Global Information Assurance Certification Paper

GIAC GCIA Practical

By: Patrick Ethier
Submitted to: SANS GIAC online training center
Version: GCIA practical exercise version 3.0
Date: January 23rd, 2002

Table of Contents

Assignment #1: Global Intrusion Detection Deployment

The need for Meta Intrusion Detection Systems

This paper treats the topic of Meta-Intrusion Detection Systems. This paper will firstly define Meta IDS and describe where MIDS fits into the global deployment of IDS and pursue in explaining the features that make MIDS a worthwhile investment. During the course of the explanation of these features, a brief discussion of the challenges faced with providing these features will be provided.

Definition

George Ho describes Meta IDS as *a technology that allows a single security console to accept from and communicate with all deployed devices that are from different vendors* [1]. Pete Loshin, from Information Security Magazine adds that it is *a system that can accept security alerts from all deployed security devices, massage the raw data, extract useful information and present that information in a manageable format* [3].

Taken in this context, Meta-IDS uses information provided by various security devices and analyzes, performs trend analysis, sorts, correlates and presents security information to the network administrator. Since the intrusion detection doesn't originate from network data it is called Meta IDS from the use of meta data used in its analysis. But Meta IDS is much more than a super console for intrusion detection.

Meta IDS is the solution for enterprise-wide security deployments. Many vendors such as ISS and NFR offer collection servers that are able to centralize the management and monitoring of their various sensors. Certain technologies, such as IceCAP from ISS/NetworkICE are able to monitor and manage both HIDS and NIDS solutions. The convergence of IDS solutions and the growing acceptance of Intrusion Detection Message Exchange Format [2] [4](IDMEF) will undermine the current definition of Meta IDS given above. Meta IDS will need to rely upon the other advantages that it offers to the enterprise-wide deployment in order to prove its worth.

Identifying the need

The need for meta IDS arises from the inability of current intrusion detection systems to gain awareness of the "network" due to lack of scope. This is because individual IDS systems access data flowing through a particular channel at a particular point on a network. If an attack is aimed at a portion of the network which the sensor doesn't cover or the attack is launched on a host beyond the control point offered by the IDS sensor then that sensor cannot relate to events detected by other IDS systems deployed on the network.

HIDS and NIDS rely on raw data affecting a host or flowing through a network to identify anomalies or look for attack signatures. The result is a constant flow of trigger messages based on some sort of pattern matching. The problem is that regular, harmless network activities can contain these patterns and the result is the production a lot of alerts of which a good percentage indicate normal traffic. Many network administrators will disable the detection of certain attacks in order to reduce the amount of information that needs to be processed. Automating the preliminary operations that a network security technician would do in analyzing data as well as providing the ability to take this interpreted data and remove known or explained occurrences is another identified need for enterprise-wide deployment of IDS.

A huge problem often encountered in the deployment of security monitoring in an enterprise is the topology of the network. Network security specialists do not always deal with ideal situations. Internal connections, business-to-business links, flat networks, segmented networks; heterogeneous networks already pose enough of a headache with IDS in terms of coverage, performance, and efficiency. Added to this is the need to deal with vulnerabilities, storage of sensitive information and the need to keep systems available for business operations. Providing the ability to process IDS events in terms of Vulnerability Assessments, Risk Assessments and Threat Assessment identifies one of the most interesting advantages that MIDS offers to large organizations.

Deployment

When deploying MIDS, it is important to take a few factors into consideration. First, MIDS must access IDS sensors that are deployed throughout a network. Secondly, MIDS must be accessible to multiple security operators from various locations in order for them to take advantage of the system's features. Thirdly, MIDS must be deployed in a secured environment. These conditions are usually found in the Network Operations Center (NOC) of a company. Properly deployed operations centers usually offer redundant, out of band connections with controlled access.

Considerations in deploying MIDS on an enterprise network should include scalability and flexibility. Scalability means that the capacity for the MIDS to process a set amount of ids events should be distributable across multiple engines without losing any of the advantages offered by the MIDS correlation engine. Flexibility means that the MIDS engine should be open to handling new types of events as well as accept information from new types of IDS engines after the initial deployment without removing any efficiency from the correlation engine.

Features

Features that should be found on these meta IDS systems must address the handling of events in a network context, correlation based on access policy, vulnerability assessment, threat assessment and risk assessment, a distributed architecture to spread the load of processing imposing amounts of data and to make the system redundant as well as a modular/programmable interface to allow for the expansion of the system to adopt future technologies.

Handling of events in a network context means that events generated throughout the network are analyzed and matched across technologies to enforce, or promote the importance of a series of events. In this case correlation can be presented in various forms.

Gauging the importance of an intrusion event is derived from a relationship between a few things. Meta IDS can automate this process. In reference [6], there is discussion of the classification of attacks in terms of danger and transferability. The proposition here is that more factors be used in assigning criticality with respect to an organization. MIDS must be able to compute these factors in near real-time.

Intrusion attempt must be compared to a vulnerability assessment. The MIDS contains a listing of hosts on the network and a listing of the last vulnerability assessment. If the host has been identified as being "patched" for this particular intrusion attempt then the alerted is demoted. If a doubt exists about the resistance of the host to that particular vulnerability then the intrusion attempt is promoted. Secondly, the intrusion attempt must be compared to a threat assessment. If the host is situated in a position where it is prone to being attacked and that measures have been taken to reduce the threat then the intrusion attempt is demoted. If the host is situated in an area that has not been deemed prone to attack and that the measures taken to protect are not as tight then the intrusion attempt is promoted. Thirdly, the intrusion attempt must be compared to a risk assessment. If either target or source host contains highly sensitive information or if the risk imposed by the possibility that the host has been compromised is high then the intrusion attempt is promoted. If the information on the host is insignificant and the access controls on the network make it so that this host being compromised is of little importance then the intrusion attempt is demote.

Another facet of correlation is scenario matching. Scenario matching consists of taking a series of events together and turning them into a single event. Hence, vulnerability scans on a mail server matched with a zone transfer from your DNS server and ARP floods of a port on your switch might indicate that somebody is trying to take over your mail system. Being able to explain the relationship between events might take an event that is otherwise perceived as being harmless and put it into context of a global attack. This type of correlation can be done by an expert system, which learns by taking scenarios first inputted by security engineers and learned over time or it can be done using data mining techniques adapted to intrusion detection.

Wenke Lee and Salvatore Stolfo [7] [5] have discussed at great lengths the implications of using data mining techniques for intrusion detection. Although their paper discusses the use of data mining approach on tcpdump data and on sendmail logs, it is possible to abstract their methods to be used on IDMEF messages.

Correlation faces many challenges. The most important is the lack of standardization for the relationship between a known vulnerability and a type of attack. Although the arachnids database, the CVE database and other commercial databases of the sort aim to label all known vulnerabilities, no two vendors use the same convention to report similar findings. Hence, a port scan, which is a very common and general occurrence, can be detected in a multitude of ways. Port scans detected by SNORT and port scans detected by BlackICE do not always mean the same thing. IDMEF [2] was conceived to exchange data between intrusion detection systems but does not provide a mechanism to say, "This is a SYN scan" in a universal language. In order to apply data mining on data sets produced from varied technologies MIDS must overcome this challenge.

The possibility of tracking events is another feature offered by MIDS. This leaks over to the realm of ticketing and CRM software but is also an important part of intrusion detection. Offering the capability of an operator to see if a similar event has happened in the past and how the situation was resolved is of immeasurable value to an organization in dealing with security related issues. This feature is also important to allow for coordination between geographically separated security experts working on a common case. Using the MIDS as a dispatch center, to fill forms and store data about events becomes a crucial aspect in the race to secure a network by synchronizing actions undertaken by personnel. Lastly, the ability to gauge the efficiency of the technologies deployed and to offer statistics indicating how many events were detected and how many were explained/resolved means that a clear picture can be painted for the need to "beef up" security in certain areas and the justify budget for the maintenance of security levels in others.

MIDS offers the ability to act upon events. Taking into account that correlation and incident tracking can provide a certain window of warning, the MIDS engine can provide the option to gracefully shut down a server and minimize the loss of information. Understandably, care must be taken to avoid new types of denial of service attacks using these automated mechanisms. Certain IDS environments, such as SNORT using the flexresp module, already offer this feature. These IDS can deal with certain low-level decision making in order to automate responses but their lack of scope means that they are not well suited in making decisions involving many factors. MIDS has this scope and can therefore push the envelope of streamlined decision making to a higher level.

MIDS is able to manage multiple security devices from a common platform. This facilitates the application of policies throughout the network. Certain technologies, such as OPSEC and SNMP already offer the possibility to remotely reconfigure devices. Hence, MIDS should be conceived to convert between different vendor formats and allow operators to tune individual sensors from one platform. There is some debate on whether this approach should be taken using a deployed software agent [] on each host or a modular network agent that can convert between a universal language and the agents already deployed/integrated with each host.

The main feature of MIDS should be the ability to provide a global state of security. This means that reports should be generated to include common targets, common intruders, comparisons between events being detected by one type of technology but not another, etc. This state of security will allow security experts to make sound decisions as they have solid metrics on which to base their decisions on. MIDS, linked with industry best practices, has the ability to make the networking world a better and safer place.

In conclusion, MIDS is a relatively new technology which, like the network management consoles in the early 90's will allow for the ability to overcome the problems of deploying a large amount of IDS on a network and reducing the amount of effort and resources that need to be dedicated to them. This will let organizations to pursue their business and not worry about integration of security technologies onto their networks.

References:[1]

1 - http://rr.sans.org/intrusion/tomorrow.php
2 - http://www.ietf.org/ids.by.wg/idwg.html
3 - http://www.infowar.com/iwftp/icn/05Jul2001_standardized_IDS_reporting_format.shtml
4 - http://www.infosecuritymag.com/articles/august01/cover.shtml
5 - http://www.securityfocus.com/data/library/ieee_sp99_lee.ps
6 - http://www.cs.nps.navy.mil/people/faculty/rowe/barruspap.html
7 - http://www.cs.columbia.edu/~sal/hpapers/USENIX/usenix.html

[1] Nota: Pointers to references have been included in square [ ] brackets in this document. Citations have been italicized and their source pointed to by square [ ] brackets as well.

Assignment #2: Network Detects

Detect #1

```
[**] [1:1325:1] EXPLOIT ssh CRC32 overflow filler [**]
[Classification: Executable code was detected] [Priority: 1]
12/25-13:19:38.942722 24.202.58.131:49177 -> 123.456.789.123:22
TCP TTL:47 TOS:0x0 ID:2870 IpLen:20 DgmLen:684 DF
***AP*** Seq: 0x79473EA8  Ack: 0xF811BF2E  Win: 0x8218  TcpLen: 32
TCP Options (3) => NOP NOP TS: 64931 103687685
[Xref => http://www.securityfocus.com/bid/2347]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-
0144]
```

```
12/25-13:19:38.942722 24.202.58.131:49177 -> 123.456.789.123:22
TCP TTL:47 TOS:0x0 ID:2870 IpLen:20 DgmLen:684 DF
***AP*** Seq: 0x79473EA8  Ack: 0xF811BF2E  Win: 0x8218  TcpLen: 32
TCP Options (3) => NOP NOP TS: 64931 103687685
00 00 02 74 0B 14 B8 8B C7 58 F1 42 CF 8E 3F 10  ...t.....X.B..?.
FE 21 E3 EE 66 D0 00 00 00 3D 64 69 66 66 69 65  .!..f....=diffie
2D 68 65 6C 6C 6D 61 6E 2D 67 72 6F 75 70 2D 65  -hellman-group-e
78 63 68 61 6E 67 65 2D 73 68 61 31 2C 64 69 66  xchange-sha1,dif
66 69 65 2D 68 65 6C 6C 6D 61 6E 2D 67 72 6F 75  fie-hellman-grou
70 31 2D 73 68 61 31 00 00 00 0F 73 73 68 2D 72  p1-sha1....ssh-r
73 61 2C 73 73 68 2D 64 73 73 00 00 00 96 61 65  sa,ssh-dss....ae
73 31 32 38 2D 63 62 63 2C 33 64 65 73 2D 63 62  s128-cbc,3des-cb
63 2C 62 6C 6F 77 66 69 73 68 2D 63 62 63 2C 63  c,blowfish-cbc,c
61 73 74 31 32 38 2D 63 62 63 2C 61 72 63 66 6F  ast128-cbc,arcfo
75 72 2C 61 65 73 31 39 32 2D 63 62 63 2C 61 65  ur,aes192-cbc,ae
73 32 35 36 2D 63 62 63 2C 72 69 6A 6E 64 61 65  s256-cbc,rijndae
6C 31 32 38 2D 63 62 63 2C 72 69 6A 6E 64 61 65  l128-cbc,rijndae
6C 31 39 32 2D 63 62 63 2C 72 69 6A 6E 64 61 65  l192-cbc,rijndae
6C 32 35 36 2D 63 62 63 2C 72 69 6A 6E 64 61 65  l256-cbc,rijndae
6C 2D 63 62 63 40 6C 79 73 61 74 6F 72 2E 6C 69  l-cbc@lysator.li
75 2E 73 65 00 00 00 96 61 65 73 31 32 38 2D 63  u.se....aes128-c
62 63 2C 33 64 65 73 2D 63 62 63 2C 62 6C 6F 77  bc,3des-cbc,blow
66 69 73 68 2D 63 62 63 2C 63 61 73 74 31 32 38  fish-cbc,cast128
2D 63 62 63 2C 61 72 63 66 6F 75 72 2C 61 65 73  -cbc,arcfour,aes
31 39 32 2D 63 62 63 2C 61 65 73 32 35 36 2D 63  192-cbc,aes256-c
62 63 2C 72 69 6A 6E 64 61 65 6C 31 32 38 2D 63  bc,rijndael128-c
62 63 2C 72 69 6A 6E 64 61 65 6C 31 39 32 2D 63  bc,rijndael192-c
62 63 2C 72 69 6A 6E 64 61 65 6C 32 35 36 2D 63  bc,rijndael256-c
62 63 2C 72 69 6A 6E 64 61 65 6C 2D 63 62 63 40  bc,rijndael-cbc@
6C 79 73 61 74 6F 72 2E 6C 69 75 2E 73 65 00 00  lysator.liu.se..
00 55 68 6D 61 63 2D 6D 64 35 2C 68 6D 61 63 2D  .Uhmac-md5,hmac-
73 68 61 31 2C 68 6D 61 63 2D 72 69 70 65 6D 64  sha1,hmac-ripemd
31 36 30 2C 68 6D 61 63 2D 72 69 70 65 6D 64 31  160,hmac-ripemd1
36 30 40 6F 70 65 6E 73 73 68 2E 63 6F 6D 2C 68  60@openssh.com,h
6D 61 63 2D 73 68 61 31 2D 39 36 2C 68 6D 61 63  mac-sha1-96,hmac
2D 6D 64 35 2D 39 36 00 00 00 55 68 6D 61 63 2D  -md5-96...Uhmac-
6D 64 35 2C 68 6D 61 63 2D 73 68 61 31 2C 68 6D  md5,hmac-sha1,hm
61 63 2D 72 69 70 65 6D 64 31 36 30 2C 68 6D 61  ac-ripemd160,hma
63 2D 72 69 70 65 6D 64 31 36 30 40 6F 70 65 6E  c-ripemd160@open
73 73 68 2E 63 6F 6D 2C 68 6D 61 63 2D 73 68 61  ssh.com,hmac-sha
31 2D 39 36 2C 68 6D 61 63 2D 6D 64 35 2D 39 36  1-96,hmac-md5-96
00 00 00 04 6E 6F 6E 65 00 00 00 04 6E 6F 6E 65  ....none....none
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00                          ........
```

1. Source of Trace.

This trace comes from a web server I operate.

2. Detect was generated by:

Snort intrusion detection system Version 1.8.3 running on Redhat Linux 7.1

The rule that triggered this detect is:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22
(msg:"EXPLOIT ssh CRC32 overflow filler";
flags:A+;
content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|";
reference:bugtraq,2347;
reference:cve,CVE-2001-0144;
classtype:shellcode-detect; sid:1325; rev:2;)
```

The packet contains a set ACK flag as well as 18 consecutive NULL bytes.

3. Probability the source address was spoofed:

This exploit requires a TCP connection to port 22 and the attacker expects to be granted a TCP session on the host. Hence, the probability that this address is spoofed is not very likely. As well, the alert/packet contains both the ACK and the PUSH flag which indicates that the handshake has already taken place.

The TTL of the packet also points towards a non-crafted packet. The number of 47 seems to be a reasonable value for a packet having traveled through a few routers.

4. Description of attack:

This attack is one of the many permutations of the SSH1 CRC-32 compensation attack detector vulnerability. It affects system not running patched SSH daemons or clients of version 1.5 of the protocol. This attack was detected because of the NULL padding.

5. Attack mechanism:

The attack usually starts with a simple port scan to port 22 of a machine.

The attack takes advantage of a buffer overflow introduced in the SSH protocol code that is supposed to provide protection against an attack on the CRC-32 aspect of the protocol. The result of this buffer overflow is that a call to a system function (malloc()) causes the OS kernel to start executing code at an arbitrary location in the program's memory space. This means that by submitting the value for a series of machine instructions a hacker can trick the program to jump in it's execution to these instructions and start, for example, the telnet daemon, to change the root password or install some malicious toolkits. A detailed description of the actual buffer overflow involved can be found at http://www.securityfocus.com/advisories/3088.

6. Correlations:

As mentioned above, this detect has already been recognized by CVE and bugtraq and seems to be a pretty harmless attack.

In this case, there was no reconnaissance (Port probes to 22 or anything else like that) from any IP address in the previous month.

In looking at the Syslog (secure) entries on the host I get the following message:

```
Dec 25 13:19:46 HOST sshd[13683]: Accepted password for ****** from
24.202.58.131 port 49177 ssh2

Incidents.org reports no other activity from this IP address.
```

7. Evidence of active targeting:

This attack hit my web server for a few times with a seemingly familiar IP addresses. I checked my Syslog entries for authentications from those IP addresses. I found that one of my users was consistently associated with those IP addresses.

The reason why this looked like an attack is because the user was using an SSH client for Mac OS X that fills the key negotiation packet with NULL bytes.

The attacker was obviously trying to gain access to my web server. The version of SSH that is operating on my system is not vulnerable to this attack

8. Severity:

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)
(4+ 4) - (4 + 1) = 3

Criticality: Machine is a web server hosting web sites for a bunch of my friends

Lethality: This is an active attack trying to gain access to my machine.

System Countermeasures: The version of SSH installed is recent and the bugfix documents specify that this particular problem is no longer and issue

Network Countermeasures: This machine is behind a firewall but this specific port is not protected

9. Defensive recommendation:

At the firewall level, the SSH port should be restricted to specific ranges of IP addresses. Since version 2 of the SSH protocol is mainly being used, version 1 should be disabled.

10. Multiple choice test questions:

Which of the following states accurately who is affected by the SSH1 CRC-32 compensation attack detector vulnerability?

a) SSH1 daemons supporting unpatched versions of SSH1 v1.5
b) SSH2 daemons accepting sessions using unpatched versions of SSH1 v1.5
c) All daemons and clients using unpatched versions of SSH1 v1.5
d) SSH1 clients using unpatched versions of SSH1 v1.5

The correct answer is C.

Detect #2

```
[**] [1:499:1] MISC Large ICMP Packet [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
01/18-20:23:56.394234 65.28.18.16 -> 123.456.789.123
ICMP TTL: 236 TOS:0x0 ID:49829 IpLen:20 DgmLen:1500 DF
Type:8  Code:0  ID:48282   Seq:61662  ECHO
[Xref => http://www.whitehats.com/info/IDS246]
```

```
01/18-20:23:56.394234 65.28.18.16 -> 123.456.789.123
ICMP TTL:236 TOS:0x0 ID:49829 IpLen:20 DgmLen:1500 DF
Type:8  Code:0  ID:48282   Seq:61662  ECHO
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

1. Source of Trace.

This trace comes from a web server I operate.

2. Detect was generated by:

Snort intrusion detection system Version 1.8.1 running on Redhat Linux 7.1

The rule that triggered this detect is

```
Alert icmp $EXTERNAL_NET any -> $HOME_NET any(msg:"MISC Large ICMP
Packet";Dsize: > 800;Reference: arachnids,246;Classtype:bad-unknown;
sid:499;rev:1;)
```

This rule looks for any icmp packet that is of size greater than 800 bytes.

3. Probability the source address was spoofed:

This is a stateless ICMP packet. Hence, no return packet is expected. This means there is a probability that this address is spoofed.

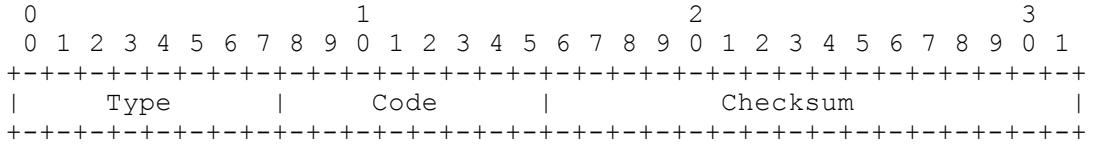
4. Description of attack:

An ICMP packet is generated as an Echo Request ICMP message with the data portion of the packet is filled with a large number of NULL bytes.

5. Attack mechanism:

ICMP messages are used to find out information about the network. The fields in the protocol change to create different control messages depending on the information that needs to be determined.

ICMP packets have the following fields in common, SNORT has decoded these as being Type = 0x8 (Echo) and Code = 0x0 (Request). The remaining NULL bytes are the DATA portion of the packet and are usually not part of a regular ping packet.



In this case, an ICMP Echo Request is sent using 1376 bytes set to NULL and a TTL set to high value and received at a value of 236. A trace indicates that there are 19 hops between my web server and the host.

The probe might have been to see how the networking stack of the host reacts to large packets or the flooding of the host in a DoS attack. The only case where this is seen as regular traffic is when this method is used to determine the maximum size of the packet that can sent without requiring fragmentation. Notice in the Snort packet data that the Don't Fragment bit is set, which means that the routers will not fragment the bits for you along the way. The high TTL is consistent with a packet meant for some type of network discovery.

6. Correlations:

Searching for this type of attack on Google yielded interesting information. The explanation consisted of saying that AIX 4.3 uses this mechanism for MTU path discovery. [2]

No reports from this IP address have been submitted through web searches on Google or Dshield.

7. Evidence of active targeting:

Since there is a policy instated where the web server is hosted that no active scanning or OS fingerprinting is allowed then there is no way to identify if this is originating from an AIX box or not. The other possibility is that this is part of a vulnerability scan looking for shaky network stacks or a DoS attack.

The fact that this occurred only once from this IP address in a short time lead to believe that this is most likely an attempt to do MTU path discovery.

[2] http://lists.jammed.com/incidents/2001/07/0267.html
http://project.honeynet.org/scans/arch/scan4.txt

8. Severity:

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

```
(4+ 3) - (5 + 2) = 0
```

Criticality: Machine is a web server hosting web sites for a bunch of my friends

Lethality: This is an active attack trying to gain access to my machine.

System Countermeasures: No known flaws in the Linux 2.2.12 kernel indicates problems with large ICMP packets (5)

Network Countermeasures: This machine is behind a firewall but ICMP packets are let through. Snort is also running as IDS for signature traces (2)

9. Defensive recommendation:

This alert should be disabled from SNORT or at least a threshold should be set in order to suspect this as a DoS attack.

10. Multiple choice test questions:

Which of these ICMP messages can contain a DATA field?

a) ICMP Source Quench
b) ICMP Echo Request
c) ICMP Port Unreachable
d) ICMP Redirect

The answer is B. All other requests contain data but that data is specifically defined as being of a certain type. Echo requests contain a field where information can be inserted called DATA by the RFC.

Detect #3

```
[**] [1:525:4] BAD TRAFFIC udp port 0 traffic [**]
[Classification: Misc activity] [Priority: 3]
01/17-14:28:07.055581 65.94.222.141:1234 ->
123.456.789.123:0
UDP TTL:48 TOS:0x0 ID:17185 IpLen:20 DgmLen:28
Len: 8
```


```
01/17-14:28:07.055581 65.94.222.141:1234 ->
123.456.789.123:0
UDP TTL:48 TOS:0x0 ID:17185 IpLen:20 DgmLen:28
Len: 8
```


1. Source of Trace.

This trace comes from a web server I operate.

2. Detect was generated by:

Snort intrusion detection system Version 1.8.1 running on Redhat Linux 7.1

The rule that triggered this detect is

```
Alert udp $EXTERNAL_NET any <> $HOME_NET 0 (msg:"BAD TRAFFIC udp port 0
traffic"; sid:525; classtype:misc-activity; rev:4;)
```

This alert reports any connection attempt to UDP port 0.

3. Probability the source address was spoofed:

UDP doesn't require a handshake process and there is obviously no application level protocol going on here since there is no payload data. This means that the source address could be spoofed and is highly likely.

4. Description of attack:

A UDP packet is sent from an arbitrary source port to UDP port 0 as a reconnaissance attack. The idea is that certain firewalls don't filter out port 0 connections (On some older Checkpoint and Pix versions).

This UDP port 0 connection was detected on my web server from this particular IP address 3

times. Since I have no access to other machines on this subnet I was not able to confirm that this was an actual subnet scan attempt.

5. Attack mechanism:

The concept here is simple. Some older firewall suites had a bug in them that disregarded UDP port 0 as it is a reserved port and is not supposed to occur in a network deployment. Thus, the port was bypassed.

Another concept involves scanning a host on a port that is guaranteed not to have a service listening and then looking for a return ICMP unreachable packet or something of the sort. If the destination host does not return this then it can be deduced that a DROP UDP packet rule is being used between the scanning host and the firewall. This is a way to identify that a host exists behind a firewall when conventional pings do not work.

Many network scanning tools, notably Nmap and Hping2 use this technique.

6. Correlations:

None from the other hosts on the same LAN segment. This IP address isn't reported as having been used in any suspicious activity from the DShield utility from incidents.org.

7. Evidence of active targeting:

A single attempt was made from the IP address mentioned. This seems to be a technique used by network scanners to detect active hosts for further targeting. My snort logs do not contain any other types of access from this IP address. This may be a misconfigured piece of network equipment or a type of stealth scan from a spoofed. This would mean that any of the other scans or alerts directed at my firewall may be coming from the same attacker. There is no way to know.

Reverse lookup says this is a high speed connection using ppp (Probably DSL modem of sorts)

MTL-HSE-ppp200347.qc.sympatico.ca [65.94.222.141]

8. Severity:

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

```
(4 + 2) - (4 + 3) = -1
```

Criticality: Machine is a web server hosting web sites for a bunch of my friends (4)

Lethality: This is a seemingly a probe of no importance. No other types of connections originate from this address.(2)

System Countermeasures: My IP chains firewall blocks this port although I am not sure if I am able to tell it to send back the proper ICMP port unreachable response. Snort is also running on this host. (4)

Network Countermeasures: This host is behind a firewall but this packet should have never made it to the target host.(3)

9. Defensive recommendation:

The firewall gateway serving connections to my web server should block any port 0 communications and return the proper expected packet so that this is no longer an issue for the hosts it protects.

10. Multiple choice test questions:

Which of the following is NOT an explanation for this large ICMP Echo Request?

a) This packet is part of a Denial of Service Attack
b) This packet is part of a MTU discovery
c) This packet is a PING packet
d) This packet is part of a ICMP port scan

The correct answer is D, there is no such thing as ports in ICMP. As explained above, the other three are possibilities.described in this detect.

Detect #4

```
[**] WEB-MISC telnet attempt [**]
01/14-13:49:19.515719 194.117.133.118:48209 -> 12.33.247.6:80
TCP TTL:47 TOS:0x0 ID:58830 IpLen:20 DgmLen:723 DF
***AP*** Seq: 0xF07EB26B  Ack: 0x3D4416C3  Win: 0x2238  TcpLen: 32
TCP Options (3) => NOP NOP TS: 533930 397771996
47 45 54 20 2F 69 6D 61 67 65 73 2F 53 43 4F 52  GET /images/SCOR
45 6C 6F 67 6F 53 4D 2E 67 69 66 20 48 54 54 50  ElogoSM.gif HTTP
2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 77 77 77 2E  /1.1..Host: www.
73 61 6E 73 2E 6F 72 67 0D 0A 43 6F 6E 6E 65 63  sans.org..Connec
74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 76 65  tion: keep-alive
0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 74 65  ..User-Agent: te
6C 6E 65 74 2E 65 78 65 20 28 6F 70 74 69 6D 69  lnet.exe (optimi
7A 65 64 20 66 6F 72 20 77 77 77 2E 73 61 6E 73  zed for www.sans
2E 6F 72 67 29 0D 0A 41 63 63 65 70 74 3A 20 74  .org)..Accept: t
65 78 74 2F 78 6D 6C 2C 20 61 70 70 6C 69 63 61  ext/xml, applica
74 69 6F 6E 2F 78 6D 6C 2C 20 61 70 70 6C 69 63  tion/xml, applic
61 74 69 6F 6E 2F 78 68 74 6D 6C 2B 78 6D 6C 2C  ation/xhtml+xml,
20 74 65 78 74 2F 68 74 6D 6C 3B 71 3D 30 2E 39   text/html;q=0.9
2C 20 69 6D 61 67 65 2F 70 6E 67 2C 20 69 6D 61  , image/png, ima
67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 65 2F 67  ge/jpeg, image/g
69 66 3B 71 3D 30 2E 32 2C 20 74 65 78 74 2F 70  if;q=0.2, text/p
6C 61 69 6E 3B 71 3D 30 2E 38 2C 20 74 65 78 74  lain;q=0.8, text
2F 63 73 73 2C 20 2A 2F 2A 3B 71 3D 30 2E 31 0D  /css, */*;q=0.1.
0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65  .Accept-Language
3A 20 65 6E 2D 75 73 0D 0A 41 63 63 65 70 74 2D  : en-us..Accept-
45 6E 63 6F 64 69 6E 67 3A 20 64 65 66 6C 61 74  Encoding: deflat
65 2C 20 67 7A 69 70 0D 0A 41 63 63 65 70 74 2D  e, gzip..Accept-
43 68 61 72 73 65 74 3A 20 49 53 4F 2D 38 38 35  Charset: ISO-885
39 2D 31 2C 20 75 74 66 2D 38 3B 71 3D 30 2E 36  9-1, utf-8;q=0.6
36 2C 20 2A 3B 71 3D 30 2E 36 36 0D 0A 52 65 66  6, *;q=0.66..Ref
65 72 65 72 3A 20 68 74 74 70 3A 2F 2F 77 77 77  erer: http://www
2E 73 61 6E 73 2E 6F 72 67 2F 69 6D 61 67 65 73  .sans.org/images
2F 53 43 4F 52 45 6C 6F 67 6F 53 4D 2E 67 69 66  /SCORElogoSM.gif
0D 0A 43 6C 69 65 6E 74 2D 49 50 3A 20 30 2E 30  ..Client-IP: 0.0
2E 30 2E 30 0D 0A 43 6F 6F 6B 69 65 32 3A 20 4D  .0.0..Cookie2: M
4F 56 45 5F 5A 49 47 5F 46 4F 52 5F 47 52 45 41  OVE_ZIG_FOR_GREA
54 5F 4A 55 53 54 49 43 45 0D 0A 43 6F 6F 6B 69  T_JUSTICE..Cooki
65 3A 20 41 4C 4C 5F 59 4F 55 52 5F 42 41 53 45  e: ALL_YOUR_BASE
5F 41 52 45 5F 42 45 4C 4F 4E 47 5F 54 4F 5F 55  _ARE_BELONG_TO_U
53 0D 0A 46 6F 72 77 61 72 64 65 64 3A 20 77 77  S..Forwarded: ww
77 2E 73 61 6E 73 2E 6F 72 67 0D 0A 56 69 61 3A  w.sans.org..Via:
20 31 2E 31 20 63 61 63 68 65 2D 68 61 72 20 28   1.1 cache-har (
4E 65 74 43 61 63 68 65 20 4E 65 74 41 70 70 2F  NetCache NetApp/
35 2E 31 52 32 44 37 44 45 42 55 47 32 29 0D 0A  5.1R2D7DEBUG2)..
58 2D 46 6F 72 77 61 72 64 65 64 2D 46 6F 72 3A  X-Forwarded-For:
20 77 77 77 2E 73 61 6E 73 2E 6F 72 67 2C 20 36   www.sans.org, 6
32 2E 33 30 2E 31 35 31 2E 35 30 0D 0A 0D 0A     2.30.151.50....
```

1. Source of Trace.

This trace comes from Intrusion.org's mailing list.[3]

2. Detect was generated by:

It seems that this is a SNORT generated alert. See source of trace for more info

The SNORT rule is

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERRVERS 80 (msg:"WEB-MISC telnet
attempt";flags: A+; content:"telnet.exe"; nocase; classtype:web-application-
activity; sid:1066; rev:2;)
```

3. Probability the source address was spoofed:

This is an HTTP request so there is a 3-way handshake. The above packet is has PUSH/ACK set in the TCP header meaning the handshake has happened.

4. Description of attack:

The thing that caught the administrator's eye was the User Agent being described as telnet.exe. There are other things that are strange with this.

5. Attack mechanism:

Get – The HTTP method to invoke
/images/SCORElogoSM.gif – File requested
HTTP/1.1 – http protocol version
Host: www.sans.org - hostname of the web server
Connection: KeepAlive – TCP session directive

Accept: text/xml, application/xml, application/xhtml+xml,text/html;q=0.9, image/png, image/jpeg, image/gif;q=0.2, text/plain;q=0.8, text/css, */*;q=0.1
Accept-Language: en-us
Accept-Encoding: deflate, gzip
Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66..
Referer: http://www.sans.org/images/SCORElogoSM.gif
------- Character sets, MIME types and decompression directives ------

[3] http://www.incidents.org/archives/intrusions/msg03304.html

Client-IP: 0.0.0.0
Cookie2: MOVE_ZIG_FOR_GREAT_JUSTICE – value of cookie
Cookie: ALL_YOUR_BASE_ARE_BELONG_TO_US – value of cookie
Forwarded: www.sans.org - Forwarded to this host
Via:1.1
cache-har (NetCache NetApp/5.1R2D7DEBUG2) – Forwarding Agent description
X-Forwarded-For:www.sans.org, 62.30.151.50 – participants in the forward

This was an HTTP request for a simple GIF file. The MIME declarations are fairly standard, nothing funny about the language or character sets.

There are a few things here that point that this anomaly originates from a caching/proxy server.

Hint #1: Forwarded and Via directives
The Forwarded directives say that the HTTP 1.1 forwarding feature was used on host cache-har (Using NetCache NetApp)

Hint #2: X-Forwarded-For directive

This shows that this session has an intermediary between www.sans.org and 62.30.151.50

Hint #3: Cookies

They seem to contain famous phrases from a "famous" video game.

Hint #4: 0.0.0.0 client IP address

This should be either the Caching server or the requesting client. Otherwise, this is a regular request for a GIF file.

The cookies probably point to hardcoded test values that are being used in this Beta version of NetCache. Programmers often set insignificant values to inside jokes.

A possible explanation for the User Agent: telnet.exe is that the NetCache utility probably uses the telnet.exe binary under Windows as an interface instead of connecting directly through the sockets API. Instead of reporting NetCache as the User-Agent it sends telnet.exe.

Another possible explanation is that NetCache forwards the User Agent information from the original request. If the person requesting this information simply wanted the HTML, then the caching server would have requested all the graphics anyhow as it processes the GET request completely before forwarding the information back to the original connection. The problem with this is that in this case this alert would be produced a bunch of times, once for each graphic included in the HTML and one for the parent document. The other problem is that telnet, as a

client, doesn't produce the User Agent directive unless the person using it has done so manually.

The last explanation is the same as for the cookies. This is a hard coded value in a DEBUG version of a Beta product.

The client IP being declared as 0.0.0.0 may be a bug, or simply not implemented and set to a default value.

6. Correlations:

The original poster reports seeing this from a few different IP addresses in the last few days but posts no details.

7. Evidence of active targeting:

According to the original post, this has happened a few times in the last day from a few other source IP addresses.

In this case, the packet's IP resolves to cache-har.cableinet.co.uk, which is consistent with what is in the GET request

The redirected source's IP resolves to pc-62-30-151-50-hr.blueyonder.co.uk

```
Checking the whois (From whois.nic.uk) of both hosts gives us their
respective owners which not surprisingly is the same

   Domain Name: BLUEYONDER.CO.UK
   Registered For: Telewest Communications PLC
   Domain Registered By: TELEWEST
   Registered on 19-Oct-1999.
   Record last updated on 26-Jul-2001 by .
   Domain servers listed in order:
   NS.BLUEYONDER.CO.UK               195.188.53.114
   NS2.BLUEYONDER.CO.UK              195.188.53.113
   WHOIS database last updated at 20:29:00 23-Jan-2002


   Domain Name: CABLEINET.CO.UK
   Registered For: Cable Internet Ltd.
   Domain Registered By: TELEWEST
   Record last updated on 14-Dec-2001 by .
   Domain servers listed in order:
   NS.CABLEINET.CO.UK                193.38.113.3
   NS2.CABLEINET.NET                 194.117.157.4
   NS3.CABLEINET.NET                 194.117.152.85
   WHOIS database last updated at 20:29:00 23-Jan-2002

It is safe to assume this proxied request was legitimate but that the HTTP
```

GET request may come from a “buggy” or unfinished NetCache product.

8. Severity:

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

No known context information about these hosts.

9. Defensive recommendation:

Contact TeleWest in the UK and ask them if they can reproduce this GET request and confirm that it does come from a NetCache proxy/caching server.

10. Multiple choice test questions:

What is the meaning of the X-Forwarded-For setting in the above packet?

a) That this session is part of a forwarded request for 62.30.151.50 to www.sans.org by an intermediary host
b) That this session is an X-Window session between 62.30.151.50 and www.sans.org
c) That this packet should be forwarded to both of these hosts
d) That the contents of this server shouldn't be cached

The answer is A.

Detect #5

```
[**] [1:237:1] DDOS Trin00:MastertoDaemon(defaultpassdetected!)
[**]
[Classification: Attempted Denial of Service] [Priority: 2]
01/17-14:23:09.109386 24.201.21.239:1024 -> 123.456.789.123:27444
UDP TTL:239 TOS:0x0 ID:9 IpLen:20 DgmLen:39
Len: 19
[Xref => http://www.whitehats.com/info/IDS197]
```

```
01/17-14:23:09.109386 24.201.21.239:1024 -> 123.456.789.123:27444
UDP TTL:239 TOS:0x0 ID:9 IpLen:20 DgmLen:39
Len: 19
70 6E 67 20 6C 34 34 61 64 73 6C                png l44adsl
```

1. Source of Trace.

This trace comes from a web server I operate.

2. Detect was generated by:

Snort intrusion detection system Version 1.8.1 running on Redhat Linux 7.1

The rule that triggered this detect is

```
alert udp $EXTERNAL_NET any -> $HOME_NET 27444 (msg:"DDOS
Trin00\:MastertoDaemon(defaultpassdetected!)"; content:"l44adsl";
references:arachnids,197; classtype:attempted-dos; sid:237; rev:1;)
```

This detect looks for the phrase l44adsl in a udp packet being sent to port 27444

3. Probability the source address was spoofed:

UDP packets do not need confirmation of receipt or "session" at the protocol level. Given that this attack looks like a password and command can be sent in the same packet it would make sense that the packet is spoofed. This means that unless Trinoo demands an application level "session" this packet could and most likely is spoofed.

4. Description of attack:

A full description of the Trinoo tool can be found on the web at http://staff.washington.edu/dittrich/misc/trinoo. In this case, a command is being sent to a Trinoo master server and was detected because the default password for the tool is being used.

5. Attack mechanism:

The targeted host is firstly compromised by some other mechanism. As a result, a Trinoo master or client program is installed.

The distributed aspect of trinoo means that the master can emit orders to its slaves and launch all types of DdoS attacks or transfer log files or do anything else.

A common occurrence is the crawling through internet hosts looking for installed trinoo in order to make them part of the distributed network. Trinoo uses as a default the string "l44adsl" as a password. Hence, if somebody has installed the Trojan with default values anybody with this default password could use it to start a DdoS attack.

6. Correlations:

No other Trinoo activity is reported from coming from this host in my SNORT files or in any

search engine.

7. Evidence of active targeting:

Again, the inability to correlate this finding with other hosts on the network is frustrating. No other scans have been detected by SNORT from this host.

I checked the IP at Dshield.org and no complaints have been logged.

8. Severity:

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

```
(4 + 4) - (4 + 3) = 1
```

Criticality: Machine is a web server hosting web sites for a bunch of my friends(4)

Lethality: This is most likely looking for a Trojan and not an indication that my host is infected (4)

System Countermeasures: IP Chains blocks incoming connections on this port (4)

Network Countermeasures: SNORT is installed on the web server and the host is behind a firewall(3)

9. Defensive recommendation:

Block this port off at the firewall gateway, execute "netstat –an" to make sure that 24777 is not listening. Install file integrity check such as tripwire to protect against Trojan installation or the installation of "r00t kits".

10. Multiple choice test questions:

What could be an administrator's first reaction when detecting a Trinoo connection with a default password?

a) run "netstat –a" on the host and verify any unexplained listening ports
b) install anti-virus or file integrity program on the host to verify for the existence of trinoo
c) Probe the source of the scan for evidence of a trinoo master
d) Remove the rule from the IDS detect list

The answer is A, because B would not be a primary step as the host would need to be taken off-

line in order to assure that the operation succeeds without leaving any doubts, C requires some sort of equally obtrusive means to figure out something on a possibly "innocent" host. D is a policy based decision and not a reactive step.

Assignement #3: Analyze this

Executive Summary

This exercises uses the SNORT logs gathered between January 3rd, 2002 and January 7th, 2002 at a University. In order to keep the anonymity, 127.127 replaced the first 16 bits of the IP address. This number was chosen because it should never occur in a network intrusion detection environment.

The logs were originally grouped into 14 files. 5 of them contained SNORT alert logs, 5 contained SNORT portscan entries and the other 4 contained logs from packets that were out of spec. Each of these logs were concatenated into 3 files as follows:

```
"cat alerts* >>alerts"
"cat scans* >> scans"
"cat oos* >> oos"
```

These files were then turned into comma-separated values (csv) using Perl scripts that I wrote for the occasion. These scripts can be found at http://www.darkelves.com/~drbones. These comma-delimited value were then imported into Microsoft Access in order to execute a series of queries. Most queries where simply charged with sorting the data by various fields and isolating other data. To count entries, the query wizard was used to count duplicates of certain values. Since this is not a lesson on SQL, little reference will be made to the actual query. Where the meaning of data is ambiguous, an explanation of the logic for the SQL query will be made.

The following graphics were made using MS Excel and pasted into this document as a picture.

There is much discussion in this document about target perspective and source perspective. **Target perspective** means that alerts were sorted by target, then by source, then by date and time, and then by message. This gives the groupings of alerts in chronological order from a specific source to a specific destination. **Source perspective** means that alerts were sorted by source, then by target, then by date and time and then by message. This gives a grouping of alerts originating from a specific source to a series of targets.

The first section of this document deals with the statistical aspect of Intrusion Detection. One important thing to keep in mind is that this data is skewed by the occurrence of false positives. These will be investigated further in the analysis portion of this document. Care was taken to provide an indication of where the attacks are originating as well.

The overall state of this network shows that it is in pretty good health besides a few minor worm infections. Care needs to be taken to identify if students are allowed to use Chat and File Sharing programs. This can be detected via the network IDS but should really be enforced at a desktop level. The only other recommendation is to fine-tune the IDS to remove any identified/explained alerts to reduce the size of logs.

Top 10 Targets[1]

Destination	# of attempts
127.127.5.1	25575
127.127.150.198	18025
127.127.152.109	4697
211.115.213.202	2720
127.127.153.154	2324
127.127.88.167	1898
127.127.88.165	1536
211.32.117.26	1260
224.0.0.2	1066
127.127.153.210	970

Top 10 Target Ports

dstport Field	NumberOfDups
515	18029
80	14035
161	9004
3320	1389
1356	1098

Top 10 Sources

Source	# of attempts
127.127.5.202	25575
127.127.153.114	5448
127.127.153.146	4744
127.127.88.181	3186
127.127.153.119	1919
203.248.242.22	1899
127.127.151.79	1821
127.127.150.198	1732
127.127.153.106	1681
127.127.150.41	1645

Top 10 Talkers

Source	Destination	# of sessions
127.127.5.202	127.127.5.1	25575
127.127.153.146	127.127.150.198	4580
127.127.153.114	127.127.150.198	2998
203.248.242.22	127.127.88.167	1898
127.127.88.181	127.127.150.198	1885
127.127.150.41	127.127.152.109	1645
127.127.153.106	127.127.150.198	1640
127.127.153.119	127.127.150.198	1626
127.127.153.114	211.115.213.202	1600
127.127.153.220	127.127.152.109	1590

Alerts List

Alert Type	# of occurrences
ICMP traceroute	25582
spp_portscan: PORTSCAN DETECTED	18939
Connect to 515 from inside	18026
spp_http_decode: IIS Unicode attack detected	12592
SNMP public access	9004
MISC Large UDP Packet	8660
INFO - ICQ Access	1731
INFO MSN IM Chat data	1314
ICMP Router Selection	1066
SMB Name Wildcard	719
High port 65535 udp - possible Red Worm - traffic	603
ICMP Echo Request L3retriever Ping	394
Watchlist 000220 IL-ISDNNET-990517	256
ICMP Destination Unreachable (Communication Administratively Prohibited)	211
ICMP Fragment Reassembly Time Exceeded	171
WEB-MISC Attempt to execute cmd	117
spp_http_decode: CGI Null Byte attack detected	96
WEB-CGI scriptalias access	96
Null scan!	60
SCAN Proxy attempt	55
ICMP Echo Request Nmap or HPING2	35

TCP SRC and DST outside network	28
ICMP Destination Unreachable (Protocol Unreachable)	28
ICMP Echo Request Windows	27
FTP DoS ftpd globbing	26
Possible Trojan server activity	20
INFO FTP anonymous FTP	20
Incomplete Packet Fragments Discarded	17
High port 65535 tcp - possible Red Worm - traffic	13
FTP passwd attempt	12
ICMP Echo Request Cisco Type.x	10
WEB-IIS _vti_inf access	10
INFO Inbound GNUTella Connect accept	9
EXPLOIT x86 setuid 0	9
INFO - Possible Squid Scan	9
WEB-FRONTPAGE _vti_rpc access	9
WEB-MISC 403 Forbidden	9
WEB-IIS view source via translate header	7
SCAN FIN	6
EXPLOIT x86 setgid 0	5
INFO Inbound GNUTella Connect request	5
SCAN Synscan Portscan ID 19104	4
Back Orifice	4
WEB-CGI formmail access	4
EXPLOIT NTPDX buffer overflow	4
IDS552/web-iis_IIS ISAPI Overflow ida nosize	4
Tiny Fragments - Possible Hostile Activity	4
Watchlist 000222 NET-NCFC	4
ICMP Echo Request CyberKit 2.2 Windows	3
NMAP TCP ping!	3
Port 55850 udp - Possible myserver activity - ref. 010313-1	3
INFO Napster Client Data	3
EXPLOIT x86 stealth noop	3
EXPLOIT x86 NOOP	2
SCAN XMAS	2
MISC traceroute	2
WEB-MISC compaq nsight directory traversal	2
Attempted Sun RPC high port access	2
SUNRPC highport access!	2

Note: Most of these will be explained in the following section.

Top 10 scanners

source Field	NumberOfDups
127.127.60.43	275031
127.127.6.50	24976
127.127.6.49	21088
127.127.6.45	13160
127.127.6.52	12931
127.127.150.143	12871
127.127.150.209	12172
127.127.6.51	8100
127.127.6.48	7215
127.127.150.165	6837

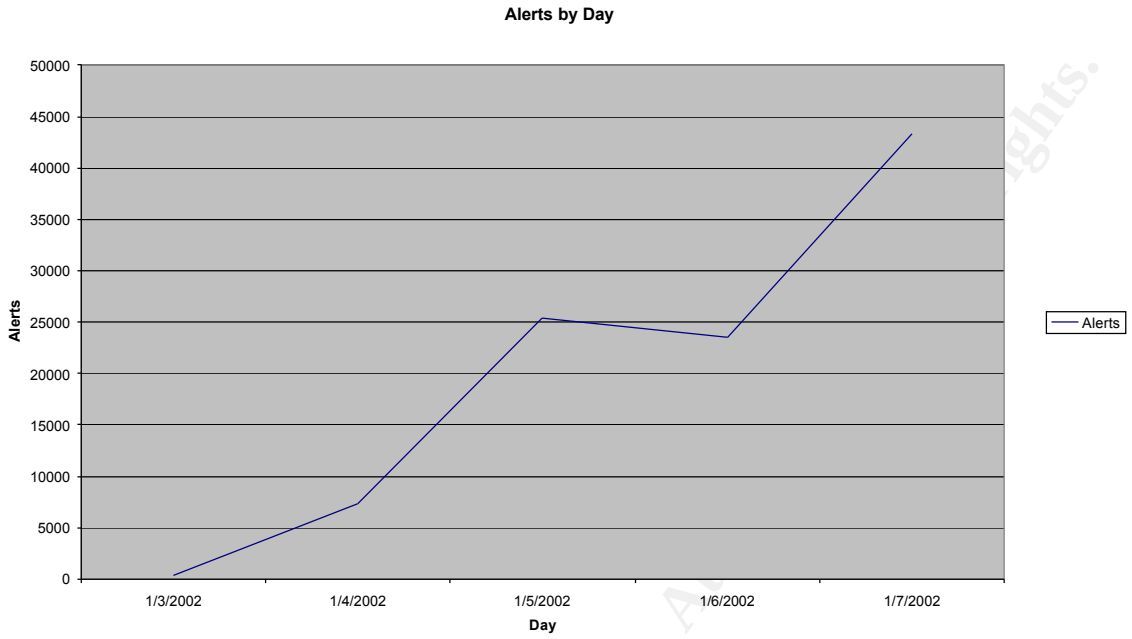
Out Of Spec Talkers

Source	Destination	# of OOS packets
144.122.42.38	127.127.88.162	14
195.132.240.41	127.127.88.162	10
130.104.19.73	127.127.88.162	8
4.61.46.216	127.127.150.143	6

Top Scan Types

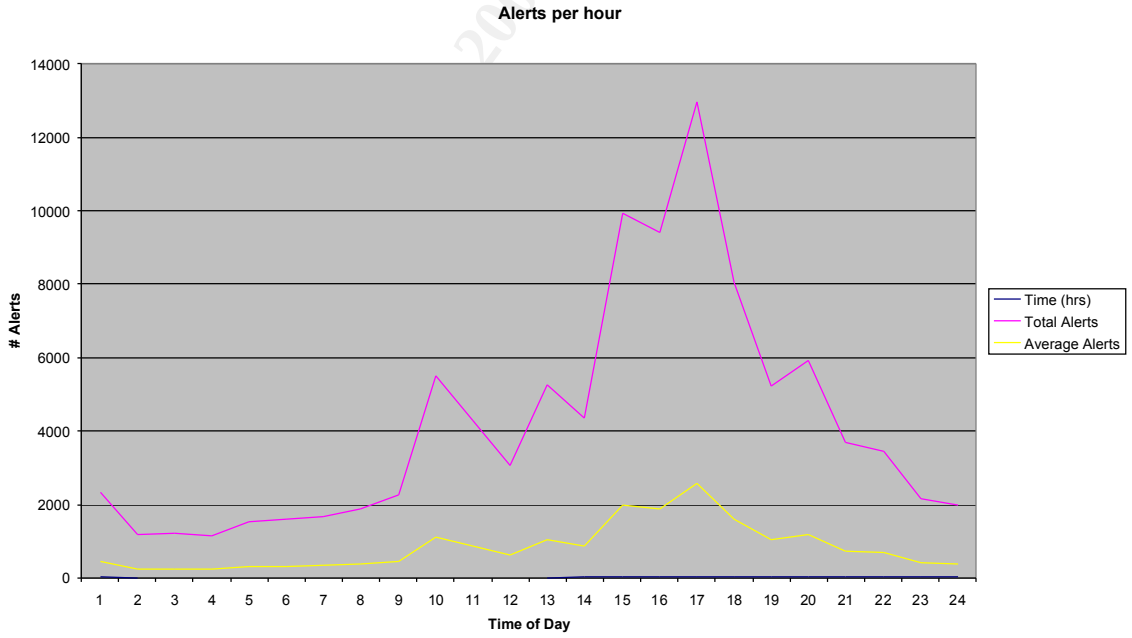
Scan Type	# of scans
UDP	497009
SYN	91213
NOACK	35
INVALIDACK	34
NULL	28
UNKNOWN	27
VECNA	15
SYNFIN	4
XMAS	3
FIN	3
FULLXMAS	2
SPAU	1
5	1
8	1
7	1
6	1
NMAPID	1

Alerts by day



Notice that alerts on January 3rd are very low. Chances are the establishment was closed for that period.

Alerts by hour



As expected, this line graph shows that the more people using the network, the more activity is reported. The fact that there is such a huge difference here demonstrates that the IDS is not tuned properly.

Top 10 Internal to Internal Sources

# of Alerts	Source	Destination	Alert Message
25575	127.127.5.202	127.127.5.1	ICMP traceroute
4580	127.127.153.146	127.127.150.198	connect to 515 from inside
2998	127.127.153.114	127.127.150.198	connect to 515 from inside
1885	127.127.88.181	127.127.150.198	connect to 515 from inside
1645	127.127.150.41	127.127.152.109	SNMP public access
1640	127.127.153.106	127.127.150.198	connect to 515 from inside
1626	127.127.153.119	127.127.150.198	connect to 515 from inside
1590	127.127.153.220	127.127.152.109	SNMP public access
1450	127.127.150.245	127.127.152.109	SNMP public access
875	127.127.88.240	127.127.150.195	SNMP public access

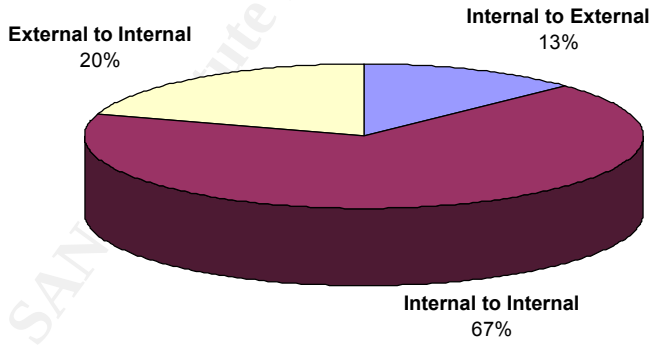
Top 10 Internal to External Sources

# of alerts	Source	Destination	Alert Message
1600	127.127.153.114	211.115.213.202	spp_http_decode: IIS Unicode attack detected
672	127.127.153.180	211.115.213.202	spp_http_decode: IIS Unicode attack detected
495	127.127.153.167	211.233.29.211	spp_http_decode: IIS Unicode attack detected
448	127.127.153.203	211.115.213.202	spp_http_decode: IIS Unicode attack detected
418	127.127.153.111	211.32.117.26	spp_http_decode: IIS Unicode attack detected
386	127.127.153.123	211.32.117.228	spp_http_decode: IIS Unicode attack detected
385	127.127.153.126	211.32.117.26	spp_http_decode: IIS Unicode attack detected
322	127.127.153.124	211.32.117.35	spp_http_decode: IIS Unicode attack detected
290	127.127.153.123	211.32.117.37	spp_http_decode: IIS Unicode attack detected
266	127.127.153.180	211.115.213.207	spp_http_decode: IIS Unicode attack detected

Top 10 External to Internal Sources

# of alerts	Source	Destination	Message
1897	203.248.242.22	127.127.88.167	MISC Large UDP Packet
1519	210.76.63.49	127.127.88.165	MISC Large UDP Packet
1263	211.233.70.161	127.127.153.154	MISC Large UDP Packet
1060	211.233.70.162	127.127.153.154	MISC Large UDP Packet
969	203.199.69.118	127.127.153.210	MISC Large UDP Packet
593	202.102.29.141	127.127.150.143	MISC Large UDP Packet
476	216.106.166.211	127.127.153.45	MISC Large UDP Packet
465	216.106.166.164	127.127.153.45	MISC Large UDP Packet
418	211.43.209.7	127.127.153.118	MISC Large UDP Packet
245	64.4.12.179	127.127.153.113	INFO MSN IM Chat data

Alert Flow



This graph shows the greatest threat to this network originating from the internal.

Case: Probable Back Orifice infection

Date	time	msecs	Source	port	Destination	port	msg

7/1/2002	1:55:02 AM	493765	127.127.150.165	1615	127.127.150.1	31337	Back Orifice
7/1/2002	1:56:40 AM	999965	127.127.150.165	1615	127.127.150.1	31337	Back Orifice

127.127.150.1 could be a router.
Let's check the source view to see if 127.127.150.1 is the source of any attacks

Date	time	msecs	src	dst	Msg
4/1/2002	4:44:47 PM	4859	127.127.150.1	127.127.150.24	ICMP Destination Unreachable (Communication Administratively Prohibited)
4/1/2002	5:35:36 PM	340663	127.127.150.1	127.127.150.24	ICMP Destination Unreachable (Communication Administratively Prohibited)
4/1/2002	5:35:42 PM	339520	127.127.150.1	127.127.150.24	ICMP Destination Unreachable (Communication Administratively Prohibited)

There is a gap of about 200 identical entries with short time intervals
This seems to confirm that 127.127.150.1 is a router as it's sending back ICMP destination unreachable messages, which is typical of a router

Let's see what originates from 127.127.150.24

date	time	msecs	src	dst	Msg
7/1/2002	12:16:44 PM	586137	127.127.150.124	224.0.0.2	ICMP Router Selection
7/1/2002	12:16:47 PM	583857	127.127.150.124	224.0.0.2	ICMP Router Selection
7/1/2002	12:16:50 PM	589132	127.127.150.124	224.0.0.2	ICMP Router Selection

We see here that there is an attempt to multicast from this host a lot.

In investigating the target of 224.0.0.2, that 510 alert generations were this ICMP Router selection message out of the 1066 alerts generated to this multicast address were from the 127.127.150 subnet (Assuming this is a class C LAN). This could be that 127.127.150.24 had a previous connection to a host and the other side suddenly dropped off the network. Since a multicast application might also warrant another channel of communication from the server to the client through a stateless protocol like UDP then it is possible to get the destination unreachable message above many times before the server stops emitting to the downed host. The router will then be the source of the ICMP message explaining the result above.

Case: An x86 root exploit

The following struck as unusual. Let's look into it more closely.

date	time	msecs	src	srcport	dst	dstport	msg
5/1/2002	2:41:12 PM	260596	207.199.1.201	80	127.127.153.142	2357	EXPLOIT x86 stealth noop
5/1/2002	3:17:14 PM	722180	207.46.177.148	80	127.127.153.211	1561	EXPLOIT x86 NOOP
5/1/2002	3:35:50 PM	713629	63.100.129.17	80	127.127.153.112	3311	EXPLOIT x86 stealth noop
5/1/2002	4:52:32 PM	665815	207.199.1.201	80	127.127.153.142	2908	EXPLOIT x86 stealth noop
6/1/2002	4:17:30 AM	354187	24.178.184.42	1214	127.127.88.162	4823	EXPLOIT x86 setuid 0
6/1/2002	4:17:57 AM	465872	24.178.184.42	1214	127.127.88.162	4823	EXPLOIT x86 setuid 0
6/1/2002	1:05:38 PM	984609	24.95.245.166	4236	127.127.150.190	20	EXPLOIT x86 NOOP
6/1/2002	3:14:22 PM	583843	24.95.245.166	4668	127.127.150.190	20	EXPLOIT x86 setgid 0
6/1/2002	5:30:01 PM	690465	63.111.13.106	80	127.127.88.165	1494	EXPLOIT x86 setuid 0
6/1/2002	6:00:43 PM	119537	130.232.134.181	1707	127.127.150.143	9876	EXPLOIT x86 setgid 0
7/1/2002	12:35:31AM	844584	130.232.134.181	2138	127.127.150.143	9876	EXPLOIT x86 setuid 0
7/1/2002	12:51:43AM	118217	130.232.134.181	2138	127.127.150.143	9876	EXPLOIT x86 setuid 0

7/1/2002	11:37:33AM	230332	136.160.130.177	14683	127.127.150.63	6970	EXPLOIT x86 setgid 0
7/1/2002	11:37:34AM	374050	136.160.130.177	31710	127.127.150.102	6970	EXPLOIT x86 setgid 0
7/1/2002	1:31:01 PM	913868	211.100.18.142	20	127.127.150.143	4762	EXPLOIT x86 setuid 0
7/1/2002	6:22:51 PM	371270	61.136.61.21	80	127.127.152.158	1927	EXPLOIT x86 setuid 0
7/1/2002	7:23:15 PM	201543	152.163.226.57	80	127.127.5.239	2588	EXPLOIT x86 setgid 0
7/1/2002	8:04:04 PM	721942	61.156.35.58	3542	127.127.152.163	1178	EXPLOIT x86 setuid 0
7/1/2002	8:29:49 PM	816069	61.156.35.58	1101	127.127.152.165	1417	EXPLOIT x86 setuid 0

Most of these are due to strings of Byte looking code that take advantage of buffer overflows to do nasty things. Active research on Google, inside the present SNORT rules and the like yield no more explanations. By looking at the destination ports, the only worry would be from 24.95.245.166 (A road runner address) as it might be trying to take advantage of an unknown buffer overflow in FTPd. The other interesting thig to point out are the connections from port 20 and port 80 to a high port. The hosts pointed to by these attacks should be checked on the port numbers above in order to make sure they are explained.

There are no port scans associated with the combination of source, destinations above.
Here is the Whois information for the 24.95.245.166 intruder:

ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-3-A)
13241 Woodland Park Road
Herndon, VA 20171
US

Netname: ROAD-RUNNER-3-A
Netblock: 24.92.160.0 - 24.95.255.255
Maintainer: SCRR

Coordinator:
ServiceCo LLC (ZS30-ARIN) abuse@rr.com
1-703-345-3416

Domain System inverse mapping provided by:

DNS1.RR.COM	24.30.200.3
DNS2.RR.COM	24.30.201.3
DNS3.RR.COM	24.30.199.7
DNS4.RR.COM	65.24.0.172

Record last updated on 30-Aug-2001.
Database last updated on 27-Jan-2002 19:56:09 EDT.

Case: A Proxy Scan

Web server exploits are always common. But this struck as odd because all the other hosts on 127.127.150.X are not associated with any activity like this.

Date	time	msecs	Src	port	dst	port	msg
7/1/2002	10:39:39AM	392342	216.152.64.151	45101	127.127.150.103	1080	SCAN Proxy attempt
7/1/2002	10:39:39AM	468652	216.152.64.151	45102	127.127.150.103	1080	SCAN Proxy attempt
6/1/2002	6:01:46 PM	270880	216.152.64.163	53390	127.127.150.103	8080	SCAN Proxy attempt
6/1/2002	6:01:46 PM	272292	216.152.64.163	53392	127.127.150.103	3128	INFO - Possible Squid Scan
6/1/2002	6:01:46 PM	273598	216.152.64.163	53393	127.127.150.103	1080	SCAN Proxy attempt

If the target is taken in from a source perspective, the only thing that appears is

Date	time	Msecs	Src	port	Dst	port	msg
7/1/2002	4:43:01 PM	503782	127.127.150.103	1370	216.136.175.131	80	spp_http_decode: IIS Unicode attack detected

Looking further into this, taking the 216.152.64.X above within a target perspective yields no results.

Looking at 216.136.175.131 from the source perspective yields no results.

DShield reports 216.152.64.151 (katana.webchat.org) as being the source of 75 complaints over 25 targets. These two 216.152.64.X addresses are looking for Proxy connections.

The following hosts should be looked at for further information as to what was trying to be achieved with these scans.

Host	# of proxy scans against
127.127.150.103	5
127.127.153.111	5
127.127.153.117	2
127.127.153.127	3
127.127.153.148	6
127.127.153.162	8
127.127.153.178	6

Since the times are so apart, there is no relation and hence not enough info the get more information. Here is the detailed Whois information for the 216.152.64.X range:

WebMaster, Incorporated (NETBLK-WEBMASTER-BLK-1)

1601 Civic Center Drive, Suite 101
Santa Clara, CA 95050
US

Netname: WEBMASTER-BLK-1
Netblock: 216.152.64.0 - 216.152.79.255
Maintainer: WBMR

Coordinator:
Owen, Mark (MO21-ARIN) mark@WEBMASTER.COM
+1-408-345-1800 (FAX) +1-408-247-9372

Domain System inverse mapping provided by:

NS1.WEBMASTER.COM 209.133.28.80
NS1.WEBCHAT.ORG 216.152.64.200

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 01-Aug-2000.
Database last updated on 27-Jan-2002 19:56:09 EDT.

Case: MISC Large UDP Packet

This is odd because there are nearly 450 iterations of it.

Date	Time	msecs	src	port	dst	port	msg
7/1/2002	4:41:43 PM	206709	202.102.29.141	1242	127.127.150.143	1568	MISC Large UDP Packet
7/1/2002	4:41:43 PM	316155	202.102.29.141	1242	127.127.150.143	1568	MISC Large UDP Packet
7/1/2002	4:41:44 PM	133358	202.102.29.141	1242	127.127.150.143	1568	MISC Large UDP Packet

Date	Time	msecs	src	port	dst	port	msg
7/1/2002	5:18:40 PM	541225	202.102.29.141	1260	127.127.150.143	1568	MISC Large UDP Packet
7/1/2002	5:18:40 PM	653412	202.102.29.141	1260	127.127.150.143	1568	MISC Large UDP Packet
7/1/2002	5:18:40 PM	750665	202.102.29.141	1260	127.127.150.143	1568	MISC Large UDP Packet

202.102.29.141 seems to be an address in China:

```
inetnum             202.102.29.0 - 202.102.29.255
netname             JSINFO
descr               JIANGSU INFORMATION SERVICE BUREAU
country             CN
admin-c             ZJ8-AP, inverse
tech-c              XQ5-AP, inverse
changed             zhengch@public1.ptt.js.cn 971019
source              APNIC


person              zhengpeng ji, inverse
address             NO.301,ZHONGSHAN BEI ROAD,NANJING,JIANGSU
country             CN
phone               +86-25-3343952
fax-no              +86-25-3343952
nic-hdl             ZJ8-AP, inverse
mnt-by              MAINT-NULL, inverse
changed             zhengch@public1.ptt.js.cn 19971019
source              APNIC

person              xiaoli.qi, inverse
address             NO.301,ZHONGSHAN BEI ROAD,NANJING,JIANGSU
country             CN
phone               +86-25-3343952
fax-no              +86-25-3343952
nic-hdl             XQ5-AP, inverse
changed             zhengch@public1.ptt.js.cn 971019
source              APNIC
```

UDP port 1568 is reported as being used for the streamworks streaming application[4] according to the GTA website. According to th official StreamWorks, this is done on port 1558. Streamworks belongs to Xing which is part of Real. There must be a lot of videostreaming going on here.(Hence the multicasting addresses)

There is a small series of alerts after this. It seems to indicate a MSN Instant Messenger Chat about ten minutes after the videoconference. This would make sense.

Date	time	msecs	src	port	dst	port	msg
7/1/2002	5:26:07PM	125918	64.4.12.183	1863	127.127.150.143	2063	INFO MSN IM Chat data
7/1/2002	5:26:26PM	449577	64.4.12.183	1863	127.127.150.143	2063	INFO MSN IM Chat data
7/1/2002	5:27:05PM	758666	64.4.12.183	1863	127.127.150.143	2063	INFO MSN IM Chat data

[4] www.gta.com/Pages/Docs/chapters/11-AppendixB.pdf

]Case: FTP Warez Site

This has been taken as an oddity because there are many anonymous FTP connections to this host but not from a wide range of IP addresses and all within a short period of time.

Date	Time	Msecs	src	port	dst	port	msg
6/1/2002	3:32:06 PM	478066	193.253.42.45	1330	127.127.150.190	21	INFO FTP anonymous FTP
7/1/2002	4:13:44 PM	870216	24.13.140.41	3781	127.127.150.190	21	INFO FTP anonymous FTP
6/1/2002	12:16:08 PM	965504	24.95.245.166	3815	127.127.150.190	21	INFO FTP anonymous FTP
Date	**Time**	**Msecs**	**src**	**port**	**dst**	**port**	**msg**
6/1/2002	5:13:07 AM	94259	62.163.158.112	1112	127.127.150.190	21	INFO FTP anonymous FTP
7/1/2002	3:18:51 AM	347818	66.30.59.155	24200	127.127.150.190	21	INFO FTP anonymous FTP

FTP connections are usually harmless. At a university this might be an indication that Warez trading is happening.

Source	Destination	# of connections
198.173.24.162	127.127.150.145	26
24.95.245.166	127.127.150.190	13
130.94.19.198	127.127.5.95	6
130.94.19.198	127.127.5.92	6
62.163.158.112	127.127.150.190	3
66.30.59.155	127.127.150.190	2

All FTP access is from the external networks. There is not a significant amount of connections to positively say that these are legitimate FTP servers. They should be checked out.

Case: Connection to port 515 from inside

This is odd because it is declared as the most common alert. It therefore needs to be explained.

It seems that this is an application that runs between computers on the 127.127.88.X, 127.127.153.X, and the host 127.127.150.198.

Looking from the target perspective, these are all connections to 127.127.150.198. It is easier to scan in on this by using a query that isolates this alert[2]. There are 18026 variations of this which

matches the number of attacks on this host making it top target.

Looking at the source perspective, 127.127.150.198 does not pop up on the radar screen but a lot of ICMP router selections going to broadcast addresses are being emitted.

Firstly, Dean White's paper[5] hints at this being a printer related issue. This may well be but this is a lot of printing activity. Indications that this is true are that there are a lot of SNMP alerts going to these hosts as well. Network printers often use SNMP for status and control.

The broadcasts emitted from the targets hint at this being some sort of Video/Audio multimedia application

Let's dive in and try to explain most of what is going on here.

A whois on some of the previous alerts pointed to realsrv.towson.edu.

Towson University boasts a lot about online learning using their blackboard web application and the fact that if you don't have a computer at home you can use one of their many labs.

Note that this is not necessarily Towson University but the university could be using the same type of application.

The 127.127.150.X subnet would contain a cluster of streaming servers. People connect to it via a gateway that is situated on 127.127.150.198 using UDP. This subnet broadcasts on a multicast channel, which explains why only this subnet is using multicast addresses.

Other observations. Since this is an interactive multimedia application, students can talk back to the system between each other. Some version of MSN IM is used to do this. Some Real Player seems to be involved as well, thus more UDP packets. More protocol detail is necessary in order to fully comprehend how the application works. SNORT should be tweaked to ignore most of the alerts it is currently producing.

Other things we can filter out are all the connections between most hosts and 127.127.151.114, as it seems to be some sort of control center using SNMP as a communication point. There are a lot of accesses between that and the 127.127.150.198 server to assume that it is either part of the system or a network management tool making sure everything is working fine. Hence, we can filter it out.

Looking at some statistics involving 127.127.150.X as scan targets reveals that it is mostly involved with UDP scans.

[5] http:// www.giac.org/practical/Dean_White_GCIA.doc

Source	Destination	Port	Type	# of attempts
12.25.239.5	127.127.150.120	0	UDP	1720
127.127.150.143	127.127.150.1	1900	UDP	760
12.25.239.5	127.127.150.120	1814	UDP	296
12.25.239.5	127.127.150.120	7001	UDP	268
12.25.239.5	127.127.150.120	3422	UDP	139
12.25.239.5	127.127.150.120	1222	UDP	36
12.25.239.5	127.127.150.120	7000	UDP	36
12.25.239.5	127.127.150.120	1448	UDP	36
12.25.239.5	127.127.150.120	1230	UDP	31
12.25.239.5	127.127.150.120	1	UDP	21
12.25.239.5	127.127.150.120	1356	UDP	21
127.127.153.121	127.127.150.83	80	SYN	18
12.25.239.5	127.127.150.120	1260	UDP	14
12.25.239.5	127.127.150.120	15677	UDP	14
127.127.153.173	127.127.150.198	28204	SYN	12
127.127.5.74	127.127.150.28	68	UDP	12
127.127.153.173	127.127.150.198	2355	SYN	12
12.25.239.5	127.127.150.120	1251	UDP	11
12.25.239.5	127.127.150.120	1273	UDP	11
12.25.239.5	127.127.150.120	3742	UDP	10
127.127.153.204	127.127.150.198	28204	SYN	10
127.127.88.148	127.127.150.198	28204	SYN	10
127.127.88.148	127.127.150.198	2355	SYN	10
127.127.153.204	127.127.150.198	2355	SYN	10
127.127.153.148	127.127.150.198	2355	SYN	9
127.127.153.209	127.127.150.198	2355	SYN	9
127.127.153.209	127.127.150.198	28204	SYN	9
12.25.239.5	127.127.150.120	1317	UDP	9
12.25.239.5	127.127.150.120	8224	UDP	9
127.127.153.148	127.127.150.198	28204	SYN	9
127.127.153.45	127.127.150.83	80	SYN	8
12.25.239.5	127.127.150.120	1267	UDP	8
12.25.239.5	127.127.150.120	1323	UDP	8
127.127.153.113	127.127.150.83	80	SYN	8
127.127.153.46	127.127.150.83	80	SYN	8
127.127.153.172	127.127.150.198	2355	SYN	8
127.127.153.124	127.127.150.83	80	SYN	8
127.127.153.126	127.127.150.83	80	SYN	8
12.25.239.5	127.127.150.120	12637	UDP	8
127.127.153.172	127.127.150.198	28204	SYN	8
127.127.153.162	127.127.150.198	28204	SYN	7
12.25.239.5	127.127.150.120	24948	UDP	7

Interesting to note here is that all UDP scans are from 12.25.239.5 and it is reported at DShield as having 6 complaints logged against it. It belongs to AT&T.

Case: Looking for scans from 12.25.239.5

Since the previous case raised a flag in looking at this IP address, a query was made to see what source of alerts, port scans and Out of Spec packets it is responsible for.

date	time	msecs	src	srcport	Dst	dstport	msg
7/1/2002	3:18:26 PM	891851	12.25.239.5	123	127.127.150.120	123	EXPLOIT NTPDX buffer overflow
7/1/2002	3:18:27 PM	544514	12.25.239.5	123	127.127.150.120	123	EXPLOIT NTPDX buffer overflow
7/1/2002	3:29:36 PM	160739	12.25.239.5	65535	127.127.150.120	65535	High port 65535 udp - possible Red Worm - traffic
7/1/2002	3:32:25 PM	132745	12.25.239.5	65535	127.127.150.120	5600	High port 65535 udp - possible Red Worm - traffic
7/1/2002	3:32:25 PM	786799	12.25.239.5	65535	127.127.150.120	5600	High port 65535 udp - possible Red Worm - traffic
7/1/2002	3:46:34 PM	985799	12.25.239.5	43263	127.127.150.120	65535	High port 65535 udp - possible Red Worm - traffic
7/1/2002	4:17:26 PM	909814	12.25.239.5	69	127.127.150.120	9984	TFTP - Internal UDP connection to external tftp server
7/1/2002	4:43:52 PM	286640	12.25.239.5	255	127.127.150.120	65535	High port 65535 udp - possible Red Worm - traffic
7/1/2002	4:43:52 PM	940807	12.25.239.5	255	127.127.150.120	65535	High port 65535 udp - possible Red Worm - traffic
7/1/2002	4:46:49 PM	685110	12.25.239.5	65535	127.127.150.120	20735	High port 65535 udp - possible Red Worm - traffic
7/1/2002	5:01:45 PM	653196	12.25.239.5	51455	127.127.150.120	65535	High port 65535 udp - possible Red Worm - traffic
7/1/2002	5:07:20PM	157367	12.25.239.5	65535	127.127.150.120	34240	High port 65535 udp - possible Red Worm - traffic

The TFTP, NTPDX and High port connections indicate that Nimda worm may also affect this IP address.

The port scans associated with this source (In frequency by type)

Source	Destination	Type	# of attempts
12.25.239.5	127.127.150.120	UDP	4755

Seems like a good possibility that this source has infected 127.127.150.120 with the Nimda virus.

Case: TFTP activity

Since the above revealed that TFTP pointed towards Nimda then a look at TFTP alerts was made.

date	time	msecs	src	Srcport	dst	dstport	msg
7/1/2002	10:41:15AM	244964	66.54.188.69	6918	127.127.153.211	69	TFTP - External UDP connection to internal tftp server
7/1/2002	4:17:26PM	909814	12.25.239.5	69	127.127.150.120	9984	TFTP - Internal UDP connection to external tftp server

66.54.188.69 is reported at DShield.org to have 6 complaints against it as well on 2 targets. Looking at port scans from this IP (This alert was the only one in the snort alert file for this IP) yields:

source Field	dest Field	type Field	NumberOfDups
66.54.188.69	127.127.153.211	UDP	40

Looks like this may be Nimda after all. We must verify 127.127.153.120 and 127.127.153.211 to see if they are showing signs of infection.

Case: Nimda worm

Looking at the activity from the above hosts it can be observed that they are responding to their original aggressors and that they are on the lookout for new victims.

date	time	msecs	Source	port	Destination	port	Alert
5/1/2002	1:06:55 PM	887315	127.127.153.211	2869	211.78.38.201	80	spp_http_decode: IIS Unicode attack detected
5/1/2002	1:06:56 PM	236511	127.127.153.211	2872	66.28.38.7	80	spp_http_decode: IIS Unicode attack detected
5/1/2002	1:06:56 PM	236983	127.127.153.211	2873	66.28.38.7	80	spp_http_decode: IIS Unicode attack detected
5/1/2002	1:07:04 PM	612032	127.127.153.211	2874	211.78.38.201	80	spp_http_decode: IIS Unicode attack detected
5/1/2002	1:07:22 PM	655421	127.127.153.211	2880	66.28.38.7	80	spp_http_decode: IIS Unicode attack detected
5/1/2002	1:07:22 PM	655895	127.127.153.211	2881	66.28.38.7	80	spp_http_decode: IIS Unicode attack detected
5/1/2002	1:07:33 PM	952202	127.127.153.211	2888	202.216.229.205	80	spp_http_decode: IIS Unicode attack detected
5/1/2002	1:07:35 PM	542618	127.127.153.211	2889	202.216.229.205	80	spp_http_decode: IIS Unicode attack detected
5/1/2002	1:07:37 PM	936014	127.127.153.211	2884	66.28.38.7	80	spp_http_decode: IIS Unicode attack detected
5/1/2002	1:14:21 PM	251409	127.127.153.211	3093	211.78.38.201	80	spp_http_decode: IIS Unicode attack detected
5/1/2002	1:14:22 PM	272964	127.127.153.211	3095	211.78.38.201	80	spp_http_decode: IIS Unicode attack detected
7/1/2002	2:53:48 PM	152276	127.127.150.120		12.25.239.5		ICMP Fragment Reassembly Time Exceeded
7/1/2002	3:19:29 PM	605216	127.127.150.120		12.25.239.5		ICMP Fragment Reassembly Time Exceeded
7/1/2002	3:20:21 PM	638634	127.127.150.120		12.25.239.5		ICMP Fragment Reassembly Time Exceeded
7/1/2002	3:30:45 PM	511262	127.127.150.120		12.25.239.5		ICMP Fragment Reassembly Time Exceeded
7/1/2002	8:26:17 PM	312595	127.127.153.211	2343	216.136.130.63	80	spp_http_decode: IIS Unicode attack detected
7/1/2002	8:26:17 PM	312595	127.127.153.211	2343	216.136.130.63	80	spp_http_decode: IIS Unicode attack detected
7/1/2002	8:26:17 PM	312595	127.127.153.211	2343	216.136.130.63	80	spp_http_decode: IIS Unicode attack detected
7/1/2002	8:26:17 PM	312595	127.127.153.211	2343	216.136.130.63	80	spp_http_decode: IIS Unicode attack detected
7/1/2002	8:26:17 PM	312595	127.127.153.211	2343	216.136.130.63	80	spp_http_decode: IIS Unicode attack detected
7/1/2002	8:37:35 PM	443681	127.127.153.211	2425	216.136.130.63	80	spp_http_decode: IIS Unicode attack detected
7/1/2002	8:37:35 PM	443681	127.127.153.211	2425	216.136.130.63	80	spp_http_decode: IIS Unicode attack detected
7/1/2002	8:37:35 PM	443681	127.127.153.211	2425	216.136.130.63	80	spp_http_decode: IIS Unicode attack detected

Port scans associated with these two hosts are indicative of the same trace as from 12.25.239.5.
T
127.127.150.120 does not seem to have been infected as it is showing no reactive signs but 127.127.153.211 is showing spurious Unicode attempts.

Here are the top port scans from 127.127.153.211 that correlates with some of the targets in the previous table.

Target	Scan Type	# of attempts
127.127.1.3	UDP	251
127.127.1.4	UDP	248
211.13.210.44	SYN	221
127.127.6.45	UDP	127
127.127.60.43	UDP	76
127.127.6.49	UDP	71
127.127.6.50	UDP	69
127.127.6.33	UDP	41
127.127.1.13	UDP	27
202.104.129.254	UDP	26
210.51.226.213	UDP	23
127.127.1.7	UDP	22
131.118.254.39	SYN	18
216.35.148.100	SYN	18
209.75.20.41	SYN	16
209.25.153.9	SYN	16
204.71.191.220	SYN	16
207.68.172.246	SYN	15
127.127.150.198	SYN	14
127.127.1.5	UDP	14
207.228.239.150	SYN	13
207.228.238.48	SYN	13
216.35.148.117	SYN	12
61.180.7.134	SYN	11
131.118.254.38	SYN	11
205.138.3.42	SYN	11
61.135.133.109	SYN	8
209.225.32.5	SYN	8
202.103.248.232	SYN	8
64.124.76.21	SYN	8

Case: SMB Name Wildcards

These occur quite often in the alert log. Again, the destination and the source are fairly consistent. We can consider this a standard Net BIOS protocol occurrence between windows machines.

Where this becomes worrisome is when there are probes that originate outside of the LAN.

Here are the SMB Name Wildcard transactions:

Source	Destination	# of attempts
127.127.5.7	127.127.5.87	264
127.127.5.87	127.127.5.7	259
127.127.150.209	127.127.5.4	40
127.127.153.158	127.127.5.4	20
127.127.150.77	127.127.5.4	19
127.127.150.28	127.127.5.4	15
127.127.150.209	127.127.5.35	14
127.127.151.125	127.127.5.4	7
127.127.150.145	127.127.5.4	6
127.127.88.183	127.127.5.35	6
127.127.88.183	127.127.5.4	6
127.127.150.77	127.127.5.35	5
127.127.150.144	127.127.5.4	5
127.127.70.177	127.127.5.239	3
127.127.70.177	127.127.5.245	3
127.127.220.26	127.127.151.114	3
127.127.150.207	127.127.5.35	3
127.127.150.144	127.127.5.35	3
127.127.150.127	127.127.5.4	3
127.127.150.207	127.127.5.4	3
127.127.107.79	127.127.150.139	2
127.127.220.26	127.127.150.143	2
127.127.220.26	127.127.150.54	2
127.127.150.143	127.127.220.26	2

These all seem to be legitimate. There seems to be a lot of traffic between 127.127.5.7 and 127.127.5.87. This should be looked into for performance reasons.

No mention of this alert was found on Google except for a complaint or two from some people who were saying that they were getting "spoofed" requests from random IP addresses. This is not the case here and this is seen as regular Net BIOS traffic.

Case: ICQ Usage

ICQ is another chat program like MSN IM. Here is a table of ICQ Usage.

Source	Destination	# of transactions
127.127.151.79	205.188.248.57	253
127.127.151.79	205.188.248.25	189
127.127.151.79	205.188.165.89	143
127.127.151.79	152.163.226.89	137
127.127.151.79	205.188.248.89	96
127.127.151.79	152.163.226.57	89
127.127.151.79	205.188.165.57	86
127.127.151.79	64.12.184.121	75
127.127.151.79	152.163.226.153	68
127.127.151.79	64.12.174.153	63
127.127.151.79	152.163.226.185	58
127.127.151.79	152.163.226.121	53
127.127.151.79	64.12.184.89	44
127.127.151.79	205.188.165.185	40
127.127.151.79	152.163.226.25	31
127.127.151.79	64.12.184.57	30
127.127.151.79	205.188.165.153	27
127.127.5.239	152.163.226.57	26
127.127.151.79	205.188.165.25	26
127.127.151.79	64.12.184.25	19
127.127.151.79	208.184.29.190	16
127.127.151.79	208.184.29.210	14

127.127.151.79	64.12.174.185	14
127.127.151.79	205.138.3.62	14
127.127.151.79	205.138.3.22	13
127.127.151.79	205.138.3.230	13
127.127.151.79	205.138.3.42	10
127.127.5.239	205.188.248.57	9
127.127.151.79	205.138.3.220	9
127.127.151.79	205.138.3.82	9
127.127.151.79	205.188.250.25	8
127.127.151.79	205.138.3.102	8
127.127.151.79	205.138.3.142	8
127.127.151.79	204.253.104.205	7
127.127.151.79	204.253.104.220	5
127.127.5.239	205.188.250.25	5
127.127.5.239	205.188.248.89	4
127.127.151.79	204.253.104.15	2
127.127.151.79	205.188.165.121	2
127.127.5.239	205.188.165.57	2

These are of NOTICE category and hence will be ignored

Case: Multiple ICMP Trace Routes

This is noted because it is one of the most detected alerts.

A sample from the trace route message has been taken.

Date	time	msecs	Src	port	dst	port	msg
4/1/2002	4:44:58 PM	87134	127.127.5.202		127.127.5.1		ICMP traceroute
4/1/2002	4:45:08 PM	84126	127.127.5.202		127.127.5.1		ICMP traceroute
4/1/2002	4:45:18 PM	89540	127.127.5.202		127.127.5.1		ICMP traceroute

4/1/2002	4:45:48 PM	76167	127.127.5.202		127.127.5.1		ICMP traceroute
4/1/2002	4:45:58 PM	71776	127.127.5.202		127.127.5.1		ICMP traceroute
4/1/2002	4:46:08 PM	66308	127.127.5.202		127.127.5.1		ICMP traceroute
4/1/2002	4:46:18 PM	63373	127.127.5.202		127.127.5.1		ICMP traceroute
4/1/2002	4:46:28 PM	57303	127.127.5.202		127.127.5.1		ICMP traceroute
4/1/2002	4:46:38 PM	52146	127.127.5.202		127.127.5.1		ICMP traceroute
4/1/2002	4:46:48 PM	48127	127.127.5.202		127.127.5.1		ICMP traceroute

Notice that these traces are always 10 seconds apart. This is consistent through the alert database. If 127.127.5.1 is a router, then maybe 127.127.4.202 is a monitoring host of sorts or another router using NAT to emit these packets.

Case: L3 Retriever Pings:

Date	time	msecs	src	port	dst	port	msg
6/1/2002	12:13:33 PM	256106	127.127.150.145		127.127.10.49		ICMP Echo Request L3retriever Ping
7/1/2002	9:49:47 AM	751302	127.127.150.127		127.127.10.49		ICMP Echo Request L3retriever Ping
7/1/2002	2:27:09 PM	882056	127.127.150.145		127.127.10.49		ICMP Echo Request L3retriever Ping
7/1/2002	11:40:29 AM	28798	127.127.143.72		127.127.150.139		ICMP Echo Request L3retriever Ping
4/1/2002	6:05:03 PM	615174	127.127.225.46		127.127.5.118		ICMP Echo Request L3retriever Ping
5/1/2002	11:59:29 AM	829152	127.127.150.209		127.127.5.35		ICMP Echo Request L3retriever Ping
6/1/2002	12:01:51 PM	75082	127.127.150.77		127.127.5.35		ICMP Echo Request L3retriever Ping
6/1/2002	12:04:40 PM	840878	127.127.150.207		127.127.5.35		ICMP Echo Request L3retriever Ping
6/1/2002	6:41:39 PM	64345	127.127.150.209		127.127.5.35		ICMP Echo Request L3retriever Ping
7/1/2002	7:57:28 AM	415854	127.127.150.144		127.127.5.35		ICMP Echo Request L3retriever Ping
7/1/2002	8:31:08 AM	64153	127.127.88.183		127.127.5.35		ICMP Echo Request L3retriever Ping
7/1/2002	12:52:39 PM	134699	127.127.150.209		127.127.5.35		ICMP Echo Request L3retriever Ping
7/1/2002	1:49:47 PM	85514	127.127.150.77		127.127.5.35		ICMP Echo Request L3retriever Ping
7/1/2002	9:09:54 PM	875650	127.127.150.209		127.127.5.35		ICMP Echo Request L3retriever Ping
4/1/2002	5:25:06 PM	946839	127.127.150.209		127.127.5.4		ICMP Echo Request L3retriever Ping
6/1/2002	12:02:04 PM	64222	127.127.150.77		127.127.5.4		ICMP Echo Request L3retriever Ping
6/1/2002	12:08:32 PM	808389	127.127.150.28		127.127.5.4		ICMP Echo Request L3retriever Ping
4/1/2002	4:52:35 PM	649189	127.127.5.7		127.127.5.87		ICMP Echo Request L3retriever Ping

These L3 Pings are being reported because they contain a big part of the alphabet in the DATA portion of the ICMP packet. This seems to be a signature left by the L3 scanning tool. Looking at the source of these scans (Most of them come in triplets, often more than once a day) for other regular activity around the same times reveals UDP and SYN scans at around the same time.

Example:

Date	time	source	dest	type
7/1/2002	7:57:29 AM	127.127.150.144	127.127.5.35	SYN
7/1/2002	7:57:30 AM	127.127.150.144	127.127.5.35	UDP
7/1/2002	7:57:33 AM	127.127.150.144	127.127.5.35	UDP

Here are the scans that match with these alerts

Date	time	source	dest	type
4/1/2002	6:16:56 PM	127.127.84.7	127.127.5.92	SYN
4/1/2002	6:17:03 PM	127.127.84.7	127.127.5.92	SYN
4/1/2002	6:16:56 PM	127.127.84.7	127.127.5.92	SYN
4/1/2002	6:16:56 PM	127.127.84.7	127.127.5.92	SYN
4/1/2002	6:16:55 PM	127.127.84.7	127.127.5.92	SYN
4/1/2002	6:16:55 PM	127.127.84.7	127.127.5.92	SYN
4/1/2002	6:16:55 PM	127.127.84.7	127.127.5.92	SYN
4/1/2002	6:16:56 PM	127.127.84.7	127.127.5.92	SYN
5/1/2002	5:17:43 PM	127.127.150.209	127.127.5.4	SYN
4/1/2002	5:25:12 PM	127.127.150.209	127.127.5.4	UDP
5/1/2002	5:17:42 PM	127.127.150.209	127.127.5.4	SYN
4/1/2002	5:25:10 PM	127.127.150.209	127.127.5.4	UDP
4/1/2002	5:25:07 PM	127.127.150.209	127.127.5.4	SYN
5/1/2002	1:29:26 PM	127.127.150.209	127.127.5.4	SYN
5/1/2002	1:29:28 PM	127.127.150.209	127.127.5.4	UDP
4/1/2002	5:25:06 PM	127.127.150.209	127.127.5.4	SYN
5/1/2002	5:17:46 PM	127.127.150.209	127.127.5.4	UDP
5/1/2002	5:17:48 PM	127.127.150.209	127.127.5.4	UDP
6/1/2002	5:42:01 PM	127.127.150.77	127.127.5.4	SYN

6/1/2002	5:42:04 PM	127.127.150.77	127.127.5.4	UDP
6/1/2002	5:42:06 PM	127.127.150.77	127.127.5.4	UDP
7/1/2002	8:19:38 PM	127.127.150.209	127.127.5.4	UDP
7/1/2002	8:19:40 PM	127.127.150.209	127.127.5.4	UDP
7/1/2002	8:19:35 PM	127.127.150.209	127.127.5.4	SYN
5/1/2002	1:29:30 PM	127.127.150.209	127.127.5.4	UDP
7/1/2002	6:10:27 PM	127.127.153.158	127.127.5.4	UDP
7/1/2002	6:10:23 PM	127.127.153.158	127.127.5.4	SYN
7/1/2002	7:57:30 AM	127.127.150.144	127.127.5.35	UDP
7/1/2002	8:36:46 AM	127.127.88.183	127.127.5.35	UDP
7/1/2002	7:57:33 AM	127.127.150.144	127.127.5.35	UDP
7/1/2002	7:57:29 AM	127.127.150.144	127.127.5.35	SYN
7/1/2002	8:36:42 AM	127.127.88.183	127.127.5.35	SYN

If we take the example above, 127.127.150.144 does a port scan at about the same time on 127.127.5.35 and the L3 Echo Request.

Taking a look at other ICMP related alerts; the same pattern can be seen with a few exceptions.

The regularity of these scans points to legitimate activity and hence we can ignore the majority of these port scans and L3 ping scans.

Case: ICMP Trace Route exceptions

These are the exception the the trace route claim made earlier.

Date	time	msecs	src	srcport	Dst	dstport	msg
4/1/2002	5:26:39 PM	291386	127.127.88.167		127.127.88.129		ICMP traceroute
4/1/2002	5:44:17 PM	98399	127.127.88.179		127.127.1.3		ICMP traceroute
7/1/2002	7:45:34 AM	41977	127.127.150.121		127.127.1.3		ICMP traceroute
7/1/2002	10:21:32 AM	244614	127.127.88.179		127.127.1.3		ICMP traceroute

7/1/2002	11:31:39 AM	777522	127.127.88.179		127.127.1.3		ICMP traceroute
7/1/2002	2:43:44 PM	168616	127.127.88.139		127.127.88.129		ICMP traceroute
7/1/2002	3:06:42 PM	854369	127.127.150.121		127.127.1.3		ICMP traceroute

The next case will discusses messages related to ICMP

Case: Miscellaneous ICMP probes

Here is an analysis of ICMP packets related alerts. Most of these seem like legitimate traffic. The first two show responses or targeting to a router and come from either network manager tools or an application trying to reach a host that is down.

Source	Destination	Alert Message	# Of occurrences
127.127.5.202	127.127.5.1	ICMP traceroute	25575
127.127.150.1	127.127.150.24	ICMP Destination Unreachable (Communication Administratively Prohibited)	211
127.127.88.244	211.174.63.106	ICMP Fragment Reassembly Time Exceeded	61
127.127.153.154	211.233.70.161	ICMP Fragment Reassembly Time Exceeded	60
127.127.153.154	211.233.70.162	ICMP Fragment Reassembly Time Exceeded	40
127.127.88.162	128.208.118.21	ICMP Destination Unreachable (Protocol Unreachable)	26
127.127.150.86	127.127.153.220	ICMP Echo Request Nmap or HPING2	20
127.127.150.200	127.127.153.220	ICMP Echo Request Nmap or HPING2	10
127.127.5.1	127.127.5.92	ICMP Echo Request Cisco Type.x	5
127.127.88.244	211.112.95.120	ICMP Fragment Reassembly Time Exceeded	5
127.127.108.1	127.127.5.92	ICMP Echo Request Cisco Type.x	5
127.127.150.120	12.25.239.5	ICMP Fragment Reassembly Time Exceeded	4
127.127.150.127	127.127.1.3	ICMP Echo Request Windows	4
127.127.150.165	212.188.66.250	ICMP Echo Request Windows	4
127.127.150.165	127.127.150.1	ICMP Echo Request Windows	4
127.127.88.167	207.68.170.122	ICMP Echo Request Windows	3
127.127.88.179	127.127.1.3	ICMP traceroute	3
127.127.88.167	64.4.60.247	ICMP Echo Request Windows	3
127.127.88.167	64.4.32.147	ICMP Echo Request Windows	3
127.127.150.26	127.127.153.220	ICMP Echo Request Nmap or HPING2	2

127.127.150.145	127.127.1.3	ICMP Echo Request Windows	2
127.127.150.121	127.127.1.3	ICMP traceroute	2
127.127.150.112	127.127.153.220	ICMP Echo Request Nmap or HPING2	2
127.127.153.162	62.163.79.16	ICMP Destination Unreachable (Protocol Unreachable)	2

Here is a list of port scans associated with these ICMP messages. Assuming that the BlackBoard application is involved here, the explanation of sending UDP packets to 127.127.1.3 and receiving ICMP Destination Unreachable would make sense.

Source	Destination	Scan type	# of scans
127.127.150.165	127.127.1.3	UDP	685
127.127.153.162	127.127.1.3	UDP	258
127.127.153.154	127.127.1.3	UDP	121
127.127.150.145	127.127.1.3	UDP	95
127.127.88.244	127.127.1.3	UDP	67
127.127.150.121	127.127.1.3	UDP	54
127.127.150.127	127.127.1.3	UDP	30
127.127.150.120	127.127.1.3	UDP	29
127.127.88.167	127.127.1.3	UDP	20
127.127.88.162	127.127.1.3	UDP	12
127.127.150.26	127.127.1.3	UDP	10
127.127.88.179	127.127.1.3	UDP	3

Case: Possible worms

This is a pattern that repeated itself throughout the alerts file. This is a single example. The table below shows the sources and destinations of this pattern as well as how many messages were observed.

This could be “Code Red” as it tries to take over a computer via the Unicode attack and then replaces the cmd.exe, thus re-executing it[6]. This could also be Nimda, but Nimda makes us of TFTP, which hasn’t been detected for these hosts.

date	Time	msecs	src	port	dst	port	msg

[6] http://www.incidents.org/react/code_redII.php

6/1/2002	11:20:49 PM	84481	130.212.18.250	3075	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:49 PM	255543	130.212.18.250	3101	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:49 PM	431692	130.212.18.250	3126	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:49 PM	594803	130.212.18.250	3149	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:49 PM	760134	130.212.18.250	3170	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:49 PM	923594	130.212.18.250	3189	127.127.150.83	80	spp_http_decode: IIS Unicode attack detected
6/1/2002	11:20:49 PM	923594	130.212.18.250	3189	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:50 PM	89341	130.212.18.250	3213	127.127.150.83	80	spp_http_decode: IIS Unicode attack detected
6/1/2002	11:20:50 PM	89341	130.212.18.250	3213	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:50PM	252024	130.212.18.250	3245	127.127.150.83	80	spp_http_decode: IIS Unicode attack detected
6/1/2002	11:20:50 PM	252024	130.212.18.250	3245	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:50 PM	415933	130.212.18.250	3265	127.127.150.83	80	spp_http_decode: IIS Unicode attack detected
6/1/2002	11:20:50 PM	415933	130.212.18.250	3265	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:50 PM	586266	130.212.18.250	3293	127.127.150.83	80	spp_http_decode: IIS Unicode attack detected
6/1/2002	11:20:50 PM	586266	130.212.18.250	3293	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:50 PM	750982	130.212.18.250	3314	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:50 PM	917974	130.212.18.250	3335	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:51 PM	80037	130.212.18.250	3352	127.127.150.83	80	WEB-MISC Attempt to execute cmd
6/1/2002	11:20:51 PM	242056	130.212.18.250	3369	127.127.150.83	80	WEB-MISC Attempt to execute cmd

Source	Destination	# sessions
194.226.220.22	127.127.5.95	32
203.229.98.65	127.127.5.96	19
130.82.102.68	127.127.150.83	19
130.212.18.250	127.127.150.83	19
211.181.253.31	127.127.5.95	16
211.93.8.74	127.127.5.245	15
203.229.99.74	127.127.150.83	15
203.229.99.1	127.127.5.95	13
130.251.80.10	127.127.5.92	13
203.229.99.13	127.127.5.96	12
127.127.153.124	127.127.150.83	4

We might want to check out 127.127.153.124 as it is trying to gain access to 127.127.150.183.

There are no port scans associated with any of these sessions.

Case: IIS Unicode

In looking at the worm above, it was found that there were thousands of reports of the IIS Unicode vulnerability being attempted. Here are the top sessions

Source	Destination	# of IIS Unicode attempts
127.127.153.123	211.32.117.228	193
127.127.153.167	211.233.29.211	155
127.127.153.119	199.244.218.42	129
127.127.150.145	64.12.184.141	84
127.127.153.114	211.115.213.202	80
127.127.153.167	211.233.29.251	67
127.127.153.126	61.78.53.102	59
127.127.153.111	211.32.117.26	56
127.127.153.126	211.32.117.26	49
127.127.153.167	211.32.117.38	47
127.127.153.180	211.115.213.202	42
127.127.153.123	211.32.117.229	41
127.127.153.123	211.233.30.92	39

Note that sorting these by source yields no pattern of scanning external hosts for vulnerabilities. It would be a good precaution to inspect these sources for traces of a worm.

As can be seen in the ports scan section below, the Unicode attacks are the source of 2791 SYN scans associated with the above sessions.

Case: 127.127.5.96 as a target

In viewing the 376 alerts left to explain, 127.127.5.96 seems to occur quite a bit. There seems to be some FrontPage access from a few external hosts as well as most of the SNMP targeting. This may mean that 127.127.5.96 is some sort of nerve center for the blackboard application.

Source	Destination	Alert Message	# Of occurrences

127.127.70.177	127.127.5.96	SNMP public access	475
130.207.92.154	127.127.5.96	WEB-FRONTPAGE _vti_rpc access	4
130.207.92.154	127.127.5.96	WEB-IIS _vti_inf access	4
130.207.92.154	127.127.5.96	WEB-IIS view source via translate header	7
203.229.98.65	127.127.5.96	spp_http_decode: IIS Unicode attack detected	7
203.229.98.65	127.127.5.96	WEB-MISC Attempt to execute cmd	14
203.229.99.13	127.127.5.96	spp_http_decode: IIS Unicode attack detected	6
203.229.99.13	127.127.5.96	WEB-MISC Attempt to execute cmd	8
208.219.64.15	127.127.5.96	WEB-FRONTPAGE _vti_rpc access	2
24.180.201.71	127.127.5.96	WEB-CGI scriptalias access	96
24.3.18.21	127.127.5.96	WEB-IIS _vti_inf access	2

There is also some indication that our worm tried to infect it from 203.229.98.65 and 203.229.99.13.

Performing a Whois on both these addresses reveals them as belonging to NOWCOM ISP in Korea. Here is the contact info:

```
Name                : Hyunho Son
Org Name            : Samyang Data System Co., Ltd
State               : SEOUL
Address             : 263, Yeonji-Dong, Chongno-GU
Zip Code            : 110-725
Phone               : 02-740-7103
Fax                 : 02-740-7098
E-Mail              : shon@samyang.co.kr
```

Note that DShield reported no other activity from these hosts.

The other hosts 130.207.92.154 (sainfortlt.isye.gatech.edu) Belongs to Georgia Institute of technology and the @home addresses are both from Maryland and these could simply be an admin making changes via Frontpage from home or another university.

Case: Napster and GNUtella usage

Here is a table of apparent Gnapster and GNUtella usage

Source	Destination	Alert Message	# of transactions
127.127.151.72	129.46.7.216	INFO Inbound GNUTella Connect accept	1
127.127.151.72	165.91.104.206	INFO Inbound GNUTella Connect accept	1
127.127.151.72	65.69.153.111	INFO Inbound GNUTella Connect accept	1
127.127.152.246	152.22.2.73	INFO Inbound GNUTella Connect accept	1
127.127.152.246	170.140.57.227	INFO Inbound GNUTella Connect accept	1
127.127.152.246	212.150.3.240	INFO Inbound GNUTella Connect accept	1
127.127.152.246	216.199.51.98	INFO Inbound GNUTella Connect accept	1
127.127.152.246	24.20.194.67	INFO Inbound GNUTella Connect accept	1
127.127.152.246	63.145.209.26	INFO Inbound GNUTella Connect accept	1
127.127.153.194	212.194.28.61	INFO Napster Client Data	2
127.127.153.194	213.66.208.205	INFO Napster Client Data	1
213.100.31.9	127.127.152.246	INFO Outbound GNUTella Connect accept	1
61.24.47.103	127.127.152.246	INFO Inbound GNUTella Connect request	1
63.122.74.100	127.127.151.72	INFO Inbound GNUTella Connect request	2
65.14.215.176	127.127.152.246	INFO Inbound GNUTella Connect request	1
80.131.134.56	127.127.152.246	INFO Inbound GNUTella Connect request	1

It can be observed that most of these connections are related to 127.127.152.246 and 127.127.151.72. This is harmless unless it violates a usage policy.

Case: Watchlist alerts

Watchlist alerts are also common. They seem to always originate from the same series of IP addresses.

Source	destination	# of tranfsers
212.179.35.118	127.127.153.148	127
212.179.35.118	127.127.153.162	51

212.179.35.118	127.127.153.178	24
212.179.35.119	127.127.153.148	21
212.179.35.119	127.127.153.162	14
212.179.38.137	127.127.150.220	9
212.179.35.119	127.127.153.178	7
212.179.28.133	127.127.5.97	3

George Bakos[7] and Faud Khan[8] both attribute this to either Gnutella or Napster traffic. These connection come from ISDN.Net from a provider in Israel:

```
inetnum:        212.179.0.0 - 212.179.255.255
netname:        IL-ISDNNET-990517
descr:          PROVIDER
country:        IL
admin-c:        NP469-RIPE
tech-c:         TP1233-RIPE
tech-c:         ZV140-RIPE
tech-c:         ES4966-RIPE
status:         ALLOCATED PA
mnt-by:         RIPE-NCC-HM-MNT
changed:        hostmaster@ripe.net 19990517
changed:        hostmaster@ripe.net 20000406
changed:        hostmaster@ripe.net 20010402
source:         RIPE
route:          212.179.0.0/17
descr:          ISDN Net Ltd.
origin:         AS8551
notify:         hostmaster@isdn.net.il
mnt-by:         AS8551-MNT
changed:        hostmaster@isdn.net.il 19990610
source:         RIPE
person:         Nati Pinko
address:        Bezeq International
address:        40 Hashacham St.
address:        Petach Tikvah  Israel
phone:          +972 3 9257761
e-mail:         hostmaster@isdn.net.il
nic-hdl:        NP469-RIPE
changed:        registrar@ns.il 19990902
source:         RIPE
person:         Tomer Peer
address:        Bezeq International
address:        40 Hashakham St.
address:        Petakh Tiqwah  Israel
phone:          +972 3 9257761
```

[7] http://openbsd.org.br/ouah/George_Bakos.html
[8] http://www.giac.org/practical/Faud_Khan_GCIA.doc

```
e-mail:     hostmaster@isdn.net.il
nic-hdl:    TP1233-RIPE
changed:    registrar@ns.il 19991113
source:     RIPE
person:     Zehavit Vigder
address:    bezeq-international
address:    40 hashacham
address:    petach tikva 49170 Israel
phone:      +972 52 770145
fax-no:     +972 9 8940763
e-mail:     hostmaster@bezeqint.net
nic-hdl:    ZV140-RIPE
changed:    zehavitv@bezeqint.net 20000528
source:     RIPE
person:     Eran Shchori
address:    BEZEQ INTERNATIONAL
address:    40 Hashacham Street
address:    Petach-Tikva 49170 Israel
phone:      +972 3 9257710
fax-no:     +972 3 9257726
e-mail:     hostmaster@bezeqint.net
nic-hdl:    ES4966-RIPE
changed:    registrar@ns.il 20000309
source:     RIPE
```

Case: CGI Null Bytes

There are 24 iterations of this alert.

Src	dst	Msg
127.127.153.171	209.143.193.105	Spp_http_decode: CGI Null Byte attack detected

This alert is repeated between the same host and destination over a shot period of time (minutes). We can assume that there is a CGI on a page that is wrongly configured. Scanning for explanations to this on Google yielded very little information. It doesn't seem to be part of a "global" attack either. The target seems to be a news site (newsstand.enews.com).

Case: Miscellaneous scans

Scans are hefty. Following is a INNER JOIN query that matches the number of port scans associated with the source and destination of alerts in the alerts file.

Matching date, time, source and destination, and then counting duplicates obtained this result. The following are the results.

Message	Scan type	# of Scans
Attempted Sun RPC high port access	UDP	109
Back Orifice	UDP	62
connect to 515 from inside	SYN	787
EXPLOIT NTPDX buffer overflow	UDP	5
FTP passwd attempt	SYN	4
High port 65535 udp - possible Red Worm - traffic	UDP	11334
ICMP Echo Request L3retriever Ping	SYN	3
ICMP Echo Request Nmap or HPING2	SYN	636
Incomplete Packet Fragments Discarded	UDP	2
INFO - ICQ Access	SYN	290
MISC Large UDP Packet	UDP	6113
NMAP TCP ping!	SYN	721
NMAP TCP ping!	UDP	2
NMAP TCP ping!	XMAS	2
Null scan!	NULL	58
Null scan!	SYN	21
Port 55850 udp - Possible myserver activity - ref. 010313-1	UDP	21
SCAN FIN	FIN	6
SCAN XMAS	FULLXMAS	2
SMB Name Wildcard	UDP	15
SNMP public access	SYN	1244
SNMP public access	UDP	1621
spp_http_decode: CGI Null Byte attack detected	SYN	72
spp_http_decode: IIS Unicode attack detected	SYN	2791
SUNRPC highport access!	SYN	636

The following are all the scans reported in the alerts file.

date	time	Src	dst	dstport	msg
7/1/2002	8:19:30 AM	144.122.42.38	127.127.88.162	1214	Null scan!
7/1/2002	2:27:35 AM	144.122.42.38	127.127.88.162	1214	Null scan!
7/1/2002	5:22:33 AM	144.122.42.38	127.127.88.162	4915	SCAN XMAS
7/1/2002	4:14:55 PM	144.122.42.38	127.127.88.162	1214	SYN-FIN scan!
7/1/2002	9:57:45 PM	144.122.42.38	127.127.88.162	1214	Null scan!
7/1/2002	9:58:18 PM	144.122.42.38	127.127.88.162	1214	SCAN FIN
7/1/2002	10:55:36 PM	144.122.42.38	127.127.88.162	1214	Null scan!
7/1/2002	4:58:38 AM	144.122.42.38	127.127.88.162	1214	Null scan!
6/1/2002	7:19:22 AM	195.132.240.41	127.127.88.162	1214	SCAN FIN
6/1/2002	6:54:35 AM	195.132.240.41	127.127.88.162	1214	Null scan!
6/1/2002	4:30:11 AM	195.132.240.41	127.127.88.162	1214	SCAN FIN
5/1/2002	11:39:18 AM	195.132.240.41	127.127.88.162	1214	Null scan!
5/1/2002	4:53:20 AM	195.132.240.41	127.127.88.162	1214	Null scan!
6/1/2002	4:36:19 PM	213.109.148.190	127.127.150.220	44416	Null scan!
7/1/2002	3:31:31 PM	213.153.216.138	127.127.150.220	14008	Null scan!
6/1/2002	2:49:50 PM	213.40.13.41	127.127.150.220	26467	Null scan!
5/1/2002	2:34:55 PM	216.152.64.142	127.127.153.148	1080	SCAN Proxy attempt
5/1/2002	2:34:54 PM	216.152.64.142	127.127.153.148	1080	SCAN Proxy attempt
6/1/2002	5:04:25 PM	216.152.64.142	127.127.153.114	1080	SCAN Proxy attempt
6/1/2002	5:04:24 PM	216.152.64.142	127.127.153.114	1080	SCAN Proxy attempt
6/1/2002	5:04:24 PM	216.152.64.142	127.127.153.114	1080	SCAN Proxy attempt
6/1/2002	5:04:23 PM	216.152.64.142	127.127.153.114	1080	SCAN Proxy attempt
5/1/2002	2:34:55 PM	216.152.64.142	127.127.153.148	1080	SCAN Proxy attempt
5/1/2002	3:06:34 PM	216.152.64.142	127.127.153.148	1080	SCAN Proxy attempt

5/1/2002	3:06:35 PM	216.152.64.142	127.127.153.148	1080	SCAN Proxy attempt
6/1/2002	11:13:14 AM	216.152.64.142	127.127.88.181	1080	SCAN Proxy attempt
5/1/2002	2:34:56 PM	216.152.64.142	127.127.153.148	1080	SCAN Proxy attempt
5/1/2002	3:06:35 PM	216.152.64.142	127.127.153.148	1080	SCAN Proxy attempt
5/1/2002	3:06:36 PM	216.152.64.142	127.127.153.148	1080	SCAN Proxy attempt
6/1/2002	11:13:14 AM	216.152.64.142	127.127.88.181	1080	SCAN Proxy attempt
6/1/2002	11:13:13 AM	216.152.64.142	127.127.88.181	1080	SCAN Proxy attempt
6/1/2002	11:13:13 AM	216.152.64.142	127.127.88.181	1080	SCAN Proxy attempt
5/1/2002	1:26:15 AM	216.152.64.150	127.127.153.123	1080	SCAN Proxy attempt
7/1/2002	11:42:17 PM	216.152.64.150	127.127.88.181	1080	SCAN Proxy attempt
7/1/2002	7:36:44 AM	216.152.64.150	127.127.153.178	1080	SCAN Proxy attempt
7/1/2002	11:42:17 PM	216.152.64.150	127.127.88.181	1080	SCAN Proxy attempt
7/1/2002	7:36:44 AM	216.152.64.150	127.127.153.178	1080	SCAN Proxy attempt
7/1/2002	9:23:04 AM	216.152.64.151	127.127.153.162	1080	SCAN Proxy attempt
7/1/2002	9:23:04 AM	216.152.64.151	127.127.153.162	1080	SCAN Proxy attempt
7/1/2002	10:39:39 AM	216.152.64.151	127.127.150.103	1080	SCAN Proxy attempt
7/1/2002	10:29:21 AM	216.152.64.151	127.127.153.111	1080	SCAN Proxy attempt
7/1/2002	10:01:53 AM	216.152.64.151	127.127.153.117	1080	SCAN Proxy attempt
7/1/2002	10:01:53 AM	216.152.64.151	127.127.153.117	1080	SCAN Proxy attempt
7/1/2002	10:29:21 AM	216.152.64.151	127.127.153.111	1080	SCAN Proxy attempt
7/1/2002	10:39:39 AM	216.152.64.151	127.127.150.103	1080	SCAN Proxy attempt
5/1/2002	12:55:36 PM	216.152.64.163	127.127.153.127	3128	INFO - Possible Squid Scan
5/1/2002	12:55:36 PM	216.152.64.163	127.127.153.127	1080	SCAN Proxy attempt
5/1/2002	12:55:36 PM	216.152.64.163	127.127.153.127	8080	SCAN Proxy attempt
6/1/2002	5:59:53 PM	216.152.64.163	127.127.153.111	1080	SCAN Proxy attempt

6/1/2002	5:59:53 PM	216.152.64.163	127.127.153.111	3128	INFO - Possible Squid Scan
5/1/2002	3:06:29 PM	216.152.64.163	127.127.153.148	8080	SCAN Proxy attempt
6/1/2002	6:01:46 PM	216.152.64.163	127.127.150.103	1080	SCAN Proxy attempt
6/1/2002	6:01:46 PM	216.152.64.163	127.127.150.103	3128	INFO - Possible Squid Scan
6/1/2002	6:01:46 PM	216.152.64.163	127.127.150.103	8080	SCAN Proxy attempt
6/1/2002	5:59:53 PM	216.152.64.163	127.127.153.111	8080	SCAN Proxy attempt
7/1/2002	8:37:11 PM	216.152.64.163	127.127.153.162	3128	INFO - Possible Squid Scan
5/1/2002	4:19:23 PM	216.152.64.163	127.127.153.178	1080	SCAN Proxy attempt
5/1/2002	2:34:50 PM	216.152.64.163	127.127.153.148	8080	SCAN Proxy attempt
7/1/2002	7:50:20 PM	216.152.64.163	127.127.153.178	8080	SCAN Proxy attempt
5/1/2002	2:34:50 PM	216.152.64.163	127.127.153.148	1080	SCAN Proxy attempt
5/1/2002	4:19:23 PM	216.152.64.163	127.127.153.178	3128	INFO - Possible Squid Scan
7/1/2002	7:50:20 PM	216.152.64.163	127.127.153.178	3128	INFO - Possible Squid Scan
5/1/2002	4:19:23 PM	216.152.64.163	127.127.153.178	8080	SCAN Proxy attempt
7/1/2002	8:37:11 PM	216.152.64.163	127.127.153.162	1080	SCAN Proxy attempt
7/1/2002	8:37:11 PM	216.152.64.163	127.127.153.162	8080	SCAN Proxy attempt
5/1/2002	2:30:19 PM	216.152.64.163	127.127.153.162	1080	SCAN Proxy attempt
5/1/2002	2:30:19 PM	216.152.64.163	127.127.153.162	3128	INFO - Possible Squid Scan
5/1/2002	2:30:19 PM	216.152.64.163	127.127.153.162	8080	SCAN Proxy attempt
5/1/2002	3:06:29 PM	216.152.64.163	127.127.153.148	1080	SCAN Proxy attempt
5/1/2002	3:06:29 PM	216.152.64.163	127.127.153.148	3128	INFO - Possible Squid Scan
5/1/2002	2:34:50 PM	216.152.64.163	127.127.153.148	3128	INFO - Possible Squid Scan
7/1/2002	7:50:20 PM	216.152.64.163	127.127.153.178	1080	SCAN Proxy attempt
6/1/2002	8:57:34 AM	216.152.64.62	127.127.153.162	1080	SCAN Proxy attempt
7/1/2002	7:02:06 AM	216.152.64.62	127.127.153.162	1080	SCAN Proxy attempt

7/1/2002	7:02:06 AM	216.152.64.62	127.127.153.162	1080	SCAN Proxy attempt
6/1/2002	9:16:29 AM	216.152.64.62	127.127.153.162	1080	SCAN Proxy attempt
6/1/2002	8:57:34 AM	216.152.64.62	127.127.153.162	1080	SCAN Proxy attempt
7/1/2002	10:57:07 AM	216.152.64.62	127.127.153.114	1080	SCAN Proxy attempt
7/1/2002	10:57:08 AM	216.152.64.62	127.127.153.114	1080	SCAN Proxy attempt
6/1/2002	9:16:28 AM	216.152.64.62	127.127.153.162	1080	SCAN Proxy attempt
4/1/2002	9:47:58 PM	217.225.192.163	127.127.88.162	1214	Null scan!
4/1/2002	5:23:40 PM	24.33.22.66	127.127.150.209	3791	Null scan!
6/1/2002	11:42:36 PM	62.131.53.136	127.127.151.18	0	Null scan!
6/1/2002	11:42:36 PM	62.131.53.136	127.127.151.18	0	Null scan!
6/1/2002	11:42:39 PM	62.131.53.136	127.127.151.18	0	Null scan!
6/1/2002	11:42:44 PM	62.131.53.136	127.127.151.18	0	Null scan!
6/1/2002	11:42:55 PM	62.131.53.136	127.127.151.18	0	Null scan!
6/1/2002	11:43:58 PM	62.131.53.136	127.127.151.18	0	Null scan!
6/1/2002	11:43:16 PM	62.131.53.136	127.127.151.18	0	Null scan!
7/1/2002	3:01:42 PM	62.59.157.134	127.127.150.220	12525	Null scan!
4/1/2002	9:21:13 PM	63.156.236.132	127.127.150.220	27744	Null scan!
6/1/2002	4:27:11 PM	63.156.48.139	127.127.150.220	41132	Null scan!
4/1/2002	5:22:44 PM	65.129.20.180	127.127.88.162	54722	Null scan!
4/1/2002	5:23:01 PM	65.129.20.248	127.127.88.162	2137	Null scan!
7/1/2002	3:27:45 PM	65.129.22.146	127.127.150.220	60997	Null scan!
6/1/2002	8:14:32 PM	65.129.58.130	127.127.88.162	11690	Null scan!
6/1/2002	10:01:29 AM	65.149.200.147	127.127.150.220	22849	Null scan!

Notice that most of the above are in some way related to the 216.152.64.X subnet. This block of IP addresses comes from webchat.org. In fact, one of them is called arena.webchat.org and the

other proxy-check.webchat.org. This would explain these scans as being proxy checks from webchat.org. The 144.122.142.48 address belongs to Middle East Technical University in Ankara, Turkey, with host name 1207.odtukent.metu.edu.tr. This last host is responsible for most of the Out-of-spec packets as well. This points to an intentional scan and more attention to this host in the future.

A bunch of the other scans come from 65.129.X.X and 62.131.53.X are addresses in Philedelphia with the common host name of philadelphia1.pa.us.da.qwest.net.

Note that the following alerts correlate to the sources in the out-of-spec log

date	time	msecs	src	srcport	dst	dstport	msg
5/1/2002	4:53:20 AM	7070	195.132.240.41	1071	127.127.88.162	1214	Null scan!
5/1/2002	4:53:20 AM	7070	195.132.240.41	1071	127.127.88.162	1214	Null scan!
5/1/2002	11:39:18 AM	922066	195.132.240.41	2137	127.127.88.162	1214	Null scan!
5/1/2002	11:39:18 AM	922066	195.132.240.41	2137	127.127.88.162	1214	Null scan!
6/1/2002	4:30:11 AM	457812	195.132.240.41	1127	127.127.88.162	1214	SCAN FIN
6/1/2002	4:30:11 AM	457812	195.132.240.41	1127	127.127.88.162	1214	SCAN FIN
6/1/2002	6:54:35 AM	215474	195.132.240.41	1618	127.127.88.162	1214	Null scan!
6/1/2002	6:54:35 AM	215474	195.132.240.41	1618	127.127.88.162	1214	Null scan!
6/1/2002	7:19:22 AM	486125	195.132.240.41	1690	127.127.88.162	1214	SCAN FIN
6/1/2002	7:19:22 AM	486125	195.132.240.41	1690	127.127.88.162	1214	SCAN FIN
7/1/2002	2:27:35 AM	195547	144.122.42.38	2972	127.127.88.162	1214	Null scan!
7/1/2002	2:27:35 AM	195547	144.122.42.38	2972	127.127.88.162	1214	Null scan!
7/1/2002	4:58:38 AM	18264	144.122.42.38	4719	127.127.88.162	1214	Null scan!
7/1/2002	4:58:38 AM	18264	144.122.42.38	4719	127.127.88.162	1214	Null scan!
7/1/2002	5:22:33 AM	673383	144.122.42.38	0	127.127.88.162	4915	SCAN XMAS
7/1/2002	5:22:33 AM	673383	144.122.42.38	0	127.127.88.162	4915	SCAN XMAS
7/1/2002	8:19:30 AM	181593	144.122.42.38	3167	127.127.88.162	1214	Null scan!
7/1/2002	8:19:30 AM	181593	144.122.42.38	3167	127.127.88.162	1214	Null scan!
7/1/2002	4:14:55 PM	701263	144.122.42.38	2718	127.127.88.162	1214	SYN-FIN scan!

7/1/2002	9:57:45 PM	674718	144.122.42.38	2106	127.127.88.162	1214	Null scan!
7/1/2002	9:57:45 PM	674718	144.122.42.38	2106	127.127.88.162	1214	Null scan!
7/1/2002	9:58:18 PM	882579	144.122.42.38	2106	127.127.88.162	1214	SCAN FIN
7/1/2002	9:58:18 PM	882579	144.122.42.38	2106	127.127.88.162	1214	SCAN FIN
7/1/2002	10:55:36 PM	585673	144.122.42.38	2775	127.127.88.162	1214	Null scan!
7/1/2002	10:55:36 PM	585673	144.122.42.38	2775	127.127.88.162	1214	Null scan!

Looks like the majority of the out-of-spec notices were due to some stealth scans from these addresses.

Case: Out of Spec and Fragment Alerts

date	Time	msecs	src	port	dst	port	msg
7/1/2002	4:42:20PM	207991	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	4:42:22PM	83531	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	4:42:32PM	452031	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	4:42:33PM	545752	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	4:42:39PM	75299	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	5:17:46PM	199677	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	5:17:49PM	270111	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	5:17:53PM	815149	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	5:17:54PM	206058	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	5:18:11PM	915587	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	5:18:18PM	552393	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded
7/1/2002	5:18:24PM	314796	202.102.29.141	0	127.127.150.143	0	Incomplete Packet Fragments Discarded

The above comes from the alerts log. These incomplete fragment packets seem to original from 202.102.29.141. This IP address is also responsible for a lot of the MISC UDP packets and therefore it can be assumed that these are errors associated with broadcasting UDP packets over

the multicast application. No scans are associated with this source file.