Global Information Assurance Certification Paper

SANS GIAC
Globally Certified Intrusion Analyst
(GCIA)

Practical Assignment Version 3.0
23 APR 2002

By Bradley D. Urwiller

Full Spectrum Intrusion Detection

Before you can begin your network analysis there are many tasks that must be accomplished. A network intrusion can occur on many different levels, a fact that is often ignored when discussing intrusion detection. Network activity is a fine indicator of an intrusion, yet before we can detect and classify an intruder we must establish knowledge of the network and its policies so that we can properly flag events for investigation. Therefore we must perform a sensor fusion that examines all layers of our network. Examining and understanding your internal policies at all layers of the network provides a vital situational awareness an analyst needs to sift through potential intrusions and false alarms. Further, this knowledge can provide insight as to the skill and knowledge of the intruder once found. The goal of this document is to cause the intrusion analyst to ask key questions and pursue a detailed understanding of the policies and baseline configuration of their network. Finally, the analyst must carefully review the methods of detection and analysis in order to minimize the risk of obfuscation of critical events.

Intrusion analysts should review their system security policies for the following areas at a minimum. We will discuss key questions in several areas but many must be explored by the analyst for there own network.

- Physical Access Control
- Resource Protection
- Logical Access Control
- Network Policy
- Configuration Management
- Hardware/Software Requirements and Controls
- Personnel Security
- Maintenance Policy

Many answers to the following questions may be found in your system security policy. If not, make sure you ask the security manager or appropriate official. Even if there is an area you had not considered before but cannot do anything about, having this knowledge will help you know what areas to provide special attention to. In the event of an incident it is better to show that a particular vulnerability was considered and found an acceptable residual risk than to be blind-sided.

Intrusions can be accomplished at a physical level in a variety of ways (i.e., access to network infrastructure, wire tap, physical intrusion at workstation/server). When an intrusion occurs you need to know where that intrusion is taking place, as much as the who and how. Consequently, a good physical and logical map of your network and information systems is vital to providing situational awareness of your network. It is vital to understand how current the map is and how rapidly it is updated when changes are made. Additionally, is the map checked for validity? Just because you thought a router was connected a certain way doesn't mean it is anymore. Networks change, with and without your permission.

Consider what physical countermeasures are in place to protect unattended workstations. Some measures may only be administrative policies, but are they being followed? Who has access and what policies are in place regarding maintenance of servers, switches and routers? Configuration management is key to maintaining a strong security posture. Understanding the configuration management process will aid the intrusion analyst in identifying potential intrusions from legitimate changes. If needed, are locks or alarms in place to prevent theft or damage? Who is alerted and what is the response plan?

One well known example both in failure to physically secure a system and failure to train users involves a remote network segment failure. The recurring network failure was finally attributed to a secretary that would disconnect the power to the router to plug in the coffee maker each morning while they brewed a fresh pot. While potentially not the concern of the intrusion analyst to enforce physical security and other system policies the analyst should know which systems are secured according to what policies.

As an intrusion analyst you likely have an intrusion detection system running on your network. Establishing a baseline for network traffic is a very difficult task. If you ask a network engineer what is 'good' traffic and what is 'bad' traffic you'll get very different responses. It pays to spend time establishing your own baseline then examine it in relation to your system security policy. For example, if your policy requires all administrators to use secure shell instead of telnet why is there a massive amount of telnet traffic appearing? Often times we find our network does not comply with our own policies. When this happens its important to either change the policy to reflect actual operations or document the exception to the rule. Rules established in your intrusion detection system should be carefully weighed. Every rule introduces a penalty in IO performance. Worse, if a rule fires false alarms frequently, we tend to adapt and ignore the events which are potentially legitimate alerts. When your IDS is running, who checks the log, how often, and how is it protected? Many intrusions go undetected because the intruder was able to erase their tracks from related log files. Consider a secured network device that simply records all traffic for offline analysis and historical archives.

Remember that all sensing devices, (IDS included), are probabilistic and not deterministic. This means that when an event occurs there is a probability that your sensor will detect it. Secondly, once it is detected there is the second probability that it will be perceived. As humans, anomalies that continually reveal themselves are eventually adapted into the 'norm' and are ignored by our perceptions. So even when an intrusion is sensed you may not perceive it, this probability increases with the frequency of the triggering event. This applies to IDS rules, log files, and all other data reviewed by the Intrusion Analyst. Data mining tools that are used to filter and sort event data should be carefully evaluated for effectiveness and reliability. These tools can greatly

reduce the risk an analyst will miss an event, but they can also allow an analyst to ignore a large quantity of signature data.

Host level countermeasures are extremely vital to the protection of a network. This includes not only BIOS and screensaver passwords but also malicious logic protection (anti-virus) and personal firewalls. Your individual environment will dictate which countermeasures are reasonable and sufficient (hopefully all). Yet you should also consider who can install software and who may have compilers? What are the password and internet usage policies? How do you determine if the host level policies are in effect or have been changed?

Many log files are generated by applications on an individual host. These log files are sources of invaluable information. If you do not collect logs on a centralized system you need to know how often log files are reviewed and how they are protected as well on each host that has them.

We've covered only a few of the basic questions that should be asked by an analyst stepping into their security role. Situational awareness and preparation for sensor fusion are vital steps an analyst should take before conducting their intrusion analysis. The Intrusion Analyst is in a unique position that requires them to bridge the gap between users, network administrators, and security manager. While maintaining their situational awareness, learning the system policies and baselines, they must retain their analytical skills for use when needed. Situational awareness and system policies simply provide a context to place intrusions in to aid in their detection and definition.

Bradley Urwiller

United States Air Force

References

DoDD 5200.28, Security Requirements for Automated Information Systems (AISs), March 21, 1988

DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985 (commonly referred to as the Orange Book)

DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997

DoD 5220.22-M National Industrial Security Program Operating Manual, January, 1995

1 Network Detection – ISS Scan

1.1 Trace Sample:

08:47:59.002636 INSIDER.MY.NET.2712 > TARGET.MY.NET.161: C=netman GetRequest(27) .1.3.6.1.2.1.1.1.0

08:47:59.002696 TARGET.MY.NET > INSIDER.MY.NET: icmp: TARGET.MY.NET udp port 161 unreachable

...

08:49:52.311397 INSIDER.MY.NET.4764 > TARGET.MY.NET.664: udp 40

08:49:52.311406 INSIDER.MY.NET.4764 > TARGET.MY.NET.665: udp 40

08:49:52.311413 INSIDER.MY.NET.4764 > TARGET.MY.NET.666: udp 40

08:49:52.311424 TARGET.MY.NET > INSIDER.MY.NET: icmp: TARGET.MY.NET udp port 664 unreachable

08:49:52.311429 TARGET.MY.NET > INSIDER.MY.NET: icmp: TARGET.MY.NET udp port 665 unreachable

08:49:52.311433 TARGET.MY.NET > INSIDER.MY.NET: icmp: TARGET.MY.NET udp port 666 unreachable

08:49:52.311559 INSIDER.MY.NET.4764 > TARGET.MY.NET.667: udp 40

08:49:52.311568 INSIDER.MY.NET.4764 > TARGET.MY.NET.668: udp 40

...

08:55:35.771517 INSIDER.MY.NET.2908 > TARGET.MY.NET.25: S 2199737628:2199737628(0) win 8192 <mss 1460> (DF)

08:55:35.771581 TARGET.MY.NET.25 > INSIDER.MY.NET.2908: R 0:0(0) ack 1 win 0

08:55:35.774668 INSIDER.MY.NET.2928 > TARGET.MY.NET.8888: udp 1036

08:55:35.774693 TARGET.MY.NET > INSIDER.MY.NET: icmp: TARGET.MY.NET udp port 8888 unreachable

1.2 Source of Trace:

Trace was collected from a private network.

1.3 Detect was generated by:

Having noted unusual amounts of activity on the workstation NIC, windump.exe was executed to capture the traffic for analysis.

1.4 Probability the source address was spoofed:

There is no chance the source address was spoofed. Using an offline database I was able to identify, locate, and stop the attacker. Let us assume however we didn't know this. Examining the captured traffic it is clear the

attacker is probing the victim's ports and looking for well known vulnerabilities. If the attacker spoofed the address the scan would serve no purpose except with two possibilities. If the spoofed address was compromised it is possible it has been setup as a listening post to collect reconnaissance data for the attacker. Secondly it is possible the intent was not reconnaissance but for a denial of service. The latter possibility is highly unlikely given there are much better tools available for establishing a denial of service. Further residual analysis indicated the attack swept the network but only a few hosts at a time. A successful DoS would require volumes of more traffic to have been effectual. The first possibility, although interesting, can be ruled out in this particular scenario given the culprit was actually caught on the original source address.

1.5 Description of attack:

Using an internally trusted address the attacker established an ISS scanner within the perimeter boundary. The ISS scan consists of TCP and UDP probes sequentially to each port, determining which are open. The sequential scan is conducted in blocks of 150 ports repeated 3 times before proceeding to next block of 150 ports. Additionally, the ISS scan initiates a number of vulnerability exploits to determine system weaknesses including SNMP community string guessing, and DNS version Bind. Many UDP packets carry the following payload (in hex):

55 44 50 20 53 63 61 6E 20 62 79 20 49 53 53 20

U D P S c a n b y I S S

1.6 Attack mechanism:

Through listening for TCP ACK's and ICMP unreachable messages the attacker determines those ports that are open on the target host. Successful responses to vulnerability probe would have indicated particular security vulnerabilities in the target host. This is a very noisy network reconnaissance probe.

1.7 Correlations:

This detect is indicative of ISS Scanner probes on a network.

1.8 Evidence of active targeting:

This was a general scan of the entire network. Log files generated from other hosts across multiple subnets were correlated to this attack.

1.9 Severity:

severity = (criticality + lethality) – (system countermeasures + network countermeasures) Each value should be ranked on a scale from 1 (lowest) to 5 (highest).	
Criticality is a measure of how	3, Network Admin desktop with

critical the targeted system is.	sensitive information.
Lethality is a measure of how severe the damage to the targeted system would be if the attack succeeded.	4, A successful IIS would reveal vulnerable exploits available on the host, potentially granting network admin access.
System countermeasures is a measure of the strength of the defensive mechanisms in place on the host itself.	4, Network sniffer, packet logging, fully patched and regulary scanned.
Network countermeasures is a measure of the strength of the defensive mechanisms in place on the network.	2, Core services hardened but host level very weak.
Severity Calculation:	**0** = (3+4) – (4+3)

1.10 Defensive recommendation:

Block ICMP responses on critical hosts deploy host level intrusion detection alert system for faster response time.

1.11 Multiple choice test question:

08:47:59.002636 INSIDER.MY.NET.2712 > TARGET.MY.NET.161: C=netman GetRequest(27) .1.3.6.1.2.1.1.1.0

08:47:59.002696 TARGET.MY.NET > INSIDER.MY.NET: icmp: TARGET.MY.NET udp port 161 unreachable

...

08:49:52.311397 INSIDER.MY.NET.4764 > TARGET.MY.NET.664: udp 40

08:49:52.311406 INSIDER.MY.NET.4764 > TARGET.MY.NET.665: udp 40

08:49:52.311413 INSIDER.MY.NET.4764 > TARGET.MY.NET.666: udp 40

08:49:52.311424 TARGET.MY.NET > INSIDER.MY.NET: icmp: TARGET.MY.NET udp port 664 unreachable

08:49:52.311429 TARGET.MY.NET > INSIDER.MY.NET: icmp: TARGET.MY.NET udp port 665 unreachable

08:49:52.311433 TARGET.MY.NET > INSIDER.MY.NET: icmp: TARGET.MY.NET udp port 666 unreachable

08:49:52.311559 INSIDER.MY.NET.4764 > TARGET.MY.NET.667: udp 40

08:49:52.311568 INSIDER.MY.NET.4764 > TARGET.MY.NET.668: udp 40

...

08:55:35.771517 INSIDER.MY.NET.2908 > TARGET.MY.NET.25: S 2199737628:2199737628(0) win 8192 <mss 1460> (DF)

08:55:35.771581 TARGET.MY.NET.25 > INSIDER.MY.NET.2908: R 0:0(0) ack 1 win 0

08:55:35.774668 INSIDER.MY.NET.2928 > TARGET.MY.NET.8888: udp 1036

08:55:35.774693 TARGET.MY.NET > INSIDER.MY.NET: icmp: TARGET.MY.NET udp port 8888 unreachable

Given the network trace above which of the following is the MOST LIKELY:

A) TARGET.MY.NET is running SNMP

B) TARGET.MY.NET has TCP Port 25 Open

C) This is an automated scan for SNMP servers

D) This is an automated general port SCAN

Answer: D, The target does not have SNMP port open nor port 25 and the scanner scans a wide range of ports beyond port 161.

2 Network Detection – Distributed Probe

2.1 Trace Sample:

```
03/06/02-13:07:29.091195 0:2:B9:A5:BF:63 -> 0:A0:C9:20:1A:3F type:0x800
len:0x4A
200.40.42.2:9466 -> xx.xx.xx.xx:22 TCP TTL:50 TOS:0x0 ID:12131 IpLen:20
DgmLen:60 DF
******S* Seq: 0x908F9800  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 6415570 0 NOP WS: 0
0x0000: 00 A0 C9 20 1A 3F 00 02 B9 A5 BF 63 08 00 45 00  ... .?.....c..E.
0x0010: 00 3C 2F 63 40 00 32 06 DE CE C8 28 2A 02 42 C8  .</c@xxxxxx(*.B.
0x0020: 05 98 24 FA 00 16 90 8F 98 00 00 00 00 00 A0 02  ..$.............
0x0030: 7D 78 5D 30 00 00 02 04 05 B4 04 02 08 0A 00 61  }x]0...........a
0x0040: E4 D2 00 00 00 00 01 03 03 00                    ..........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/06/02-13:07:32.085504 0:2:B9:A5:BF:63 -> 0:A0:C9:20:1A:3F type:0x800
len:0x4A
200.40.42.2:9466 -> xx.xx.xx.xx:22 TCP TTL:50 TOS:0x0 ID:12822 IpLen:20
DgmLen:60 DF
******S* Seq: 0x908F9800  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 6415870 0 NOP WS: 0
0x0000: 00 A0 C9 20 1A 3F 00 02 B9 A5 BF 63 08 00 45 00  ... .?.....c..E.
0x0010: 00 3C 32 16 40 00 32 06 DC 1B C8 28 2A 02 42 C8  .<2.@xxxxxx(*.B.
0x0020: 05 98 24 FA 00 16 90 8F 98 00 00 00 00 00 A0 02  ..$.............
0x0030: 7D 78 5C 04 00 00 02 04 05 B4 04 02 08 0A 00 61  }x\............a
0x0040: E5 FE 00 00 00 00 01 03 03 00                    ..........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/06/02-13:07:38.086451 0:2:B9:A5:BF:63 -> 0:A0:C9:20:1A:3F type:0x800
len:0x4A
200.40.42.2:9466 -> xx.xx.xx.xx:22 TCP TTL:50 TOS:0x0 ID:13883 IpLen:20
DgmLen:60 DF
******S* Seq: 0x908F9800  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 6416470 0 NOP WS: 0
0x0000: 00 A0 C9 20 1A 3F 00 02 B9 A5 BF 63 08 00 45 00  ... .?.....c..E.
0x0010: 00 3C 36 3B 40 00 32 06 D7 F6 C8 28 2A 02 42 C8  .<6;@.2....(*.B.
0x0020: 05 98 24 FA 00 16 90 8F 98 00 00 00 00 00 A0 02  ..$.............
0x0030: 7D 78 59 AC 00 00 02 04 05 B4 04 02 08 0A 00 61  }xY............a
0x0040: E8 56 00 00 00 00 01 03 03 00                    .V........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/06/02-15:02:07.301974 0:2:B9:A5:BF:63 -> 0:A0:C9:20:1A:3F type:0x800
len:0x4A
210.174.163.130:3436 -> xx.xx.xx.xx:111 TCP TTL:47 TOS:0x0 ID:28708 IpLen:20
DgmLen:60 DF
******S* Seq: 0x9942BB4C  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 235661285 0 NOP WS: 0
0x0000: 00 A0 C9 20 1A 3F 00 02 B9 A5 BF 63 08 00 45 00  ... .?.....c..E.
0x0010: 00 3C 70 24 40 00 2F 06 1D 07 D2 AE A3 82 42 C8  .<p$@./.......B.
0x0020: 05 98 0D 6C 00 6F 99 42 BB 4C 00 00 00 00 A0 02  ...l.o.B.L......
0x0030: 7D 78 B3 A2 00 00 02 04 05 B4 04 02 08 0A 0E 0B  }x..............
0x0040: E7 E5 00 00 00 00 01 03 03 00                    ..........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/06/02-17:52:14.490953 0:2:B9:A5:BF:63 -> 0:A0:C9:20:1A:3F type:0x800
len:0x4A
210.174.163.130:1831 -> xx.xx.xx.xx:111 TCP TTL:47 TOS:0x0 ID:44337 IpLen:20
DgmLen:60 DF
******S* Seq: 0x1B7C1D08  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 236681772 0 NOP WS: 0
0x0000: 00 A0 C9 20 1A 3F 00 02 B9 A5 BF 63 08 00 45 00  ... .?.....c..E.
0x0010: 00 3C AD 31 40 00 2F 06 DF F9 D2 AE A3 82 42 C8  .<.1@x/.......B.
0x0020: 05 98 07 27 00 6F 1B 7C 1D 08 00 00 00 00 A0 02  ...'.o.|........
0x0030: 7D 78 43 9C 00 00 02 04 05 B4 04 02 08 0A 0E 1B  }xC.............
0x0040: 7A 2C 00 00 00 00 01 03 03 00                    z,........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/06/02-21:41:42.058820 0:2:B9:A5:BF:63 -> 0:A0:C9:20:1A:3F type:0x800
len:0x4A
216.215.210.158:1578 -> xx.xx.xx.xx:22 TCP TTL:53 TOS:0x0 ID:32915 IpLen:20
DgmLen:60 DF
******S* Seq: 0xEA13BB30  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 10766293 0 NOP WS: 0
0x0000: 00 A0 C9 20 1A 3F 00 02 B9 A5 BF 63 08 00 45 00  ... .?.....c..E.
0x0010: 00 3C 80 93 40 00 35 06 D1 52 D8 D7 D2 9E 42 C8  .<..@xxxxxxxxxx
0x0020: 05 98 06 2A 00 16 EA 13 BB 30 00 00 00 00 A0 02  ...*.....0......
0x0030: 7D 78 E2 BA 00 00 02 04 05 B4 04 02 08 0A 00 A4  }x..............
0x0040: 47 D5 00 00 00 00 01 03 03 00                    G.........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/06/02-21:41:45.058387 0:2:B9:A5:BF:63 -> 0:A0:C9:20:1A:3F type:0x800
len:0x4A
```

```
216.215.210.158:1578 -> xx.xx.xx.xx:22 TCP TTL:53 TOS:0x0 ID:33327 IpLen:20
DgmLen:60 DF
******S* Seq: 0xEA13BB30  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 10766593 0 NOP WS: 0
0x0000: 00 A0 C9 20 1A 3F 00 02 B9 A5 BF 63 08 00 45 00  ... .?.....c..E.
0x0010: 00 3C 82 2F 40 00 35 06 CF B6 D8 D7 D2 9E 42 C8  .</@xxxxxxxxxx
0x0020: 05 98 06 2A 00 16 EA 13 BB 30 00 00 00 00 A0 02  ...*.....0......
0x0030: 7D 78 E1 8E 00 00 02 04 05 B4 04 02 08 0A 00 A4  }x..............
0x0040: 49 01 00 00 00 00 01 03 03 00                    I.........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/06/02-23:43:43.089523 0:2:B9:A5:BF:63 -> 0:A0:C9:20:1A:3F type:0x800
len:0x4A
202.46.29.15:3577 -> xx.xx.xx.xx:515 TCP TTL:41 TOS:0x0 ID:11273 IpLen:20
DgmLen:60 DF
******S* Seq: 0xF7BEDF51  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 5536203 0 NOP WS: 0
0x0000: 00 A0 C9 20 1A 3F 00 02 B9 A5 BF 63 08 00 45 00  ... .?.....c..E.
0x0010: 00 3C 2C 09 40 00 29 06 F6 15 CA 2E 1D 0F 42 C8  .<,.@x).......B.
0x0020: 05 98 0D F9 02 03 F7 BE DF 51 00 00 00 00 A0 02  .........Q......
0x0030: 7D 78 39 C5 00 00 02 04 05 B4 04 02 08 0A 00 54  }x9............T
0x0040: 79 CB 00 00 00 00 01 03 03 00                    y.........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/06/02-23:43:45.584093 0:2:B9:A5:BF:63 -> 0:A0:C9:20:1A:3F type:0x800
len:0x4A
202.46.29.15:3577 -> xx.xx.xx.xx:515 TCP TTL:41 TOS:0x0 ID:12339 IpLen:20
DgmLen:60 DF
******S* Seq: 0xF7BEDF51  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 5536503 0 NOP WS: 0
0x0000: 00 A0 C9 20 1A 3F 00 02 B9 A5 BF 63 08 00 45 00  ... .?.....c..E.
0x0010: 00 3C 30 33 40 00 29 06 F1 EB CA 2E 1D 0F 42 C8  .<03@x).......B.
0x0020: 05 98 0D F9 02 03 F7 BE DF 51 00 00 00 00 A0 02  .........Q......
0x0030: 7D 78 38 99 00 00 02 04 05 B4 04 02 08 0A 00 54  }x8............T
0x0040: 7A F7 00 00 00 00 01 03 03 00                    z.........
```

2.2 Source of Trace:

Trace taken from web posting by James C. Slora Jr. to incidents.org (**http://www.incidents.org/archives/intrusions/msg03507.html**), *Subject*: Ip Length 20 Datagram Length 60 TCP Window Size 7D78.

2.3 Detect was generated by:

The user had established monitoring on the host workstation and several others. Log file appears to have been generated by a recent release of tcpdump from a binary log file.

2.4 Probability the source address was spoofed:

Low, this appears to be a reconnaissance attempt (stimulus) not a response by the user or another system.

2.5 Description of attack:

A TCP connection is typically attempted by the attacker to one of the following ports (22, 23, 53, 111, 113, 515, 1080). Multiple source addresses probe through any single subnet suggesting a Distributed Probe utility is being used. Most packets share the following characteristics: IP Header length 20 (standard), Datagram length 60 (TCP Length: 40), TCP Window 0x7D78, with a negotiated MSS of 1460 and permitting selective acknowledgements.

These ports correspond to several CERT vulnerabilities (a selection listed below):

ssh	22/tcp	CA-2001-35, Recent Activity Against Secure Shell Daemons CA-1999-15, Buffer Overflows in SSH Daemon and RSAREF2 Library
telnet	23/tcp	CA-2001-21, Buffer Overflow in telnetd IN-2000-09, Systems Compromised Through a Vulnerability in the IRIX telnet daemon
domain	53/tcp53/udp	CA-2001-02, Multiple Vulnerabilities in BIND CA-2000-20, Multiple Denial-of-Service Problems in ISC BIND IN-2000-04, Denial of Service Attacks using Nameservers CA-2000-03, Continuing Compromises of Nameservers CA-1999-14, Multiple Vulnerabilities in BIND CA-1998-05, Multiple Vulnerabilities in BIND
sunrpc	111/tcp111/udp	CA-2001-05, Exploitation of snmpXdmid IN-2000-10, Widespread Exploitation of rcp.statd and wu-ftpd Vulnerabilities CA-2000-17, Input Validation Problem in rpc.statd CA-1999-16, Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind CA-1999-12, Buffer overflow in amd CA-1999-08, Buffer overflow in rpc.cmsd CA-1999-05, Vulnerability in statd exposes vulnerability in automountd CA-1998-12, Remotely Exploitable Buffer Overflow Vulnerability in mountd CA-1998-11, Vulnerability in ToolTalk RPC service
printer	515/tcp	VU#382365, LPRng can pass user-supplied input as a format string parameter to syslog() calls
socks	1080/tcp	VN-1998-03, WinGate IP Laundering

2.6 Attack mechanism:

This is a standard TCP port reconnaissance attempt. The similarity of the packets and the timing suggests either a distributed probe tool is being used in an attempt to perform a 'low and slow' scan of a network or a new script tool has been released. The TTL and window size of received packets suggests the Operating System being used is a Linux platform. Further investigation shows that a Linux platform IP stack would generate the characteristics of all the probe packets.

2.7 Correlations:

2.8 Evidence of active targeting:

There is little evidence of active targeting. While the probe attempt appears to be intentionally throttled in an attempt to avoid attention it has been reported across multiple subnets by multiple sources.

2.9 Severity:

severity = (criticality + lethality) – (system countermeasures + network countermeasures) Each value should be ranked on a scale from 1 (lowest) to 5 (highest).	
Criticality is a measure of how critical the targeted system is.	3, No detailed information of host network, must assume moderate risk.
Lethality is a measure of how severe the damage to the targeted system would be if the attack succeeded.	4, The ports probed have multiple well known vulnerabilities, if a host is vulnerable to any of these it could be compromised.
System countermeasures is a measure of the strength of the defensive mechanisms in place on the host itself.	3, There was no evidence or report of successful reconnessaince or vulnerabilities found.
Network countermeasures is a measure of the strength of the defensive mechanisms in place on the network.	2, Firewall or similar defenses failed to prevent the external host from scanning these well-known ports of the interior hosts.
Severity Calculation:	**2 =** (3+4) – (3+2)

2.10 Defensive recommendation:

Establish a NAT (network address translation) and bypass on the services necessary or alternatively block all unnecessary ports at the firewall and permit inbound traffic to specific IP address only to prevent general scans.

2.11 Multiple choice test question:

```
200.40.42.2:9466 -> xx.xx.xx.xx:22 TCP TTL:50 TOS:0x0
ID:12131 IpLen:20
DgmLen:60 DF
200.40.42.2:9466 -> xx.xx.xx.xx:22 TCP TTL:50 TOS:0x0
ID:12822 IpLen:20
DgmLen:60 DF
200.40.42.2:9466 -> xx.xx.xx.xx:22 TCP TTL:50 TOS:0x0
ID:13883 IpLen:20
DgmLen:60 DF
210.174.163.130:3436 -> xx.xx.xx.xx:111 TCP TTL:47 TOS:0x0
ID:28708 IpLen:20
DgmLen:60 DF
```

```
210.174.163.130:1831 -> xx.xx.xx.xx:111 TCP TTL:47 TOS:0x0
ID:44337 IpLen:20
DgmLen:60 DF
216.215.210.158:1578 -> xx.xx.xx.xx:22 TCP TTL:53 TOS:0x0
ID:32915 IpLen:20
DgmLen:60 DF
216.215.210.158:1578 -> xx.xx.xx.xx:22 TCP TTL:53 TOS:0x0
ID:33327 IpLen:20
DgmLen:60 DF
202.46.29.15:3577 -> xx.xx.xx.xx:515 TCP TTL:41 TOS:0x0
ID:12339 IpLen:20
DgmLen:60 DF
```

The above trace is most likely an example of:

A) Queso Fingerprint

B) DDoS

C) Distributed network probe

D) Crafted packets designed to OS fingerprint

Answer C, the trace does not bear the signature for Queso Fingerprints. Further the varied ports do not strongly indicate a DDOS. The best answer therefore is a distributed probe.

3 Network Detection – Port 50000

3.1 Trace Sample:

```
08:24:50.651213 193.61.29.239.4092 > My.NetcacheServer16.3.50000: S
1038560942:1038560942(0) win 16384  (DF)
08:24:53.559636 193.61.29.239.4092 > My.NetcacheServer16.3.50000: S
1038560942:1038560942(0) win 16384  (DF)
08:24:59.579282 193.61.29.239.4092 > My.NetcacheServer16.3.50000: S
1038560942:1038560942(0) win 16384  (DF)
08:25:11.620126 193.61.29.239.4109 > My.NetcacheServer16.3.50000: S
1044814715:1044814715(0) win 16384  (DF)
08:25:14.627656 193.61.29.239.4109 > My.NetcacheServer16.3.50000: S
1044814715:1044814715(0) win 16384  (DF)
08:25:20.646449 193.61.29.239.4109 > My.NetcacheServer16.3.50000: S
1044814715:1044814715(0) win 16384  (DF)
08:37:06.138490 My.NetcacheServer46.212.2187 > 193.61.29.239.50000: S
4066426179:4066426179(0) win 16384  (DF)

08:25:51.087592 24.207.218.242.2140 > My.NetcacheServer16.3.50000: S
2138749139:2138749139(0) win 64240  (DF)
08:25:51.089466 My.NetcacheServer16.3.50000 > 24.207.218.242.2140: R 0:0(0) ack
2138749140 win 0
08:25:51.594110 24.207.218.242.2140 > My.NetcacheServer16.3.50000: S
2138749139:2138749139(0) win 64240  (DF)
08:25:51.595661 My.NetcacheServer16.3.50000 > 24.207.218.242.2140: R 0:0(0) ack
2138749140 win 0
08:25:52.079107 24.207.218.242.2140 > My.NetcacheServer16.3.50000: S
2138749139:2138749139(0) win 64240  (DF)
08:25:52.080849 My.NetcacheServer16.3.50000 > 24.207.218.242.2140: R 0:0(0) ack
2138749140 win 0
08:25:52.135815 24.207.218.242.2141 > My.NetcacheServer16.3.50000: S
2139044495:2139044495(0) win 64240  (DF)
08:25:52.138344 My.NetcacheServer16.3.50000 > 24.207.218.242.2141: R 0:0(0) ack
2139044496 win 0

13:47:07.864620 208.166.224.60.42388 > My.NetcacheServer16.3.50000: S
3291145576:3291145576(0) win 16384  (DF)
13:47:07.866366 My.NetcacheServer16.3.50000 > 208.166.224.60.42388: R 0:0(0) ack
3291145577 win 0
13:47:08.397476 208.166.224.60.42388 > My.NetcacheServer16.3.50000: S
3291145576:3291145576(0) win 16384  (DF)
13:47:08.399129 My.NetcacheServer16.3.50000 > 208.166.224.60.42388: R 0:0(0) ack
3291145577 win 0
13:47:08.894692 208.166.224.60.42388 > My.NetcacheServer16.3.50000: S
3291145576:3291145576(0) win 16384  (DF)
13:47:08.894886 My.NetcacheServer16.3.50000 > 208.166.224.60.42388: R 0:0(0) ack
3291145577 win 0
13:47:08.962017 208.166.224.60.42389 > My.NetcacheServer16.3.50000: S
3291482005:3291482005(0) win 16384  (DF)
13:47:08.962150 My.NetcacheServer16.3.50000 > 208.166.224.60.42389: R 0:0(0) ack
3291482006 win 0

08:26:54.718873 212.38.188.66.1631 > My.NetcacheServer16.3.50000: S
3140344624:3140344624(0) win 64240  (DF)
08:26:57.597245 212.38.188.66.1631 > My.NetcacheServer16.3.50000: S
3140344624:3140344624(0) win 64240  (DF)
08:27:03.633648 212.38.188.66.1631 > My.NetcacheServer16.3.50000: S
3140344624:3140344624(0) win 64240  (DF)
08:27:15.606421 212.38.188.66.1632 > My.NetcacheServer16.3.50000: S
3145588744:3145588744(0) win 64240  (DF)
08:27:18.624528 212.38.188.66.1632 > My.NetcacheServer16.3.50000: S
3145588744:3145588744(0) win 64240  (DF)
08:27:24.659473 212.38.188.66.1632 > My.NetcacheServer16.3.50000: S
3145588744:3145588744(0) win 64240  (DF)
```

3.2 Source of Trace:

Trace taken from web posting by Carey, Steve T ISD to incidents.org (http://www.incidents.org/archives/intrusions/msg04547.html), *Subject*: Port 50000 Connections.

3.3 Detect was generated by:

3.4 Probability the source address was spoofed:

Low, this appears to be a reconnaissance attempt (stimulus) not a response by the user or another system.

3.5 Description of attack:

User reported numerous connections as shown in the trace inbound requesting TCP port 50000 to the web proxy server. On a few occasions internal users established outbound connections on port 50000.

Responding individuals reported several university systems participating in a 'Bolo' game that utilizes ports 50000-50005. This theory bears out to the extent that some of the connecting hosts belong to universities:

```
inetnum:        193.61.23.0 - 193.61.63.255
netname:        BIRKBECK
descr:          Birkbeck College
country:        GB
admin-c:        KB2711-RIPE
tech-c:         KB2711-RIPE
status:         ASSIGNED PA
notify:         jips-nosc@xxxxxxxxxxx
mnt-by:         JANET-HOSTMASTER
changed:        kevin@xxxxxxxxxxxx 19930310
changed:        kevin@xxxxxxxxxxx 19931206
changed:        ripe-dbm@xxxxxxxx 19990706
changed:        ripe-dbm@xxxxxxxx 20000225
changed:        hostmaster@xxxxxxxxxx 20010920
changed:        hostmaster@xxxxxxxxxx 20011024
source:         RIPE

route:          193.60.0.0/14
descr:          JANET
descr:          c/o ULCC
descr:          20 Guilford Street
descr:          London
descr:          WC1N 1DZ
descr:          UNITED KINGDOM
origin:         AS786
mnt-by:         JIPS-NOSC
changed:        selina@xxxxxxx 19951011
source:         RIPE

person:         Kevin Brunt
address:        Central Computing Services
address:        Birkbeck College
address:        Malet Street
address:        London WC1E 7HX
address:        United Kingdom
phone:          +44 71 631 6557
```

```
e-mail:        kevin@xxxxxxxxxxxx
nic-hdl:       KB2711-RIPE
changed:       kevin@xxxxxxxxxxx 19931206
changed:       ripe-dbm@xxxxxxxx 19990615

Registrant Data
Registrant id#: 1
Domain Name: bbk.ac.uk
Registered For: Birkbeck College
Domain Registered By: JANET
Record updated on 28-Feb-2002 by naming-admin@xxxxxxxxxxx
Delegated Name Servers:
   BAS-A.BCC.AC.UK
   LINK-1.TS.BCC.AC.UK
   NS0.JA.NET
```

3.6 Attack mechanism:

Remote hosts request a TCP connection to the web proxy for port 50000. After repeated attempts the TCP request times out (after standard 3,6,12 second retries). A legitimate probe for port 50000 would likely have scanned more IP addresses than just the web proxy. However this may be an attempt to locate the SubSARI 1.0 - 1.2 trojan.

3.7 Correlations:

There have been no other recent correlations that would indicate recent increase in the SubSARI Trojan or ICU II vulnerability scans.

3.8 Evidence of active targeting:

This was active targeting. This traffic appears to be the response to a user supplied stimulus. Does not appear to be port scan at this time.

3.9 Severity:

Severity = (criticality + lethality) – (system countermeasures + network countermeasures) Each value should be ranked on a scale from 1 (lowest) to 5 (highest).	
Criticality is a measure of how critical the targeted system is.	3, No detailed information of host network, must assume moderate risk.
Lethality is a measure of how severe the damage to the targeted system would be if the attack succeeded.	4, The ports probed have multiple well known vulnerabilities, if a host is vulnerable to any of these it could be compromised.
System countermeasures is a measure of the strength of the defensive mechanisms in place on the host itself.	3, There was no evidence or report of successful reconnaissance or vulnerabilities found.

Network countermeasures is a measure of the strength of the defensive mechanisms in place on the network.	2, Firewall or similar defenses failed to prevent the external host from scanning these well-known ports of the interior hosts.
Severity Calculation:	**2 =** (3+4) – (3+2)

3.10 Defensive recommendation:

The attack in this example appears to be non malicious use of a university game server. However, there are a number of vulnerabilities associated with TCP port 50000 for Videoconferencing (such as ICU II), as well as a Trojan (SubSARI 1.0 - 1.2). Repeat connections to port 50000 should be closely monitored. Inquiries to users to verify if they have been playing games should be done to verify the nature of the threat.

3.11 Multiple choice test question:

```
08:24:50.651213 193.61.29.239.4092 >
My.NetcacheServer16.3.50000: S 1038560942:1038560942(0) win
16384  (DF)
08:24:53.559636 193.61.29.239.4092 >
My.NetcacheServer16.3.50000: S 1038560942:1038560942(0) win
16384  (DF)
08:24:59.579282 193.61.29.239.4092 >
My.NetcacheServer16.3.50000: S 1038560942:1038560942(0) win
16384  (DF)
08:25:11.620126 193.61.29.239.4109 >
My.NetcacheServer16.3.50000: S 1044814715:1044814715(0) win
16384  (DF)
08:25:14.627656 193.61.29.239.4109 >
My.NetcacheServer16.3.50000: S 1044814715:1044814715(0) win
16384  (DF)
08:25:20.646449 193.61.29.239.4109 >
My.NetcacheServer16.3.50000: S 1044814715:1044814715(0) win
16384  (DF)
08:37:06.138490 My.NetcacheServer46.212.2187 >
193.61.29.239.50000: S 4066426179:4066426179(0) win 16384
(DF)
```

Which of the following is most likely:

A) This is a SubSARI Trojan call

B) This is a low and slow port scan

C) This is a failed TCP connection

D) This is a successful reconnaissance attempt

The correct answer is C, Notice the timing of the TCP connection requests, and lack of response from the destination port.

4 Network Detection – Net Controller

4.1 Trace Sample:

```
Mar 12 20:04:08 - snort [1:0:0] TCP to 123 ntp
  Source IP: 211.184.140.152   Source port: 2310
Source host: 211.184.140.152
  Target IP: 12.82.141.8   Target port: 123   Proto: TCP
Target host: 8.seattle-15-20rs.wa.dial-access.att.net
```

```
snort packet capture:
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/12-20:04:08.441571 211.184.140.152:2310 -> 12.82.141.8:123
TCP TTL:42 TOS:0x0 ID:54713 IpLen:20 DgmLen:60 DF
******S* Seq: 0xFE8C9E93  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 78715899 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

4.2 Source of Trace:

Trace taken from log files of John Sage provided at http://www.finchhaven.com/pages/incidents/

4.3 Detect was generated by:

Snort IDS

4.4 Probability the source address was spoofed:

Low, as a reconnaissance tool or legitimate use of NTP spoofing the source IP address would circumvent any usefulness of the attempt. There is not sufficient volume to assume this is a DoS. Potential wrong number.

4.5 Description of attack:

A TCP SYN packet is sent to port 123. NTP is the Network Time Protocal and typicall resides on port 123. It is used to synchronize time clocks on servers (primarily unix based). NTP however is predominantly UDP. Most TCP usages of port 123 belong to the NetController Windows Trojan. A lookup of the source IP address reveals that 211.184.140.152 belongs to:

inetnum	**211.184.140.128 - 211.184.140.191**
netname	BOSUNG-GMS-KR
descr	BOSUNG GIRL MIDDLE SCHOOL
descr	295-3 USANRI BOSEONGEUB BOSEONGKUN
descr	CHONNAM
descr	546-800
country	KR
admin-c	JJ1852-KR, inverse
tech-c	JJ1853-KR, inverse
remarks	This IP address space has been allocated to KRNIC.
remarks	For more information, using KRNIC Whois Database

remarks whois -h whois.nic.or.kr
remarks This information has been partially mirrored by APNIC from
remarks KRNIC. To obtain more specific information, please use the
remarks KRNIC whois server at whois.krnic.net.
mnt-by MNT-KRNIC-AP, inverse
changed hostmaster@nic.or.kr 20020415
source KRNIC

4.6 Attack mechanism:

Per http://www.simovits.com/trojans/tr_data/y1142.html:

Name: Net Controller
Aliases:
Ports: 123, 6969 (ports can be changed)
Files: Netcontroller.zip - 614,439 bytes Netcontroller2000.zip - 719,774 bytes Netctrlr.exe - 314,368 bytes Netctrlr.exe - 374,272 bytes Netsrvr.exe - 306,688 bytes Netsrvr.exe - 351,232 bytes System.exe - Config.ini - 4,087 bytes Config.ini - 3,633 bytes
Created: July 1999
Requires:
Actions: Remote Access / Keylogger / FTP server
The client is similar to the older versions of NetBus.
Versions: 1.08, 2000,
Registers:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\windows\CurrentVersion\Run\
Notes: Works on Windows 95, 98, ME and NT.
Country: written in Brazil
Program:

Net Controller is a Trojan that is very similar to NetBus.

4.7 Correlations:

Cert does not presently show active amounts of targeting for the NetController Trojan. However given the unusual nature of the packet (TCP versus UDP), the source origination is a middle school, there is a large possibility this was a genuine Trojan probe versus a misdialed NTP sync.

4.8 Evidence of active targeting:

None, as there has not been repeated activity from the source host it is likely this was part of a general Trojan sweep.

4.9 Severity:

Severity = (criticality + lethality) – (system countermeasures + network countermeasures) Each value should be ranked on a scale from 1 (lowest) to 5 (highest).	
Criticality is a measure of how	2, Personal PC, potential for financial,

critical the targeted system is.	business or identity data loss.
Lethality is a measure of how severe the damage to the targeted system would be if the attack succeeded.	4, If the targeted host was infected this probe may have resulted in the loss of the host.
System countermeasures is a measure of the strength of the defensive mechanisms in place on the host itself.	4, host level IDS and packet monitoring
Network countermeasures is a measure of the strength of the defensive mechanisms in place on the network.	4, Use of firewall, IDS and NFR
Severity Calculation:	**-2 =** (2+4) – (4+4)

4.10 Defensive recommendation:

Not specifically stated if network address translation is being used by the personal network. This is highly recommended for continual internet exposure.

4.11 Multiple choice test question:

Given that NTP is predominantly a UDP protocol how should the following be classified?

```
03/12-20:04:08.441571 211.184.140.152:2310 ->
12.82.141.8:123
TCP TTL:42 TOS:0x0 ID:54713 IpLen:20 DgmLen:60 DF
******S* Seq: 0xFE8C9E93  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 78715899 0 NOP WS:
0

WHOIS Excerpt:
inetnum              211.184.140.128 - 211.184.140.191
netname              BOSUNG-GMS-KR
descr                BOSUNG GIRL MIDDLE SCHOOL
```

A) Denial of Service

B) Port reconnaissance or Trojan search

C) Out of Spec Data packet

D) A and D

E) B and C

The correct answer is E. While this is likely to be a Trojan search we cannot conclusively prove this based on the data provided. Therefore it could be simply an Out of Spec datagram.

5 Network Detection – ICMP Unreachable

5.1 Trace Sample:

```
[**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**]
02/05-15:07:53.061214 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1090 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:63363 IpLen:20 DgmLen:44
Seq: 0xA32ECF4F
** END OF DUMP
45 00 00 2C F7 83 40 00 EF 06 E0 BD D8 CE 5A 02  E..,..@xxxxxxxxx
98 32 E8 86 00 19 08 01 A3 2E CF 4F              .2.........O

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**]
02/05-15:07:55.957378 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1091 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:63364 IpLen:20 DgmLen:40
Seq: 0xA32ECF50
** END OF DUMP
45 00 00 28 F7 84 40 00 EF 06 E0 C0 D8 CE 5A 02  E..(..@xxxxxxxxx
98 32 E8 86 00 19 08 01 A3 2E CF 50              .2.........P

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**]
02/05-15:08:02.160527 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1096 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:63366 IpLen:20 DgmLen:40
Seq: 0xA32ECF50
** END OF DUMP
45 00 00 28 F7 86 40 00 EF 06 E0 BE D8 CE 5A 02  E..(..@xxxxxxxxx
98 32 E8 86 00 19 08 01 A3 2E CF 50              .2.........P

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**]
02/05-15:08:03.224922 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1097 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:63367 IpLen:20 DgmLen:44
Seq: 0xA32ECF4F
** END OF DUMP
45 00 00 2C F7 87 40 00 EF 06 E0 B9 D8 CE 5A 02  E..,..@xxxxxxxxx
98 32 E8 86 00 19 08 01 A3 2E CF 4F              .2.........O

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**]
02/05-15:08:14.006581 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1098 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:63368 IpLen:20 DgmLen:40
Seq: 0xA32ECF50
```

```
** END OF DUMP
45 00 00 28 F7 88 40 00 EF 06 E0 BC D8 CE 5A 02  E..(..@xxxxxxxxx
98 32 E8 86 00 19 08 01 A3 2E CF 50              .2.........P

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**]
02/05-15:08:16.673466 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1099 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:63369 IpLen:20 DgmLen:44
Seq: 0xA32ECF4F
** END OF DUMP
45 00 00 2C F7 89 40 00 EF 06 E0 B7 D8 CE 5A 02  E..,..@xxxxxxxxx
98 32 E8 86 00 19 08 01 A3 2E CF 4F              .2.........O

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**]
02/05-15:08:43.683633 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1104 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:63370 IpLen:20 DgmLen:44
Seq: 0xA32ECF4F
** END OF DUMP
45 00 00 2C F7 8A 40 00 EF 06 E0 B6 D8 CE 5A 02  E..,..@xxxxxxxxx
98 32 E8 86 00 19 08 01 A3 2E CF 4F              .2.........O

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**]
02/05-15:09:37.669110 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1116 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:36911 IpLen:20 DgmLen:44
Seq: 0xA32ECF4F
** END OF DUMP
45 00 00 2C 90 2F 40 00 EF 06 48 12 D8 CE 5A 02  E..,./@xxxxxxxxx
98 32 E8 86 00 19 08 01 A3 2E CF 4F              .2.........O

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**]
02/05-15:10:37.840949 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1128 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:31375 IpLen:20 DgmLen:44
Seq: 0xA32ECF4F
** END OF DUMP
45 00 00 2C 7A 8F 40 00 EF 06 5D B2 D8 CE 5A 02  E..,z.@xxx]...Z.
98 32 E8 86 00 19 08 01 A3 2E CF 4F              .2.........O

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**]
02/05-15:11:37.703355 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1142 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:25839 IpLen:20 DgmLen:40
Seq: 0xA32ECF50
** END OF DUMP
```

```
45 00 00 28 64 EF 40 00 EF 06 73 56 D8 CE 5A 02  E..(d.@xxxxxxxxx
98 32 E8 86 00 19 08 01 A3 2E CF 50              .2........P

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

5.2 Source of Trace:

Posted by Ray Nichols to http://www.incidents.org/archives/intrusions/msg03095.html Subject: ICMP Traffic Help.

5.3 Detect was generated by:

SNORT IDS

5.4 Probability the source address was spoofed:

Low, based on the whois records below it would appear this is a result of a policy based rule for the router connecting Lord Corporation to the Internet.

5.4.1 216.54.219.98

```
Time Warner Telecom (NETBLK-TWTC-DRHM-I-DS1IFAC-
1)
   3235 Intertech Drive
   Brookfield, WI 53045
   US

   Netname: TWTC-DRHM-I-DS1IFAC-1
   Netblock: 216.54.219.0 - 216.54.219.255

   Coordinator:
      Time Warner Telecom  (HOS8-ORG-ARIN)
hostmaster@twtelecom.net
      800-898-6473

   Record last updated on 28-Jun-2000.
   Database last updated on  21-Apr-2002 19:57:48
EDT.
```

5.4.2 152.40.232.134

```
Lord Corporation (NET-LORD-NET)
   405 Gregson Drive
   Cary, NC 27511-7900
   US

   Netname: LORD-NET
   Netblock: 152.50.0.0 - 152.50.255.255

   Coordinator:
```

```
      Stribling, Tom  (TS1-ARIN)
tom_stribling@lord.com
      (919) 469-3443 ext. 2704 ext. 404 (FAX)
(919) 469-9114

   Domain System inverse mapping provided by:

   LORDNS1.CRD.LORD.COM          152.50.232.151
   LORDNS2.CPD.LORD.COM          152.50.61.1
   NCNOC.NCREN.NET         192.101.21.1
   REGGAE.NCREN.NET        128.109.131.3

   Record last updated on 31-Jan-2001.
   Database last updated on  21-Apr-2002 19:57:48
EDT.
```

5.5 Description of attack:

Host reports receiving large number of ICMP packet unreachable(s) that match the trace sample above. Appears that a client at LORD-NET is connecting to a mail server at the host network. An intermediated device (216.54.219.98) intercepts the packet and refuses the traffic. This refusal is possible due to the destination port (2049) which is used by NFS. This may be a self defense mechanism by LORD-NET or its ISP to prevent NFS exploits from the internet.

5.6 Attack mechanism:

An ICMP Unreachable message of this nature is returned by a router when a policy has been set to restrict access to a particular host (or range) or port.

5.7 Correlations:

ICMP Unreachable messages are extremely common and despite multitudes of ICMP Unreachable messages in conjunction with mail services there do not appear to be direct correlation of source, destination, or ports. The likely hood that this is a DoS is minimal. Care should be taken though to monitor the growth rate of ICMP unreachable received and the ports used.

5.8 Evidence of active targeting:

None, this appears to be a misconfiguration by the destination to use the NFS port.

5.9 Severity:

Severity = (criticality + lethality) – (system countermeasures + network countermeasures) Each value should be ranked on a scale from 1 (lowest) to 5 (highest).

Criticality is a measure of how critical the targeted system is.	4, SMTP is a mail service. Large number of vulnerabilities and potential exploits
Lethality is a measure of how severe the damage to the targeted system would be if the attack succeeded.	4, Potential for DoS launching pad, loss of corporate image and potentially sensitive data.
System countermeasures is a measure of the strength of the defensive mechanisms in place on the host itself.	3, There was no evidence that the SMTP server itself is protected. We assume that minimal protection is used such as updates, patching, and anti-virus.
Network countermeasures is a measure of the strength of the defensive mechanisms in place on the network.	3, The presence of an IDS suggests there is also a firewall present (hopefully). These devices do not appear to have been configured to filter traffic to reduce workload however increasing risk of attack.
Severity Calculation:	**2 =** (4+4) – (3+3)

5.10 Defensive recommendation:

Recommend that the destination router silence the administrative ICMP replies. This enables a would-be hacker to learn the administrative security policies and rule set too easily. Further, the host should verify if traffic to/from the destination host was acceptable if not consider filtering/blocking this traffic.

5.11 Multiple choice test question:

```
[**] ICMP Destination Unreachable (Communication
Administratively Prohibited) [**]
02/05-15:07:53.061214 216.54.219.98 -> x.x.x.2
ICMP TTL:242 TOS:0x0 ID:1090 IpLen:20 DgmLen:56
Type:3  Code:13  DESTINATION UNREACHABLE: PACKET FILTERED
** ORIGINAL DATAGRAM DUMP:
x.x.x.2:25 -> 152.50.232.134:2049
TCP TTL:239 TOS:0x0 ID:63363 IpLen:20 DgmLen:44
Seq: 0xA32ECF4F
** END OF DUMP
45 00 00 2C F7 83 40 00 EF 06 E0 BD D8 CE 5A 02
E..,..@xxxxxxxxx
98 32 E8 86 00 19 08 01 A3 2E CF 4F
.2.........O
```

Which of the following is correct:

A) x.x.x.2 is attempting to connect to NFS (port 2049) on host 152.50.232.134

B) 152.50.232.134 is attempting to connect to SMTP (port 25) on host x.x.x.2

C) 216.54.219.98 is a router

D) A and B

E) B and C

The correct answer is E. ICMP Unreachable messages are generated by a router, further the trace is indicative of a TCP connect request on port 25.

1 "Analyze This" Scenario - Executive Summary

This analysis covers the period of 01 APR 2002 to 05 APR 2002 for the University Network. Data was compiled from the following source files:

alert.020401.gz	alert.020402.gz	alert.020403.gz
alert.020404.gz	alert.020405.gz	oos_Apr.1.2002.gz
oos_Apr.2.2002.gz	oos_Apr.3.2002.gz	oos_Apr.4.2002.gz
oos_Apr.5.2002.gz	scans.020401.gz	scans.020402.gz
scans.020403.gz	scans.020404.gz	scans.020405.gz

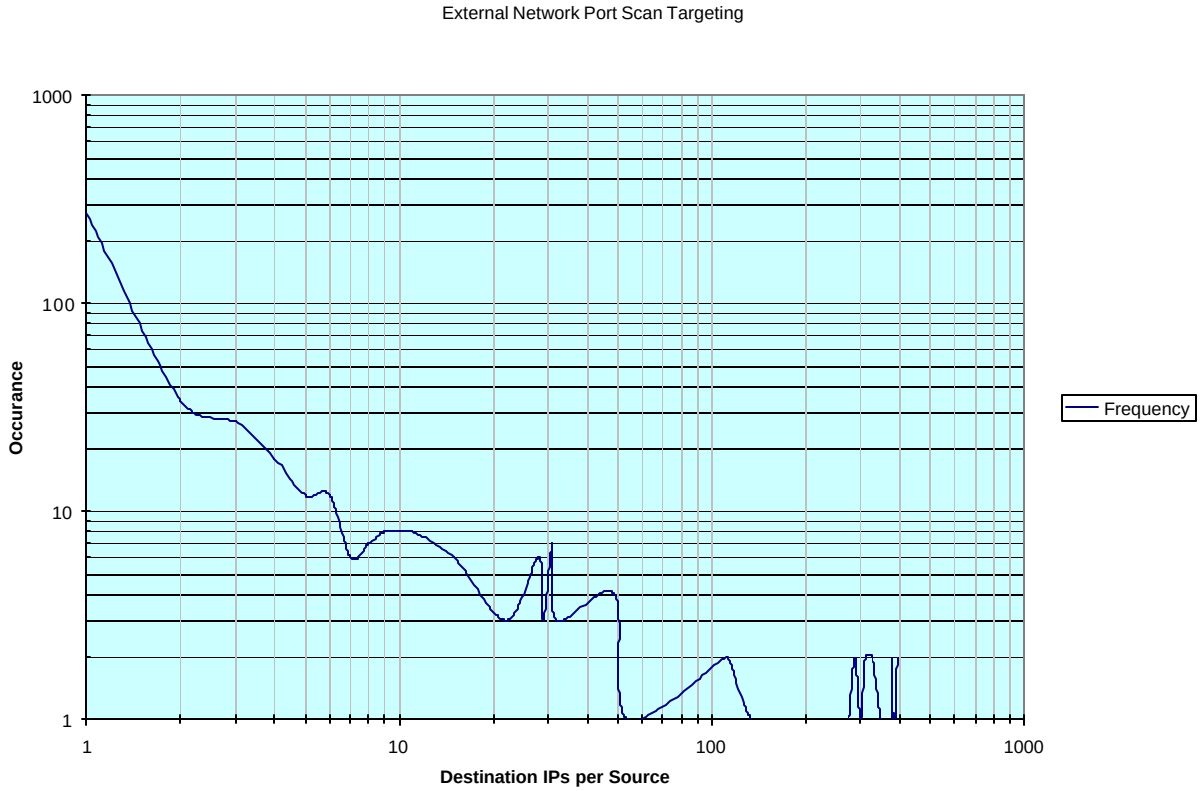
The University network suffers from a number of vulnerabilities and threats which are summarized here. Most internal traffic scans consist of HTTP, FTP and UNIX protocols. There is a large amount of machines search for MSN Gaming Zone and Peer-to-Peer servers. A larger number of network scans probe the internal network from external addresses looking for Peer-to-Peer (P2P) Clients such as KAZAA and GNUTella.

Some threats previously identified on the network are growing in severity such as the internal port 515 access, and Large UDP Packets. These threats have been noted in several of the previous GIAC Practical assignments.

The security policy for the network should be reviewed to eliminate a number of these threats/vulnerabilities.

2 Scans Log Analysis

The Scans Log includes 861 unique Source addresses. Of these, 346 originated outside of the home network. The following graph illustrates the rate of occurrence for the distribution of port scans. Approximately 86% of all external port scans (inbound) targeted fewer than 10 internal IP addresses. These focused scans (fewer than 10 internal addresses) probed a collective group of 106 internal IP addresses (those with fewer than 5 internal addresses probed a group of 81 internal addresses).

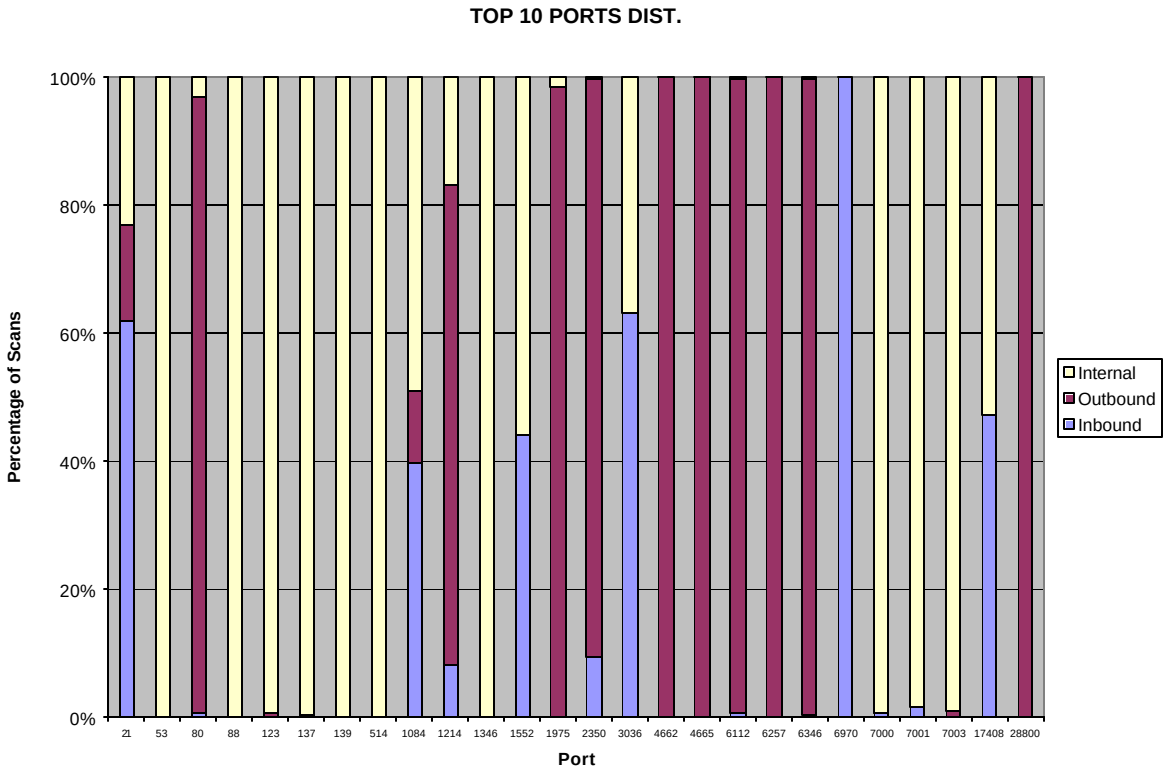


2.1 Port Analysis

2.1.1 Internal Traffic

TOP 10 INTERNAL SCANNED PORTS

Port	Inbound	Outbound	Internal	IANA Registered Service	Known Trojans
7001	7,212	0	483,673	afs3-callback	Freak88
7000	1,833	194	277,397	afs3-fileserver	Exploit Translation Server, Kazimas, Remote Grab, SubSeven 2.1 Gold
53	39	25	199,280	domain	
514	17	0	89,809	syslog	RPC Backdoor
1346	15	0	89,331	alta-ana-lm	
137	28	142	75,234	netbios-ns	
7003	5	346	35,912	afs3-vlserver	
123	18	154	27,009	ntp	
88	6	24	24,660	kerberos	
139	5	12	20,907	netbios-ssn	



Examining the top scanned ports for internal traffic we surmise the following:

The internal network utilizes a series of servers that run AFS. AFS provides a method for accessing network file servers in a reasonable and scalable manner. From a user standpoint, it's much like SMB/CIFS and Appleshare. AFS is dependent on Kerberos authentication so we should expect to see it in the top list as well (which we do for internal traffic). The remaining internal traffic appears to be fairly standard for any university network. We see a number of port scans for Netbios, network time protocol, syslog, etc. Port 1346 could be of concern unless the network is truly using Alta Analytics License Manager.

2.1.2 Inbound Traffic

TOP 10 INBOUND SCANNED PORTS

Port	Inbound	Outbound	Internal	IANA Registered Service	Known Trojans
6970	12,130	0	12	RealAudio Incoming Audio Streams	GateCrasher
7001	7,212	0	483,673	afs3-callback	Freak88

1552	5,051	0	6,406	pciarray	
80	2,304	387,224	12,736	HTTP	AckCmd, Back End, CGI Backdoor, Executor, Hooker, RingZero
21	1,998	487	750	FTP	Back Construction, Blade Runner, Doly Trojan, Fore, Invisible FTP, Juggernaut 42 , Larva, Motlv FTP, Net Administrator, Senna Spy FTP server, Traitor 21, WebEx, WinCrash
7000	1,833	194	277,397	afs3-fileserver	Exploit Translation Server, Kazimas, Remote Grab, SubSeven 2.1 Gold
1084	1,211	344	1,489	Anasoft License Manager	
3036	1,077	0	629	Hagel DUMP	
2350	994	9,368	54	psbserver	
17408	979	0	1,095		

Half of the Inbound port scans are fairly typical, such as for web servers, ftp, real audio, and the AFS shares we discussed above. However the remaining port scans draw some concern (ports 1084, 3036,17408), in particular as port 17408 has no assigned service and we see a large number of probes both internally and inbound looking for this port. Perhaps there are compromised machines, or simply a misconfigured service.

In a corporate environment the perimeter defenses are most often set to deny all connections and ports except those explicitly allowed. Since this is a university it may not be practical to block NetBios, and the AFS shares from external access. This is especially true if this network space provides access to dorm students. If this is the case, non-dorm users and systems that shouldn't be publicly accessible should be protected behind a specially configured firewall to block access to these common ports.

2.1.3 Outbound Traffic

TOP 10 OUTBOUND SCANNED PORTS

Port	Inbound	Outbound	Internal	IANA Registered Service	Known Trojans
80	2,304	387,224	12,736	HTTP	AckCmd, Back End, CGI Backdoor, Executor, Hooker, RingZero
4665	16	145,175	45	Edonkey2000	
28800	5	101,538	79	MSN GameZone	
4662	26	37,031	26	Edonkey2000	
2350	994	9,368	54	psbserver	
6257	1	9,113	4		

1975	0	5,819	103	tcoflashagent	
6112	31	5,626	16	dtspcd	
6346	14	3,765	16	gnutella-svc	
1214	393	3,675	835	KAZAA	

Some outbound scans appear fairly harmless depending on our campus use policy. We see a number of users making use of potentially dangerous P2P clients such as EDonkey2000, GNUTELLA and KAZAA. Gaming on Microsoft's GameZone appears to be big as well. Port 1975 could be an undocumented Trojan or more likely is a variant of the Go!zilla style of web marketing (advertising data is pulled on port 1975 by some companies such as http://www.aureate.com). Port 6112 is of concern as there is a recent vulnerability identified in the Common Desktop Environment. Since most traffic is outbound on this port, it is unlikely that this is malicious (if we can trust our users…).

Port 6257 is of concern as there is no registered service or Trojan for this port. We have the potential for either misconfigured software or a new Trojan (or variant).

It is entirely possible none of these scans are harmless and that our internal users are indeed searching for exploitable web servers, etc. If the university uses a proxy server and has a closed firewall policy we may become more concerned. Until then the majority of these internally generated scans appear harmless.

To secure the network further P2P software should be forbidden and the ports should be closed on the perimeter. If necessary DMZ should be established using firewalls to allow access to these services by dorm users and similar public domain access, while protecting university servers and services.

2.2 Who's doing the scanning?

2.2.1 TOP 10 Internal Hosts (by Ports scanned)

Source IP	Ports	Destinations	Probes
MY.NET.6.49	37981	136	179920
MY.NET.6.48	37714	140	181565
MY.NET.6.52	37008	141	168898
MY.NET.6.50	32331	136	136484
MY.NET.6.51	15616	91	46173
MY.NET.6.53	8626	142	83955
MY.NET.6.60	7467	146	72094
MY.NET.60.43	6753	173	462096
MY.NET.6.45	6266	156	196947
MY.NET.11.6	3940	59	24324

The MY.NET.6 subnet is generating fairly large scans of the internal network. It is likely these machines are security assets that are assigned to dedicated subnets on the internal network (the number of destinations are

roughly symmetric). If these are not security assets these machines should be investigated closely for signs of compromise or malicious user use.

2.2.2 TOP 10 External Hosts (by Ports scanned)

Source IP	Ports	Destinations	Probes
64.124.157.16	4957	2	14867
64.124.157.10	1703	1	4860
66.28.225.156	1250	2	3314
66.28.14.37	1097	2	2798
66.28.8.69	1092	2	3033
64.232.138.142	1056	1	3251
63.250.205.35	983	6	2512
66.28.14.36	898	2	2617
63.250.205.7	831	4	2373
64.124.157.64	787	2	3272

The external hosts generating these scans have a very limited number of target destinations which would indicate they have preexisting knowledge of our network either due to prior reconnaissance or information leaks in the network itself. These IP addresses along with the others in the scan log should be identified as legitimate or threat. Assuming there are no legitimate reason for these scans to exist (not threat assessment box, etc.) these IPs should be placed on a watch list. Firewall ACLs should be modified to block all non essential ports and limit access to all others to those IP spaces that are trusted or require access.

3 Alert Log Analysis

3.1 TOP 10 Alerts

There are a total of 81 different alerts in the log files. We will discuss the threat and vulnerabilities associated with the 10 referenced alerts. Many of these alerts have been seen previously on the GCIA Practical Assignment reports. However, several of these alerts have elevated in status including "connect to 515 from inside", "SNMP public access", and "inbound GNUTella". SNMP escalation in particular is not surprising given the increase in SNMP vulnerabilities.

TOP 10 ALERTS	
Alert	**Count**
connect to 515 from inside	549967
spp_http_decode: IIS Unicode attack detected	68225
SNMP public access	53480
SMB Name Wildcard	51637
spp_http_decode: CGI Null Byte attack detected	39025
ICMP Echo Request L3retriever Ping	25684
INFO MSN IM Chat data	16512
MISC Large UDP Packet	15295
High port 65535 udp - possible Red Worm - traffic	10335
INFO Inbound GNUTella Connect request	8087

3.1.1 connect to 515 from inside

Source Ips	Count Src	% of Source	Destination Ips	Count Dest	% of Dest
MY.NET.150.83	283645	51.57%	MY.NET.151.77	283645	51.57%
MY.NET.153.164	60335	10.97%	MY.NET.150.198	261781	47.60%
MY.NET.153.118	56595	10.29%	MY.NET.150.83	4515	0.82%
MY.NET.153.126	22195	4.04%	MY.NET.1.63	25	0.00%
MY.NET.153.211	8088	1.47%	MY.NET.5.35	1	0.00%
MY.NET.153.113	8071	1.47%			
MY.NET.153.119	7592	1.38%			
MY.NET.153.121	5294	0.96%			
MY.NET.151.77	4515	0.82%			
MY.NET.153.184	3833	0.70%			

There are a number of buffer overflow vulnerabilities associated with the lpr service. In particular CERT Advisory CA-2001-15 Buffer Overflow In Sun Solaris in.lpd, and CERT Advisory CA-2001-32 Buffer Overflow in HP-UX Line Printer Daemon Print Daemon are most prevalent. It is recommended that all services that are non-essential be restricted or turned off. Given the massive number of alerts that were generated and the limited number of destination IP addresses related to those alerts we surmise that the Destination IP's listed above are UNIX printer servers. If this is not the case then we are left with the usual possibilities of misconfigured workstations or compromised workstation. Given the extremely limited number of destinations we assume that these IPs are legitimate UNIX printer servers. Access to printers should be denied from external IP addresses.

3.1.2 spp_http_decode: IIS Unicode attack detected

Source Ips	Count Src	% of Source	Destination Ips	Count Dest	% of Dest
MY.NET.153.146	4644	6.81%	211.115.213.202	6384	9.36%
MY.NET.153.120	3434	5.03%	211.115.213.207	2325	3.41%
MY.NET.153.124	3309	4.85%	211.233.29.218	2214	3.25%
MY.NET.153.110	3065	4.49%	61.78.53.102	1582	2.32%
MY.NET.153.171	2851	4.18%	211.32.117.26	1532	2.25%
MY.NET.153.189	2341	3.43%	211.32.117.31	1463	2.14%
MY.NET.153.165	2179	3.19%	211.110.11.145	1256	1.84%
MY.NET.153.106	2052	3.01%	211.233.28.53	1138	1.67%
MY.NET.88.254	1925	2.82%	211.233.28.18	1075	1.58%
MY.NET.153.108	1786	2.62%	211.233.28.44	1021	1.50%

Per the Lucent Whitepaper on IIS Unicode Attacks:

> The Unicode exploit is not new, but rather a variation on an old vulnerability called the "Dot Dot" attack. The Dot Dot

> attack occurs when an attacker sends a malformed URL to a web server that looks something like this:
>
> http://www.example.com/../../../../../winnt/repair/sam._
>
> The attack itself is relatively simple to understand: the web server will just look for the file in the web-root directory called "../../../../../winnt/repair/sam._. The "../" tells the web server to look up one directory, so five "../" 's in a row will make the web server look in the document root for a file called winnt/repair/sam._. The number of "../" 's does not matter as long as there are enough of them to recurse back to the root of the file system (either c:\ or / on Unix systems). The IIS Unicode exploit uses the http protocol and malformed URLs to traverse directories and execute arbitrary commands on vulnerable web servers, much like the "Dot Dot" attack. The IIS Unicode exploit uses a Unicode representation of a directory delimiter (/) to fool IIS into doing the same thing as the old Dot Dot attack. The fix to the Dot Dot attack does not recognize the Unicode representation of the slash, which is why this exploit works.

The majority of source IPs generating this and the *spp_http:decode: GI Null Byte attack detected* alerts are generated from within the network. Further the majority of destination IPs are external web addresses. Without a detailed packet analysis it is impossible to determine if these alerts are legitimate. It appears that most of these alerts are false positives. According, to the SNORT FAQ:

> Q: I am getting too many "IIS Unicode attack detected" and/or "CGI Null Byte
> attack detected" false positives. How can I turn this detection off?
>
> A: These messages are produced by the http_decode preprocessor. If you wish
> to turn these checks off, add -unicode or -cginull to your http_decode
> preprocessor line respectively.
>
> preprocessor http_decode: 80 8080 -unicode -cginull
>
> Your own internal users normal surfing can trigger these alerts in the
> preprocessor. Netscape in particular has been known to trigger them.
>
> Instead of disabling them,try a BPF filter to ignore your outbound http

traffic such as:

snort -d -A fast -c snort.conf not (src net xxx.xxx and dst port 80)

This has worked very well for us over a period of 5-6 months and Snort is
still very able to decode actual and dangerous cgi null and unicode attacks
on our public web servers.

The SNORT recommendation to BPF filter the outbound traffic out is preferable to simply turning off this rule.

3.1.3 SNMP public access

Source Ips	Count Src	% of Source	Destination Ips	Count Dest	% of Dest
			MY.NET.150.195	32005	59.84%
			MY.NET.152.109	4202	7.86%
			MY.NET.5.127	2074	3.88%
			MY.NET.5.97	1839	3.44%
			MY.NET.5.96	1758	3.29%
			MY.NET.151.114	1256	2.35%
			MY.NET.150.84	1227	2.29%
			MY.NET.113.202	1172	2.19%
			MY.NET.150.231	771	1.44%
			MY.NET.150.147	757	1.42%

The top 10 destination addresses all reside within the internal network. Further approximately 60% of the queries target MY.NET.150.95. This box should be strenuously scrutinized for potential compromise. Further all internal network SNMP community strings should be altered from their default of PUBLIC. All university firmware and workstations should be updated with the latest release/service pack to eliminate a number of SNMP related vulnerabilities.

3.1.4 SMB Name Wildcard

Source Ips	Count Src	% of Source	Destination Ips	Count Dest	% of Dest
MY.NET.11.6	12204	23.63%	MY.NET.11.6	12116	23.46%
MY.NET.11.7	8397	16.26%	MY.NET.11.7	8381	16.23%
MY.NET.11.5	4201	8.14%	MY.NET.11.5	4169	8.07%
MY.NET.152.168	663	1.28%	MY.NET.152.168	672	1.30%
MY.NET.152.167	622	1.20%	MY.NET.152.167	624	1.21%
MY.NET.152.161	583	1.13%	MY.NET.5.4	603	1.17%
MY.NET.152.177	573	1.11%	MY.NET.152.161	589	1.14%
MY.NET.152.166	535	1.04%	MY.NET.152.177	576	1.12%
MY.NET.152.171	531	1.03%	MY.NET.152.166	540	1.05%

MY.NET.152.172	529	1.02%	MY.NET.152.171	529	1.02%

SMB Wildcards are generated when performing a NetBios Status query on a host. This can be initiated on any Windows based platform or Unix platform running SAMBA. Often an indication of an impending attack, especially if directed from an external address. However, in our situation we note that almost all of the IP addresses that originate the alert are in the list of destinations. MY.NET.11.5 through MY.NET.11.7 perform a Wildcard query on the host that initiates a query against them, thus the reason why these IP's are on both the source and destination top 10. This activity takes place on a nearly constant basis throughout the five days of the log files. It can be inferred that these three machines are Windows Domain servers.

There are a few instances of external addresses performing queries against internal addresses. It is recommended that NetBios be blocked at the firewall for all servers and network infrastructure (especially if dorm users, etc, are cordoned off in their own DMZ).

3.1.5 spp_http_decode: CGI Null Byte attack detected

Source Ips	Count Src	% of Source	Destination Ips	Count Dest	% of Dest
MY.NET.153.197	15829	40.56%	209.10.239.135	26026	66.69%
MY.NET.153.193	8730	22.37%	152.163.210.75	4020	10.30%
MY.NET.153.208	4279	10.96%	207.189.79.124	2712	6.95%
MY.NET.153.171	4139	10.61%	205.188.132.67	2232	5.72%
MY.NET.153.153	2222	5.69%	207.189.75.40	1632	4.18%
MY.NET.152.11	1169	3.00%	216.241.219.22	1169	3.00%
MY.NET.153.194	946	2.42%	206.61.145.3	402	1.03%
MY.NET.153.184	661	1.69%	63.162.230.3	384	0.98%
MY.NET.153.210	627	1.61%	MY.NET.5.96	75	0.19%
MY.NET.88.189	108	0.28%	199.104.95.15	64	0.16%

CGI Null Attacks come in a variety of forms but most share a common attribute. A null byte is inserted into the stream of commands to allow malicious code to be overlooked by CGI security checks not specifically designed to check for 'null byte' attacks. The majority of these alerts appear to be false positives along with *spp_http_decode: IIS Unicode attack detected.* Recommend implementing a BPF filter to eliminate outbound HTTP traffic.

3.1.6 ICMP Echo Request L3retriever Ping

Source Ips	Count Src	% of Source	Destination Ips	Count Dest	% of Dest
MY.NET.152.168	666	2.59%	MY.NET.11.6	12235	47.64%
MY.NET.152.167	618	2.41%	MY.NET.11.7	8446	32.88%
MY.NET.152.161	579	2.25%	MY.NET.11.5	4175	16.26%
MY.NET.152.177	568	2.21%	MY.NET.5.4	403	1.57%
MY.NET.152.166	541	2.11%	MY.NET.10.49	176	0.69%

MY.NET.152.171	538	2.09%	MY.NET.5.92	141	0.55%
MY.NET.152.172	537	2.09%	MY.NET.5.96	60	0.23%
MY.NET.152.21	518	2.02%	MY.NET.5.35	33	0.13%
MY.NET.152.163	507	1.97%	MY.NET.5.119	6	0.02%
MY.NET.152.183	502	1.95%	MY.NET.130.166	3	0.01%

This event may indicate that someone is scanning the network using the L3 "Retriever 1.5" security scanner. Since this event was caused by a ICMP packet, the source IP address could be easily forged. However, it has been noted that the intruder is likely to expect or desire a response to their packets, so it is more probable the source IP address is not spoofed. Further it has been reported that standard windows 2000 workstations generate matching ping packets when communicating with the domain.

This last case is consistent with the percentage of source addresses and percentage of destination addresses and correlates with the findings for the SMB Wildcard alert. Again it appears that MY.NET.11.5 through 7 are domain controllers. Further it seems we may be able to identify the internal network as a Windows 2000 network. Unless there is reason to be particularly alarmed by ICMP traffic generated internally it is recommended that a BPF filter for SNORT be created to ignore ICMP traffic (but not ICMP Reponses) initiated within MY.NET. Further blocking ICMP response traffic from exiting the network at the perimeter is advised.

3.1.7 INFO MSN IM Chat data

Source Ips	Count Src	% of Source	Destination Ips	Count Dest	% of Dest
MY.NET.153.113	826	5.00%	MY.NET.153.107	1138	6.89%
MY.NET.153.107	683	4.14%	MY.NET.153.111	1082	6.55%
64.4.12.180	674	4.08%	MY.NET.153.113	1004	6.08%
MY.NET.153.111	673	4.08%	64.4.12.171	447	2.71%
64.4.12.171	664	4.02%	64.4.12.180	431	2.61%
64.4.12.152	604	3.66%	64.4.12.166	414	2.51%
MY.NET.88.151	543	3.29%	64.4.12.154	370	2.24%
64.4.12.154	423	2.56%	64.4.12.152	356	2.16%
64.4.12.178	363	2.20%	64.4.12.178	339	2.05%
MY.NET.153.125	347	2.10%	64.4.12.170	302	1.83%

This appears to be legitimate MSN IM traffic. The IP addresses for 64.4.12.xxx belong to Microsoft and are registered similarly as:

msgr-sbXX.msgr.hotmail.com

Further this traffic is evenly distributed, though it appears that MY.NET.153.107, .111, and .113 received far more traffic than it sent, probably the result of file transfer. IM technology such as Microsoft's and AOL present serious security risks for virus infections. Where possible this traffic should be blocked from the firewall.

3.1.8 MISC Large UDP Packet

Source Ips	Count Src	% of Source	Destination Ips	Count Dest	% of Dest
63.240.15.205	2129	13.92%	MY.NET.153.171	5349	34.97%
61.78.35.42	2106	13.77%	MY.NET.153.174	3689	24.12%
61.78.35.44	2027	13.25%	MY.NET.153.153	2129	13.92%
210.94.0.146	1584	10.36%	MY.NET.153.164	1584	10.36%
216.106.173.144	1474	9.64%	MY.NET.153.121	780	5.10%
216.106.173.150	1295	8.47%	MY.NET.152.183	623	4.07%
63.240.15.207	1216	7.95%	MY.NET.153.157	621	4.06%
216.106.173.146	920	6.02%	MY.NET.153.165	260	1.70%
211.115.206.105	780	5.10%	MY.NET.150.215	212	1.39%
140.142.8.72	618	4.04%	MY.NET.153.211	26	0.17%

This activity is highly suspect. All of the traffic is generated externally and is directed inbound. Source ports are all high typically in the 40-42000 or 50-52000 range with destination ports typically between 1500-2000. The external host begins transmitting to the internal host and maintains this connection for an average of 30 minutes before a new IP address takes over. The source and destination ports change simultaneously approximately every 3 minutes. Occasionally both external and internal hosts jump to a high port (i.e. 32639). There are a few incidences of the port being reflexive (both using the same port).

Most of the external IP addresses belong to the Asia Pacific NIC, the remainder belong to AT&T CERFnet, iBEAM (which has filed Chapter 11), and the University of Washington.

Internal host should be closely examined for signs of compromise/infection. The External hosts should be watched more closely. It is recommended further packet analysis be conducted on this traffic to determine its nature.

3.1.9 High port 65535 udp - possible Red Worm – traffic

Source Ips	Count Src	% of Source	Destination Ips	Count Dest	% of Dest
MY.NET.6.48	2324	22.49%	MY.NET.152.246	395	3.82%
MY.NET.6.49	1979	19.15%	MY.NET.152.165	243	2.35%
MY.NET.6.52	1957	18.94%	MY.NET.152.180	212	2.05%
MY.NET.6.50	1750	16.93%	MY.NET.152.163	193	1.87%
MY.NET.6.51	597	5.78%	MY.NET.152.171	183	1.77%
MY.NET.6.53	318	3.08%	MY.NET.153.202	183	1.77%
MY.NET.6.60	242	2.34%	MY.NET.153.210	176	1.70%
64.124.157.16	144	1.39%	MY.NET.152.184	158	1.53%
MY.NET.6.45	128	1.24%	MY.NET.153.209	157	1.52%
MY.NET.60.43	84	0.81%	MY.NET.153.163	148	1.43%

While there is a number of external IP addresses attempting to communicate with internal IP addresses it does not appear that any internal IP

addresses are transmitting to on or to this port outbound. Unfortunately, this does appear to be Red Worm activity. Hosts generating this activity should be cleaned as soon as possible (update virus signatures), in particular the MY.NET.6.XXX subnet is generating an exorbitant amount of traffic.

3.1.10 INFO Inbound GNUTella Connect request

Source Ips	Count Src	% of Source	Destination Ips	Count Dest	% of Dest
167.159.1.2	23	0.28%	MY.NET.153.143	4244	52.48%
160.36.47.174	18	0.22%	MY.NET.153.175	1972	24.38%
205.149.70.203	13	0.16%	MY.NET.153.170	974	12.04%
172.146.23.220	13	0.16%	MY.NET.153.194	631	7.80%
24.162.202.131	12	0.15%	MY.NET.153.164	158	1.95%
206.135.92.142	12	0.15%	MY.NET.150.209	71	0.88%
131.187.254.2	11	0.14%	MY.NET.153.174	32	0.40%
140.77.128.53	11	0.14%	MY.NET.152.185	4	0.05%
213.98.15.165	10	0.12%	MY.NET.153.171	1	0.01%
200.18.223.18	10	0.12%			

It would appear as though some internal users have established a GNUTella node that has been advertised to a wide variety of external IP addresses (note the % share of the External IP addresses inbound is very low given the total number of alert references). There is only a single GNUTELLA connect accept (MY.NET.153.164) in the log however it is still likely these internal IP addresses are GNUTELLA servers. If GNUTella is banned then the internal hosts listed above should be disconnected pending cleanup (especially MY.NET.153.143).

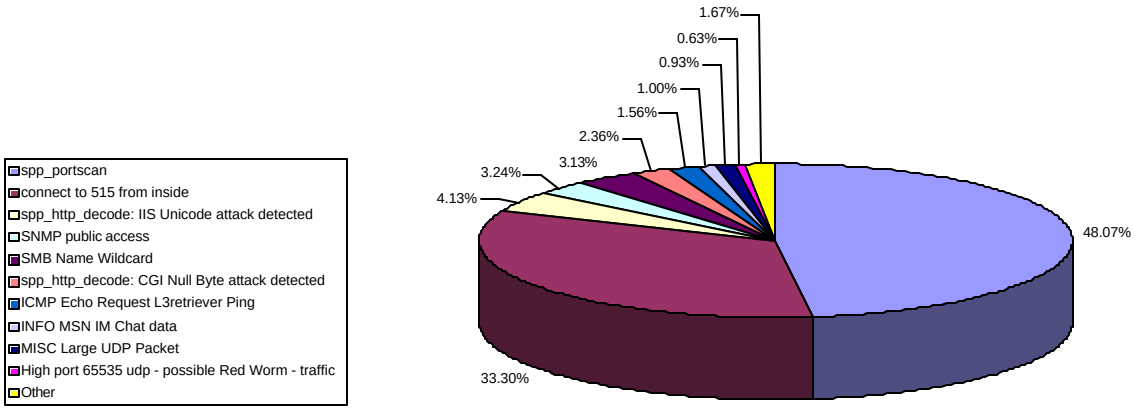
This depends on the network use policies at the university, however, GNUTELLA, KAZAA and their relatives represent serious security risks and potential liability for litigation.

3.2 Other notes on the remaining vulnerabilities

Of the 2300 (app.) WEB warnings in the log (other than those above) the majority (over half) of the source IP addresses were generated by Dial UP and Cable modems. (AOL, CableCom, etc.). Assuming Web traffic inbound is required (likely), the web servers should be checked to verify they have latest patches and are secured properly. Consider adding repeat offenders to a watch or banned list.

3.3 Alert Log Totals

Alert Entries



Alert Category	Count
spp_portscan	793975
connect to 515 from inside	549967
spp_http_decode: IIS Unicode attack detected	68225
SNMP public access	53480
SMB Name Wildcard	51637
spp_http_decode: CGI Null Byte attack detected	39025
ICMP Echo Request L3retriever Ping	25684
INFO MSN IM Chat data	16512
MISC Large UDP Packet	15295
High port 65535 udp - possible Red Worm - traffic	10335
INFO Inbound GNUTella Connect request	8087
ICMP Echo Request Nmap or HPING2	4335
FTP DoS ftpd globbing	3960
Watchlist 000220 IL-ISDNNET-990517	3385
ICMP Fragment Reassembly Time Exceeded	1723
ICMP Router Selection	1129
WEB-IIS view source via translate header	989

WEB-MISC Attempt to execute cmd	613
NMAP TCP ping!	598
INFO Outbound GNUTella Connect request	425
WEB-IIS _vti_inf access	235
WEB-FRONTPAGE _vti_rpc access	215
WEB-CGI scriptalias access	154
ICMP Echo Request Windows	149
Possible trojan server activity	138
Watchlist 000222 NET-NCFC	131
SCAN Proxy attempt	124
INFO napster login	122
Null scan!	111
INFO Napster Client Data	89
ICMP Destination Unreachable (Communication Admini	88
INFO Possible IRC Access	74
WEB-CGI ksh access	74
ICMP Echo Request BSDtype	60
ICMP traceroute	59
INFO - Possible Squid Scan	41
INFO FTP anonymous FTP	28
ICMP Destination Unreachable (Protocol Unreachable	26
EXPLOIT x86 NOOP	26
Attempted Sun RPC high port access	26
WEB-MISC compaq nsight directory traversal	25
Queso fingerprint	24
EXPLOIT NTPDX buffer overflow	23
INFO napster upload request	22
SUNRPC highport access!	20
Back Orifice	20
WEB-MISC 403 Forbidden	17
SCAN Synscan Portscan ID 19104	15
EXPLOIT x86 setuid 0	14
MYPARTY - Possible My Party infection	13
MISC traceroute	12
EXPLOIT x86 stealth noop	10
RPC tcp traffic contains bin_sh	8
Port 55850 udp - Possible myserver activity - ref.	8
WEB-MISC http directory traversal	7
Port 55850 tcp - Possible myserver activity - ref.	7
EXPLOIT x86 setgid 0	5

IDS552/web-iis_IIS ISAPI Overflow ida nosize	5
WEB-IIS encoding access	4
SCAN FIN	4
Incomplete Packet Fragments Discarded	4
INFO Outbound GNUTella Connect accept	3
MISC PCAnywhere Startup	3
RFB - Possible WinVNC - 010708-1	3
TFTP - External UDP connection to internal tftp se	2
WEB-MISC webdav search access	2
MISC Invalid PCAnywhere Login	2
MISC source port 53 to <1024	2
TFTP - Internal UDP connection to external tftp se	2
suspicious host traffic	2
WEB-MISC whisker head	2
Probable NMAP fingerprint attempt	2
WEB-CGI formmail access	2
IDS475/web-iis_web-webdav-propfind	1
TELNET access	1
TCP SMTP Source Port traffic	1
INFO Inbound GNUTella Connect accept	1
WEB-CGI redirect access	1
WEB-IIS asp-dot attempt	1
ICMP Router Selection (Undefined Code!)	1

4 Out of Spec Analysis

There was a limited number of OOS packets captured for these five days. Most OOS packets can be categorized into three categories. Those with CWR and ECN set and those with odd combinations of flags such as SYN FIN or SYN FIN RST.

4.1 SYNFIN packets

There was only a single occurrence of this by host 209.176.66.227. The following are the Scan Log entry records for this host. Both packets are returned to MY.NET.153.191. The OOS packet dump indicates the source is a cable modem.

SourceIP	SPort	DestIP	DPort	Date	Time	Flags
209.176.66.227	514	MY.NET.153.191	514	4/1/2002	12:52:24 AM	SYNFIN *2****SF
209.176.66.227	53	MY.NET.153.191	3744	4/1/2002	1:13:51 AM	FIN *******F

MY.NET.153.191 appears to be running a KAZAA client. This host is continually excessive number of port 1214 probes are transmitted from this client

to the internet. It is likely this OOS packet is a response to a stimulus provided by MY.NET.153.191.

4.2 CWR-ECN Flags

A number of these log entries do not appear to be malicious. These packets match many of the traits of a Queso Fingerprint attempt as is recored in the Alert log (High TTL, CWR and ECN flags set), however the TTL on this is not unusually high (above 225), most are below 110.

Several of these requests are bound for P2P clients such as GNUTella and KAZAA. The remainder appear to be requests to HTTP on MY.NET.5.92 and MY.NET.150.83. If these are not truly web servers the sender may have misdialed or could be trying a variant of Queso Fingerprinting. The number of packets though indicates this is not fingerprinting.

4.3 CHRISTMAS TREE FLAGS (SFR, SFRP, etc)

These remaining external hosts should be added to a watch list. These appear to be reconnaissance probes using OS fingerprinting techniques using TCP header flag and options flags. Banning selective IP addresses is not efficient over time but may be feasible for a short duration. Consider blocking all non-essential ports inbound as a more effective policy.

5 WHOIS Records

The following WHOIS records where queried using ARIN.NET. Predominantly the hosts queried are from the TOP 10 SCANS external hosts. It appears much of the scanning activity is generated from Abovenet Communications or Cogent Communications owned IP addresses.

5.1 TOP 10 External Scanning Host

5.1.1 Search results for: 64.124.157.16

TOP 10 External Scanning Host

```
Abovenet Communications, Inc. (NETBLK-ABOVENET)
   50 W. San Fernando Street, Suite 1010
   San Jose, CA 95113
   US

   Netname: ABOVENET
   Netblock: 64.124.0.0 - 64.125.255.255
   Maintainer: ABVE

   Coordinator:
      Metromedia Fiber Networks/AboveNet  (NOC41-ORG-
ARIN)  noc@ABOVE.NET
      408-367-6666
Fax- 408-367-6688

   Domain System inverse mapping provided by:
```

```
   NS.ABOVE.NET              207.126.96.162
   NS3.ABOVE.NET         207.126.105.146

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 27-Apr-2001.
   Database last updated on  22-Apr-2002 19:59:02 EDT.
```

5.1.2 Search results for: 66.28.225.156

```
Cogent Communications (NETBLK-COGENT-NB-0000)
   1015 31st Street, NW
   Washington, DC 20007
   US

   Netname: COGENT-NB-0000
   Netblock: 66.28.0.0 - 66.28.255.255
   Maintainer: COGC

   Coordinator:
      Cogent Communications  (ZC108-ARIN)
noc@cogentco.com
      +1-877-875-4311

   Domain System inverse mapping provided by:

   AUTH1.DNS.COGENTCO.COM   66.28.0.14
   AUTH2.DNS.COGENTCO.COM   66.28.0.30

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
   Reassignment information for this block can be found
at
   rwhois.cogentco.com 4321

   Record last updated on 05-Dec-2001.
   Database last updated on  22-Apr-2002 19:59:02 EDT.
```

5.1.3 Search results for: 64.232.138.142

```
New Edge Networks (NET-NEN-AW5)  NEN-AW5
64.232.0.0 - 64.232.255.255
STREAMING MEDIA CORPORATION (NETBLK-ATWORK-49180-41072)
   ATWORK-49180-41072
                              64.232.138.0 -
64.232.138.255
```

5.2 Large UDP Packets TOP 10 external host lookup

5.2.1 Search results for: 64.240.15.205

```
SAVVIS Communications Corporation (NETBLK-SAVVIS8)
SAVVIS8
                                 64.240.0.0 -
64.243.255.255
```

```
SecureWorks (NETBLK-SAVV-SECUREW1) SAVV-SECUREW1
64.240.15.0 - 64.240.15.255
```

5.3 Verification of MSN IM traffic destinations

5.3.1 Search results for: 64.4.12.171

```
MS Hotmail (NETBLK-HOTMAIL)
   1065 La Avenida
   Mountain View, CA 94043
   US

   Netname: HOTMAIL
   Netblock: 64.4.0.0 - 64.4.63.255

   Coordinator:
      Myers, Michael  (MM520-ARIN)  icon@HOTMAIL.COM
      650-693-7072

   Domain System inverse mapping provided by:

   NS1.HOTMAIL.COM          216.200.206.140
   NS3.HOTMAIL.COM          209.185.130.68

   Record last updated on 09-Jan-2001.
   Database last updated on  22-Apr-2002 19:59:02 EDT.
```

6 Summary Recommendations

There are two primary areas of concern. First the rule set run through SNORT should be reviewed and modified to more accurately reflect the network. As mentioned in the preceding sections BPF filters are needed to sort out data from internal hosts, as well some rules should be updated. One example is the Queso Fingerprint rule, typically a Queso fingerprint has the CWR and ECN flags set with a TTL of 225 or higher. SNORT is triggering this event where the TTL is well below this threshold. By modifying the rules database there will be fewer alerts to sort and filter by hand increasing the odds of finding events that require attention.

Secondly, a great deal of attention is being drawn to the internal network for the purposes of P2P, Gaming and ICQ. If this traffic is allowed it is recommend that this traffic be segregated from the university proper (servers, mainframes, etc.) by use of VLAN or similar tool. If this is done a separate firewall ACL could be established for the dorms, etc., than for the corporate resources such as the servers. Similarly a separate set of rules should be applied by SNORT to this traffic (either separate SNORT engines or duplicate the rules and modify the IP strings).

7 References

American Registry for Internet Numbers, URL: http://www.arin.net

Carey, Steve, "Port 50000 Connections", URL: http://www.incidents.org/archives/intrusions/msg04547.html

Cert Advisory, "Neohapsis Archives - CERT COAST CIAC - CERT Advisory CA-2002-01 Exploitation of Vulnerability in CDE Subprocess – From cert-adv", Neohapsis, URL: http://archives.neohapsis.com/archives/cc/2002-q1/0000.html

Espinola, Michael, "Neohapsis Archives - ISS-XForce - RE Strange Port = 1975 - From micheale@ix.netcom.com", URL: http://archives.neohapsis.com/archives/iss/2000-q1/0378.html

Hagel Technologies, "Welcome to Hagel Technologies", URL: http://hageltech.com/

Hays, Bil "AFS for Darwin-OS X", URL: http://www.ibiblio.org/macsupport/osx_arla.html

Holland, Jeff, "GCIA Practical Assignment", URL: http://www.giac.org/practical/Jeff_Holland_GCIA.doc

MetaMachine, "eDonkey2000", URL: http://www.edonkey2000.com/

Miller, Nate, "Microsoft IIS Unicode Exploit", Lucent Technologies Worldwide Services, URL: http://www.lucent.com/livelink/197020_Whitepaper.pdf

SANS Institute, "ID FAQ - What port numbers do well-known trojan horses use" URL: http://www.sans.org/newlook/resources/IDFAQ/oddports.htm

SANS Institute, "Passive OS Fingerprinting", URL: http://www.incidents.org/papers/OSfingerprinting.php

SANS Institute, "SANS Alerts and Analysis - Increased probes to TCP port 515", URL: http://www.sans.org/newlook/alerts/port515.htm

SANS Institute, "What are some of the signs of Internet Gaming", incidents.org URL: http://www.incidents.org/detect/gaming.php

Seifried, Kurt "Information security – Ports", URL: http://seifried.org/security/ports/

Shinberg, Scott, "GCIA Practical Assignment", URL: http://www.giac.org/practical/Scott_Shinberg_GCIA.doc

Whitehats, Inc., "arachnids", URL: http://www.whitehats.com/ids/index.html

Last Updated: July 26th, 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
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 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
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