Global Information Assurance Certification Paper

GCIA Practical Assignment

Jeffrey M. Wirth
Intrusion Detection in Depth/GCIA
Version 3.0

Assignment 1 - Describe the State of Intrusion Detection

Creating NIDS Reports for Management

I believe that most intrusion detection analyst would agree that we deal with a complicated subject matter. At times it difficult to discuss topics with individuals familiar with the technology let alone explaining incidents to a CEO or CTO. Yes, in fairness, intrusion detection is not the job of the CEO, but when you are asked about "Return on Investment" or to "Explain the Benefits of IDS" what do you tell them? This is where I found myself not to long ago and believe me I had no clue where to begin.

After pondering the problem, I began to realize that what management needed from the IDS Department was no different from what they received for other technology groups, reporting. And not just any reports, reports that they could understand! After coming to this awareness, I put together a list of bullets attempting to outline my keys to "NIDS Reporting for Management".

- Develop a simple document to establish a baseline understanding of hacker activity.
- Stay away from text descriptions and log dumps. Use charts or graphs to make a point.
- Drive home the fact that every organization is a target no matter how large or small.
- Show correlation with data collected by other sources.
- And most important, keep it simple to understand.

Level Setting Management

As I mentioned, it would be important to develop a baseline of understanding with management. I decided that the best way to accomplish this would be to create a document that briefly outlines and/or explains the following:

1. Hacker Methods
2. General "IDS & Hacking" terms.

Hacker Methods

Hacking for the most part is a methodical process involving research, time and patience. One of my favorite hacking analogies is the comparison to a bank robber. Most bank robbers, or I guess at least the ones that hope to get away with their crime, are going to spend a significant amount of time "casing the joint". They will monitor the banks daily activity, research the banks security system and develop a plan of attack. This is similar to the process a hacker will take when attempting to break into a computer system.

A hacker will begin their assault by compiling detailed information concerning a corporation's network infrastructure. This process is referred to as "Footprinting" and is

accomplished using various tools, techniques and data sources. During this process the hacker is looking to assemble data that includes the following:

1. Domain Names
2. Network Blocks
3. Publicly accessible IP Addresses
4. System Architecture (i.e. X86 or AIX)
5. Network Protocols
6. Authentication Mechanisms

It is important to understand that some of this information can be obtained without directly requesting data from a corporation's network. Services provided by various Internet consortiums, technology website and search engines make this information available to anyone with an Internet connection. An example of this is the service provide by Netcraft (www.netcraft.com). This website regularly queries website and stores information which includes operating system, web server vender and IP Address. The following is data gained after requesting information on www.microsoft.com:

Uptime Summary for www.microsoft.com

Note: Uptime - the time since last reboot is explained in the FAQ

Time in Days

	Plotted Value	No. samples	Max	Latest
Windows 2000		546	143.00	36.25
90-day Moving average		823	86.47	26.16

OS, Web Server and Hosting History for www.microsoft.com

OS Server Last changed IP address Netblock Owner
Windows 2000 Microsoft-IIS/5.0 14-Sep-2001 207.46.197.113 Microsoft Corporation
Windows 2000 Microsoft-IIS/5.0 23-Jun-2001 207.46.197.101 Microsoft Corporation
Windows 2000 Microsoft-IIS/5.0 20-Jun-2001 207.46.197.100 Microsoft Corporation
Windows 2000 Microsoft-IIS/5.0 15-Jun-2001 207.46.197.102 Microsoft Corporation
Windows 2000 Microsoft-IIS/5.0 21-Jan-2001 207.46.230.241 Microsoft Corporation
Windows 2000 Microsoft-IIS/5.0 10-Dec-2000 207.46.130.75 Microsoft Corporation

The next step for the hacker is to activity scan a corporation's IP address block looking for active servers and what services they provide. This process could take hours, days

or months depending on the size of the network and how inconspicuous the attacker what's to be. The data collected during the scanning exercise will be used later to pinpoint servers running specific services, i.e. web servers, mail servers or domain name servers.

Now that the hacker knows what services you offer and on what servers they run on, it is time to see which ones have known (or possible unknown) exploits and exploit them. This is where the hacker has the greatest advantage over a corporation's system and network administrators. The hacker only needs to find one open, whereas the administrator needs to guard against 100's of potential vulnerabilities.

So to wrap-up the basic approach that a hacker will take in the attempt to compromise a systems is as following:

Footprinting -> Scanning -> System/Network Hacking

IDS & Hacker Terms

Footprinting: This is the process of collecting detailed information about an organizations technology infrastructure.

Scan (a.k.a. Probe, Recon, Portscan): The process of sending packets (stimulus) to a device looking for a response to indicate whether the IP address is in use or a particular service is being provided.

Enumeration: The process of extracting valid user accounts.

Intrusion Detection Systems (IDS): A systems (host or network based) that monitors network activity looking for malicious activity or activity that falls outside of the corporation's acceptable usage policy.

Severity: Is a mechanism for rating the affect of malicious network activity. This would include both portscanning and exploit events.

Severity Level	Description
High	• Device, server, and/or service security posture is UNKNOWN and may run on an older operating system. • Possibly not protected by a firewall or filter device. • The service provided is of high corporate valve.
Moderate	• Device, server, and/or service runs on a current operating system. • System may not be updated with current security fixes. • The service may not be vital to network operations

Low	• Device, server, and/or service security posture is known. • System stat has been verified with a vulnerability assessment within the last month.

** Note: This a simplified version of the "Severity" matrix for use with individuals outside of the security realm.

Vulnerability: A known or unknown security hole that allows unauthorized access to a service, application or operating system.

Exploit: An exploit is an attack on a computer system that takes advantage of a particular vulnerability that the system offers to intruders.

Attack Signature: Once a vulnerability has been researched a signature can be created to detect it in the wild.

Alert Classification: The following table lists the name and description of attack signature classification used by our corporate intrusion detection system.

Class Name	Description	Default Priority
not-suspicious	Not Suspicious Traffic	0
unknown	Unknown Traffic	1
bad-unknown	Potentially Bad Traffic	2
attempted-recon	Attempted Information Leak	3
successful-recon-limited	Information Leak	4
successful-recon-largescale	Large Scale Information Leak	5
attempted-dos	Attempted Denial of Service	6
successful-dos	Denial of Service	7
attempted-user	Attempted User Privilege Gain	8
unsuccessful-user	Unsuccessful User Privilege Gain	7
successful-user	Successful User Privilege Gain	9
attempted-admin	Attempted Administrator Privilege Gain	10
successful-admin	Successful Administrator Privilege Gain	11

Dshield (www.deshield.org): Dshield provides an online service for IDS administrators to upload event logs for analysis and incident reporting. Utilizing the data uploaded from around the world, Dshield tracks global activity and presents the data in the form of graphs, charts and tables for public consumption.

Creating the Reports

The data used to create these reports was generated by Snort 1.8.1, specifically the

application's alert and portscan logs. From this data two types for reports have been created, one that focuses on daily activity and the second that displays events over some period on time. The details of these reports are described below, but before the reports are created it is necessary to perform verification on the data that has been collected, i.e. remove the false positives.

Data Verification

A report is only as good as the data that is used to create it. This makes data verification a pivotal part of the reporting process. The process involved here could easily be broken out into a paper of it's own, but I will run through a few examples.

Verification - Portscan Logs

As the name suggests, the Snort Portscan log holds entries concerning events classified as portscans. So what does Snort consider a portscan? According the application's user manual a portscan is classified as follows:

> Taken from "Snort Users Manual" Release 1.8
>
> "A portscan is defined as TCP connection attempts to more that P ports in T seconds or UDP packets sent to more than P ports in T seconds. Ports can be spread across any number of destination IP addresses, and may all be the same port if spread across multiple IPS. This version does single->single and single->many portscans….A portscan is also defined as a single 'stealth scan' packet, such as NULL, FIN, SYNFIN, XMAS, etc."

Valid Data

First lets look at some examples of valid data. The following is an example of single-> many portscan. This particular event shows a scan from one host to many on the same port (111).

```
Dec  6 17:05:37 A.HACKER.SCANNING.ATTEMPT:50786 -> A.SCANNED.HOST.1:111 SYN ******S*
Dec  6 17:05:37 A.HACKER.SCANNING.ATTEMPT:50787 -> A.SCANNED.HOST.2:111 SYN ******S*
Dec  6 17:05:37 A.HACKER.SCANNING.ATTEMPT:50788 -> A.SCANNED.HOST.3:111 SYN ******S*
Dec  6 17:05:37 A.HACKER.SCANNING.ATTEMPT:50789 -> A.SCANNED.HOST.4:111 SYN ******S*
Dec  6 17:05:37 A.HACKER.SCANNING.ATTEMPT:50790 -> A.SCANNED.HOST.5:111 SYN ******S*
Dec  6 17:05:37 A.HACKER.SCANNING.ATTEMPT:50791 -> A.SCANNED.HOST.6:111 SYN ******S*
Dec  6 17:05:37 A.HACKER.SCANNING.ATTEMPT:50792 -> A.SCANNED.HOST.7:111 SYN ******S*
Dec  6 17:05:37 A.HACKER.SCANNING.ATTEMPT:50793 -> A.SCANNED.HOST.8:111 SYN ******S*
Dec  6 17:05:37 A.HACKER.SCANNING.ATTEMPT:50794 -> A.SCANNED.HOST.9:111 SYN ******S*
```

Next we have an example of a single->single scan. Which indicates one host scanning a single host for multiple ports.

```
Dec  3 18:11:05 A.HACKER.SCANNING.ATTEMPT:4715 -> A.SCANNED.HOST.250:21 SYN ******S*
Dec  3 18:11:05 A.HACKER.SCANNING.ATTEMPT:4716 -> A.SCANNED.HOST.250:22 SYN ******S*
Dec  3 18:11:05 A.HACKER.SCANNING.ATTEMPT:4717 -> A.SCANNED.HOST.250:23 SYN ******S*
Dec  3 18:11:05 A.HACKER.SCANNING.ATTEMPT:4730 -> A.SCANNED.HOST.250:43 SYN ******S*
Dec  3 18:11:08 A.HACKER.SCANNING.ATTEMPT:4794 -> A.SCANNED.HOST.250:70 SYN ******S*
Dec  3 18:11:08 A.HACKER.SCANNING.ATTEMPT:4811 -> A.SCANNED.HOST.250:79 SYN ******S*
Dec  3 18:11:10 A.HACKER.SCANNING.ATTEMPT:4839 -> A.SCANNED.HOST.250:88 SYN ******S*
Dec  3 18:11:13 A.HACKER.SCANNING.ATTEMPT:4896 -> A.SCANNED.HOST.250:113 SYN ******S*
```

```
Dec  3 18:11:20 A.HACKER.SCANNING.ATTEMPT:1139 -> A.SCANNED.HOST.250:210 SYN ******S*
```

And the last event that snort will detect is the single malformed packet or "stealth scan". These entries would indicate the detection of network traffic that is "Out of Spec" and a possible fingerprint attempt.

```
Dec 1 05:25:52 A.HACKER.SCANNING.ATTEMPT:18245 -> A.SCANNED.HOST.250:80 NOACK **U*PRSF
Dec 1 05:25:52 A.HACKER.SCANNING.ATTEMPT:18245 -> A.SCANNED.HOST.250:80 INVALIDACK *2*APRSF
```

False Positive

There are numerous and legitimate network events that could cause Snort (or any network or host based IDS for that matter) to record what it believes to be a portscan. Including a miss-configured or malfunctioning server or network device.

The following log entry is an example of activity classified a portscan, which in actuality was created due to a known malfunctioning router type.

```
Nov 28 04:19:32 62.58.51.172:18245 -> 159.137.136.250:21536 NOACK *2U*PRS*
Nov 28 04:19:36 62.58.51.172:18245 -> 159.137.136.250:21536 INVALIDACK *2*APRSF
```

Also, services that by design generate large numbers of ports over a short time span tend to trip up IDS. Below is an example of legitimate DNS traffic that Snort logged as a portscan:

```
Nov 29 08:54:30 A.GOOD.DNS.SERVER:53 -> OUR.EXTERNAL.DNS.SERVER:27380 UDP
Nov 29 08:54:31 A.GOOD.DNS.SERVER:53 -> OUR.EXTERNAL.DNS.SERVER:27393 UDP
Nov 29 08:54:32 A.GOOD.DNS.SERVER:53 -> OUR.EXTERNAL.DNS.SERVER:27418 UDP
Nov 29 08:54:32 A.GOOD.DNS.SERVER:53 -> OUR.EXTERNAL.DNS.SERVER:27437 UDP
Nov 29 08:54:33 A.GOOD.DNS.SERVER:53 -> OUR.EXTERNAL.DNS.SERVER:27456 UDP
Nov 29 08:54:35 A.GOOD.DNS.SERVER:53 -> OUR.EXTERNAL.DNS.SERVER:27488 UDP
Nov 29 08:54:35 A.GOOD.DNS.SERVER:53 -> OUR.EXTERNAL.DNS.SERVER:27511 UDP
Nov 29 08:54:35 A.GOOD.DNS.SERVER:53 -> OUR.EXTERNAL.DNS.SERVER:27512 UDP
Nov 29 08:54:36 A.GOOD.DNS.SERVER:53 -> OUR.EXTERNAL.DNS.SERVER:27541 UDP
```

Daily Reports

The intension of the daily report is to show activity over a 24 hour period. The report is created using validated data obtained from the Snort portscans and alert logs.

Portscanning

Data Source

Snort Portscan Log

Reason for Inclusion

This chart gives the reader an indication of ports scanned over the last 24 hours, which maybe an indication of things to come.

Question(s) to answer

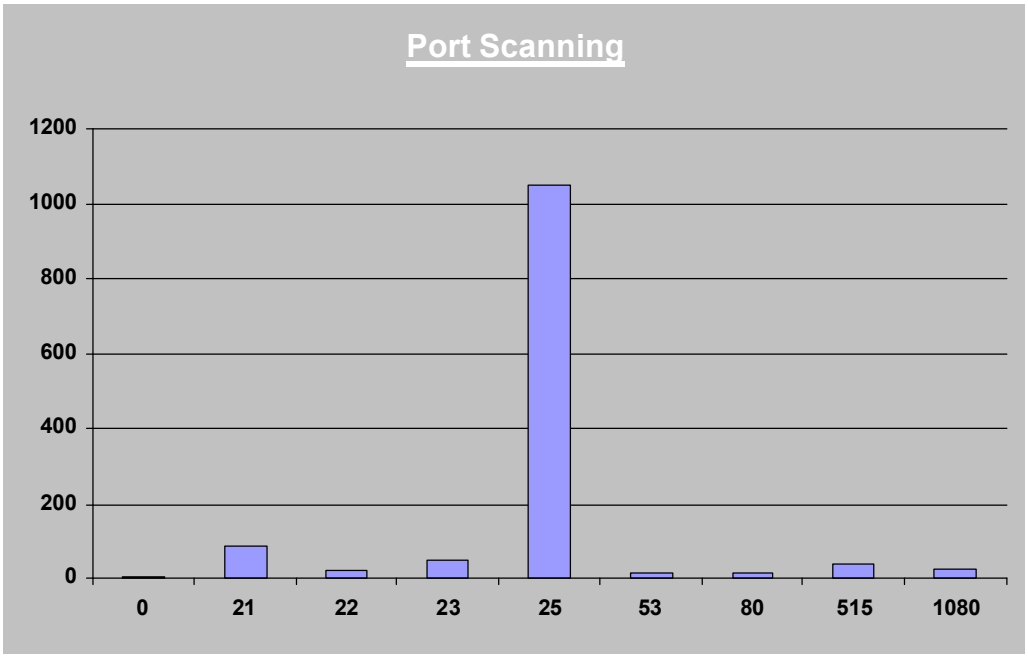
1. What ports where scanned?
2. Do we run the scanned services?

3. Should we be concerned (Severity Level)?

Analysis

This chart indicates that port 25, which is the standard port for "Simple Mail Transfer Protocol" (SMTP), saw the greatest amount of scanning activity over the last 24 hours. Activity of this magnitude may point towards a new SMTP vulnerability or a hacker looking for open SMTP relays. The severity of this activity, as it relates to our external SMTP servers, should be considered LOW. Our SMTP relays are known to be running the latest product version and are properly patched.

Of the remaining ports, 80 (HTTP), 21 (FTP) and 53 (DNS) are also used on our external network and accessible by the general public. HTTP and FTP have recently released exploits for the products currently deployed in the corporate DMZ. With the servers in this state combined with the value of the service, the severity level here is HIGH. The system administrators will be contacted to assess whether any remediation is required. The servers running DNS are in known, stable security state, placing the severity level at LOW.



Service Attacks

Data Source

Snort Alert Log

Reason for Inclusion

This chart provides the viewer with an indication of services targeted over the last 24 hours.

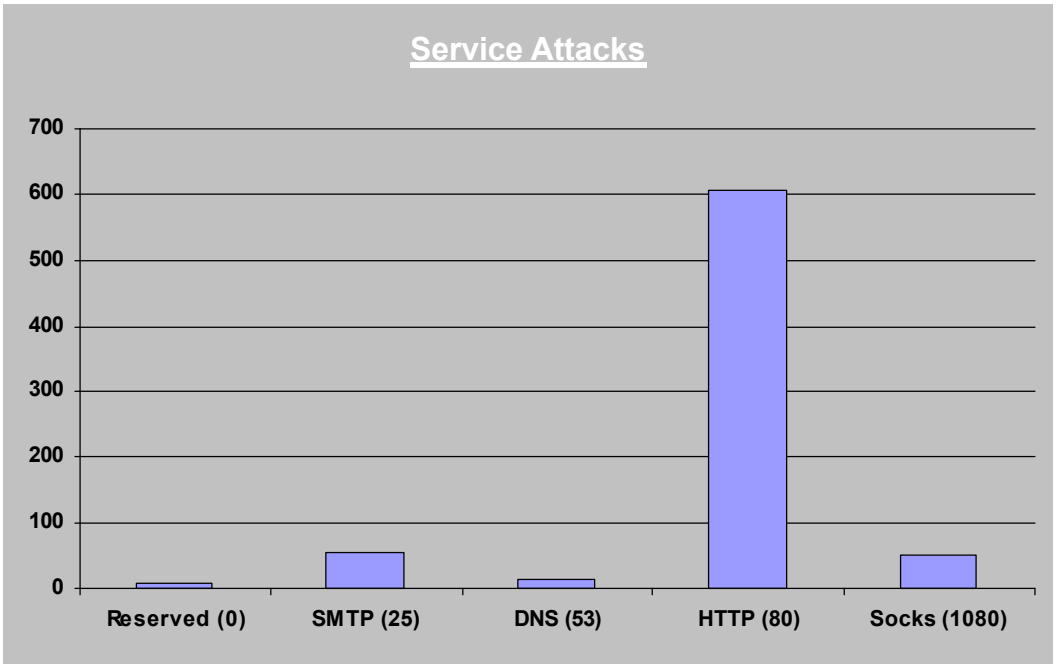
Question(s) to answer

1. What services saw exploit activity?
2. Do we run the scanned services?
3. Should we be concerned (Severity Level)?

Analysis

Over the last 24 hours it appears a significant amount of exploit activity was directed towards HTTP services. Based on the large number of web servers currently in service combined with the unknown patch and version state this would place the severity level at HIGH.

Concerning the remaining services, only SMTP (25) and DNS (53) are run on our external network. As mentioned in the "Portscanning" section, the servers running these services are in a stable and secure state.



Correlation (Dshield.org)

Source of Data

Dshield

Reason for Inclusion

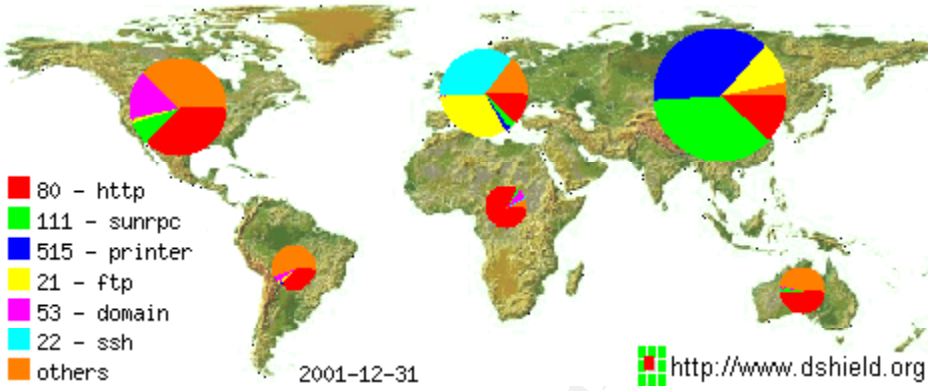
This graph is provided by Dshield.org and illustrates global activity for the date of the report. Including this graph provides correlation to what our intrusion detection recorded.

Question(s) to answer

1. Are we the only one's be scanned?

Analysis

Comparing our data to the information in the graph below it appears that the activity seen on our network was similar to what was seen elsewhere. In particular ports 80 (HTTP) and 53 (DNS) saw significant activity in North America.



Attacking IP Address

Source of Data

Snort Portscan and Alert Logs
Geektools

Reason for Inclusion

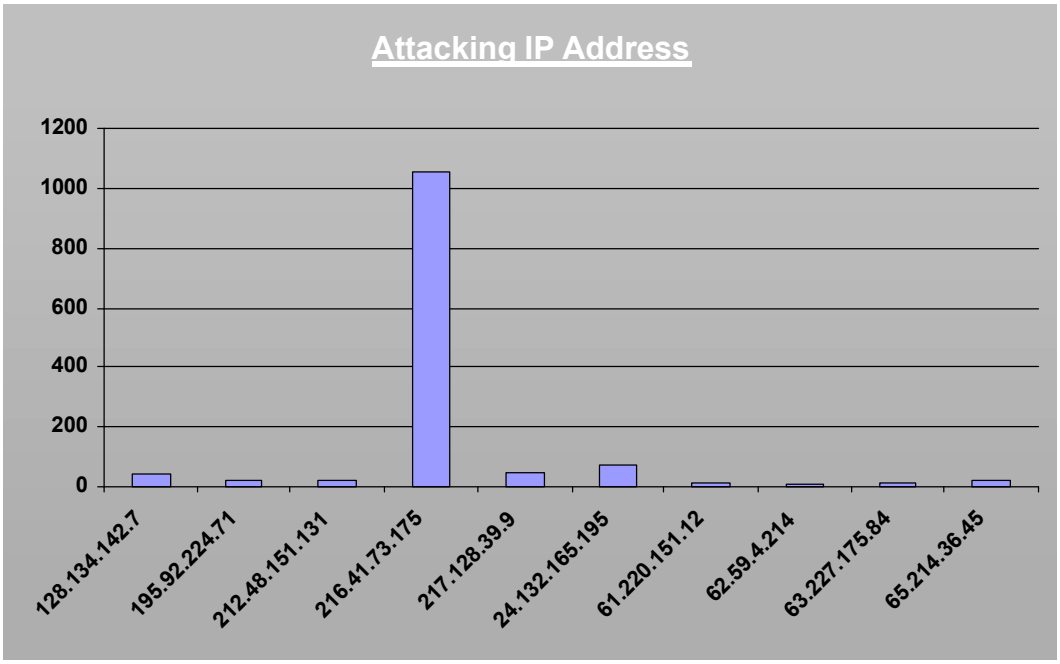
The purpose of this chart is to show that the hacker community is indeed global and that an attack can originate from any country and any network.

Question(s) to answer

1. Who's scanning us?

Analysis

Based on the IP address and "Country of Origin" in the table below it appears that hacker activity was seen from various parts of the world. The largest activity seems to be coming from a USA based Internet Services Provider, Galaxy Internet, based in Newton, MA.



"Whois" lookup information provided by Geektools (www.geektools.com)

IP Address	Block Owner	Country of Origin
128.134.142.7	Korea Telecom	Korea
195.92.224.71	Planet Online Limited	United Kingdom
212.48.151.131	Online Resource Center	Russia
216.41.73.175	Galaxy Internet	USA
217.128.39.9	France Telecom (DSL)	France
24.132.165.195	Kabeltelevisie Amsterdam	Netherlands
61.220.151.12	Chunghwa Telecom	Taiwan
62.59.4.214	Zonnet Dialpool	Netherlands
63.227.175.84	Thecenteredsoul.com	USA
65.214.36.45	UUNET Technologies	USA

Alert Classification

Source of Data

Snort Alert Log

Reason for Inclusion

Describing exploit activity in terms of specific attack signatures may not be the right approach for an audience outside the IT security realm. The question is, will a manager actually know what a "Multiple Decode Attempt" is, probably not. To avoid this problem, but still give information on the types of attack signatures seen, I created a chart that presents "Alert Classification" instead of alert signature names. Since this

information is general it is hopefully easer to understand.

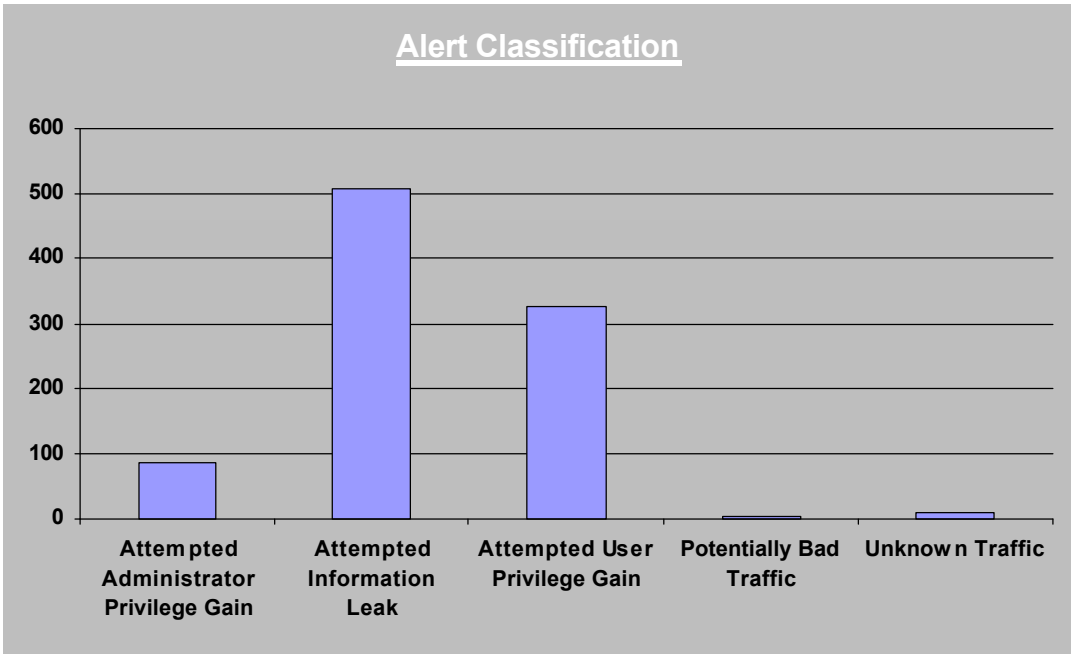
Question(s) to answer

1. What types of attack signatures are we seeing?

Analysis

The majority of the attack signature traffic appears to fall into one of three classification categories: "Attempted Administrator Privilege Gain", "Attempted Information Leak" and "Attempted User Privilege Gain". By far the most active is "Attempted Information Leak" which may include some of the following attempts:

1. DNS zone transfers
2. Various Microsoft IIS exploit attempts



Trend Analysis

All Scanning Activity Trends

Source of Data

Snort Portscan Log

Reason for Inclusion

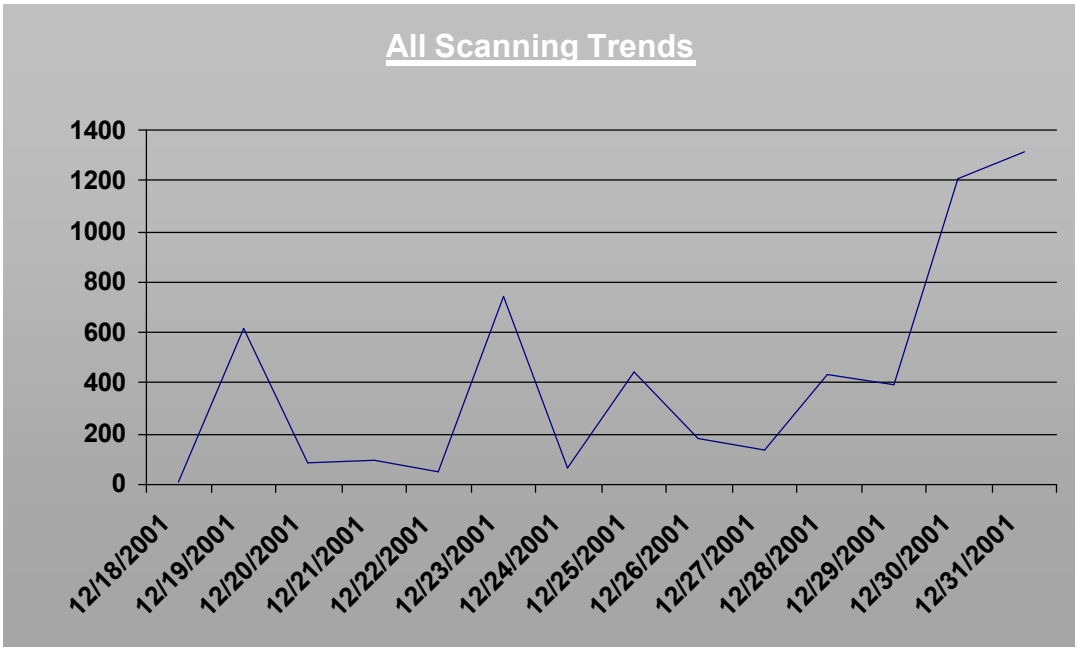
This chart shows overall scanning activity over a period of time. From the data presented it is possible to point out increasing, decreasing, or spikes in activity.

Question(s) to answer

1. Did scanning activity increase or decrease during this time period?
2. Are there days that saw increased activity?

Analysis

Form the chart it appears that portscan activity over this time period was on an upward trend. It is also evident the activity peaked on the weekends and holidays. This may indicate that hackers focus their activity during times support or administrative coverage is low.



Destination Port Trends (Scanning)

Source of Data

Snort Portscan Log

Reason for Inclusion

This chart shows ports of interest over a period of time. From the data presented it is possible to point out increasing, decreasing, or spikes in activity.

Question(s) to answer

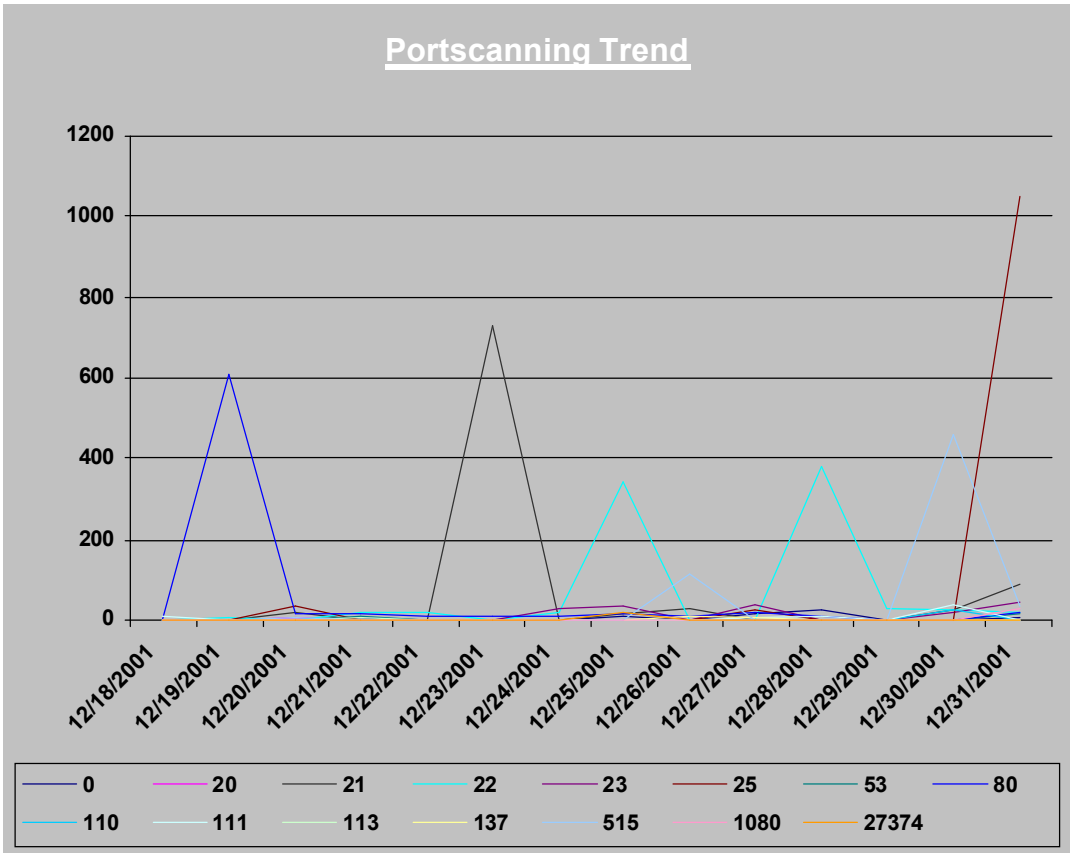
1. What ports where scanned?
2. Do we run the scanned services?
3. Are there any developing trends?

Analysis

Of the ports presented in the chart below the following are currently used by services deployed on our external network: 20 (FTP), 21 (FTP), 25 (SMTP), 53 (DNS) and 80 (HTTP). Severity level for the servers/services are LOW with the exception of HTTP

(80). The HTTP services have recently released exploits for the products currently deployed in the corporate DMZ. With the servers in this state combined with the value of the service, the severity level here is HIGH. The system administrators will be contacted to assess whether any remediation is required.

Reviewing the spikes in the trend lines indicts high volume activity for ports 80, 21, 22, 515, and 25 on individual days. In particular the activity for port 25 on 12/31/2001 is almost off the chart with comparatively no previous activity. This may indicate that all of our external subnets where scanned for port 25.



Service Attack Trends

Source of Data

Snort Alert Log

Reason for Inclusion

This chart shows services of interest over a period of time. From the data presented it is possible to point out increasing, decreasing, or spikes in activity.

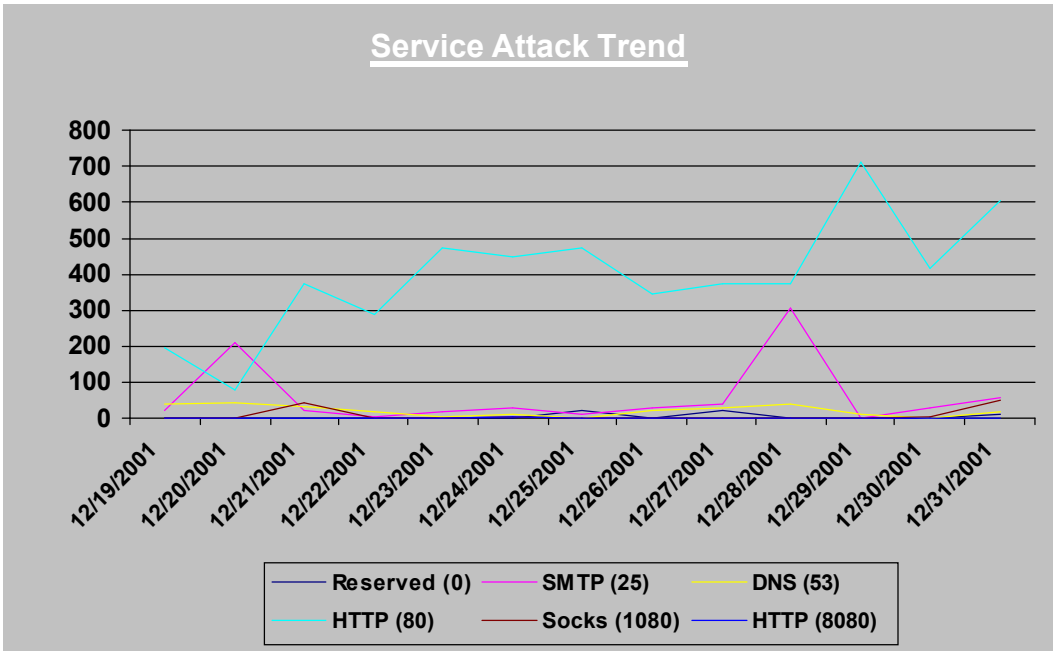
Question(s) to answer

1. What services saw exploit activity?

2. Do we run the scanned services?
3. Should we be concerned (Severity Level)?

Analysis

During the time frame covered in the chart below activity concerning the HTTP (80) service is by far the most prevalent. The trend is on a steady rise with additional spikes of increased activity. As indicated in the "Portscan Trend" analysis this service and the servers involved have a HIGH severity level.



Correlation (Dshield.org)

Source of Data

Dshield

Reason for Inclusion

This chart was created using data provided by Dshield.org and illustrates global activity over the time span cover in this report. Including this chart provides correlation to what our intrusion detection recorded.

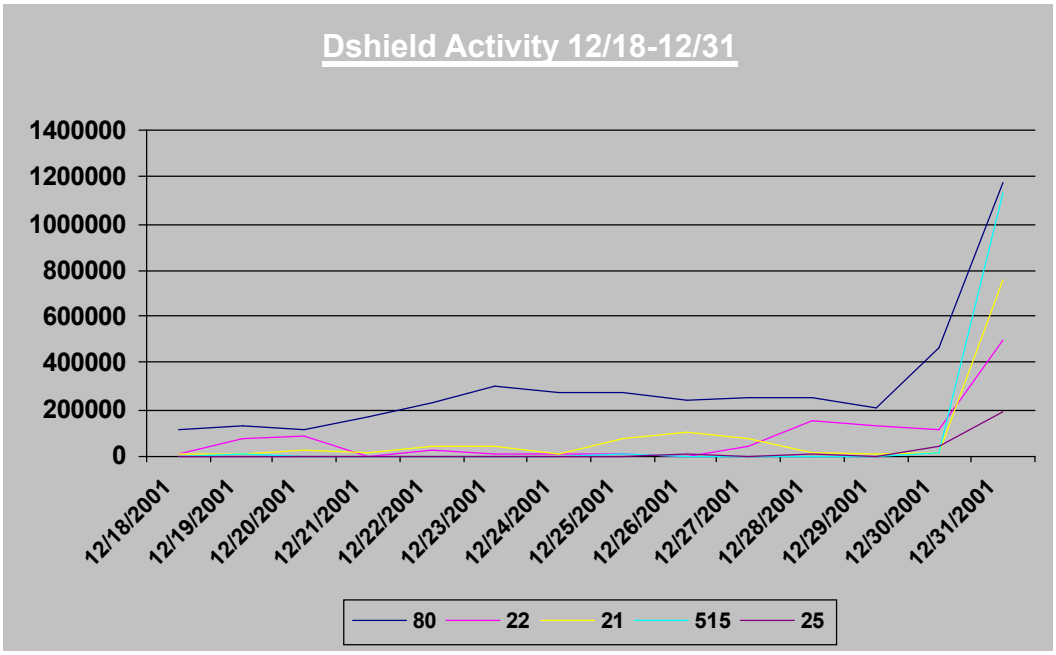
Question(s) to Answer

1. Are others experiencing the same trends in portscan and exploit activity?

Analysis

In comparing the chart below with data presented by "Portscan Trends" and "Service Attack Trends" there appears to be correlation in a couple of areas. First, the global

trend for HTTP (80) is on a steady increase and begins to spike on 12/28/2001. Second, activity for SMTP (25) is relatively flat and then dramatically spikes on 12/31/2001.



Alert Classification Trends

Source of Data

Snort Alert Log

Reason for Inclusion

This chart shows attack signature activity categorized by "Alert Classification" over a period of time. From the data presented it is possible to point out increasing, decreasing, or spikes in activity.

Question(s) to answer

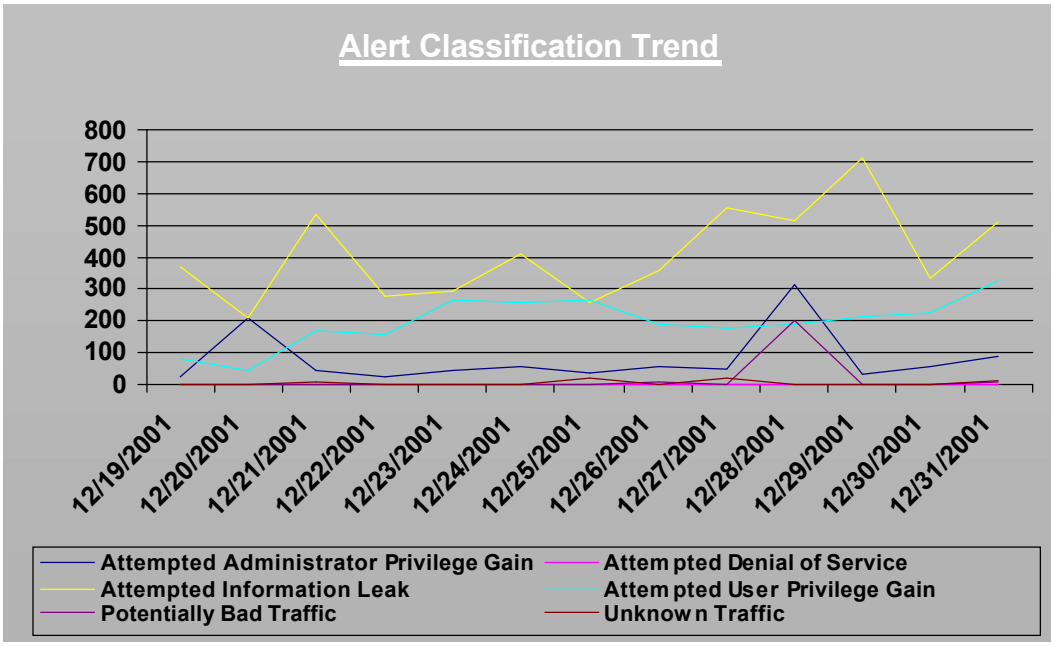
1. What types of attack signatures are we seeing?
2. Are there any developing trends?

Analysis

In the chart below the alert classifications "Attempted Information Leak" and "Attempted User Privilege Gain" comprise a large percentage of the overall activity. The trend for "Attempted Information Leak" appears to be on a steady climb with peaks of activity on three separate days. Exploits that fall into these categories would include the following:

1. DNS zone transfers
2. Various Microsoft IIS exploit attempts

3. Operating Systems fingerprinting attempts



Assignment 2 - Network Detects

Network Detect - 1 (DNS named version attempt)

Trace

```
--------------------------------------------------------------------------------
#(2 - 190652) [2001-09-05 23:26:27] [arachNIDS/278]  DNS named version attempt
IPv4: BLACK.HAT.221.35 -> OUR.NET.136.168
      hlen=5 TOS=0 dlen=58 ID=65145 flags=0 offset=0 TTL=43 chksum=49432
UDP:  port=3711 -> dport: 53 len=38
Payload:  length = 30

000 : 12 34 00 80 00 01 00 00 00 00 00 00 07 76 65 72   .4.........ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
--------------------------------------------------------------------------------
#(2 - 172298) [2001-08-31 23:42:25] [arachNIDS/278]  DNS named version attempt
`IPv4: BLACK.HAT.221.35 -> OUR.NET.136.204
      hlen=5 TOS=0 dlen=58 ID=27550 flags=0 offset=0 TTL=43 chksum=21456
UDP:  port=4921 -> dport: 53 len=38
Payload:  length = 30

000 : 12 34 00 80 00 01 00 00 00 00 00 00 07 76 65 72   .4.........ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
--------------------------------------------------------------------------------
#(2 - 171745) [2001-08-31 19:57:43] [arachNIDS/278]  DNS named version attempt
IPv4: BLACK.HAT.221.35 -> OUR.NET.136.94
      hlen=5 TOS=0 dlen=58 ID=30318 flags=0 offset=0 TTL=43 chksum=18798
UDP:  port=2865 -> dport: 53 len=38
Payload:  length = 30

000 : 12 34 00 80 00 01 00 00 00 00 00 00 07 76 65 72   .4.........ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
--------------------------------------------------------------------------------
#(2 - 131062) [2001-08-26 02:29:51] [arachNIDS/278]  DNS named version attempt
IPv4: BLACK.HAT.221.35 -> OUR.NET.136.66
      hlen=5 TOS=0 dlen=58 ID=18906 flags=0 offset=0 TTL=43 chksum=30238
UDP:  port=4673 -> dport: 53 len=38
Payload:  length = 30

000 : 12 34 00 80 00 01 00 00 00 00 00 00 07 76 65 72   .4.........ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
--------------------------------------------------------------------------------
#(2 - 129735) [2001-08-25 02:58:31] [arachNIDS/278]  DNS named version attempt
IPv4: BLACK.HAT.221.35 -> OUR.NET.146.203
      hlen=5 TOS=0 dlen=58 ID=37622 flags=0 offset=0 TTL=43 chksum=8825
UDP:  port=2900 -> dport: 53 len=38
Payload:  length = 30

000 : 12 34 00 80 00 01 00 00 00 00 00 00 07 76 65 72   .4.........ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
```

```
-------------------------------------------------------------------------------
#(2 - 67216) [2001-08-22 09:22:13] [arachNIDS/278]  DNS named version attempt
IPv4: BLACK.HAT.221.35 -> OUR.NET.136.117
      hlen=5 TOS=0 dlen=58 ID=63850 flags=0 offset=0 TTL=43 chksum=50778
UDP:  port=2701 -> dport: 53 len=38
Payload:  length = 30

000 : 12 34 00 80 00 01 00 00 00 00 00 00 07 76 65 72   .4.........ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
-------------------------------------------------------------------------------
#(2 - 40179) [2001-08-21 14:51:10] [arachNIDS/278]  DNS named version attempt
IPv4: BLACK.HAT.221.35 -> OUR.NET.136.60
      hlen=5 TOS=0 dlen=58 ID=39041 flags=0 offset=0 TTL=43 chksum=10109
UDP:  port=4955 -> dport: 53 len=38
Payload:  length = 30

000 : 12 34 00 80 00 01 00 00 00 00 00 00 07 76 65 72   .4.........ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
-------------------------------------------------------------------------------
#(2 - 8721) [2001-08-20 20:37:39] [arachNIDS/278]  DNS named version attempt
IPv4: BLACK.HAT.221.35 -> OUR.NET.136.222
      Hlen=5 TOS=0 dlen=58 ID=7836 flags=0 offset=0 TTL=43 chksum=41152
UDP:  port=1228 -> dport: 53 len=38
Payload:  length = 30

000 : 12 34 00 80 00 01 00 00 00 00 00 00 07 76 65 72   .4.........ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03         sion.bind.....
-------------------------------------------------------------------------------
```

Source of Trace

This activity was detected on our network between August 26, 2001 and September 5, 2001.

Detect was Generated By

The data in this trace was the result of an ACID v0.9.6b13 query on alerts generated by Snort v1.8.1.

Probability the Source Address Was Spoofed

Low. The probability that the source address was spoofed is low, because the hacker is looking for a response from the destination server.

Description of Attack

It appears the attacker was looking to compile reconnaissance information for particular versions of BIND (4.9.7 and higher) which will return a version number when queried. Once the version of BIND is known, the hacker can then focus on vulnerabilities for that version. This type of activity is by no means new and in some

cases could be considered legitimate traffic, but there where a few things that caught my attention. First the source IP is the same in all the alerts. Second, the queries where spaced over a couple of days. And finally the destination IP appears to be random. All of these points would leave me to believe that the queries where scripted, possibly a hacker looking to build a database of BIND servers and their versions.

Attack Mechanism

This query can be accomplished by any number of DNS query tools, i.e. nslookup or dig. The following is an example of a BIND version query using nslookup run against a test server:

```
#nslookup
> server my.test.dns.server
Default Server:  my.test.dns.server
Address:  XXX.XXX.XXX.XXX
> set class=chaos
> set type=txt
> version.bind
Server:  my.test.dns.server
Address:  XXX.XXX.XXX.XXX

VERSION.BIND    text =

      "named 4.9.6a-Rel-Friday-4-July-97
      GregSchueman-LarryKahn-VirajBais-LeonMcCalla"
>
```

Correlations

Using the BIND version query feature as a reconnaissance tool has been document by various sources including the authors of "Hacking Exposed, Network Security Secrets & Solutions."

Evidence of Active Targeting

Yes. There is evidence of activity targeting since reconnaissance information gained could be used at a later date to target specific servers.

Severity

Low: The service/application vulnerable to this exploit are not running on our network.

Attack Severity = (5+1) - (3+4) = -1

Severity Component	Rating	Description
Criticality	5	The service exploit by this attack, DNS is a vital network component.

Lethality	1	Are DNS server does not run BIND
System Countermeasures	3	Latest Operating system and unknown security patch level.
Network Countermeasures	4	Multiple restrictive firewalls

Defensive Recommendation

As with any software it is recommended that BIND be updated to the latest stable release.

Multiple Choice Test Question

What tool(s) can be used to generate a BIND version query?

A. ifconfig
B. nslookup
C. netstat
D. ping

Answer: B

Network Detect - 2 (TCP Port 0 Invalid Flag Activity)

Trace

Acid Query (Snort Alerts)

```
---------------------------------------------------------------------------
#(1 - 40353) [2001-11-06 10:21:48]  MISC TCP port 0 traffic
IPv4: 62.59.192.34 -> OUR.NET.146.166
      hlen=5 TOS=0 dlen=110 ID=15262 flags=0 offset=0 TTL=112 chksum=40542
TCP:  port=5635 -> dport: 0  flags=21**P*S* seq=1426128896
      ack=1359151126 off=4 res=5 win=6952 urp=22782 chksum=57480
Payload:  length = 42

000 : F2 8A 69 F1 68 18 AD 9D 9F DE 33 D9 A5 3E 3F C4   ..i.h.....3..&gt;?.
010 : 9E F2 B2 11 7F 6C 19 20 36 00 00 00 42 73 D0 43   .....  l. 6...Bs.C
020 : 48 55 21 DA 2E F4 2F 5B 75 57                     HU!.../[uW
---------------------------------------------------------------------------
#(1 - 40354) [2001-11-06 10:21:48]  MISC TCP port 0 traffic
IPv4: 62.59.192.34 -> OUR.NET.146.166
      hlen=5 TOS=0 dlen=110 ID=15266 flags=0 offset=0 TTL=112 chksum=40538
TCP:  port=5635 -> dport: 0  flags=**U***S* seq=1426128896
      ack=1359151136 off=13 res=11 win=6283 urp=26718 chksum=39804
      Options:
       #1 - 175 len=40 data=32E4CBEDD75C90F0C11BE3082E0241F664D9E8A9E720360000004273D043485521DA2EF42F5B
Payload:  length = 10

000 : 48 55 21 DA 2E F4 2F 5B 75 57                     HU!.../[uW
```

```
-------------------------------------------------------------------------------
#(1 - 40356) [2001-11-06 10:22:18]  MISC TCP port 0 traffic
IPv4: 62.59.192.34 -> OUR.NET.146.166
      hlen=5 TOS=0 dlen=110 ID=15368 flags=0 offset=0 TTL=112 chksum=40436
TCP:  port=5635 -> dport: 0  flags=**UAPRS* seq=1426128896
      ack=1359151247 off=10 res=7 win=54635 urp=36894 chksum=20442
      Options:
       #1 - 29 len=40 data=7BD5013B0A26D83D4F483933C0CFDA962163EF4A2A20360000004273D043485521DA2EF42F5B
Payload:  length = 22

000 : EF 4A 2A 20 36 00 00 00 42 73 D0 43 48 55 21 DA   .J* 6...Bs.CHU!.
010 : 2E F4 2F 5B 75 57                                 ../[uW
-------------------------------------------------------------------------------
#(1 - 40363) [2001-11-06 10:23:39]  MISC TCP port 0 traffic
IPv4: 62.59.192.34 -> OUR.NET.146.166
      hlen=5 TOS=0 dlen=110 ID=15414 flags=0 offset=0 TTL=112 chksum=40390
TCP:  port=5635 -> dport: 0  flags=2*UAP**F seq=1426128896
      ack=1359151214 off=14 res=14 win=4668 urp=434 chksum=14424
      Options:
       #1 - 243 len=40 data=2075F0936C4EB69566535FB1E9E90787B4228E2A9820360000004273D043485521DA2EF42F5B
Payload:  length = 6

000 : 2E F4 2F 5B 75 57                                 ../[uW
-------------------------------------------------------------------------------
#(1 - 40365) [2001-11-06 10:23:54]  MISC TCP port 0 traffic
IPv4: 62.59.192.34 -> OUR.NET.146.166
      hlen=5 TOS=0 dlen=110 ID=15459 flags=0 offset=0 TTL=112 chksum=40345
TCP:  port=5635 -> dport: 0  flags=21U**R*F seq=1426128896
      ack=1359151352 off=1 res=3 win=55062 urp=1513 chksum=59859
Payload:  length = 42

000 : 04 4E 1F DC 71 2D AE A8 95 7A FB F9 AB D5 EC 7A   .N..q-...z.....z
010 : 4A E0 96 BA 80 F8 09 20 36 00 00 00 42 73 D0 43   J..... 6...Bs.C
020 : 48 55 21 DA 2E F4 2F 5B 75 57                     HU!.../[uW
-------------------------------------------------------------------------------
#(1 - 40366) [2001-11-06 10:23:57]  MISC TCP port 0 traffic
IPv4: 62.59.192.34 -> OUR.NET.146.166
      hlen=5 TOS=0 dlen=110 ID=15476 flags=0 offset=0 TTL=112 chksum=40328
TCP:  port=5635 -> dport: 0  flags=*1*APRS* seq=1426128896
      ack=1359151302 off=14 res=2 win=12212 urp=43630 chksum=15507
      Options:
       #1 - 115 len=40 data=0C0FF75C1E918F8C55D4245670B37C06D4E1B7ECAD20360000004273D043485521DA2EF42F5B
Payload:  length = 6

000 : 2E F4 2F 5B 75 57                                 ../[uW
-------------------------------------------------------------------------------
#(1 - 40367) [2001-11-06 10:24:02]  MISC TCP port 0 traffic
IPv4: 62.59.192.34 -> OUR.NET.146.166
      hlen=5 TOS=0 dlen=110 ID=15499 flags=0 offset=0 TTL=112 chksum=40305
TCP:  port=5635 -> dport: 0  flags=21U**R** seq=1426128896
      ack=1359151216 off=8 res=2 win=25664 urp=40804 chksum=33048
      Options:
       #1 - 156 len=40 data=476C531E86B6DCAB5DAEBC10672A74DB245B238A00200B000000594F03CF36D601F7E3460845
Payload:  length = 30
```

```
000 : BC 10 67 2A 74 DB 24 5B 23 8A 00 20 0B 00 00 00   ..g*t.$[#.. ....
010 : 59 4F 03 CF 36 D6 01 F7 E3 46 08 45 95 C1         YO..6....F.E..
-------------------------------------------------------------------------------
#(1 - 40369) [2001-11-06 10:24:59]  MISC TCP port 0 traffic
IPv4: 62.59.192.34 -> OUR.NET.146.166
     hlen=5 TOS=0 dlen=110 ID=15563 flags=0 offset=0 TTL=112 chksum=40241
TCP:  port=5635 -> dport: 0  flags=2*UAPR** seq=1426128896
     ack=1359151224 off=2 res=15 win=56540 urp=18640 chksum=17988
Payload:  length = 42

000 : A3 71 FF DD 1C 41 B7 18 CC CA C9 C3 D5 53 99 34   .q...A.......S.4
010 : E7 11 AA BC 26 6E 6A 20 0B 00 00 00 59 4F 03 CF   ....&amp;nj ....YO..
020 : 36 D6 01 F7 E3 46 08 45 95 C1                     6....F.E..
-------------------------------------------------------------------------------
#(1 - 40370) [2001-11-06 10:26:11]  MISC TCP port 0 traffic
IPv4: 62.59.192.34 -> OUR.NET.146.166
     hlen=5 TOS=0 dlen=110 ID=15620 flags=0 offset=0 TTL=112 chksum=40184
TCP:  port=5635 -> dport: 0  flags=21UAPR** seq=1426128896
     ack=1359151204 off=15 res=11 win=40628 urp=65217 chksum=52680
     Options:
      #1 - 95 len=28 data=241E7E295B76ECE9A31FEB5ED747424CA62AD777EF200B000000
      #2 - 89 len=40 data=03CF36D601F7E346084595C1696F6E0A6D696370093935094D494350090923204D6F62696C65
Payload:  length = 2

000 : 95 C1                                             ..
-------------------------------------------------------------------------------
#(1 - 40371) [2001-11-06 10:26:11]  MISC TCP port 0 traffic
IPv4: 62.59.192.34 -> OUR.NET.146.166
     hlen=5 TOS=0 dlen=110 ID=15632 flags=0 offset=0 TTL=112 chksum=40172
TCP:  port=5635 -> dport: 0  flags=*1****S* seq=1426128896
     ack=1359151330 off=6 res=14 win=23800 urp=5415 chksum=31585
     Options:
      #1 - 187 len=40 data=A75ABA266C6601F6E032E1FB02FAF187B3A179C04F200B000000594F03CF36D601F7E3460845
Payload:  length = 38

000 : BA 26 6C 66 01 F6 E0 32 E1 FB 02 FA F1 87 B3 A1   .&amp;lf...2........
010 : 79 C0 4F 20 0B 00 00 00 59 4F 03 CF 36 D6 01 F7   y.O ....YO..6...
020 : E3 46 08 45 95 C1                                 .F.E..
-------------------------------------------------------------------------------
```

Shadow Trace (TCPDUMP) A - All "Out of Spec" Traffic

```
10:21:42.750384 62.59.192.34.32814 > OUR.NET.146.166.259: R [ECN-Echo] 5376:5424(48) win 0 urg 3 (DF)
10:21:48.311538 62.59.192.34.5635 > OUR.NET.146.166.0: SP [ECN-Echo,CWR] 1426128896:1426128970(74) win 6952 (DF)
10:21:48.412068 62.59.192.34.5635 > OUR.NET.146.166.0: S 1426128896:1426128934(38) win 6283 urg 26718 <[bad opt]> (DF)
10:22:18.137913 62.59.192.34.5635 > OUR.NET.146.166.0: SRP 1426128896:1426128946(50) ack 1359151247 win 54635 urg
36894 <[bad opt]> (DF)
10:23:39.304884 62.59.192.34.5635 > OUR.NET.146.166.0: FP [CWR] 0:34(34) ack 4294967264 win 4668 urg 434 <[bad opt]> (DF)
10:23:54.695150 62.59.192.34.5635 > OUR.NET.146.166.0: FR [ECN-Echo,CWR] 1426128896:1426128982(86) win 55062 urg 1513
(DF)
10:23:57.867972 62.59.192.34.5635 > OUR.NET.146.166.0: SRP [ECN-Echo] 1426128896:1426128930(34) ack 1359151302 win
12212 <[bad opt]> (DF)
10:24:02.522468 62.59.192.34.5635 > OUR.NET.146.166.0: R [ECN-Echo,CWR] 1426128896:1426128954(58) win 25664 urg 40804
<[bad opt]> (DF)
```

10:24:59.532237 62.59.192.34.5635 > OUR.NET.146.166.0: RP [CWR] 0:82(82) ack 4294967219 win 56540 urg 18640 (DF)

10:26:11.398359 62.59.192.34.5635 > OUR.NET.146.166.0: RP [ECN-Echo,CWR] 0:30(30) ack 4294967199 win 40628 urg 65217 <opt-95:241e7e295b76ece9a31feb5ed747424ca62ad777ef200b000000,[bad opt]> (DF)

10:26:11.797110 62.59.192.34.5635 > OUR.NET.146.166.0: S [ECN-Echo] 1426128896:1426128962(66) win 23800 <[bad opt]> (DF)

Shadow Trace (TCPDUMP) B - Portion of the entire trace

10:21:40.955553 62.59.192.34.1126 > OUR.NET.146.166.443: S 1087421447:1087421447(0) win 8760 <mss 460,nop,nop,sackOK> (DF)

10:21:40.957071 OUR.NET.146.166.443 > 62.59.192.34.1126: S 727760000:727760000(0) ack 1087421448 win 8760 <mss 1460>

10:21:41.074285 62.59.192.34.1126 > OUR.NET.146.166.443: . ack 1 win 8760 (DF)

10:21:42.750384 62.59.192.34.32814 > OUR.NET.146.166.259: R [ECN-Echo] 5376:5424(48) win 0 urg 3 (DF)

10:21:45.738146 62.59.192.34.1126 > OUR.NET.146.166.443: P 1:49(48) ack 1 win 8760 (DF)

10:21:45.740051 OUR.NET.146.166.443 > 62.59.192.34.1126: P 1:791(790) ack 49 win 8712

10:21:46.139419 62.59.192.34.1126 > OUR.NET.146.166.443: P 49:193(144) ack 791 win 7970 (DF)

10:21:46.141666 OUR.NET.146.166.443 > 62.59.192.34.1126: P 791:862(71) ack 193 win 8568

10:21:46.430398 62.59.192.34.1126 > OUR.NET.146.166.443: . ack 862 win 7899 (DF)

10:21:47.767767 62.59.192.34.1126 > OUR.NET.146.166.443: P 193:665(472) ack 862 win 7899 (DF)

10:21:47.769930 OUR.NET.146.166.443 > 62.59.192.34.1126: P 862:1028(166) ack 665 win 8096

10:21:48.031708 62.59.192.34.1126 > OUR.NET.146.166.443: . ack 1028 win 7733 (DF)

10:21:48.103178 62.59.192.34.1126 > OUR.NET.146.166.443: P 665:1062(397) ack 1028 win 7733 (DF)

10:21:48.105234 OUR.NET.146.166.443 > 62.59.192.34.1126: P 1028:1194(166) ack 1062 win 7699

10:21:48.129778 62.59.192.34.1126 > OUR.NET.146.166.443: R 1087422509:1087422509(0) win 0 (DF)

10:21:48.165604 62.59.192.34.1127 > OUR.NET.146.166.443: S 1089262550:1089262550(0) win 8760 <mss 1460,nop,nop,sackOK> (DF)

10:21:48.167424 OUR.NET.146.166.443 > 62.59.192.34.1127: S 737470000:737470000(0) ack 1089262551 win 8760 <mss 1460>

10:21:48.239741 62.59.192.34.1126 > OUR.NET.146.166.443: R 1087422509:1087422509(0) win 0

10:21:48.269545 62.59.192.34.1128 > OUR.NET.146.166.443: S 1089333918:1089333918(0) win 8760 <mss 1460,nop,nop,sackOK> (DF)

10:21:48.270837 OUR.NET.146.166.443 > 62.59.192.34.1128: S 737660000:737660000(0) ack 1089333919 win 8760 <mss 1460>

10:21:48.274868 62.59.192.34.1129 > OUR.NET.146.166.443: S 1089378979:1089378979(0) win 8760 <mss 1460,nop,nop,sackOK> (DF)

10:21:48.275941 OUR.NET.146.166.443 > 62.59.192.34.1129: S 737680000:737680000(0) ack 1089378980 win 8760 <mss 1460>

10:21:48.284051 62.59.192.34.1127 > OUR.NET.146.166.443: . ack 1 win 8760 (DF)

10:21:48.311538 62.59.192.34.5635 > OUR.NET.146.166.0: SP [ECN-Echo,CWR] 1426128896:1426128970(74) win 6952 (DF)

10:21:48.384703 62.59.192.34.1128 > OUR.NET.146.166.443: R 1089333919:1089333919(0) win 0

Source of Trace

This activity was detected on our network on November 06, 2001.

Detect was Generated By

The data in this trace was the result of an ACID v0.9.6b13 query on alerts generated by Snort v1.8.1. and tcpdump data provided by SHADOW.

Probability the Source Address Was Spoofed

Unlikely. After reviewing the various trace information a TCP three-way handshake took place.

Description of Attack

The activity from the client starts off looking like a normal HTTPS session. First we see

a SYN from the client, followed by a SYN ACK from the destination server and then the three-way handshake is complete when the client sends an ACK back.

```
10:21:40.955553 62.59.192.34.1126 > 159.137.146.166.443: S 1087421447:1087421447(0) win 8760 <mss 460,nop,nop,sackOK> (DF)
10:21:40.957071 159.137.146.166.443 > 62.59.192.34.1126: S 727760000:727760000(0) ack 1087421448 win 8760 <mss 1460>
10:21:41.074285 62.59.192.34.1126 > 159.137.146.166.443: . ack 1 win 8760 (DF)
```

But then things begin to look a little strange. After the ACK is sent, the client sends a packet that I would consider "Out of Spec" and most certainly not part of a normal HTTPS connection.

```
10:21:42.750384 62.59.192.34.32814 > 159.137.146.166.259: R [ECN-Echo] 5376:5424(48) win 0 urg 3 (DF)
```

There are a few parts of this packet that struck me as odd. First, the client appeared to be initiating a HTTPS session (port 443) and the sends a RST to port 259. Second, a RST without an ACK is usually an indication of a "Half-Open" connection. According to W. Richard Stevens, in his book "TCP/IP Illustrated, Volume 1", a "Half-Open" session occurs when one of the communicating machines has closed or aborted a session with the knowledge of the other. This would occur if a machine crashes or losses power suddenly. And third, why are the reserve bit (ECN-Echo) and URG bits set.

Moving further into the trace more odd packets begin to appear. The first is another RST again without an ACK.

```
10:21:48.129778 62.59.192.34.1126 > 159.137.146.166.443: R 1087422509:1087422509(0) win 0 (DF)
```

And then another "Out of Spec" packet, this one with the flags SYN PUSH set with both reserve bits set.

```
10:21:48.311538 62.59.192.34.5635 > 159.137.146.166.0: SP [ECN-Echo,CWR] 1426128896:1426128970(74) win 6952 (DF)
```

At this point, with the help of a BPF filter, I took a look at all the packets without port 443. This produced a dump of "Out of Spec" packets that had some similar characteristics.

```
10:21:42.750384 62.59.192.34.32814 > 159.137.146.166.259: R [ECN-Echo] 5376:5424(48) win 0 urg 3 (DF)
10:21:48.311538 62.59.192.34.5635 > 159.137.146.166.0: SP [ECN-Echo,CWR] 1426128896:1426128970(74) win 6952 (DF)
10:21:48.412068 62.59.192.34.5635 > 159.137.146.166.0: S 1426128896:1426128934(38) win 6283 urg 26718 <[bad opt]> (DF)
10:22:18.137913 62.59.192.34.5635 > 159.137.146.166.0: SRP 1426128896:1426128946(50) ack 1359151247 win 54635 urg 36894 <[bad opt]> (DF)
10:23:39.304884 62.59.192.34.5635 > 159.137.146.166.0: FP [CWR] 0:34(34) ack 4294967264 win 4668 urg 434 <[bad opt]> (DF)
```

With the exception of the first packet all source and destination ports where 5635 and 0 respectively. Also the sequence numbers on some of the packets are the same and the "Don't Fragment" bit is set.

Attack Mechanism

It appears that this traffic is crafted and the attacker could be looking to perform an "OS fingerprint" with the "Out of Spec" packets.

Correlations

Correlating data was obtained through www.sans.org from a post by Curt Wilson to handler@incidents.org on January 09, 2001. The following is an except from the post:

> (Curt Wilson)
>
> INTERNET SUSPICIOUS ACTIVITY - Dec 26 - Jan 31, 2000
>
> Detect 3: A020-0044.SANT.splitrock.net shows possible network trouble or some type of hacking/scanning attempt with crafted packets. The second entry could possibly indicate an OS fingerprint scan, more research needed on detects 3 and 5. Can anyone help????
>
> Dec 27 00:31:04 [firewall.ip.address] %PIX-5-500003: Bad TCP hdr length (hdrlen=0, pktlen=45) from 63.254.149.44/32811 to cidr.net.addr.98/259, flags: RST URG , on interface outside
> Dec 27 00:31:10 [firewall.ip.address] %PIX-4-500004: Invalid transport field for protocol=6, from 63.254.149.44/5635 to cidr.net.addr.98/0

Evidence of Active Targeting

Possibly. There is evidence of activity targeting, but the reason behind the traffic is unknown.

Severity

Low: The intent of this traffic is unknown.

Attack Severity = (5+4) - (3+4) = 2

Severity Component	Rating	Description
Criticality	5	This activity was directed towards one our vital secure web servers.
Lethality	4	The intent of this traffic is unknown.
System Countermeasures	3	Latest Operating system and unknown security patch level.
Network Countermeasures	4	Multiple restrictive firewalls

Defensive Recommendation

It is unknown what the intent of this traffic is, so defense recommendations would be difficult. That said, as always verify firewall rules are correct and that all the servers involved are fully patched. Also since the nature of the traffic is unknown, create a custom IDS signature to track future activity.

Multiple Choice Test Question

What combination of TCP flags would indicate a "Half-Open" connection?

A. SYN, ACK
B. PSH, ACK
C. RST
D. RST, ACK

Answer: C

Network Detect - 3 (SYN SCAN and FTP Directory Traversal Attempt)

Trace

Snort Portscan Log

Nov	14	5	48	21	FTP.HACKER.53.239	3940	->	OUR.NET.175.19	21	SYN	******S*
Nov	14	5	48	21	FTP.HACKER.53.239	4021	->	OUR.NET.175.100	21	SYN	******S*
Nov	14	5	48	21	FTP.HACKER.53.239	4022	->	OUR.NET.175.101	21	SYN	******S*
Nov	14	5	48	21	FTP.HACKER.53.239	4023	->	OUR.NET.175.102	21	SYN	******S*
Nov	14	5	48	21	FTP.HACKER.53.239	4025	->	OUR.NET.175.104	21	SYN	******S*
Nov	14	5	48	22	FTP.HACKER.53.239	4028	->	OUR.NET.175.107	21	SYN	******S*
Nov	14	5	48	22	FTP.HACKER.53.239	4041	->	OUR.NET.175.120	21	SYN	******S*
Nov	14	5	48	22	FTP.HACKER.53.239	4172	->	OUR.NET.175.251	21	SYN	******S*
Nov	14	5	48	22	FTP.HACKER.53.239	4175	->	OUR.NET.175.254	21	SYN	******S*
Nov	14	5	48	23	FTP.HACKER.53.239	4171	->	OUR.NET.175.250	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	3923	->	OUR.NET.175.2	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	3924	->	OUR.NET.175.3	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	3926	->	OUR.NET.175.5	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	3928	->	OUR.NET.175.7	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	3930	->	OUR.NET.175.9	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	4024	->	OUR.NET.175.103	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	4026	->	OUR.NET.175.105	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	4027	->	OUR.NET.175.106	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	4029	->	OUR.NET.175.108	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	4030	->	OUR.NET.175.109	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	4032	->	OUR.NET.175.111	21	SYN	******S*
Nov	14	5	48	24	FTP.HACKER.53.239	4033	->	OUR.NET.175.112	21	SYN	******S*
Nov	14	5	48	25	FTP.HACKER.53.239	4028	->	OUR.NET.175.107	21	SYN	******S*
Nov	14	5	48	25	FTP.HACKER.53.239	4041	->	OUR.NET.175.120	21	SYN	******S*
Nov	14	5	48	25	FTP.HACKER.53.239	4025	->	OUR.NET.175.104	21	SYN	******S*
Nov	14	5	48	25	FTP.HACKER.53.239	4022	->	OUR.NET.175.101	21	SYN	******S*
Nov	14	5	48	25	FTP.HACKER.53.239	4175	->	OUR.NET.175.254	21	SYN	******S*
Nov	14	5	48	25	FTP.HACKER.53.239	4172	->	OUR.NET.175.251	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	3923	->	OUR.NET.175.2	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	3930	->	OUR.NET.175.9	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	3924	->	OUR.NET.175.3	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	3928	->	OUR.NET.175.7	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	3926	->	OUR.NET.175.5	21	SYN	******S*

Nov	14	5	48	30	FTP.HACKER.53.239	4032	->	OUR.NET.175.111	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	4029	->	OUR.NET.175.108	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	4026	->	OUR.NET.175.105	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	4033	->	OUR.NET.175.112	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	4030	->	OUR.NET.175.109	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	4027	->	OUR.NET.175.106	21	SYN	******S*
Nov	14	5	48	30	FTP.HACKER.53.239	4024	->	OUR.NET.175.103	21	SYN	******S*
Nov	14	5	48	31	FTP.HACKER.53.239	4028	->	OUR.NET.175.107	21	SYN	******S*
Nov	14	5	48	31	FTP.HACKER.53.239	4041	->	OUR.NET.175.120	21	SYN	******S*
Nov	14	5	48	31	FTP.HACKER.53.239	4025	->	OUR.NET.175.104	21	SYN	******S*
Nov	14	5	48	31	FTP.HACKER.53.239	4022	->	OUR.NET.175.101	21	SYN	******S*
Nov	14	5	48	31	FTP.HACKER.53.239	4175	->	OUR.NET.175.254	21	SYN	******S*
Nov	14	5	48	31	FTP.HACKER.53.239	4172	->	OUR.NET.175.251	21	SYN	******S*

RST/ACK - Closed Port

```
05:48:22.782017 FTP.HACKER.53.239.4171 > OUR.NET.175.250.21: S 3601181356:3601181356(0) win 16384 <mss
1360,nop,nop,sackOK> (DF)
05:48:22.783529 OUR.NET.175.250.21 > FTP.HACKER.53.239.4171: R 0:0(0) ack 3601181357 win 0

05:48:23.977386 FTP.HACKER.53.239.4171 > OUR.NET.175.250.21: S 3601181356:3601181356(0) win 16384 <mss
1360,nop,nop,sackOK> (DF)
05:48:23.978568 OUR.NET.175.250.21 > FTP.HACKER.53.239.4171: R 0:0(0) ack 1 win 0
```

Open FTP Servers

```
05:48:21.547359 FTP.HACKER.53.239.3940 > OUR.NET.175.19.21: S 3589512893:3589512893(0) win 16384 <mss
1360,nop,nop,sackOK> (DF)
05:48:21.547639 OUR.NET.175.19.21 > FTP.HACKER.53.239.3940: S 557651437:557651437(0) ack 3589512894 win 65535 <mss
512>
05:48:21.976742 FTP.HACKER.53.239.4021 > OUR.NET.175.100.21: S 3593575647:3593575647(0) win 16384 <mss
1360,nop,nop,sackOK> (DF)
05:48:21.978392 OUR.NET.175.100.21 > FTP.HACKER.53.239.4021: S 3492066640:3492066640(0) ack 3593575648 win 9520 <mss
1360> (DF)
05:48:21.985756 FTP.HACKER.53.239.4023 > OUR.NET.175.102.21: S 3593687380:3593687380(0) win 16384 <mss
1360,nop,nop,sackOK> (DF)
05:48:21.986819 OUR.NET.175.102.21 > FTP.HACKER.53.239.4023: S 1096109419:1096109419(0) ack 3593687381 win 9520 <mss
1360> (DF)
```

Trace of FTP Command Activity - Requests for "/_private", "/cgi-bin/", "/usr/"

```
05:48:34.861090 FTP.HACKER.53.239.4023 > OUR.NET.175.102.21: P 584:600(16) ack 1606 win 17439 (DF)
0x0000   4500 0038 b4a8 4000 7406 ddc7 c1fb 35ef        E..8..@.t.....5.
0x0010   ccfe af66 0fb7 0015 d633 539c 4155 53b2        ...f.....3S.AUS.
0x0020   5018 441f c43c 0000 4357 4420 2f5f 7072        P.D..<..CWD./_pr
0x0030   6976 6174 652f 0d0a                            ivate/..
05:48:34.863501 OUR.NET.175.102.21 > FTP.HACKER.53.239.4023: P 1606:1650(44) ack 600 win 9520 (DF) [tos 0x10]
0x0000   4510 0054 465a 4000 fe06 c1e9 ccfe af66        E..TFZ@.......f
0x0010   c1fb 35ef 0015 0fb7 4155 53b2 d633 53ac        ..5.....AUS..3S.
0x0020   5018 2530 f658 0000 3535 3020 2f5f 7072        P.%0.X..550./_pr
0x0030   6976 6174 652f 3a20 4e6f 2073 7563 6820        ivate/:.No.such.
0x0040   6669 6c65 206f 7220 6469 7265 6374 6f72        file.or.director
0x0050   792e                                          y.
05:48:35.011491 FTP.HACKER.53.239.4021 > OUR.NET.175.100.21: P 600:615(15) ack 1651 win 17395 (DF)
```

```
0x0000   4500 0037 b4aa 4000 7406 ddc8 c1fb 35ef        E..7..@.t.....5.
0x0010   ccfe af64 0fb5 0015 d631 9f37 d024 bbc4        ...d.....1.7.$..
0x0020   5018 43f3 f83d 0000 4357 4420 2f63 6769        P.C..=..CWD./cgi
0x0030   2d62 696e 2f0d 0a                              -bin/..
05:48:35.013914 OUR.NET.175.100.21 > FTP.HACKER.53.239.4021: P 1651:1694(43) ack 615 win 9520 (DF) [tos 0x10]
0x0000   4510 0053 8d05 4000 fe06 7b41 ccfe af64        E..S..@...{A...d
0x0010   c1fb 35ef 0015 0fb5 d024 bbc4 d631 9f46        ..5......$...1.F
0x0020   5018 2530 6fe9 0000 3535 3020 2f63 6769        P.%0o...550./cgi
0x0030   2d62 696e 2f3a 204e 6f20 7375 6368 2066        -bin/:.No.such.f
0x0040   696c 6520 6f72 2064 6972 6563 746f 7279        ile.or.directory
0x0050   2e0d                                          ..
05:48:35.015628 FTP.HACKER.53.239.4023 > OUR.NET.175.102.21: P 600:615(15) ack 1650 win 17395 (DF)
0x0000   4500 0037 b4ac 4000 7406 ddc4 c1fb 35ef        E..7..@.t.....5.
0x0010   ccfe af66 0fb7 0015 d633 53ac 4155 53de        ...f.....3S.AUS.
0x0020   5018 43f3 3a79 0000 4357 4420 2f63 6769        P.C.:y..CWD./cgi
0x0030   2d62 696e 2f0d 0a                              -bin/..
05:48:35.017992 OUR.NET.175.102.21 > FTP.HACKER.53.239.4023: P 1650:1693(43) ack 615 win 9520 (DF) [tos 0x10]
0x0000   4510 0053 465b 4000 fe06 c1e9 ccfe af66        E..SF[@........f
0x0010   c1fb 35ef 0015 0fb7 4155 53de d633 53bb        ..5.....AUS..3S.
0x0020   5018 2530 b224 0000 3535 3020 2f63 6769        P.%0.$..550./cgi
0x0030   2d62 696e 2f3a 204e 6f20 7375 6368 2066        -bin/:.No.such.f
0x0040   696c 6520 6f72 2064 6972 6563 746f 7279        ile.or.directory
0x0050   2e0d                                          ..
05:48:35.165667 FTP.HACKER.53.239.4021 > OUR.NET.175.100.21: P 615:626(11) ack 1694 win 17352 (DF)
0x0000   4500 0033 b4ae 4000 7406 ddc8 c1fb 35ef        E..3..@.t.....5.
0x0010   ccfe af64 0fb5 0015 d631 9f46 d024 bbef        ...d.....1.F.$..
0x0020   5018 43c8 82e8 0000 4357 4420 2f75 7372        P.C.....CWD./usr
0x0030   2f0d 0a                                        /..
05:48:35.168100 OUR.NET.175.100.21 > FTP.HACKER.53.239.4021: P 1694:1733(39) ack 626 win 9520 (DF) [tos 0x10]
0x0000   4510 004f 8d06 4000 fe06 7b44 ccfe af64        E..O..@...{D...d
0x0010   c1fb 35ef 0015 0fb5 d024 bbef d631 9f51        ..5......$...1.Q
0x0020   5018 2530 fa6c 0000 3535 3020 2f75 7372        P.%0.l..550./usr
0x0030   2f3a 204e 6f20 7375 6368 2066 696c 6520        /:.No.such.file.
0x0040   6f72 2064 6972 6563 746f 7279 2e0d 0a          or.directory...
05:48:35.169105 FTP.HACKER.53.239.4023 > OUR.NET.175.102.21: P 615:626(11) ack 1693 win 17352 (DF)
0x0000   4500 0033 b4b0 4000 7406 ddc4 c1fb 35ef        E..3..@.t.....5.
0x0010   ccfe af66 0fb7 0015 d633 53bb 4155 5409        ...f.....3S.AUT.
0x0020   5018 43c8 c523 0000 4357 4420 2f75 7372        P.C..#..CWD./usr
0x0030   2f0d 0a                                        /..
05:48:35.171458 OUR.NET.175.102.21 > FTP.HACKER.53.239.4023: P 1693:1732(39) ack 626 win 9520 (DF) [tos 0x10]
0x0000   4510 004f 465c 4000 fe06 c1ec ccfe af66        E..OF\@........f
0x0010   c1fb 35ef 0015 0fb7 4155 5409 d633 53c6        ..5.....AUT..3S.
0x0020   5018 2530 3ca8 0000 3535 3020 2f75 7372        P.%0<...550./usr
0x0030   2f3a 204e 6f20 7375 6368 2066 696c 6520        /:.No.such.file.
0x0040   6f72 2064 6972 6563 746f 7279 2e0d 0a          or.directory...
```

Source of Trace

This activity was detected on our network November 14, 2001.

Detect was Generated By

The data in this trace was the result of an ACID v0.9.6b13 query on alerts generated by Snort v1.8.1. and tcpdump data provided by SHADOW.

Probability the Source Address Was Spoofed

Unlikely. After reviewing the various trace information, it appears that a TCP three-way handshake took place.

Description of Attack

At first glance this activity appeared to be a simple SYN scan to port 21. As a standard response to a portscan, detailed information was gather from SHADOW (tcpdump).

First a query was compiled looking for any SYN/ACK activity. A SYN/ACK packet would indicate the server offers FTP as a service.

SYN/ACK(s)

```
05:48:21.547359 FTP.HACKER.53.239.3940 > OUR.NET.175.19.21: S 3589512893:3589512893(0) win 16384 <mss 1360,nop,nop,sackOK> (DF)
05:48:21.547639 OUR.NET.175.19.21 > FTP.HACKER.53.239.3940: S 557651437:557651437(0) ack 3589512894 win 65535 <mss 512>
05:48:21.976742 FTP.HACKER.53.239.4021 > OUR.NET.175.100.21: S 3593575647:3593575647(0) win 16384 <mss 1360,nop,nop,sackOK> (DF)
05:48:21.978392 OUR.NET.175.100.21 > FTP.HACKER.53.239.4021: S 3492066640:3492066640(0) ack 3593575648 win 9520 <mss 1360> (DF)
05:48:21.985756 FTP.HACKER.53.239.4023 > OUR.NET.175.102.21: S 3593687380:3593687380(0) win 16384 <mss 1360,nop,nop,sackOK> (DF)
05:48:21.986819 OUR.NET.175.102.21 > FTP.HACKER.53.239.4023: S 1096109419:1096109419(0) ack 3593687381 win 9520 <mss 1360> (DF)
```

The list of servers generated in the trace all run "Anonymous" FTP and checked out. Next a search was done for any servers responding with RST/ACK, which would indicate a "Closed Port" and more importantly a possible firewall configuration error.

RST/ACK(s)

```
05:48:22.783529 OUR.NET.175.250.21 > FTP.HACKER.53.239.4171: R 0:0(0) ack 3601181357 win 0
05:48:23.978568 OUR.NET.175.250.21 > FTP.HACKER.53.239.4171: R 0:0(0) ack 1 win 0
```

At this point any FTP sessions where reviewed in more detail. A query was created to review all PSH/ACK(s) that passed between the attacker and the three anonymous FTP servers.

PSH/ACK(s)

```
05:48:34.861090 FTP.HACKER.53.239.4023 > OUR.NET.175.102.21: P 584:600(16) ack 1606 win 17439 (DF)
0x0000   4500 0038 b4a8 4000 7406 ddc7 c1fb 35ef        E..8..@.t.....5.
0x0010   ccfe af66 0fb7 0015 d633 539c 4155 53b2        ...f.....3S.AUS.
0x0020   5018 441f c43c 0000 4357 4420 2f5f 7072        P.D..<..CWD./_pr
0x0030   6976 6174 652f 0d0a                            ivate/..
05:48:35.011491 FTP.HACKER.53.239.4021 > OUR.NET.175.100.21: P 600:615(15) ack 1651 win 17395 (DF)
0x0000   4500 0037 b4aa 4000 7406 ddc8 c1fb 35ef        E..7..@.t.....5.
0x0010   ccfe af64 0fb5 0015 d631 9f37 d024 bbc4        ...d.....1.7.$..
```

```
0x0020   5018 43f3 f83d 0000 4357 4420 2f63 6769        P.C..=..CWD./cgi
0x0030   2d62 696e 2f0d 0a                       -bin/..
05:48:35.015628 FTP.HACKER.53.239.4023 > OUR.NET.175.102.21: P 600:615(15) ack 1650 win 17395 (DF)
0x0000   4500 0037 b4ac 4000 7406 ddc4 c1fb 35ef        E..7..@.t.....5.
0x0010   ccfe af66 0fb7 0015 d633 53ac 4155 53de        ...f.....3S.AUS.
0x0020   5018 43f3 3a79 0000 4357 4420 2f63 6769        P.C.:y..CWD./cgi
0x0030   2d62 696e 2f0d 0a                       -bin/..
05:48:35.165667 FTP.HACKER.53.239.4021 > OUR.NET.175.100.21: P 615:626(11) ack 1694 win 17352 (DF)
0x0000   4500 0033 b4ae 4000 7406 ddc8 c1fb 35ef        E..3..@.t.....5.
0x0010   ccfe af64 0fb5 0015 d631 9f46 d024 bbef        ...d.....1.F.$..
0x0020   5018 43c8 82e8 0000 4357 4420 2f75 7372        P.C.....CWD./usr
0x0030   2f0d 0a                                /..
05:48:35.169105 FTP.HACKER.53.239.4023 > OUR.NET.175.102.21: P 615:626(11) ack 1693 win 17352 (DF)
0x0000   4500 0033 b4b0 4000 7406 ddc4 c1fb 35ef        E..3..@.t.....5.
0x0010   ccfe af66 0fb7 0015 d633 53bb 4155 5409        ...f.....3S.AUT.
0x0020   5018 43c8 c523 0000 4357 4420 2f75 7372        P.C..#..CWD./usr
0x0030   2f0d 0a                                /..
```

After reviewing the data it appeared that this incident was much more then a simple SYN scan. Once the attacker found an open FTP server they attempt to logon anonymously and access certain directories. The directories attempted, "/_private", "/cgi-bin", and "/usr" are known web server and system roots that should not be accessible via anonymous FTP.

Attack Mechanism

Based on the relatively speed (< 30 seconds) it appears that the attackers activity was scripted. The script will apparently perform a SYN scan to port 21 on any number of IPs. If the destination host replies with a SYN/ACK the script will logon anonymously and attempt command line executions.

Correlations

www.DSHIELD.org has report port 21 (FTP) as one of it's "TOP 10 Probed Ports" for sometime. On November 14, 2001 DSHIELD reported over 40,000 counts of FTP probes, which accounted for 2.5% of all submissions.

Evidence of Active Targeting

Yes. The attacker scanned a portion of our network then attempted to access various system directories via FTP.

Severity

Low: Need to verify that systems responding with RST/ACK are secure.

Attack Severity = (3+1) - (3+4) = -3

Severity Component	Rating	Description
Criticality	3	The machines in question are anonymous FTP servers holding public accessible documents.

Lethality	1	A directory traversal attempt was unsuccessful.
System Countermeasures	3	Latest Operating system and unknown security patch level.
Network Countermeasures	4	Multiple restrictive firewalls

Defensive Recommendation

Verify all firewall rules, which allow FTP traffic and attempt to account for the RST/ACK traffic seen in the traces above. Establish that all anonymous FTP servers have been locked down and patched properly. If not already configured, configure syslogs on FTP servers to track failed attempts and monitor on a regular basis.

Multiple Choice Test Question

Which tcpdump filter would show TCP SYN activity only?

A. tcpdump -r file "tcp[13]=SYN"
B. tcpdump -r file "SYN flag"
C. tcpdump -r file "tcp[13]=2"
D. tcpdump -r file "tcp[13]=18"

Answer: C

Network Detect - 4 (ICMP Broadscan Smurf Scanner)

Trace

```
---------------------------------------------------------------------------
#(1 - 19920) [2001-10-27 18:47:34]  ICMP Broadscan Smurf Scanner
IPv4: SMURF.SCAN.205.254 -> OUR.NET.136.0
     hlen=5 TOS=0 dlen=32 ID=2517 flags=0 offset=0 TTL=244 chksum=34988
ICMP: type=Echo Request code=0
     checksum=63487 id=0 seq=0
Payload:  length = 4

000 : 9F 89 88 00                                    ....
---------------------------------------------------------------------------
#(1 - 19921) [2001-10-27 18:47:34]  ICMP Broadscan Smurf Scanner
IPv4: SMURF.SCAN.205.254 -> OUR.NET.136.8
     hlen=5 TOS=0 dlen=32 ID=2517 flags=0 offset=0 TTL=244 chksum=34980
ICMP: type=Echo Request code=0
     checksum=63487 id=0 seq=0
Payload:  length = 4

000 : 9F 89 88 08                                    ....
```

```
------------------------------------------------------------------------------
#(1 - 19922) [2001-10-27 18:47:34]  ICMP Broadscan Smurf Scanner
IPv4: SMURF.SCAN.205.254 -> OUR.NET.136.63
      hlen=5 TOS=0 dlen=32 ID=2517 flags=0 offset=0 TTL=244 chksum=34925
ICMP: type=Echo Request code=0
      checksum=63487 id=0 seq=0
Payload:  length = 4

000 : 9F 89 88 3F                                    ...?
------------------------------------------------------------------------------
#(1 - 19923) [2001-10-27 18:47:34]  ICMP Broadscan Smurf Scanner
IPv4: SMURF.SCAN.205.254 -> OUR.NET.136.64
      hlen=5 TOS=0 dlen=32 ID=2517 flags=0 offset=0 TTL=244 chksum=34924
ICMP: type=Echo Request code=0
      checksum=63487 id=0 seq=0
Payload:  length = 4

000 : 9F 89 88 40                                    ...@
------------------------------------------------------------------------------
#(1 - 19924) [2001-10-27 18:47:34]  ICMP Broadscan Smurf Scanner
IPv4: SMURF.SCAN.205.254 -> OUR.NET.136.127
      hlen=5 TOS=0 dlen=32 ID=2517 flags=0 offset=0 TTL=244 chksum=34861
ICMP: type=Echo Request code=0
      checksum=63487 id=0 seq=0
Payload:  length = 4

000 : 9F 89 88 7F                                    ...
------------------------------------------------------------------------------
#(1 - 19925) [2001-10-27 18:47:34]  ICMP Broadscan Smurf Scanner
IPv4: SMURF.SCAN.205.254 -> OUR.NET.136.128
      hlen=5 TOS=0 dlen=32 ID=2517 flags=0 offset=0 TTL=244 chksum=34860
ICMP: type=Echo Request code=0
      checksum=63487 id=0 seq=0
Payload:  length = 4

000 : 9F 89 88 80                                    ....
------------------------------------------------------------------------------
```

Source of Trace

This activity was detected on our network October 27, 2001.

Detect was Generated By

The data in this trace was the result of an ACID v0.9.6b13 query on alerts generated by Snort v1.8.1.

Probability the Source Address Was Spoofed

Very Low. The probability that the source address was spoofed is low, because the hacker is looking for a response from the destination server.

Description of Attack

This activity is an indication of a hacker looking to compile a list of network broadcast addresses for a future DoS attack.

Attack Mechanism

The script used for this attack will generate traffic to known network broadcast addresses. In this case addresses created when large address blocks are divided into smaller subnets. If the hacker receives a response them can use this information in conjunction with tools like smurf, papsmurf or fraggle and attempt a denial of services attack.

Correlations

DoS attacks and tools are widely documented. A document written by DeokJo Jeon, "Understanding DDOS Attack, Tools and Free Anti-tools with Recommendation" is available on the sans website at http://www.sans.org/infosecFAQ/threats/understanding_ddos.htm

Evidence of Active Targeting

Yes. The attack in this case is looking to gain information on how our network is subnetted.

Severity

Low: Security mechanisms are in place to deny this attack.

Attack Severity = (5+4) - (4+4) = 1

Severity Component	Rating	Description
Criticality	5	This activity is a precursor to an attack that could affect the entire network.
Lethality	4	If successful the attacker could use the information gather to launch a denial of service attack.
System Countermeasures	4	Latest Operating system and unknown security patch level.
Network Countermeasures	4	Multiple restrictive firewalls

Defensive Recommendation

In the implementation of firewall or router ACL rules be very cautions about allowing ICMP traffic. Although ICMP tools like ping are invaluable for network troubleshooting, they can be used against you. As a general rule of thumb, only allow ICMP traffic to those servers that absolutely require it.

Multiple Choice Test Question

A hacker using "Broadscan Smurf Scanner" is looking to compile what information about your network?

A) Network mask
B) IP address
C) Gateways
D) Broadcast Addresses

Answer: D

Network Detect - 5 (SYN Scan to ports above 1024)

Trace

Snort Portscan Log

Nov	7	20	0	16	SYN.SCAN.214.5	54152	->	OUR.NET.175.6	20010	SYN	******S*
Nov	7	20	0	17	SYN.SCAN.214.5	54153	->	OUR.NET.175.6	48110	SYN	******S*
Nov	7	20	0	17	SYN.SCAN.214.5	54154	->	OUR.NET.175.6	48773	SYN	******S*
Nov	7	20	0	17	SYN.SCAN.214.5	54155	->	OUR.NET.175.6	53159	SYN	******S*
Nov	7	20	0	17	SYN.SCAN.214.5	54156	->	OUR.NET.175.6	17182	SYN	******S*
Nov	7	20	0	18	SYN.SCAN.214.5	54157	->	OUR.NET.175.6	49018	SYN	******S*
Nov	7	20	0	18	SYN.SCAN.214.5	54158	->	OUR.NET.175.6	64129	SYN	******S*
Nov	7	20	0	18	SYN.SCAN.214.5	54159	->	OUR.NET.175.6	21799	SYN	******S*
Nov	7	20	0	18	SYN.SCAN.214.5	54160	->	OUR.NET.175.6	50765	SYN	******S*
Nov	7	20	0	19	SYN.SCAN.214.5	54161	->	OUR.NET.175.6	49266	SYN	******S*
Nov	7	20	0	19	SYN.SCAN.214.5	54162	->	OUR.NET.175.6	55069	SYN	******S*
Nov	7	20	0	19	SYN.SCAN.214.5	54163	->	OUR.NET.175.6	24049	SYN	******S*
Nov	7	20	0	19	SYN.SCAN.214.5	54164	->	OUR.NET.175.6	54949	SYN	******S*
Nov	7	20	0	19	SYN.SCAN.214.5	54165	->	OUR.NET.175.6	19838	SYN	******S*
Nov	7	20	0	20	SYN.SCAN.214.5	54166	->	OUR.NET.175.6	49515	SYN	******S*
Nov	7	20	0	20	SYN.SCAN.214.5	54168	->	OUR.NET.175.6	46010	SYN	******S*
Nov	7	20	0	20	SYN.SCAN.214.5	54169	->	OUR.NET.175.6	13782	SYN	******S*
Nov	7	20	0	20	SYN.SCAN.214.5	54170	->	OUR.NET.175.6	23587	SYN	******S*
Nov	7	20	0	20	SYN.SCAN.214.5	54171	->	OUR.NET.175.6	53423	SYN	******S*
Nov	7	20	0	21	SYN.SCAN.214.5	54173	->	OUR.NET.175.6	49763	SYN	******S*
Nov	7	20	0	21	SYN.SCAN.214.5	54174	->	OUR.NET.175.6	36950	SYN	******S*
Nov	7	20	0	21	SYN.SCAN.214.5	54175	->	OUR.NET.175.6	56738	SYN	******S*
Nov	7	20	0	21	SYN.SCAN.214.5	54176	->	OUR.NET.175.6	22494	SYN	******S*
Nov	7	20	0	22	SYN.SCAN.214.5	54177	->	OUR.NET.175.6	50009	SYN	******S*
Nov	7	20	0	22	SYN.SCAN.214.5	54178	->	OUR.NET.175.6	27892	SYN	******S*
Nov	7	20	0	22	SYN.SCAN.214.5	54179	->	OUR.NET.175.6	57761	SYN	******S*
Nov	7	20	0	22	SYN.SCAN.214.5	54180	->	OUR.NET.175.6	25377	SYN	******S*
Nov	7	20	0	22	SYN.SCAN.214.5	54181	->	OUR.NET.175.6	56079	SYN	******S*
Nov	7	20	0	23	SYN.SCAN.214.5	54182	->	OUR.NET.175.6	50257	SYN	******S*
Nov	7	20	0	23	SYN.SCAN.214.5	54183	->	OUR.NET.175.6	18832	SYN	******S*
Nov	7	20	0	23	SYN.SCAN.214.5	54184	->	OUR.NET.175.6	58526	SYN	******S*
Nov	7	20	0	23	SYN.SCAN.214.5	54185	->	OUR.NET.175.6	25150	SYN	******S*

Nov	7	20	0	24	SYN.SCAN.214.5	54186	->	OUR.NET.175.6	50505	SYN	******S*
Nov	7	20	0	24	SYN.SCAN.214.5	54187	->	OUR.NET.175.6	9774	SYN	******S*
Nov	7	20	0	24	SYN.SCAN.214.5	54188	->	OUR.NET.175.6	37228	SYN	******S*
Nov	7	20	0	24	SYN.SCAN.214.5	54189	->	OUR.NET.175.6	27166	SYN	******S*
Nov	7	20	0	25	SYN.SCAN.214.5	54190	->	OUR.NET.175.6	60315	SYN	******S*
Nov	7	20	0	26	SYN.SCAN.214.5	54191	->	OUR.NET.175.6	27808	SYN	******S*
Nov	7	20	0	26	SYN.SCAN.214.5	54192	->	OUR.NET.175.6	50999	SYN	******S*
Nov	7	20	0	26	SYN.SCAN.214.5	54193	->	OUR.NET.175.6	56167	SYN	******S*
Nov	7	20	0	26	SYN.SCAN.214.5	54195	->	OUR.NET.175.6	28954	SYN	******S*
Nov	7	20	0	28	SYN.SCAN.214.5	54196	->	OUR.NET.175.6	62103	SYN	******S*
Nov	7	20	0	28	SYN.SCAN.214.5	54198	->	OUR.NET.175.6	30463	SYN	******S*
Nov	7	20	0	28	SYN.SCAN.214.5	54199	->	OUR.NET.175.6	30743	SYN	******S*
Nov	7	20	0	28	SYN.SCAN.214.5	54201	->	OUR.NET.175.6	64046	SYN	******S*
Nov	7	20	0	29	SYN.SCAN.214.5	54202	->	OUR.NET.175.6	51741	SYN	******S*
Nov	7	20	0	29	SYN.SCAN.214.5	54205	->	OUR.NET.175.6	28988	SYN	******S*
Nov	7	20	0	29	SYN.SCAN.214.5	54206	->	OUR.NET.175.6	63893	SYN	******S*
Nov	7	20	0	29	SYN.SCAN.214.5	54207	->	OUR.NET.175.6	33119	SYN	******S*
Nov	7	20	0	30	SYN.SCAN.214.5	54208	->	OUR.NET.175.6	51989	SYN	******S*
Nov	7	20	0	30	SYN.SCAN.214.5	54209	->	OUR.NET.175.6	19930	SYN	******S*
Nov	7	20	0	30	SYN.SCAN.214.5	54211	->	OUR.NET.175.6	32531	SYN	******S*
Nov	7	20	0	30	SYN.SCAN.214.5	54212	->	OUR.NET.175.6	2193	SYN	******S*
Nov	7	20	0	31	SYN.SCAN.214.5	54213	->	OUR.NET.175.6	52238	SYN	******S*
Nov	7	20	0	31	SYN.SCAN.214.5	54214	->	OUR.NET.175.6	10872	SYN	******S*
Nov	7	20	0	31	SYN.SCAN.214.5	54215	->	OUR.NET.175.6	29875	SYN	******S*
Nov	7	20	0	31	SYN.SCAN.214.5	54216	->	OUR.NET.175.6	1171	SYN	******S*
Nov	7	20	0	32	SYN.SCAN.214.5	54217	->	OUR.NET.175.6	35776	SYN	******S*
Nov	7	20	0	32	SYN.SCAN.214.5	54218	->	OUR.NET.175.6	52486	SYN	******S*
Nov	7	20	0	32	SYN.SCAN.214.5	54219	->	OUR.NET.175.6	1814	SYN	******S*
Nov	7	20	0	32	SYN.SCAN.214.5	54220	->	OUR.NET.175.6	34320	SYN	******S*
Nov	7	20	0	32	SYN.SCAN.214.5	54221	->	OUR.NET.175.6	4849	SYN	******S*
Nov	7	20	0	33	SYN.SCAN.214.5	54222	->	OUR.NET.175.6	52732	SYN	******S*
Nov	7	20	0	33	SYN.SCAN.214.5	54224	->	OUR.NET.175.6	57264	SYN	******S*
Nov	7	20	0	33	SYN.SCAN.214.5	54225	->	OUR.NET.175.6	9342	SYN	******S*
Nov	7	20	0	33	SYN.SCAN.214.5	54226	->	OUR.NET.175.6	2959	SYN	******S*
Nov	7	20	0	34	SYN.SCAN.214.5	54227	->	OUR.NET.175.6	38432	SYN	******S*
Nov	7	20	0	34	SYN.SCAN.214.5	54228	->	OUR.NET.175.6	52980	SYN	******S*
Nov	7	20	0	34	SYN.SCAN.214.5	54229	->	OUR.NET.175.6	48206	SYN	******S*
Nov	7	20	0	34	SYN.SCAN.214.5	54230	->	OUR.NET.175.6	36110	SYN	******S*
Nov	7	20	0	34	SYN.SCAN.214.5	54231	->	OUR.NET.175.6	7504	SYN	******S*
Nov	7	20	0	35	SYN.SCAN.214.5	54232	->	OUR.NET.175.6	53228	SYN	******S*
Nov	7	20	0	35	SYN.SCAN.214.5	54233	->	OUR.NET.175.6	39146	SYN	******S*
Nov	7	20	0	35	SYN.SCAN.214.5	54234	->	OUR.NET.175.6	53321	SYN	******S*
Nov	7	20	0	35	SYN.SCAN.214.5	54235	->	OUR.NET.175.6	4748	SYN	******S*

Shadow Trace (TCPDUMP) - SYN,ACK Responses to SYN

```
20:00:12.219929 OUR.NET.175.6.47794 > SYN.SCAN.214.5.54148: S 4271772298:4271772298(0) ack 199720311 win 65535 <mss 512>
20:00:12.373504 OUR.NET.175.6.9213 > SYN.SCAN.214.5.54149: S 1407479487:1407479487(0) ack 199812457 win 65535 <mss 512>
20:00:12.612456 OUR.NET.175.6.21 > SYN.SCAN.214.5.54151: S 305666938:305666938(0) ack 199907346 win 65535 <mss 512>
20:00:16.849960 OUR.NET.175.6.20010 > SYN.SCAN.214.5.54152: S 2175663871:2175663871(0) ack 200938526 win 65535 <mss 512>
```

20:00:17.281476 OUR.NET.175.6.48110 > SYN.SCAN.214.5.54153: S 3755643851:3755643851(0) ack 201078876 win 65535 <mss 512>
20:00:17.496184 OUR.NET.175.6.48773 > SYN.SCAN.214.5.54154: S 202298400:202298400(0) ack 201172464 win 65535 <mss 512>
20:00:17.714756 OUR.NET.175.6.53159 > SYN.SCAN.214.5.54155: S 742655014:742655014(0) ack 201259431 win 65535 <mss 512>
20:00:17.934675 OUR.NET.175.6.17182 > SYN.SCAN.214.5.54156: S 3344704210:3344704210(0) ack 201362499 win 65535 <mss 512>
20:00:18.151477 OUR.NET.175.6.49018 > SYN.SCAN.214.5.54157: S 1197186564:1197186564(0) ack 201459591 win 65535 <mss 512>
20:00:18.371498 OUR.NET.175.6.64129 > SYN.SCAN.214.5.54158: S 1254851676:1254851676(0) ack 201566486 win 65535 <mss 512>
20:00:18.589068 OUR.NET.175.6.21799 > SYN.SCAN.214.5.54159: S 2253914878:2253914878(0) ack 201675455 win 65535 <mss 512>
20:00:18.812087 OUR.NET.175.6.50765 > SYN.SCAN.214.5.54160: S 3326024096:3326024096(0) ack 201786912 win 65535 <mss 512>
20:00:19.026291 OUR.NET.175.6.49266 > SYN.SCAN.214.5.54161: S 674890947:674890947(0) ack 201878788 win 65535 <mss 512>
20:00:19.246306 OUR.NET.175.6.55069 > SYN.SCAN.214.5.54162: S 2454877622:2454877622(0) ack 201971839 win 65535 <mss 512>
20:00:19.465072 OUR.NET.175.6.24049 > SYN.SCAN.214.5.54163: S 3585485050:3585485050(0) ack 202061697 win 65535 <mss 512>
20:00:19.682536 OUR.NET.175.6.54949 > SYN.SCAN.214.5.54164: S 1662421939:1662421939(0) ack 202169398 win 65535 <mss 512>
20:00:19.904514 OUR.NET.175.6.19838 > SYN.SCAN.214.5.54165: S 3734724926:3734724926(0) ack 202265603 win 65535 <mss 512>
20:00:20.121659 OUR.NET.175.6.49515 > SYN.SCAN.214.5.54166: S 3172773304:3172773304(0) ack 202359754 win 65535 <mss 512>
20:00:20.340420 OUR.NET.175.6.46010 > SYN.SCAN.214.5.54168: S 3060553471:3060553471(0) ack 202442663 win 65535 <mss 512>
20:00:20.557786 OUR.NET.175.6.13782 > SYN.SCAN.214.5.54169: S 252944784:252944784(0) ack 202536823 win 65535 <mss 512>
20:00:20.775204 OUR.NET.175.6.23587 > SYN.SCAN.214.5.54170: S 1143263797:1143263797(0) ack 202647276 win 65535 <mss 512>
20:00:20.995301 OUR.NET.175.6.53423 > SYN.SCAN.214.5.54171: S 12100380:12100380(0) ack 202731477 win 65535 <mss 512>
20:00:21.213255 OUR.NET.175.6.49763 > SYN.SCAN.214.5.54173: S 1497669871:1497669871(0) ack 202841142 win 65535 <mss 512>
20:00:21.431717 OUR.NET.175.6.36950 > SYN.SCAN.214.5.54174: S 371524834:371524834(0) ack 202926545 win 65535 <mss 512>
20:00:21.648854 OUR.NET.175.6.56738 > SYN.SCAN.214.5.54175: S 3364583699:3364583699(0) ack 203022637 win 65535 <mss 512>
20:00:21.870910 OUR.NET.175.6.22494 > SYN.SCAN.214.5.54176: S 1155667071:1155667071(0) ack 203115255 win 65535 <mss 512>
20:00:22.092329 OUR.NET.175.6.50009 > SYN.SCAN.214.5.54177: S 3440917101:3440917101(0) ack 203226128 win 65535 <mss 512>
20:00:22.305898 OUR.NET.175.6.27892 > SYN.SCAN.214.5.54178: S 4249594746:4249594746(0) ack 203320388 win 65535 <mss 512>
20:00:22.525620 OUR.NET.175.6.57761 > SYN.SCAN.214.5.54179: S 3255787495:3255787495(0) ack 203415614 win 65535 <mss 512>
20:00:22.743101 OUR.NET.175.6.25377 > SYN.SCAN.214.5.54180: S 833788285:833788285(0) ack 203529302 win 65535 <mss 512>
20:00:22.961547 OUR.NET.175.6.56079 > SYN.SCAN.214.5.54181: S 2862663802:2862663802(0) ack 203626998 win 65535 <mss 512>
20:00:23.181875 OUR.NET.175.6.50257 > SYN.SCAN.214.5.54182: S 1622049152:1622049152(0) ack 203724196 win 65535 <mss 512>
20:00:23.400054 OUR.NET.175.6.18832 > SYN.SCAN.214.5.54183: S 3814903847:3814903847(0) ack 203834704 win 65535 <mss 512>
20:00:23.617889 OUR.NET.175.6.58526 > SYN.SCAN.214.5.54184: S 3950295419:3950295419(0) ack 203948239 win 65535 <mss 512>
20:00:23.837019 OUR.NET.175.6.25150 > SYN.SCAN.214.5.54185: S 1506108260:1506108260(0) ack 204059712 win 65535 <mss 512>
20:00:24.057759 OUR.NET.175.6.50505 > SYN.SCAN.214.5.54186: S 1462359117:1462359117(0) ack 204155768 win 65535 <mss 512>
20:00:24.275209 OUR.NET.175.6.9774 > SYN.SCAN.214.5.54187: S 3844445034:3844445034(0) ack 204249210 win 65535 <mss 512>
20:00:24.492853 OUR.NET.175.6.37228 > SYN.SCAN.214.5.54188: S 3242248108:3242248108(0) ack 204357058 win 65535 <mss 512>
20:00:24.713531 OUR.NET.175.6.27166 > SYN.SCAN.214.5.54189: S 1543366882:1543366882(0) ack 204445147 win 65535 <mss 512>
20:00:25.952942 OUR.NET.175.6.60315 > SYN.SCAN.214.5.54190: S 3630748036:3630748036(0) ack 204765824 win 65535 <mss 512>
20:00:26.132753 OUR.NET.175.6.27808 > SYN.SCAN.214.5.54191: S 1438222429:1438222429(0) ack 204875652 win 65535 <mss 512>
20:00:26.350997 OUR.NET.175.6.50999 > SYN.SCAN.214.5.54192: S 3120243478:3120243478(0) ack 204990334 win 65535 <mss 512>
20:00:26.570465 OUR.NET.175.6.56167 > SYN.SCAN.214.5.54193: S 1015258468:1015258468(0) ack 205085961 win 65535 <mss 512>
20:00:26.898962 OUR.NET.175.6.28954 > SYN.SCAN.214.5.54195: S 1465805481:1465805481(0) ack 205200974 win 65535 <mss 512>
20:00:28.214887 OUR.NET.175.6.62103 > SYN.SCAN.214.5.54196: S 584330685:584330685(0) ack 205548876 win 65535 <mss 512>
20:00:28.488048 OUR.NET.175.6.30463 > SYN.SCAN.214.5.54198: S 1742553095:1742553095(0) ack 205654544 win 65535 <mss 512>
20:00:28.647201 OUR.NET.175.6.30743 > SYN.SCAN.214.5.54199: S 2420416339:2420416339(0) ack 205750932 win 65535 <mss 512>
20:00:28.867603 OUR.NET.175.6.64046 > SYN.SCAN.214.5.54201: S 1989350730:1989350730(0) ack 205861996 win 65535 <mss 512>
20:00:29.085571 OUR.NET.175.6.51741 > SYN.SCAN.214.5.54202: S 4256282064:4256282064(0) ack 205948685 win 65535 <mss 512>
20:00:29.303105 OUR.NET.175.6.28988 > SYN.SCAN.214.5.54203: S 905686790:905686790(0) ack 206037031 win 65535 <mss 512>
20:00:29.521842 OUR.NET.175.6.28988 > SYN.SCAN.214.5.54205: S 1675459022:1675459022(0) ack 206141195 win 65535 <mss 512>
20:00:29.739655 OUR.NET.175.6.63893 > SYN.SCAN.214.5.54206: S 1079465147:1079465147(0) ack 206237337 win 65535 <mss 512>
20:00:29.958740 OUR.NET.175.6.33119 > SYN.SCAN.214.5.54207: S 2953157700:2953157700(0) ack 206339928 win 65535 <mss 512>
20:00:30.177361 OUR.NET.175.6.51989 > SYN.SCAN.214.5.54208: S 3861345071:3861345071(0) ack 206430648 win 65535 <mss 512>
20:00:30.396459 OUR.NET.175.6.19930 > SYN.SCAN.214.5.54209: S 2685968384:2685968384(0) ack 206540025 win 65535 <mss 512>
20:00:30.614628 OUR.NET.175.6.32531 > SYN.SCAN.214.5.54211: S 59313675:59313675(0) ack 206625215 win 65535 <mss 512>
20:00:30.834553 OUR.NET.175.6.2193 > SYN.SCAN.214.5.54212: S 3309609718:3309609718(0) ack 206738758 win 65535 <mss 512>
20:00:31.053621 OUR.NET.175.6.52238 > SYN.SCAN.214.5.54213: S 1464963968:1464963968(0) ack 206832579 win 65535 <mss 512>

```
20:00:31.271495 OUR.NET.175.6.10872 > SYN.SCAN.214.5.54214: S 2951821205:2951821205(0) ack 206941112 win 65535 <mss 512>
20:00:31.490462 OUR.NET.175.6.29875 > SYN.SCAN.214.5.54215: S 2601579850:2601579850(0) ack 207027636 win 65535 <mss 512>
20:00:31.801195 OUR.NET.175.6.1171 > SYN.SCAN.214.5.54216: S 4235182068:4235182068(0) ack 207140393 win 65535 <mss 512>
20:00:32.036840 OUR.NET.175.6.35776 > SYN.SCAN.214.5.54217: S 3806524513:3806524513(0) ack 207256130 win 65535 <mss 512>
20:00:32.254328 OUR.NET.175.6.52486 > SYN.SCAN.214.5.54218: S 3669765887:3669765887(0) ack 207350232 win 65535 <mss 512>
20:00:32.473392 OUR.NET.175.6.1814 > SYN.SCAN.214.5.54219: S 3811395629:3811395629(0) ack 207452560 win 65535 <mss 512>
20:00:32.692386 OUR.NET.175.6.34320 > SYN.SCAN.214.5.54220: S 1661737183:1661737183(0) ack 207551998 win 65535 <mss 512>
20:00:32.910340 OUR.NET.175.6.4849 > SYN.SCAN.214.5.54221: S 493797711:493797711(0) ack 207643978 win 65535 <mss 512>
20:00:33.129743 OUR.NET.175.6.52732 > SYN.SCAN.214.5.54222: S 4223679915:4223679915(0) ack 207757991 win 65535 <mss 512>
20:00:33.349213 OUR.NET.175.6.57264 > SYN.SCAN.214.5.54224: S 1642369713:1642369713(0) ack 207859430 win 65535 <mss 512>
20:00:33.575153 OUR.NET.175.6.9342 > SYN.SCAN.214.5.54225: S 1845237307:1845237307(0) ack 207955795 win 65535 <mss 512>
20:00:33.785806 OUR.NET.175.6.2959 > SYN.SCAN.214.5.54226: S 253622603:253622603(0) ack 208042679 win 65535 <mss 512>
20:00:34.005665 OUR.NET.175.6.38432 > SYN.SCAN.214.5.54227: S 1535818124:1535818124(0) ack 208137903 win 65535 <mss 512>
20:00:34.227989 OUR.NET.175.6.52980 > SYN.SCAN.214.5.54228: S 2813021155:2813021155(0) ack 208221019 win 65535 <mss 512>
20:00:34.441949 OUR.NET.175.6.48206 > SYN.SCAN.214.5.54229: S 790341668:790341668(0) ack 208328459 win 65535 <mss 512>
20:00:34.660177 OUR.NET.175.6.36110 > SYN.SCAN.214.5.54230: S 747722047:747722047(0) ack 208419536 win 65535 <mss 512>
20:00:34.878683 OUR.NET.175.6.7504 > SYN.SCAN.214.5.54231: S 237313435:237313435(0) ack 208523466 win 65535 <mss 512>
20:00:35.097461 OUR.NET.175.6.53228 > SYN.SCAN.214.5.54232: S 1455920923:1455920923(0) ack 208612294 win 65535 <mss 512>
20:00:35.318271 OUR.NET.175.6.39146 > SYN.SCAN.214.5.54233: S 571352739:571352739(0) ack 208707864 win 65535 <mss 512>
20:00:35.535207 OUR.NET.175.6.53321 > SYN.SCAN.214.5.54234: S 421688837:421688837(0) ack 208806938 win 65535 <mss 512>
20:00:35.752835 OUR.NET.175.6.4748 > SYN.SCAN.214.5.54235: S 3104212011:3104212011(0) ack 208901224 win 65535 <mss 51
```

Source of Trace

This activity was detected on our network on November 7, 2001.

Detect was Generated By

The data in this trace was the result of an ACID v0.9.6b13 query on alerts generated by Snort v1.8.1. and tcpdump data provided by SHADOW.

Probability the Source Address Was Spoofed

Unlikely. After reviewing the various trace information, it appears that a TCP three-way handshake took place.

Description of Attack

The Attacker sent at total of 79 SYN packets to random ports, of which the majority where above port 1024.

```
Nov  7  20  0  16  SYN.SCAN.214.5  54152  ->  OUR.NET.175.6  20010  SYN  ******S*
Nov  7  20  0  17  SYN.SCAN.214.5  54153  ->  OUR.NET.175.6  48110  SYN  ******S*
Nov  7  20  0  17  SYN.SCAN.214.5  54154  ->  OUR.NET.175.6  48773  SYN  ******S*
Nov  7  20  0  17  SYN.SCAN.214.5  54155  ->  OUR.NET.175.6  53159  SYN  ******S*
Nov  7  20  0  17  SYN.SCAN.214.5  54156  ->  OUR.NET.175.6  17182  SYN  ******S*
```

Our standard response to a portscan is to review all traffic related to the source IP with SHADOW.

```
20:00:12.219929 OUR.NET.175.6.47794 > SYN.SCAN.214.5.54148: S 4271772298:4271772298(0) ack 199720311 win 65535 <mss 512>
```

```
20:00:12.373504 OUR.NET.175.6.9213 > SYN.SCAN.214.5.54149: S 1407479487:1407479487(0) ack 199812457 win 65535 <mss 512>
20:00:12.612456 OUR.NET.175.6.21 > SYN.SCAN.214.5.54151: S 305666938:305666938(0) ack 199907346 win 65535 <mss 512>
20:00:16.849960 OUR.NET.175.6.20010 > SYN.SCAN.214.5.54152: S 2175663871:2175663871(0) ack 200938526 win 65535 <mss 512>
20:00:17.281476 OUR.NET.175.6.48110 > SYN.SCAN.214.5.54153: S 3755643851:3755643851(0) ack 201078876 win 65535 <mss 512>
20:00:17.496184 OUR.NET.175.6.48773 > SYN.SCAN.214.5.54154: S 202298400:202298400(0) ack 201172464 win 65535 <mss 512>
20:00:17.714756 OUR.NET.175.6.53159 > SYN.SCAN.214.5.54155: S 742655014:742655014(0) ack 201259431 win 65535 <mss 512>
```

Evaluating the data from SHADOW showed that the destination host appears to have responded to all of these packets with a SYN/ACK (based on a BFP filter run on an hourly tcpdump file: tcpdump -r - "dst host 64.132.214.5 and tcp[13]=18").

This is the part that is extremely odd. Why did the server or device respond to with a SYN/ACK to all these ports? Especially, the ones over port 1024. If there was to be any response to this scan I would have expected RST/ACK instead of SYN/ACK

Attack Mechanism

This attack could a have been accomplished by any number of scanning tools. This would include nmap, hping or netcat.

Correlations

SYN scan are and will remain a poplar method of system and network reconnaissance. The attack mechanism has be reported numerous times in the past at www.sans.org, including this post : http://www.sans.org/y2k/042200.htm

Evidence of Active Targeting

Yes. There the attacker scanned a specific server looking for open ports above 1024.

Severity

High: It is unknown what the function and purpose of the destination server is.

Attack Severity = (4+4) - (0+4) = 4

Severity Component	Rating	Description
Criticality	4	Function, location, state and owner of server is UNKNOWN.
Lethality	4	Function, location, state and owner of server is UNKNOWN.
System Countermeasures	0	Function, location, state and owner of server is UNKNOWN.
Network Countermeasures	4	Multiple restrictive firewalls

Defensive Recommendation

As mention previously the function and location of this server is unknown. The server or network device administrator needs to be found and questioned about this machine

and why it responded in the manner it did.

Multiple Choice Test Question

What combination of TCP flags would indicate the second part of a three-way handshake?

A. SYN, ACK
B. PSH, ACK
C. RST
D. RST, ACK

Answer: A

Assignment 3 - Analysis This

Introduction

The purpose of this report is to analysis Snort alert files provided by client X. Analysis was completed in three areas, including Signature Alerts, Portscan Activity and Out of Spec traffic. Each of the three areas was broken out to reveal statistical data showing what activity was seen most frequently, who was creating it and why.

Alert Summary

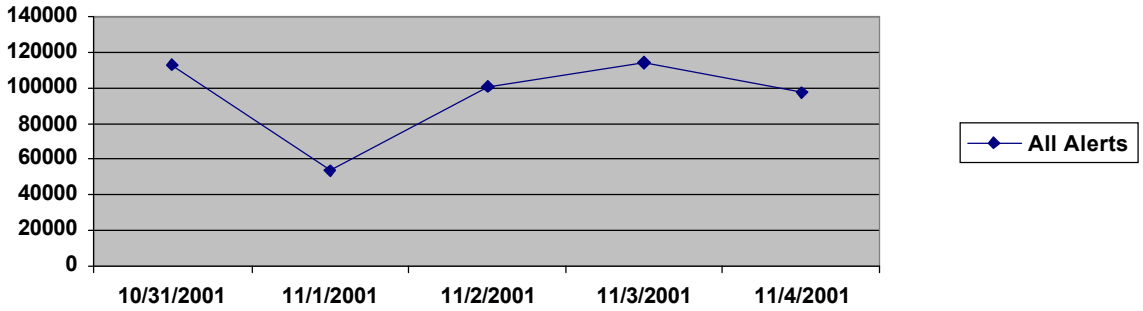
The log begins from: 10/31/01 00:01:01
The log ends at: 11/04/01 23:52:14
Total events: 166293
Signatures recorded: 22
Source IP recorded: 24414
Destination IP recorded: 9644

% of Alerts	# of Alerts	Alert Signature
56.26	93562	UDP SRC and DST outside network
14.17	23565	TCP SRC and DST outside network
12.69	21103	Tiny Fragments - Possible Hostile Activity
9.94	16525	SMB Name Wildcard
2.05	3403	Possible trojan server activity
2.00	3321	Watchlist 000222 NET-NCFC
0.82	1371	External RPC call
0.67	1111	High port 65535 udp - possible Red Worm - traffic
0.59	982	Watchlist 000220 IL-ISDNNET-990517
0.35	583	Queso fingerprint
0.12	199	connect to 515 from outside
0.05	90	Null scan!
0.05	80	High port 65535 tcp - possible Red Worm - traffic
0.05	77	WinGate 1080 Attempt
0.05	76	Port 55850 tcp - Possible myserver activity - ref. 010313-1
0.04	70	connect to 515 from inside
0.04	67	NMAP TCP ping!
0.02	41	SUNRPC highport access!
0.02	35	Back Orifice
0.02	25	SNMP public access

0.00	5	Attempted Sun RPC high port access
0.00	2	ICMP SRC and DST outside network

Five-Day Trend

Chart 1



Top 5 Alerts - Analysis

UDP SRC and DST outside network

These alerts are the result of a UDP packet whose source and destination IP address are not part of the clients network architecture. The cause of this type of activity could be the result of a miss-configured network device.

After parsing the alert files, it was determined that this alert was triggered 93,562 times over the five day period. Within these alerts it appears that there where 59 distinct source address and 602 distinct destination address.

Alert Signature	# Alerts	# Sources	# Destinations
UDP SRC and DST outside network	93562	59	602

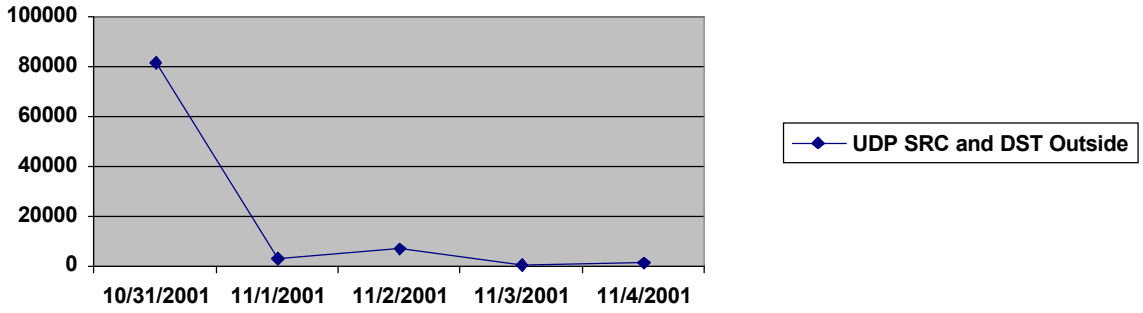
Top Ten "Source" Talkers

Source	# Alerts	# Dsts
159.134.237.178	34075	1
129.105.153.48	24699	1
63.250.213.100	6278	1
63.250.213.39	5623	1
3.0.0.99	5541	1

203.109.158.50	4998	3
192.168.1.106	4213	41
129.105.153.49	3860	1
134.192.73.204	2001	2

Five-Day Trend

Chart 2



Analysis

Reviewing the activity associated with the "Top Ten Source Talkers" revealed that the majority, if not all, the traffic is destined for "Multicast" address space. Looking at a sample of the alerts generated by 159.134.237.178, we see 233.21.90.1 was the destination address with source port 1639 and destination port 11000.

```
10/31-10:32:44.857690  [**] UDP SRC and DST outside network [**] 159.134.237.178:1639 -> 233.21.90.1:11000
10/31-10:32:45.157541  [**] UDP SRC and DST outside network [**] 159.134.237.178:1639 -> 233.21.90.1:11000
10/31-10:32:46.286013  [**] UDP SRC and DST outside network [**] 159.134.237.178:1639 -> 233.21.90.1:11000
```

According to RFC 2770, "GLOB Addressing in 233/8", 233.0.0.0/8 is an experimental multicast address space that is used in conjunction with an "Autonomous System Number", ASN. This experimental space is governed by IANA, the "Internet Assigned Numbers Authority".

Further analysis of the top ten list revels that the following source IPs where also involved in similar multicast activity:

129.105.153.48

```
10/31-14:42:29.289998  [**] UDP SRC and DST outside network [**] 129.105.153.48:1408 -> 233.0.103.30:4446
10/31-14:42:29.292402  [**] UDP SRC and DST outside network [**] 129.105.153.48:1408 -> 233.0.103.30:4446
10/31-14:42:29.386223  [**] UDP SRC and DST outside network [**] 129.105.153.48:1408 -> 233.0.103.30:4446
```

63.250.213.100

```
10/31-08:31:13.835876  [**] UDP SRC and DST outside network [**] 63.250.213.100:1038 -> 233.28.65.209:5779
10/31-08:31:14.035850  [**] UDP SRC and DST outside network [**] 63.250.213.100:1038 -> 233.28.65.209:5779
10/31-08:31:19.431304  [**] UDP SRC and DST outside network [**] 63.250.213.100:1038 -> 233.28.65.209:5779
```

63.250.213.39
```
10/31-08:57:26.433419  [**] UDP SRC and DST outside network [**] 63.250.213.39:1030 -> 233.40.70.50:5779
10/31-08:57:27.626312  [**] UDP SRC and DST outside network [**] 63.250.213.39:1030 -> 233.40.70.50:5779
10/31-08:57:32.382820  [**] UDP SRC and DST outside network [**] 63.250.213.39:1030 -> 233.40.70.50:5779
```

203.109.158.50
```
10/31-09:32:34.806088  [**] UDP SRC and DST outside network [**] 203.109.158.50:1885 -> 233.29.233.3:38950
10/31-09:32:35.148653  [**] UDP SRC and DST outside network [**] 203.109.158.50:1885 -> 233.29.233.3:38950
10/31-09:32:35.588411  [**] UDP SRC and DST outside network [**] 203.109.158.50:1885 -> 233.29.233.3:38950
```

129.105.153.49
```
10/31-15:09:51.588881  [**] UDP SRC and DST outside network [**] 129.105.153.49:1740 -> 233.0.103.31:4446
10/31-15:09:51.606481  [**] UDP SRC and DST outside network [**] 129.105.153.49:1740 -> 233.0.103.31:4446
10/31-15:09:51.622181  [**] UDP SRC and DST outside network [**] 129.105.153.49:1740 -> 233.0.103.31:4446
```

In total the multicast activity accounted for 85% (79,990 alerts) of all the alerts generated by this signature. Furthermore it appears that all the incidents occurred on 10/31/01, which would account for the spike seen in the "Five Day Trend" chart above.

The rest of the alerts not related to multicasting, appears to be MS Windows name service traffic. Looking at the alerts generated by source IPs 3.0.0.9, 192.168.1.106 and 134.192.73.204 we see source port 137 and destination ports of 137 and 53. Port 137 is register as the NETBIOS Name Service, which facilitates name resolution between MS Windows operating systems and the "Windows Internet Name Service", WINS. Activity from port 137 to port 53 would indicate a WINS server attempting to communicate with a "Domain Name Server", DNS. Detailed information on this process can be found on Microsoft's knowledge database. (Q173161)

3.0.0.9
```
10/31-00:04:48.780910  [**] UDP SRC and DST outside network [**] 3.0.0.99:137 -> 10.0.0.1:137
10/31-00:08:44.283591  [**] UDP SRC and DST outside network [**] 3.0.0.99:137 -> 10.0.0.1:137
10/31-00:12:42.861206  [**] UDP SRC and DST outside network [**] 3.0.0.99:137 -> 10.0.0.1:137
```

192.168.1.106
```
10/31-00:59:27.520443  [**] UDP SRC and DST outside network [**] 192.168.1.106:137 -> 24.3.0.36:53
10/31-02:59:27.010831  [**] UDP SRC and DST outside network [**] 192.168.1.106:137 -> 24.3.0.36:53
10/31-03:29:20.483437  [**] UDP SRC and DST outside network [**] 192.168.1.106:137 -> 24.3.0.36:53
```

134.192.73.204
```
11/02-16:41:45.042450  [**] UDP SRC and DST outside network [**] 134.192.73.204:137 -> 134.192.64.25:137
11/02-16:41:46.572038  [**] UDP SRC and DST outside network [**] 134.192.73.204:137 -> 134.192.64.25:137
11/02-16:41:51.054639  [**] UDP SRC and DST outside network [**] 134.192.73.204:137 -> 134.192.64.25:137
```

TCP SRC and DST outside network

As with the previous, this alert is also detecting packets with both source and destination outside the client's architecture. The difference is this alert is detects TCP traffic instead of UDP.

Initial analysis revealed that 23,565 alerts of this type where detected. Of the 23,565 alerts it appears that 99% of these involved unique source addresses.

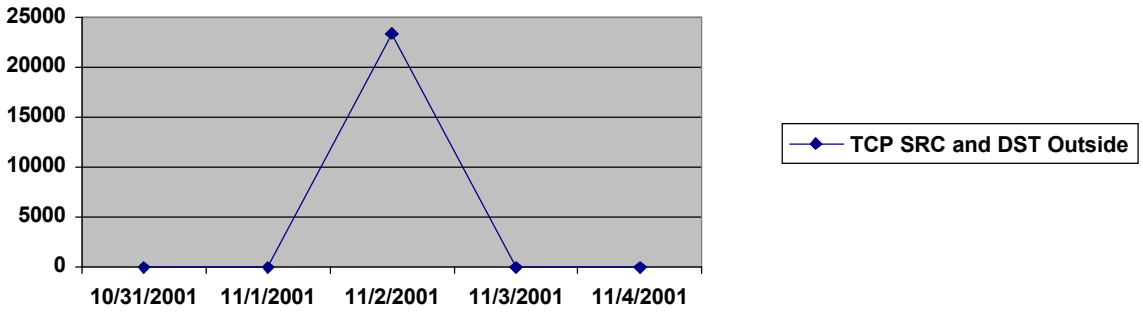
Alert Signature	# Alerts	# Sources	# Destinations
TCP SRC and DST outside network	23565	23435	107

Top Ten " Source" Talkers

Source	# Alerts	# Dsts
192.168.1.106	51	44
192.168.1.100	16	16
66.92.222.245	14	3
134.192.133.116	12	10
192.168.0.155	10	5
169.254.101.152	9	4
10.109.106.231	9	6
192.168.0.96	9	8
192.168.0.202	4	1
10.42.28.5	3	1

Five-Day Trend

Chart 3



Analysis

Seven out of the "Top Ten Source Talker" IP addresses belong to the address spaces reserved for internal network use only, as outlined in RFC 1918. This activity would indicate possible external spoofing for Denial of Service attempts or that these address are part of the internal network architecture. Reviewing the alerts generated by these addresses, paying specific attention to the destination ports, it appears that the activity can be classified as known client-server connections and possibly part of the internal network.

192.168.1.106
10/31-07:09:57.921507 [**] TCP SRC and DST outside network [**] 192.168.1.106:1357 -> 66.71.1.189:1214
10/31-17:38:46.391924 [**] TCP SRC and DST outside network [**] 192.168.1.106:1078 -> 213.47.84.150:1214
10/31-17:38:46.424804 [**] TCP SRC and DST outside network [**] 192.168.1.106:1070 -> 205.146.215.79:1214
10/31-17:38:47.449667 [**] TCP SRC and DST outside network [**] 192.168.1.106:1073 -> 24.5.141.80:1214

192.168.1.100
11/01-16:03:24.395889 [**] TCP SRC and DST outside network [**] 192.168.1.100:1075 -> 170.140.74.21:1214
11/01-16:03:30.126338 [**] TCP SRC and DST outside network [**] 192.168.1.100:1074 -> 147.4.225.88:1214
11/01-16:03:30.126435 [**] TCP SRC and DST outside network [**] 192.168.1.100:1072 -> 131.204.197.251:1214
11/01-16:03:33.857630 [**] TCP SRC and DST outside network [**] 192.168.1.100:1061 -> 134.155.57.71:1214

10.109.106.231
11/04-21:29:18.656675 [**] TCP SRC and DST outside network [**] 10.109.106.231:1073 -> 128.101.72.59:1214
11/04-21:29:21.873481 [**] TCP SRC and DST outside network [**] 10.109.106.231:1078 -> 132.239.228.120:1214
11/04-21:29:23.428468 [**] TCP SRC and DST outside network [**] 10.109.106.231:1079 -> 152.16.234.212:1214
11/04-21:29:25.334442 [**] TCP SRC and DST outside network [**] 10.109.106.231:1069 -> 128.253.27.189:1214

192.168.0.96
11/01-20:51:48.277173 [**] TCP SRC and DST outside network [**] 192.168.0.96:2024 -> 152.19.233.18:1214
11/01-20:51:48.356703 [**] TCP SRC and DST outside network [**] 192.168.0.96:2027 -> 170.140.78.89:1214
11/02-15:32:11.484227 [**] TCP SRC and DST outside network [**] 192.168.0.96:3733 -> 137.52.212.171:1214
11/02-15:32:12.058701 [**] TCP SRC and DST outside network [**] 192.168.0.96:3720 -> 64.78.94.242:1214

Port 1214 is a well-known port used for a peer-to-peer file sharing service called KaZaA (www.kazaa.com). Users can down load client software and share media files with anyone on the internet that also uses the service.

192.168.0.155
11/01-21:53:00.174383 [**] TCP SRC and DST outside network [**] 192.168.0.155:3658 -> 211.233.10.19:1755
11/01-21:53:09.878304 [**] TCP SRC and DST outside network [**] 192.168.0.155:3658 -> 211.233.10.19:1755
11/01-21:53:21.863894 [**] TCP SRC and DST outside network [**] 192.168.0.155:3650 -> 132.206.203.182:1214
11/01-21:53:29.068059 [**] TCP SRC and DST outside network [**] 192.168.0.155:3658 -> 211.233.10.19:1755

Port 1755 is a well-know port used for Microsoft NetShow. NetShow is used to deliver pre-recorded or live streaming video over the Internet or local network.

192.168.0.202
11/01-18:12:26.595352 [**] TCP SRC and DST outside network [**] 192.168.0.202:3070 -> 152.3.50.179:8888
11/01-18:14:10.108879 [**] TCP SRC and DST outside network [**] 192.168.0.202:3089 -> 152.3.50.179:8888
11/01-18:14:14.769519 [**] TCP SRC and DST outside network [**] 192.168.0.202:3092 -> 152.3.50.179:8888
11/01-18:14:14.783851 [**] TCP SRC and DST outside network [**] 192.168.0.202:3091 -> 152.3.50.179:8888

Port 8888 is a well-known port used for a news service, NewsEDGE.

10.42.28.5
11/02-16:34:58.796657 [**] TCP SRC and DST outside network [**] 10.42.28.5:1058 -> 152.128.178.4:139
11/02-16:35:01.711559 [**] TCP SRC and DST outside network [**] 10.42.28.5:1058 -> 152.128.178.4:139
11/02-16:35:07.859892 [**] TCP SRC and DST outside network [**] 10.42.28.5:1058 -> 152.128.178.4:139

Port 139 is a well-know port used for the NETBIOS Session Service. The NETBIOS Session Service is used by MS Windows operating system to create a session before data is transferred.

After reviewing the top ten talkers it was clear that the amount of activity seen did not

match up to the spike of activity visible on the Five Day Trend chart on 11/2. Further analysis was complied, specifically looking for at destination addresses on 11/2, and revealed that IP address 200.208.9.7 occurred in over 23,418 alerts (99% of alert activity).

Destination	# Alerts	# Dsts
200.208.9.7	23418	23418

Whois Lookup: 200.208.9.7

Comite Gestor da Internet no Brasil (NETBLK-BRAZIL-BLK2)
R. Pio XI, 1500
Sao Paulo, SP 05468-901
BR

Netname: BRAZIL-BLK2
Netblock: 200.128.0.0 - 200.255.255.255
Maintainer: BR

Coordinator:
Registro.br (NF-ORG-ARIN) blkadm@nic.br
+55 19 9119-0304

Looking into the actual alerts associated with 200.208.9.7 exposed some very odd behavior. The activity appears to be some sort of distributed port scan attempted.

```
11/02-14:26:41.769436  [**] TCP SRC and DST outside network [**] 59.253.108.60:60250 -> 200.208.9.77:2
11/02-14:26:41.769650  [**] TCP SRC and DST outside network [**] 213.215.249.77:29426 -> 200.208.9.77:3
11/02-14:26:41.769698  [**] TCP SRC and DST outside network [**] 111.178.134.95:64139 -> 200.208.9.77:4
11/02-14:26:41.771658  [**] TCP SRC and DST outside network [**] 61.66.45.20:37204 -> 200.208.9.77:7
11/02-14:26:41.771748  [**] TCP SRC and DST outside network [**] 113.247.70.55:41093 -> 200.208.9.77:9
11/02-14:26:41.772005  [**] TCP SRC and DST outside network [**] 115.60.7.15:18048 -> 200.208.9.77:14
.
.
.
.
11/02-14:26:43.413983  [**] TCP SRC and DST outside network [**] 225.242.122.78:8906 -> 200.208.9.77:3108
11/02-14:26:43.414234  [**] TCP SRC and DST outside network [**] 21.168.148.113:12795 -> 200.208.9.77:3110
11/02-14:26:43.416309  [**] TCP SRC and DST outside network [**] 227.55.59.38:51396 -> 200.208.9.77:3113
11/02-14:26:43.417176  [**] TCP SRC and DST outside network [**] 23.237.84.73:55285 -> 200.208.9.77:3115
11/02-14:26:43.425581  [**] TCP SRC and DST outside network [**] 27.119.213.120:9194 -> 200.208.9.77:3125
11/02-14:26:43.426727  [**] TCP SRC and DST outside network [**] 181.81.98.10:43907 -> 200.208.9.77:3126
.
.
.
.
11/02-14:27:00.610782  [**] TCP SRC and DST outside network [**] 30.62.211.127:34274 -> 200.208.9.77:32982
11/02-14:27:00.610877  [**] TCP SRC and DST outside network [**] 184.24.96.17:3451 -> 200.208.9.77:32983
11/02-14:27:00.610922  [**] TCP SRC and DST outside network [**] 236.205.121.52:7340 -> 200.208.9.77:32985
11/02-14:27:00.611022  [**] TCP SRC and DST outside network [**] 134.168.6.70:42052 -> 200.208.9.77:32986
11/02-14:27:00.611119  [**] TCP SRC and DST outside network [**] 32.131.147.87:11229 -> 200.208.9.77:32987
11/02-14:27:00.611164  [**] TCP SRC and DST outside network [**] 186.93.32.105:45941 -> 200.208.9.77:32988
```

Tiny Fragments - Possible Hostile Activity

Hackers will craft packets that are smaller then standard to bypass firewalls or boarder

filtering devices.

Analysis of this activity revealed that 21,103 alerts of this type where detected. The alerts where generated by only 3 unique source and destination IP addresses.

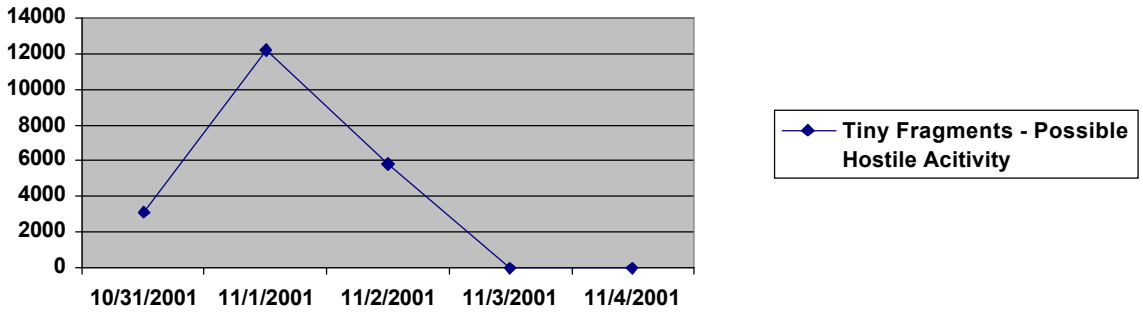
Alert Signature	# Alerts	# Sources	# Destinations
Tiny Fragments - Possible Hostile Activity	21103	3	3

Top Three "Source" Talkers

Source	# Alerts	# Dsts
0.0.8.1	21100	1
66.87.66.236	2	1
138.89.71.149	1	1

Five-Day Trend

Chart 4



Analysis

99.9 % of the alerts recorded where generated by the internal source address MY.NET.8.1 (0.0.8.1). All the activity with this source IP had the same internal destination address MY.NET.16.42 (0.0.16.42).

```
10/31-17:22:48.560888  [**] Tiny Fragments - Possible Hostile Activity [**] 0.0.8.1 -> 0.0.16.42
10/31-17:22:59.145347  [**] Tiny Fragments - Possible Hostile Activity [**] 0.0.8.1 -> 0.0.16.42
10/31-17:22:59.791366  [**] Tiny Fragments - Possible Hostile Activity [**] 0.0.8.1 -> 0.0.16.42
10/31-17:22:59.794318  [**] Tiny Fragments - Possible Hostile Activity [**] 0.0.8.1 -> 0.0.16.42
```

The activity on 11/01 increased 383% over the pervious days activity, which is visible on the "Five Day Trend" chart. A search on other alerts with these IP addresses provided no results. It is unclear with the data provided what could have caused this

activity, but a malfunctioning application or OS is possible.

Reviewing the other two IP address, 138.89.71.149 and 66.87.66.236, involved in these alerts revealed only 3 instances. Again a search was done for other alerts triggered with these IP addresses, but there were no results.

SMB Name Wildcard

This activity is an example of potential normal MS Windows traffic used by a hacker to gain information about a system.

Analysis of this activity revealed that 16525 alerts of this type where detected. The alerts where generated by 379 unique source and 6602 unique destination IP addresses.

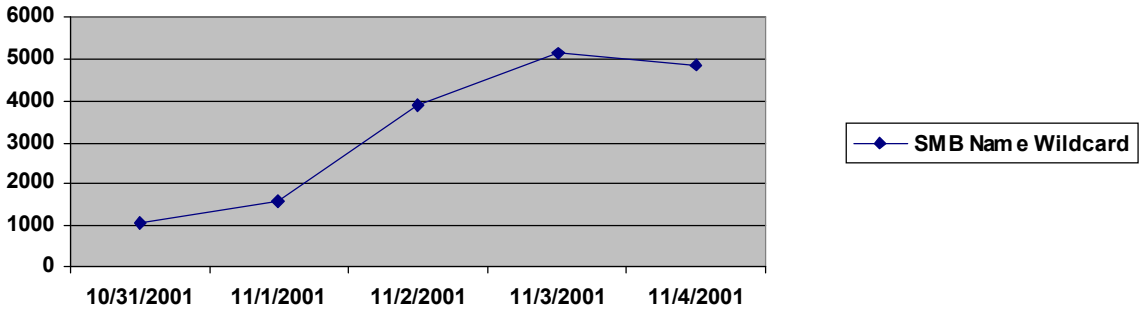
Signature	# Alerts	# Sources	# Destinations
SMB Name Wildcard	16525	379	6602

Top Ten "Source" Talkers

Source	# Alerts	# Dsts
216.150.152.145	5890	2
0.0.163.53	3626	2504
0.0.233.142	1081	772
0.0.239.78	963	681
0.0.205.138	879	596
0.0.205.114	850	585
0.0.218.130	552	386
0.0.226.234	360	141
0.0.140.120	336	269
0.0.99.217	279	157

Five-Day Trend

Chart 5



Analysis

Activity of this type has a high probability of beginning legitimate traffic, especially if both the source and destination addresses are internal. On the other hand, activity that is generated from external host should be considered a reconnaissance attempt.

Of the "Top Ten Source Talkers" there is only one external IP address, 216.150.152.145, which has apparently made over 5000 attempts on two internal hosts.

Whois Lookup: 216.150.152.145

```
SpyralNet, LLC (NETBLK-SPYRALNET-152)
99 Main St.
Nyack, NY 10960
US

Netname: SPYRALNET-152
Netblock: 216.150.152.0 - 216.150.159.255

Coordinator:
Beckwith, Ted  (TB346-ARIN)  ted@SPYRAL.NET
914-348-7676
```

```
10/31-00:01:07.286006  [**] SMB Name Wildcard [**] 216.150.152.145:137 -> 0.0.5.45:137
10/31-00:04:23.237209  [**] SMB Name Wildcard [**] 216.150.152.145:137 -> 0.0.5.45:137
10/31-00:14:29.971745  [**] SMB Name Wildcard [**] 216.150.152.145:137 -> 0.0.5.45:137
10/31-00:29:24.336271  [**] SMB Name Wildcard [**] 216.150.152.145:137 -> 0.0.5.44:137
10/31-00:30:39.700927  [**] SMB Name Wildcard [**] 216.150.152.145:137 -> 0.0.5.44:137
10/31-00:32:09.662937  [**] SMB Name Wildcard [**] 216.150.152.145:137 -> 0.0.5.45:137
10/31-00:44:13.874906  [**] SMB Name Wildcard [**] 216.150.152.145:137 -> 0.0.5.44:137
10/31-00:58:33.092501  [**] SMB Name Wildcard [**] 216.150.152.145:137 -> 0.0.5.45:137
10/31-01:04:30.565725  [**] SMB Name Wildcard [**] 216.150.152.145:137 -> 0.0.5.45:137
10/31-01:04:35.377751  [**] SMB Name Wildcard [**] 216.150.152.145:137 -> 0.0.5.44:137
```

Typically a reconnaissance attempt would only require a few SMB Name attempts two retrieve any data. This lends us to the possibility that the server at 216.150.152.145 is configured to communicate with the machines MY.NET.5.45 and MY.NET.5.44.. Further information would be required to analyze this event.

As mentioned before the rest of the "Top Ten Source Talkers" are all internal

machines. A search was run to verify that the destination addresses on all alerts where also internal machines. The results showed that all destination machines where also internal hosts, which would potentially rule out reconnaissance attempts. An audit should be completed on these machines to ascertain why they are creating all of these requests.

Possible Trojan Server Activity

The signature that generates this alert is looking for the default server port "27347" of the Trojan program "SubSeven".

Initial analysis showed that the alert was generated 3,403 times over the five-day period of alert files. There were 106 and 2,138 unique source and destination IP address involved.

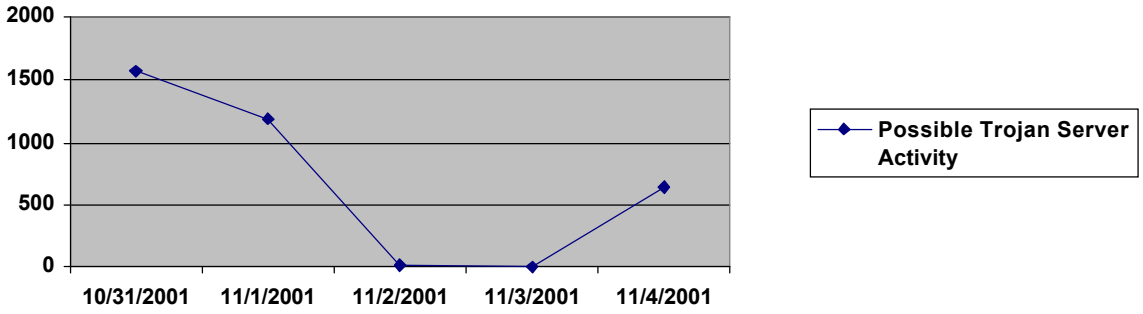
Signature	# Alerts	# Sources	# Destinations
Possible trojan server activity	3403	106	2138

Top Ten "Source" Talkers

Source	# Alerts	# Dsts
0.0.98.127	1429	1064
66.108.114.41	369	345
202.108.65.13	367	360
65.65.8.98	97	74
66.168.57.102	89	81
65.96.189.120	85	52
24.7.220.90	84	72
208.13.135.127	82	71
213.73.196.232	75	69
65.11.196.246	75	59
64.160.204.88	72	50

Five-Day Trend

Chart 6



Analysis

The first IP address on the "Top Ten Source Talkers" is an internal IP address. And after review all the alerts contain this IP address, 0.0.98.127 (MY.NET.98.127), it appears that this machines has accessed external machines via "SubSeven".

10/31-20:20:11.368263 [**] Possible trojan server activity [**] 128.187.89.43:27374 -> 0.0.98.127:2103
10/31-20:20:11.368369 [**] Possible trojan server activity [**] 128.187.89.49:27374 -> 0.0.98.127:2109
10/31-20:20:11.368415 [**] Possible trojan server activity [**] 128.187.89.51:27374 -> 0.0.98.127:2111
10/31-20:20:11.368572 [**] Possible trojan server activity [**] 128.187.89.50:27374 -> 0.0.98.127:2110
10/31-20:20:12.700651 [**] Possible trojan server activity [**] 0.0.98.127:2136 -> 128.187.89.77:27374
10/31-20:20:12.749194 [**] Possible trojan server activity [**] 0.0.98.127:2130 -> 128.187.89.71:27374
10/31-20:20:12.813759 [**] Possible trojan server activity [**] 128.187.89.71:27374 -> 0.0.98.127:2130
10/31-20:20:13.179847 [**] Possible trojan server activity [**] 0.0.98.127:2108 -> 128.187.89.48:27374
10/31-20:20:13.373666 [**] Possible trojan server activity [**] 0.0.98.127:2099 -> 128.187.89.39:27374
10/31-20:20:13.406000 [**] Possible trojan server activity [**] 0.0.98.127:2102 -> 128.187.89.42:27374
10/31-20:20:13.406045 [**] Possible trojan server activity [**] 0.0.98.127:2103 -> 128.187.89.43:27374
10/31-20:20:13.725697 [**] Possible trojan server activity [**] 0.0.98.127:2139 -> 128.187.89.80:27374
10/31-20:20:13.805003 [**] Possible trojan server activity [**] 0.0.98.127:2123 -> 128.187.89.64:27374
10/31-20:20:13.821796 [**] Possible trojan server activity [**] 0.0.98.127:2124 -> 128.187.89.65:27374
10/31-20:20:13.821842 [**] Possible trojan server activity [**] 0.0.98.127:2125 -> 128.187.89.66:27374
10/31-20:20:13.821933 [**] Possible trojan server activity [**] 0.0.98.127:2126 -> 128.187.89.67:27374
10/31-20:20:13.821979 [**] Possible trojan server activity [**] 0.0.98.127:2127 -> 128.187.89.68:27374
10/31-20:20:13.835255 [**] Possible trojan server activity [**] 0.0.98.127:2128 -> 128.187.89.69:27374
10/31-20:20:13.835476 [**] Possible trojan server activity [**] 0.0.98.127:2129 -> 128.187.89.70:27374
10/31-20:20:13.853312 [**] Possible trojan server activity [**] 0.0.98.127:2132 -> 128.187.89.73:27374
10/31-20:20:13.853354 [**] Possible trojan server activity [**] 0.0.98.127:2133 -> 128.187.89.74:27374
10/31-20:20:13.853406 [**] Possible trojan server activity [**] 0.0.98.127:2143 -> 128.187.89.84:27374
10/31-20:20:13.901255 [**] Possible trojan server activity [**] 0.0.98.127:2144 -> 128.187.89.85:27374
10/31-20:20:13.933863 [**] Possible trojan server activity [**] 0.0.98.127:2106 -> 128.187.89.46:27374
10/31-20:20:13.933909 [**] Possible trojan server activity [**] 0.0.98.127:2107 -> 128.187.89.47:27374
10/31-20:20:13.965211 [**] Possible trojan server activity [**] 0.0.98.127:2108 -> 128.187.89.48:27374
10/31-20:20:14.106435 [**] Possible trojan server activity [**] 128.187.89.50:27374 -> 0.0.98.127:2110
10/31-20:20:14.140733 [**] Possible trojan server activity [**] 0.0.98.127:2111 -> 128.187.89.51:27374
10/31-20:20:14.140777 [**] Possible trojan server activity [**] 0.0.98.127:2114 -> 128.187.89.54:27374
10/31-20:20:14.253040 [**] Possible trojan server activity [**] 0.0.98.127:2137 -> 128.187.89.78:27374
10/31-20:20:14.283524 [**] Possible trojan server activity [**] 128.187.89.40:27374 -> 0.0.98.127:2100
10/31-20:20:14.283575 [**] Possible trojan server activity [**] 128.187.89.39:27374 -> 0.0.98.127:2099
10/31-20:20:14.426494 [**] Possible trojan server activity [**] 128.187.89.71:27374 -> 0.0.98.127:2130
10/31-20:20:14.443036 [**] Possible trojan server activity [**] 128.187.89.75:27374 -> 0.0.98.127:2134
10/31-20:20:14.602446 [**] Possible trojan server activity [**] 128.187.89.84:27374 -> 0.0.98.127:2143
10/31-20:20:20.145265 [**] Possible trojan server activity [**] 0.0.98.127:2135 -> 128.187.89.76:27374
10/31-20:20:20.321811 [**] Possible trojan server activity [**] 0.0.98.127:2133 -> 128.187.89.74:27374
10/31-20:20:20.349240 [**] Possible trojan server activity [**] 0.0.98.127:2145 -> 128.187.89.86:27374

The port of interest with "SubSeven" is 27374. This is the default port that the Trojan will listen on waiting for a client connection. In the alerts above we see the internal host making a request to an external machine on destination port 27374, which is followed with what appears to be a response. The following is a whois lookup on the potentially compromised external IP address:

Whois Lookup: 128.187.89.40

Brigham Young University (NET-BYU-NET)
167 TMCB
Provo, UT 84602
US

Netname: BYU-NET
Netblock: 128.187.0.0 - 128.187.255.255

Coordinator:
Humphries, T Jay (TJH17-ARIN) tjay@BYU.EDU
(801) 378-7513 (FAX) (810) 378-7874

The rest of the "Top Ten Source Talkers" are external IP addresses so we are interested in internal machines that responded to an original request. A query was run to reveal all internal servers responding to the "Top Ten Source Talkers" with source port 27347. The following were the results:

```
11/01-15:49:30.608294  [**] Possible trojan server activity [**] 0.0.5.44:27374 -> 66.108.114.41:2554
11/01-16:23:29.368997  [**] Possible trojan server activity [**] 0.0.132.1:27374 -> 66.108.114.41:3002
11/01-16:23:44.842643  [**] Possible trojan server activity [**] 0.0.133.1:27374 -> 66.108.114.41:3256
11/01-16:24:01.042270  [**] Possible trojan server activity [**] 0.0.134.12:27374 -> 66.108.114.41:3521
11/01-16:24:01.050675  [**] Possible trojan server activity [**] 0.0.134.1:27374 -> 66.108.114.41:3510
11/01-16:24:01.052513  [**] Possible trojan server activity [**] 0.0.134.11:27374 -> 66.108.114.41:3520
11/01-16:24:01.144992  [**] Possible trojan server activity [**] 0.0.134.13:27374 -> 66.108.114.41:3522
11/01-16:24:01.585588  [**] Possible trojan server activity [**] 0.0.134.12:27374 -> 66.108.114.41:3521
11/01-16:24:01.640254  [**] Possible trojan server activity [**] 0.0.134.13:27374 -> 66.108.114.41:3522
11/01-16:24:02.057390  [**] Possible trojan server activity [**] 0.0.134.11:27374 -> 66.108.114.41:3520
11/01-16:24:16.503151  [**] Possible trojan server activity [**] 0.0.135.1:27374 -> 66.108.114.41:3764
11/01-16:24:16.520166  [**] Possible trojan server activity [**] 0.0.135.3:27374 -> 66.108.114.41:3766
11/01-16:24:17.051164  [**] Possible trojan server activity [**] 0.0.135.3:27374 -> 66.108.114.41:3766
11/01-16:24:17.438474  [**] Possible trojan server activity [**] 0.0.135.1:27374 -> 66.108.114.41:3764
11/01-16:24:17.945181  [**] Possible trojan server activity [**] 0.0.135.1:27374 -> 66.108.114.41:3764
11/01-16:24:18.040771  [**] Possible trojan server activity [**] 0.0.135.3:27374 -> 66.108.114.41:3766
11/01-16:24:18.048158  [**] Possible trojan server activity [**] 0.0.135.5:27374 -> 66.108.114.41:3768
11/01-16:24:48.603585  [**] Possible trojan server activity [**] 0.0.137.1:27374 -> 66.108.114.41:4272
11/01-16:24:49.122924  [**] Possible trojan server activity [**] 0.0.137.1:27374 -> 66.108.114.41:4272
11/01-16:38:59.727059  [**] Possible trojan server activity [**] 0.0.190.1:27374 -> 66.108.114.41:1847
11/01-16:38:59.814206  [**] Possible trojan server activity [**] 0.0.190.10:27374 -> 66.108.114.41:1856
11/01-16:38:59.838161  [**] Possible trojan server activity [**] 0.0.190.13:27374 -> 66.108.114.41:1859
11/01-16:38:59.846266  [**] Possible trojan server activity [**] 0.0.190.14:27374 -> 66.108.114.41:1860
11/01-16:38:59.859570  [**] Possible trojan server activity [**] 0.0.190.16:27374 -> 66.108.114.41:1862
11/01-16:39:00.820692  [**] Possible trojan server activity [**] 0.0.190.14:27374 -> 66.108.114.41:1860
11/01-16:39:01.314375  [**] Possible trojan server activity [**] 0.0.190.11:27374 -> 66.108.114.41:1857
11/01-14:42:50.240338  [**] Possible trojan server activity [**] 0.0.133.1:27374 -> 202.108.65.13:1662
11/01-14:42:55.152627  [**] Possible trojan server activity [**] 0.0.135.2:27374 -> 202.108.65.13:2173
11/01-14:42:55.154312  [**] Possible trojan server activity [**] 0.0.135.7:27374 -> 202.108.65.13:2178
11/01-14:44:25.227207  [**] Possible trojan server activity [**] 0.0.190.16:27374 -> 202.108.65.13:4281
11/01-14:44:25.228608  [**] Possible trojan server activity [**] 0.0.190.20:27374 -> 202.108.65.13:4285
```

```
11/01-14:44:25.253766  [**] Possible trojan server activity [**] 0.0.190.19:27374 -> 202.108.65.13:4284
11/01-10:12:48.169789  [**] Possible trojan server activity [**] 0.0.134.10:27374 -> 66.168.57.102:4649
11/01-10:12:48.176152  [**] Possible trojan server activity [**] 0.0.134.11:27374 -> 66.168.57.102:4650
11/01-10:12:48.181861  [**] Possible trojan server activity [**] 0.0.134.12:27374 -> 66.168.57.102:4651
11/01-10:12:49.163088  [**] Possible trojan server activity [**] 0.0.134.11:27374 -> 66.168.57.102:4650
11/04-23:48:25.128437  [**] Possible trojan server activity [**] 0.0.190.20:27374 -> 65.96.189.120:2377
11/01-10:12:03.345515  [**] Possible trojan server activity [**] 0.0.133.1:27374 -> 213.73.196.232:3144
11/01-10:13:57.520360  [**] Possible trojan server activity [**] 0.0.134.1:27374 -> 213.73.196.232:3423
11/01-10:13:57.567235  [**] Possible trojan server activity [**] 0.0.134.10:27374 -> 213.73.196.232:3432
11/01-10:13:58.157795  [**] Possible trojan server activity [**] 0.0.134.1:27374 -> 213.73.196.232:3423
11/01-10:13:58.258620  [**] Possible trojan server activity [**] 0.0.134.10:27374 -> 213.73.196.232:3432
11/04-23:48:13.478958  [**] Possible trojan server activity [**] 0.0.134.10:27374 -> 64.160.204.88:4595
11/04-23:48:13.488285  [**] Possible trojan server activity [**] 0.0.134.11:27374 -> 64.160.204.88:4596
```

Based on the pervious results a new query was run to reveal ALL internal servers responding to stimulus with source port of 27374. The query helped create the following list of potentially compromised internal servers:

List of Potentially Compromised Servers:

0.0.132.1
0.0.134.10
0.0.134.11
0.0.134.12
0.0.134.13
0.0.135.1
0.0.135.2
0.0.135.3
0.0.135.5
0.0.135.7
0.0.137.1
0.0.190.1
0.0.190.10
0.0.190.11
0.0.190.13
0.0.190.14
0.0.190.15
0.0.190.16
0.0.190.19
0.0.190.20
0.0.190.32
0.0.190.51
0.0.5.44

Note: "MY.NET" was replaced with "0.0" for analysis.

Portscan Activity

Portscan Summary

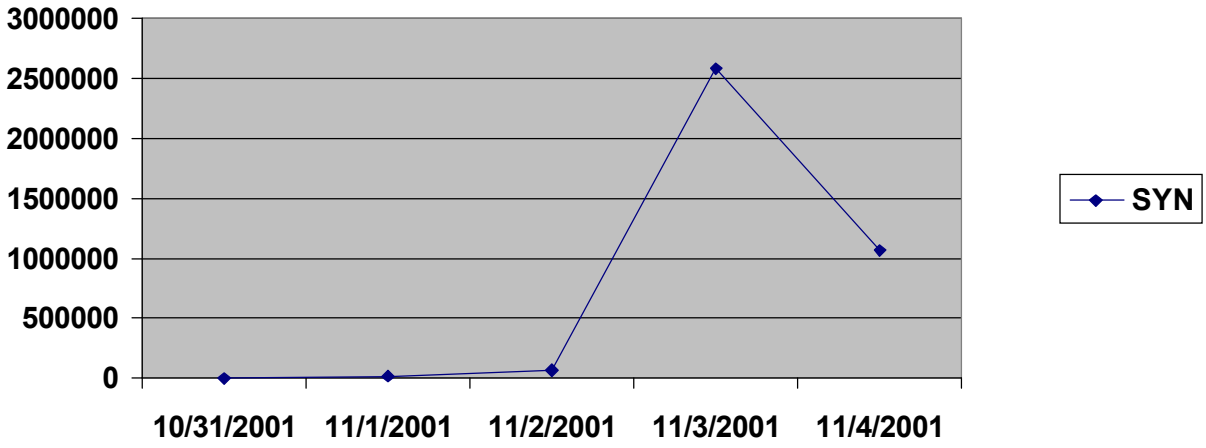
% of Scans	# of Scans	Type of Scan
65	3734456	SYN
35	2043750	UDP
< 1	387	VECNA
< 1	101	NULL
< 1	73	INVALIDACK
< 1	43	NOACK
< 1	31	UNKNOWN
< 1	9	FIN
< 1	5	XMAS
< 1	4	SPAU
	2	SYNFIN

SYN SCANS

% of Scans	# of Scans	Type of Scan
65	3734456	SYN

Five-Day Trend

Chart 8



Top Destination Ports

% of Scans	# of Scans	Destination Port
98	3,659,349	22

.008	28986	23
.005	17452	21

Analysis

Port 22

While reviewing the SYN scan activity it became clear very quickly that port 22 (SSH) was the most prevalent. In fact 98% of the SYN scan activity had a destination port of 22. After further investigation it became apparent that two source IP addresses account for the majority of this activity.

MY.NET.179.84 (0.0.179.84)

The internal IP address MY.NET.179.84 (0.0.179.84) performed 3 million scans over a period of 5 days. Reviewing the actual alerts revealed that this IP address began to scan entire address spaces beginning on Nov 2. Below is a listing of the various addresses spaces that where involved in the scan:

1. 213.0.0.0
2. 205.0.0.0
3. 11.0.0.0
4. 198.0.0.0

Looking at a portion of the scan log shows that the attack used a reflexive probing mechanism, which means both the source and destination port are the same. This is mechanism is used to exploit poorly configured boarder filtering devices. Also, it was quit evident that the hacker was not attempting to mask their activity.

```
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.1:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.5:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.6:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.7:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.9:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.11:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.13:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.15:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.16:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.17:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.19:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.20:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.21:22 SYN **S*****
Nov  2 15:15:51 0.0.179.84:22 -> 213.0.0.22:22 SYN **S*****
```

Whois Lookup: 213.0.0.1

```
inetnum:    213.0.0.0 - 213.0.3.255
netname:    RIMA
descr:      Telefonica De Espana SAU (NCC#1999085999 )
descr:      Red de servicios IP
descr:      Spain
country:    ES
```

admin-c: LJP3-RIPE
tech-c: FLT14-RIPE
status: ASSIGNED PA
notify: luisfernando.jimenezpalop@telefonica.es
mnt-by: MAINT-AS3352
changed: antoniopablo.fuentesgallego@telefonica.es 20011016
source: RIPE

12.26.124.12
Beginning on Nov 2 the IP addresses 12.26.124.12 began a reflexive scan to destination port 22, which appears to have covered all internal subnets. Below is a whois lookup on the address from www.arin.net:

Whois Lookup: 12.26.124.12

SUNLIT CORPORATION (NETBLK-ATT21344-124)
804 THORN STREET
PRINCETON, WV 24740
US

Netname: ATT21344-124
Netblock: 12.26.124.0 - 12.26.124.255

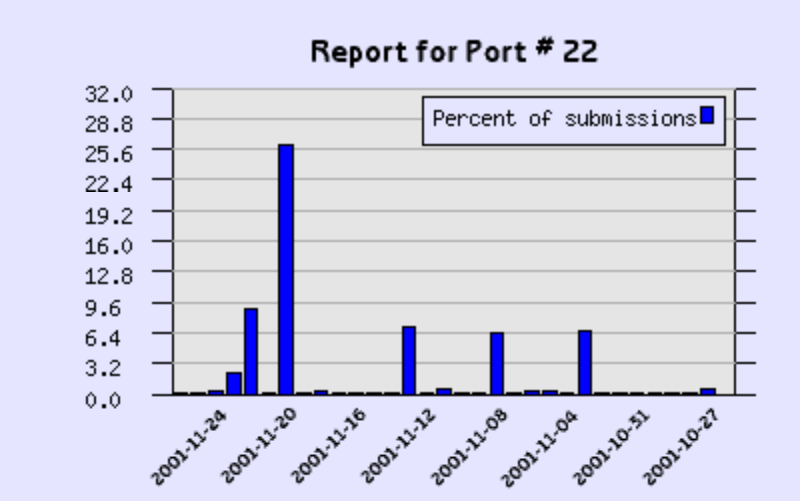
Coordinator:
Sword, Aaron (AS601-ARIN) tunester@i-plus.net
540-980-5155

The scan mechanism is the same as the previous reflexive scan that originated from the internal network. Below is a portion of the alert file:

```
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.79:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.87:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.91:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.98:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.99:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.94:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.95:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.96:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.97:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.100:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.102:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.101:22 SYN **S*****
Nov  2 08:57:54 12.26.124.12:22 -> MY.NET.1.103:22 SYN **S*****
```

Correlation

Below is data provided by www.dshields.com that shows an increase interest in port 22 (SSH) around 11/01/01.



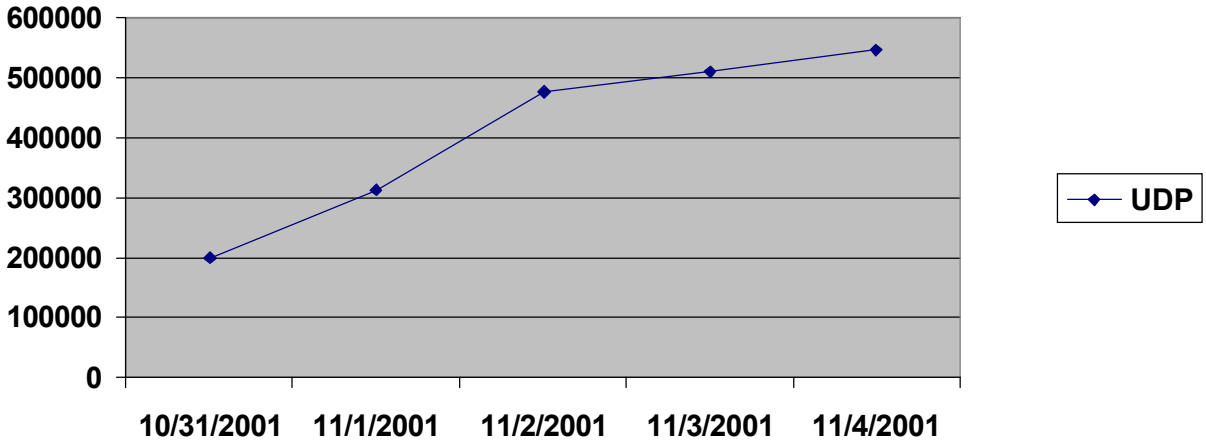
Date	Count	% of Submissions
2001-11-05	1107	0.09%
2001-11-04	2021	0.21%
2001-11-03	2148	0.36%
2001-11-02	1513	0.15%
2001-11-01	66609	6.49%
2001-10-31	259	0.03%

UDP SCANS

% of Scans	# of Scans	Type of Scan
35	2043750	UDP

Five-Day Trend

Chart 9



Top Destination Ports

% of Scans	# of Scans	Destination Ports
50	960,287	68
29	599,407	27005
10	202,417	6970

Analysis

Port 68

Port 67 is a well-known client port associated with the "Bootstrap Protocol Client", BOOTPC. BOOTP is a service, that among others things, this allows for a booting machines to configure IP address information without any user interaction. The 960,287 alerts generated all appear to be part of the normal BOOTP process. All the hosts involved are internal and the same two source hosts appear in each occurance. The follow in a portion of the alerts associated with destination port 68.

```
Nov  2 13:45:02 0.0.5.76:67 -> 0.0.206.210:68 UDP
Nov  2 13:45:02 0.0.5.76:67 -> 0.0.202.158:68 UDP
Nov  2 13:45:02 0.0.5.76:67 -> 0.0.205.194:68 UDP
Nov  2 13:45:02 0.0.5.76:67 -> 0.0.208.18:68 UDP
Nov  2 13:45:02 0.0.5.76:67 -> 0.0.201.166:68 UDP
Nov  2 13:45:02 0.0.5.76:67 -> 0.0.205.202:68 UDP
Nov  2 13:45:02 0.0.5.76:67 -> 0.0.204.134:68 UDP
Nov  2 13:45:03 0.0.5.76:67 -> 0.0.203.170:68 UDP
Nov  2 13:45:04 0.0.5.76:67 -> 0.0.206.174:68 UDP
Nov  2 13:45:06 0.0.5.76:67 -> 0.0.206.190:68 UDP
Nov  2 13:45:06 0.0.5.76:67 -> 0.0.208.122:68 UDP
Nov  2 13:45:06 0.0.5.76:67 -> 0.0.209.114:68 UDP
Nov  2 13:45:04 0.0.5.75:67 -> 0.0.229.50:68 UDP
Nov  2 13:45:04 0.0.5.75:67 -> 0.0.224.82:68 UDP
Nov  2 13:45:05 0.0.5.75:67 -> 0.0.228.6:68 UDP
Nov  2 13:45:06 0.0.5.75:67 -> 0.0.220.154:68 UDP
Nov  2 13:45:06 0.0.5.75:67 -> 0.0.240.154:68 UDP
```

```
Nov  2 13:45:06 0.0.5.75:67 -> 0.0.227.106:68 UDP
Nov  2 13:45:06 0.0.5.75:67 -> 0.0.224.26:68 UDP
Nov  2 13:45:06 0.0.5.75:67 -> 0.0.225.66:68 UDP
Nov  2 13:45:06 0.0.5.75:67 -> 0.0.223.202:68 UDP
```

Out Of Spec Activity

Destination Port 25

After analyzing the "Out of Spec" data, it appears that 68% of the alerts have a destination port of 25 (SMTP). Further digging reveled that the same two source IP addresses, 199.183.24.194 and 131.211.28.48 where involved in the majority of alerts.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/01-03:07:29.016795 199.183.24.194:49955 -> MY.NET.100.217:25
TCP TTL:52 TOS:0x0 ID:1422  DF
21S***** Seq: 0xDECC6FEB   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 710774454 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/01-03:14:24.966297 131.211.28.48:58035 -> MY.NET.53.61:25
TCP TTL:45 TOS:0x0 ID:23883  DF
21S***** Seq: 0xFF5658F4   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 23397823 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/01-03:17:17.646054 199.183.24.194:54361 -> MY.NET.6.35:25
TCP TTL:52 TOS:0x0 ID:25559  DF
21S***** Seq: 0x9F4174A   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 710833309 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/01-03:19:20.808469 199.183.24.194:55719 -> MY.NET.100.217:25
TCP TTL:52 TOS:0x0 ID:57200  DF
21S***** Seq: 0x11C97BC8   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 710845624 0 EOL EOL EOL EOL

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

The TCP settings in all the alerts have similar characteristics, including flags, windows size and TCP Options. This may indicate a malfunctioning SMTP server or network device corrupting traffic.

Source Port 18245

There appears to be 14 alert entries that match a known signature from malfunctioning router hardware. The hardware is believed to be a Nortel CVX router that removes the entire TCP header and recreates it based on the first four bits of the payload. More detailed information can be obtained from this posting http://archives.linuxbe.org/arch055/0229.html.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/01-03:43:53.598476 65.129.20.19:18245 -> MY.NET.253.114:21536
TCP TTL:120 TOS:0x0 ID:9984  DF
```

```
2*SF***U Seq: 0x2F686F6D   Ack: 0x6573756E   Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E  esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A                    1..Accept:
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/01-08:42:48.847646 63.159.13.18:18245 -> MY.NET.253.114:21536
TCP TTL:118 TOS:0x0 ID:10129  DF
2*SF***U Seq: 0x2F686F6D   Ack: 0x6573756E   Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E  esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A                    1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/01-08:54:07.712253 213.109.42.24:18245 -> MY.NET.253.125:21536
TCP TTL:111 TOS:0x0 ID:46344  DF
**SFRP*U Seq: 0x2F7E7265   Ack: 0x6C686167   Win: 0x6475
31 2F 64 75 61 61 6C 69 73 74 2E 68 74 6D 6C 20  1/duaalist.html
48 54 54 50 2F 31                                HTTP/1

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

Recommendations

Compromised Servers

As revealed in the "Possible Trojan Server Activity" selection, the following server need to be audited for possible compromise.

MY.NET.132.1
MY.NET.134.10
MY.NET.134.11
MY.NET.134.12
MY.NET.134.13
MY.NET.135.1
MY.NET.135.2
MY.NET.135.3
MY.NET.135.5
MY.NET.135.7
MY.NET.137.1
MY.NET.190.1
MY.NET.190.10
MY.NET.190.11
MY.NET.190.13
MY.NET.190.14
MY.NET.190.15
MY.NET.190.16
MY.NET.190.19
MY.NET.190.20
MY.NET.190.32

MY.NET.190.51
MY.NET.5.44

Snort Signatures

UDP SRC and DST outside network

To cut down on unwanted noise the Snort administrator my wish to customized this signature to exclude "Multicast" traffic.

TCP SRC and DST outside network

Verify with network (WAN) administrator exactly what RFC 1918 address schemes are used in your current environment.

Portscan Plugin

Verify the IP addresses of any BOOTP servers on your network and possible add them to the group of servers the Portscan Plugin will ignore. This will potentially reduce the number of false positives related to BOOTP activity.

Defense Recommendations

It is difficult to give recommendations without fully understanding your current network architecture and more importantly our security policies. But here are a few recommendations to consider:

1. Introduce a more restrictive boarder filtering mechanism. This can be accomplished with a firewall or filtering router.
2. Know and understand what protocols/services are allowed by our organization's operational policies (or security policies).
3. Implement regular system audits and maintain system status reports.

List of Files Analyzed

Alert Logs:

Alert.011031.gz
Alert.011101.gz
Alert.011102.gz
Alert.011103.gz
Alert.011104.gz

Portscan Logs:

Scans.011031.gz
Scans.011101.gz
Scans.011102.gz
Scans.011103.gz
Scans.011104.gz

Out of Spec Logs:

Oos_Oct.31.2001.gz
Oos_Nov.1.2001.gz
Oos_Nov.2.2001.gz
Oos_Nov.3.2001.gz
Oos_Nov.4.2001.gz

Analysis Process

Tools Used

1. Snort Stat
2. SnortSnarf
3. Various Unix Command Line Tools (cat, grep, sed)

Steps Completed

Alert Logs

1. Files where downloaded
2. All log files where combined into one file. (cat alerts* >> all_alerts)
3. Snort Stat and SnortSnarf are unable to parse "MY.NET" as an IP address, so sed was used to replace "MY.NET" with "0.0". (cat all_alerts | sed s/MY.NET/0.0/g > all_alerts_mod)
4. Snort Stat was run on the large alert file to reveal the alert summary. (cat all_alerts_mod | ./snort-stat.pl)
5. New alert files where created for each of the top five alerts. (cat all_alerts_mod | grep "Tiny Fragments" > all_Tiny_Fragement_alerts)
6. SnortSnarf was then run on the new alert files.

Portscan Logs

1. Files where downloaded.
2. All log files where combined into one file. (cat scans* >> all_scans)
3. SnortSnarf is unable to parse "MY.NET" as an IP address, so sed was used to replace "MY.NET" with "0.0". (cat all_scans | sed s/MY.NET/0.0/g > all_scans_mod)
4. New alert files where created for each of the possible scan mechanisms. (cat all_scans_mod | grep "INVALIDACK" > all_INVALIDACK_scans)
5. SnortSnarf was then run on the new alert files.

Out of Spec Logs

1. Files where downloaded.
2. All log files where combined into one file. (cat oos* >> all_oos)
3. The new file was parsed manually looking for redundancy.
4. Grep was used for counting occurances.

References

1. Network Intrusion Detection - An Analyst's Handbook 2nd Edition - Stephen Northcutt, Judy Novak
2. TCP/IP Illustrated Volume 1 - The Protocols - W. Richard Stevens
3. Track 3 - Intrusion Detection In-Depth Course Material - The SANS Institute - David Hoelzer, Stephen Northcutt, Judy Novak
4. Track 3 - Intrusion Detection In-Depth Course Material/Intrusion Detection Snort Style - The SANS Institute - Marty Roesch
5. Hacking Exposed 2nd Edition - Joel Scambray, Stuart McClure, George Kurtz
6. www.sans.org
7. www.securityfocus.com
8. www.google.com
9. www.rfc-index.com
10. www.whatis.com
11. www.netcraft.com
12. www.geekktools.com

Last Updated: July 28th, 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