# Global Information Assurance Certification Paper

# GIAC Certified Intrusion Analyst (GCIA)

Practical Assignment
Version 3.5

Frank Birkmair

Submitted: October 6, 2004





© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Summary:

This paper contains my SANS Certified Intrusion Analyst (GCIA) practical assignment submission.
The paper is splitted in 3 independent parts.
The first part includes a Design from Enterprise IDS Architecture.
Three practical network detect are the second part. The last part is an analysis from NIDS files from the University of Maryland Baltimore with an execute summary and improvement suggestions.

Table of Contents:

## PART 1

**Question:**

An executive summary of the enterprise network you are designing. Within this summary describe the challenges you face which you will deliver upon within your assignment. For example: Is there a central office with multiple small satellite offices that are all being monitored with network IDS? Are there several large offices across the world, all with many isolated subnets that are being monitored? Is there a single enterprise at a single location, but with multiple points of presence?

**Answer:**

To increase the security in our environment I decided to install the Proventia IPS (Intrusion Prevention System) network sensors from ISS. The biggest improvements through these devices for the company are:

1) Instead of only Detection with IDS network sensors, the IPS sensors can react against malicious traffic with possible dynamic blocking.
2) It is a tool that helps to save time in the installation and update phases.
3) It is possible to install a huge number of sensors and manage them all with one centralized management system called SiteProtector.
4) With this centralized management system, it is also possible to manage Server and Desktop Sensors (HIDS) if required in the future.

IPS is not a replacement for a firewall however IPS enhances security on the application layer.

*The biggest challenges in my assignment were:*

1) To get service downtimes to work on the IPS sensors. The IPS is placed in aggregation points of all traffic streams (It works as a Layer two bridge). Therefore every change, testing, update, etc, affects the whole network. In a HIGH availability environment, getting downtimes is quite challenging.
2) To convince the network team to enable the blocking mode is another challenge. Their concern is that it could affect the regular traffic by false positives and disable business traffic.
3) At the start of the Project, the ISS Proventia G appliance was not capable of working properly in a Cisco HSRP HIGH Availability Environment. It was hard work together with ISS Developers to implement our requirement in the product.
   (E.g. If the Proventia G appliance is located between two routers which use static routes (in our network this is the case towards our redundantly attached ISP routers in the here not described e-commerce environment because of the paper size limit) a one side link down resulted in black hole routes because the physical link on the other side was not taken down and the router still "saw" and active interface and forwarded packets through it which then where dropped on the G appliance. I provided test details to ISS and they integrated a new patch for this problem. I already tested the

patch and will roll it out in our environment shortly). Now the Proventia G runs smoothly in the HSRP/static route environment.

4) For the fine-tuning of the detection policy and response policy, it is necessary to know which devices have which functions and who is responsible. At the start of this project, there was no asset inventory available in the company and to find out all this necessary information delayed the project over 2 months.
5) Although it was obvious from the beginning, I needed to prove that the Proventia G100 is not interfering with the normal traffic flows in many time consuming tests (including reporting etc).

**Question:**

What network and/or host IDS (NIDS/HIDS) are being used to monitor your networks and assets? Any IDS is acceptable, and more common ones would include Snort, ISS RealSecure(R), Cisco Secure IDS, Cisco Secure Agent, McAfee Entercept, Sourcefire, etc. Describe the model, speed (100Mb or Gigabit), memory, disk size, agent software specifics etc. Be specific including management options.

**Answer:**

I decided to go the inline way and use an IPS solution (Intrusion Prevention System) as network IDS to monitor and protect the network. For the placement and number of sensors, please refer to the attached network diagram.
I decided to go with the ISS Proventia G Series 100. The Proventia G model can be operated in 3 different ways:
a) In passive monitoring position as “classical IDS with a tape or on a mirror port from a switch for example.
b) Inline in “inline simulation mode”.
c) Inline in “inline protection mode”.
The difference between simulation and protection mode is that the sensor reports in simulation mode only if an “evil” packet would be blocked. In protection mode these packets becomes blocked. Which kind of packet or event becomes blocked is adjustable in the policy. I would everybody recommend to start with the simulation mode. In normal cases should everybody after 4-6 weeks fine tuning able to get a policy which can be switched to the protection mode.

*Datasheet Proventia G 100 IPS Box:*

Most of the information I found in the /var/log/dmesg and the /var/log/boot.log files by logging in with SSH to a Proventia sensor.

1) It is an appliance box based on Red Hat Linux 8.0.
   The Kernel is based on 2.4.18 and modified by ISS.
   The operating system can be easily self-installed/updated with the CD Image provided by ISS in less than 10 minutes.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

If an NTP Service is desired, it is necessary to modify the default installation and modify the running iptables firewall on the Proventia. Information can be found in the knowledge base on the ISS web site: https://iss.custhelp.com/cgi-bin/iss.cfg/php/enduser/std_alp.php

2) The sensors are powered by 2 Intel(R) Xeon(TM) CPU 2.40GHz stepping 05 MHz processors.
3) A Proventia G100 fits in a 19'' rack and has the height of 1 U.
4) It has 4 Interfaces:
   One for inbound and one for the outbound traffic (10/100 Mbps Copper). Both of these interfaces work together as a layer 2 bridge to provide the IDS/IPS function.
   The third interface is for the management (10/100 Mbps Copper).The fourth is for the case that the Proventia is used as classic IDS sensor.
5) With this interface it is possible to connect the appliance to the network and send reset packets (RSKill) as response for events.
6) One serial port is also available. Can be used as out of band management.
7) For installation or upgrade a SAMSUNG CD-ROM SN-124, ATAPI CD/DVD-ROM drive has been built in.
8) It has redundant internal cooling fans.
9) An IDE Floppy drive with 1.44M is included.
10) 1 GB RAM memory is available.
    It works internally with 16 RAM disks of 4096KB size and 1024 block size
11) One RAID-1 SCSI device with a 40 GB storage capacity.
12) The File system used is EXT3.
13) ISS guarantees 100 Mbps throughput detection.
14) The throughput is limited via the G100 software license.
15) The integrated fail-open bypass which ensures the traffic continuity is very important in the case of power loss or system instability. This is realized through a mechanical relay.
16) The Proventia has additionally a Video and a Keyboard plug.

Under
http://www.iss.net/products_services/enterprise_protection/proventia/g_series.php
it is always possible to find the newest Information about the different models/sizes of the Proventia G series.

*Datasheet of the Management Platform SiteProtector:*

For the Proventia box a management platform is necessary. It is called SiteProtector. It is possible to install all required software components on one server or split the installation to several servers. The software is free of charge. The important functions of SiteProtector are to handle updates, policies, responses, alerts (reactions) and license management for the IPS sensors. With the SiteProtector it is also possible to manage Host IDS. ISS offers several HIDS software (Server Sensor, Real Desktop Protection). But this software was not part of my Installation.

Here I describe the Hardware/Software that I have selected and which is required to install the SiteProtector on one server:

The management software SiteProtector requires Microsoft Windows as operation system. It is possible to use Windows 2000 Server, Adv. Server or Windows 2003. I decided to use Windows 2003.

*SiteProtector requires following Third-Party Software*:

- Microsoft Data Access component MDAC 2.8 or later,
- Microsoft SQL Server 2000 or Enterprise Version,
- Sun Java 2 Runtime Environment (JRE) 1.4.1 Standard Edition,
- Internet Explore 6.0 or later,
- Adobe Acrobat Reader 5.0 or later.

The SiteProtector Software can be downloaded from the ISS web site (the URL is: http://www.iss.net/download/) or taken from CD's delivered by ISS.

Here I do not describe the Installation Process, because there is a paper size limit for the Practical which I would exceed only with the installation procedure.

The minimum recommended hardware by ISS for a basis installation is 1 GHz Intel Pentium III with 1 GB RAM and 30 GB HD. With this hardware it is possible to manage 5 Proventia G 100 sensors and ~1000 events per day.
The updated recommended hardware is always online available from ISS.

*I used for my installation:*

-1 HP ProLiant DL 380 Server,
    This server has redundant power supplies.
-2x Intel(R) Xeon(TM) CPU 2.8 GHz Processor,
-4 GB RAM
    For me it was a very good fitting calculation for the RAM:
    For every 10 GB Data on the Hard drive which should be processed by the SQL Server I would recommend to take 1 GB RAM. Below this value, the application becomes very slow!
-2 BCM5703 Gigabit Ethernet Network Cards.
    The first Card is only responsible for the communication with the Proventia sensors, the second is used for administration (Console-GUI,….).
-4 Hard Disks with 73 GB capacity, configured as 2 x RAID-1
    The Disk Space can be calculated with the following formula:
    (Assumption to maintain 30 days of event data)
    For about 1000 events per day there are 45 MB free space necessary.

    Following partitions were installed on the Hard drive.
    Hard Drive 1:

a) 15 GB for the Operation System and the SiteProtector Software
b) 58 GB for the transaction logs of the Microsoft SQL Server (Should be always on another Partition as the SQL Database logs)

Hard Drive 2:
Only 1 Partition with 73 GB for the SQL Database table space.

For backup purposes I installed an additional tape drive from Iomega.

**Question:**
A detailed network diagram of your architecture. This could be a single network diagram, or one for each remote office being monitored and one for the corporate office. List pipe sizes, IP addresses of key devices (sanitized for the purposes of the assignment), stealthed interfaces or network taps if used, etc. Again, be specific.

You may use a network diagram and design from previously posted GIAC GCFW **honors** practicals (http://www.giac.org/GCFW.php) as a basis for your enterprise network architecture. This will place less focus on designing a network from the ground up to actually covering what were looking for in this practical assignment. In reality very few IDS solutions are architected into a network design within version 1.0 anyway; IDS is almost always an addition to an existing architecture determined by the organization and their networks maturity. If you do use a GCFW honors practical as a basis for you network design, be sure and list the practical used, including a hyperlink to it.

**Answer:**
I take the possibility to use one of the previously posted GIAC GCFW honors practical from http://www.giac.org/GCFW.php as a basis for my enterprise IDS architecture. I used the practical http://www.giac.org/practical/Emily_Gladstone_GCFW.zip.
I decided to use this one, because it was very similar to what I had in real life in my company for my IDS/IPS rollout. I changed only a few devices on the template so that they fit to my real world environment.

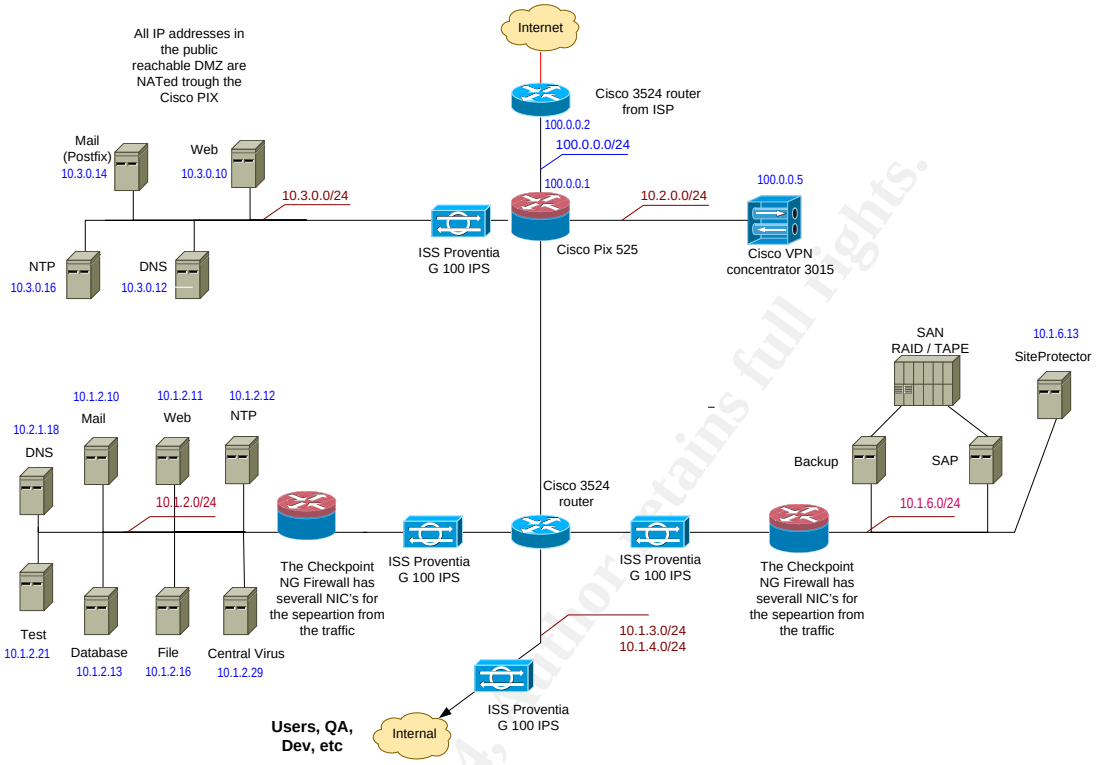
*Short Note to the used devices/software and the size of the pipes:*

- Both internal used firewalls are Checkpoint NG firewalls with FP3 on a Windows Platform. We renounce to upgrade to AI (Application Intelligence) because of financial aspects and through the fact that behind every firewall there is a Proventia IPS.
- The 3 ISS Proventia which are connected to the internal Cisco 3640 router could be substituted with one big Proventia G1200. This model has 8 interfaces and is useful if someone has so many internal DMZ's. But it was too expensive for us.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- The external connection is a 100 MBit/s Line.
- All internal connections have as well a throughput of 100 MBit/s.
- The network is only using TCP/IP protocols (No IPX).




**Question:**

How will sensors and/or consoles be managed both locally and remotely?

**Answer:**

The Management Server SiteProtector is the heart of the whole IDS/IPS System and therefore this server needs a higher protection. Therefore it should be physically located in a Data Center.
In a Data Center is it easier to take measures to protect this computer. A few examples are:

a) Physical Access Controls to come in this room with log entries
b) UPS in case of emergency for permanent energy provision
c) Video surveillance on the entrance
d) Air Conditioned rooms

Administrators should be the only ones who have a login for the Operating System and for the SQL Database. Other Users only have the possibility to access the management Platform SiteProtector remotely via Console GUI or with a browser. Additionally, “normal” users have no Terminal Server access to the server!

There are a few conditions to connect remotely to the SiteProtector:

a) The IP address of the computer which will connect to the SiteProtector must be in the allowed group on the Firewall in front of the SiteProtector.
b) An RSA SecurID Token is necessary to connect through the Firewall to the SiteProtector (Proxy Authentication). Therefore every connection can be logged.

Almost all work on the Management Server and the sensors is done remotely.
A few additional reasons are:

a) The sensors are wide spread in different countries, locations and rooms.
b) Only a few people have the training to manage these complicated systems and they are all located on one location.

The authorization permissions are defined in 3 different roles:
RSSP-Operator (Nearly a view only role with remote access)
RSSP-Analyst (For the daily doing with only remote access)
RSSP-Administrator (Can do all remote and locally)
The exact rights for every role can be defined in the file
*C:\Program Files\ISS\Real Secure SiteProtector\Application Server\config\security.xml*
This is the default location of this File during Installation.

<u>The Proventia sensors itself are managed totally trough the SiteProtector over the TCP Port 2998.</u>

The Proventia sensors can be independently accessed in two different ways.

a) remotely via SSH (OpenSSH)
b) locally via serial port.

Local access to a Proventia is only necessary one time, during the initial installation from the sensor.
This is done over the Serial port using a generic terminal program, like for example Hyper Terminal or Terra Term on a Windows Operating System.

Whereas the Administrator must use the CD provided from ISS and type in a few entries. For example (IP address of the management interface, the IP address of the SiteProtector server, name of the sensor, etc,….).
The setup Process duration takes round about 10 minutes.
If you want the Proventia to have its time synchronized with a NTP Service, this can easily be done after the installation, or is also possible later via a remote session. For remote offices is it so possible to pre-configure all necessary settings so that the local people only must plug in the network cables and press the power button.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Normally it is not necessary to remotely login directly to a Proventia sensor. All further settings, updates are done only from the SiteProtector. I personally needed the SSH access only in a few very rare cases for special debugging.

**Question:**
Is there out of band management?

**Answer:**
No. An own out of the band management network with own switches or routers is too expensive. It would be necessary to go such a step if the communication between the devices could not be encrypted. But the Proventia has two own dedicated Management Interfaces, which I use. Additionally, the access to the sensors and the management Station SiteProtector is limited trough Access Lists on the Router/Switches and the Firewall.

**Question:**
How are configuration updates to remote sensors pushed out?

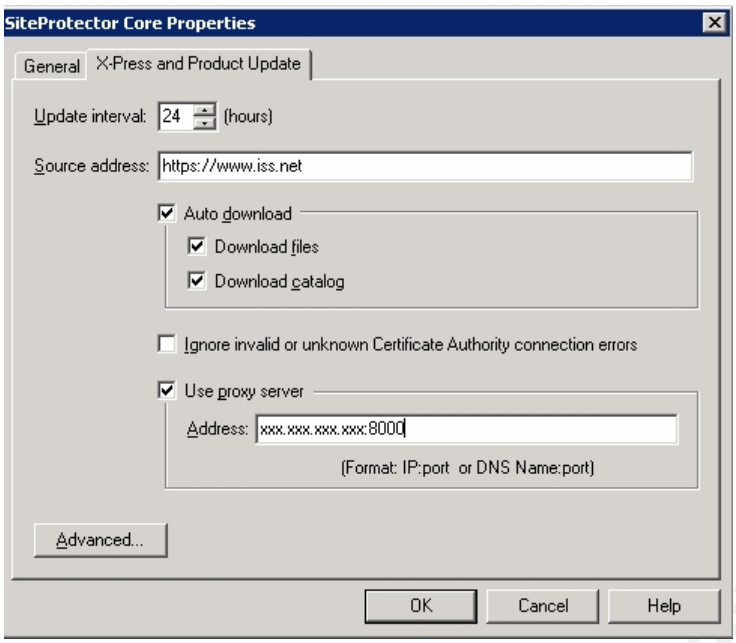
**Answer:**
All necessary things are pushed to the Proventia sensors from the SiteProtector over an encrypted channel.
That includes:

a) New Policies (that defines, what the sensor should look for) That's similar to the snort.config file on SNORT IDS.
b) Response Policy (that defines, how the Proventia should react if an event occurs and a notification or reaction is wished).
c) Upgrades of Signatures. They are called X-Press Update (XPU) by ISS.
d) Product Upgrades (Similar like Service Packs from Microsoft. That sometimes includes fixes and sometimes new features or both).

In the SiteProtector it is possible to adjust how often the software should look for updates on the ISS web side https://www.iss.net/ . In my installation I have configured one time in 24 hours (See Picture).




© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



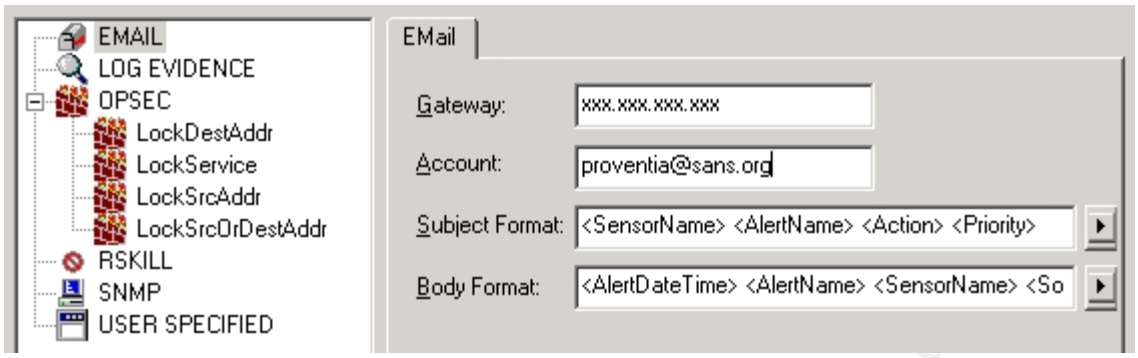

Additionally, it is necessary to decide if updates are available and if they should be pushed automatically to the sensors or if you want only to get a notification of update availability. I recommend for the first weeks to do it manually to investigate how the network traffic reacts. If an update is pushed to the sensor the sensors gets a kind of a HUP (Hang up Process Signal) and reads the config new. In this time frame all network traffic is queued in a buffer and a minimal delay in the transport of the packets occurs. See for a more detailed description including test script and construction to the Appendix.
Every kind of update is tunable for every sensor separately. For detection policies and response polices it is the same. It is possible to enable this via scheduler or manually.

**Question:**
How are alerts updated/created/deleted?

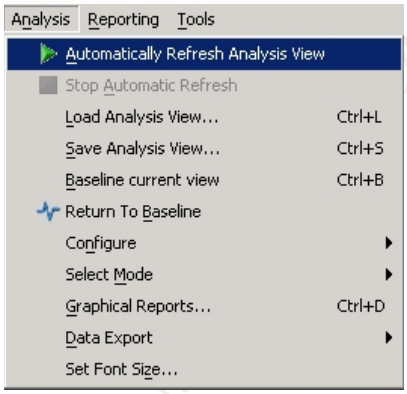
**Answer:**
On a Proventia it is possible with a policy to adjust which event (attack) the sensor should search in the data stream with different methods. If one of these events occurs, the Proventia has the possibility to create different kinds of alerts (See Picture).



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



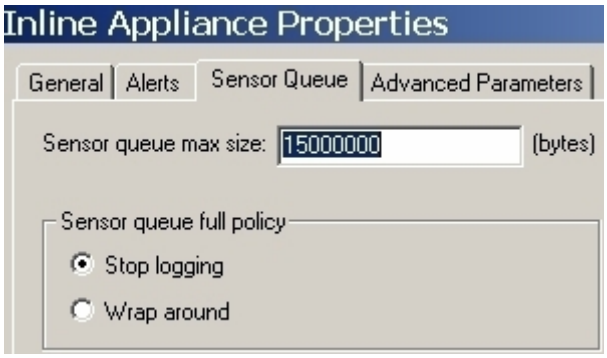

1) The sensor can send a snmp trap.
2) It is possible to send a mail notification for every event. For this mail a Relay Server is necessary.
3) A message can be sent to the SiteProtector and then displayed in the Console-GUI (If the Console-GUI is open).
4) For a better overview the functions „*Baseline Current View*“ and „*Automatically Refresh Analysis View”* exist. This means that the Administrator can build up a picture of events what he wants to see and this view will be refreshed every 60 seconds and a difference to the past view will be displayed. As well it is possible to refresh this with the F5 key manually. All events will be saved additionally in the SQL Database. This happens also if the Proventia blocks bad traffic (See Picture).




The Proventia itself never connects to the Event Collector. The Event Collector (As in my Installation on the SiteProtector machine) opens a connection to the sensors. This must be taken into consideration on rule sets of stateful firewalls. After this, the attacks will immediately be recognized by the sensor over the Event Collector. It sends to the SiteProtector Database. Only if the connection is discontinued or the Event collector gets too many messages and can not handle it, then events are locally saved in the buffer „sensorqueue.adf“ of the Proventia until the connection comes back.
The size of the buffer and the behavior if the buffer becomes full can be configured on the SiteProtector and does not affect the blocking or recognizing from new traffic (See picture).



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.




5) The Proventia can make extra changes over the OPSEC interface to a Checkpoint Firewall in the firewall rule set. This will be reported (if enabled) in the Checkpoint Logs.

6) In the Console, uninteresting events can be marked as “cleared” and later deleted by stored procedures in the SQL database.
ISS offers for free a lot of different SQL stored procedures for hardening, reconnaissance and for management.

**Question:**
Include sequence diagrams and data flow diagrams to better explain the path of traffic, alerts and logs throughout your IDS architecture.

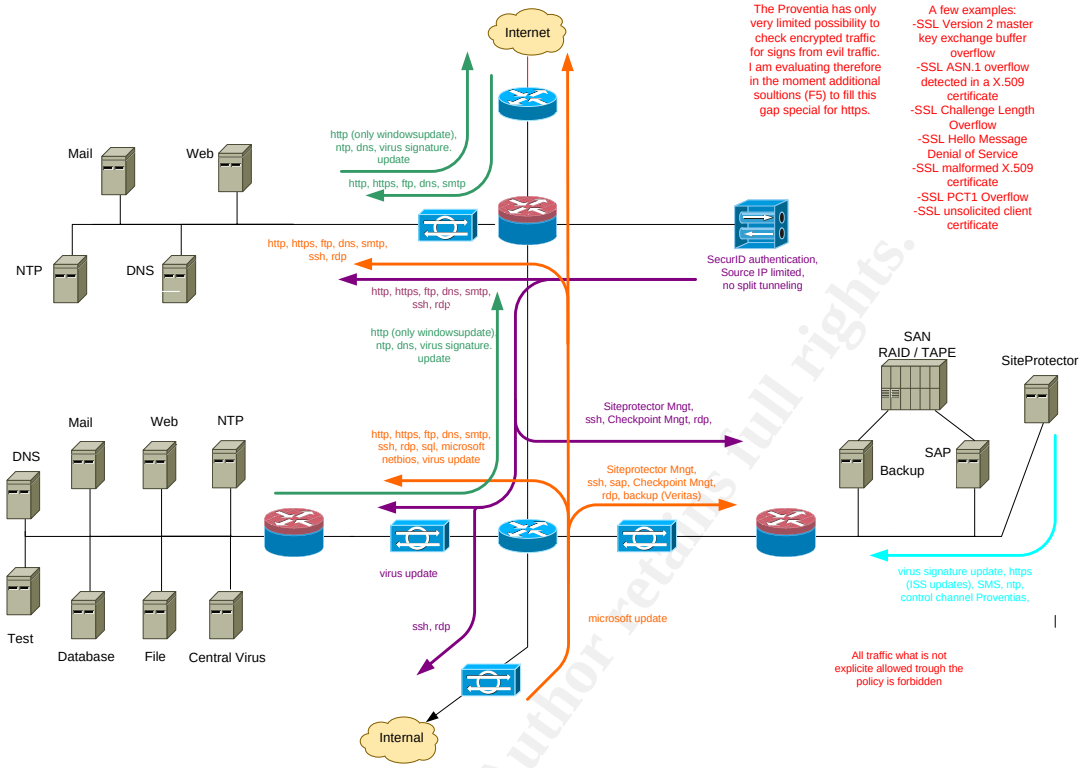
**Answer:**
Sequence Diagram (For one Proventia):

1. The Proventia detects “evil” traffic. In the policy on every sensor is defined how the Proventia should react (pass, alert, drop with RST packet or without,….). The Proventia react stand alone without communication to other devices. The Proventia controls the traffic in both directions.
2. The Proventia can send several different types of alerts (mail, snap, own defined reaction,….) after detecting from “evil” traffic and reaction (If enabled in the Response Policy).
3. Additional (if enabled) becomes the events transferred to the SiteProtector Database or Console-GUI (or both). SiteProtector starts always the communication. One event has without raw packets round about 2 Kb. With enabled raw packets increases this value to a much higher value. If the connection between the SiteProtector and the Proventia is trough any reason broken stores the Proventia the events in their internal buffer and waits until the connection is alive again.




© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The traffic flow diagram is based on the Network diagram.




**Question:**

Describe/discuss the use of network taps if they are to be employed, including these devices in your network diagram.

**Answer:**

I used an Intrusion Prevention System (IPS). This works in Layer two bridge mode and therefore I did not need network taps.

**Question:**

Describe how alerts will be collected, analyzed and stored both locally at remote sites and centrally at one or more consolation points.

**Answer:**

All alerts from the sensors will be collected at one central point by a software component called Event Collector. Here the alerts are processed and sent to the SQL Database. In my Installation this Event Collector is running on the same machine where the SQL Database and the other SiteProtector components are installed. One Event Collector can handle 10 Proventia IPS sensors. If you have more then 10, you can install additional Event Collectors on separate machines as required. These Event Collectors can now send their events to the main SQL Database or to several independent working SQL Databases. In an ISP

scenario, events can also be pushed from one Event Collector to two different SiteProtectors simultaneously.

**Question:**
Are they sysloged, SCPd, FTPd, etc?

**Answer:**
The logs are transported via an ISS proprietary mechanism. It uses an encrypted TCP connection. Default is the Port Range between 901 and 904 TCP. ISS has not disclosed details about the protocols used.
The Proventia Appliance uses a standard Linux Syslog-NG for the local system logs. I tried successfully to pipe the logs from the device to another Syslog server with the goal to get a common monitoring of all network devices. But this constitutes a change in the Operation System build and thus creates problems with the Support contract of ISS for the sensors. I requested for a change in the contract but until now have I no answer (There is a license agreement shown whenever you login as root).

**Question:**
Are the alerts stored to tape, DVD and/or RAID?

**Answer:**
The Alerts are first stored on a RAID-1 on the SiteProtector in the SQL database. This alert data will be stored on a tape drive if the size reaches a defined level and at then stored in a safe.

**Question:**
For how long? This does not need to be a full policy document; however it should cover the major issues involved with the collection and retention of logs as well as some minor focus on disaster recovery of stored information. Some of the motivating factors affecting this mandatory requirement may be legislative in nature. If so, briefly identify them and reference the appropriate laws and you or your legal teams' interpretation of these laws.

**Answer:**
*A short notice about disaster Backup*.
I would recommend after a successful Installation of the SiteProtector Management Software to image the whole machine(s) with for example ghost. By default no Backup function for the important files in the SiteProtector are available. What I would also recommend is a permanent backup of the running polices and the response policies on the sensors. This is possible via an export function on the SiteProtector. The Knowledge Base of ISS contains an article with instructions how the database could be recovered with backups in case of a crash.

*The general Monitoring Requirements in case of Alerts/logs is written down in a Policy Document:*

*The IT Department expects the full utilization of security controls for the protection of the company, its assets, and its shareholders.*

1) *Logs of system events that are useful to IT Security must be collected and retained for no less than 180 days. Access to such logs must be made available to IT Security at any time. Determination of useful log data is at the sole discretion of the IT Security Department.*
2) *All systems that create, store or send security related log information must have their system time synchronized with an acceptable time-sync source.*
3) *Detective log analysis will be performed on intrusion detection system logs at least once per week when no alarms are received and within one hour when an alarm is received. Since current technology provides means to automatically detect interesting events, manual log analysis on other systems is only used as a forensics tool (e.g. post security incident investigation) and will not be reviewed routinely. Automated event detection must always be preferred to manual analysis due to the cost and inefficiency of manual methods. The IT management must make every effort to purchase commercial grade automated analysis tools whenever cost effective and feasible.*
4) *Security controls (e.g. Intrusion Detection / Intrusion Prevention systems etc.) should automatically alert security personnel when an event of high interest occurs. Email alerting via cellular telephone text messaging is preferred. The appropriate choice of which controls should alert is at the sole discretion of IT Security.*

**Question:**

How will the Concept of Operations (CONOPS) be handled? How will monitoring be employed and what will be done with events of interest or incidents once they are identified?

**Answer:**

The Operational Duties are completely covered by the Network Team. They also operate all routers, switches and firewalls. The design of the firewalls, IPS, the policies for detection and the policies for the response are covered by the Security Team. A Proventia development has a Life Cycle Model. After design and reference implementation a testing phase follows during that the Proventia works only in “Network Simulation” mode. The sensor works as a “normal IDS” passive inline system. In a time frame of round about 8 weeks the Security Team develops the detection and response policy. These 8 weeks are usually enough to catch all business relevant traffic and make the necessary exclude filters and



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

fine-tuning. After this the policy is enabled in “Inline Protection” mode and the operational tasks are handed over to the Networking Team. This means that the Proventia now is in strike back mode and blocks/drops evil or unwanted packets. This does not mean that the policy will stay forever in this stage. Because of risk-, traffic- and environment changes this policy needs to be reviewed and adapted frequently.

*About the event monitoring:*
During business hours (8 am to 7 pm) one person of the Network Team has the duty to permanently check the events in the SiteProtector log. The events are grouped by the Proventia in 3 classes (HIGH, MEDIUM, and LOW).
For critical HIGH events (e.g. slammer worm), the Proventia is configured to send mail alerts to the Networking and Security Team.
What is considered as a HIGH event is defined by the detection policy.
By the use of mail rules some of the HIGH events (most critical) are forwarded from the mail server to the blackberry mobile devices of the Networking Team as alarm.
*Such an event requires an immediate reaction*. For these events, plans are available which steps are necessary to minimize damage. If an unclear event occurs then the Network Team must contact the Security Team which then makes a decision what reaction needs to be taken by the operations teams. Currently no defined time frame is defined for the necessary action. Of course that must be done as fast as possible.
In cases of MEDIUM or LOW events, the Networking Team has a scope to decide them selves how to react. Through the fact that they as well monitor the other networking devices, they have the possibility to correlate these events and in the most cases enough experience to know what is to be done. In unclear situations they must contact the Security Team.
To avoid that these unclear situations happen in the future again, a Guideline is written after solving such issues.
On the beginning of every week the Network Team must deliver a report to the Security Team what occurred in the last week and how they have reacted.

**Question:**
How does the Intrusion Detection component of the big security picture fit into your organization to add value?

**Answer:**
No IDs or IPS can substitute a firewall or a router/switch with ACL’s.
It represents an additional layer of Security. Especially protecting from Worms and Viruses within allowed traffic flows constitutes an additional benefit. No Stateful Inspection firewall and no proxy firewall currently have the capability to check nearly the whole traffic stream for these threats. This task can be solved by an IDS/IPS. The advantage of an IPS against an IDS System is that it has the capability to block such threats in real time. Another advantage is that if a



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

signature for a known threat is available like for example for the sasser worm can this threat be blocked and the people which are responsible for the Web servers have more time to test if the from the vendor applied patches are working properly. This can be also be dangerous because some people think then they must never patch there systems. That's not true!

**Question:**
If you intend on providing 24/7 monitoring, discuss how this is to be implemented. What staff, alerting capability and on-call procedures exists?

**Answer:**
Our Operations/Monitoring Team is only available from 8 am until 7 pm.
The benefit of providing 24/7 monitoring is too low and to implement this service with internal or external staff is too expensive for our company. If the Firewall or IPS Systems detects a real big problem (for example flooding) then the second level support gets an automated email message via the blackberry mobile device. In this case, they are responsible for taking appropriate action.

**Question:**
In detail, describe how encryption either does or does not play a part in your architecture for the purposes of securing logged events of interest at any point in time.

**Answer:**
Our company decided not to have an out of band management network. Nevertheless, the IPS appliance has an out of band management interface. To reduce the risk of eavesdropping on logs, it becomes very clear that all communication with logs SHOULD be encrypted.

*Selected Product:*
I used the Proventia G Series from ISS in inline mode (IPS) with the Management Platform SiteProtector. All necessary components for the SiteProtector are running on one same Server.

*Here follows a description about all data flows where logs are involved and how the encryption is solved:*

*Transport of the logs from the IPS sensor to the Management Stations Database (Microsoft SQL 2000 Server Enterprise):*
By default, the complete communication from the IPS sensor (Proventia) to the Management Station is encrypted. The communication goes over the TCP Ports 2998 (Command and Control Cannel) and 901 (Event/Log Cannel). Both use a public/private key encryption. The encryption method is selectable during the installation. ISS offers two different types of encryption:

a) Certicom (239-bit encryption)
b) RSA (with 1024-bit RC4 (128) or 1536-bit 3DES)

It is also possible to add third party encryption modules if desired.
I decided to use the 1536-bit 3DES Method.
The Session Keys are automatically changed after 1 GB sent Data or latest after 6 hours.

*To view the logs produced by the IPS, I enabled 3 possibilities:*

1) To connect with MS RDP Terminal Service (with HIGH encryption enabled) to the Windows 2003 Server on which the SiteProtector Software is installed and start the Management Console GUI locally to browse through the logs. The Terminal Service uses port 3389/tcp by default.
2) To connect from an Administrator PC via the JAVA based Management Console GUI to the SiteProtector. This communication is also encrypted and uses the TCP port range from 3994 to 3998.
3) To access the SiteProtector with a browser and HTTPS.
The browser solution offers only a read only capability.
For this purpose, an Apache 2 Web Server with OpenSSL runs on the SiteProtector system. ISS provides the necessary patches and upgrades also for these software components.

*Backup of the SQL Database on the SiteProtector with the IPS Logs:*
In our SiteProtector SQL Database, currently there is space for nearly 73 GB of logs. To fill this space, it takes round about 3 months. The Companies Log Retention Policy requires to store the logs for a longer period. If it is necessary to dump the Database, this is done manually. The dumps are stored on a tape-drive, which is attached to the server. The backup tapes are stored in a safe.

*Indirect Information about logs through sending of alerts by email:*
The Proventia sensor itself is able to send alerts of different types. I enabled email alerts for a few specially selected events. These alerts are sent in clear text to an internal mail relay server and from there to the administrators or/and operators. This connection is not encrypted. The only protection are Access Lists on the Switches between the Proventia and the mail relay server and entries on the internal mail relay to allow this IPS boxes to relay mails.
This is the only point where indirect log data are viewable if an attacker would sniff the wire.

*Storing of Incident logs:*
If an incident occurs and an administrator downloads parts of the log via the Console GUI or exports logs from the SQL Database to make a further incident handling then he is obligated to store these logs only on encrypted devices. For example can he use PGP Disk.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## Appendix (Test script and construction):

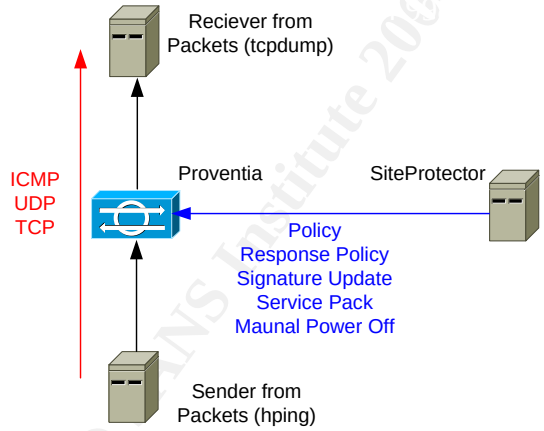
The Proventia works as a Layer two bridge transparent to the network
Every action like:

- Enabling new Policies
- Enabling new Response Policies
- Upgrades of Signatures
- Product Upgrades (Service Pack)
- Manual power off during full operations (Mechanical relay switches machine into bypass mode)

influences the packet forwarding delay due to the necessary restart of the ISS daemon on the IPS appliance.

While the restart of the daemon the Proventia IPS appliance buffers all traffic internally, processes the task (action) and after successful completion forwards the buffered traffic. To prove that this increase of delay does not impact other applications (no interruption or session timeout) I tested the possible loss rate and delay of ICMP, UDP and TCP packets in several scenarios (in Lab setup up and during downtime in the productive network). Restarts of the daemon showed maximum losses of 2 UDP packets and maximum time delay increases to 1.2 seconds (typically the delay increased to values up to 150 msec).

Test construction:




```
#!/bin/bash

INTERVAL=u250000
UDP_DSTPORT=161
TCP_DSTPORT=139

if [ ! $# -eq 3 ]
then

echo "Usage: ./test_ips.sh  Test_Nr  IP_Address  Name_of_Test"
echo Nr. 1. hping2 --interval $INTERVAL -1 -K 8 ipaddress
DESC1="Permanent Ping , Intervall $INTERVAL"
```



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
echo $DESC1
echo
echo Nr. 2. hping2 -n -2 --interval $INTERVAL --baseport 1025 --destport 161 ipaddress
DESC2="Permanent UDP Ping Dest Port $UDP_DSTPORT , Intervall $INTERVAL"
echo $DESC2
echo
echo Nr. 3. hping2 -n --interval $INTERVAL --destport $TCP_DSTPORT  ipaddress
DESC3="Permanent TCP Ping Dest Port $TCP_DSTPORT , Intervall $INTERVAL with 0 Flags in TCP header"
echo $DESC3
echo
echo Nr. 4. hping2 -n --interval $INTERVAL --destport $TCP_DSTPORT  ipaddress
DESC4="Permanent TCP Ping Dest Port $TCP_DSTPORT , Intervall $INTERVAL with S Flag in TCP header"
echo $DESC4
exit 1
exit 1
fi

RESULT=$3_$1_$2_`date +%H:%M:%S`_`date -I`.log

case "$1" in
1)
        rm -rf ./$1_tmp*
        echo Results are stored in $RESULT
        echo $DESC1 >  $RESULT
        echo >> $RESULT
        echo "hping2 --interval u500000 -1 -K 8 $2" >> $RESULT
        sleep 2
        hping2 --interval $INTERVAL -1 -K 8 $2 1>$1_tmp1 2>$1_tmp2;cat $1_tmp* >> $RESULT
        exit 0
        ;;
2)
        rm -rf ./$1_tmp*
        echo Results are stored in $RESULT
        echo $DESC2 >  $RESULT
        echo >> $RESULT
        echo "hping2 -n -2 --interval $INTERVAL --baseport 1025 --destport $UDP_DSTPORT $2" >> $RESULT
        sleep 2
        hping2 -n -2 -c 120  --interval $INTERVAL --baseport 1025 --destport $UDP_DSTPORT  $2 1>$1_tmp1
2>$1_tmp2;cat $1_tmp* >> $RESULT
        exit 0
        ;;
3)
        rm -rf ./$1_tmp*
        echo Results are stored in $RESULT
        echo $DESC3 >  $RESULT
        echo >> $RESULT
        echo "hping2 -n --interval $INTERVAL --destport $TCP_DSTPORT  $2" >> $RESULT
        sleep 2
        hping2 -n --interval $INTERVAL --destport $TCP_DSTPORT $2 1>$1_tmp1 2>$1_tmp2;cat $1_tmp* >>
$RESULT
        exit 0
        ;;
4)
        rm -rf ./$1_tmp*
        echo Results are stored in $RESULT
        echo $DESC4 >  $RESULT
        echo >> $RESULT
        echo "hping2 -n -S --interval $INTERVAL --destport $TCP_DSTPORT  $2" >> $RESULT
        sleep 2
        hping2 -n -S --interval $INTERVAL --destport $TCP_DSTPORT $2 1>$1_tmp1 2>$1_tmp2;cat $1_tmp* >>
$RESULT
    exit 0
        ;;
*)
        echo NO parameters specified
        ;;
esac

exit 0
```





© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

**PART 2**

**Network Detect 1: XDCMP**

_____

[**] [1:517:1] MISC xdmcp query [**]
[Classification: Attempted Information Leak] [Priority: 2] 08/30-02:36:33.674488
64.24.134.112:1155 -> 138.97.128.28:177 UDP TTL:110 TOS:0x0 ID:35871
IpLen:20 DgmLen:35 Len: 7
[Xref => http://www.whitehats.com/info/IDS476]

[**] [1:517:1] MISC xdmcp query [**]
[Classification: Attempted Information Leak] [Priority: 2] 08/30-02:36:35.684488
64.24.134.112:1155 -> 138.97.128.28:177 UDP TTL:110 TOS:0x0 ID:36127
IpLen:20 DgmLen:35 Len: 7
[Xref => http://www.whitehats.com/info/IDS476

2.1 Source of Trace:

_____

The raw log was taken from the practical logs.
http://isc.sans.org/logs/Raw/2002.7.30
The data seems to be captured between
*tcpdump -ttt -nqnr 2002.7.30 | awk '{print $1 " " $2 " " $3}' | head -1*
Aug 30 02:02:46.944488 (First Packet)
and
*tcpdump -ttt -nqnr 2002.7.30 | awk '{print $1 " " $2 " " $3}' | tail -1*
Aug 31 01:59:42.544488 (Last Packet)
The elapsed time was 23:56:55 hours.
Do not forget the IP's were sanitized and therefore the checksums of the packets are not correct.

The following has been taken for the analysis:

*OpenBSD 3.5,*
*Snort Version 2.2.0 (Build 30),*
*Snort rule snapshot from August 20th 2004,*
*Snort_sort,*
*tcpdump version 3.4.0,*
*libpcap version 0.5,*
*Ethereal 10.6*



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In principal I followed the excellent described way of P. H .Storm's GIAC Practical Assignment.

Before I start there is an overall view about the used fields from awk in the extracted fields from tcpdump by means of the first package of the analysis.

02:02:46.944488 0:0:c:4:b2:33 0:3:e3:d9:26:c0 0800 1514: 138.97.18.88.62050
*1* *2* *3* *4* *5* *6*
Time DST-MAC SRC-MAC PROT SIZE SRC-IP

> 64.154.80.51.80
*7 8*
DST-IP

I started with a look at the involved destination MAC addresses:
*tcpdump -ner 2002.7.30 | awk '{print $2}' | sort -u*
0:0:c:4:b2:33
0:3:e3:d9:26:c0

The source MAC addresses was next:
*tcpdump -ner 2002.7.30 | awk '{print $3}' | sort -u*
0:0:c:4:b2:33
0:3:e3:d9:26:c0

There were only two MAC's.

Both MAC's are very well know vendor codes from Cisco. Others could be found under:
http://standards.ieee.org/regauth/oui/index.shtml

CISCO SYSTEMS, INC.
170 WEST TASMAN DRIVE
SAN JOSE CA 95134-1706

Which destination addresses come from the first (0:0:c:4:b2:33) MAC?
*tcpdump -ner 2002.7.30 ether dst 0:0:c:4:b2:33 | awk '{print $8}' | awk -F \.'{print $1 "." $2 "." $3 "." $4}' | sort -u*
138.97.0.24
138.97.100.42
138.97.113.74
138.97.118.62
....
49 different IP's but all were from the same 138.97.0.0/16 Network.

Which destination addresses come from the second (0:3:e3:d9:26:c0) MAC?
*tcpdump -ner 2002.7.30 ether dst 0:3:e3:d9:26:c0 | awk '{print $8}' | awk -F \. '{print $1 "." $2 "." $3 "." $4}' | sort -u*
12.101.121.235
12.213.64.246
12.217.160.102
....
543 different IP's occurred.

Which source addresses come from the first (0:0:c:4:b2:33) MAC?
*tcpdump -ner 2002.7.30 ether src 0:0:c:4:b2:33 | awk '{print $6}' | awk -F \.'{print $1 "." $2 "." $3 "." $4}' | sort -u*
Only one:
138.97.18.88
That seems the IP address from one of the Cisco Devices.

Which source addresses come from the second (0:3:e3:d9:26:c0) MAC?
*tcpdump -ner 2002.7.30 ether src 0:3:e3:d9:26:c0 | awk '{print $6}' | awk -F \.'{print $1 "." $2 "." $3 "." $4}' | sort -u*
12.120.37.14
130.228.101.40
….
67 different IP's occurred.

My assumption is that this dump came from a network with asymmetric routing or it was sniffed over a tap?
I tried to get Light in the Dark with Filters for the 3 Way handshake.

A Filter for SYN:
---
*tcpdump -nr 2002.7.30 "(tcp[13] &0x3f = 2)"*
11:05:21.044488 62.248.106.208.4471 > 138.97.18.88.3128: S 2298415038:2298415038(0) win 32767 <mss 1460,nop,nop,sackOK> (DF)
11:05:21.104488 62.248.106.208.4472 > 138.97.18.88.8080: S 2298503855:2298503855(0) win 32767 <mss 1460,nop,nop,sackOK> (DF)
11:05:21.114488 62.248.106.208.4476 > 138.97.18.88.1080: S 2298554789:2298554789(0) win 32767 <mss 1460,nop,nop,sackOK> (DF)
11:05:21.744488 62.248.106.208.4471 > 138.97.18.88.3128: S 2298415038:2298415038(0) win 32767 <mss 1460,nop,nop,sackOK> (DF)
<snip>
Only SYN Packets in one direction to hosts in the 138.97.0.0/16 network.

A Filter for a SYN/ACK:

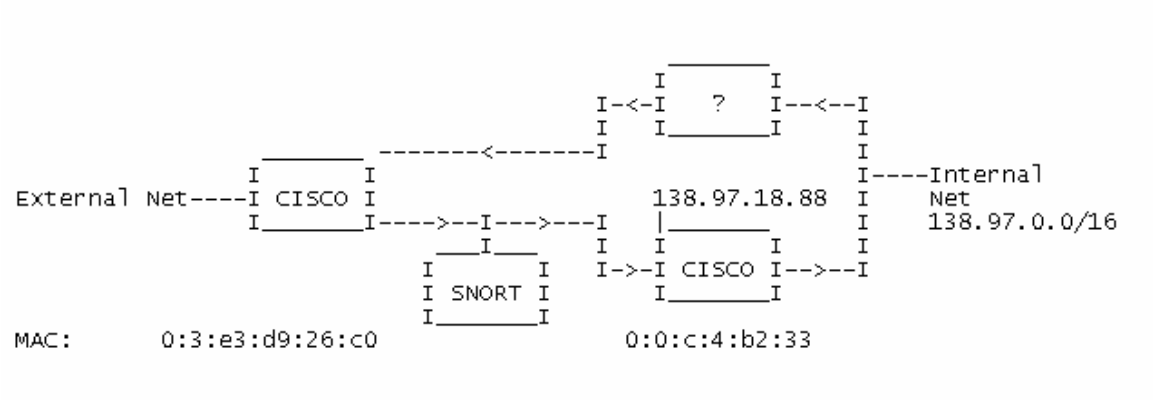
---
*tcpdump -nr 2002.7.30 "(tcp[13] &0x3f = 18)"*
19:36:22.524488 161.69.201.237.6005 > 138.97.18.88.61010: S 373906:373906(0) ack 637081413 win 17520 <mss 1460,nop,nop,sackOK>

Only this one appeared.
The origin from this connection seems to be the 138.97.18.88 itself. I do not see for this connection the SYN and the ACK. These both seem to go over the other direction.

A Filter for ACK:
---
*tcpdump -nr 2002.7.30 "(tcp[13] &0x3f = 16)"*
02:21:43.134488 204.253.104.205.80 > 138.97.18.88.63317: . 4282858582:4282860042(1460) ack 515833289 win 17055
02:21:43.154488 204.253.104.205.80 > 138.97.18.88.63317: . 1460:2920(1460) ack 1 win 17055
02:21:43.214488 204.253.104.205.80 > 138.97.18.88.63317: . 10220:11680(1460) ack 1 win 17055
06:10:58.004488 207.46.249.126.80 > 138.97.18.88.61919: . 626020851:626022311(1460) ack 1317473651 win 17190 (DF)
<snip>
Here again. Only ACK Packets in one direction to hosts in the 138.97.0.0/16 network.

This supports my theory that this dump must be from a tap or through an asymmetric routing.

Here is a picture how it could be:
---




An attempt to identify the purpose of the devices with a quick look to the incoming Ports (Destination 138.97.0.0/16 Network) from the MAC 0:3:e3:d9:26:c0.
*tcpdump -ner 2002.7.30 ether dst 0:3:e3:d9:26:c0 | awk '{print $8}' | awk -F \. '{print $5}' | sort -u*
Here are the interesting Ports and what is usually behind them:

| | |
|---|---|
| 22: | SSH |
| 80: | World Wide Web HTTP |
| 1863-23542: | Several Ports in this range. |

433 different Ports total.

A quick look at the outgoing Ports from the MAC 0:0:c:4:b2:33
*tcpdump -ner 2002.7.30 ether dst 0:0:c:4:b2:33 | awk '{print $8}' | awk -F \. '{print $5}' | sort -u*

| | |
|---|---|
| 53: | DNS |
| 80: | World Wide Web HTTP |
| 515: | Spooler (lpd) |
| 177: | X Display Manager Control Protocol |
| 1080: | Socks |
| 3128: | Squid-HTTP |
| 8080: | Common HTTP proxy/second web server port |
| 61010-64817: | 73 Ports in this range. |
| 9793: | Unassigned |

81 different Ports total.

This is only a snapshot from the used ports because the dump only has a time frame of 23:56:55 hours.
Therefore is it not proven that other ports are not used and thus unfortunately there is no deep declaration possible.

2.2 Detect was generated by:

_____

I ran Snort Version 2.2.0 (Build 30) with the rule snapshot from August 20th 2004 against the raw file 2002.7.30.

I used the command:
*sans@:/tmp>snort -c /etc/snort.conf -k none -r /tmp/2002.7.30 -l . –h 138.97.0.0/16 -r 2002.7.30 -y -e -v -d > summary.txt*

From man Snort:

| | |
|---|---|
| -c config-file | Use the rules located in file config-file |
| -d | Dump the application layer data when displaying packets in verbose or packet logging mode |
| -k checksum-mode | Decided for none because of the obfuscated and manipulated raw file.<br>none means turns off the entire checksum verification subsystem |
| -r file | Read the tcpdump-formatted file tcpdump-file. |
| -l | log-dir |

-h home-net
-y Include the year in alert and log file.
-e Display/log the link layer packet headers.
-v Be verbose.

To get a fast overall view about the attacks I took the script snort_sort.pl from Andrew R. Baker <andrewb@uab.edu>

The Output was:
*[119:18:1] (http_inspect) WEBROOT DIRECTORY TRAVERSAL*
*[1:526:9] BAD-TRAFFIC data in TCP SYN packet*
*[1:517:1] MISC xdmcp query*
*[119:2:1] (http_inspect) DOUBLE DECODING ATTACK*
*[119:15:1] (http_inspect) OVERSIZE REQUEST-URI DIRECTORY*
*[119:13:1] (http_inspect) NON-RFC HTTP DELIMITER*
*[119:7:1] (http_inspect) IIS UNICODE CODEPOINT ENCODING*
*[116:46:1] (snort_decoder) WARNING: TCP Data Offset is less than 5!*
*[119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING*
*[119:12:1] (http_inspect) APACHE WHITESPACE (TAB)*

The output during the Snort run was:
==========

Snort processed 3347 packets.
==========
*Breakdown by protocol:*
*TCP: 3342 (99.851%)*
*UDP: 2 (0.060%)*
*ICMP: 0 (0.000%)*
*ARP: 0 (0.000%)*
*EAPOL: 0 (0.000%)*
*IPv6: 0 (0.000%)*
*IPX: 0 (0.000%)*
*OTHER: 0 (0.000%)*
*DISCARD: 3 (0.090%)*
==========
Action Stats:
ALERTS: 449
LOGGED: 449
PASSED: 0
==========
*Fragmentation Stats:*
*Fragmented IP Packets: 5 (0.149%)*
*Fragment Trackers: 5*

*Rebuilt IP Packets:* *0*
*Frag elements used:* *0*
*Discarded (incomplete):* *0*
*Discarded (timeout):* *0*
*Frag2 memory faults:* *0*
==========

TCP Stream Reassembly Stats:
TCP Packets Used: 3339 (99.761%)
Stream Trackers: 2108
Stream flushes: 0
Segments used: 0
Stream4 Memory Faults: 0
==========

Strange Result with 2 UDP Packets occurs. What was the purpose of these packets?
Let's have a deeper look.

With
*tcpdump -n -ttt -r 2002.7.30 udp*
got I this:
Aug 30 02:36:33.674488 64.24.134.112.1155 > 138.97.128.28.177: udp 7
Aug 30 02:36:35.684488 64.24.134.112.1155 > 138.97.128.28.177: udp 7

Destination Port 177 is X Display Manager Control Protocol.

Then I found in the in the Alert file:
*[**] [1:517:1] MISC xdmcp query [**] [Classification: Attempted Information Leak] [Priority: 2] 08/30-02:36:33.674488 64.24.134.112:1155 -> 138.97.128.28:177 UDP TTL:110 TOS:0x0 ID:35871 lpLen:20 DgmLen:35 Len: 7*
*[Xref => http://www.whitehats.com/info/IDS476]*

*[**] [1:517:1] MISC xdmcp query [**]*
*[Classification: Attempted Information Leak] [Priority: 2] 08/30-02:36:35.684488 64.24.134.112:1155 -> 138.97.128.28:177 UDP TTL:110 TOS:0x0 ID:36127 lpLen:20 DgmLen:35*

To check for other activities with this IP I searched with:
*tcpdump -n -ttt -r 2002.7.30 host 138.97.128.28*
and got again only these 2 entries:
Aug 30 02:36:33.674488 64.24.134.112.1155 > 138.97.128.28.177: udp 7
Aug 30 02:36:35.684488 64.24.134.112.1155 > 138.97.128.28.177: udp 7

Maybe it was a scan?
I took a look to the Source Address:
*tcpdump -n -ttt -r 2002.7.30 host 64.24.134.112*

Here was the same. Only these 2 Connections occurred.

The time difference between both of these connections was exactly 2.0 sec. This could be a start of Retransmissions? 2, 4, 8,....
But where were the other packets?

With the Payload from 00 01 00 03 00 01 00 was it possible to identify that it was really a xdmcp query.
Reference Signatures:
http://www.whitehats.com/info/IDS476

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

*08/30/02-02:36:33.674488 0:3:E3:D9:26:C0 -> 0:0:C:4:B2:33 type:0x800 len:0x3C 64.24.134.112:1155 -> 138.97.128.28:177 UDP TTL:110 TOS:0x0 ID:35871 IpLen:20 DgmLen:35*

*Len: 7*
*00 01 00 03 00 01 00 .....*

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

*08/30/02-02:36:35.684488 0:3:E3:D9:26:C0 -> 0:0:C:4:B2:33 type:0x800 len:0x3C*
*64.24.134.112:1155 -> 138.97.128.28:177 UDP TTL:110 TOS:0x0 ID:36127 IpLen:20 DgmLen:35*

*Len: 7*
*00 01 00 03 00 01 00 .....*

To identify the target as a Unix Host with passive fingerprinting in this case p0f helps not because it requires TCP Packets.

2.3 Probability the source address was spoofed:
_____

UDP itself is very easily to spoof. In this case it can not be answered if it was a discovery attempt or a trial of an exploit, dos or simply a wrong typed IP. It was not possible through the obfuscation of the IP's to control the checksums.

To check the IP header was as well not really useable because the packets was trough the obfuscation changed. I do not know if the TTL was as well changed? If not can I only guess that the attacker maybe uses a Windows (TTL 128) and http://www.cygwin.com.

Netware has as well a TTL from 128 but it is not a typical attack platform.

2.4 Description of the attack:

_____

I describe all three possibilities of this attack.

1) Miss typed IP.
A XDMCP Query Runtime Host Prompt goes this way: If a User starts an XDMCP-Query-Session, without any entry in the Host-Field, normally there appears a display box in which the user can type in the IP. In this case the User probably typed the wrong one?
For example you can do cygwin under windows:
*/cygwin/usr/X11r6/bin/Xwin -query machine_name.org -from 10.10.10.10 (SRC-IP)*

2) Xdmcp query can be used to discover responses.
An attacker can take a random or directed IP and then wait for an answer from the X display manager (xdm) which provides authentication and management for X Windows.
If this xdm answered, the attacker gets a login screen. So the attacker would get Information about this host and in some rare cases (older Linux) a list of logged in users.

A very good description about xdmcp and indirect xdmcp queries can be found there:
XDM: The basic concept:
http://www.menet.umn.edu/~kaszeta/unix/xterminal/basics.html

Steps to Setting up Xdmcp Indirect
http://www.hummingbird.com/support/nc/exceed/ex60253.html?cks=y

Xdmcp query
http://www.whitehats.com/info/IDS476

3) Lately there occurred a few new xdmcp vulnerabilities:
Maybe the attacker searched for an open system?
With special crafted xdmcp packets is it possible to exploit or crash the target.

References:
http://secunia.com/search/?search=xdmcp
Sun Solaris XDMCP Parsing Vulnerability
http://secunia.com/advisories/12257/
Sun Solaris X Display Manager does not handle invalid XDMCP requests properly
http://www.kb.cert.org/vuls/id/139504
Sun Solaris CDE dtlogin XDMCP Parsing Vulnerability



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

http://secunia.com/advisories/11214/
Common Desktop Environment dtlogin XDMCP Parsing Vulnerability
http://secunia.com/advisories/11210/
HP-UX dtlogin XDMCP Parsing Vulnerability
http://secunia.com/advisories/11614/

So what? The reason for this connection stays unclear.

2.5 Attack mechanism:

_____

Please see one point above.

2.6 Correlation:

_____

I found no other attacks of this source address in the Databases from:
http://www.mynetwatchman.com/
or
http://www.dshield.org/

So I searched myself to get a few more information about the attacker.

To whom belongs the IP?

http://www.geektools.com/whois.php

OrgName: Starnet, Inc.
OrgID: STNI
Address: 579 First Bank Drive,
Address: Suite 100
City: Palatine
StateProv: IL
PostalCode: 60067
Country: US

NetRange: 64.24.0.0 - 64.24.255.255
CIDR: 64.24.0.0/16
NetName: STARNET-CIDR-BLK-2
NetHandle: NET-64-24-0-0-1
Parent: NET-64-0-0-0-0
NetType: Direct Allocation
NameServer: NS1.STARNETINC.COM
NameServer: NS3.STARNETINC.COM
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate: 1999-12-29
Updated: 2002-04-19

TechHandle: SH1253-ARIN
TechName: StarNet Hostmaster, StarNet
TechPhone: +1-847-963-0116
TechEmail: hostmaster@starnetusa.net

OrgAbuseHandle: SAD-ARIN
OrgAbuseName: StarNet Abuse Desk
OrgAbusePhone: +1-847-963-0116
OrgAbuseEmail: abuse@starnetusa.net

OrgNOCHandle: STARN-ARIN
OrgNOCName: StarNet NOC
OrgNOCPhone: +1-847-963-0116
OrgNOCEmail: noc@starnetusa.net

OrgTechHandle: SH1253-ARIN
OrgTechName: StarNet Hostmaster, StarNet
OrgTechPhone: +1-847-963-0116
OrgTechEmail: hostmaster@starnetusa.net

# ARIN WHOIS database, last updated 2004-08-23 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.

It seems to be an ISP with a large IP Range and probably many different Users.

2.7 Evidence of active targeting:

_____

It could not be declared if it was the discovery of an attack or only a typo in the IP. Think bad and survive ;-) Probably is this more an attack.

2.8 Severity:

_____

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

Criticality = 3
---
I can not make a declaration about this. Assumption 3 because X Systems normal offer a wide range on services and the loss of one of these systems can cause trouble.

Lethality = 4
---

Trough the newly discovered weakness in xdmcp I would suggest a 4.

System countermeasures = 2
---
If the target is a machine which runs an X Server allowed only by internal addresses queries over SSH forwarded Tunnel. Be sure you have patched your system with the necessary patches.

Network countermeasures = 2
---
If you have X Servers on your Network do not allow xdmcp queries directly in your network. If, then only with RSA SecurID Token and over a SSH or VPN Tunnel.

2.9 Defensive recommendation:

_____
Please see below to System and Network countermeasures and apply patches or vendor workarounds if you have an affected system with the new xdmcp weakness.

2.10 Multiple choice test question:

_____

To which Port does an xdmcp query go?

A) 177
b) 22
C) 80
D) 1155

Correct answer: A)

**Network Detect 2: ICMP PING NMAP and HTR CHUNKED OVERFLOW**

_____

All started when I found in one Snort alert File the entry:
*08/25-09:50:25.801768 [**] [1:469:3] ICMP PING NMAP [**] [Classification:Attempted Information Leak] [Priority: 2] {ICMP} 217.147.43.33 -> xxx.xxx.xxx.21*

and

| Time, | | Event, |
|---|---|---|
| *25.08.2004* | *10:02:42,* | *TCP_Probe_HTTP,* |
| *25.08.2004* | *10:14:36,* | *HTTP_IIS_HTR_Chunked_Overflow,* |

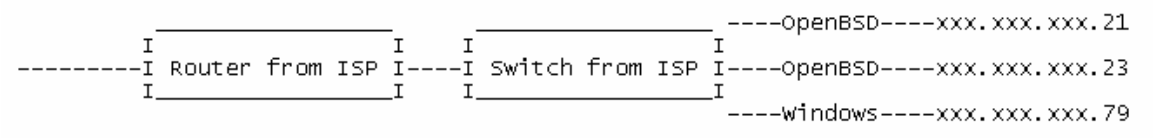
| Intruder IP, | Count, | Protocol ID, | Destination Port, |
|---|---|---|---|
| *217.147.43.33,* | *2,* | *TCP,* | *443,* |
| *217.147.43.33,* | *1,* | *TCP,* | *80* |

| Source Port, | Parameter(s) |
|---|---|
| *54423,* | *port=443&reason=Firewalled* |
| *56008,* | *URL=/ASPA.htr&server=xxx.xxx.xxx.79* |

2.1 Source of Trace:

_____

The traces come from 3 different machines all on the same public Class C Network. All Destination IP's are sanitized.




2.2 Detect was generated by:

_____

a) OpenBSD 3.5,
Snort Version 2.2.0 (Build 30),
OpenBSD pf Firewall,
tcpdump version 3.4.0,
libpcap version 0.5

b) OpenBSD 3.3,
Snort Version 2.2.0 (Build 30),
OpenBSD pf Firewall,
tcpdump version 3.4.0,
libpcap version 0.5
The used Snort rule set on both machines was the snapshot from August 20th 2004.

c) Windows 2000 Server with ISS Black ICE Server Protection 3.6 cno.
Black ICE is a commercial Firewall/IDS (IPS) System.
More Information can be found there: http://blackice.iss.net
The Windows Machine belongs to a friend of mine and he allows me to check and use his logs to correlate additional things. Thanks!
The condition to get access to the windows host was to sanitize Information about the host. On this Host runs a Microsoft IIS 5.0 web server.

All started when I found in the Snort alert File from the OpenBSD 3.5 the entry:
*08/25-09:50:25.801768 [**] [1:469:3] ICMP PING NMAP [**] [Classification:Attempted Information Leak] [Priority: 2] {ICMP} 217.147.43.33 -> xxx.xxx.xxx.21*

The Snort rules which triggered this discovery attempt were the icmp.rules
The content is:
*alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP"; dsize:0; itype:8; reference:arachnids,162; classtype:attempted-recon; sid:469; rev:3;)*

I get hundreds of these alerts every week but in this case I tried to find out more about the purpose of this discovery attempt. The Snort Log had not enough information to understand the whole picture. To find out more about the attempt/attacker I first searched in my OpenBSD pf firewall log (pflog) and found the ICMP there too. So no error or false alert from Snort occurred.

The pflog Files on OpenBSD are in Tcpdump readable Format.
To extract the /var/log/pflog in text format I used the following command:
*tcpdump -tttnn -r /var/log/pflog > sans.log*
With a grep "217.147.43.33" sans.log I got this output:

Aug 25 09:50:25.801779 rule 29/0(match): block in on xl0: 217.147.43.33 > xxx.xxx.xxx.21: icmp: echo request
The rule 29 was on my firewall "block drop in log proto icmp all"

But no other entries from this IP address.

The next step was to get to my second OpenBSD box and search if the entry was there again.
Yes, it was and I found just as well an entry in the Snort logs from the same IP.
*08/25-09:52:40.668327 [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 217.147.43.33 -> xxx.xxx.xxx.23*

and as well in the OpenBSD pf firewall log (pflog)
*Aug 25 09:52:40.668458 rule 25/0(match): block in on xl0: 217.147.43.33 > xxx.xxx.xxx.23: icmp: echo request*
The rule 25 was on this firewall "block drop in log proto icmp all"
Here it was the same as in my first box. No other entries in the Snort or in the firewall log.

With this behavior I could assume that not only one machine (from me) was the target.

First thought:
It is very likely that someone makes a random ping sweep over the C Class Network.
The question was only: What does he want to achieve with that?

Then had I the idea to ask a friend of mine if he would allow me to have a look at his log files. His Windows 2000 Server machine with a Black Ice Firewall/IDS System was in the same C Class Network.
In the event viewer (GUI) of his Black ICE Firewall/IDS System I searched for this IP from my "ICMP PING NMAP" and soon found a result.

| Time, | | Event, | | |
|---|---|---|---|---|
| *25.08.2004* | *10:02:42,* | *TCP_Probe_HTTP,* | | |
| *25.08.2004* | *10:14:36,* | *HTTP_IIS_HTR_Chunked_Overflow,* | | |
| Intruder IP, | Count, | Protocol ID, | Destination Port, | |
| *217.147.43.33,* | *2,* | *TCP,* | *443,* | |
| *217.147.43.33,* | *1,* | *TCP,* | *80* | |
| Source Port, | Parameter(s) | | | |
| *54423,* | *port=443&reason=Firewalled* | | | |
| *56008,* | *URL=/ASPA.htr&server=xxx.xxx.xxx.79* | | | |

In the Status Line from the GUI was an additional Info for the TCP_Probe_HTTP: [Host Sensor] This signature detects TCP port probes directed at port 80 or 443, which may indicate an attacker's attempt to discover an HTTP server on your system.

This was a much higher quality as the "ICMP PING NMAP" discovery!

Black ICE unfortunately writes in the event viewer nothing about ping.

To check if this machine was also pinged (before the attacks occured) it was necessary to open the Black ICE log files logxxx.enc and evdxxx.enc. For this I used Ethereal 10.6 which I installed on this Windows machine.

But before I go further I want to give you a short explanation what the enc Files from the ISS Black ICE are.
From https://iss.custhelp.com, Answer ID 1048
*The Packet Log and Evidence Log features of the software generate files with the extension ".enc".*
*These ".enc" files contain actual network traffic and in the case of evidence files, they contain traffic which were part of the detected attacks. These files are not readable by normal text editor programs, such as Notepad, but must instead be decoded by standard protocol analyzer programs (sniffers) that network technicians typically use to analyze network traffic*.




© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

By a default Installation these logs can be found under:
*C:\Program Files\ISS\BlackICE*
With a Filter in Ethereal for ICMP I got I the result very fast that this machine got an "echo request" from the attacker as well. (IP 217.147.43.33).

The time difference to the other two machines was approximately 30 seconds. All 3 machines are NTP synchronized. That would fit to a scan over the complete Class C Network.
The machine responded very likely with an "echo reply" (because echo reply was not disabled at this time).

To find the HTTP_IIS_HTR_Chunked_Overflow attack in the hugh log file I used the following Ethereal filter:
*ip.src == 217.147.43.33 and tcp.port == 56008*
56008 was the source Port from the attacker's machine.

To view the content of the packet I marked this package and then selected the *"Follow TCP Stream"* Option.
At least I saved this packet in ASCII Format. The Output was:

*POST /ASPA.htr HTTP/1.1*
*Host: xxx.xxx.xxx.79*
*Transfer-Encoding: chunked*

*20*
*XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX*
*0*

I searched further in the log Files but the attacker sends no further packets. In the following 12 hours of the log were no additional HTTP Request found. It seems that this attacker tried something and then lost his interest or found something easier?

2.3 Probability the source address was spoofed:
_____

Very unlikely that the source address was spoofed. Only one attacker appeared (no Decoy Scans) for the attacks (ping, scan and exploit) in a short timeframe.

2.4 Description of the attack:
_____

The picture from this attack/attacker is probably clear.

1) The attacker tried with an unknown scanning tool (maybe nmap but not proven) and sending from ICMP packets to catalogize targets which are reachable.

The "ICMP NMAP SCAN" was described well on:
http://www.snort.org/snort-db/sid.html?sid=469

2) Scanned later (maybe with a versions Banner/OS Scan) the PING reachable hosts if they have an open Port 80 or 443 and if the right Service is running on it (IIS Web Server).

3) Tries to exploit the IIS .htr weakness on machines which fit in point 2.

References to Microsoft's IIS ISAPI HTR chunked encoding heap buffer overflow Weakness:

This was the first description I got from the ISS Black ICE Protection when I followed the Event ID 2114002 with a Browser (was displayed with the Attack in the event viewer)
http://www.iss.net/security_center/reference/2114002.html

eEye Digital Security Advisory AD20020612
Windows 2000 and NT4 IIS .HTR Remote Buffer Overflow
http://www.eeye.com/html/Research/Advisories/AD20020612.html

This is from Microsoft about the weakness in their product and hints how to patch it. Microsoft Security Bulletin MS02-028 Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise (Q321599)
http://www.microsoft.com/technet/security/bulletin/ms02-028.mspx

CERT Vulnerability Note VU#313819
Microsoft Internet Information Server (IIS) contains remote buffer overflow in chunked encoding data transfer mechanism for HTR
http://www.kb.cert.org/vuls/id/313819

Common Vulnerabilities and Exposures
Buffer overflow in the chunked encoding transfer mechanism in IIS 4.0 and 5.0 allows attackers to execute arbitrary code via the processing of HTR request sessions, aka "Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise."
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0364

2.5 Attack mechanism:

_____

Please see one point above.

2.6 Correlation:

_____

I found no other attacks of this source address in the Databases from:
http://www.mynetwatchman.com/
or
http://www.dshield.org/

So I searched to get a few more information for myself about the attacker.

First step:
To whom belongs this IP address?

*$whois -h whois.ripe.net 217.147.43.33*
% This is the RIPE Whois secondary server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.

inetnum: 217.147.42.0 - 217.147.43.255
netname: INIT-LT
descr: Init Corporation
descr: Laisves al. 30a
descr: LT-3000, Kaunas
descr: Lithuania
country: LT
admin-c: IH2155-RIPE
tech-c: IH2155-RIPE
status: ASSIGNED PA
notify: hostmaster@init.lt
mnt-by: INIT-LT
changed: andrius@interneka.lt 20021017
source: RIPE

route: 217.147.42.0/23
descr: Init Corporation
origin: AS24877
notify: hostmaster@init.lt
mnt-by: INIT-LT
changed: andrius@interneka.lt 20010404
changed: hostmaster@init.lt 20030226
source: RIPE

role: INIT Hostmaster
address: Laisves al. 30a
address: LT-3000, Kaunas
address: Lithuania
phone: +370 37 422648
fax-no: +370 37 422246
e-mail: hostmaster@init.lt




© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
admin-c:     GK3254-RIPE
tech-c:      GK3254-RIPE
tech-c:      VK708-RIPE
nic-hdl:     IH2155-RIPE
notify:      hostmaster@init.lt
mnt-by:      INIT-LT
changed:     andrius@interneka.lt 20010118
changed:     andrius@interneka.lt 20020423
changed:     gintaras@init.lt 20030513
source:      RIPE
```

The IP address belongs to a Company in east Europe (Lithuania was formerly a country in the east block).

The second step was to get more info about the attacker's machine:

My Snort and firewall Logs did not have enough information to make conclusions with passive Fingerprinting.
So I took the log file from the ISS Black ICE (logxxx.enc) and used it.

To enable passive fingerprinting I converted the ISS own log format in tcpdump format.

I used the ISS Tool capconv.exe to do it.

```
Usage:  capconv [-A | -Oformat] infile outfile
Where:        infile is a capture file to convert
              outfile is an output capture file
              -A appends to the output file
              -R reverses bits in MAC addresses (for FDDI)
              -O sets the output capture format as follows:
              -Os  or -Osnoop     = Sun Solaris snoop format (RFC-1761)
              -Ot  or -Otcpdump   = Van Jacobson libpcap/tcpdump format
              -On  or -Onetmon    = Microsoft Network Monitor format
              -On2 or -Onetmon2   = Microsoft Network Monitor Version 2 format
              -Or  or -Orscapture = RealSecure capture format
              -Op  or -Ox         = NAI SnifferPro aka Cinco NetXray format
              -Osniffer           = NAI Sniffer 4.x format
               -O is not necessary if output file extension matches a known
              format, such as: .cap (for NetMon), .rsc (for RealSecure capture),
              .enc, .trc or .fdc (for Sniffer), .snoop, or .tcpdump.
Note .cap is used redundantly by many tools.
```

The used command was:
*capconv -Ot logxxx.enc converted.tcpdump*

This file I copied to my OpenBSD box and run this command

*tcpdump tttn -o -r converted.tcpdump | grep 217.147.43.33 | more*

tcpdump (from man)
-ttt Print day and month in timestamp.
-n Do not convert addresses (i.e., host addresses, port numbers, etc.) to names.
-o Print a guess of the possible operating system(s) of hosts that sent TCP SYN packets.
See pf.os(5) for a description of the passive operating system fingerprints.
Only available on OpenBSD!
-r Read packets from a file which was created with the -w option. Standard input is used if file is `-'.

For passive fingerprinting uses OpenBSD an in tcpdump integrated p0f.
http://www.w4g.org/fingerprinting.html

The result was:
....
Aug 25 10:14:36.682427 212.144.33.24.3596 > xxx.xxx.xxx.173.80: S (src OS: Windows XP, Windows 2000 SP2)
970901248:970901248(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)
....

One assumption can be made with this passive fingerprinting.
The attacker uses probably Windows XP or Windows 2000.
Nmap would run on both for the discovery scan.

2.7 Evidence of active targeting:
_____

The scan was totally random and not directed against one specific host. The attack itself goes probably only to servers which have port 80 or 443 open. I have no access to other Web servers in this range to check this.

2.8 Severity:
_____

Severity = 3 =
(Criticality + Lethality) - (System Countermeasures + Network Countermeasures)
( 3 + 5 ) - ( 4 + 1 )

Criticality = 3
---
All 3 machines are not really business critical for one of us.
I would set the criticality level to 3.

Lethality = 5
---
The scan itself has a rate of 1 but the attack itself has the Lethality of 5 because if the attack succeeds the attacker has a machine completely under his control.

System countermeasures = 4
---
On the Windows Box should ping be disabled because of this would a machine more invisible against many discovery methods.

Network countermeasures = 1
---
The Network from the attacker belongs to a very big ISP with many different customers whichever must have access to this network and it is not possible to filter all the IP addresses.

2.9 Defensive recommendation:

_____

Be sure that you have always the latest possible Patch Level and give as less as possible information about your servers. For example: Disable Ping.

I found a possibility on the ISS web side how to disable ping for the Black ICE. I would give the machine a 4 because all Microsoft patches are available and the Black ICE works as a IPS (Intrusion Prevention System) and blocks attacks active.

This article explains how to block Pings (ICMP).
This information applies to:
BlackICE PC Protection and BlackICE Server Protection version 2.9 and higher.
(Formerly BlackICE Defender for Workstation and BlackICE Defender for Server)

Fix Version:
N/A

Related Articles:

| |
|---|
| Can BlackICE block ICMP traffic? (Answer ID 1743)<br>Answer<br>By default, the software does not block pings. However, you can edit the firewall.ini file to tell BlackICE to block pings. REJECT statements must be manually added to the [MANUAL ICMP....] section of the firewall.ini.<br>If this is a new installation, the file will be located at C:/Program Files/ISS/BlackICE. If you have an older version of BlackICE that has been updated, the path will be: C:/Program Files/NetworkICE/BlackICE |

This statement will block all ICMP Echo traffic for all IP addresses.
REJECT, 8:0, ICMP, 2001-10-15 00:01:00, PERPETUAL, 1000, MANUAL

This statement will allow ICMP Echo traffic from 10.10.0.29
ACCEPT, 10.10.0.29:8:0, ICMP, 2001-10-15 00:01:00, PERPETUAL, 1000, MANUAL

This statement blocks ICMP Echo traffic from the specified IP address range (10.10.0.30 - 10.10.0.142).
REJECT, 10.10.0.30 - 10.10.0.142:8:0, ICMP, 2001-10-15 00:01:00, PERPETUAL, 1000, MANUAL

These statements block ICMP Timestamp and ICMP Address Mask requests respectively.

REJECT, 13:0, ICMP TIMESTAMP, 2001-10-15 00:01:00, PERPETUAL, 1000, MANUAL
REJECT, 17:0, ICMP MASKREQ, 2001-10-15 00:01:00, PERPETUAL, 1000, MANUAL

This attack can also be detected with Snort. The existing Rule is in the web-iis.rules

*alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS*
*(msg:"WEB-IIS .htr*
*chunked Transfer-Encoding";*
*flow:to_server,established; uricontent:".htr"; nocase;*
*content:"Transfer-Encoding|3A|"; nocase; content:"chunked";*
*nocase; distance:0; reference:bugtraq,4855; reference:bugtraq,5003;*
*reference:cve,2002-0364;*
*classtype:web-application-attack; sid:1806; rev:8;)*

2.10 Multiple choice test question:

_____

What means sid 524 in the triggered Snort rule?

A) Source Port
b) Destination Port
C) Identify Snort rule
D) Session ID

Correct answer: C)

**Network Detect 3: OVERSIZE REQUEST-URI DIRECTORY**

_____



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

I published this detect to the **intrusions@incidents.org** mailing list. The questions and answers (improvements) to this detect are published at the end.

[**] [119:15:1] (http_inspect) OVERSIZE REQUEST-URI DIRECTORY [**]
08/26-17:57:17.112865 217.184.254.169:4064 -> xxx.xxx.xxx.79:80 TCP
TTL:119 TOS:0x0 ID:23827 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xE0D3EACB  Ack: 0x3C599219  Win: 0x2238  TcpLen: 2

or

| Time, | Event, | Intruder IP, |
|---|---|---|
| *26.08.2004 17:57:20,* | *HTTP_URL_Name_Very_Long,* | *217.184.254.169,* |

| Count, | Protocol ID, | Destination Port, | Source Port |
|---|---|---|---|
| *1,* | *TCP,* | *80,* | *4064* |

Parameter(s)
*URL=/.±.....&URL-length=14593&accessed=no&code=400*

2.1 Source of Trace:

_____

Please see one point below.

2.2 Detect was generated by:

_____

From an ISS Black ICE Server Protection 3.6 cno Firewall/IDS System which was running on a Windows 2000 Server.
Under http://blackice.iss.net more Information can be found about this software. The Windows Machine belongs to a friend of mine and he allows me to use his logs for the SANS Practical. He was happy because I saved him from having to look at his logs himself ;-). The condition to get access to his logs was to sanitize Information about the host.

To get a second meaning (not only the BlackICE alert) from this detect I transferred the log from the commercial ISS System to tcpdump and loaded the Black ICE log File in Ethereal, marked everything and then I saved this File in the libpcap (tcpdump, Ethereal, etc.) format.

Now was it possible to run snort against this file with the command:
*c:\snort\bin\snort.exe -c:\snort\etc\snort.conf -b -l .*

I got two Files.
a) The alert.ids File
b) The snort.log.xxx File (Log in binary Format)

The result from the alert.ids shows 3 attacks from the attacker IP.

*[**] [1:1070:7] WEB-MISC WebDAV search access [**]*
*[Classification: access to a potentially vulnerable web application] [Priority: 2]*
*08/26-17:57:17.112865 217.184.254.169:4064 -> 217.147.106.19:80*
*TCP TTL:119 TOS:0x0 ID:23827 IpLen:20 DgmLen:1500 DF*
****A**** Seq: 0xE0D3EACB  Ack: 0x3C599219  Win: 0x2238  TcpLen: 20*
*[Xref => http://www.whitehats.com/info/IDS474]*

*[**] [119:15:1] (http_inspect) OVERSIZE REQUEST-URI DIRECTORY [**]*
*[Classification: access to a potentially vulnerable web application] [Priority: 2]*
*08/26-17:57:17.112865 217.184.254.169:4064 -> 217.147.106.19:80*
*TCP TTL:119 TOS:0x0 ID:23827 IpLen:20 DgmLen:1500 DF*
****A**** Seq: 0xE0D3EACB  Ack: 0x3C599219  Win: 0x2238  TcpLen: 20*
*[Xref => http://www.whitehats.com/info/IDS474]*

*[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]*
*08/26-17:57:17.112865 217.184.254.169:4064 -> 217.147.106.19:80*
*TCP TTL:119 TOS:0x0 ID:23828 IpLen:20 DgmLen:1500 DF*
****A**** Seq: 0xE0D3F07F  Ack: 0x3C599219  Win: 0x2238  TcpLen: 2*

The matching pattern for WEB-MISC WebDAV search access came from the web-misc.rules
The other two are from the file gen-msg.map which is located in the c:\Snort\etc directory.

During the analysis I used:
Windows XP Professional SP1,
*Version 2.2.0-ODBC-MySQL-FlexRESP-WIN32 (Build 30),*
*the default snort rule set,*
*Ethereal 10.6,*
*Winpcap 3.01 alpha,*
*Windump 3.8 alpha,*
*p0f version 2.0.4*

To get more Info I had to do as follows:
To view the content of the attack packet I loaded the original Black ICE Log File logxxx.enc into Ethereal and searched with the Filter:
*ip.src == 217.184.254.169 and tcp.port == 4064* for the attack.

After selecting the packet and taking "Follow TCP Stream" I saved this result as an ASCII file (I shorten the endless dots).

SEARCH

/.....
.....
.....
.....
.....
.....
.....
.....<snip>

2.3 Probability the source address was spoofed:

_____

It was an established TCP connection so it is very unlikely that the source address is spoofed. This means it occurred a TCP three way handshake.
I checked this with:
*windump -n -r transformed_tcpdump.tcpdump host 217.184.254.169 and port 4064*
The result was:

Syn
---
17:57:16.628479 IP 217.184.254.169.4064 > xxx.xxx.xxx.79.80: S
3771984586:3771984586(0) win 8760 <mss 1460,nop,nop,sackOK> (DF)

Syn/Ack from the web server
---
17:57:16.628479 IP xxx.xxx.xxx.79.80 > 217.184.254.169.4064: S
1012503064:1012503064(0) ack 3771984587 win 65535 <mss 1460,nop,nop,sackOK> (DF)

Ack from the attacker's machine
---
17:57:17.034739 IP 217.184.254.169.4064 > xxx.xxx.xxx.79.80: . ack 1 win 8760

2.4 Description of the attack:

_____

My first assumption was that this is an old attack against Microsoft web server because of the endless dots. It could remember me that an attack against IIS 2.0 and 3.0 (NT 4.0) with this pattern exists. My second assumption was an attack that has to do with WebDAV. The SEARCH / command leads me to this.

After a research with this below listed references my suspicion seems confirmed.

Resources:
That was included in the snort signature as description
http://www.whitehats.com/info/IDS474

Microsoft IIS WebDAV long request buffer overflow
http://xforce.iss.net/xforce/xfdb/11533

Critical WebDAV Vulnerability: Are Your Exchange Servers Safe?
http://www.winnetmag.com/Article/ArticleID/38396/38396.html

WebDAV BO Signature
http://archives.neohapsis.com/archives/iss/2003-q1/0442.html

Unchecked Buffer In Windows Component Could Cause Server Compromise (815021)
http://www.microsoft.com/technet/security/bulletin/MS03-007.mspx

New attack vectors and a vulnerability dissection of MS03-007
http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0144.html

Good Paper
http://www.nextgenss.com/papers/ms03-007-ntdll.pdf

Microsoft Windows ntdll.dll Buffer Overflow Vulnerability Many exploits available
http://www.securityfocus.com/bid/7116

Good description
http://www.giac.org/practical/GCIH/Brandon_Young_GCIH.pdf

2.5 Attack mechanism:

_____

The attacker sends a special crafted overlong URL to a vulnerable web server. This could cause a buffer overflow and trough which the attacker could gain access to unpatched or unprotected machines. Several exploits exists in the world.

2.6 Correlation:

_____

I found no other attacks from this IP in the Databases from:
http://www.mynetwatchman.com/

or
http://www.dshield.org/

So I tried to get a few more information about the attacker.

First step:
Who is the owner of this address?

*whois -h whois.ripe.net 217.184.254.169*

```
% This is the RIPE Who is secondary server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.

inetnum:      217.184.0.0 - 217.185.255.255
netname:      MWAYS-BIGDIAL
descr:        various Online Services
country:      DE
admin-c:      ABU1-RIPE
tech-c:       ABU1-RIPE
status:       ASSIGNED PA
remarks:      send hack and spam complaints to:
remarks:      abuse@mediaways.net
mnt-by:       MDA-Z
changed:      hostmaster@mediaways.net 20020415
source:       RIPE

route:        217.184.0.0/13
descr:        mediaWays GmbH
origin:       AS6805
remarks:      netname: DE-MEDIAWAYS
mnt-by:       MDA-Z
changed:      ip@mediaways.net 20010315
source:       RIPE

person:       mediaWays abuse
address:      Telefonica Deutschland GmbH
address:      Huelshorstweg 30
address:      D-33415 Verl
address:      Germany
phone:        +49 05241 80 1701
e-mail:       abuse@telefonica.de
nic-hdl:      ABU1-RIPE
remarks:      +----------------------------------+
remarks:      | Send hack and spam complaints to:  |
remarks:      |       abuse@telefonica.de          |
remarks:      +----------------------------------+
changed:      hostmaster@telefonica.de 20030324
source:       RIPE
```

It is a very big ISP. If I look at the side http://www.telefonica.de is this probably one of the largest in Germany (Europe).




© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The second step was to get more info about the attacker's machine:

I did it with the Tool p0f
I took the tcpdump format of the Black ICE log and run the following command against it:
*p0f -s transformed_tcpdump.tcpdump -o attacker_os.txt*

The result was:
....
<Thu Aug 26 17:57:16 2004> 217.184.254.169:4064 - Windows XP, 2000 SP2+
-> xxx.xxx.xxx.79:80 (distance 9, link: ethernet/modem)
....

2.7 Evidence of active targeting:
_____

I am not sure if the attacker tries to search for random targets or if it was an attack. The source does not appear in http://www.dshield.org as a "big" well known attacker so it is very difficult to give an answer about it.

2.8 Severity:
_____

Severity = 3 =
(Criticality + Lethality) - (System Countermeasures + Network Countermeasures)
( 3 + 5 ) - ( 4 + 1 )

Criticality = 3
---
The machine is not really critical. So I would rate it with 3

Lethality = 5
---
If the attack is successful I would rate it with 5. It could mean that the machine can be totally compromised if no other defensive lines are in place. Like Buffer Overflow Protection trough the NAI 8 Virus Scanner.

System countermeasures = 4
---
All is patched on the last possible level, a Firewall and an IPS are running there but nothing is really save so I suggest a System countermeasure of 4.

Network countermeasures = 1
---
To check URLs for evil content is very difficult because the requirements for

everybody are so different and nearly impossible for this big ISP.

2.9 Defensive recommendation:

_____

Be sure that you have always the latest possible Patch Level and have disabled all services which do you not need (E.g. WebDAV if it is not used).
If you really need WebDAV check if it is possible to limit the IP addresses which have access to this service. If this is not possible think about an Intrusion Prevention box in front of this service.
Additionally should URLScan be used, which is a part of the Microsoft IIS Lockdown Tool. It blocks this attack in its default configuration.
http://www.microsoft.com/technet/security/tools/urlscan.mspx

2.10 Multiple choice test question:

_____

What means DF in the triggered Snort rule?
TCP TTL:119 TOS:0x0 ID:23827 IpLen:20 DgmLen:1500 DF

A) Do not fragment
b) Data Field
C) Data Format
D) Defensive Format

Correct answer: A)

**Question and Answer from the intrusions@incidents.org mailing list**

_____

I posted my original detect on Wed, 15 Sep 2004 6:06 AM

*I got only one reply from:*
*Date: Wed, 15 Sep 2004 10:13 AM*
*From: "McKinlay, Ken" <ken.mckinlay@dy4.com>*
*Subject:RE: [Intrusions] LOGS: GIAC CIA Version 3.5 Practical Detect Frank Birkmair*

My answers are below his questions:

*Date: Wed, 15 Sep 2004 3:54 PM*
*To: "McKinlay, Ken" <ken.mckinlay@dy4.com>*
*Subject: RE: [Intrusions] LOGS: GIAC CIA Version 3.5 Practical Detect Frank Birkmair*

*> You might want to describe in a little detail what p0f does and why you*
*> used it to determine the type of system. What does this information give*
*> you? Does it help any with the analysis?*
http://lcamtuf.coredump.cx/p0f.shtml is the web side from p0f.
Directly from there:
P0f v2 is a versatile passive OS fingerprinting tool.
P0f can identify the system on:
- machines that connect to your box (SYN mode),
- machines you connect to (SYN+ACK mode),
- machine you cannot connect to (RST+ mode),
- machines that talk through or near your box.

In my case was it possible to use this tool because I had a SYN and a SYN/ACK packet. I used p0f because I tried to find out so much as possible over the attacker. One reason was to check later in the analysis if the TTL from the attacker's packets could match to the Operating System (Possible hint if the packet was spoofed).

*> What can you tell me about the system the event was logged on? Why did it*
*> accept an HTTP connection? Is it running IIS? Or is it running Apache on*
*> Windows 2000? This might affect your severity score since on an Apache*
*> system, it wouldn't matter, but IIS might be in trouble.*
On this machine runs an IIS 5.0. That is the reason because it accepts a HTTP Connection.
WebDAV runs never on this machine. The banner was not changed for obfuscating. To change banners from running services is an additional system countermeasure which I forgot in the 2.9 Defensive recommendations.
Thanks for the indirect hint.

*> Are the dots ('.') actually the '.' character or is it something else? I*
*> can't tell from your detect since you are only presenting an ASCII*
*> representation of the event. If they are not 0x2e (46 decimal) characters*
*> ('.'), what are they? You might want to include part of the hexidecimal dump*
*> of the packet for clarification.*
Here is the hex dump:
windump -nX -r long_url_dmp.dmp
17:57:17.112865 IP 217.184.254.169.4064 > xxx.xxx.xxx.79.80: .
3771984587:3771986047(1460)
ack 1012503065 win 8760 (DF)

```
0x0000   4500 05dc 5d13 4000 7706 xxxx d9b8 fea9       E...].@.w.....x
0x0010   xxxx xxxx 0fe0 0050 e0d3 eacb 3c59 9219       xxx....P....<Y..
0x0020   5010 2238 eceb 0000 5345 4152 4348 202f       P."8....SEARCH./
0x0030   9002 b102 b102 b102 b102 b102 b102 b102       ................
0x0040   b102 b102 b102 b102 b102 b102 b102 b102       ................
0x0050   b102 b102 b102 b102 b102 b102 b102 b102       ................
0x0060   b102 b102 b102 b102 b102 b102 b102 b102       ................
0x0070   b102 b102 b102 b102 b102 b102 b102 b102       ................
0x0080   b102 b102 b102 b102 b102 b102 b102 b102       ................
```

```
0x0090   b102 b102 b102 b102 b102 b102 b102 b102        ................
0x00a0   b102 b102 b102 b102 b102 b102 b102 b102        ................
0x00b0   b102 b102 b102 b102 b102 b102 b102 b102        ................
<snip>
```

*> In the "Probability of Spoofing", you might also want to comment that the*
*> packets reported by the windump also appear to be associated with the*
*> analyzed packet since the SYN/SYN ACK/ACK packet time stamps are close*
*> to the time of the specific packet. Remember that that IP and port combination*
*> is not necessarily unique. However with time correlation, you can then match*
*> up the alert with the original SYN packet.*
Correct. I forgot to write this.

*> Is the packet/session crafted in any way, other than the payload? Is the*
*> TTL reasonable? I'm not saying it isn't, but it is something that you might*
*> want to state in the paper*.
From the Snort alert:
08/26-17:57:17.112865 217.184.254.169:4064 -> xxx.xxx.xxx.79:80
TCP TTL:119 TOS:0x0 ID:23827 IpLen:20 DgmLen:1500 DF
The TTL was 119.
I did a tracroute back to this IP address. The result was 9 hops.
TTL from 119+9 =128. This is a reasonable initial TTL value.
Through the results from p0f it is probably that the attackers
machine was a Windows System.
<Thu Aug 26 17:57:16 2004> 217.184.254.169:4064 - Windows XP, 2000 SP2+
-> xxx.xxx.xxx.79:80 (distance 9, link: ethernet/modem)
In the List of fingerprints for passive fingerprint monitoring from the Honeynet Project (lance@spitzner.net) exist 5 entries for OS with a TTL from over 119.

| | |
|---|---|
| Netware | 128 |
| Windows 9x/NT | 128 |
| Windows 2000 | 128 |
| Cisco 12.0 | 255 |
| Solaris 2.x | 255 |

Cisco and Solaris are to far away. So for me the TTL is reasonable and fits to the result from p0f.

*> Go into detail on how this "OVERSIZE REQUEST-URI DIRECTORY" can*
*> cause a system to be compromised.*

An excellent description wrote Blaine Hein.
http://www.dshield.org/pipermail/intrusions/2004-April/007910.php

The http data field within this packet starts with the string "SEARCH /" which conforms to the http method encoding standard. Therefore, the rule "Bare Byte Unicode Encoding" does not fire. While the HTTP method "search" in this packet is not in the HTTP 1.1 Specification, it is included in the "Web-based Distributed Authoring and Versioning" (WebDAV) specification.
However, the length of the http data field is larger than the configured maximum for a directory query.
This triggers the "OVERSIZE REQUEST-URI DIRECTORY."

The HTTP 1.1 Specification can be found in RFC 2616.
The WebDAV related RFC's are 2518, 3648 and 3253

The for me best follow up is from (This was in my reference list)
http://xforce.iss.net/xforce/xfdb/11533
WebDAV is an extension to the HTTP 1.1 protocol to add distributed authoring and version control to Web content. An overflow in a path conversion function occurs within NtDLL, which is called from a common API exported from the Kernel32 library. However, the specific API in question is reachable through the WebDAV component of IIS 5.0. Exploitation will yield local SYSTEM privileges on vulnerable IIS servers. Since the vulnerability is in an underlying library function and not within the IIS server, it is conceivable that other portions of the IIS server or completely unrelated services might also be affected.

I will here not describe how a buffer overflow works.
But here are a two very good links:
http://www.linuxjournal.com/article.php?sid=6701
http://www.cultdeadcow.com/cDc_files/cDc-351/page1.html

*> Was the attempt successful? How can this be found out?*
The attempt was not successful.
Black ICE blocked this attempt. On this machine runs an additional Buffer Overflow Protection from ISS and in this log was nothing.
Before I installed the Buffer Overflow Protection made I a hash over the complete HD with http://md5deep.sourceforge.net/. I booted from a Knoppix CD http://knoppix-std.org/ to catch all files. If you execute md5sum during Windows is running the access to several files will be blocked from Windows. I run two days after this attack again from the CD md5deep over the complete HD. I compared both files and nothing was changed. On this machine run as well an every day updated Virus Scanner from F-Secure. Trough the possibility that this was a worm checked I the logs from the scanner. Nothing was in it. I tested at least with Nessus (http://www.nessus.org) and this nasl (iis_webdav_overflow.nasl and webdav_iss.nasl) if this system was vulnerable. It was not.

## Part 3 Analyze This

Execute Summary:

This summary report based on 3 different data files from a Network Intrusion Detection System. These files represent a summary over 5 sequential days from a Snort IDS that was placed on a GIAC University. The version from Snort was unknown. Every alert file contains information over possible alerts and additional port scan status reports. The scan files contain information over port scans against the MY.NET network (GIAC University). The OOS are “Out of Specification” information, i.e. these are suspicious packets but these may not necessarily be attacks. Other valued information (i.e. config Files from the IDS, contact persons, network diagrams,….) was not available. Additional to this fact of less information was the huge amount from data a quite challenge.
Anyhow was it possible to find real interesting security relevant things in the noise. Based on the available information I could made security defensive recommendation that should help the University to improve their security. Through the 75 page side limit was it only possible to cover the important things.

Files Analyzed:

All files are downloaded from http://isc.sans.org/logs/

| Alert Files | MD5 Hash |
|---|---|
| alert.040303 | 136e33f04686ac39cffb158eba8beabb |
| alert.040304 | f2aa0df1e6c111c9afdaf03ee0864361 |
| alert.040305 | E2a8835ec15d26e544e87e0e6ed994fc |
| alert.040306 | 1fe54f0ee36acbeb5bb23bc95b21a5c7 |
| alert.040307 | af13d2aa7098e08b88ee554be2cc7eae |

| Scan Files | MD5 Hash |
|---|---|
| scans.040303 | 886a134f0e0bae572eacd82dd8044f4b |
| scans.040304 | 6c244d03ea1b358b9a1316d1551d817c |
| scans.040305 | Ff66591ca8e939f646dcf7a9b137f818 |
| scans.040306 | ee610afcec649f80880961cd5cdb625a |
| scans.040307 | 4a6aff8ffd3f3c989908d82cacd2a07d |

| OOS Files | MD5 Hash |
|---|---|
| OOS_report_040303 | 4d5a0c0ad79c852bb2020d7a9ed7457f |
| OOS_report_040304 | 952921e2f849c2a738085137ebc53ab9 |
| OOS_report_040305 | 9f3c7c7fd0e1ef707d072ebf99e67bf0 |
| OOS_report_040306 | 016e0b855a554c9112eb4db896027a7c |
| OOS_report_040307 | 08efef91e51d80ecad86e260870d9150 |

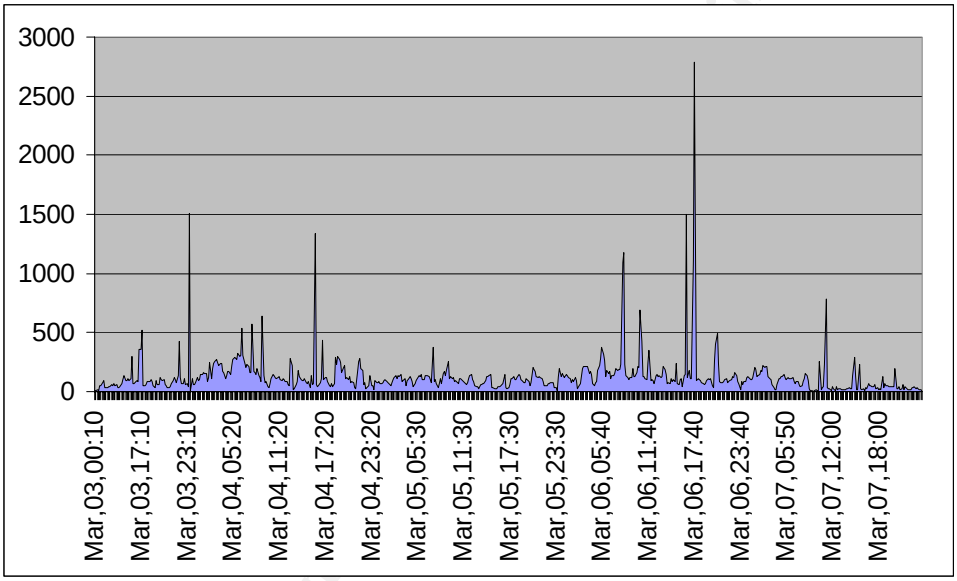
The description how I performed the analysis and which tools I used is in the last section.
A list of information over the analyzed Alerts:

Number of all Alerts sorted by Date:

| | |
|---|---|
| 8278 | March 03, 2004 |
| 22519 | March 04, 2004 |
| 13620 | March 05, 2004 |
| 28707 | March 06, 2004 |
| 10674 | March 07, 2004 |

83798 Totals

A graphical overview over the alerts from the 5 days period:




All Alerts sorted by message type:

| | |
|---|---|
| 17532 | MY.NET.30.4 activity |
| 6478 | SMB Name Wildcard |
| 6310 | MY.NET.30.3 activity |
| 1909 | Incomplete Packet Fragments Discarded |
| 1180 | EXPLOIT x86 NOOP |
| 1140 | [UMBC NIDS IRC Alert] IRC user /kill detected, possible trojan |
| 1049 | SUNRPC high port access! |
| 753 | High port 65535 tcp - possible Red Worm - traffic |
| 625 | NMAP TCP ping! |
| 392 | Null scan! |
| 182 | High port 65535 udp - possible Red Worm - traffic |
| 137 | IRC evil - running XDCC |



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | |
|---|---|
| 83 | TCP SRC and DST outside network |
| 77 | SMB C access |
| 66 | Possible trojan server activity |
| 54 | TCP SMTP Source Port traffic |
| 51 | FTP passwds attempt |
| 47 | [UMBC NIDS IRC Alert] Possible Incoming XDCC Send Request Detected |
| 44 | EXPLOIT x86 setuid 0 |
| 38 | External RPC call |
| 35 | Tiny Fragments - Possible Hostile Activity |
| 32 | [UMBC NIDS] External MiMail alert |
| 30 | [UMBC NIDS IRC Alert] K\:line'd user detected |
| 28 | connect to 515 from inside |
| 28 | TFTP - Internal TCP connection to external tftp server |
| 24 | connect to 515 from outside |
| 23 | TFTP - Internal UDP connection to external tftp server |
| 23 | EXPLOIT x86 setgid 0 |
| 19 | FTP DoS ftpd globbing |
| 14 | EXPLOIT NTPDX buffer overflow |
| 11 | [UMBC NIDS IRC Alert] User joining XDCC channel detected. Possible XDCC bot |
| 9 | DDOS mstream handler to client |
| 6 | EXPLOIT x86 NOPS |
| 6 | EXPLOIT x86 stealth noop |
| 4 | External FTP to HelpDesk MY.NET.53.29 |
| 4 | SYN-FIN scan! |
| 4 | ICMP SRC and DST outside network |
| 3 | RFB - Possible WinVNC - 010708-1 |
| 3 | External FTP to HelpDesk MY.NET.70.50 |
| 3 | External FTP to HelpDesk MY.NET.70.49 |
| 3 | DDOS shaft client to handler |
| 3 | DDOS mstream client to handler |
| 3 | [UMBC NIDS IRC Alert] User joining Warez channel detected. Possible XDCC bot |
| 2 | NETBIOS NT NULL session |
| 2 | HelpDesk MY.NET.70.49 to External FTP |
| 2 | TFTP - External TCP connection to internal tftp server |
| 1 | NIMDA - Attempt to execute cmd from campus host |
| 1 | Attempted Sun RPC high port access |
| 1 | [UMBC NIDS] Internal MiMail alert |
| 1 | [UMBC NIDS IRC Alert] Possible sdbot floodnet detected attempting to IRC |
| 1 | Probable NMAP fingerprint attempt |
| 1 | TFTP - External UDP connection to internal tftp server |
| Total Alerts: 83798 | Number of unique Alerts: 53 |



Descriptions from the Top 10 Alerts:

***1. MY.NET.30.4 activity***

The 3 most hit destination ports on MY.NET.30.4 were:

- Port 51443 with14325 hits. All source IP addresses came from external networks. That port is normally used from the Novell NetStorage Service. This service should not be available from the Internet.
  Information over NetStorage Installation and Configuration:
  http://www.novell.com/documentation/nw65/index.html?page=/documentation/nw65/confgenu/data/am0oz5z.html
  Overview of NetStorage:
  http://developer.novell.com/research/appnotes/2002/june/03/a0206033.htm

- Port 524 with 1858 hits.
  The Novell Netware Core Protocol (NCP) uses port 524 for all communication between Netware 5 clients-servers and time synchronization between server-server running IP. This is similar to the name resolution service on Microsoft port 137, although more powerful. I assume through the fact that port 524 and 51443 are used this is a Novell operating system. If it is, then is a NCP requestor (Client) able to compromise a Novell server, especially if NDS or Bindery authentication were known. It will allow Internet access to a Novell file server if this server has IP access enabled. That should always be disabled! If the port 524 is open, and the [PUBLIC] object has browse rights to the NDS tree, then enumerating information is also possible.

  Information regarding Ports and Protocols used by NetWare 5.X and 6.X:
  http://support.novell.com/cgi-bin/search/searchtid.cgi?/10013531.htm
  In rare case this port is also used from Linux with a web server and the NCP services.
  http://www.linux-magazin.de/Service/Books/Buecher/Netzwerk/netz1502.htm
  http://www.faqs.org/docs/linux_network/x11757.html

- Port 80 with 1261hits.
  I found information that Novell NetStorage (probably on port 51443 for this machine) installs an Apache web server by default during the NetWare installation. The connections to the web server can be normal and these alerts are possibly from a web spider from a search machine? It is necessary to verify this further (e.g. with checking from the web server log files).

The Top 5 source IP addresses were:

| Count | Source IP | Name or Info |
|---|---|---|
| 8710 | 68.50.102.64 | bgp01546912bgs.longhl01.md.comcast.net |
| 1710 | 68.55.191.197 | pcp05510211pcs.owngsm01.md.comcast.net |
| 963 | 63.159.88.57 | 0-1pool88-57.nas26.vienna1.va.us.da.qwest.net |
| 661 | 68.33.138.193 | No DNS entry but belong also to Comcast Cable Communications, Inc. |
| 593 | 68.55.148.5 | pcp259943pcs.howard01.md.comcast.net |

Total were 17536 alerts counted. Nearly the half came from the single IP (68.50.102.64) with the target port 51443. The time distances were infrequent so



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

that it was probably not an automated access. The same was with the source ports from 68.50.102.64. They are all above 1024 but totally randomized. Purpose from this connection stays unclear.

Recommendation:
I would recommend checking the server for traces of compromise and review the config so that the 'probably' unnecessary internet access to this box gets removed!

Correlation:
http://www.giac.org/practical/Patrik_Sternudd_GCFW.doc
http://www.giac.org/practical/GCIA/Blaine_Hein_GCIA.pdf
http://www.giac.org/practical/GCIA/Marshall_Heilman_GCIA.doc.pdf

### *2. SMB Name Wildcard*

The Top 5 destination IP addresses were:

| Count | Destination IP | Info |
|---|---|---|
| 1405 | 62.166.61.120 | VERSATEL-CUST-VERSNET-ADSL-1 (Whois below) |
| 1305 | MY.NET | |
| 1248 | 169.254.0.0 | IANA |
| 690 | 64.246.65.158 | INTELLISPACE, INC New York |
| 596 | 169.254.45.176 | IANA |

All source IP addresses came from the MY.NET network.

The destination port for these alerts was always 137, the standard Microsoft NETBIOS name service port. The SMB protocol, which is used there, has the purpose to share information over the LAN/WAN. If an attacker can connect to this port, then it is possible to get information about domain, workstation name, etc In the payload from the attack you will normally see the pattern CKAAA. When resolving a name with only the IP address available, windows machines will send these UDP queries as part of normal operations. The CKAAA pattern is generated from the null NetBIOS name "00 00 00", as a wildcard with the translation function being performed to finish the mapping. Port 137 is one of the most attacked ports, statistics over the attack counts can be found under www.dshield.org or www.mynetwatchman.com. A number of vulnerabilities for this port have occurred in the past and many of them are still not fixed. Therefore, this is an easy target for an attacker.

Recommendation:
Modify the snort rule such that only the connections with the Destination MY.NET are monitored. Additional forbid with a firewall rule or with an ACL on a router before MY.NET the outgoing 137 port. I would also check deeper the outgoing connections. The Purpose from this can only be guessed?

Correlation:
Blaine Hein
http://www.dshield.org/pipermail/intrusions/2004-April/007896.php
nreichen at lanexpert.ch
http://www.dshield.org/pipermail/intrusions/2002-October/005508.php
http://www.giac.org/practical/GCIA/Billy_Smith_GCIA.doc

Whois from 62.166.61.120

```
inetnum:      62.166.0.0 - 62.166.63.255
netname:      VERSATEL-CUST-VERSNET-ADSL-1
descr:        Zon internet is one of the largest free ISP in the
Netherlands
country:      NL
status:       ASSIGNED PA
mnt-by:       AS13127-MNT
changed:      hostmaster@versatel.net 20000918
source:       RIPE

route:        62.166.0.0/16
descr:        Versatel customers
origin:       AS13127
notify:       hostmaster@versatel.net
notify:       rob.vanderkooi@versatel.nl
mnt-by:       AS13127-MNT
changed:      marct@versatel.net 20010104
changed:      Hostmaster@versatel.net 20020205

role:         ZONnet Administrator
address:      Hullenbergweg 101
address:      1107 CL  Amsterdam Zuidoost
address:      the Netherlands
phone:         (0)20 7507772
fax-no:        (0)20 7507750
e-mail:       andre.zantingh@versatel.nl
nic-hdl:      ZA134-RIPE
```

The description tells a lot. It is a free ISP in Europe. So Ii is clear that probably no University Partnership is the reason for this access.

### *3. MY.NET.30.3 activity*

6107 from the total count of 6312 connections went to port 524. As the assumption that MY.NET.30.4 is probably a Novell OS and this machine also has the destination port 524 open, this could also be a Novell operating system. This was the same for the MY.NET.30.4 address - all source IP addresses came from external networks.

Here are the Top 5 source IP addresses which connected to MY,NET.30.3:

| Count | Source IP | Info |
|---|---|---|
| 510 | 131.92.177.18 | Army Information Systems Command - Aberdeen US |

| | | |
|---|---|---|
| 454 | 68.55.178.168 | Comcast Cable Communications, Inc. US |
| 310 | 141.157.21.74 | Verizon Internet Services US |
| 301 | 68.34.27.67 | Comcast Cable Communications, Inc. US |
| 298 | 68.55.243.80 | Comcast Cable Communications, Inc. US |

Recommendation:
This is the same question as for MY.NET.30.4, is it necessary that that port 524 is publicly available, or is this machine compromised? I would recommend checking this machine for a compromise as well.

### *4. Incomplete Packet Fragments Discarded*

Top 5 Source IP addresses:

| Count | Source IP | Name or Info |
|---|---|---|
| 725 | MY.NET.21.67 | |
| 697 | MY.NET.21.69 | |
| 231 | MY.NET.21.68 | |
| 151 | MY.NET.21.89 | |
| 9 | 217.225.111.204 | pD9E16FCC.dip.t-dialin.net -> IP from ISP in De |

Top 5 Destination IP addresses:

| Count | Destination IP | Name or Info |
|---|---|---|
| 855 | 213.100.69.160 | c213-100-69-160.swipnet.se |
| 414 | 209.68.61.41 | dankohn.com |
| 214 | 172.185.36.253 | ACB924FD.ipt.aol.com |
| 170 | 199.182.184.45 | as02-okc-ok-199-182-184-45.rasserver.net |
| 9 | MY.NET.153.79 | |

A fragmentation occurs normally only when a packet is too large for one of the devices between sender and receiver, or for the receiver. This will then be split and sent in several smaller packets.
From:
http://www.linuxsecurity.com/docs/Hack-FAQ/data-networks/packet-fragmentation.shtml
Every network has an MTU (Maximum Transmission Unit) size. The MTU is the size of the largest packet that network can transmit. Packets larger than the allowable MTU size must be broken down into multiple smaller packets, or fragments, to enable them to traverse the network. Packet Fragmentation Attacks are described here as well. This alert was not triggered from a Snort alert rule. It is triggered trough the Snort defrag preprocessor which must be enabled in the Snort config file.

The output seems to come from the old Snort defrag preprocessor (Marty Roesch)
http://marc.theaimsgroup.com/?l=snort-users&m=100681596629407&w=2



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The alerts can also have other reasons instead of attacks. I found in the snort mailing list the following comment:
http://marc.theaimsgroup.com/?l=snort-users&m=98201599426605&w=2
"This can be caused by:
- transmission errors
- broken stacks
- and fragmentation attacks"

Recommendation:
1804 from 1909 alerts came from the internal MY.NET network.
I would first recommend installing a newer version from Snort and then to use the new frag2 preprocessor. After this I would check if these alerts still occur. I would also check if the router/switches in front of MY.NET are properly configured, as these devices may discard the packets. In some rarer cases a streaming protocol may cause these alerts.

Correlation:
http://www.giac.org/practical/GCIA/Vance_Victorino_GCIA.pdf

### *5. EXPLOIT x86 NOOP*

There were 1180 alerts from 479 different attackers. All IP addresses came from external networks.
The Top 5 source IP addresses:

| Count | Source IP | Name or Info |
|---|---|---|
| 665 | 161.53.66.27 | krov.zvne.fer.hr (Whois below) |
| 148 | 142.150.80.236 | walid-bioinfo.med.utoronto.ca |
| 105 | 80.145.59.11 | p50913B0B.dip.t-dialin.net |
| 18 | 131.118.254.130 | news.ums.edu |
| 13 | 128.8.10.18 | grapevine.wam.umd.edu |

The Top 5 destinations IP addresses:
(All destination addresses were from MY.NET):

| Count | Destination IP |
|---|---|
| 604 | MY.NET.42.5:80 |
| 148 | MY.NET.150.67:80 |
| 104 | MY.NET.5.25:80 |
| 49 | MY.NET.190.93:135 |
| 42 | MY.NET.112.226:80 |

A description what this alert indicates:
The rule triggers if a buffer overflow attack seems to occur. Therefore Snort searches in the data stream (payload) for the character 0x90 as this represents a NOOP (No operation) instruction. NOOP is used in a buffer overflow because it is not exactly known where the code execution on the attacked system will begin.

The Snort rule which triggers this event was:
*alert any $EXTERNAL_NET any -> $HOME_NET any (msg:"EXPLOIT x86 NOOP"; content:"|90 90 90 90 90 90 90 90 90 90 90 90 90 90|";)*
This was part of the old Snort rule set and this version should not longer be used. In the new 2.2.0 Version this rule no longer exists in this form. It is improved and can be found in the shellcode.rules and exploit.rules.

In my experience, this was the signature that produced the most "false positives", especially with huge http or ftp downloads.

Definition of a Buffer overflow:
http://www.wordiq.com/definition/Buffer_overflow
One of the best papers to this theme:
Smashing The Stack For Fun And Profit
http://www.phrack.org/show.php?p=49&a=14

Recommendation:
Independently from my experience with the false positives, I would recommend at least checking the top 5 targets from the attack list for traces from evil stuff.

Correlation:
http://www.giac.org/practical/GCIA/Bruce_Auburn_GCIA.pdf

Whois from IP: 161.53.66.27 (krov.zvne.fer.hr). It was only connections to 3 different web server (31x MY.NET.112.226:80, 30x MY.NET.150.67:80, 604x MY.NET.42.5:80). If I calculate with the time difference from Europe to US (6 hours) happens this during normal study times at a European University. After a look to the space between the connections, the sequencing between the 3 servers and the used source ports is this source IP suspicious for me. It does not look how a search on the MY.NET websites or a download from there.
This IP does not appear in www.dshield.org or www.mynetwatchman.com.

```
inetnum:      161.53.0.0 - 161.53.255.255
descr:        University Computing Centre
descr:        SRCE, Prisavlje bb, 41000 Zagreb, Croatia
admin-c:      MI286-RIPE
tech-c:       MI286-RIPE
netname:      CARNET
descr:        Croatian Academic and Research Network (CARNet)
country:      HR
status:       ASSIGNED PA
admin-c:      CNIP1-RIPE
tech-c:       CNIP1-RIPE
mnt-by:       AS2108-MNT
changed:      er-transfer@ripe.net 20040218
route:        161.53.0.0/16
origin:       AS2108
mnt-by:       AS2108-MNT
```



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
source:       RIPE

role:         CARNet IP address administrator
address:      J.Marohnica bb
address:      10000 Zagreb
address:      Croatia
phone:        +385 1 6165 520
fax-no:       +385 1 6165 559
e-mail:       net-admin@carnet.hr
nic-hdl:      CNIP1-RIPE
```

### *6. [UMBC NIDS IRC Alert] IRC user /kill detected*

Top 5 source IP addresses:
All source IP addresses are from external networks.

| Count | Source IP | Destination IP addresses |
|---|---|---|
| 936 | 209.126.201.99 (Whois below) | 930 x MY.NET.27.103, 6 x MY.NET.80.5 |
| 90 | 65.248.51.47 | 90 x MY.NET.42.3 |
| 19 | 69.50.189.88 | 6 different MY.NET |
| 8 | 203.56.139.100 | 3 different MY.NET |
| 7 | 69.28.250.108 | 2 different MY.NET |

Top 5 destination IP addresses:
All destination IP addresses are going to MY.NET.

| Count | Destination IP |
|---|---|
| 930 | MY.NET.27.103 |
| 96 | MY.NET.42.3 |
| 22 | MY.NET.42.5 |
| 17 | MY.NET.42.2 |
| 13 | MY.NET.42.4 |

Recommendation:
These alerts are not generated from any default snort rule set. I assume that this rule was written from the stuff from the MY.NET University. Trough this fact could I only speculate for the purpose of this rule. Maybe because the IRC protocol is under students very popular and problems in the past occur? The /Kill command disconnects an IRC user from the IRC server. On the other hand the used source ports special the ports, 6669, 7000 are typical Trojans ports. Check the destination hosts for traces from compromises.

Information over IRC and the Kill command:
Kill message
http://www.valinor.sorcery.net/docs/rfc2812/3.7.1-kill-message.html
http://cwrulug.cwru.edu/talks/irc/irc3.html (More advanced IRC commands)
http://www.ircbeginner.com/ircinfo/h-klines.html
SANS IDS FAQ. What port numbers do well-known Trojan horses use?



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

http://www.sans.org/resources/idfaq/oddports.php

Correlation:
http://www.giac.org/practical/GCIA/Don_Murdoch_GCIA.pdf
http://www.giac.org/practical/GCIA/Ben_Allen_GCIA.pdf

Whois from IP: 209.126.201.99 (desire.of.hotgirlz.org)
The name of the source IP with the most connections sounds very dubious. In the moment the side is no longer available and the only referential what I found was under the address: http://www.shell.web.id/vhost.txt. On this site the offer dubious Domain names that you can use for vhosts (One is desire.of.hotgirlz.org). A Whois shows me that the company to which the site www.shell.web.id belongs came from Indonesia. http://www.vip.net.id/ It is an ISP. I could not identify which relationship exists between the US ISP and the ISP in Indonesia. This IP does not appear in www.dshield.org or www.mynetwatchman.com.

The Whois from 209.126.201.99.

```
OrgName:    California Regional Internet, Inc.
OrgID:      CALI
Address:    8929A COMPLEX DRIVE
City:       SAN DIEGO
StateProv:  CA
PostalCode: 92123
Country:    US

NetRange:   209.126.128.0 - 209.126.255.255
CIDR:       209.126.128.0/17
NetName:    CARI
NetHandle:  NET-209-126-128-0-1
Parent:     NET-209-0-0-0-0
NetType:    Direct Allocation
NameServer: NS1.ASPADMIN.COM
NameServer: NS2.ASPADMIN.COM
RegDate:    1999-03-12
Updated:    2003-07-01

TechHandle: IC63-ARIN
TechName:   California Regional Intranet, Inc.
TechPhone:  +1-858-974-5080
TechEmail:  sysadmin@cari.net

OrgTechHandle: SYSAD5-ARIN
OrgTechName:   sysadmin
OrgTechPhone:  +1-858-974-5080
OrgTechEmail:  sysadmin@cari.net
```




© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

### *7. SUNRPC high port access!*

All connections go to the port 32771. This high port is often used from Sun Solaris for RPC services additional to the traditional portmapper port 111. It is also called *Ghost portmapper*. On this port listens then the rpcbind application.

Top 5 Destination addresses:

| Count | Destination IP |
|---|---|
| 570 | MY.NET.70.247 |
| 328 | MY.NET.82.61 |
| 53 | MY.NET.97.80 |
| 21 | MY.NET.25.70 |
| 6 | MY.NET.97.108 |

Top 5 Source addresses:

| Count | Source IP | Name or Info |
|---|---|---|
| 522 | 128.2.194.60 | openafs.org |
| 328 | 128.193.0.3 | ftp-old.oregonstate.edu |
| 53 | 207.242.93.22 | wwwa.accuweather.com |
| 47 | 66.187.232.50 | Red Hat, Inc |
| 8 | 213.87.4.1 | www.mts.ru |

Recommendation:
A few firewalls/router often do not filter at high ports and this can allow the attacker access to portmapper even when the port 111 is blocked. The SUN RPC service is since a long time in the top 5 from vulnerabilities from the FBI and SANS. This port should never be open to the internet because it offers a lot of reconnaissance information.
Check all these systems for compromises and be sure that all machines are on the last possible patch level.

Information:
SANS Intrusion Detection FAQ. The trouble with RPC's.
http://www.sans.org/resources/idfaq/trouble_rpcs.php
http://www.uni-duesseldorf.de/~cappel/betriebs-kurs/node40.html
http://probing.csx.cam.ac.uk/about/sunrpc.html
http://www.ietf.org/rfc/rfc1057.txt (Remote Procedure Call)
Is blocking port 111 sufficient to protect your systems from RPC attacks?
http://www.sans.org/resources/idfaq/blocking.php

Correlation:
http://www.giac.org/practical/GCIA/John_Melvin_GCIA.pdf

### *8. High port 65535 tcp - possible Red Worm – traffic*

This vulnerability affects Linux Systems. The Red Worm scans for weaknesses in the services from BIND named, wu-ftpd, rpc.statd and lpd services. If these boxes are vulnerable then uses the worm this and installed a backdoor on it. This backdoor listens on port 65535 for a special crafted ping packet. This packet opens the backdoor a shell. There are several different versions in the wild.

Adore Worm
http://www.sans.org/y2k/adore.htm
http://www.f-secure.com/v-descs/adore.shtml

Top 5 destination IP addresses:

| Count | Destination IP | Name or Info |
|---|---|---|
| 195 | MY.NET.12.6 | |
| 29 | 69.6.68.10 | noname.wholesalebandwidth.com (Whois below) |
| 33 | MY.NET.53.56 | |
| 27 | 206.35.36.4 | Cambridge Health Alliance |
| 26 | 64.12.26.136 | America Online, Inc. |

Top 5 source IP addresses:

| Count | Source IP | Name or Info |
|---|---|---|
| 191 | 64.12.137.7 | imo-m26.mx.aol.com |
| 41 | MY.NET.24.44 | |
| 31 | 64.12.26.136 | America Online, Inc. |
| 30 | MY.NET.25.68 | |
| 28 | MY.NET.12.6 | |

The probably problem from these alerts is that the signature which triggers these alerts only looks for the use from the high port 65535. Therefore can false positives occur.

Recommendation:
Use a scanner how http://www.nessus.org to check the complete MY.NET network for vulnerable machines. If some are found clean them and patch this immediately. This vulnerability is old (Starts April 2001) and should not longer happen today in a good watched network! All Vendors had delivered patches in a very short timeframe. If a machine is infected is it possible to clean the worm with a virus scanner.

Correlation:
http://www.giac.org/practical/GCIA/Doug_Kite_GCIA.pdf
http://www.giac.org/practical/GCIA/Shakeel_Akhter_GCIA.pdf
http://www.giac.org/practical/GCIA/Al_Williams_GCIA.pdf



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Whois IP 69.6.68.10:

This IP does not appear in www.dshield.org or www.mynetwatchman.com.

```
OrgName:    Internet Access Group, Inc.
OrgID:      IAG-17
Address:    PO Box 12963
City:       Austin
StateProv:  TX
PostalCode: 78711-2963
Country:    US
NetRange:   69.6.68.0 - 69.6.68.255
CIDR:       69.6.68.0/24
NetName:    INTACC-BLK-69-6-68-0
NetHandle:  NET-69-6-68-0-1
Parent:     NET-69-6-0-0-1
NetType:    Reassigned
NameServer: NS1.WHOLESALEBANDWIDTH.COM
NameServer: NS2.WHOLESALEBANDWIDTH.COM
Comment:
RegDate:    2004-07-20
Updated:    2004-07-20

OrgTechHandle: TECHN151-ARIN
OrgTechName:   Technical Dept
OrgTechPhone:  +1-512-473-8266
OrgTechEmail:  admin@internetaccessgroup.com

# ARIN WHOIS database, last updated 2004-10-04 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

### *9. NMAP TCP ping!*

That Snort rule set is in the actual Version (2.2.0) deleted.
But a description can be still found in the deleted.rules.
From there:

*deleted.rules,v 1.33.2.2 2004/08/10*
*# These signatures have been deleted for various reasons, but we are keeping*
*# them here for historical purposes.*

*#nmap is no longer as dumb as it once was...*
*alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap TCP"; ack:0; flags:A,12; flow:stateless; reference:arachnids,28; classtype:attempted-recon; sid:628; rev:7;)*

Here is it good viewable that this rule was triggered when the attack packet has the ACK flag set and additional the ACK field is 0.

After a quick look to the first 2 destination IP addresses and the used ports thought I this was DNS traffic and a false positive.

The Top 5 destination IP addresses were:

| Count | Destination IP and port |
|---|---|
| 317 | MY.NET.1.3:53 |
| 52 | MY.NET.1.5:53 |

| | |
|---|---|
| 47 | MY.NET.12.4:143 |
| 35 | MY.NET.34.11:80 |
| 24 | MY.NET.1.4:53 |

On the second view including a correlation with the sources IP addresses and other GIAC practical becomes it as well possible that this was file sharing traffic.

The Top 5 source IP addresses:

| Count | Source IP and port | Name |
|---|---|---|
| 92 | 64.152.70.68:80 | proximitycheck2.allmusic.com |
| 83 | 63.211.17.228:80 | proximitycheck2.allmusic.com |
| 78 | 64.152.70.68:53 | proximitycheck1.allmusic.com |
| 69 | 63.211.17.228:53 | proximitycheck1.allmusic.com |
| 28 | 216.5.176.162:80 | Allegiance Telecom Companies |

Correlation:
http://www.giac.org/practical/Tod_Beardsley_GCIA.doc
Tod Beardsley pointed out that the KaZaaA file sharing network also demonstrates this behavior. He mentions as well that this occur only with nmap version older then 2.54BETA2. These alerts are probably not triggered from scans because the nmap version 2.54BETA2 is very old and at the time where these alerts were generated was still nmap 3.x version alive. I assume that they came all from file sharing which is very popular on Universities.
I could verify with a nslookup and set type=ms that MY.NET1.3/4/5 are all public reachable DNS Server from MY.NET. I think because of no other signs from compromises in the alert, scan or OOS files for this destination IP's is it more likely that this legitimate traffic.

Recommendation:
Upgrade Snort to the newest version and be sure (Independent from the real reason) that the Users of the University network are informed via a policy and aware that file sharing can cause legal issues. Fine tune the snort rules for the DNS Traffic.

### *10. Null scan!*

This type of scan is absolute best described in the "man nmap":
*The Null scan turns off all flags. Unfortunately Microsoft (like usual) decided to completely ignore the standard and do things their own way. Thus this scan type will not work against systems running Windows95/NT. On the positive side, this is a good way to distinguish between the two platforms. If the scan finds open ports, you know the machine is not a Windows box. If a -sF, -sX, or -sN scan shows all ports closed, yet a SYN (-sS) scan shows ports being opened, you are probably looking at a Windows box. This is less useful now that nmap has proper OS detection built in. There are also a few other systems that are broken in the same way Windows is. They include Cisco, BSDI,*



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

*HP/UX, MVS, and IRIX. All of the above send resets from the open ports when they should just drop the packet.*

Top 5 source IP addresses (attackers):

| Count | Source IP | Name or Info |
|---|---|---|
| 84 | 68.122.128.1 (Whois below) | adsl-68-122-128-1.dsl.sndg02.pacbell.net |
| 78 | 63.251.52.75 | www.shockwave.com(Game site) |
| 25 | 217.0.157.58 | ISP Deutsche Telekom AG |
| 25 | 130.94.123.236 | mailer-ext.lindows.com |
| 11 | 195.10.45.152 | hide-152.nhs.uk |

Top 5 destination IP addresses:

| Count | Destination IP |
|---|---|
| 85 | MY.NET.12.4 (Only to port 110) |
| 79 | MY.NET.66.31 |
| 65 | MY.NET.12.6 |
| 26 | MY.NET.84.235 |
| 12 | MY.NET.11.4 |

References:
RFC 793 TRANSMISSION CONTROL PROTOCOL
http://www.insecure.org/nmap
http://www.linux-magazin.de/Artikel/ausgabe/2000/12/SnortNmap/SnortNmap.html

Recommendation:
To get scanned is not possibly to avoid for public reachable machines. The only thing what can be done is to secure these machines as good as possible. As well would I recommend to use only so less as possible machines which are public reachable. Every further public obtainable machine increases the risk. At least with the information from Snort or other IDS Systems would I inform the ISP from where the scanning IP addresses are coming about this evil activity
.
Correlation:
http://www.giac.org/practical/GCIA/John_Melvin_GCIA.pdf
http://www.giac.org/practical/GCIA/Darrin_Wassom_GCIA.pdf

Additional Information:
All connection from the source IP address with the highest count went to MY.NET.12.4 port 110 (POP3). I found in the OOS files more Information.
One example:

```
03/07-00:19:43.152662 68.122.128.1:60440 -> MY.NET.12.4:110
TCP TTL:78 TOS:0x0 ID:4660 IpLen:20 DgmLen:40
******** Seq: 0xA799001  Ack: 0x71A1E2F5  Win: 0x800  TcpLen: 20
```

It is good to see that this packet (For all other was it the same) has no flags.

In the scan files I found further scan attempts (Example):

```
Mar  4 03:56:38 68.122.128.1:12312 -> MY.NET.12.4:110 SYN ******S*
Mar  4 03:56:38 68.122.128.1:12312 -> MY.NET.12.4:110 NULL ********
```

Whois 68.122.128.1 (adsl-68-122-128-1.dsl.sndg02.pacbell.net)

```
CustName:   PPPoX Pool - Rback3 SNDG02
Address:    268 Bush St #5000
City:       San Francisco
StateProv:  CA
PostalCode: 94104
Country:    US
RegDate:    2003-07-14
Updated:    2003-07-14

NetRange:   68.122.128.0 - 68.122.129.255
CIDR:       68.122.128.0/23
NetName:    SBC068122128000030714
NetHandle:  NET-68-122-128-0-1
Parent:     NET-68-120-0-0-1
NetType:    Reassigned
RegDate:    2003-07-14
Updated:    2003-07-14

OrgNOCHandle: SPBI-ARIN
OrgNOCName:   Support - Pacific Bell Internet
OrgNOCPhone:  877-722-3755
OrgNOCEmail:  support@pacbell.net
```



**Top 10 Talkers (Alerts, scans and OOS):**

| Alerts by Source IP (Internal Only) | Count | Additional short Info |
|---|---|---|
| MY.NET.27.103 | 45325 | All connects to 209.126.201.99 (possible Trojan or IRC) |
| MY.NET.190.97 | 1415 | All destination ports are 135,137,139 and 445 (MS Traffic) |
| MY.NET.70.37 | 1299 | Seems to be a Solaris OS with RPC. Maybe Samba? |
| MY.NET.11.7 | 1151 | All alerts because MY.NET.11.7:137 -> 169.254.0.0:137 |
| MY.NET.21.67 | 725 | Incomplete Packet Fragments Disc. to 5 public IP addresses |
| MY.NET.21.69 | 697 | Is the same how for above |
| MY.NET.190.93 | 484 | Many EXPLOIT x86 NOOP attempts (seems Microsoft-OS) |
| MY.NET.75.13 | 361 | Possible trojan server activity. Other only port 137 connects |
| MY.NET.190.92 | 343 | Nearly all SMB Name Wildcard alerts with destination port 137. All alerts was nearly with several destination IP's |
| MY.NET.150.198 | 267 | All was SMB Name Wildcard alerts. |

| Alerts by Source IP (External Only) | Count | Additional short Info |
|---|---|---|
| 68.50.102.64 | 8708 | Only connections to MY.NET.30.4 port 80 and 51443<br>*bgp01546912bgs.longhl01.md.comcast.net -> ISP* |

| | | |
|---|---|---|
| 68.55.191.197 | 1710 | Only connections to MY.NET.30.4 port 80 and 51443 *pcp05510211pcs.owngsm01.md.comcast.net* |
| 68.34.27.67 | 1518 | Only connections to MY.NET.30.3:524 *pcp09629026pcs.frnkmd01.md.comcast.net* |
| 68.55.250.229 | 1256 | Only connections to MY.NET.30.3 and 30.4 Dst. port 524 *pcp261188pcs.howard01.md.comcast.net* |
| 63.159.88.57 | 963 | Only connections to MY.NET.30.4 port 80 and 51443 *0-1pool88-57.nas26.vienna1.va.us.da.qwest.net* |
| 68.55.148.5 | 860 | Only connections to MY.NET.30.3 and 30.4 Dst. port 524 *pcp259943pcs.howard01.md.comcast.net* |
| 161.53.66.27 | 665 | Only EXPLOIT x86 NOOP to different MY.NET IP's port 80 *Croatian Academic and Research Network (CARNet)* |
| 68.33.138.193 | 660 | Only connections to MY.NET.30.4 port 80 and 51443 *Comcast Cable Communications, Inc.* |
| 141.157.21.74 | 642 | 99% connections gone to MY.NET.30.3:524 (30.3:3019) *SRC IP is from Verizon Internet Services* |
| 128.2.194.60 | 522 | All connections to MY.NET.70.247:32771 (SUNRPC highport access!) *Source. IP is from Carnegie Mellon University* |

The red tagged IP is recognized from www.dshield.org and www.mynetwatchman.com as attacker.

| Scans Top 10 Source IP (External Only) | Count | Additional short Info (If assumption is possible and realistic) |
|---|---|---|
| MY.NET.1.3 | 2201304 | Connected Ports 53, 113 -> 1. DNS Server MY.NET |
| MY.NET.110.72 | 246730 | |
| MY.NET.1.4 | 237541 | Connected Ports 53, 113 -> 2. DNS Server MY.NET |
| MY.NET.53.169 | 236881 | Many outgoing Gnutella Connections |
| MY.NET.34.14 | 144770 | Connected Ports 25, 113 -> Mail Server MY.NET? |
| MY.NET.81.39 | 141837 | All to destination port 135 (Several IP's) |
| MY.NET.80.224 | 112616 | All to destination port 135 (Several IP's) |
| MY.NET.112.216 | 63539 | |
| MY.NET.153.79 | 55904 | Many connections to port 4662 (often used for file sharing) |
| MY.NET.97.74 | 48816 | Many outgoing Gnutella Connections |

I could verify with a simple nslookup and a set type=ns that MY.NET.1.3, MY.NET1.4 and MY.NET1.5 are the Name server for MY.NET.

| Scans Top 10 by Dst. IP (External Only) | Count | Additional short Info (If assumption is possible and realistic) |
|---|---|---|
| 69.6.68.10 | 44345 | Nearly all from MY.NET.1.3 -> 69.6.68.10:53. A few from MY.NET.25.69 -> 69.6.68.10:25 (Both WholesaleBandwidth) |
| 69.6.68.11 | 43773 | All from MY.NET.1.3 -> 69.6.68.11:53 (WholesaleBandwidth) |
| 192.26.92.30 | 39679 | All from MY.NET.1.3 -> 192.26.92.30:53 (c.gtld-servers.net) |
| MY.NET.25.70 | 36816 | |
| 192.48.79.30 | 33891 | All from MY.NET.1.3 -> 192.48.79.30:53 (VeriSign Global Registry Services) |
| 203.20.52.5 | 30718 | All from MY.NET.1.3 -> 203.20.52.5:53 (Company DNS Server) |
| 4.13.52.66 | 27231 | wbar6.dal1-4-13-052-066.dsl-verizon.net |
| 192.5.6.30 | 25391 | All from MY.NET.1.3 -> 192.5.6.30:53 (VeriSign Global Registry Services) |

| | | |
|---|---|---|
| 192.52.178.30 | 24272 | All from MY.NET.1.3 -> 192.52.178.30:53 (k.gtld-servers.net) |
| 216.109.116.17 | 22917 | All from MY.NET1.3 -> 216.109.116.17:53 (ns5.yahoo.com) |

It seems that the most of this recorded scan activities occur through normal DNS traffic. That should be customized in the Snort rule set.

| OOS Destination IP with port | Count | Additional short Info (If assumption is possible and realistic) |
|---|---|---|
| MY.NET.6.7:110 | 746 | All from 68.54.84.49:56557 to port110. Seems Pop3 Server |
| MY.NET.12.6:25 | 542 | Several different ext. IP's all to port 25. Is Mail Server |
| MY.NET.6.47:25 | 210 | Several different IP's all to port 25. Seems Mail Server |
| MY.NET.24.44:80 | 180 | Seems Web Server. Only Syn Flags recorded |
| MY.NET.153.79:4662 | 146 | From http://www.overnet.com/documentation/donkeyfaq.html Donkey uses port 4662 to connect to other clients. |
| MY.NET.12.7:443 | 103 | Only internal MY.NET connections from 199.158 -> 12.7 |
| MY.NET.24.34:80 | 79 | Web server with internal and external requests |
| MY.NET.12.4:110 | 40 | Pop3 and IMAP Server |
| MY.NET.6.7:80 | 36 | Seems additional to POP3 server a Web server |
| MY.NET.34.11:80 | 30 | Only Syn Flags to port 80 recorded |

I could verify with a simple nslookup and a set type=mx that MY.NET.12.6 is a mail Server.

| OOS Source IP with port | Count | Additional short Info |
|---|---|---|
| 68.54.84.49:110 | 764 | pcp01741335pcs.howard01.md.comcast.net |
| 217.125.5.139:4662 | 131 | 139.Red-217-125-5.pooles.rima-tde.net |
| MY.NET.199.138:443 | 77 | |
| 67.114.19.186:80 | 73 | adsl-67-114-19-186.dsl.pltn13.pacbell.net |
| 66.225.198.20:25 | 65 | Server Central Network -> ISP |
| MY.NET.199.158:80 | 44 | |
| 68.122.128.1:110 | 40 | adsl-68-122-128-1.dsl.sndg02.pacbell.net |
| 35.8.2.252:25 | 33 | Michigan State University |
| MY.NET.199.158:443 | 30 | |
| MY.NET.199.138:80 | 28 | |

The red tagged IP is recognized from www.dshield.org and www.mynetwatchman.com as attacker.

**A list of additional information from the analyzed Scans and OOS files:**

Scans sorted by type:

| | |
|---|---|
| 3239246 | UDP scan (Externally-based) |
| 1351394 | SYN scan (Externally-based) |
| 12893 | FIN scan (Externally-based) |
| 1100 | INVALID ACK scan (Externally-based) |
| 262 | NULL scan (Externally-based) |
| 218 | NOACK scan (Externally-based) |
| 161 | UNKNOWN scan (Externally-based) |
| 54 | VECNA scan (Externally-based) |



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

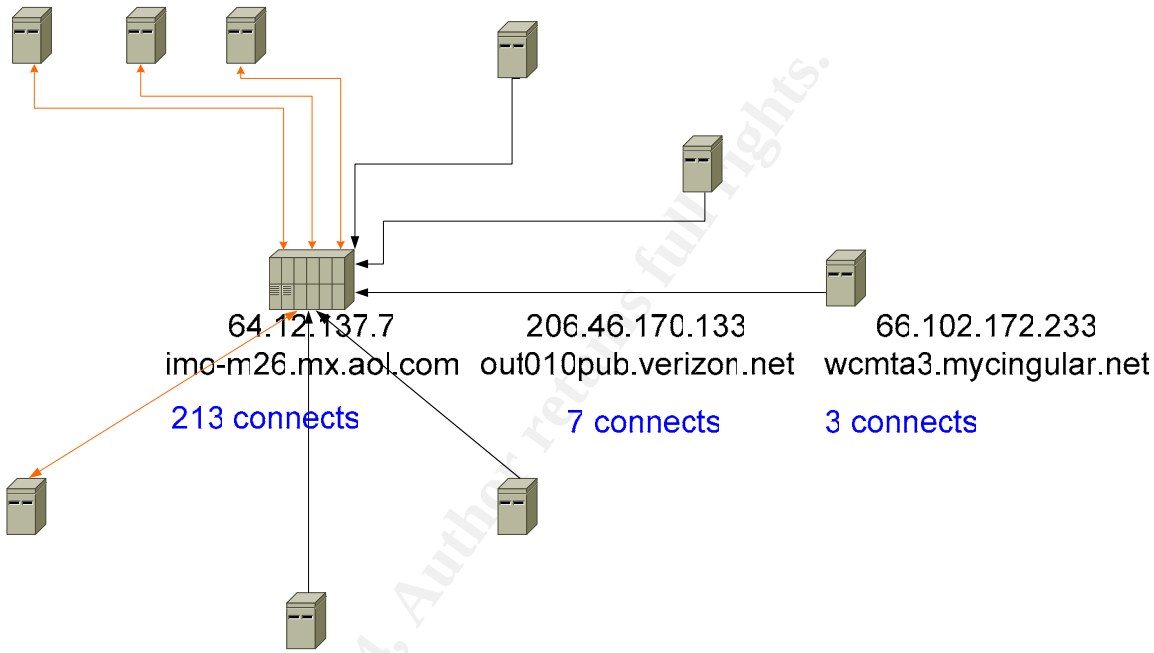
| | |
|---|---|
| 11<br>10<br>10<br>8<br>8 | XMAS scan (Externally-based)<br>SYNFIN scan (Externally-based)<br>FULLXMAS scan (Externally-based)<br>NMAPID scan (Externally-based)<br>SPAU scan (Externally-based) |
| Total amount from scans:<br>4605384 | |

| Flags from OOS files | Count | Flags from OOS files | Count |
|---|---|---|---|
| flags: 12****S* | 2216 | flags: 12*A*RSF | 1 |
| flags: ******** | 55 | flags: 12UAP*SF | 1 |
| flags: 12***R** | 5 | flags: ****PRSF | 1 |
| flags: **U***** | 3 | flags: 12UA**SF | 1 |
| flags: 12U**RS* | 3 | flags: *2UAP*SF | 1 |
| flags: 12UAPRSF | 2 | flags: *2UA*RSF | 1 |
| flags: 12UA*RSF | 2 | flags: 12**P*SF | 1 |
| flags: *2U*PRSF | 2 | flags: 12*A*R*F | 1 |
| flags: **U**RSF | 2 | flags: ***A*RSF | 1 |
| flags: 12*A**** | 2 | flags: 12**P*S* | 1 |
| flags: 12****SF | 2 | flags: 12U*P*SF | 1 |
| flags: **U*PRSF | 1 | flags: 1*U**RSF | 1 |
| flags: 12UA**** | 1 | flags: 12UA***F | 1 |
| flags: 1*****SF | 1 | flags: *2U**RSF | 1 |
| flags: ****P*SF | 1 | flags: *2U*P*SF | 1 |
| flags: 12U**R*F | 1 | flags: 1***P*SF | 1 |
| flags: 12UAPRS* | 1 | | |
| | | Total packets : 2316 | No tcpopt : 64, tcpopt : 2252 |

Link Graph:

The system MY.NET.12.6 in involved in several alerts and scans. I draw for a better overview a Link Graph that shows the connections to and from this host. I used as a basis for this all 3 kind of available files (alert, scan and OOS) to get this picture.
As a summary can I mention that it is very probably that this machine was compromised trough the Red Worm. With the possible Trojan have I big doubts. The source IP address was mx2.freebsd.org. In the community was nothing known that this server (belongs to the www.freebsd.org project) was hacked or did evil activities. I looked additional to www.dshield.org and www.mynetwatchman.com. On both sites were entries available. But they are not substantial. For me is this alert a false positive. Independent I would recommend

to do a full forensic analyzes to destroy any doubts if the server was compromised or not. For the case of compromise is then a complete rebuild with trusted sources necessary.




Defensive Recommendation:

1) Upgrade the Snort Version to the newest available.
2) Make a better fine tuning from the Snort Rules. Special in the OOS files are examples for normal traffic which produces enormous log files and makes it harder to find in the noise really worst scans or attacks.
3) Think about a Content Proxy HTTP Filter for outgoing connections I found in the OOS files successful HTTP request from MY.NET.97.67 to a sex site. Be sure that you have a fitting code of ethic agreement for all Internet users.
4) Upgrade your Security Information sides (The in the moment available sides are not up to date (www.umbc.edu)
5) Think about an IPS (Intrusion Prevention system) instead of an IDS system. This could help not only to detect violation. With this you can block evil or unwanted requests very easily.
6) With a limiting of bandwidth is it possible to impede the use of file sharing.
7) Do regular vulnerability assessments over all IT equipment.




© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8) Make active enlightenment for the stuff and the students from the University what IT Security means and try to get a higher awareness for problems which can happen with unworried Internet use.

Methodology:

I found several errors in the syntax from the alert and scans files. It was necessary to correct this before I could run the analysis. Maybe this happened during the obfuscating from the IP addresses? In the OOS files was the displayed date wrong. For example the file OOS_report_040304 shows inside the date from the 03/09. Maybe the IDS system was not NTP synchronized?
For all 3 types of files (Alert, scan and OOS) I summarized all single files to one common file. For example, for the scan files I used the dos command copy 'C:\copy scans.040303+ scans.040304+ scans.040305+ scans.040306+ scans.040307 all-scans'.
I tried first Snort Snarf but this program died very shortly. It is very nice for small log files but not useable for these huge files (several 100 MB).
After this experience and reading from several other practical I used two excellent scripts from http://www.giac.org/practicals/Tod_Beardsley_GIAC.doc.
The first script cvs.pl reads the alert and the scan files (each separate) and translates the records into comma-separated values. I processed these files further with his second script summarize.pl. This script takes the results from step one and summarized the contents, groups the alerts,….
I used to analyze the OOS files a script from http://www.giac.org/practical/GCIA/Erik_Montcalm_GCIA.pdf. This script counts source IP, destination IP, packet combinations,…. It produces as well a summary at the end. I must correct this script a little because of obvious typos in the posted version from Erik before it works.
At least I used the basic UNIX tools cat, awk, sort, grep and uniq to get a more sorted output from the results. I used therefore the operation system OpenBSD.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.