is:

Criticality: 1 (appears to be a user workstation as it was surfing a web server on the Internet)

Lethality: 0 (The detect was measured to be a false positive from analysis of the IDS alert and Snort dump files)

System Countermeasures: 2 (We do not know the system and should not assume that these system controls are in place and effective)

Network Countermeasures: 1(We do not know the network nor if the workstation is in place of a firewall with adequate countermeasure security)

Severity: -2

9. Defensive Recommendation

No defensive recommendation is required. However, default Snort rules should be understood how these alerts are triggered. Too general and there are more false positives, too specific and attacks are not registered with the IDS. With "packet grepping" type rules, these scenarios will always be imperfect. The next time they are encountered, they should first be quarantined and investigated before defensive recommendations can be applied effectively. Overall, it is suggested that the best defence for buffer overflow attacks is to ensure a timely process for patching system and security patches from the vendor is in place. If the platform is Unix, the nit might be also possible to make kernel adjustments that make the stack non executable, this will not prevent overflowing to the heap but the majority of buffer overflow attacks do occur as a result of an executable stack on the operating system. Today new security products like Host based intrution detection systems like Okena, and e-trust Access Control as well as some open source tools like Tripwire can be used to monitor and control file and code integrity that can protect from buffer overflow attacks.

10. Multiple Choice Test Question

Buffer overflow attacks typically come from

A) Established TCP/IP sessions

B) Spoofed TCP/IP sessions

C) Demon Networks

D) Malformed packet crafting

Answer: A

Assignment 3: "Analyze This" Scenario

1. Executive Summary

Edmond Chiu has been asked by the University to perform a review and analysis of its IDS system and identify potential network problems and signs of compromised systems. The University has provided 3 datasets over a 5 day period beginning March 27 2002 – March 31 2002. The logs were derived from an open source IDS solution called Snort. Over the 5-day period, 3 sets of logs were reviewed: Scan, Alert and OOS logs. Scan logs are detects that Snort records network reconnaissance. Alert logs contain IDS signature rule matches. OOS are Out of Specification logs that have unconventional TCP flags set.

To summate, universities are open entities and their networks no different, it is critical for the University to establish policy on what type of ports, protocols and applications are known and advocated. By establishing a known baseline of network activity, it becomes easy for the University to know and understand unknown and deviant traffic.

Our analysis of the logs was without context. Our review is without a formal understanding of what security perimeter devices exist and the formal processes around those devices that make them effective. Our observations and information about the perimeter devices, configurations, and network architecture are purely deductive on the analysis of the logs that were received. Therefore we are not at liberty to assume that the alerts are or not false positives but only can hypothesize given the nature of the organization. It appears that the top ten alerts are commensurate with University activity. Given that most inter traffic communication existed within the University and the nature of activity focuses around printing, instant messaging and peer to peer file transfers. This can almost be considered normal traffic. In this case we recommend the University Network and Security group to reconfigure the IDS to ensure that normal traffic is tuned out so IDS administrators are capable of detecting malicious traffic, low and slow scans, and high risk signatures.

Reconfiguring and tuning the IDS will also have greater accuracy when dealing with false positives. Since IDS signature pattern matching is a difficult art form, we must be able to know how much to trust the validity of a Snort rule. From the top ten alerts noted the Spp_http_decode: IIS Unicode attack detected is one, which can be noted for high false positive rates. This is because the Snort rule is prone to false positives. We noted that in our SPP_http_decode example the target IP address was a Chinese Web Mail Login site that probably uses Unicode characters and hence the false impression that it was a legitimate attack.

However we should not assume that all detects picked up by the IDS is non-malicious. The best recommendation is to ensure that patches (viruses and system) on systems are kept up to date and hosts are configured with HIDS (Host Intrusion Detection Systems) to detect anomaly traffic and preserve data confidentiality and integrity of University resources. Again, if hosts and systems are patched, up to date, this preventative control is far more effective than what an IDS is a detective control. One good example demonstrated by our analysis deals with the high activity

discovered around the use of MSN Instant Messenger Chat (6th top alert reported). A widely publicized vulnerability has been released (CERT® Advisory CA-2002-13 Buffer Overflow in Microsoft's MSN Chat ActiveX Control). This vulnerability could be mitigated if patches from the vendor are installed on a timely basis.

Top talkers should also be investigated on high anomaly activity as they can be an indicator on active reconnaissance or active targeting before a potential compromise. Out-of-spec scans should almost always be investigated as they are sure signs of malicious activity. A formal incident response team should ensure that events like OOS are investigated and recorded as they may be signs of potential denial of service attacks or passive OS fingerprint techniques.

What is also interesting is the fact that the following GIAC past security reviews had found similar top 7 of 10 alerts as our log sample.
They are:
http://www.giac.org/practical/Angela_Orebaugh_GCIA.doc
http://www.giac.org/practical/Martha_Flick_GCIA.zip
http://www.giac.org/practical/Todd_Chapman_GCIA.doc

Shared top 10 alerts include: Spp_Http_Decode, Smb Name Wildcard, Snmp Public Access, Icmp Echo Request L3retriever Ping, High Port 65536 Udp, Info Msn Im Chat Data, Connect To 515 From Inside.

2. Scope and Approach

The scope of this audit is to provide a security assessment on the University network over 5 consecutive days based on the provided logs. Upon analysis of the logs, pertinent security recommendations will be rendered in order to allow controls to be strengthened and risks to be mitigated within the University network. In order to maximize resources and lower the costs, it should be noted that not all alerts would be individually assessed. For those alerts that fall into general categories, general assumptions would be used. Only those alerts that present risks and likely exploits would be analyzed in greater details.

The files that were given are as follows:

#	Day	Alert	Scan	OOS
1.	March 27 02	Alert.020327.gz	Scan.020327.gz	Oos_Mar.27.2002.gz
2.	March 28 02	Alert.020328.gz	Scan.020328.gz	Oos_Mar.28.2002.gz
3.	March 29 02	Alert.020329.gz	Scan.020329.gz	Oos_Mar.29.2002.gz
4.	March 30 02	Alert.020330.gz	Scan.020330.gz	Oos_Mar.30.2002.gz
5.	March 31 02	Alert.020331.gz	Scan.020331.gz	Oos_Mar.31.2002.gz

Upon analyzing the dates of the files, it was noted that they spanned over 5 days at the end of the

March 2002 that included normal weekday and weekend.

3. Analysis

During the 5-day period, a total of 3,823,119 scans were logged. It is noted that majority i.e. 94% of the scans were of ports scanning/reconnaissance nature. Out of all the scans, there were 382,869 alert log entries. In addition, there were 42 OOS files were detected. For the Top-Ten alerts, a description of the alerts, analysis and recommendations were provided in order to enable the University to take appropriate course of actions.

Statistical Breakdown: Alerts Logs 5 day period

Name of Alert	*# of Counts*	*% of Total*
Spp_http_decode: IIS Unicode attack detected	**57675**	**23.73**
SMB Name Wildcard	**47283**	**19.46**
Connect to 515 from inside	**44979**	**18.51**
SNMP public access	**37562**	**15.46**
ICMP Echo Request L3retriever Ping	**23126**	**9.52**
INFO MSN IM Chat Data	**7654**	**3.15**
ICMP Echo Request Nmap or HPING2	**3742**	**1.54**
INFO Outbound GNUTella Connect Request	**2933**	**1.21**
High Port 65535 UDP – Possible Red Worm – Traffic	**2242**	**0.92**
INFO Inbound GNUTella Connect Request	**2190**	**0.90**
Watchlist 000220 IL-ISDNNET-990517	2134	0.88

ICMP Fragment Reassembly Time Exceeded	1735	0.71
MISC Large UDP Packet	1727	0.71
WEB-IIS view source via translate Header	891	0.37
WEB-MISC Attempt to execute cmd	883	0.36
ICMP Router Selection	874	0.36
NMAP TCP ping!	865	0.36
Port 55850 tcp - Possible Myserver Act.	861	0.35
FTP DoS Ftpd Globbing	548	0.23
Null scan!	382	0.16
Watchlist 000222 NET-NCFC	348	0.14
SCAN Proxy attempt	219	0.09
INFO FTP Anonymous FTP	210	0.09
Possible Trojan Server Activity	208	0.09
WEB-FRONTPAGE _vti_rpc Access	188	0.08
WEB-IIS _vti_inf Access	184	0.08
INFO Napster Login	140	0.06
WEB-CGI scriptalias access	131	0.05
Suspicious Host Traffic	119	0.05
INFO Possible IRC Access	93	0.04

ICMP Destination Unreachable (Com. Admin. Proh.)	90	0.04
INFO - Possible Squid Scan	87	0.04
INFO Napster Client Data	79	0.03
Queso Fingerprint	60	0.02
Incomplete Packet Fragments	55	0.02
FTP CWD / - possible Warez Site	54	0.02
WEB-MISC 403 Forbidden	53	0.02
High port 65535 tcp – Possible Red Worm – Traffic	51	0.02
Spp_http_decode: CGI Null Byte Attack Detected	46	0.02
ICMP Echo Request Windows	42	0.02
SCAN Synscan Portscan ID 19104	42	0.02
EXPLOIT x86 setuid 0	24	0.01
Russia Dynamo - SANS Flash 28-jul-00	24	0.01
EXPLOIT x86 NOOP	22	0.01
ICMP Traceroute	19	0.01
WEB-MISC Compaq Nsight Directory Traversal	17	0.01
EXPLOIT x86 setgid 0	12	0.00
Attempted Sun RPC High Port Access	10	0.00
ICMP Echo Request BSDtype	10	0.00

Tiny Fragments - Possible Hostile Activity	9	0.00
Back Orifice	7	0.00
MISC Traceroute	7	0.00
TCP SRC and DST Outside Network	7	0.00
WEB-MISC http directory Traversal	6	0.00
EXPLOIT NTPDX Buffer Overflow	5	0.00
WEB-IIS Unauthorized IP Access Attempt	5	0.00
ICMP Destination Unreachable (Protocol Unreachable)	4	0.00
SCAN FIN	4	0.00
BACKDOOR NetMetro Incoming Traffic	4	0.00
X86 NOOP – Unicode BUFFER OVERFLOW ATTACK	3	0.00
INFO Inbound GNUTella Connect Accept	3	0.00
WEB-MISC ICQ Webfront HTTP DOS	3	0.00
RPC tcp traffic Contains bin_sh	2	0.00
Port 55850 udp - Possible myserver Activity - ref. 010313-1	2	0.00
ICMP Echo Request CyberKit 2.2 Windows	2	0.00
BACKDOOR NetMetro File List	2	0.00

X11 Outgoing	1	0.00
TFTP - External UDP Connection To Internal Tftp Server	1	0.00
TFTP – Internal UDP Connection To External Tftp Server	1	0.00
EXPLOIT x86 Stealth Noop	1	0.00
SYN-FIN scan!	1	0.00
SMB CD...	1	0.00
ICMP Echo Request Sun Solaris	1	0.00
EXPLOIT x86 NOPS	1	0.00
WEB-MISC webdav search access	1	0.00

Top 10 Alert Descriptions

Name of Alert	*Description of Alert*

Spp_http_decode: IIS Unicode attack detected	**Description:** Microsoft IIS Based Attack. If web server is vulnerable, attacker is able to execute commands or scripts on box. According to http://www.cve.mitre.org and SANS http://www.sans.org/top20.htm , IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters. However http://www.Snort.org/docs/faq.html#4.17 has posted that this signature is prone to false positives. Similar to what the FAQ has reported, internal users normally surfing the Internet can trigger these alerts with the Snort http decode preprocessor. In addition it was also noted that Netscape and foreign texts (UTF-8 encoding) can cause these false positives as well. **Analysis:** Unicode character substitution is detected in URL stream. Numerous hosts were found to be under this attack. The hosts targeted may be unpatched and thus susceptible to this attack. The example below illustrates most of internal users surfing external sites generated these signatures. The following alert is most likely to be a false positive. **Example of Detect taken from Snort:** 03/27-08:54:54.812862 [**] spp_http_decode: IIS Unicode attack detected [**] 1.1.153.197:2288 -> 211.233.28.183:80 03/27-08:54:54.812862 [**] spp_http_decode: IIS Unicode attack detected [**] 1.1.153.197:2288 -> 211.233.28.183:80 03/27-08:54:54.812862 [**] spp_http_decode: IIS Unicode attack detected [**] 1.1.153.197:2288 -> 211.233.28.183:80 **Recommendation:** Although this is probably a false positive, the University should always ensure that all hosts that run MS IIS servers should be applied with the latest patch. Patches could be found in http://www.Microsoft.com/Downloads/Release.asp?ReleaseID=32061 http://www.Microsoft.com/Downloads/Release.asp?ReleaseID=32011 Web servers that are hosted by the University should also be fitted with a reverse proxy to secure incoming http connections and servers should be hardened against industry standard and information from http://www.Microsoft.com/security for hardening tools and documentation. A recommendation for the Snort IDS would be to ignore your outbound http traffic such as: " Snort -d -A fast -c Snort.conf not (src net xxx.xxx and dst port 80)" `Source: (FAQ,v 1.14 2002/03/25 15:20:50 chrisgreen)` University

SMB Name Wildcard	**Description:** According to http://archives.neohapsis.com/archives/Snort/2000-01/0222.html and http://www.sans.org/top20.htm Windows machines typically send these types of queries in normal operation, particularly when filesharing is active, to determine NetBIOS names when only IP addresses are known. This type of query, when originating from an external network, is usually a pre-attack probe to gather NetBIOS name table information such as workstation name, domain, and a list of currently logged in users. **Analysis:** Upon reviewing the log files, it appears that hosts in this case are requesting the NetBIOS information from the target hosts as part of the Windows file sharing protocol to obtain domain, user and host id. This would be considered normal. **Example of Detect taken from Snort:** 03/27-00:00:02.076277 [**] SMB Name Wildcard [**] 1.1.11.6:137 -> 1.1.152.14:137 03/27-00:00:37.799237 [**] SMB Name Wildcard [**] 1.1.11.6:137 -> 1.1.152.249:137 03/27-00:01:31.806186 [**] SMB Name Wildcard [**] 1.1.11.6:137 -> 1.1.152.10:137 **Recommendation:** UniversityThe University perimeter router should block The NetBIOS connection to any outside host as NetBIOS is not a secure protocol and can allow for global sharing over the Internet. This is typically done by having filtering rules to block port 137, 138 and 139.

Connect to 515 from inside	**Description:** This vulnerability pertains to the Unix/Linux hosts running unpatched LPRng software. According to http://www.cert.org/advisories/CA-2000-22.html and http://www.ciac.org/ciac/bulletins/l-025.shtml. This vulnerability may allow remote users to execute arbitrary code on vulnerable systems. In addition, the printing service may be disrupted or disabled entirely. **Analysis:** Upon analyzing the logs, it appears that this is only a case of internal host attempting to connect with internal host. We can only assume that this type of traffic is typical with printers for a University. Another indication that the vast amount of scans might lead to a false positive lies with the nature of the connections, not only were these connections mostly internal but if this was an un-patched line printer server we would expect to see excessive port scans on destination port 515. We cannot see that evidence from our analysis "Top 10 Scan Log Talkers Destination IP" below. Another indication that this is probably normal traffic is the "many" to "few" relationship among alerts with this detect. This means that internally there are relatively many students sharing few print servers. This is something we expect in a University as there is definitely not a one-one relationship between University computers and print servers. We can correlate this scenario by observing Roland Lee's Feb 26 2002 "Analyse This" paper: Roland noted "As all of the sources were within the internal network, there is no sign of port probing on port 515 from outsiders." This confirms that this was also prevalent in another students hypothesis. We can also correlate this from our own analysis as the following alert had 76 unique source IP addresses but only 3 unique destination IP addresses 1.1.150.198, 1.1.1.63, and 1.1.150.114 **Example of Detect taken from Snort:** 03/27-16:03:27.440199 [**] connect to 515 from inside [**] 1.1.153.203:3934 -> 1.1.150.198:515 03/27-16:03:27.440272 [**] connect to 515 from inside [**] 1.1.153.203:3934 -> 1.1.150.198:515 03/27-16:03:27.440642 [**] connect to 515 from inside [**] 1.1.153.203:3934 -> 1.1.150.198:515 **Recommendation:** All University computers connected to the Internetshould always be patched with the latest vendor patch. As well, it is good security practice to uninstall any services that are not required. Another good recommendation is to reconfigure Snort to ignore known traffic patterns such as the 3 principal line print servers (IP addresses 1.1.150.198, 1.1.1.63, and 1.1.150.114) in the University. This way anomalies of abnormal traffic with regards to connect to 515 from inside will be more noticeable and in all probability something to investigate as normal traffic pattern will be tuned out from the IDS.

SNMP public access	**Description:** SNMP is Simple Network Management Protocol a Server Client tool used to manage network devices. This protocol assists network administrator to manage network performance, locates any networking issue and problem. The alert is triggered when the content public is targeted to SNMP designated ports UDP Port 161. Numerous alerts have been issued by the various Security agencies. Some of them can be found in http://www.cert.org/advisories/CA-2002-03.html and http://www.sans.org/top20.htm#_Toc526136821 **Analysis:** Upon reviewing the log entries, majority of the SNMP access appeared to be internal traffic between hosts. This is considered to be normal as network administrators conduct network related maintenance i.e. querying the router for operational information as well as updating the router configuration. **Example of Detect taken from Snort:** 03/27-00:06:29.442323 [**] SNMP public access [**] 1.1.70.177:1080 -> 1.1.5.92:161 03/27-00:06:29.442600 [**] SNMP public access [**] 1.1.70.177:1080 -> 1.1.5.92:161 03/27-00:06:29.472064 [**] SNMP public access [**] 1.1.70.177:1080 -> 1.1.5.92:161 **Recommendation:** Any SNMP traffic from internal MY.NET hosts not authorized should be prohibited. As well, the border router should disallow any SNMP traffic. This will prevent malicious hackers from obtaining useful information about the network and the router.

ICMP Echo Request L3retriever Ping	**Description:** A legitimate security scanner tool called L3retriever triggers this alert. This alert pertains to some host installed with this tool attempting to send out pings to other hosts. **Analysis:** Unless the source is trusted, this tool can be used to profile host machines for vulnerabilities. What makes this attack signature suspicious can be inferred from information obtained from whitehats.com (http://www.whitehats.com/info/IDS311) Whitehats writes "This signature is based on the characteristic ping of the L3 Networks security scanner called "Retriever 1.5". These probes should be rare, since the software is usually restricted to limited IP address ranges. L3 has been absorbed into Symantec, so more information is available at http://www.symantec.com/ " Given the fact that we should not be seeing such a high alert count only amounts to one of two possible scenarios: either the days for which the five day logs were obtained happened to be days in which the University was doing a vulnerability assessment on University networks or the more probable reason is that this is a false positive and the L3retriever scans are similar signatures to what is found in the payload of communications between win2k domain controllers and workstations. The latter explanation seems more probable as we can correlate the Windows/SMB communications via the large number of SMB Wildcard Alerts detected as part of the top 10 alerts in this analysis. **Example of Detect taken from Snort:** 03/27-00:13:47.235684 [**] ICMP Echo Request L3retriever Ping [**] 1.1.152.21 -> 1.1.11.6 03/27-00:28:49.562357 [**] ICMP Echo Request L3retriever Ping [**] 1.1.152.21 -> 1.1.11.6 03/27-00:43:51.892094 [**] ICMP Echo Request L3retriever Ping [**] 1.1.152.21 -> 1.1.11.6 **Recommendation:** Due to the fact that this alert is a potential false positive that caused by communications between Win2k domain controllers and workstations, Snort rules should reconfigure to only report on alerts that are triggered by external to internal hosts or vice versa. Snort should be configured to ignore internal hosts communicating to internal hosts with this signature. In addition, if L3retriver scanner is being used at the University, its source IP addresses should be restricted and have the IP addresses of the network scanners exempted from the IDS. This will eliminate unwanted traffic and logs that the IDS will bitterly process.

INFO MSN IM Chat Data	**Description:** Clients using Instant Messaging Chat over port 80 trigger this alert. Microsoft hosts this service. **Analysis:** Upon reviewing the log files, it was noted that numerous hosts are actively engaging in this traffic. We can confirm the accuracy of this signature as the destination IP addresses according to ARIN corroborate this. **Search results for: 64.4.12.191** MS Hotmail (NETBLK-HOTMAIL) 1065 La Avenida Mountain View, CA 94043 US Netname: HOTMAIL Netblock: 64.4.0.0 - 64.4.63.255 Coordinator: Myers, Michael (MM520-ARIN) icon@HOTMAIL.COM 650-693-7072 Domain System inverse mapping provided by: NS1.HOTMAIL.COM 216.200.206.140 NS3.HOTMAIL.COM 209.185.130.68 NS2.HOTMAIL.COM 216.200.206.139 NS4.HOTMAIL.COM 64.4.29.24 Although this alert is accurate, it should be known that there have been buffer overflows reported with the use of Instant Messenger.). A widely publicized vulnerability has been released (CERT® Advisory CA-2002-13 Buffer Overflow in Microsoft's MSN Chat ActiveX Control) **Example of Detect taken from Snort:** 03/27-07:14:09.005667 [**] INFO MSN IM Chat data [**] 1.1.150.165:1717 -> 64.4.12.191:1863 03/27-07:14:28.392387 [**] INFO MSN IM Chat data [**] 1.1.150.165:1717 -> 64.4.12.191:1863 03/27-07:14:37.586149 [**] INFO MSN IM Chat data [**] 1.1.150.165:1717 -> 64.4.12.191:1863 **Recommendation:** The University should have a policy governing the use of this service. If the use of this service is not in conformance with the policy, any accessing of this service should then be blocked. However, if this service is allowed, any vulnerability related to this service should be patched on a timely basis. If Instant Messenger Internet services are against University code of conduct or information security policies, then it is recommended that these messenger services be blocked at the firewall and border routers by the IP addresses associated to MSN, AOL, Yahoo to block the majority of the popular IM sites.

ICMP Echo Request Nmap or HPING2	**Description:** Nmap and HPING2 are well-known port scanner. This is typically used for reconnaissance purposes. **Analysis:** This scanning would appear to be OS fingerprinting. Nmap, hping2 and other mapping tools send bogus TCP flag combinations to attempt OS discovery since different OS's IP stacks respond differently to various flag combinations. However, upon reviewing the log files. This traffic was directed to certain internal hosts port 0. **Example of Detect taken from Snort:** 03/28-15:03:09.200054 [**] ICMP Echo Request Nmap or HPING2 [**] 1.1.253.10 -> 1.1.5.79 03/28-15:03:15.284834 [**] ICMP Echo Request Nmap or HPING2 [**] 1.1.253.10 -> 1.1.5.83 03/28-15:03:15.285337 [**] ICMP Echo Request Nmap or HPING2 [**] 1.1.253.10 -> 1.1.5.85 **Recommendation:** The use of Nmap and other reconnaissance tools should be approved by the Network and Security departments within the University. For blocking external scans, various mechanisms are outlined in http://rr.sans.org/tools/labrea.php
INFO Outbound GNUTella Connect Request	**Description:** GNUTella is a peer-to-peer file-sharing program for audio, video and software. **Analysis:** There are systems within the University requesting for connection externally. No real security risk involved except this may consume network bandwidth. **Example of Detect taken from Snort:** 03/31-20:12:06.117817 [**] INFO Outbound GNUTella Connect request [**] 1.1.88.223:1118 -> 208.239.76.99:6346 03/31-20:12:09.335647 [**] INFO Outbound GNUTella Connect request [**] 1.1.88.223:1127 -> 198.82.88.153:6346 03/31-20:12:09.525803 [**] INFO Outbound GNUTella Connect request [**] 1.1.88.223:1129 -> 66.68.170.200:6346 **Recommendation:** A review whether this service is allowed should be performed. If this is not allowed based on the policy, the host/users should be warned and any further connection should be terminated.

High port 65535 udp – Possible Red Worm – Traffic	**Description:** Alert was generated to suspect that potential Red Worm, exploit was detected on the network. This alert can be found in : www.sans.org/y2k/adore.htm http://www.securityfocus.com/archive/75/174776 Detailed analysis can be found on Michael Reiter's practical http://www.sans.org/y2k/practical/Michael_Reiter_GCIH.zip. And http://www.redhat.com/support/alerts/Adore_worm.html **Analysis:** This worm scans Internet for Linux hosts for vulnerability in rpc-statd, Bind, LPRng, wu-ftpd. The detected traffic is not normal. The UDP port 65535 should not frequently appear in network traffic due to the fact that this high port is not associated with any known services. This may be a case where some attackers were probing the University systems for the ping backdoor or even have successfully connected to it. There is a caveat on the following analysis in that this vulnerability is approximately over 2 years old. The network administrators should not overreact and assume that this is a mass scan of the Adore Worm. As seen in the example below, traffic is mostly internal. If the worm were scanning from the Internet we would see more outside networks scanning internal hosts. The large amount of scans had all internally addressed IP addresses originating mostly from internal hosts. The fact that this is more of a general rule it is not specific or accurate to a specific vulnerability, the purpose of this rule is to flag high ephemeral ports that typically are not reserved for service ports that are mainly used <1024. **Example of Detect taken from Snort:** 03/27-09:48:34.629471 [**] High port 65535 udp - possible Red Worm - traffic [**] 1.1.6.48:65535 -> 1.1.152.180:65280 03/27-09:48:34.714801 [**] High port 65535 udp - possible Red Worm - traffic [**] 1.1.6.48:65535 -> 1.1.152.180:65535 03/27-10:22:44.728867 [**] High port 65535 udp - possible Red Worm - traffic [**] 1.1.6.48:65535 -> 1.1.153.150:65535 **Recommendation:** All internal Linux hosts should ensure that rpc-statd, Bind, LPRng, wu-ftpd are patched with the latest patch. A useful tool from Symantec can be downloaded for free for the scanning of this vulnerability. http://www.symantec.com/avcenter/venc/data/codered.removal.tool.html As the worm is old and typically should not be a reflection of the resurrection of an old worm, it still is prudent to always maintain the latest patches for University servers as well as reconfigure the Snort rule to only detect this signature from external networks destined for internal University hosts thereby eliminating network noise that is probably not relevant to the IDS administrator.

INFO Inbound GNUTella Connect Request	**Description:** GNUTella is a peer to peer file-sharing program for audio, video and software. **Analysis:** There are systems requesting for connection. This is a good indication that they may be system with GNUTella on the network. No real security risk involved except this may consume network bandwidth. **Example of Detect taken from Snort:** 03/31-20:13:18.540580 [**] INFO Inbound GNUTella Connect request [**] 213.122.54.48:2079 -> 1.1.88.223:6346 03/31-20:20:31.281755 [**] INFO Inbound GNUTella Connect request [**] 213.122.54.48:2344 -> 1.1.88.223:6346 03/31-20:21:30.122621 [**] INFO Inbound GNUTella Connect request [**] 213.122.54.48:2405 -> 1.1.88.223:6346 **Recommendation:** A review whether this service is allowed should be performed. If this is not allowed based on the policy, the host/users should be warned and any further connection should be terminated.

Note: MY.NET.X.X references have been changed to 1.1.X.X notation for data parsing.

Analysis:

Following is a summarized top ten talkers that triggered alert signature listed by source IP address and destination IP address. It was noted that five 1.1.153.X hosts were the sources of alert activity and represented 40.68 % of the total top ten activity. It is recommended that the Network or Security department to conduct an analysis to determine what was producing single packets to so many hosts and whether these packets were anomalous or represented threatening behaviour.

Top 10 Alert Log Talkers By Source IP

Rank	Total # Alerts	**Source IP**	# Signatures triggered	Destinations involved
rank #1	20730 alerts	**1.1.153.197**	3 signatures	(70 destination IPs)
rank #2	19500 alerts	**1.1.70.177**	3 signatures	(33 destination IPs)
rank #3	14293 alerts	**1.1.11.6**	1 signatures	(46 destination IPs)
rank #4	7468 alerts	**1.1.11.7**	1 signatures	(40 destination IPs)
rank #5	7108 alerts	**1.1.153.203**	4 signatures	(56 destination IPs)
rank #6	5100 alerts	**1.1.153.119**	2 signatures	(4 destination IPs)
rank #7	4872 alerts	**1.1.150.198**	1 signatures	(103 destination IPs)
rank #8	4502 alerts	**1.1.152.19**	6 signatures	(51 destination IPs)
rank #9	4351 alerts	**1.1.153.118**	1 signatures	1.1.150.198
rank #10	3726 alerts	**1.1.153.115**	2 signatures	(59 destination IPs)

Top 10 Alert Log Talkers By Destination IP

Rank	Total # Alerts	**Destination IP**	# Signatures triggered	Originating sources
rank #1	44301 alerts	**1.1.150.198**	3 signatures	(72 source IPs)
rank #2	30604 alerts	**1.1.11.6**	3 signatures	(50 source IPs)
rank #3	16158 alerts	**1.1.11.7**	3 signatures	(45 source IPs)
rank #4	12636 alerts	**211.115.212.150**	1 signatures	1.1.153.197
rank #5	7364 alerts	**1.1.150.195**	7 signatures	(26 source IPs)
rank #6	3796 alerts	**1.1.5.248**	4 signatures	1.1.70.177, 1.1.253.10
rank #7	2959 alerts	**1.1.152.109**	1 signatures	(3 source IPs)
rank #8	2657 alerts	**1.1.5.137**	4 signatures	(3 source IPs)
rank #9	2646 alerts	**61.78.53.102**	1 signatures	1.1.153.115, 1.1.153.137
rank #10	2638 alerts	**1.1.5.143**	1 signatures	1.1.70.177

Analysis:

Following is the Top 10 source IP and port scanned. The Network or Security department should investigate to determine why such large amount of scan activity was performed by these two addresses 1.1.60.43 and 1.1.11.8 respectively.

Top 10 Scan Log Talkers By Source IP

Rank	**Source IP**	# of Ports Scanned	% of Ports Scanned
rank #1	**1.1.60.43**	363399	20.70932
rank #2	**1.1.11.8**	334259	19.04869
rank #3	**1.1.150.143**	198475	11.31066
rank #4	**1.1.150.113**	125524	7.153339
rank #5	**1.1.6.45**	27087	1.543629
rank #6	**1.1.6.50**	26352	1.501743
rank #7	**1.1.6.49**	25242	1.438486
rank #8	**1.1.6.48**	24013	1.368448
rank #9	**1.1.152.21**	22449	1.27932
rank #10	**1.1.6.52**	22096	1.259203

Top 10 Scan Log Talkers By Source Port

Rank	**Source Port**	# of Ports Scanned	% of Ports Scanned
rank #1	123	338272	19.27738
rank #2	1347	334368	19.0549
rank #3	1057	136381	7.772056
rank #4	1257	111058	6.328953
rank #5	7000	77629	4.423907
rank #6	7001	75392	4.296426
rank #7	137	53801	3.066002
rank #8	0	30458	1.735735
rank #9	28800	29162	1.661879
rank #10	6970	25483	1.452221

Analysis:

Following is the Top 10 destination host and ports scanned. They are all on the 1.1.X.X network segment. Most of the scanning occurred on the 1.1.152.X network segment. This warrants some analysis to be performed by the Network or Security department to determine the nature of the scan and the identify of the hosts so that defensive measures may be taken.

Top 10 Scan Log Talkers Destination IP

Rank	**Destination IP**	# of Ports Scanned	% of Ports Scanned
rank #1	1.1.1.3	38681	2.204346
rank #2	1.1.11.6	28787	1.640508
rank #3	1.1.1.4	20196	1.150926
rank #4	1.1.153.46	18234	1.039116
rank #5	1.1.152.20	16502	0.940413
rank #6	1.1.152.12	16327	0.93044
rank #7	1.1.152.249	16065	0.915509
rank #8	1.1.152.162	16022	0.913059
rank #9	1.1.152.16	16000	0.911805
rank #10	1.1.152.18	15992	0.911349

B) Top 10 Scan Log Talkers Destination Port

Rank	**Destination Port**	# of Ports Scanned	% of Ports Scanned
rank #1	1346	334452	19.05969
rank #2	4665	238274	13.57872
rank #3	80	138179	7.87452
rank #4	7001	77593	4.421856
rank #5	53	60289	3.435739
rank #6	7000	54085	3.082186
rank #7	137	45088	2.569467
rank #8	28800	27006	1.539013
rank #9	0	25073	1.428856
rank #10	6346	23723	1.351922

Analysis:

Following is the Out-of-Specification with the RFC compliancy. Snort detected these packets as they do not meet IP specification that is required by RFC. These packets could be crafted to generate undesired behaviour on the target host. Other reasons for these Out-of Specification packet could be because of packet crafting to evade firewalls and ids's as well as signatures for denial of service tools or attacks.

Top 10 OOS Log Talkers By Source IP

Rank	Total Count	**Source IP**	Destination IP
rank #1	29	**80.133.124.114**	1.1.150.113
rank #2	4	**213.169.245.41**	1.1.152.21
rank #3	2	**128.97.84.53**	1.1.153.210
rank #4	1	**0.192.5.106**	1.1.153.191
rank #5	1	**140.110.30.59**	1.1.150.220
rank #6	1	**212.242.58.14**	1.1.150.226
rank #7	1	**213.132.137.149**	1.1.150.113
rank #8	1	**217.82.123.75**	1.1.152.21
rank #9	1	**61.216.83.124**	1.1.150.220
rank #10	1	**80.144.189.160**	1.1.153.196

Investigative Hosts and Why

Host 1: Rank #1 from the Out of Specifications file. 80.133.124.114 is chosen because it repeated out of spec packets 29 times for a single host.

The site that it came from was

Search results for: 80.133.124.114

```
European Regional Internet Registry/RIPE NCC (NET-80-RIPE)
   These addresses have been further assigned
   to European users. Contact information can
   be found in the RIPE database at whois.ripe.net
   NL

   Netname: 80-RIPE
   Netblock: 80.0.0.0 - 80.255.255.255
   Maintainer: RIPE

   Coordinator:
      Reseaux IP European Network Co-ordination Centre Singel
```

```
258   (RIPE-NCC-ARIN)   nicdb@RIPE.NET
      +31 20 535 4444
```

Because packets were Out of Spec, this is a red flag as the activity cannot be mistaken as intentional or normal traffic

Host 2: Rank #2 from the OOS packets repeated 4 times from host 213.169.245.41. For nearly the same reasons as host number one, this host should be investigated.

The site that it came from was

Search results for: 213.169.245.41

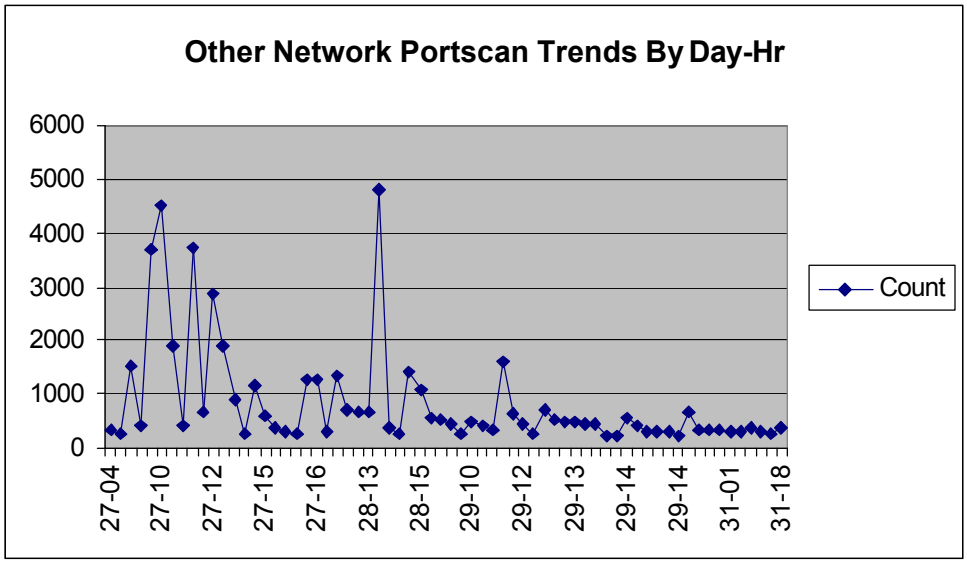
```
European Regional Internet Registry/RIPE NCC (NETBLK-213-RIPE)
   These addresses have been further assigned to European
users.
   Contact info can be found in the RIPE database, via the
   WHOIS and TELNET servers at whois.ripe.net, and at
   http://www.ripe.net/perl/whois/
   NL

   Netname: RIPE-213
   Netblock: 213.0.0.0 - 213.255.255.255
   Maintainer: RIPE

   Coordinator:
      Reseaux IP European Network Co-ordination Centre Singel
258   (RIPE-NCC-ARIN)   nicdb@RIPE.NET
      +31 20 535 4444
```

Host 3: Rank #1 for scan log takers 1.1.1.3. This host was chosen because it was scanned 38 thousand times over a 5-day period. This host may be a source of a target as we need to investigate if that pattern of usage is normal given the service it is providing. It definitely raises a flag as the next ranked talker in the category does not have such a high-scanned ports.

Host 4: A potential compromised host could be found from 1.1.153.197 an internal address which was the originating source address to a destination IP 211.115.212.150. This is suspicious as it logged 12 thousand alerts from one signature. This was the spp_http_decode: IIS Unicode attack detected. It is highly probable that this host is compromised or being probed by the same host (211.115.212.150) repeatedly.

Host 5: The 5th host that was chosen to be investigated was an internal source triggering ICMP Echo L3retreiver Pings. This host is 1.1.152.161 and it triggered the most 834 alerts and 1723 signatures. Because L3retriever is a scanner tool, we must ensure that this host is authorized as in the wrong hands these automated scanner are capable to profiling the weaknesses of a network from a hacker quite easily and with minimum knowledge to exploit discovered vulnerabilities.

Network Portscan Trend by Day and Hour



The graph above represents the pattern of other non-University initiated traffic scanning the University. The link graph represents that reconnaissance patterns actually reflect typical peak University network usage. One indicator is that frequency of scan patterns drop significantly on the 29th of March as this is a Friday and most users are not at the University. Peak scan times seem to occur during morning and noon periods when overall network traffic is at its highest. This is odd as one might hypothesise that other network scans would be greatest during weekends and off-peak hours. This is typically the best time to perform reconnaissance when administrators are not actively attending logs and less people are around to notice.

Analysis Process (Methodology)

The approach taken to perform the analysis was not innovative as the best solutions to analyze the situation had been already performed by previous students. Particularly Angela D. Orebaugh GIAC December 2001 was used to analyze large scan files under Windows. For Alerts.gz files. Snort Snarf was used www.silicondefense.com to parse and correlate the data for all 5 days of alert logs. This tool uses Perl and php to sort and parse Snort alert log files. As well it automatically ignored the scan files embedded in the alert files so data massaging of the alert file was unnecessary. For Scans.gz files a series of files were concatenated and imported to an Access Database. As these files used 2 delimeters : and tabs it was necessary to import and export the file twice to include all fields. Info from Access was then built on queries to do statistical analysis. Typically SQL queries were built using simple "group by" and "count" to get the top ten reports of the files. Oos.gz files only had info for 2 days. This was achieved using excel spreadsheet. Data from the oos files was easy as they were extremely small and easily manipulated in a spreadsheet.