Global Information Assurance Certification Paper

SANS GIAC

GCIA Practical

Version 3.0

SANS FIRE Washington DC,

July 30 – August 4, 2001

Edward T. Peck, CISSP

Table of Contents

Assignment 1 – Describe the State of Intrusion Detection

Introduction

While Cisco Systems is the recognized market leader in networking devices, Cisco also produces a line of Intrusion Detection designed for the enterprise. The Cisco Intrusion Detection System (IDS), formerly known as Cisco NetRanger, consists of a collection of Network IDS (NIDS), Host IDS (HIDS), along with a director console for remote administration. The remote management console is also the tool used to manage other Cisco network devices like the PIX Firewall, routers, switches and Virtual Private Networks (VPN's). This central management console allows the security administrator to configure and administer the entire network security posture through one interface.

Network-based Intrusion Detection System (NIDS)

As with most IDS', Cisco's Secure IDS is designed to detect and react to possible malicious activity throughout a specified network. What differentiates Cisco's product from the rest of the market is its ability to drop existing connections that are deemed malicious in intent. By using pre-defined criteria, the Cisco Secure IDS will determine if certain network traffic is unauthorized and potentially dangerous. The Secure IDS can modify the Access Control Lists (ACL's) of Cisco routers and effectively "shun" the attackers address from reaching the protected network. This "shunning" can last indefinitely or can only be temporary. The advantage here is to ensure normal and authorized network traffic keep flowing while protecting critical network assets.

The Cisco Secure IDS comes in three flavors; the low-end IDS-4210 appliance, the high-end IDS-4230 appliance, and the IDS module that physically inserts into a Cisco Catalyst 6000 switch. The IDS-4210 and the IDS-4230 are modeled after the traditional IDS, which is a separate platform placed onto a network and listens to traffic passing in and out of that monitored network. Cisco recommends these two appliances to be connected to the Switched Port Analyzer (SPAN) port on a Cisco switch. By utilizing the SPAN port, the IDS sensor will be able to monitor all switched packets, vice only the packets destined for the monitored network segment. When deciding which of these two products to purchase one should consider the bandwidth of the network to be monitored. The IDS-4210 is ideal for the 45-Mbps environment and works splendidly on multiple T1/E1, T3 and Ethernet networks. However, if monitoring is needed on a 100-Mbps, Fast Ethernet, or multiple T3 networks, the IDS-4230 is specifically designed to handle the traffic load.

The Catalyst 6000 IDS Module is actually a blade that inserts into the Catalyst 6000 Switch and monitors all traffic passing throughout the switched network. This is an ideal solution for the enterprise that has limited rack space at their disposal. Another beneficial feature of the Catalyst 6000 IDS Module is the ability to monitor network traffic passing through multiple Virtual Local Area Networks (VLAN's). The module does not interfere

with the switch performance while providing all the capabilities of a traditional IDS appliance.

Host-based Intrusion Detection System (HIDS)

Cisco recently started to market a host-based solution to network security through their IDS Host Sensor, which is powered by Entercept. The HIDS is designed to detect misuse or attacks on an individual host, vice anomalous network traffic that a NIDS detects. A well-known shortcoming of a NIDS is that exploits sometimes act differently on the intended host than they do on the NIDS, thus providing either a False Positive Alert or more alarming, a False Negative. If the NIDS reconstructs a packet is it deems it as harmless, no alert is sent; however, once that packet reaches the intended host, an entirely different result occurs.

Generally, a HIDS monitors system/audit logs, application logs, process/kernel and file integrity. Cisco's IDS Host Sensor can actually protect the host by monitoring and evaluating requests to the operating system and the application-programming interface (API) before they are processed. The Cisco IDS Host Sensor comes in two different flavors, the Standard Edition and the Web Edition.

The Standard Edition of the Cisco IDS Host Sensor is installed in concurrence with the Operating System or kernel and is therefore able to seize and validate incoming OS requests. Potentially harmful requests will be rejected while valid and authorized requests will be allowed. The IDS Host Sensor determines if an action is dangerous by comparing it to a constantly updated attack signature database that identifies both well-known attacks and typical malicious behavior. The attack signature database is divided into three categories:

- **Individual attack** – matches known attack signatures against the software request to the OS or kernel. These are typically lone exploits against a well-known vulnerability.

- **Generic attack** – guards against a general class of well-known attacks by identifying typical traits. A good example is Buffer Overflow Exploits.

- **Resource protection –** guards against unauthorized access to critical system resources such as registry keys, password files, services, etc.

A policy database is incorporated into the product, which allows administrators to customize how the HIDS should behave. This database can be administered through a central management console, but each agent is able to function separate from the console. The advantage here being the absence of a communication port being utilized, thus limiting the security exposure of that host. Each agent "pulls" signature updates and policy changes from the management console and is encrypted with Triple DES encryption.

The Web Application Edition addresses the unique challenges that are inherent in an enterprises web server. The Web Application Edition is essentially an add-on to the Standard Edition; therefore, the web server has its Operating System/kernel and API is protected as well as by monitoring requests to the web application. Cisco attains this by essentially placing a "shield" around the server and utilizes HTTP protection. These two functions are described as such:

- **Shielding** – specifically designed for Microsoft Internet Information Server (IIS), Apache, or iPlanet web servers. The process starts with a discovery of the server's configuration. Cisco calls this "adaptive auditing." Next, the shield provides a protective shell surrounding the server's resources and application processes. This saves the server from penetration and misuse, such as web page defacements.

- **HTTP protection** – addresses vulnerabilities inherent in HTTP requests to Microsoft Internet Information Server (IIS), Apache, or iPlanet. This is achieved by examining the HTTP data stream, tags the malicious requests, and blocks them from executing on the targeted web server. This is effective in preventing the more prevalent attacks, such as directory traversal. Cisco cites that HTTP protection is able to detect malicious activity even if application-level encryption such as SSL is used. However, Cisco warns, "full application protection is only achieved in conjunction with other Cisco defense methodologies."

Cisco Secure IDS Director

The Cisco Secure IDS Director is a central management system that monitors the activity of multiple Cisco Secure IDS sensors. It displays a GUI-based geographical display of each sensor and by using color schemes; each sensor can be displayed with a severity of activity. By using HP OpenView's Network Node Management (NNM) user interface, each alarm is displayed as an icon. This icon can be selected and a view of what triggered the alarm on the sensor, as well as source, destination, type and date/time. All of the critical data can be logged into an adjacent database for later analysis. Other uses of the database include attack correlation, plotting of long-term malicious activity, and metrics for management reporting.

Other features included in the Cisco Secure IDS Director include:

- **Centralized Configuration Management** – the Director can standardize the rules base for all subordinate sensors, or the Director can create a customized set of rules for each individual sensor. The administrator can even create multiple configuration versions on one sensor with the capability of activating them for different times of the days (normal business hours and after hours). This also comes in handy when an administrator makes a configuration change that is erroneous. The administrator can then roll back to a previous version, one that is known to be in correct. Since a copy of the configuration is saved on the Director, when a sensor is replaced, the correct configuration can be quickly and

easily restored.

- **E-mail Notification and Script Execution** – this function enables alarm notification through e-mail or dialing a pager number. The scripts execution deals with if the sensor performs any active response to the attack. An example is to modify the router's ACL to shun the offending host from communicating with the protected network.

- **Network Security Database** – this database houses explanations for all the alarms the sensor forwards to the Director. It also contains links, countermeasure recommendations, related vulnerabilities, and possible conditions that could cause a false alarm.

Conclusion

There are some shortcomings of the Cisco Secure IDS. The many varied features of the Secure IDS come at a price. This is not a turnkey operation, but requires some knowledge and other specialized skill. For example, the Secure IDS can be managed by either using the IDS Director running under HP OpenView, or using the standalone Cisco Security Policy Manager (CSPM) IDS (known as "CSPM-I"). Utilizing the CSPM can be tricky and requires patience. Customizing signatures are also more difficult than some of the Secure IDS competitors. Another shortcoming is the lack of reporting capabilities. The information provided is fundamental at best. However, by the nature of working seamlessly with other Cisco products, the benefits far outweigh the shortcomings.

The Cisco Secure IDS suite of products is all part of what Cisco terms its "SAFE Blueprint." This concept helps enterprises determine which security solutions should be used in its network through "modules" that simplify security design, rollout, and management. Each module contains part of Cisco's networking devices that may include VPNs, firewalls, encryption, and of course, intrusion detection.

List of References

1. "Cisco Intrusion Detection." URL: http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml (1 Oct. 2001)

2. "Cisco Secure IDS (Formerly NetRanger)." 18 Sep 2001. URL: http://www.cisco.com/univercd/cc/td/doc/pcat/nerg.htm (1 Oct. 2001)

3. "Data Sheet Cisco IDS Host Sensor, Standard Edition." 16 Aug 2001. URL: http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/sddi_ds.htm (2 Oct 2001).

4. "Data Sheet Cisco IDS Host Sensor, Web Application Protection." 4 Sep 2001. URL: http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/wdsi_ds.htm (2 Oct 2001)

5. Shipley, Greg and Patrick Mueller. "Dragon Claws its Way to the Top." 20 Aug 2001. URL: http://www.networkcomputing.com/1217/1217f2.html (2 Oct 2001)

6. Kaeo, Merike. Designing Network Security. Indianapolis: Cisco Press, 1999. 250-251.

Assignment 2 – Network Detects

Network Detect 1

Aug 19 15:13:38 212.156.76.97:2700 ->128.148.19.4:44767 UDP
Aug 19 15:13:38 212.156.76.97:2702 ->128.148.19.6:44767 UDP
Aug 19 15:13:38 212.156.76.97:2709 ->128.148.19.13:44767 UDP
Aug 19 15:13:38 212.156.76.97:2706 ->128.148.19.10:44767 UDP
Aug 19 15:13:38 212.156.76.97:2713 ->128.148.19.17:44767 UDP
Aug 19 15:13:38 212.156.76.97:2715 ->128.148.19.19:44767 UDP
Aug 19 15:13:38 212.156.76.97:2722 ->128.148.19.26:44767 UDP
Aug 19 15:13:38 212.156.76.97:2724 ->128.148.19.28:44767 UDP
Aug 19 15:13:38 212.156.76.97:2726 ->128.148.19.30:44767 UDP
Aug 19 15:13:38 212.156.76.97:2727 ->128.148.19.31:44767 UDP
Aug 19 15:13:38 212.156.76.97:2731 ->128.148.19.35:44767 UDP
Aug 19 15:13:38 212.156.76.97:2733 ->128.148.19.37:44767 UDP
Aug 19 15:13:38 212.156.76.97:2732 ->128.148.19.36:44767 UDP
Aug 19 15:13:38 212.156.76.97:2735 ->128.148.19.39:44767 UDP
Aug 19 15:13:38 212.156.76.97:2736 ->128.148.19.40:44767 UDP
Aug 19 15:13:38 212.156.76.97:2738 ->128.148.19.42:44767 UDP
Aug 19 15:13:39 212.156.76.97:2937 ->128.148.19.240:44767 UDP
Aug 19 15:13:39 212.156.76.97:2940 ->128.148.19.243:44767 UDP
Aug 19 15:13:39 212.156.76.97:2942 ->128.148.19.245:44767 UDP
Aug 19 15:13:39 212.156.76.97:2950 ->128.148.19.253:44767 UDP

I searched for this port and found a few references to it on the incidents.org list from 2000, but nothing else. Anyone else seeing this?

Thanks,
Paul

1. Source of Trace

This trace was downloaded from http://www.incidents.org/archives/intrusions/msg01484.html and is from Paul Asadoorian

2. Type of Event Generator

This event was generated by TCPDump. The format is as follows:

DATE TIME Source IP:Port Destination IP:Port Protocol

3. Probability the Source Address was Spoofed

The source address is in all likelihood not spoofed. I utilized ARIN to determine who owns 212.156.76.97, turns out is was allocated to RIPE (who is essentially Europe's version of ARIN). After doing a whois on RIPE's database, the address has been issued to Turk Telekom and is part of the Turkish National Backbone.

```
inetnum:        212.156.0.0 - 212.156.193.255
netname:        TTNET
descr:          Turk Telekom TTnet national backbone
country:        TR
admin-c:        TTBA1-RIPE
tech-c:         TTBA1-RIPE
status:         ASSIGNED PA
mnt-by:         AS9121-MNT
changed:        hostmaster@ripe.net 19990908
changed:        ipg@telekom.gov.tr 19991216
changed:        ipg@telekom.gov.tr 20000609
source:         RIPE
```

While it is unlikely that the Turkish government is performing the scan, a more likely scenario is that 212.156.76.97 has been compromised and the attacker is logging the response to the scan. This is not a 3rd Party (or collateral damage) since the destination has incrementing host id's.

4. Description of the Attack

This is a reconnaissance of some sort. I could not find any reference to what port 44767 is used for. The attacker is targeting hosts located on the 128.148.19.0 network, but there seems to be no pattern to the host id's chosen besides being incremental. It also looks to be launched through a script due to the time stamp indicating the scan was done within a 1 second time frame. This can also be verified by the close sequence of source ports.

5. Attack Mechanism

This looks like an attacker is trying to find hosts infected with a particular trojan. The attacker is looking for a response to his initiated request. My best guess as to why someone would want to probe port 44767 is that someone is looking for a Trojan listening to port 44767 and will respond to the UDP probe. It is unclear whether this is a previously unknown Trojan or if it's a well-known Trojan that has been modified to listen on a port other than its default. The close timing of each successive probes indicates that this was script based.

6. Correlation

Paul Asadoorian stated he found a few references of port 44767 on the incidents.org list from 2000. I also found a references to this type of activity on the Security Focus web site at:
http://:www.securityfocus.com/archive/75/62183
http://:www.securityfocus.com/archive/75/178630

7. Evidence of Active Targeting

This is a case of targeting, but not of active targeting. While the 128.148.19 network was probed, this looks like a script is targeting a vast quantity of address looking for responses

8. Severity

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

Criticality = 3
Seems to be a shotgun effect (looking for any response) and not specifically targeting critical servers. Since I'm unsure of which hosts responded, I chose three.

Lethality = 2
Reconnaissance scan. I'm a little worried because I do not know why port 44767 was chosen.

System Countermeasures = 3
Again, I'm unsure of the attackers intent. If this is a new Trojan, the system is more than likely not patched. Fortunately, I did not see any response.

Network Countermeasures = 3
I'm unsure of the network configuration. I assume this was blocked at the firewall, but I do not know if there is more than one entryway into the network.

9. Severity = -1
Seems harmless, but should watched closely.

10. Defensive Recommendations

My defensive recommendations are to scan internal hosts to try and locate any possible compromise via UDP port 44767. I would also recommend all outbound traffic originating from port 44767 at the firewall or perimeter router.

11. Multiple Choice Question

What would be the expected response from the host if it were not listening to port 44767?
Aug 19 15:13:39 212.156.76.97:2950 ->128.148.19.253:44767 UDP

a. SYN/ACK
b. RST/ACK
c. ICMP Host Unreachable
d. ICMP Port Unreachable

Answer: d

Network Detect 2

Aug 20 01:55:51 hosth snort: DNS named version attempt [Classification: Attempted Information Leak Priority: 3]: 203.117.101.194:1570 -> a.b.f.104:53

1. Source of Trace

This trace was downloaded from http://www.incidents.org/archives/intrusions/msg01493.html and is from Laurie Zirkle.

2. Type of Event Generator

Snort IDS generated this alert in the Syslog format.

3. Probability the Source Address was Spoofed

The source address is in all likelihood not spoofed. I utilized ARIN to determine who owns 203.117.101.194, turns out is was allocated to APNIC (who is essentially Asia's version of ARIN). After doing a whois on APNIC's database, the address has been issued to Davidcan.com Pte Ltd., a Wireless Application Developer.

Search results for '203.117.101.194'

inetnum	203.117.101.192 - 203.117.101.223
netname	DAVIDCAN-SG
descr	Davidcan.com Pte Ltd
country	SG
admin-c	KC9-AP, inverse
tech-c	KE2-AP, inverse
notify	ipaddradmin@cyberway.com.sg, inverse
mnt-by	MAINT-AS4657-AP, inverse
changed	ipaddradmin@cyberway.com.sg 20000529
source	APNIC

The goal of this probe was to elicit a response (BIND version) and therefore would not use a spoofed address.

4. Description of the Attack

This is a reconnaissance probe with the intent of gaining the version of BIND running on a DNS server.

5. Attack Mechanism

The following attack description was taken from the Network ICE web site: "The BIND DNS server has a feature whereby its database contains a CHAOS/TXT record with the name "VERSION.BIND". If somebody queries this record, the version of the BIND software will be returned. This event triggers whenever anybody does such a lookup. This is not an attack itself, but a simple reconnaissance scan."

6. Correlations

I would have like to have viewed the syslog of the targeted host to see the response to this probe. I used the following web sites as resources in researching this reconnaissance probe:
http://:www.whitehats.com/info/IDS278
http://advice.networkice.com/Advice/Intrusions/2000417/default.htm

7. Evidence of Active Targeting

Since there was no other detects of hosts targeted on the a.b.f network, I'm assuming that this was indeed active targeting. The probe was focused on one individual host on this particular network. If this host is indeed a DNS server, this also indicates previous mapping by the attacker, who was looking for DNS servers.

8. Severity

*Assumption is that the **a.b.f.104** host is a DNS Server

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

Criticality = 5
Aimed at a DNS server.

Lethality = 2
This particular probe is information gathering only.

System Countermeasures = 5
Since a response is not shown I'll assume the DNS server did not respond to this probe, thus preventing the attacker from gaining the BIND version.

Network Countermeasures = 3
Typically the DNS server is outside of an organizations firewall. The main network defenses for a DMZ server are the routers and IDS. Snort, an IDS, detected this probe.

Severity = -1

9. Defensive Recommendation

I would like to review the entire snort log file to determine if the targeted host did indeed reply. I would also recommend verifying the version of BIND and ensuring it has been strengthened with the latest security patches. Lastly, I would watch closely any incoming requests from 203.117.101.194. If this was indeed a reconnaissance probe, further malicious activity could reasonably be expected.

10. Multiple Choice Test Question

In the trace provided, what was the IP protocol used to deliver this probe?

Aug 20 01:55:51 hosth snort: DNS named version attempt [Classification: Attempted Information Leak Priority: 3]: 203.117.101.194:1570 -> a.b.f.104:53

a. TCP
b. UDP
c. ICMP
d. DNS

Answer: b

Network Detect 3

209.125.59.114 - - [21/Aug/2001:06:20:40 -0400] "GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3
%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u90
90%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0"
400 289

1. **Source of Trace**

   This trace was downloaded from
   http://www.incidents.org/archives/intrusions/msg01500.html and is from Laurie
   Zirkle.

2. **Type of Event Generator**

   This is a sample from an Apache access log.

3. **Probability the Source Address was Spoofed**

   The source address is in all probability not spoofed. This looks to have occurred in the middle of a TCP session. A TCP session starts with a three-way handshake between two hosts, with each part of the handshake expecting a response from the targeted host.

4. **Description of the Attack**

   This attack targets TCP port 80 HTTP, and then attempts to exploit a known vulnerability in Microsoft IIS servers. The Cert Incident Note IN-2001-09 "Code Re II:" Another Worm Exploiting Buffer Overflow in IIS Indexing Service DLL describes this attack and how it differs form the original Code Red Worm as described in CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL.

5. **Attack Mechanism**

   According to CERT Incident Note IN-2001-09: "The Code Red II worm attempts to connect to TCP port 80 on a randomly chosen hosts assuming that a web server will be found. Upon a successful connection to port 80, the attacking host sends out a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Indexing Service described in CERT advisory CA-2001-13." Due to the self-

propagating nature of the worm, similar HTTP GET requests are sent to other randomly chosen hosts. If successful, the worm will check to see if the host has been previously infected; checks the default system language and spawns threads for propagation; copies %SYSTEM%\CMD.EXE to root.exe in the IIS scripts and msadc folders; and finally creates a Trojan horse copy of explorer.exe and copies it to C:\and D:\. The Trojan explorer.exe calls the legit explorer.exe to mask its existence, and creates a virtual mapping which exposes the C: and D: drives.

6. Correlations

The above signature string exactly matches the System Footprint in CERT Incident Note IN-2001-09.

7. Evidence of Active Targeting

There is evidence of targeting (the worm tried to infect this host); however, due to the nature of the worm, this was a randomly targeted victim.

8. Severity

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

Criticality = 3
Aimed at a web server.

Lethality = 4
If successful, the server will be defaced or could even launch a denial of service attack.

System Countermeasures = 5
This worm only exploits Microsoft IIS servers, the victim was a Unix server running Apache.

Network Countermeasures = 1
The worm was able to query the Apache server, so none of the network devices stopped or triggered the incoming activity

Severity = 1
Code Red II affects Microsoft IIS, this site was running Apache. No need to worry but would probably notify the attacking host's organization regarding their infection.

9. Defensive Recommendations

This server is not vulnerable since Code Red does not affect to Apache servers. If the organization owns Windows-based servers, I recommend ensuring that the servers have the latest security patches loaded. As an added precaution, I would suggest monitoring all outbound traffic to detect any possible internal infection.

10. Multiple Choice Test Question

What is an HTTP 400 message?

a. Bad Request
b. Not Found
c. OK
d. Bad Gateway

Answer: a

Network Detect 4

inetnum: 202.85.160.0 - 202.85.191.255
netname: IADVANTAGE
descr: iAdvantage Limited
country: HK

Aug 21 07:05:09 hostdr portsentry[353]: [ID 702911 daemon.notice] attackalert: Connect from host: 202.85.172.112/202.85.172.112 to TCP port: 514
Aug 21 07:05:09 hostst portsentry[5747]: [ID 702911 daemon.notice] attackalert: Connect from host: 202.85.172.112/202.85.172.112 to TCP port: 513
Aug 21 07:05:10 hosts telnetd[25478]: refused connect from 202.85.172.112
Aug 21 07:05:12 hostba portsentry[585]: [ID 702911 daemon.notice] attackalert: Connect from host: 202.85.172.112/202.85.172.112 to TCP port: 514
Aug 21 07:05:12 hostl portsentry[11156]: [ID 702911 daemon.notice] attackalert: Connect from host: 202.85.172.112/202.85.172.112 to TCP port: 513
Aug 21 07:05:25 hostko /kernel: Connection attempt to TCP z.y.w.21:515 from 202.85.172.112:4131
Aug 21 07:07:03 hostmau portsentry[223]: attackalert: Connect from host: 202.85.172.112/202.85.172.112 to TCP port: 513
Aug 21 07:07:03 hostmau snort: connect to 515 from outside: 202.85.172.112:4122 -> z.y.w.12:515
Aug 21 07:07:03 hostmau snort: connect to 515 from outside: 202.85.172.112:4122 -> z.y.w.12:515
Aug 21 07:07:03 hostmau snort: connect to 515 from outside: 202.85.172.112:4122 -> z.y.w.12:515
Aug 21 07:07:05 hostmau snort: connect to 515 from outside: 202.85.172.112:4122 -> z.y.w.12:515

1. Source of Trace

This trace was downloaded from http://www.incidents.org/archives/intrusions/msg01500.html and is from Laurie Zirkle.

2. Type of Event Generator

This is a sample from an UNIX message log that includes PortSentry and Snort alerts. It also appears to be a syslog server collecting syslogs from various servers.

The PortSentry format is as follows:

Date/Time	Target Host	Process	Process ID (PID)	Alert	Source Host (Reverse Lookup / IP Address)	Protocol	Port
Aug 21 07:05:09	hostdr	portsentry	353	attackalert	202.85.172.112/202.85.172.112	TCP	514

[ID 702911 daemon.notice] appears to be the process collecting the alerts.

The Snort format is as follows:

Date/Time	Target Host	Alert	Source Host:Port	Destination Host:Port
Aug 21 07:07:03	hostmau	Connect to 515 from outside	208.85.172.112.4122	z.y.w.12:515

3. Probability the Source Address was Spoofed

The source address is likely not spoofed. By trying to connect to ports 513 and 514 (BSD rlogin and rshd) the attacker is trying to gain unauthorized access. By spoofing the source address, the attacker will never know if access was gained or not. The likely scenario is that the intruder is originating their attack from a compromised server.

4. Description of the Attack

The attacker seems to be trying to gain access to seven different UNIX hosts. The following table displays how each host was attacked:

Host	**Port / Service**
Hostdr	514 – rshd (Remote Shell Daemon)
Hostst	513 – rlogin (Remote Login)
Hosts	23 – Telnet
Hostba	514 – rshd
Hostl	513 – rlogin
Hostko	515 – lpd (Print Spooler)
Hostmau	513 – rlogin
z.y.w.12	515 - lpd

The attack lasted just under two minutes, which would lead to a script-based attack; however, there is no discernable pattern since seven different hosts were targeted at different ports. The likely solution would be an attacker, who has already performed some sort of reconnaissance, inserted the targeted IP addresses into a homegrown script. The connections all looked like attempts to gain unauthorized access.

This could also be an attempt for scanning a network looking for live hosts and possibly performing OS fingerprinting; however, this is a rather "noisy" way of performing this and there are easier and stealthier ways of obtaining this information.

5. Attack Mechanism

The rshd, rlogin, and telnet attempts were designed to gain access. Whether or not the attacker had previously obtained userids and passwords are unknown. Obviously some sort of reconnaissance was performed since the attacker is specifically targeting ports on individual hosts. The lpd probe could be an attempt to exploit a third party product to the generic lpd program shipped with most versions of Unix called LPDng. An unpatched version of LPDng will allow an attacker to execute code through a buffer overflow condition.

6. Correlations

It would have been interesting to see their reconnaissance efforts of this attacker and to see what userid they used while trying to gain access. The configurations of the targets would need to be known to determine if the targeted ports are active. I used the following web sites to research this detect:
http://:www.whitehats.com/info/IDS456
http://:www.whitehats.com/info/IDS457
http://:www.cert.org/advisories/CA-2000-22.html
http://:www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0917

7. Evidence of Active Targeting

There is evidence of active targeting since specific ports were probed on individual hosts. Since the attacker has targeted specific hosts with specific ports, it can be reasonably assumed that the attacker performed some previous reconnaissance on the victims network. The attacker knew which hosts he/she wanted to probe and which hosts were UNIX based to try to exploit the LPDng program.

8. Severity

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

Criticality = 3
Unknown what type of hosts were targeted. What is known is that the operating system is some flavor of UNIX. I'm assuming the targets were UNIX servers.

Lethality = 5
If successful, the attacker gains access (root access is trivial once access is granted) or in the case of the lpd probe, possible buffer overflow code execution.

System Countermeasures = 3
Host "hosts" refused a telnet connection; however, it's unknown if the other hosts disallowed the connection attempts.

Network Countermeasures = 2
The attackers activity was reported by the individual hosts syslog, therefore all these probes bypassed whatever network countermeasures were in place. The lone exception is the Snort sensor, but this is an alert, not a prevention measure.

Severity = 3

9. Defensive Recommendations

If the organization does indeed have UNIX based hosts that utilize the LPDng program have the latest security and system patches applied. As an added precaution, I would also load all applicable security and system patches, concentrating primarily on the targeted hosts, and then proceed to other corporate assets. If feasible, I would also configure the IDS' to monitor all activity from source host 202.85.172.112.

10. Multiple Choice Test Question

Why is the source IP address listed twice?

Aug 21 07:05:09 hostdr portsentry[353]: [ID 702911 daemon.notice] attackalert: Connect from host: 202.85.172.112/202.85.172.112 to TCP port: 514

a. Two hosts are attacking at the same time
b. Address is spoofed
c. Unable to perform DNS resolution
d. Source routing

Answer: c

Network Detect 5

Aug 25 15:33:16 hosth /kernel: Connection attempt to TCP a.b.c.62:27374 from 65.92.93.219:2027

Aug 25 15:33:17 hosth /kernel: Connection attempt to TCP a.b.c.62:27374 from 65.92.93.219:2027

1. Source of Trace

This trace was downloaded from http://www.incidents.org/archives/intrusions/msg01523.html and is from Laurie Zirkle.

2. Type of Event Generator

This is a sample from an UNIX message log.

3. Probability the Source Address was Spoofed

The source address is likely not spoofed. This is the beginning of a three-way handshake to establish a TCP connection. The source host is needs a response to continue in establishing a session. This scan looking for hosts infected with the SubSeven Trojan.

4. Description of the Attack

The SubSeven Trojan infects Windows-based systems. This is a scan looking for hosts that are acting as SubSevenServers (S7S), which by default listen on port 27374. Once a connection is established, the remote client then has control of the server and can perform many malicious acts such as modifying the registry, uploading files, stealing passwords or even sniffing the network.

This could also be a worm called Win32.Chainsaw, which attempts to connect to a S7S through port 27374. If successful, the S7S will upload a file named chainsaw.exe and then execute that executable to infect that machine with the Win32.Chainsaw worm.

5. Attack Mechanism

This is a Stimulus-Response attack, which means the attacker is sending a connection request (stimulus) and is awaiting a connection acknowledgement (response). If a response is received, the attacker then proceeds to access the victim workstation

6. Correlations

I used the following web sites for research of the SubSeven Trojan:
http://www.nipc.gov/warnings/advisories/2000/00-056.htm
http://ca.com/virusinfo/encyclopedia/descriptions/s/subseven.htm

I also found information regarding SubSeven in "Hacking Exposed, Second Edition", (pg. 127 & 128). Information regarding the Win32.Chainsaw worm was gained from:
http://ca.com/virusinfo/encyclopedia/descriptions/c/chainsaw.htm

7. Evidence of Active Targeting

There is evidence of active targeting since one specific host was targeted by port 27374.

8. Severity

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

SubSeven

Criticality = 3
Unknown what type of hosts were targeted. What is known is that the operating system is some flavor of UNIX. I'm assuming the targets were UNIX servers.

Lethality = 5
If successful, the attacker gains unauthorized system access.

System Countermeasures = 5
This is a Unix-based system (the trace was from a Unix Message Log) and is not susceptible to the SubSeven Trojan. The SubSeven Trojan only affects windows-based system.

Network Countermeasures = 1
The attackers activity was reported by the individual syslog, therefore this probe bypassed whatever network countermeasures were in place.

Severity = 2
This is of no concern since SubSeven infects Windows hosts.

9. Defensive Recommendations

Since this host is running some form of Unix, this particular host is immune. I would recommend scanning all internal windows-based platforms for Trojans by using MooSoft's Cleaner utility. An evaluation copy can be obtained at http://www.moosoft.com/download.php.

10. Multiple Choice Test Question

What type of program is SubSeven commonly referred as?

a. Worm
b. Virus
c. Logic Bomb
d. Remote Access Trojan

Answer: d

Assignment 3 – "Analyze This" Scenario

Executive Summary

Overview

Our company performed a five-day security audit for the University from September 5 through September 9. We utilized the Snort Open Source Network Intrusion Detection system to monitor network traffic both entering and exiting the University's Local Area Network (LAN). We capture three categories of information: Alerts, Scans and Out of Specification (OOS). Most of the network activities flagged by the IDS included the Code Red Worm, and its variants, probing for vulnerable servers with the intent of propagation. In addition, multiple reconnaissance scans were launched against the network as well as probing for well-known vulnerabilities. Finally, Snort detected some questionable Internet activity and most disturbing, numerous backdoors into the University's network.

Out of Specification (OOS)

This description is for all packets that display some evidence of crafting. Each protocol should behave a certain way and each subscribes ruling RFC's. If a packet is discovered that violates those rules, it is considered OOS. Also, in order to be in violation of accepted rules, the packet must have been altered in some way, and that way is usually through crafting tools.

Scans

Typically, a scan is used to gain useful tidbits of information regarding the protected internal network. Information such as listening services, IP addresses, Operating System fingerprinting as well as installed security patches. Scans are usually a harbinger of later malicious activity. This works in the favor of the security staff since they will know which systems are targeted and can estimate which type of attack will be launched.

Potential Exploits

Exploits ranged from Microsoft's Internet Information Server, Microsoft Frontpage, and CGI scripts. There was also evidence of numerous buffer overflow attempts targeted at internal hosts.

Questionable Services

Gnutella and Napster activity has been found on several hosts within the University. Also, evidence points to at least one campus host offering online gaming services. A prudent Network Security Policy should disallow potentially dangerous activity on an internal network. To ensure the integrity of your network, the network operations staff needs to know what services are being offered and what information is entering and leaving your network.

Conclusions

It is clear that the University's network has been compromised. All focus should be directed at closing these security holes before the network is used to launch malicious Internet activity. This can be accomplished removing the Trojans and any Code Red Worms, as well as stopping all Napster, GNUTella and gaming server traffic. Finally, all internal hosts should be hardened with all the latest security patches, hot fixes and service packs. Due diligence must be taken to stop current activity and to prevent future incidents.

Alerts

Below is a comprehensive listing of the types of attacks the Snort IDS detected, followed by a brief description of each type of event.

142654 WEB-MISC Attempt to execute cmd
127098 IDS552/web-iis_IIS ISAPI Overflow ida nosize
107989 spp_portscan
31253 MISC Large UDP Packet
28279 Watchlist 000220 IL-ISDNNET-990517
14210 ICMP Destination Unreachable
9608 MISC source port 53 to <1024
7955 INFO MSN IM Chat data
7607 ICMP Echo Request Nmap or HPING2
7292 MISC traceroute
6032 WEB-MISC prefix-get //
5249 CS WEBSERVER - external web traffic
4140 Null scan!
3189 Possible trojan server activity
3007 WEB-IIS 5 Printer-beavuh
2836 INFO napster login
1595 ICMP Echo Request BSDtype
1537 UDP SRC and DST outside network
1306 Port 55850 tcp - Possible myserver activity - ref. 010313-1
1279 SMTP relaying denied
1152 Incomplete Packet Fragments Discarded
1129 Watchlist 000222 NET-NCFC
1127 High port 65535 tcp - possible Red Worm - traffic
845 INFO Inbound GNUTella Connect accept
824 ICMP traceroute
808 INFO Possible IRC Access
619 TCP SRC and DST outside network
597 INFO Napster Client Data
581 ICMP Fragment Reassembly Time Exceeded
388 SCAN Proxy attempt
363 EXPLOIT x86 NOOP
354 ICMP Echo Request Sun Solaris
339 FTP DoS ftpd globbing
291 ICMP Echo Request CyberKit 2.2 Windows
289 INFO Outbound GNUTella Connect accept
287 TFTP - Internal TCP connection to external tftp server
245 ICMP Echo Request Windows
242 External RPC call
223 ICMP Source Quench
192 ICMP Echo Request L3retriever Ping
174 WEB-MISC 403 Forbidden

108 Queso fingerprint
87 Russia Dynamo - SANS Flash 28-jul-00
83 SMB Name Wildcard
77 TELNET login incorrect
72 WEB-MISC http directory traversal
71 x86 NOOP - unicode BUFFER OVERFLOW ATTACK
61 spp_http_decode
50 INFO FTP anonymous FTP
49 WEB-FRONTPAGE _vti_rpc access
42 MISC Large ICMP Packet
41 High port 65535 udp - possible Red Worm - traffic
41 beetle.ucs
39 EXPLOIT x86 setuid 0
33 CS WEBSERVER - external ftp traffic
30 WEB-MISC count.cgi access
27 WEB-FRONTPAGE fpcount.exe access
22 WEB-IIS _vti_inf access
19 Tiny Fragments - Possible Hostile Activity
17 NMAP TCP ping!
17 ICMP SRC and DST outside network
14 connect to 515 from
12 WEB-FRONTPAGE fourdots request
12 SCAN FIN
12 EXPLOIT x86 setgid 0
10 Probable NMAP fingerprint attempt
10 INFO napster upload request
10 INFO - Web Cmd completed
10 ICMP Echo Request Delphi-Piette Windows
9 EXPLOIT x86 stealth noop
8 WinGate 1080 Attempt
8 WEB-MISC L3retriever HTTP Probe
8 SUNRPC highport access!
7 INFO Outbound GNUTella Connect request
7 INFO - Possible Squid Scan
7 BACKDOOR NetMetro File List
6 X11 outgoing
6 WEB-IIS view source via translate header
6 WEB-CGI scriptalias access
6 BACKDOOR NetMetro Incoming Traffic
5 WEB-MISC whisker head
5 WEB-CGI rsh access
5 WEB-CGI redirect access
5 WEB-CGI files.pl access
5 Virus - Possible MyRomeo Worm
5 Port 55850 udp - Possible myserver activity - ref. 010313-1

4 WEB-FRONTPAGE author.exe access
4 SCAN Synscan Portscan ID 19104
3 WEB-IIS scripts-browse
3 WEB-CGI upload.pl access
3 WEB-CGI ksh access
3 TELNET access
3 SYN-FIN scan!
3 INFO Inbound GNUTella Connect request
3 FTP CWD / - possible warez site
2 WEB-CGI csh access
2 WEB-CGI calendar access
2 Virus - Possible scr Worm
2 Virus - Possible pif Worm
2 SNMP public access
2 SCAN XMAS
2 RPC tcp traffic contains bin_sh
2 RFB - Possible WinVNC - 010708-1
2 IDS50/trojan_trojan-active-subseven
2 ICMP Timestamp Reply
1 WEB-MISC Lotus Domino directory traversal
1 WEB-MISC compaq nsight directory traversal
1 WEB-IIS Unauthorized IP Access Attempt
1 WEB-COLDFUSION administrator access
1 WEB-CGI w3-msql access
1 WEB-CGI archie access
1 SITE EXEC - Possible wu-ftpd exploit - GIAC000623
1 INFO napster new user login
1 INFO - Web File Copied ok
1 ICMP Redirect
1 ICMP Mobile Registration Reply
1 FTP MKD . - possible warez site
1 External FTP to HelpDesk MY.NET.83.197
1 EXPLOIT identd overflow
1 EXPLOIT FTP passwd appe path
1 DNS zone transfer
1 Back Orifice

WEB-MISC Attempt to execute cmd

This alert indicates an attacker tried to execute a MS-DOS shell from a remote web browser. This is usually an indication of the Code Red worm.

IDS552/web-iis_IIS ISAPI Overflow ida nosize

This event is likely the probe of the Code Red Worm trying to exploit a vulnerability in Microsoft IIS. An unchecked buffer in the Microsoft IIS Index Server ISAPI Extension could enable a remote intruder to gain SYSTEM access to the web server.

spp_portscan

This is a Snort Preprocessor Plugin that handles portscans that are characterized by probing many ports in a very short time. The default configuration for Snort is a scan accessing a minimum 4 ports in less than 3 seconds.

MISC Large UDP Packet

This event indicates that an abnormally large UDP packet (payload was greater than 4000 bytes) was sent to the server. This may indicate a denial of service attack or the use of a covert channel.

Watchlist 000220 IL-ISDNNET-990517

The watchlist is provided because of the frequency of scans that are launched from the offending network. The IL-ISDNNET indicates an ISP called ISDNNET located in Israel. It is provided as a signature, and the recommendation is to keep a close watch on the types of traffic coming into your network. If you are able to block these addresses at the firewall without impacting your business, it is recommended that you do so.

ICMP Destination Unreachable

This is a response from a router back to the source host informing it that the destination address does not exist.

MISC sourceport 53 to < 1024

This event indicates that an attacker is making a connection to a privileged port using the source port 53 (dns). This should not normally occur. When a client makes a name request to a dns server, it originates form an ephemeral port (>1024). Thus, when the dns server responds, it responds to the requesting ephemeral port. Old or misconfigured packetfilters may allow the connection if they allow all dns traffic.

INFO MSN IM Chat data

This alert indicates that an internal user is using Microsoft Network's (www.msn.com) Instant Messenger capability. This could be in violation of internal policy.

ICMP Echo Request Nmap or HPING2

This event indicates that a ping request was sent to the network. This is usually used as a test to check whether a host is responsive. However, it can be misused to map a network. Nmap 2.36BETA (or earlier) versions, or the HPING2 utility, probably generated this particular ping.

MISC Traceroute

This event indicates that a traceroute was attempted from outside your network, probably from a Windows-class machine. Traceroute is a tool that can be used to discover the route that packets take to reach your host.

WEB-MISC prefix-get //

This event indicates a possible attempt to map a network by receiving a response from a web server.

CS WEBSERVER – external web traffic

The CS Webserver is the Computer Sciences web server. This alert indicates web traffic leaving the campus network.

Null scan!

This event indicates that a TCP frame has been seen with a sequence number of zero and all control bits are set to zero. This frame should never be seen in normal TCP operation. An attacker may be scanning the system by sending these specially formatted frames to see what services are available.

Possible Trojan server activity

This event alerts to the fact that an internal server is answering queries on a high port (> than 1024).

WEB-IIS 5 Printer-beavuh

There is a buffer overflow vulnerability in the web authentication on the RealServer administrator port. By sending a long user/password pair you can overflow the buffer and execute arbitrary code.

INFO napster login

Napster is a internet file sharing application with the goal of sharing .mp3 files between users. This event indicates that either an internal user logged onto a napster server or an internal host is acting as a napster server.

ICMP Echo Request BSDtype

This event indicates that a ping request was sent to your network. Ping requests are usually used to determine whether a host is responsive, but can be misused to map your network. This particular ping was probably generated by BSD/OS, FreeBSD, NetBSD, OpenBSD 2.5, Linux, or Solaris 2.5-2.7. A possible false positive is as follows: "A company named Speedera has a new technology that uses rougly 90 machines distributed around the world to detect the closest web server to you for large corporate sites. They seem to test internet latency using BSD type pings. Each time someone connectes to a Speedera hosted site, you will see roughly 90 hosts ping you with a BSD type payload."

UDP SRC and DST outside network

This alert reports that neither the source nor the destination IP addresses are contained within the internal network. While this may be totally harmless, it is anomalous traffic and could indicate packet crafting.

Port 5580 tcp – Possible myserver activity – ref. 010313-1

MyServer is a Trinoo-style Denial of Service tool that usually communicates over port 55850.

SMTP relaying denied

This event indicates an unsuccessful attempt to use an internal mail server to relay email to a third party.

Incomplete Packet Fragments Discarded

This event describes that an IP datagram was fragmented and all fragments did not arrive. This could be innocent or it could indicate an attacker performing some form of reconnaissance.

Watchlist 000222 NET-NCFC

The watchlist is provided because of the frequency of scans that are launched from the offending network. The NET-NCFC is the Computer Network Center Chinese Academy of Sciences. It is provided as a signature, and the recommendation is to keep a close watch on the types of traffic coming into your network. If you are able to block these addresses at the firewall without impacting your business, it is recommended that you do so.

High port 65535 tcp – possible Red Worm – traffic

Normal traffic should never access port 65535. This alert indicates that whoever wrote the rules file for Snort noticed Code Red Worm traffic accesses port 65535.

INFO Inbound GNUTella Connect accept

This information alert indicates that an outside user has accessed an internal host through GNUTella. GNUTella is a form of distributed information sharing throughout the Internet. An internal host is allowing outside users to access files, folders or even the entire hard drive.

ICMP traceroute

This event indicates that a traceroute was attempted from outside your network, probaby from a Windows-class machine. Traceroute is a tool that can be used to discover the route that packets take to reach your host.

INFO Possible IRC Access

This event indicates that an internal user and external entities are using the Internet Relay Chat (IRC) functionality. This may be in violation of internal policy.

TCP SRC and DST outside network

This alert reports that neither the source nor the destination IP addresses are contained within the internal network. While this may be totally harmless, it is anomalous traffic and could indicate packet crafting.

INFO Napster Client data

Napster is a internet file sharing application with the goal of sharing .mp3 files between users. This event indicates that .mp3 files are either entering or leaving the network. This event is triggered on traffic to destination port 6699.

ICMP Fragment Reassembly Time Exceeded

This is a message sent from a destination host informing the source host that all the packet fragments of a datagram did not arrive. The destination host has a preset time-out value to keep the fragments and will discard them once that time has been met.

SCAN Proxy attempt

Most application proxies listen on port 1080. An attacker can use a vulnerable proxy to launch attacks from the proxy, thus hiding their true source address.

EXPLOIT x86 NOOP

This event may indicate that a string of the character 0x90 was detected. Depending on the context, this usually indicates the NOP operation in x86 machine code. Many remote buffer overflow exploits send a series of NOP (no-operation) bytes to pad their chances of successful exploitation.

ICMP Echo Request Sun Solaris

This event indicates that a ping request was sent by the SING tool running on a Solaris system.

FTP DoS ftpd globbing

This event indicates that a remote attacker may be attempting to crash the ftpd server software by sending a wildcard request to create a denial of service on vulnerable ftp servers.

ICMP Echo Request CyberKit 2.2 Windows

This event indicates that a ping request was sent to your network. Ping requests are usually used to determine whether a host is responsive, but can be misused to map your network. CyberKit 2.2 software running on a Windows system probably generated this particular ping.

INFO Outbound GNUTella Connect accept

This information alert indicates that an inside user has accessed an external host through GNUTella. GNUTella is a form of distributed information sharing throughout the Internet. An internal user is allowing accessing external (and unknown) files, folders or even the entire hard drive.

TFTP – Internal TCP connection to external tftp server

This alert is of interest for two reasons. First, an internal host is connecting to an external tftp server, this could indicate a compromised host, a trojan, or an internal user violating policy. Secondly, tftp is an UDP application and this alert shows it was a TCP connection.

ICMP Echo Request Windows

This event indicates that a ping request was sent to your network. Ping requests are usually used to determine whether a host is responsive, but can be misused to map your network. Microsoft Windows probably generated this particular ping.

External RPC call

This alert indicates that an external host, possibly hostile, has tried to access one of the internal hosts Remote Procedure Call (RPC) ports.

ICMP Source Quench

A Source Quench originates from the sending host informing the destination host to slow down the transmission rate

ICMP Echo Request L3triever Ping

This event may indicate that someone is scanning your network using the L3 "Retriever 1.5" security scanner. This legitimate security tool is for authorized security assessment and should not be used on unauthorized networks. Win2K hosts talking to Win2K domain controllers will generate a false positive.

WEB-MISC 403 Forbidden

This event indicates that an external user tried to access an access-controlled file on an internal web server.

Queso fingerprint

Queso is a tool used for OS fingerprinting on a targeted host.

Russia Dynamo – SANS Flash 28-jul-00

Here is an excerpt from the SANS Flash 29-jul-00:

SANS Flash Report: Trojans Sending More Data To Russia
July 28, 2000, 6:20 pm, EDT

This is preliminary information. The GIAC (Global Incident Analysis Center) has received several submissions showing large amounts of data being sent, illegitimately, from Windows 98 machines to a Russian IP address (194.87.6.X). The cause is most probably a Trojan, but whatever it is, it is moving fast.

More information can be found at
http://archives.neohapsis.com/archives/sans/2000/0068.html

SMB Name Wildcard

This event indicates a standard netbios name table retrieval query. Windows machines often exchange these queries as a part of the filesharing protocol to determine NetBIOS names when only IP addresses are known. An attacker could use this same query to extract useful information such as workstation name, domain, and users who are currently logged in.

TELNET login incorrect

This event indicates a failed login attempt through the telnet service.

WEB-MISC http directory traversal

This event may indicate an attempt to traverse directory limitations through a vulnerable web server daemon or CGI script. This alert could be caused by several different attacks based on directory traversal.

X86 NOOP – Unicode BUFFER OVERFLOW ATTACK

This event may indicate that a string of the character 0x90 was detected. Depending on the context, this usually indicates the NOP operation in x86 machine code. Many remote buffer overflow exploits send a series of NOP (no-operation) bytes to pad their chances of successful exploitation.

spp_http_decode

This is a Snort Preprocessor Plugin that converts Unicode traffic and null bytes in CGI's to non-obfuscated ASCII strings. By using Unicode and null bytes attackers can bypass content analysis strings used to examine HTTP traffic for suspicious activity.

INFO FTP anonymous FTP

This event is a notification that an anonymous FTP connection was completed. This may be a violation depending on the security policy.

WEB-FRONTPAGE_vti_rpc access

Due to the way Front Page Server Extensions (FPSE) handles the processing of web forms, IIS is subject to a denial of service. By supplying malformed data to one of the FPSE functions IIS will stop responding. A restart of the service is required in order to gain normal functionality.

MISC Large ICMP Packet

This event indicates that an abnormally large ICMP packet was sent to your server. This may indicate a denial of service attack or the use of a covert channel.

High port 65535 udp – possible Red Worm – traffic

Normal traffic should never access port 65535. This alert indicates that whoever wrote the rules file for Snort noticed Code Red Worm traffic accesses port 65535.

beetle.ucs

Beetle.ucs is a host that houses a CD-R. This alert indicates that users are copying information form the Internet and saving it to a CD-R.

EXPLOIT x86 setuid 0

This event may indicate an exploit attempt where the attacker sent the setuid(0) system call for the x86 platform. This signature is the most effective when monitoring protocols that usually consist of plaintext printable ASCII to catch remote x86 exploits.

CS WEBSERVER – external ftp traffic

The CS Webserver is the Computer Sciences web server. This alert indicates ftp traffic leaving the campus network.

WEB-MISC count.cgi access

This event indicates an attempt to exploit a vulnerability by executing an arbitrary command via buffer overflow in Count.cgi (wwwcount) cgi-bin program.

WEB-FRONTPAGE fpcount.exe access

If Internet Information Server 4.0 is installed from the NT Option Pack and FrontPage Server Extensions are installed, the 'fpcount.exe' utility found in the '/_vti_bin/' directory contains an exploitable buffer overrun.

WEB-IIS_vti_inf access

This is an alert that an outside individual is performing some form of reconnaissance, the goal here is to find IIS web servers.

Tiny Fragments – Possible Hostile Activity

The smallest fragment that should be sent/receive is 25 bytes; this event triggered on a fragment that was smaller that 25 bytes.

NMAP TCP ping!

This event indicates that a remote user has used the NMAP portscanning tool to probe the server. An NMAP TCP ping was sent to determine if a host is reachable.

ICMP SRC and DST outside network

This alert reports that neither the source nor the destination IP addresses are contained within the internal network. While this may be totally harmless, it is anomalous traffic and could indicate packet crafting.

Connect to 515 from

This event could signal a LPRng buffer overflow attack. LPRng is a linux printer server.

WEB-FRONTPAGE fourdots request

This event indicates a possible attempt at exploiting this vulnerability. A directory traversal vulnerability has been discovered that affects many versions of FrontPage Personal Web Server (Frontpage-PWS32/3.0.2.926).

SCAN FIN

This event indicates a FIN scan packet, where the TCP packet had only the FIN flag set. This can be used in stealth portscanning.

EXPLOIT x86 setgid 0

This event may indicate an exploit attempt where the attacker sent the setgid(0) system call for the x86 platform. This signature is the most effective when monitoring protocols that usually consist of plaintext printable ASCII to catch remote x86 exploits.

Probable NMAP fingerprint attempt

This event indicates that a remote used used the NMAP tool to attempt to determine the server operating system. OS Fingerprinting is a common practice and may provide useful information to an attacker. Typically, this particular signature is only seen when probing an open TCP port.

INFO – Web Cmd Completed

This event alerts the fact that an internal web server transmitted the following message "Command completed."

INFO – napster upload request

Napster is a internet file sharing application with the goal of sharing .mp3 files between users. This event indicates that either an internal user logged onto a napster server and has requested .mp3 files.

ICMP – Echo Request Delphi-Piette Windows

This event indicates that a ping request was sent to your network. Ping requests are usually used to determine whether a host is responsive, but can be misused to map your network. This particular ping was probably generated by software using Delphi code (written by F. Piette).

EXPLOIT x86 stealth noop

This event may indicate that someone attempted to overflow one of your daemons with jmp 0x02 "stealth nops".

WinGate 1080 Attempt

This event indicates that someone is scanning your system to see if it is running WinGate SOCKS. This may be a hacker that desires to "bounce" traffic through your system or a chat server (trying to determine if someone is bouncing through your system to chat anonymously).

WEB-MISC L3retriever HTTP Probe

This event indicates that someone may be scanning your network using the L3 "Retriever 1.5" security scanner. This legitimate security tool is for authorized security assessment and should not be used on unauthorized networks.

SUNRPC highport access!

This incident indicates that a SUNRPC port (in this case port 443) was probed from a port above 1024. This could be legitimate, a reconnaissance probe, or an actual exploit.

INFO – Possible Squid Scan

Squid is a popular Unix proxy that listens on port 3128. An attacker can use a vulnerable proxy to launch attacks from the proxy, thus hiding their true source address.

INFO Outbound GNUTella Connect request

This information alert indicates that an inside user is requesting access an external host through GNUTella. GNUTella is a form of distributed information sharing throughout

the Internet. An internal user is wanting to connect to outside hosts to access files, folders or even entire hard drives.

BACKDOOR NetMetro File List

This event indicates that a known trojan may be operating on the host. This is not a scan or probe, but a successful connection.

X11 outgoing

This event indicates that an XTERM session was initiated, sending the output to an external x-server. This is considered insecure traffic and it is often a sign of compromise. This may also be legitimate traffic by authorized users.

WEB-IIS view source via translate header

This event indicates that a remote intruder has attempted to exploit the default IIS functionality to view the source of scripts on a server. This may also be a WebDAV request.

WEB-CGI scriptalias access

This event indicates an attempt to exploit the scriptalias bug to view the source of CGI scripts that are normally only executable.

BACKDOOR NetMetro Incoming Traffic

This event indicates that a known trojan may be operating on the host. This is not a scan or probe, but a successful connection.

WEB-MISC whisker head

Whisker is a CGI script vulnerability tool, which means, it looks for vulnerable WEB-CGI scripts. This event triggered on the possible whisker probe.

WEB-CGI rsh access

Perl, sh, csh, or other shell interpreters are installed in the cgi-bin directory on a WWW site, which allows remote attackers to execute arbitrary commands.

WEB-CGI redirect access

ColdFusion ClusterCATS appends stale query string arguments to a URL during HTML redirection, which may provide sensitive information to the redirected site.

WEB-CGI files.pl access

This alert indicates that the files.pl file was queried. This could be a reconnaissance probe.

Virus – Possible MyRomeo Worm

Here is Symantec's Anti-Virus Center's description of the MyRomeo Worm:

This worm arrives with one of several different subject lines and has two attachments named Myjuliet.chm and Myromeo.exe. Once you read the message, the two attachments are automatically saved and launched. When launched, this worm attempts to send itself out to all names in the Microsoft Outlook address book using one of several Internet mail servers located in Poland. Otherwise this worm does no harm to the infected system.

Port 55850 udp – Possible myserver activity – ref. 010313-1

MyServer is a Trinoo-style Denial of Service tool that usually communicates over port 55850.

WEB-FRONTPAGE author.exe access

This is an alert that an outside individual is performing some form of reconnaissance; the goal here is to find IIS web servers.

SCAN Synscan Portscan ID 19104

This event indicates a portscan from the popular portscanner "synscan" by psychoid.

WEB-IIS scripts-browse

This is an alert that an outside individual is performing some form of reconnaissance; the goal here is to find IIS web servers and attempt to browse the /scripts directory looking for exploitable scripts.

WEB-CGI upload.pl access

This alert indicates that the upload.pl file was either invoked or was queried. This could be a reconnaissance probe or part of an exploit script. Upload.pl allows files to be copied to a web server from a hosts browser.

WEB-CGI ksh access

Perl, sh, csh, or other shell interpreters are installed in the cgi-bin directory on a WWW site, which allows remote attackers to execute arbitrary commands.

TELNET access

This event indicates that a successful telnet connection has been established from outside the local network. Telnet is a very insecure protocol and should be replaced with SSH immediately.

SYN-FIN scan!

This event indicates a SYN-FIN scan packet, where the TCP packet had both the SYN and the FIN flag set. This can be used in stealth portscanning.

INFO Inbound GNUTella Connect request

This information alert indicates that an outside user has trying to access an internal host through GNUTella. GNUTella is a form of distributed information sharing throughout the Internet. An internal host might be allowing outside users to access files, folders or even the entire hard drive.

FTP CWD / - possible warez site

This alert indicates that a user, authorized or not, has changed directories on a FTP server. Warez sites are repositories for crackers to place malicious scripts and/or root kits.

WEB-CGI csh access

Perl, sh, csh, or other shell interpreters are installed in the cgi-bin directory on a WWW site, which allows remote attackers to execute arbitrary commands.

WEB-CGI calendar access

A security vulnerability in the Calendar CGI script allows remote users to execute arbitrary commands on the web server with the privileges of the httpd process.

Virus – Possible scr Worm

Many worms infect hosts through modified screen savers, which have an .scr extension. This alert triggers on an .scr file arriving via POP3.

Virus – Possible pif Worm

Many worms infect hosts through modified applications, or more specific to this alert, through their shortcut filenames, which have a .pif extension. This alert triggers on a .pif file arriving via POP3.

SNMP – public access

A lot of network devices (such as intelligent switches, WAN/LAN routers, ISDN/DSL modems, remote access machines and even some user-end operating systems) are by default configured with SNMP enabled and unlimited access with write privileges. This allows attackers to modify routing tables, get the status of network interfaces and other vital system data, and is considered extremely dangerous from a security perspective.

SCAN XMAS

This event indicates that an intruder is scanning your computer for available TCP services by sending "Xmas-tree" packets. These packets have the a sequence number of zero and the SYN, FIN, ACK, URG, PSH, and RST flags set. This packet should never be seen in normal TCP operation.

RPC tcp traffic contains bin_sh

This event alerts to the fact that someone is trying to open a root shell on a host.

RFB – Possible WinVNC – 010708-1

AT&T WinVNC is a free package available from AT&T Labs Cambridge that allows an existing desktop of a PC to be available on the desktop of a remote host.

IDS50/trojan_trojan-active-subseven

This event indicates that a known trojan may be operating on the host. This is not a scan or probe, but a successful connection.

ICMP Timestamp Reply

This message is sent to the source host from a router for the purpose of clock synchronization.

WEB-MISC Lotus Domino directory traversal

A Lotus Domino server running the HTTP task may permit an intruder to read files on file systems or drives that house Lotus Notes databases. By using a specially crafted URL containing ".." and the name of an existing file, an intruder may be able to cause a Domino server to return the contents of the file to the intruder over the HTTP connection. If this file contains sensitive information, an intruder may be able to leverage that information to gain additional access

WEB-MISC Compaq nsight directory traversal

This event indicates that an intruder has attempted to exploit a directory traversal vulnerability in the Compaq Web Management Agent. This allows a remote attacker to read arbitrary files.

WEB-IIS Unauthorized IP Access Attempt

This event alerts to the fact that a user has tried to access a protected file or folder. The file or folder is usually protected through access controls.

WEB-COLDFUSION administrator access

This alert indicates that a user, whether hostile or not, has gained administrator access to a ColdFusion web server.

WEB-CGI w3-msgl access

This event indicates that an attempt was made to access the cgi component of miniSQL called w3-msql. Versions 2.0.4.1 - 2.0.11 are vulnerable to a remote buffer overflow.

WEB-CGI archie access

This is likely a reconnaissance attempt to see if this server is an archie server.

SITE EXEC – Possible wu-ftpd exploit – GIAC000623

This event indicates the possibility of a portion of the remote ftpd attack against wu-2.6.0. This probe is common in both the Linux and BSD versions of the published exploit.

INFO – Web File Copied ok

This alert indicates that a file has been uploaded to a web server. The trigger is "1 file(s) copied".

INFO napster new user logon

Napster is a internet file sharing application with the goal of sharing .mp3 files between users. This event indicates that either an internal user logged onto a napster server or an internal host is acting as a napster server.

ICMP Redirect

This message is sent to the source host from a router informing the host that it is not the optimum router and sends the address of the more optimum router. An attacker could use this information for network mapping.

ICMP Mobile Registration Reply

This event signals that a mobile computing device registered itself with a wireless routing device. The mobile device could be internal or external to the internal network.

FTP MKD . – possible warez site

This alert indicates that a user, authorized or not, has created a directory. Warez sites are repositories for crackers to place malicious scripts and/or root kits.

External FTP to HelpDesk MY.NET.83.197

This alert indicates a FTP connections has been established to the internal HelpDesk, originating form outside the network.

EXPLOIT identd overflow

This exploit sends a buffer overflow condition to the identd service in the attempt to gain root access.

EXPLOIT FTP passwd appe path

This event may indicate that an intruder is attempting to append to a password file to the ftp server. If the ftp server is misconfigured, the attacker may be able to add to the existing passwd file and gain access to the server.

DNS zone transfer

This event indicates that an outside host requested a zone transfer from an internal DNS server. This could be legitimate traffic from a secondary DNS server, or an attacker gathering information about your domain. A DNS zone transfer may be permitted if the requesting host is a secondary DNS server.

Back Orifice

This event indicates that a remote attacker has sent an information request to a Back Orifice trojan. If the trojan is running on the server, then the server has been compromised.

Below is an examination of the top ten source IP addresses from five days worth of alerts. These addresses include both external and internal addresses. An important note of caution, the source addresses owners might not be aware of the possible malicious activity originating from their network. These hosts could have been compromised and are being used to either launch attacks or act as information gathering assets. In addition, these sources might not be intentionally malicious; there is the possibility that these hosts or devices are improperly configured. All address resolution was obtained through http://www.geektools.com/cgi-bin/proxy.cgi. Below is a table of the top ten alert addresses:

24299	212.179.27.6
14919	61.153.17.244
11478	211.90.176.59
6656	61.153.17.24
5812	MY.NET.226.18
5337	211.90.164.34
4904	MY.NET.14.1
4902	MY.NET.16.5
4124	200.250.65.1
3654	195.46.229.103

1. **212.179.27.6** – Source is ISDNNET located in Israel.

   This address is included in a watchlist and is described above. The destination ports are of particular interest.

Number	Port No	Description
24296	1214	Kazaa
1	2637	Impoprt Document Service
1	4180	Unassigned
1	6346	GNUTella

   The majority of this traffic is through Kazaa. Kazaa is an Internet Media File Sharing community, similar to Napster. This could be legitimate and harmless traffic, but it could also not be. As stated above, all traffic from the source should be considered suspect and blocked if possible.

2. **61.153.17.244** – Source is Ningbo Telecommunication Corporation in Ningbo, China.

   The majority of this traffic was "MISC Large UDP Packet" which indicated that the UDP payload was greater than 4000 bytes, which is unexpected and anomalous traffic. This could be unintentional and harmless, or it could be either a covert channel or a denial of service. Hidden within this packet is a curious exchange between this host and the hosts MY.NET.111.221 and MY.NET.153.193. The traffic sent to MY.NET.111.221 was TCP in nature and

fragmented. However, not all the fragments arrived and the reassembly time expired. This could indicate a primitive denial of service or a reconnaissance attempt. The traffic sent to MY.NET.153.193 was also TCP and fragmented, but the fragments were discarded. The item of note was the source and destination ports, both were 0. Port 0 should not be used under normal network communications. This was probably some form of reconnaissance attempt.

3. **211.90.176.59** – Source is China United Telecommunications Corporation.

   This is a Code Red Worm trying to propagate throughout the MY.NET network. Included in this detect are "possible trojan activity" alerts. Snort detected traffic originating from port 27374, which is a well known port for the Ramen worm or the SubSeven backdoor. However, I do not believe this was trojan activity. This host used ephemeral (typically greater that port 1024) source port 27374 arbitrarily. Typically, hosts use available ephemeral ports in ascending fashion. The use of port 27374 was just this host had used the lower ephemeral ports and port 27374 was next.

4. **61.153.17.24** – Source is Ningbo Telecommunication Corporation in Ningbo, China.

   This detect contained two types of events, portscan and "Large UDP packets". I concentrated on the "Large UDP packets" and noticed this host targeted two internal hosts: MY.NET.111.221 and MY.NET.153.153. A majority of the source and destination ports were port zero, which is almost always used for reconnaissance purposes. This is almost certainly a reconnaissance scan from this host with the purpose of mapping the destination network and possibly performing OS fingerprinting.

5. **MY.NET.226.18** – Source is internal host.

   The most disturbing portion of this detect was that this internal host was actively pinging three external hosts. The external hosts are as follows:

Number of Requests	IP Address	Whois
2913	206.79.171.51	Lycos
2833	204.71.200.75	Yahoo-SNV
66	204.152.190.70	M.I.B.H. LLC

   This would indicate that either this internal host has been compromised and is being used for information gathering, or an internal user is using this host for information gathering. The Snort rule stated it was probably a crafted ICMP Echo Request, and the tools used to craft this packet was either Nmap or HPING2. This may or may not be the case. An ICMP packet can indeed be crafted with these tools, or maybe the IP stack is corrupted and is mangling ICMP packets. If the latter is the case, this is innocent traffic with no ulterior motives.

The other events that targeted this host were various Code Red worm attacks. Looking at the network traffic, it looks like the worm was unsuccessful. A good indication of a successful worm infection is a response from the IIS server stating a web file was successfully copied, of which none were displayed with this host.

6. **211.90.164.34** - Source is China United Telecommunications Corporation.

   This host is infected with the Code Red Worm and is trying to propagate itself onto this internal network.

7. **MY.NET.14.1** - Source is internal host.

   This detect is someone on the internal network is performing traceroutes throughout the network. Best guess is that this host is a router since a vast majority of the traffic within this detect are "ICMP Destination Unreachable (Communication Administratively Prohibited)." This indicates that a network administrator configured this router to send this message to hosts that try to ping or traceroute its protected subnet. This may be a malicious individual trying to map that subnet, or it could be a network administrator performing some form of network maintenance.

8. **MY.NET.16.5** - Source is internal host.

   This is similar to the above detect. This detect includes mostly "ICMP Destination Unreachable (Communication Administratively Prohibited)" messages from this host, which is probably a router. However, unlike the above detect, there was no tracerout alerts. By looking at this detect it is unknown what triggered the router to respond like this. It would be helpful to know the IP address of this subnet and monitor traffic destined for this addresses. At this time, it is unknown whether this is malicious or not.

9. **200.250.65.1** – Source is Pluma Conforto E Turismo S/A in Curitiba, Puerto Rico.

   This is another Code Red infected host trying to propagate itself onto this internal network. An additional event was router MY.NET.30.2 sending a "Network Unreachable" message to this host. This means that the Code Red worm tried to probe a non-existent subnet.

10. **195.46.229.103** – Source is Commune Esch-sur-Alzette in Esch-sur-Alzette, Luxembourg.

    This is the same exact situation as above; this host is infected with the Code Red worm and is trying to propagate itself onto this internal network. This detect even contains the same message from router MY.NET.30.2.

Scans

Top Ten Sources

Below is a listing of source IP addresses that have shown the most interest in the monitored network. MY.NET indicates the monitored network.

Number of Scans	Source IP
41408	MY.NET.160.114
31551	MY.NET.218.78
22504	MY.NET.201.42
19427	MY.NET.213.6
15036	205.188.246.121
9737	205.188.233.185
9157	MY.NET.234.162
6880	MY.NET.201.66
6221	MY.NET.236.246
5965	MY.NET.237.98

Below is an examination of the top ten source IP addresses from five days worth of alerts. These addresses include both external and internal addresses. An important note of caution, the owners of the source addresses owners might not be aware of the possible scanning activity originating from their network. These hosts could have been compromised and are being used to as an information-gathering asset. In addition, these devices might be improperly configured. All address resolution was obtained through http://www.geektools.com/cgi-bin/proxy.cgi. All port number information was gained through http://www.portsdb.org/bin/portsdb.cgi.

1. **MY.NET.160.114** – Source is an internal host.

   This was a UDP scan originating from an internal host. The curious thing about this traffic was that source ports were 777 and 888. Port 777 is typically used for Multiling HTTP; however, two known Trojans also use port 777. The Trojans are AimSpy and Undetected (http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html).

   Port 888 is used with the CD Database Protocol (CDDBP). CDDB is a database that stores information regarding music CD's, which can be accessed through the Internet. http://www.freedb.org is an example of a CDDB. This looks like this host is accessing and download Internet music files from various CDDB's, some of which are overseas, thus the need for Multilingual HTTP.

2. **MY.NET.218.78** - Source is an internal host.

   The majority of activity originating from this host was targeted to port 137

(NETBIOS NameService) on external hosts. This would indicate a script on the MY.NET.218.78 searching for Microsoft Windows hosts. Other activity included SYN scans to the following ports:

Port Number	Function
1214	Kazaa –Internet Media File Sharing utility
2420	DSL Remote Management
4912	N/A
5000	SSDS - WindowsME ships with a program called "SSDPSRV.EXE", or Simple Service Discover Protocol Server, which is used for Universal Plug and Play. This process listens on TCP 5000 for XML exchange.

The following are actually targeting MY.NET.218.78. The first scan contains the reservedbits "21", which might be legitimate traffic. These two TCP flags can be used for Explicit Congestion Notification, which is used by a router to notify a sender that there was congestion on the network. However, the more plausible explanation is that this is an attempt at OS fingerprinting (nmap).

Sep 5 17:28:16 |24.155.24.180:2544|MY.NET.218.78:1214 UNKNOWN
21***PA* RESERVEDBITS

The next scan indicates that no TCP flags were set, which may not be malicious, it is anomalous.

Sep 6 06:59:42 |216.187.158.15:32848|MY.NET.218.78:63268 NULL ********

3. **MY.NET.201.42** - Source is an internal host.

The scans originating from this host were all UDP scans from various ports, to various hosts and ports. I concentrated on the source ports and have listed the top ten ports in terms of activity:

Number	Port No	Description
7178	2202	Int. Multimedia Teleconferencing Cosoritium
4204	2010	pipe_server
3003	1404	Infinite Graphics License Manager
2986	1249	Mesa Vista Co
1025	1695	rrilwm
935	1711	pptconference
898	2346	Game Connection Port - Red Storm
771	13139	N/A

525	6500	BoKS Master

Looking at the differences in the above table, I would estimate that this host is either a proxy server or a DMZ host used for teleconferencing. The only caution I could observe from the above table is the Red Storm game activity (port 2346).

4. **MY.NET.213.6** - Source is an internal host.

   Again, the detected activity from this host is UDP traffic. The piece of information that jumped out was the destination of the majority of the traffic. Here is a listing of the top three destinations:

Number	ID Address	Owner
10507	66.44.42.75	
7067	66.44.49.193	
565	24.216.118.25	

   Upon further examination of the scan file, specifically focusing on the above three addresses, I noticed it was a port scan. The time were all under 6 minutes and almost the entire range of ports were under 1024, or the well-known ports.

5. **205.188.246.121** – Source is America Online, Inc in Sterling, VA.

   The unusual aspect of this detect was that all the traffic was destined for port 6970. Research found that this port is typically associated with RealAudio; probably RealAudio servers at AOL sending ads to client desktops. Reference was http://www.shmoo.com/mail/firewalls/jun99/msg00791.html and http://www.networkice.com/advice/Exploits/Ports/6970/default.htm. This probably is not malicious traffic, but it could be in violation of the local security policy.

6. **205.188.233.185** – Source is America Online, Inc in Sterling, VA.

   This has the same explanation as above. All traffic was destined for port 6970.

7. **MY.NET.234.162** - Source is an internal host.

   This detect is showed a lot of traffic from source port 28800 to destination port 28800. Research showed this to be more than likely connections to the MSN Gaming Zone. The following articles were used for correlation:

   http://support.microsoft.com/support/kb/articles/Q159/0/31.ASP
   http://cert.uni-stuttgart.de/archive/incidents/2000/09/msg00045.html
   http://cert.uni-stuttgart.de/archive/incidents/2000/12/msg00171.html

   While this is not malicious activity, this could be in violation of local security

policy.

Number	Port No	Description
3659	2175	Unassigned
3624	28800	MSN Gaming Zone
760	3095	Panasas Rendezvous Port
380	1756	Capfast-lmd
346	2961	Boldsoft-LM
340	1955	ABR Secure Data
48	2346	Game Connection – Red Storm_Join

Red Storm is also an online gaming network. Port 2175 is of some concern. I was unable to determine what programs use that port; however, according to http://cert.uni-stuttgart.de/archive/incidents/2000/12/msg00171.html, this might be part of Microsoft's Net Meeting.

8. **MY.NET.201.66** - Source is an internal host.

The most alarming traffic from this detect was this host scanning other internal hosts, which could indicate that this host has been compromised and is being used to map the internal network. This led me to investigate the alerts file for evidence of compromise. The follow alerts show that indeed it does look like this host was compromised.

09/05-19:01:04.463233 [**] INFO FTP anonymous FTP [**] 217.162.127.5:1726 -> MY.NET.201.66:21
09/05-20:20:23.006221 [**] WEB-MISC Attempt to execute cmd [**] 130.95.176.30:2065 -> MY.NET.201.66:80
09/06-15:57:21.395798 [**] WEB-MISC Attempt to execute cmd [**] 217.32.152.158:3844 -> MY.NET.201.66:80
09/08-12:27:28.858060 [**] IDS552/web-iis_IIS ISAPI Overflow ida nosize [**] 200.68.53.10:3763 -> MY.NET.201.66:80
09/09-19:16:12.537973 [**] IDS552/web-iis_IIS ISAPI Overflow ida nosize [**] 147.52.126.64:1143 -> MY.NET.201.66:80
09/09-22:29:59.316111 [**] connect to 515 from inside [**] MY.NET.201.66:3208 -> MY.NET.0.5:515
09/09-22:31:07.066722 [**] Possible trojan server activity [**] MY.NET.201.66:4297 -> MY.NET.0.1:27374
09/09-22:33:07.544057 [**] Possible trojan server activity [**] MY.NET.201.66:3190 -> MY.NET.0.13:27374
09/09-22:40:08.247338 [**] connect to 515 from inside [**] MY.NET.201.66:4767 -> MY.NET.0.57:515
09/09-22:42:12.611920 [**] Possible trojan server activity [**] MY.NET.201.66:3676 -> MY.NET.0.55:27374
09/09-22:47:22.074503 [**] connect to 515 from inside [**] MY.NET.201.66:3832 -> MY.NET.0.89:515
09/09-22:50:09.205549 [**] Possible trojan server activity [**] MY.NET.201.66:3472 -> MY.NET.0.97:27374

09/09-22:59:25.442174 [**] Possible trojan server activity [**] MY.NET.201.66:4875 -> MY.NET.0.135:27374
09/09-22:59:46.427712 [**] connect to 515 from inside [**] MY.NET.201.66:3101 -> MY.NET.0.147:515
09/09-23:12:36.863317 [**] connect to 515 from inside [**] MY.NET.201.66:4169 -> MY.NET.0.207:515
09/09-23:14:43.002516 [**] connect to 515 from inside [**] MY.NET.201.66:3751 -> MY.NET.0.219:515
09/09-23:17:07.145473 [**] connect to 515 from inside [**] MY.NET.201.66:3122 -> MY.NET.0.229:515
09/09-23:19:32.525303 [**] Possible trojan server activity [**] MY.NET.201.66:4621 -> MY.NET.0.237:27374
09/09-23:19:43.075931 [**] Possible trojan server activity [**] MY.NET.201.66:3823 -> MY.NET.0.239:27374

9. **MY.NET.236.246** - Source is an internal host.

   Below is a listing of source ports for the traffic originating from this host:

Number	Port No	Description
2584	1671	Netview-aix-11
2340	2812	Atmtcp
1296	28800	MSN Gaming Zone
1	3014	Broker Service

   What immediately jumps out is the MSN Gaming Zone traffic. Again, this is not malicious, but might be in violation of local security policy.

10. **MY.NET.237.98** - Source is an internal host.

    Again, the majority of this traffic is targeted at port 28800, MSN Gaming Zone.

Out of Specifications (OOS)
Top Ten Sources

Below is a listing of source IP addresses that have shown the most interest in the monitored network. MY.NET indicates the monitored network.

Number of Scans	Source IP
34	198.186.202.147
22	199.183.24.194
20	128.46.156.155
11	151.38.84.194
9	130.207.193.70
7	212.124.64.22
7	193.137.96.74
5	MY.NET.237.6
5	66.31.20.215
5	193.231.20.2

Below is an examination of the top ten source IP addresses from five days worth of alerts. These addresses include both external and internal addresses. An important note of caution, the owners of the source addresses owners might not be aware of the possible activity originating from their network. These hosts could have been compromised and are either being used to launch an attack or acting as an information-gathering asset. In addition, these devices might be improperly configured. All address resolution was obtained through http://www.geektools.com/cgi-bin/proxy.cgi. All port information was obtained from http://www.portsdb.org/bin/portsdb.cgi.

1. **198.186.202.147** – Source is Dandelion Digital in Incline Village, Nevada.

   This host sent TCP packets with the Explicit Congestion Notification (ECN) bits set. This is not normal TCP traffic and could be used for remote operating system fingerprinting. However, some routers do use these bits to notify a sender that there is congestion in the network and to request the sender to reduce its sending rate. Another interesting bit of information is that the destination port is port 113, which is the Ident or Auth port. Ident identifies the owner of a connection between the client and a server, but is often used when sending e-mail. Auth is an Authentication Service used for system to authenticate with each other. This may be innocuous, but does deserve close observation in the future. Here is a sample of the offending TCP packets:

```
09/05-00:05:01.429911 198.186.202.147:50839 -> MY.NET.253.52:113
TCP TTL:47 TOS:0x0 ID:33000  DF
21S***** Seq: 0x8C64C1FA   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 113066258 0 EOL EOL EOL EOL
```

2. **199.183.24.194** – Source is Red Hat Software in Chapel Hill, North Carolina.

   This is very similar to the above traffic. Both ECN bits are set; however, traffic is destined for port 25, which is the SMTP port. Again, this could be OS fingerprinting or could be a router telling the internal hosts to slow down their outbound TCP traffic. Here is a sample of these packets:

```
09/07-04:37:21.613280 199.183.24.194:40645 -> MY.NET.253.43:25
TCP TTL:53 TOS:0x0 ID:52999  DF
21S***** Seq: 0xBE8B48A   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 235764621 0 EOL EOL EOL EOL
```

3. **129.46.156.155** – Source is Purdue University in West Lafayette, Indiana.

   This is again a TCP packet with the ECN bits set with the exception of the destination port, which in this case is port 80. This is the well-known HTTP or web traffic. Here is a sample:

```
09/05-01:30:29.630046 128.46.156.155:44984 -> MY.NET.99.85:80
TCP TTL:55 TOS:0x0 ID:24273  DF
21S***** Seq: 0xCF10E79B   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 46184778 0 EOL EOL EOL EOL
```

4. **151.38.84.194** – Source is Infostrada SpA in Milan, Italy.

   This host looks like it is trying to perform OS fingerprinting on host MY.NET.235.94, since the ECN echo, SYN, FIN, and RST bits are all set. The targeted destination port 27970 is a port often used for Quake III by Internet gaming server. MY.NET.235.94 is more than likely an online gaming server running Quake III. Here is a sample:

```
09/05-11:00:21.548861 151.38.84.194:27960 -> MY.NET.235.94:27970
TCP TTL:113 TOS:0x0 ID:17437  DF
*1SFR*** Seq: 0x34771E   Ack: 0x41060000   Win: 0x16CA
TCP Options => EOL EOL EOL EOL EOL EOL SackOK
```

5. **130.207.193.70** – Source is Georgia Institute of Technology in Atlanta, Georgia.

   This host sent TCP packets with the Explicit Congestion Notification (ECN) bits set. This is not normal TCP traffic and could be used for remote operating system fingerprinting. However, some routers do use these bits to notify a sender that there is congestion in the network and to request the sender to reduce its sending rate. Another interesting bit of information is that the destination port is port 113, which is the Ident or Auth port. Ident identifies the owner of a connection between the client and a server, but is often used when sending e-mail. Auth is an Authentication Service used for system to authenticate with each other. This may be innocuous, but

does deserve close observation in the future. Here is a sample of the offending TCP packets:

```
09/06-12:56:19.364788 130.207.193.70:4341 -> MY.NET.253.52:113
TCP TTL:56 TOS:0x0 ID:12720  DF
21S***** Seq: 0x2A9CE175   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 334942405 0 EOL EOL EOL EOL
```

6. **212.124.64.22** – Source is Internet Bulgaria, Ltd. in Sophia, Bulgaria.

   This is again a TCP packet with the ECN bits set with the exception of the destination port, which in this case is port 80. This is the well-known HTTP or web traffic. Here is a sample:

```
09/06-12:20:55.089704 212.124.64.22:36065 -> MY.NET.100.165:80
TCP TTL:47 TOS:0x0 ID:50822  DF
21S***** Seq: 0xA32279BA   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 383369020 0 EOL EOL EOL EOL
```

7. **193.137.96.74**– Source Universidade de Tras-os-Montes e Alto Douro in Vila Real, Portugal.

   This is another group of TCP packets that has the ECN bits set. This could be an attempt of OS fingerprinting or a router trying to slow down traffic being routed through itself. Another item if interest is the destination port of 6346, which is a port used with GNUTella Internet File Sharing Service. A brief description of GNUtella services is provided in the above alerts explanation.

```
09/05-09:05:58.902955 193.137.96.74:33408 -> MY.NET.219.142:6346
TCP TTL:52 TOS:0x0 ID:1053  DF
21S***** Seq: 0xF78FCC74   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 182377 0 EOL EOL EOL EOL
```

8. **MY.NET.237.6** – Source is an internal host.

   This group of OOS detects follows no pattern except originating from the same host, MY.NET.237.6. There is definitely suspicious traffic. My best guess is that someone has obtained a copy of Nmap and is playing with its capabilities. Other explanations include an internal malicious user performing reconnaissance for future activity, or this host has been compromised and is being used as an information-gathering asset.

   All of the TCP bits were flagged in differing combinations of the five packets. All of them violated the TCP protocol and were thus logged. The destination addresses were all different and no pattern was detected with the ports. Port 7668 was used more than once, but again, in no discernable pattern. The source and destination ports are included in the following table:

Port	Service
3267	IBM Dial Out
7668	Internet Calendar Access Protocol
1104	XRL
1061	KIOSK
49289	N/A

9. **66.31.20.215** – Source is MediaOne Northeast in Chelmsford, Massachusetts.

   This is another group of TCP packets that has the ECN bits set. This could be an attempt of OS fingerprinting or a router trying to slow down traffic being routed through itself. Another item if interest is the destination port of 6346, which is a port used with GNUTella Internet File Sharing Service. A brief description of GNUtella services is provided in the above alerts explanation.

```
09/07-22:28:00.546928 66.31.20.215:32970 -> MY.NET.53.40:6346
TCP TTL:47 TOS:0x0 ID:18230  DF
21S***** Seq: 0x2247C6E6   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 557520 0 EOL EOL EOL EOL
```

10. **193.231.20.2** – Source is "Babes-Bolyai" University of Cluj-Napoca in Cluj-Napoca, Romania.

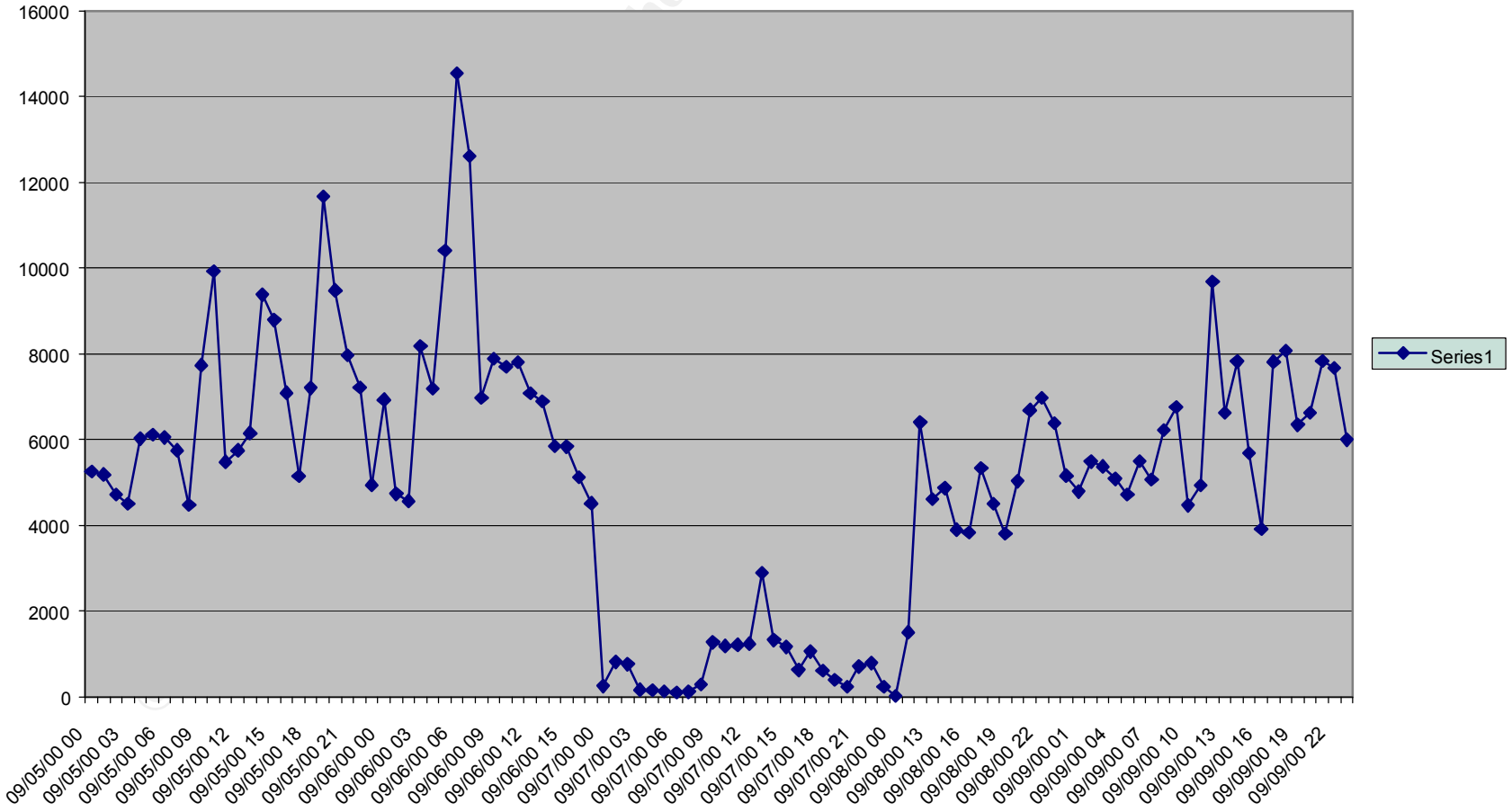
    This is a group of TCP packets with the ECN bits set and the destination of port 80. This is the well-known HTTP or web traffic. Here is a sample:

```
09/06-03:36:02.337155 193.231.20.2:58847 -> MY.NET.6.7:80
TCP TTL:46 TOS:0x0 ID:51736  DF
21S***** Seq: 0xE6F0AA79   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 113598561 0 EOL EOL EOL EOL
```

References

1. http://www.snort.org
2. http://www.whitehats.com
3. http://www.incidents.org
4. www.cert.org
5. http://cve.mitre.org/cve
6. http://www.securiteam.com
7. http://www.sans.org/y2k/practical/Charles_Hutson_GCIA.doc
8. http://www.sans.org/y2k/practical/Scott_Crimminger_GCIA.doc
9. http://www.symantec.com/avcenter
10. http://www.geektools.com
11. http://www.portsdb.org
12. http://www.moosoft.com
13. RFC 2002 “IP Mobility Support”

Chart of Alerts by Hour



Defensive Recommendations

The first action to take are to remove the hosts that display infected symptoms of Trojans or backdoors (NetMetro, SubSeven, MyServer, MyRomeo and any .pif/.scr) and clean them by either formatting the hard drive and rebuild, or use an automated tool such as "The Cleaner" from MooSoft.com. Second, I would review the logs of all the MY.NET.x.x that was discussed in the above explanations. Specifically, host MY.NET.201.66 looks to be compromised. I would suggest taking the system offline and run "The Cleaner" to remove all Trojans, review the systems logs, and finally review the users list to detect any unauthorized user accounts. Changing all system passwords would be a prudent action. I would also access all internal and DMZ servers and ensure all the latest security patches, hot fixes and service packs are installed and properly configured. A prudent course of action would be to block the two "Watchlist" addresses (NET-NCFC and IL-ISDN-990715). A good recommendation is to enforce the Network Security Policy and disallow Napster and GNUTella activity, along with removing any and all On-Line Gaming Servers. If there is no Network Security Policy, or the policy does not address Napster and GNUTella, I strongly suggest drafting one. I suggest reviewing the firewall policies and tightening any glaring security holes. By looking and the IDS traffic, I would suggest Napster and GNUTella default ports be blocked, ports 55850 and 65535 be closely monitored, and ensure internal hosts do not reply to external IMCP requests.

Description of Analysis Process

I downloaded the requisite files from the provided ftp server and saved them to a secure system. The files spanned Sep 5 through Sep 9 and included the alerts, scans and OOS. I then used CAT and combined all five alert files into one large file.

#cat alert.* >> all-alerts.txt

I first attempted to use Snort Snarf to provide analysis statistics. However, the input Snort alert file was too large for Snarf to handle. I then used a recommended analysis tool from the Snort web page called snort_stat.pl. This provided some useful information, but the output file was too large and unwieldy. I then found Charles Hutson's practical and fortunately he described various shell scripts that he used to analyze Snort alert files. I would like to take this moment to thank Mr. Hutson for his helpful scripts. Because of these handfuls of scripts, I now know more about sed, awk, and grep than I ever wanted to.

Most of the alerts in the alert file followed a standard format that can be described as:

Date/Timestamp [**] Alert [**] SourceIP:Port -> DestinationIP:Port

The only alerts that did not follow this format were the Snort Preprocessor Plugins (spp_). An example of this is as follows:

09/05-00:16:05.361335 [**] spp_portscan: PORTSCAN DETECTED from MY.NET.218.50 (THRESHOLD 4 connections exceeded in 3 seconds) [**]

Armed with this knowledge, I used Mr. Hutson's snortalf script to change the alert file into a common format with common delimiters. The script is as follows:

```
#!/bin/sh
#
#snortalf – snort alert formatter
#
#Charles L. Hutson
#3/26/01
#
#Takes the file listed as the first command line argument and formats
#for better intrusion analysis. A '|' is used to delimit fields for later
#later manipulation using awk.
#
#The following modifications to the standard Snort Alert output files
#are made:
#
#sed #1: removes [**] and replaces with delimiter
#sed #2: removes -> and replaces with delimiter
#sed #3: delimits the "from" field from the IP address field on
#       "spp_portscan status entries"
#sed #4: remove : followed by a space on "spp_portscan" entries and
#       add a delimiter
#sed #5: insert a delimiter before the left parenthesis that common oin
#       "spp_portscan status entires"
#sed #6: take a mistakenly placed delimiter out on "spp_portscan" entries.

cat $1 | sed 's/\[\*\*\]/\|/g' | sed 's/->/\|/g' | sed 's/from/from\|/g' | sed 's/: /\|/g' |
sed 's/ (/\|(/g' | sed 's/spp_portscan\|/spp_portscan-/g' >> $1.alf
```

This script takes the alert file containing all five days of alert data and creates a "|" delimited file with a .alf extension. A side note, sed #6 did not work properly, it ended up creating a file containing all "spp_portscans". I removed this sed command and the script worked wonderfully. The following command produced the file I needed to apply more in depth analysis:

#./snortalf all-alerts.txt

I then used his third script. The reason I did not use the second script was because there was over 120 alerts and by using his second script, that would mean I would have to execute that script over 120 times. Too much time and effort, and that would only produce too specific data. I need a quick look at what was launched against the network and how often it occurred. The following script was what I used:

```
#!/bin/sh
#snortsome –snortsome summarization tool.
#Charles L. Hutson
#3/27/01
#
#Uses filename.alf files as a source (see 'snortalf' program developed by
#Charles Hutson) and generates various snort summaries.
#
#Input: 1st argument is the .alf formatted file to summarize
#

#
#Group by attack
#
cat $1 | grep –v spp | awk –F"|" '{print $2 ":"$3}' | awk –F":" '{print $1 ":"$2}'
| sort | uniq –c | sort >> attack-src

#
#Group by Source IP
#
cat $1 | grep –v spp | awk –F"|" '{print $2 ":"$3}' | awk –F":" '{print $2 ":"$3}'
| sort | uniq –c | sort >> src-attack

#
#All Sources Sorted
#
cat $1 | grep –v spp | awk –F"|" '{print $2 ":"$3}' | awk –F":" '{print $2}' | sort
| uniq –c | sort –r >> attackers

#
#All Destinations Sorted
#
cat $1 | grep –v spp | awk –F"|" '{print $4}' | awk –F":" '{print $1}' | sort |
uniq –c | sort –r >> targets
```

The first and third commands produced the most useful output. The first organized all the unique attacks that were monitored and then totaled each attack. This data was then imported into an Excel spreadsheet to provide a sorted list of all the unique attacks, starting with the most frequent. The third totaled how often a source IP sent packets to the network. This was the basis for the "Top Ten Talkers" table.

Next came the daunting task of providing a brief description of each attack that was detected. My first step was to obtain Snorts 1.8 configuration file and all associated rules file. I combined all the rules files into one file to ease searching for unique strings. I loaded the combined rules file into WordPad and used WordPad's Find function to locate which rule was triggered for each alert. Most of the rules contained a reference Arachnids, CVE or Bugtraq identification number. I used Arachnids whenever possible or CVE if no Arachnids was provided. For the rules that did not contain references, I used CERT and searched their site for keywords. After exhausting that resource, I then

searched through Securiteam's web site. For the Trojans and viruses I utilized Symantec's Anti-Virus Center for descriptions. The remaining few alerts required further investigation. For the ICMP message regarding "Mobile Registration", I consulted RFC 2002 "IP Mobility Support" an explanation. I found a reference to "Printer-beavuh" on the SecurityFocus message boards. Seems some hacker nicknamed "Beavuh" discovered a buffer-overflow vulnerability. Finally, I used Google to find beetle.ucs and CS Webserver.

I used the same methodology for OOS and Scans with the exception of describing the alert. The second Charles Hutson script was used in each case.

Then, by using the 'grep', 'sed', and 'awk' utilities, I was able to sort by the amount of times a particular source address initiated communication. I was able to find the top ten talkers for alerts, scans and OOS. I then examined each listing, and again using the above utilities, I isolated anomalies such as port numbers, addresses and TCP bits.

Last Updated: July 27th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced