# SANS Intrusion Detection in Depth
# GCIA Practical Assignment
# Version 3.2

**Prepared By:**
**Sanjay Menon CNE, MCSE, CCNA, SPS, CISSP**

## TABLE OF CONTENTS

# Assignment 1 The State of Intrusion Detection

## EVALUATING A MODERN DAY IDS

## Introduction

This is an evaluation guide, which provides suggested criteria for evaluating modern IDS. It divides the criteria into nine categories and provides a brief explanation of each. I have based this evaluation guide on the features available with ISS Real secure & Symantec Manhunt who are the major heavyweights in the commercial IDS space. The general categories are:

- Detection
- Analysis
- Response
- Performance and scalability
- High Availability
- Management
- Installation and Configuration
- Reporting
- Hardware Requirements

## Detection.

### Signature based

Most Intrusion Detection Systems available in the market are signature based. This IDS are only as good as their signatures and are efficient against known style of attacks. For this type of IDS to be successful, its database has to be updated regularly and even then there would be a chance of the signatures being not in place for a particular type of attack .ISS Real secure has over 1200 signatures.

### Anomaly Detection

Any organization which is looking for a more thorough and safer solution should consider using anomaly based IDS. This type of IDS captures all the headers of the IP packets running towards the network and then filters out all known and legal traffic which includes web traffic to the organizations web server, mail traffic to and from its mail server, outgoing traffic from company employees and DNS traffic to and from its DNS server. Anomaly detection can be further subdivided into Behavioral Anomaly detection and Protocol anomaly detection which is briefly explained below

#### Behavioral Anomaly Detection

In this type of anomaly detection, a baseline of certain system statistics or patterns of behavior is created. These pattern of behavior are tracked continually by the system and any changes in these patterns are used to indicate an attack. Some of these examples include detection of excessive use, detection of use at unusual hours and detection of changes in system calls made by user processes. The benefit of this approach is that it can detect the anomalies without having to understand the underlying cause behind the anomalies; however, legitimate use of the system can trigger anomalies leading to a very high number of false positives, ISS Real secure provides statistical anomaly protection by making use Site protector and Fast Analysis.

**Protocol Anomaly Detection**

Protocol anomaly detection is performed at the application protocol layer. It focuses on the structure and content of the communications. Many attacks target protocols such as Telnet, HTTP, RPC, SMTP, and Rlogin for example. When protocol rules are modeled directly in the sensors, it is easy to identify traffic that violates the rules, such as unexpected data, extra characters, and invalid characters. That is exactly how some of these attacks can be identified. Protocol-based IDSes, for example, can detect code Red, because they model the HTTP protocol exactly as it is reflected in the RFC. The Code Red attack violates the HTTP protocol specification because it uses a GET request to post and execute malicious code on the victim server. The IDS recognizes this as a violation of the protocol and alerts the system administrator to the violation. While the same kind of attack is making its way past signature-based systems, this attack is recognized by the IDS as a protocol violation and is reported to the system administrators, giving them hours, sometimes even days to respond to the new threat before a signature for this type of attack is developed and distributed. Symantec Manhunt uses core protocol Anomaly detection and is effective against even Zero day attacks like Nimda and Codered.ISS realsecure uses a Protocol Analysis detection which is signature based and uses over 1200 unique signatures.

The IDS should also be capable of the following type of detections:

**Denial of Service Detection**

Hackers make use of DOS and DDOS attacks to deny legitimate users access to critical network services. This is normally achieved by launching attacks that consume excessive network bandwidth, host processing cycles or other network resources.IDS products detect a DOS attack by comparing the traffic with a pre-programmed threshold but this also can lead to several instances of false alarm and also many attacks which is below the threshold will be missed. To detect Do S attacks an IDS much have some ability to monitor traffic characteristics (spikes, floods, etc.) as well as detect various types of malformed traffic (SYN floods, malformed ICMP packets etc. ISS Realsecure provides this detection but has problems in detecting Teardrop, Syndrop, NewTear or targa DOS attacks (http://lists.insecure.org/lists/ids/2000/Feb/0053.html.). Symantec ManHunt provides this type of detection.

**Network Infrastructure Attack Detection**:

Threats to network infrastructure (routers, switches, etc.) are rising. An IDS must be able to monitor the protocols that are used to maintain and administer this infrastructure. This includes such protocols as BGP, OSPF, SNMP, and HSRP.Symantec ManHunt has this detection.

**Stateful Signature Capability**

Although protocol analysis by itself is a very powerful technique, it is limited to examining a single request or response. Of course, many attacks cannot be detected by looking at one request - the attack may involve a series of requests. The best way to detect such attacks is by adding stateful characteristics to protocol analysis. When we perform stateful protocol analysis, we monitor and analyze all of the events within a connection or session. The IDS sensor can "remember" significant events and data for the duration of the session. This allows the sensor to find correlations among different events within a session, identifying attacks with multiple components that cannot be detected otherwise. Without the ability to keep state, we can only examine each packet, request or response on its own, completely independent of the rest of the session. ISS Realsecure has the stateful packet inspection capability. Symantec Manhunt also has stateful packet inspection capability.

### Custom Signature Capability

Because many sites have their own site-specific applications or protocols or are concerned with threats which the general user may not be, it's important for An IDS to allow a site to define a custom signature. Ideally this should be done in a fairly easy-to-use format which allows the user to take advantage of the various public and open sources of signature development experience. Symantec ManHunt supports Snort signature format and users who are accustomed to snort signatures can import their signatures into Manhunt. .ISS Realsecure makes use of TRONS for Snort signature compatibility.

### Full Protocol Decode

Protocol decode-based signatures are in many ways intelligent extensions to stateful pattern matches. This class of signature is implemented by decoding the various elements in the same manner as the client or server in the conversation would. When the elements of the protocol are identified, the IDS applies rules defined by the RFCs to look for violations. In some instances, these violations are found with pattern matches within a specific protocol field, and some require more advanced techniques that account for such variables as the length of a field or the number of arguments. Note that pattern matching and protocol decoding are not mutually exclusive, as some would lead you to believe.

Not doing full protocol decodes can also lead to false negatives if the protocol allows for behavior that the pattern-matching algorithms have difficulty dealing with. Symantec Manhunt provides full protocol Decode.ISS Real secure provides Full Protocol Decode for more than 60 protocols. (http://www.der-keiler.de/Mailing-Lists/securityfocus/focus-ids/2002-06/0093.html.)

### Evasion Detection and Resistance to IDS Attack

Attackers have grown smart about the types of defenses being used. They have learned how to evade detection and in some cases are even able to successfully attack the IDS itself. It's important that the IDS you choose be at least resistant to basic evasion and attack methods. This means that it is able to detect attacks even if the attackers are using tools like stick, fragrouter, whisker, or any of the various shell code permutation tools. Both Symantec Manhunt and ISS Realsecure do provide evasion detection and resistance to IDS attack.

### Full Multi-Interface Session Reassembly

Since many networks have traffic traveling along asymmetric paths it is important for an IDS to be able to effectively reassemble the session and perform detection even if it is split across multiple sensors. Note that systems which require multiple physical sensors to monitor multiple locations often have several problems dealing with this situation. ISS Realsecure and, Symantec Manhunt do provide Full Multi-Interface Session Reassembly.

## Analysis

### Third-party Event Integration

Since you are likely to deploy more defenses than just IDS, an important consideration is whether or not the IDS can accept events from your other devices and perform its analysis, response, etc. on those events in concert with its own sensors events. Lack of this functionality means you will be managing multiple systems, your administrative cost will increase and your ability to respond to incidents will be hampered by the time and effort it takes you to do this manually. Symantec Manhunt provides this integration by making use of Manhunt Smart Agents for Dragon,Firewall-1, Realsecure, Snort, Tripwire.

**Real time Event Aggregation**

As above, real networks have multiple sensors. From a management perspective it is critical that the data produced by these sensors be aggregated into a single view so that analysis and review can take into account the complete picture of what is happening in the network. It is also important for this aggregation to be done in a scalable way both from a storage perspective and from a presentation perspective. Symantec ManHunt aggregates related events into a single incident.ISS Realsecure makes use of siteprotector for the advanced event consolidation.

**Real Time Analysis**

If a product offers analysis capability, it's important to understand if this is performed in real time. Often analysis is classified into real time, near real time, and after the fact. While after the fact analysis can provide useful trending information and damage assessment, it is best used as a complement to a real time system. Real time (or very near real time) analysis is required in order to be able to stop the attack, limit damage, or perform most methods of identification and tracking.ISS Realsecure uses Workgroup manager for Realtime Data Analysis by transmitting alerts to Event collectors and stored in databases. Symantec Manhunt provides Real time analysis.

**Automated Correlation and Prioritization**

Threat Analysis requires both a human element and an automated element. The automated aspect should start with correlated data (providing it is accurate), that is then analyzed using a number of other variables such as prioritization and validity of the threat, anomaly detection data (behavior etc), vulnerability information, perspective of the attack and a number of other variables that improve accuracy and completeness.

Much of the confusion comes from vendors who imply that correlation is threat analysis when that is really not the case. Correlation is simply the process of defining relationships between data sets and does not provide the prioritization that threat analysis does. It doesn't provide the information that an analyst needs to make good judgments. A very valuable feature to have is the ability to automatically correlate event data. This provides a first level analysis of how events are related to each other, how they are prioritized, etc. This allows security personnel to immediately understand the events in context and avoid the costly manual correlation efforts. Products, which support these features, also have much lower costs of operation and front line NOC personnel require less expertise. Symantec Manhunt provides automated Correlation and prioritization.

**Cross-Node Event Correlation**

With cross node analysis, network administrators can quickly interpret incidents requiring immediate attention. In any but the simplest networks there will be multiple IDS products or sensors, often deployed across multiple physical locations. If the product supports analysis, it is important that it be able to perform the analysis across the entire space monitored, not just on a per sensor basis. If it does not, the administrator will be left to the very painful, time consuming and manual task of comparing detected events across sensors. Cross-node correlation also allows the administrator to observe threats, which may span large networks. These can be much more difficult to detect when looking at multiple, individual systems.

Manhunt provides cross node analysis among multiple ManHunt sensors. Realsecure provides event consolidation from its HIDS/NIDS/Scanner with Site Protector.

### Full Packet Capture

In order to provide sufficient data for later analysis by a trained security expert An IDS should support some mechanism by which the entire packet or packets, which triggered an alarm, is captured. This includes capturing both the payload and headers and providing some easy mechanism by which the administrator may view them. This functionality works best when integrated with some sort of incident drill down capability offered in the administrative interface (e.g. the GUI console). Symantec Manhunt provides Full Packet Capture. RealSecure 7.0 gives you the ability to run a full packet capture mode by the sensor itself if you choose. However, this would definitely degrade the sensor performance. If you're running RS 7.0 on a fully utilized 100Mbps network segment this is not advisable (http://cert.uni-stuttgart.de/archive/issforum/2002/07/msg00171.html.)

### Secure Data Store

Since the data an IDS stores can be very important during response (including possible legal responses) it's very important that the data store used be trusted. This means two things. First is that the system the data is stored on be access limited and that any transport of the data is across authenticated and encrypted channels. Second is that data stored be tamper proof or tamper evident. Typically this is done via some cryptographic mechanism (digital signatures, etc.). The global is to preserve data integrity. Symantec Manhunt provides this feature.

### Duplicate Suppression

An IDS should support some form of duplicate event suppression so as to avoid flooding the administrator with alarms or events. Some will allow you to track the number of duplicate events (usually via some counters) without overloading the user with data. Both Symantec Manhunt and ISS Realsecure provide duplicate suppression.

### User Tunable Controls

Good analysis and management systems should expose some amount of tunable analysis parameters to allow you to customize the product to your environment. While it's possible to build a product that self tunes some factors environments differ enough that some customization will be required**.** Both Symantec Manhunt and ISS Realsecure does provide User Tunable Controls.

## Response

### Automated Policy-Based Response

IDS products usually include some form of automated response capability. This allows the system to take predefined actions even if the administrator is not actively monitoring. It also allows the system to take action very quickly and in a very scalable manner. The best response mechanisms are integrated to the product (not an "add on" or second product) and are policy based. The more flexible the policy can be and the more response mechanisms supported, the better. Both ISS Realsecure and Symantec Manhunt provide automated Policy-Based Response.

**Alerting (SNMP, email, console log)**

IDS should include both SMTP (email) and SNMP (network management) alerting capabilities integrated into the product. Some may also claim “pager” support but this can be accomplished with common email/pager gateways. Some products may expect the user to create “email scripts” or “alerting scripts”. Those products do not tend to work very well and have high administrative overhead. Both Symantec Manhunt and ISS Realsecure provide the Alerting feature.

**Session Termination**

Many IDS solutions offer some form of session termination. This has some value with respect to terminating session based TCP threats though is of little or no utility against scans, UDP attacks, and various DoS attacks. The best implementations of this are those, which are tightly integrated to the product.

Both Symantec Manhunt and ISS Realsecure provides the Session Termination feature.

**User-Defined Response Actions**

In most environments it’s very important that a product’s response mechanism be extensible. This allows an administrator to add their own custom response mechanisms (scripts, tools, etc.). These can be extremely useful in gathering more information, integrating to local ticketing systems, driving configuration changes, etc. Both Symantec Manhunt and ISS Realsecure provides the feature of User-Defined Response Actions.

**Traffic Recording and Playback**

Basically this allows the IDS to record network traffic. The best implementations do this as the result of a policy decision (as mentioned above) usually in response to something suspicious observed. Systems should not only allow this on a policy response basis but also allow narrowing the scope of the traffic observed (by address, port, etc.). This will capture of only relevant information. Both ISS Realsecure and Symantec Manhunt provide this feature.

**Remote Threat Tracing**

The ability to trace back a remote attack is a very powerful feature. The general concept is that the product provides some means by which attacks (even those with forged source addresses) can be traced back to the source or at least the entry point to the local network. Note that such things as host name resolution and trace route do not provide this functionality as they still rely on the provided source address and are thus vulnerable to misdirection by forgery. Symantec ManHunt employs methods like FlowChaser and TrackBack to find the point of entry of an attack especially for Distributed Denial of Service attacks with spoofed source addresses.

**Peer Network Notification**

Another important consideration for an IDS product is the ability to notify a peer network in some automated fashion during an incident. It requires that systems in both networks be able to dynamically notify each other and share incident data. It also requires that this be done in a secure, authenticated, and robust manner. Symantec Manhunt provides peer network notification.

### Session Blocking Suggestions or Integration

It's worth considering what other response mechanisms a product offers. In general, more is better. It's hard to create a definitive list of response mechanisms available since it continually changes however those currently available include attack tracing, filter or quality-of-service ACL suggestions, firewall reconfiguration, and audible alarms. Both ISS Realsecure and Symantec Manhunt provide this feature.

## Performance and Scalability

### Full 1Gbps Throughput (no packet loss)

It is important to evaluate the maximum amount of traffic the IDS can handle. In modern networks an IDS should be able to handle at least 1 Gbps of traffic. Most servers and core enterprise networks are deployed or are deploying Gigabit Ethernet and this capability will be required even for many edge deployments. Symantec Manhunt can go upto 2 gigabits/sec depending on the system configuration. ISS Realsecure provides an interface for Gigabit support and uses a sampling model in high saturation mode for high performance.

### Multiple 100Mbps Segment Throughput (no packet loss)

It is also important for a system to be able to monitor multiple 100Mbps segments with no loss. Symantec Manhunt is capable of this.

### Handle 500,000 or more Simultaneous TCP Sessions

An IDS should be able to handle at least 500,000 simultaneous sessions or "flows". While many IDS products can handle the traffic rates for a given environment, they fail under real traffic loads when they attempt to maintain state for all of the simultaneous open sessions. The threshold of 500,000 is based on both observation and calculation of the traffic passing through gigabit networks. While the actual number of flows will vary depending on the network, applications in use, user activity, etc. it is quite possible to generate hundreds of thousands of concurrent flows in a gigabit network. RealSecure 7 can handle 500k sessions by default, and you can configure it up to 3-million concurrent TCP sessions.

### Scales to 100's of Sensors

In modern switched networks, there are often a very large number of network segments. Given the number of critical resources available on the network and the growing concern over insider threats, it is important in most networks to be able to monitor many locations rather than just the perimeter (e.g. the firewall). An IDS product should easily scale to accommodate hundreds of sensors. Symantec manhunt can scale up 100 sensors while Realsecure can scale up to 30 Sensors according to the FAQ.

### Robust Under Edge Conditions

IDS products must be able to handle variations in traffic, both natural and induced, without failure or loss of coverage. Products should be able to handle high fragmentation, variations in peak load, extreme packet sizes, unusual distributions of protocol and addresses, and malformed traffic. Both Symantec Manhunt and ISS Realsecure are capable of this.

### High Availability

In environments where high availability is an issue, products should support H/A capabilities. The best solutions are products, which provide tightly integrated H/A support without third party hardware. Symantec Manhunt provides this feature.

### Automatic Fail over and Fail back

An IDS should support a high availability mechanism, which provides the capability all monitoring components (sensors, data stores, analysis systems, etc.) to fail over to backups. It should also provide the capability to fail back when the primary node is restored to operation. Symantec Manhunt provides this feature. Symantec Manhunt does provide this feature.

### High-Speed Fail over

High availability functionality should provide fail over in a very short time frame so as to minimize any gap in coverage. Shorter is better but fail over time should be at worst 30 seconds. Symantec Manhunt does have High-Speed Fail over.

### "Five Nines" (99.999%) Reliability

An IDS in a H/A configuration should be able to provide 99.999% uptime. The vendor should able to provide actual documentation of this uptime estimate.

### Cost-Effectives High-Availability Deployment Configurations

A H/A configuration should not require the purchase of expensive load balancers, disk vaults or other hardware kits. Ideally it would require nothing more than the additional backup system.

## Management

### Secure Remote Management

Solutions should include a good mechanism for secure remote management of the system. Management is usually done via a graphical user interface (GUI) console, which can connect to the system via a secure channel. The communications channel should be authenticated and encrypted (without requiring additional VPN setup, etc.). Both Symantec Manhunt and ISS Realsecure provides Secure Remote Management.

### Broad Platform Support for Management

Ideally the administration console should support installation on a variety of platforms including both Windows and UNIX (Linux, Solaris, etc.) to accommodate a wide audience (NOC personnel, analysts, managements, etc.). Symantec Manhunt provides support for Solaris, Windows 98,Windows NT, and Windows 2000 for management console. ISS Realsecure has console support for Windows platform.

**Scalable Information Presentation**

One of the most critical things to consider about an IDS management console is information presentation. If a big linear list of alarms is presented, users will quickly become swamped even under a modest threat. The best solutions offer automated management and organization of data. Ideally this is done via some intelligent analysis and presented in a compact form, which allows you to make easy, high-level assessments prior to drilling down to detailed event data. Both Symantec Manhunt and ISS Realsecure provides Scalable Information Presentation.

**Incident Drill Down Capability**

Since IDS products collect a great deal of data, it's important that they offer incident "drill down" mechanism. This allows the user (typically via the GUI console) to change the level of detail presented from a high level summary down to detailed event data. The event level should provide information about type, time, protocol, etc. It should also provide the ability to see packet level data (payload, headers, etc.) and be able to display additional reference information about the type of event. Both Symantec Manhunt and ISS Realsecure provides Incident Drill Down Capability.

**Additional Reference Data Provided**

An IDS product should provide additional reference data for each attack type. This should be easily accessible while viewing an event (e.g. a link or something similar). It should provide descriptive details about the nature of the event. It should also provide references where applicable to CVE, CERT, and Bugtraq sources. Both Symantec Manhunt and ISS Realsecure provide the additional reference data.

**Cluster Administration Support**

If you're deploying more than one system, sensor, etc. the ability to deploy as a cluster should be examined. Lack of this feature can cause enormous increases in cost of operation due to time spent manually making changes, updates, etc. Cluster support typically means that administrative operations (configuration changes, patch updates, etc.) only need to be done one time for the entire cluster. It also means that all monitoring, drill down, and Interaction can be done from a single point. Realsecure uses

SensorMgr to allow users to push configuration policies and issue commands to groups of RealSecure sensors.

**Incident Annotation/Auditing**

An IDS should provide an integrated ability for product operators to create a running audit log as they review events and incidents within the system. This should allow for operators to store arbitrary data along with the detection data (usually comments, additional data points, etc.). It is important that annotations can be added to audit logs with timestamp and user information and should be stored with the event data. It should be easy to retrieve, view, and backup. Symantec Manhunt provides Incident Annotation/Auditing Feature.

## Deployment

### Multiple Interface Support (Gigabit and Fast Ethernet)

Symantec ManHunt supports 4 high speed Gigabit or 12 fast Ethernet interfaces on backplane.

### Sensor Roaming in Switched Networks

In modern switched networks it's very important that an IDS be able to monitor multiple network segments from a single machine. Systems which require deployment of a physical sensor per segment requires massive number of devices or only watch choke points, resulting in either an administrative nightmare or significant blind spots in coverage. Symantec Manhunt does allow you to monitor multiple network segments from a single machine.

### Easy to Deploy and Install

An IDS should be deployable in less than two hours. This includes machine setup, product installation and basic configuration and tuning. Both ISS Realsecure and Symantec Manhunt are quite easy to install.

### VLAN-aware Detection

In order to operate in any modern switched network and IDS should be VLAN aware. This means both being aware of VLAN groupings as well as being able to handle various forms of encapsulation. Symantec Manhunt can monitor multiple segments, switches and VLANs and does provide VLAN-aware detection.

## Reporting

### Integrated Deep Drill-Down Console Reporting

An IDS should support an integrated reporting facility The native console should be able to present incident and event data in tabular and chart form. It should support basic interactive drill down on the reports. The reports should be savable and printable in some easy to transport format (e.g. PDF). Both Symantec Manhunt and ISS Realsecure provides Integrated Deep Drill-Down Console Reporting.

### Web-based Reporting

An IDS should also support web based reporting. This is useful for sites with many groups of administrators or customers to whom reporting data is provided. This should be easy to configure and support multiple platforms and browsers. Both Symantec Manhunt and ISS Realsecure provide Web-based Reporting.

### SQL Export

Many sites have local storage requirements, third party trending analysis systems or other site local tools, which require data storage in a SQL database. An IDS should have some scalable mechanism to export its data in real time to a SQL database without significant effort or manual integration. Both Symantec Manhunt and ISS Realsecure provide the feature of SQL export.

## Hardware

### Multiple Sensors per Unit

An IDS should allow deployment with minimal amount of physical hardware for allowing multiple sensors to run on a single system. This should allow concurrent monitoring of multiple network segments without requiring multiple physical machines. Symantec Manhunt can monitor multiple switches from single machine and ISS Realsecure also allows Multiple Sensors per Unit.

### Multi-Processor Scalable

An IDS should to take advantage of multi-processor systems to increase its capabilities (detection, analysis, etc.). This allows deployment with fewer systems and thus decreases the administrative overhead of operating the IDS.Symantec Manhunt provides the Multi-Processor scalability.

### References.

http://www.scmagazine.com/scmagazine/sc-online/2002/article/23/article.html. A good discussion on signature bases vs anomaly based IDS.

http://www.intruvert.com/technology/understanding_ids.htm. A detailed explanation of DoS attack detection by IDS.

http://www.isp-planet.com/news/2002/symantec_020924.html. A good article on Symantec Manhunt.

http://www.isp-planet.com/perspectives/ids_p3.html. A detailed explanation on different

Types of anomaly based IDS.

http://www.iss.net. For details about the Realsecure network IDS.

http://www.symantec.com For details about Manhunt IDS

# Assignment 2 Network Detects

## 2.1 Detect #1 – WEB-IIS view source via translate header

### 2.1.1 Ethereal output of the detect:

```
Frame 222 (319 on wire, 319 captured)
Ethernet II
Internet Protocol, Src Addr: 207.230.250.69 (207.230.250.69), Dst Addr: 46.5.180.133 (46.5.180.133)
```

Transmission Control Protocol, Src Port: 3949 (3949), Dst Port: 80 (80), Seq: 1562772876, Ack: 4044721747
Hypertext Transfer Protocol

```
0000  00 00 0c 04 b2 33 00 03 e3 d9 26 c0 08 00 45 00   .....3....&...E.
0010  01 31 51 dd 40 00 6f 06 12 39 cf e6 fa 45 2e 05   .1Q.@.o..9...E..
0020  b4 85 0f 6d 00 50 5d 26 05 8c f1 15 8e 53 50 18   ...m.P]&.....SP.
0030  1f 7a 87 c0 00 00 47 45 54 20 2f 5f 76 74 69 5f   .z....GET /_vti_
0040  69 6e 66 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e   inf.html HTTP/1.
0050  31 0d 0a 44 61 74 65 3a 20 53 75 6e 2c 20 31 34   1..Date: Sun, 14
0060  20 4a 75 6c 20 32 30 30 32 20 31 37 3a 33 39 3a    Jul 2002 17:39:
0070  31 31 20 47 4d 54 0d 0a 4d 49 4d 45 2d 56 65 72   11 GMT..MIME-Ver
0080  73 69 6f 6e 3a 20 31 2e 30 0d 0a 41 63 63 65 70   sion: 1.0..Accep
0090  74 3a 20 2a 2f 2a 0d 0a 55 73 65 72 2d 41 67 65   t: */*..User-Age
00a0  6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 32 2e 30 20   nt: Mozilla/2.0
00b0  28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 20   (compatible; MS
00c0  46 72 6f 6e 74 50 61 67 65 20 34 2e 30 29 0d 0a   FrontPage 4.0)..
00d0  48 6f 73 74 3a 20 77 77 77 2e 58 58 58 58 2e 63   Host: www.XXXX.c
00e0  6f 6d 0d 0a 41 63 63 65 70 74 3a 20 61 75 74 68   om..Accept: auth
00f0  2f 73 69 63 69 6c 79 0d 0a 43 6f 6e 74 65 6e 74   /sicily..Content
0100  2d 4c 65 6e 67 74 68 3a 20 30 0d 0a 43 6f 6e 6e   -Length: 0..Conn
0110  65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69   ection: Keep-Ali
0120  76 65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f   ve..Cache-Contro
0130  6c 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 0d 0a      l: no-cache....
```

Frame 223 (444 on wire, 444 captured)
Ethernet II
Internet Protocol, Src Addr: 207.230.250.69 (207.230.250.69), Dst Addr: 46.5.180.133 (46.5.180.133)
Transmission Control Protocol, Src Port: 3953 (3953), Dst Port: 80 (80), Seq: 1563512477, Ack: 4041417864
Hypertext Transfer Protocol

```
0000  00 00 0c 04 b2 33 00 03 e3 d9 26 c0 08 00 45 00   .....3....&...E.
0010  01 ae 51 e8 40 00 6f 06 11 b1 cf e6 fa 45 2e 05   ..Q.@.o......E..
0020  b4 85 0f 71 00 50 5d 31 4e 9d f0 e3 24 88 50 18   ...q.P]1N...$.P.
0030  22 38 64 a9 00 00 50 4f 53 54 20 2f 5f 76 74 69   "8d...POST /_vti
0040  5f 62 69 6e 2f 73 68 74 6d 6c 2e 65 78 65 2f 5f   _bin/shtml.exe/_
0050  76 74 69 5f 72 70 63 20 48 54 54 50 2f 31 2e 31   vti_rpc HTTP/1.1
0060  0d 0a 44 61 74 65 3a 20 53 75 6e 2c 20 31 34 20   ..Date: Sun, 14
0070  4a 75 6c 20 32 30 30 32 20 31 37 3a 33 39 3a 31   Jul 2002 17:39:1
0080  32 20 47 4d 54 0d 0a 4d 49 4d 45 2d 56 65 72 73   2 GMT..MIME-Vers
0090  69 6f 6e 3a 20 31 2e 30 0d 0a 55 73 65 72 2d 41   ion: 1.0..User-A
00a0  67 65 6e 74 3a 20 4d 53 46 72 6f 6e 74 50 61 67   gent: MSFrontPag
00b0  65 2f 34 2e 30 0d 0a 48 6f 73 74 3a 20 77 77 77   e/4.0..Host: www
00c0  2e 58 58 58 58 2e 63 6f 6d 0d 0a 41 63 63 65 70   .XXXX.com..Accep
00d0  74 3a 20 61 75 74 68 2f 73 69 63 69 6c 79 0d 0a   t: auth/sicily..
00e0  43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20   Content-Length:
00f0  34 31 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65   41..Content-Type
0100  3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d   : application/x-
0110  77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f   www-form-urlenco
0120  64 65 64 0d 0a 58 2d 56 65 72 6d 65 65 72 2d 43   ded..X-Vermeer-C
0130  6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70   ontent-Type: app
0140  6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77 2d 66   lication/x-www-f
0150  6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a   orm-urlencoded..
0160  43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70   Connection: Keep
0170  2d 41 6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 6f   -Alive..Cache-Co
```

```
0180  6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 0d   ntrol: no-cache.
0190  0a 0d 0a 6d 65 74 68 6f 64 3d 73 65 72 76 65 72   ...method=server
01a0  2b 76 65 72 73 69 6f 6e 25 33 61 34 25 32 65 30   +version%3a4%2e0
01b0  25 32 65 32 25 32 65 34 37 31 35 0a               %2e2%2e4715.
<snip>

<snip>

Frame 230 (218 on wire, 218 captured)
Ethernet II
Internet Protocol, Src Addr: 207.230.250.69 (207.230.250.69), Dst Addr: 46.5.180.133 (46.5.180.133)
Transmission Control Protocol, Src Port: 3956 (3956), Dst Port: 80 (80), Seq: 1568029610, Ack:
4077247107
Hypertext Transfer Protocol

0000  00 00 0c 04 b2 33 00 03 e3 d9 26 c0 08 00 45 00   .....3....&...E.
0010  00 cc 52 04 40 00 6f 06 12 77 cf e6 fa 45 2e 05   ..R.@.o..w...E..
0020  b4 85 0f 74 00 50 5d 76 3b aa f3 05 da 83 50 18   ...t.P]v;.....P.
0030  1e 16 81 41 00 00 50 52 4f 50 46 49 4e 44 20 2f   ...A..PROPFIND /
0040  6d 61 69 6e 2f 20 48 54 54 50 2f 31 2e 31 0d 0a   main/ HTTP/1.1..
0050  44 65 70 74 68 3a 20 30 0d 0a 74 72 61 6e 73 6c   Depth: 0..transl
0060  61 74 65 3a 20 66 0d 0a 55 73 65 72 2d 41 67 65   ate: f..User-Age
0070  6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 57 65   nt: Microsoft-We
0080  62 44 41 56 2d 4d 69 6e 69 52 65 64 69 72 2f 35   bDAV-MiniRedir/5
0090  2e 31 2e 32 36 30 30 0d 0a 48 6f 73 74 3a 20 77   .1.2600..Host: w
00a0  77 77 2e 58 58 58 58 2e 63 6f 6d 0d 0a 43 6f 6e   ww.XXXX.com..Con
00b0  74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d 0a   tent-Length: 0..
00c0  43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70   Connection: Keep
00d0  2d 41 6c 69 76 65 0d 0a 0d 0a                     -Alive....
```

### 2.1.2 Snort Dump of Detect

```
[**] [1:990:5] WEB-IIS _vti_inf access [**]
[Classification:    ] [Priority: 2]
07/14-22:07:56.394488 207.230.250.69:3949 -> 46.5.180.133:80
TCP TTL:111 TOS:0x0 ID:20957 IpLen:20 DgmLen:305 DF
***AP*** Seq: 0x5D26058C  Ack: 0xF1158E53  Win: 0x1F7A  TcpLen: 20

[**] [1:937:6] WEB-FRONTPAGE _vti_rpc access [**]
[Classification:    ] [Priority: 2]
07/14-22:07:57.904488 207.230.250.69:3953 -> 46.5.180.133:80
TCP TTL:111 TOS:0x0 ID:20968 IpLen:20 DgmLen:430 DF
***AP*** Seq: 0x5D314E9D  Ack: 0xF0E32488  Win: 0x2238  TcpLen: 20
[Xref => http://www.securityfocus.com/bid/2144]

[**] [1:1042:6] WEB-IIS view source via translate header [**]
[Classification:    ] [Priority: 2]
07/14-22:08:12.144488 207.230.250.69:3954 -> 46.5.180.133:80
TCP TTL:111 TOS:0x0 ID:20980 IpLen:20 DgmLen:221 DF
***AP*** Seq: 0x5D68329F  Ack: 0xF2098374  Win: 0x2238  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS305]
[Xref => http://www.securityfocus.com/bid/1578]
<snip>

<snip>
 [**] [1:1042:6] WEB-IIS view source via translate header [**]
```

```
[Classification:    ] [Priority: 2]
07/14-22:08:16.404488 207.230.250.69:3956 -> 46.5.180.133:80
TCP TTL:111 TOS:0x0 ID:20996 IpLen:20 DgmLen:204 DF
***AP*** Seq: 0x5D763BAA  Ack: 0xF305DA83  Win: 0x1E16  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS305]
[Xref => http://www.securityfocus.com/bid/1578].
```

Lets us look at the interesting fields for the WEB-IIS view source via translate header alert.

Source IP :207.230.250.69.The ARIN lookup given below suggests that the IP is assigned to AT&T Canada Telecom Services Company.

Source Port : 3954 & 3956 .It is a normal empheral port normally used by Windows since it uses the traditional BSD range of 1024 through 4999 for its ephemeral port range

Destination IP: 46.5.180.133.This is the Web server for Public access.

Destination Port: 80.This indicates that the traffic was HTTP traffic.

TTL : 111.This indicates the source machine to be a Windows variant and 17 hops have been traversed.

Flags : Acknowledgement and Push flags have been set indicating that three way handshake has been completed and the application wants the data to be processed immediately without waiting for the buffer to fill up.

The IP ID is changing normally and the source port is also changing. So the traffic so far indicates that there is nothing malicious about the packets so far captured. The interesting thing about this detect would be the
Content.

### 2.1.3 Snort Rule for Detect

```
 alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS view source via translate header"; flags:A+; content: "Translate|3a| F"; nocase; reference:arachnids,305; reference:bugtraq,1578; classtype:web-application-activity; sid:1042;  rev:6;)
```

The alert was generated because there was content " Translate|3a| F" in the packet . The packet offset is zero, meaning that content string is looked from the start of the packet data. This is not a case sensitive search.

### 2.1.4 Source of Trace

The source of this trace was from the file http://www.incidents.org/logs/raw/2002.6.14 .The raw file was then further analyzed using Ethereal and snort.

### 2.1.5 Detect Generated By

This detect was generated by Snort 1.8.6 running on windows 2000 SP2 and using snort.conf,v 1.77.2.19 dated  2002/06/29.

Snort was used with the command line option:

```
snort -c snort.conf -d -e -l log -r 2002.6.14.
```

The options used are:

-c  snort.conf =use rules from snort.conf
-d =Dump the application layer
-e= Display the second layer header info
-l log=log directory
-r 2002.6.14=to read and process Tcpdump file  2002.6.14

The log was further analyzed using Ethereal ver 0.9.3 running on windows 2000 sp2 with the filter

IP.addr eq 207.230.250.69 and IP.addr eq 46.5.180.133

### 2.1.6 Probability the Source Address was spoofed

The possibility that source is spoofed is low since the objective of the attack is to make use of the vulnerability existing in pre-windows 2000 sp1 machines where by when someone makes request for ASP/ASA (or any other scriptable page) and adds "Translate: f" into headers of HTTP GET request there is a serious security bug in Windows 2000 (unpatched by SP1) that in return gives complete ASP/ASA code instead of processed file and to achieve this  the three way handshake has to be completed and data transfer has to take place. Looking at the Ethereal output above we can see the SYN and ACK flags set indicating the three way handshake has been set. Also the IP ID is changing with each packet and source port is also changing. Probability of source routing and sniffing on remote host exists but this probability would be too small.

The ARIN lookup of the source address 207.230.250.69 gives the following output, which indicates

AT&T Canada Telecom Services Company ATTCANADA-16 (NET-207-230-224-0-1)
207.230.224.0 - 207.230.255.255
MDI Internet NETBLK-MDI-BLK1 (NET-207-230-250-0-1)
207.230.250.0 - 207.230.250.255

# ARIN Whois database, last updated 2002-11-07 19:05
# Enter ? for additional hints on searching ARIN's Whois database.
This indicates that the source over here is one of the customers of MDI Inc Canada

### 2.1.7 Description of the Attack

When someone makes request for ASP/ASA (or any other scriptable page) and adds "Translate: f" into headers of HTTP GET request (headers are _not_ part of URL, they are part of HTTP request), any machine which is not patched up with SP1 will give the entire ASP/ASA code instead of the processed file. But to achieve This objective the attacker has to place an trailing slash "/" to the end of the requested Url. Most important and dangerous aspect of bugs leading to source of ASP/ASA is not in giving away your business logic. It is not worth of trying to download all ASP/ASA Files and decode how something works. Most important aspect is in showing PASSWORDS to access SQL Server Databases and LOCATIONS of Access databases. This is how sites are hacked and private sensitive data are falling in hands of strangers.

### 2.1.8 Attack Mechanism.

By appending a "\" character to a request for a server side script, and adding an HTTP header with the value "Translate: f", any attacker can retrieve the source code of server side scripts, such as ASP scripts. Obtaining the source code of server side scripts grants the attacker deeper knowledge of the logic behind the web application. This knowledge helps the attacker to develop further attacks, which are by far more dangerous. For example the following communication is a malicious attempt to use the vulnerability to access the login.asp.

```
GET /login.asp\ HTTP/1.0
Host: 192.168.1.2:80
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Content-Type: application/x-www-form-urlencoded
Translate: f
```

But Translate: f" is legitimate header for WebDAV if it is used as it should be -
adding this to HTTP GET is sign for WebDAV component to really return SOURCE
code of file and bypass processing. It is used in FrontPage2000 and any
WebDAV compatible client to get file for editing. It has to be accompanied
by some other information, which should not let anyone access sources.

To make sure that this is not a false a positive, TCP Stream analysis of Ethereal was used on the downloaded raw file and the output was:

```
GET /_vti_inf.html HTTP/1.1
Date: Sun, 14 Jul 2002 17:39:11 GMT
MIME-Version: 1.0
Accept: */*
User-Agent: Mozilla/2.0 (compatible; MS FrontPage 4.0)
Host: www.XXXX.com
Accept: auth/sicily
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache

POST /_vti_bin/shtml.exe/_vti_rpc HTTP/1.1
Date: Sun, 14 Jul 2002 17:39:12 GMT
MIME-Version: 1.0
User-Agent: MSFrontPage/4.0
Host: www.XXXX.com
Accept: auth/sicily
Content-Length: 41
Content-Type: application/x-www-form-urlencoded
X-Vermeer-Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Cache-Control: no-cache
method=server+version%3a4%2e0%2e2%2e4715
PROPFIND /main HTTP/1.1
Depth: 0
translate: f
User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
Host: www.XXXX.com
Content-Length: 0
Connection: Keep-Alive
Pragma: no-cache

PROPFIND /main/ HTTP/1.1
Depth: 0
translate: f
```

```
User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
Host: www.XXXX.com
Content-Length: 0
Connection: Keep-Alive
Pragma: no-cache

<snip>

<snip>
OPTIONS / HTTP/1.1
translate: f
User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
Host: www.XXXX.com
Content-Length: 0
Connection: Keep-Alive

PROPFIND /main HTTP/1.1
Depth: 0
translate: f
User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
Host: www.XXXX.com
Content-Length: 0
Connection: Keep-Alive

PROPFIND /main/ HTTP/1.1
Depth: 0
translate: f
User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
Host: www.XXXX.com
Content-Length: 0
Connection: Keep-Alive.
```

Clearly the Tanslate f: was not used by any "\" at the end of request to retrieve any critical ASP file and this indicates a harmless webdav communication between the client and the server.

### 2.1.9 Correlations

Microsoft has talked about this vulnerability in their Security Update of August 23,2000 which can be found at:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23769.

SecutiyFocus discusses this vulnerability in detail at with the exploit code.

http://online.securityfocus.com/bid/1578

Similar detect was submitted by Danny C. Boulineau the details of which is posted at

cert.uni-stuttgart.de/archive/intrusions/ 2002/10/maillist.html

Where he has also come to the conclusion that the traffic was non-malicious.

### 2.1.10 Evidence of Active Targeting

Going through the traffics coming in from 207.230.250.69,I could see that this host was involved in only the http communication with the web server 46.5.180.133 and hence this can be considered to be active targeting even though the traffic is non-malicious.

### 2.1.11 Severity

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

Criticality: 5 –Since this is a web server used for public use, any attack should be considered to be critical.

Lethality: 4 –The loss of critical information could have lead to further compromise of the system.

System Countermeasures: 2 – Only pre SP1 Windows 2000 machines running IIS 5.0 is vulnerable to this exploit. So any machine having SP1 and above is non-vulnerable to this exploit. Since I am not sure whether the machine has been indeed patched up, I will give lower points to this.

Network Countermeasures: 2 –Since you cannot have much restriction for the web servers, which is for Public use, using application level firewalls to protect your web servers will certainly reduce lot of attack launched from valid http traffic. Since I do not have information into the type of firewall in place here, I would give lower points here.

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

### 2.1.12 Defensive Recommendation.

1] Make sure your Web server does not have any sample scripts or unnecessary scripts or files that can leak precious information. Install only what is necessary.

2] There are numerous tools to choose from to audit Web servers like Enterprise security Manager from Symantec which can tell you Vulnerabilities existing on you web server and you can schedule it to run at prespecified intervals to automate frequent audits.

3] Make sure you have the latest word on the wire: subscribe to security-oriented mailing lists such as BugTraq.

4] Apply the patches and Service packs released by the Vendors as soon as it is available so as to secure yourself from any vulnerability, which would be taken care by this patches.

### 2.1.13 Multiple Choice Test Question

Translate: f is associated with which IIS exploit?

A . WEB-IIS Transfer-Encoding
B. WEB-IIS view source via translate header
C. WEB-IIS ASP contents view
D. WEB-IIS SAM Attempt

Ans : B

### 2.1.14 E-mail Response

My E-Mail response to Robert Wagner’s query with respect to my submission.

Hi Robert,

Thanks for the questions. Please find my response below.

> How did the server respond to the attack:

This is not an attack but a harmless Webdav communication between the client and server.

> Is SNORT setup so you
> can see how the server responds.

Snort is setup to take external net as any.I could see the response from this particular
server to six other IP`s but the RAW file do not have any reponse from the server for
this particular communication.

> Does the
> attacker have some sort of insider information?

This particular communication do not suggest that the attacker had any inside information since the http headers indicate a normal client-server communication.

> What does the auth/sicily mean

auth/sicily is code name for Distributed Password Authentication (DPA)implemented by the frontpage server extensions.

On Mon, 11 Nov 2002 Robert Wagner wrote :

> Defense: How did the server respond to the attack? Is SNORT setup so you
> can see how the server responds? What does the auth/sicily mean? Does the
> attacker have some sort of insider information?

## Detect #2 WEB-MISC whisker HEAD with large datagram

### 2.2.1 Ethereal output of the detect:

```
Frame 81 (633 on wire, 633 captured)
Ethernet II
Internet Protocol, Src Addr: 192.18.17.3 (192.18.17.3), Dst Addr: 46.5.180.133 (46.5.180.133)
Transmission Control Protocol, Src Port: 39502 (39502), Dst Port: 80 (80), Seq: 429850516, Ack:
1435944200
Hypertext Transfer Protocol

0000  00 00 0c 04 b2 33 00 03 e3 d9 26 c0 08 00 45 00   .....3....&...E.
0010  02 6b 24 eb 00 00 ec 06 fa 07 c0 12 11 03 2e 05   .k$............
0020  b4 85 9a 4e 00 50 19 9e ff 94 55 96 c5 08 50 18   ...N.P....U...P.
0030  fa f0 fd 37 00 00 48 45 41 44 20 2f 66 74 70 70   ...7..HEAD /ftpp
```

```
0040  75 62 2f 63 68 69 70 73 2f 61 70 70 6e 6f 74 65   ub/chips/appnote
0050  2f 69 72 5f 75 74 69 6c 73 2e 7a 69 70 20 48 54   /ir_utils.zip HT
0060  54 50 2f 31 2e 30 0d 0a 48 6f 73 74 3a 20 77 77   TP/1.0..Host: ww
0070  77 2e 58 58 58 58 2e 63 6f 6d 0d 0a 55 73 65 72   w.XXXX.com..User
0080  2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f   -Agent: Mozilla/
0090  35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b   5.0 (Windows; U;
00a0  20 57 69 6e 39 38 3b 20 65 6e 2d 55 53 3b 20 72    Win98; en-US; r
00b0  76 3a 30 2e 39 2e 39 29 20 47 65 63 6b 6f 2f 32   v:0.9.9) Gecko/2
00c0  30 30 32 30 33 31 31 0d 0a 41 63 63 65 70 74 3a   0020311..Accept:
00d0  20 74 65 78 74 2f 78 6d 6c 2c 61 70 70 6c 69 63    text/xml,applic
00e0  61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 70 6c 69 63   ation/xml,applic
00f0  61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c   ation/xhtml+xml,
0100  74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30 2e 39 2c   text/html;q=0.9,
0110  74 65 78 74 2f 70 6c 61 69 6e 3b 71 3d 30 2e 38   text/plain;q=0.8
0120  2c 76 69 64 65 6f 2f 78 2d 6d 6e 67 2c 69 6d 61   ,video/x-mng,ima
0130  67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f 6a 70 65   ge/png,image/jpe
0140  67 2c 69 6d 61 67 65 2f 67 69 66 3b 71 3d 30 2e   g,image/gif;q=0.
0150  32 2c 74 65 78 74 2f 63 73 73 2c 2a 2f 2a 3b 71   2,text/css,*/*;q
0160  3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d 4c 61 6e   =0.1..Accept-Lan
0170  67 75 61 67 65 3a 20 65 6e 2d 67 62 2c 20 65 6e   guage: en-gb, en
0180  2d 75 73 3b 71 3d 30 2e 35 30 0d 0a 41 63 63 65   -us;q=0.50..Acce
0190  70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69   pt-Encoding: gzi
01a0  70 2c 20 64 65 66 6c 61 74 65 2c 20 63 6f 6d 70   p, deflate, comp
01b0  72 65 73 73 3b 71 3d 30 2e 39 0d 0a 41 63 63 65   ress;q=0.9..Acce
01c0  70 74 2d 43 68 61 72 73 65 74 3a 20 49 53 4f 2d   pt-Charset: ISO-
01d0  38 38 35 39 2d 31 2c 20 75 74 66 2d 38 3b 71 3d   8859-1, utf-8;q=
01e0  30 2e 36 36 2c 20 2a 3b 71 3d 30 2e 36 36 0d 0a   0.66, *;q=0.66..
01f0  4b 65 65 70 2d 41 6c 69 76 65 3a 20 33 30 30 0d   Keep-Alive: 300.
0200  0a 50 72 61 67 6d 61 3a 20 6e 6f 2d 63 61 63 68   .Pragma: no-cach
0210  65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c   e..Cache-Control
0220  3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 46 6f 72 77   : no-cache..Forw
0230  61 72 64 65 64 3a 20 62 79 20 68 74 74 70 3a 2f   arded: by http:/
0240  2f 70 68 61 6e 74 6f 6d 2e 73 69 6e 67 61 70 6f   /phantom.singapo
0250  72 65 2e 73 75 6e 2e 63 6f 6d 3a 38 30 38 30 20   re.sun.com:8080
0260  28 4e 65 74 73 63 61 70 65 2d 50 72 6f 78 79 2f   (Netscape-Proxy/
0270  33 2e 35 31 29 0d 0a 0d 0a                        3.51)....
```

```
Frame 82 (633 on wire, 633 captured)
Ethernet II
Internet Protocol, Src Addr: 192.18.17.3 (192.18.17.3), Dst Addr: 46.5.180.133 (46.5.180.133)
Transmission Control Protocol, Src Port: 40492 (40492), Dst Port: 80 (80), Seq: 553061832, Ack:
1459479871
Hypertext Transfer Protocol
```

```
0000  00 00 0c 04 b2 33 00 03 e3 d9 26 c0 08 00 45 00   .....3....&...E.
0010  02 6b 24 f1 00 00 ec 06 fa 01 c0 12 11 03 2e 05   .k$.............
0020  b4 85 9e 2c 00 50 20 f7 0d c8 56 fd e5 3f 50 18   ...,.P ...V..?P.
0030  fa f0 c2 2f 00 00 48 45 41 44 20 2f 66 74 70 70   .../..HEAD /ftpp
0040  75 62 2f 63 68 69 70 73 2f 61 70 70 6e 6f 74 65   ub/chips/appnote
0050  2f 69 72 5f 75 74 69 6c 73 2e 7a 69 70 20 48 54   /ir_utils.zip HT
0060  54 50 2f 31 2e 30 0d 0a 48 6f 73 74 3a 20 77 77   TP/1.0..Host: ww
0070  77 2e 58 58 58 58 2e 63 6f 6d 0d 0a 55 73 65 72   w.XXXX.com..User
0080  2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f   -Agent: Mozilla/
0090  35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b   5.0 (Windows; U;
00a0  20 57 69 6e 39 38 3b 20 65 6e 2d 55 53 3b 20 72    Win98; en-US; r
00b0  76 3a 30 2e 39 2e 39 29 20 47 65 63 6b 6f 2f 32   v:0.9.9) Gecko/2
```

```
00c0  30 30 32 30 33 31 31 0d 0a 41 63 63 65 70 74 3a   0020311..Accept:
00d0  20 74 65 78 74 2f 78 6d 6c 2c 61 70 70 6c 69 63    text/xml,applic
00e0  61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 70 6c 69 63   ation/xml,applic
00f0  61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c   ation/xhtml+xml,
0100  74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30 2e 39 2c   text/html;q=0.9,
0110  74 65 78 74 2f 70 6c 61 69 6e 3b 71 3d 30 2e 38   text/plain;q=0.8
0120  2c 76 69 64 65 6f 2f 78 2d 6d 6e 67 2c 69 6d 61   ,video/x-mng,ima
0130  67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f 6a 70 65   ge/png,image/jpe
0140  67 2c 69 6d 61 67 65 2f 67 69 66 3b 71 3d 30 2e   g,image/gif;q=0.
0150  32 2c 74 65 78 74 2f 63 73 73 2c 2a 2f 2a 3b 71   2,text/css,*/*;q
0160  3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d 4c 61 6e   =0.1..Accept-Lan
0170  67 75 61 67 65 3a 20 65 6e 2d 67 62 2c 20 65 6e   guage: en-gb, en
0180  2d 75 73 3b 71 3d 30 2e 35 30 0d 0a 41 63 63 65   -us;q=0.50..Acce
0190  70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69   pt-Encoding: gzi
01a0  70 2c 20 64 65 66 6c 61 74 65 2c 20 63 6f 6d 70   p, deflate, comp
01b0  72 65 73 73 3b 71 3d 30 2e 39 0d 0a 41 63 63 65   ress;q=0.9..Acce
01c0  70 74 2d 43 68 61 72 73 65 74 3a 20 49 53 4f 2d   pt-Charset: ISO-
01d0  38 38 35 39 2d 31 2c 20 75 74 66 2d 38 3b 71 3d   8859-1, utf-8;q=
01e0  30 2e 36 36 2c 20 2a 3b 71 3d 30 2e 36 36 0d 0a   0.66, *;q=0.66..
01f0  4b 65 65 70 2d 41 6c 69 76 65 3a 20 33 30 30 0d   Keep-Alive: 300.
0200  0a 50 72 61 67 6d 61 3a 20 6e 6f 2d 63 61 63 68   .Pragma: no-cach
0210  65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c   e..Cache-Control
0220  3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 46 6f 72 77   : no-cache..Forw
0230  61 72 64 65 64 3a 20 62 79 20 68 74 74 70 3a 2f   arded: by http:/
0240  2f 70 68 61 6e 74 6f 6d 2e 73 69 6e 67 61 70 6f   /phantom.singapo
0250  72 65 2e 73 75 6e 2e 63 6f 6d 3a 38 30 38 30 20   re.sun.com:8080 
0260  28 4e 65 74 73 63 61 70 65 2d 50 72 6f 78 79 2f   (Netscape-Proxy/
0270  33 2e 35 31 29 0d 0a 0d 0a                        3.51)....
```

### 2.2.2 Snort Dump of Detect

```
[**] [1:1171:6] WEB-MISC whisker HEAD with large datagram [**]
[Classification: Attempted Information Leak] [Priority: 2]
07/15-13:15:37.724488 192.18.17.3:39502 -> 46.5.180.133:80
TCP TTL:236 TOS:0x0 ID:9451 IpLen:20 DgmLen:619
***AP*** Seq: 0x199EFF94  Ack: 0x5596C508  Win: 0xFAF0  TcpLen: 20
[Xref => http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html]

[**] [1:1171:6] WEB-MISC whisker HEAD with large datagram [**]
[Classification: Attempted Information Leak] [Priority: 2]
07/15-13:16:00.414488 192.18.17.3:40492 -> 46.5.180.133:80
TCP TTL:236 TOS:0x0 ID:9457 IpLen:20 DgmLen:619
***AP*** Seq: 0x20F70DC8  Ack: 0x56FDE53F  Win: 0xFAF0  TcpLen: 20
[Xref => http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html]
```

Let us look at the interesting fields in this detect:

Source IP: 192.18.17.3 .The ARIN lookup given below suggests that the IP is assigned to SUN Microsystems which can be considered to be a friendly IP unless the IP is spoofed.

Source Port : 39502 & 40492 .It is a normal empheral port.

Destination IP: 46.5.180.133.This is the Web server for Public access.

Destination Port: 80.This indicates that the traffic was HTTP traffic.

TTL: 236.This indicates the source machine to be a Unix variant and 19 hops have been traversed.

Flags: Acknowledgement and Push flags have been set indicating that three way handshake has been completed and the application wants the data to be processed immediately without waiting for the buffer to fill up.

The IP ID is changing normally and the source port is also changing. So the traffic so far indicates that there is nothing malicious about the packets so far captured. The interesting thing about this detect would be the content " HEAD /ftppub/chips/appnote/ir_utils.zip" which is suspiciously different from the GET parameter which you normally find in a regular HTTP request.

### 2.2.3 Snort Rule for Detect

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC whisker HEAD with large datagram"; content:"HEAD"; offset: 0; depth: 4; nocase; dsize:>512; flags:A+; classtype:attempted-recon; reference:url,www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html; sid:1171;  rev:6;)

The alert was generated because the datagram was greater than 512 bytes and also had the content "HEAD" in it.

### 2.2.4 Source of Trace

The source of this trace was from the file http://www.incidents.org/logs/raw/2002.6.15.  The raw file was then further analyzed using Ethereal and snort.

### 2.2.5 Detect Generated By

This detect was generated by Snort 1.8.6 running on windows 2000 SP2 and using snort.conf,v 1.77.2.19 dated 2002/06/29
The snort command used to generate the above snort alert was:

```
snort -c snort.conf -d -e -l log -r 2002.06.15
```

The options used are:

-c  snort.conf =use rules from snort.conf
-d =Dump the application layer
-e= Display the second layer header info
-l log=log directory
-r 2002.6.15=to read and process Tcpdump file  2002.6.15

The log was further analyzed using Ethereal ver 0.9.3 running on windows 2000 sp2 with the filter

```
    IP.addr eq 192.18.17.3 and IP.addr eq 46.5.180.133
```

### .2.2.6 Probability the Source Address was spoofed

The possibility that source is spoofed is remote since the objective of the attack is to run Whisker which is a CGI vulnerability scanner and to get the results and use it as launching pad for further attacks. Moreover going through the Ethereal output we could see that three-way handshake already has been made and the data transfer was taking place. Probability of source routing and sniffing exists but this probability would be too small.

**Search results for: 192.18.17.3**

```
OrgName:    Sun Microsystems, Inc
OrgID:      SUN

NetRange:   192.18.0.0 - 192.18.194.255
CIDR:       192.18.0.0/17, 192.18.128.0/18, 192.18.192.0/23, 192.18.194.0/24
NetName:    SUN1
NetHandle:  NET-192-18-0-0-1
Parent:     NET-192-0-0-0-0
NetType:    Direct Allocation
NameServer: NS.SUN.COM
NameServer: NS.EU.SUN.COM
NameServer: NS.USEC.SUN.COM
Comment:
RegDate:    1985-09-09
Updated:    2002-01-16

TechHandle: IS189-ARIN
TechName:   Sun Microsystems, Inc.
TechPhone:  +1-303-272-7000
TechEmail:  Netmaster@sun.com

# ARIN Whois database, last updated 2002-11-09 19:05
# Enter ? for additional hints on searching ARIN's Whois database.
```

This indicates that request came from an IP from the SUN organization. From the ethereal TCP stream analysis, it is clearly suggested request indeed came from sun proxy server and HEAD is a TCP header quite commonly used by proxy servers to check for the validity of their cached information. Taking also into consideration that the file in question here is a zip file while whisker is mainly used to scan for CGI scripts, this looks like a perfectly legitimate connection from the SUN proxy server enquiring the web server about the requested file and hence no need for the machine to use a spoof the IP.

### 2.2.7 Description of the Attack.

Whisker is a tool that will scan for CGIs that are badly written and contains security problems. This tool can be used by an attacker to scan the web server and then launch an attack based on the information obtained. Whisker evades IDS systems by slightly modifying the http request. As most IDS systems are expecting to pattern match particular requests to indicate an attack, modifying the request may allow the attacker to scan without detection.

Whisker utilizes various techniques to evade detection including this method in which HEAD method is used instead of GET to evade detection by the IDS. The HEAD method allows the attacker to determine the existence, for example, of a vulnerable CGI script or file on the Web Server. If an IDS does not detect the HEAD method, the scan may go unnoticed

### 2.2.8 Attack Mechanism.

In this particular attack using, the attacker uses the HEAD method instead of the GET method for the CGI scan hoping that IDS implementation at the victim site would not be scanning for the HEAD method. From the RFC for HTTP/1.1,HEAD method is defined as:

The HEAD method is identical to GET except that the server MUST NOT return a message-body in the response. The metainformation contained in the HTTP headers in response to a HEAD request SHOULD be identical to the information sent in response to a GET request. This method can be used for obtaining metainformation about the entity implied by the request without transferring the entity-body itself. This method is often used for testing hypertext links for validity, accessibility, and recent modification.

Attacker will have to use the GET method later to exploit the CGI but it is often possible to use the HEAD and POST depending on how the CGI is coded.

Now going through the default scan.db used by Whisker, it scans for cgi, cfm,cgi,sh,exe,htr,pl &idc files. If we observe the ethereal TCP stream analysis below, the file requested by this HEAD request is a zip file which is not included with default scan.db but of course this can be included but then a zip file cannot be vulnerability and an attacker doing a vulnerability CGI scan would not be interested in the existence of zip file. The TCP stream analysis done using Ethereal gives the output as below:

```
HEAD /ftppub/chips/appnote/ir_utils.zip HTTP/1.0
Host: www.XXXX.com
User-Agent: Mozilla/5.0 (Windows; U; Win98; en-US; rv:0.9.9) Gecko/20020311
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-
mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1
Accept-Language: en-gb, en-us;q=0.50
Accept-Encoding: gzip, deflate, compress;q=0.9
Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66
Keep-Alive: 300
Pragma: no-cache
Cache-Control: no-cache
Forwarded: by http://phantom.singapore.sun.com:8080 (Netscape-Proxy/3.51)

HEAD /ftppub/chips/appnote/ir_utils.zip HTTP/1.0
Host: www.XXXX.com
User-Agent: Mozilla/5.0 (Windows; U; Win98; en-US; rv:0.9.9) Gecko/20020311
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-
mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1
Accept-Language: en-gb, en-us;q=0.50
Accept-Encoding: gzip, deflate, compress;q=0.9
Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66
Keep-Alive: 300
Pragma: no-cache
Cache-Control: no-cache
Forwarded: by http://phantom.singapore.sun.com:8080 (Netscape-Proxy/3.51)
```

Now the above TCP stream also indicates that the HTTP request has come from phantom.Singapore.sun.com and our above ARIN output for the source IP 192.18.17.3 has indicated that the source was originating from the SUN.com range of IP`s. So combining this with the facts that the requested file is a harmless zip file and the requesting source is a proxy server which uses the HEAD method to validate its cache information we can safely consider this to be a false positive. The large datagram size is to the large no of options, which has been, send along with the HTTP header. Other thought to this can be whether the attacker is trying to see whether he can evade the IDS by trying to request the zip file but lack of any further communication from the source using the HEAD method suggests us that this was just a one time access for the zip file.

**2.2.9 Correlations**

The entire details of how Whisker can be used to evade NIDS can be found in the URL.

http://rr.sans.org/intrusion/net_id.php

The white paper for the Whisker can be found at:

http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html.

### 2.2.10 Evidence of Active Targeting

Since we can see only this FTP communication from the source 192.18.17.3, this can be termed as an active targeting even though we could not find any malicious intent from the source.

### 2.2.11 Severity

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

Criticality: 5 –Since the destination of the above suspected probe is a public web server, the criticality can be considered to be very high

Lethality: 4**-** Since such type of scans can give information about the vulnerable scripts and files on the web server and this vulnerability can be used by the attacker to launch more lethal attacks on the server later on, we can consider it to be severe.

System Countermeasures: 2 – Some of the System countermeasure for such attacks would be to make sure that vulnerable scripts do not exist in the CGI folder. Since I am not sure whether such a precaution has been taken care in case of this server, I would be giving low points to this.

Network Countermeasures: 2–The Network countermeasures, which could be useful for such exploits, would be as follows:

NIDS implemented should be able to detect attacks with HEAD methods and should be updated with current signature base to detect current attacks. In case of Web servers for the public access, even though there cannot be much access control in place, an application level proxy firewall can detect application level attacks at the perimeter itself and can reduce the risk to web server itself. Also integrating your NIDS with the firewall using protocols like SAMP to blacklist the culprit source IP can really strengthen the protection against such attacks.

But since I am not sure whether such countermeasures which are in place here, I would assign a low point here.

Severity = (5 + 4) **-** (2 + 2) = 5

### 2.2.12 Defensive Recommendation

1] Make sure your Web server does not have any sample scripts or unnecessary scripts or files that can leak precious information. Install only what is necessary. The default scripts that come along with web servers should be deleted. Scripts downloaded from popular sites should not be used and if new scripts are being written, the security of these scripts should be thoroughly checked.

2] There are numerous tools to choose from to audit Web servers like Enterprise Security Manager from Symantec which can tell you Vulnerabilities existing on you web server and you can schedule it to run at prespecified intervals to automate frequent audits.

3] Make sure you have the latest word on the wire: subscribe to security-oriented mailing lists such as BugTraq.

4] Apply the patches and Service packs released by the Vendors as soon as it is available so as to secure yourself from any vulnerability, which would be taken care by this patches.

5] Make sure that you have proper ACL`S implemented at the Gateway routers and firewall so that only the valid traffic passes to the critical server. Make sure you have updated signatures running on the NIDS to detect such attacks.

### 2.2.13 Multiple Choice Test Question

snort alert "**WEB-MISC whisker HEAD with large datagram"** would signify the datagram size to be greater than

A . 64 bytes
B. 80 bytes
C. 512 bytes
D. 1024 bytes

The correct answer is C

## Detect #3 – WEB-CGI formmail access

### 2.3.1 Ethereal output of the detect:

```
Frame 375 (363 on wire, 363 captured)
    Arrival Time: Jul 16, 2002 14:53:47.504488000
    Time delta from previous packet: 0.000000000 seconds
    Time relative to first packet: 33521.620000000 seconds
    Frame Number: 375
    Packet Length: 363 bytes
    Capture Length: 363 bytes
Ethernet II
    Destination: 00:00:0c:04:b2:33 (00:00:0c:04:b2:33)
    Source: 00:03:e3:d9:26:c0 (00:03:e3:d9:26:c0)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 4.60.116.235 (4.60.116.235), Dst Addr: 46.5.180.133 (46.5.180.133)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 349
    Identification: 0x49ef
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 113
    Protocol: TCP (0x06)
    Header checksum: 0x6900 (incorrect, should be 0x62fa)
    Source: 4.60.116.235 (4.60.116.235)
    Destination: 46.5.180.133 (46.5.180.133)
Transmission Control Protocol, Src Port: 4516 (4516), Dst Port: 80 (80), Seq: 3247506754, Ack: 97929686
    Source port: 4516 (4516)
    Destination port: 80 (80)
    Sequence number: 3247506754
    Next sequence number: 3247507063
    Acknowledgement number: 97929686
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17520
    Checksum: 0x54ae (incorrect, should be 0xfd0a)
Hypertext Transfer Protocol
    GET /cgi-bin/formmail.pl?email=f2@aol.com&subject=www.XXXX.com/cgi-
bin/formmail.pl&recipient=organizedring@AOL.COM&msg=w00t 0AOL%2ECOM&msg=w00t
HTTP/1.1Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Gozilla/4.0 (compatible; MSIE 5.5; windows 2000)\r\n
    Host: www.XXXX.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

Let us look at the interesting fields here.

Source IP: 4.60.116.235.

Whois information of the source:

```
Genuity GNTY-4-0 (NET-4-0-0-0-1)
                                  4.0.0.0 - 4.255.255.255
GTE Intelligent Network Services GTEINS-60-88-30 (NET-4-60-88-0-1)
                                  4.60.88.0 - 4.60.131.255 .
```

Source Port: 4516.I could not find anything wrong with this port. Checking in Google also could get any sinister information about this port.

Destination IP: 46.5.180.133.This is web server used for Public access.

Destination Port: 80 indicating web communication.

IP ID: 18927.This also do not indicate any thing wrong in the packet.

TTL: 113.this suggests mostly the source is window based machine and the packet has traversed 15 hops.

Flags: The push and acknowledgement flag is set is indicating that the three way handshake has been completed and the application wants the data to be processed immediately.

The interesting part of this capture would be the content

```
GET /cgi-bin/formmail.pl?email=f2@aol.com&subject=www.XXXX.com/cgi-
bin/formmail.pl&recipient=organizedring@AOL.COM&msg=w00t 0AOL%2ECOM&msg=w00t.
```

Now the email address of f2@aol.com and organizedring@AOL.com sounds fishy and hence suggesting that the attacker in this case wants to make use of vulnerability existing in the formmail.pl and send himself the e-mail and once this gets successful, he can be sure that the web server is running the vulnerable version of the formmail.pl and then launch further attacks based on this information.

### 2.3.2 Snort Dump of Detect

```
[**] [1:884:6] WEB-CGI formmail access [**]
[Classification: _] [Priority: 2]
07/16-14:53:47.504488 4.60.116.235:4516 -> 46.5.180.133:80
TCP TTL:113 TOS:0x0 ID:18927 IpLen:20 DgmLen:349 DF
***AP*** Seq: 0xC1910542  Ack: 0x5D649D6  Win: 0x4470  TcpLen: 20
[Xref => http://www.securityfocus.com/bid/1187]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0172]
[Xref => http://www.whitehats.com/info/IDS226]
```

### 2.3.3 Snort Rule for Detect

```
 $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-CGI formmail
access";flags:A+; uricontent:"/formmail"; nocase; reference:bugtraq,1187; reference:cve,CVE-1999-0172;
reference:arachnids,226; classtype:web-application-activity; sid:884;  rev:6;)
```

The alert is generated when Snort detects the content “/formmail” in the uri content with destination port as 80.

### 2.3.4 Source of Trace

The source of this trace was from the file http://www.incidents.org/logs/raw/2002.6.16 .The raw file was then further analyzed using Ethereal and snort.

### 2.3.5 Detect Generated By

This detect was generated by Snort 1.8.6 running on windows 2000 SP2 and using snort.conf,v 1.77.2.19 dated 2002/06/29.

Snort was used with the command line option:

```
snort -c snort.conf -d -e -l log -r 2002.6.16.
```

The options used are :

-c  snort.conf =use rules from snort.conf
-d =Dump the application layer
-e= Display the second layer header info
-l log=log directory
-r 2002.6.16=to read and process Tcpdump file  2002.6.16

The log was further analyzed using Ethereal ver 0.9.3 running on windows 2000 sp2 with the filter

```
    IP.addr eq 4.60.116.235  and IP.addr eq 46.5.180.133.
```

### 2.3.6 Probability the Source Address was spoofed.

Since the attacker will have to establish the three way handshake before he can use the GET option and since the Push and acknowledgement flag is set in the packet captured, it indicates that three way handshake has been completed and hence the probability of the IP address being spoofed is very low. However we cannot rule the Sequence number prediction by sniffing or having static route added but the probability would be quite low.

### 2.3.7 Description of the Attack.

Formmail is perl based web-based e-mail gateway on Linux, Unix variants and Window based machines. It allows form-based input to be e-mailed to the specified used. It is very widely used but one of the downfalls of this program is that it do not perform enough security check to prevent anonymous e-mail using vulnerable host as mail relays and this leads to remote users being able to send emails to arbitrary reciepents. The main reason for this that the script relies on a HTTP variable for this email address and do not provide any information on the original sender in the email and this lack of security is exploited by users with malicious intent to send anonymous Spam or forged e-mail. Eventhough Formmail does perform a basic security check on the HTTP_REFERER server variable but this is only used to make sure that form submitted by a user came from the proper or designated domain but even this can be bypassed by passing raw HTTP request faking the HTTP referrer.

### 2.3.8 Attack Mechanism.

The attack works by completing the TCP three-way handshake, then sending an HTTP GET to the server. In this case, the request looks like this GET /cgi-bin/formmail.pl?email=f2@aol.com&subject=www.XXXX.com/cgi-bin/formmail.pl&recipient=organizedring@AOL.COM&msg=w00t 0AOL%2ECOM&msg=w00t HTTP/1.1.

The GET appears to set the recipient value to organizedring@AOL.COM . It also sets a fake sender address f2@aol.com and the subject is set to the URL (web server) that is being tested.

The attacker here is exploiting this vulnerability to send anonymous SPAM, as no indication of the original sender (via the CGI interface) will be in the email. That means the attacker could possibly send SPAM that appeared to come from our web servers. Also once he is successful in getting the reply from the above exploit, he will know that the server is running the vulnerable version of Formmail and then he can make use of other vulnerabilities associated with the formmail which would be more harmful.

### 2.3.9 Correlations

Montgomery Toren has discussed this exploit in detail in his GCIA submission at

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

The formmail Recipient CGI Variable Spamming Vulnerability is discussed in great detail at

http://online.securityfocus.com/bid/2469/discussion/.

How the Formmail.pl Can Be Used As An Open Mail Relay is described in

http://www.securiteam.com/securitynews/Formmail_pl_Can_Be_Used_As_An_Open_Mail_Relay.html

### 2.3.10 Evidence of Active Targeting

Since the only communication from 4.60.116.235 is to the web server 46.5.180.133 this definitely is active targeting.

### 2.3.11 Severity

Severity = (Criticality + Lethality) - (System Countermeasures + Network
Criticality = 5.Since the server is the corporate web server used for Public access.

Lethality =3.Since this exploit cannot possibly bring down the server. But if the server is used for SPAM and comes into any Blackhole list, it could be a loss of face for the organization. Moreover the attacker can use the result of this exploit to ensure that the server is running the vulnerable formmail.pl and then launch other lethal attacks on the server.

System Countermeasure=2.The System Countermeasure for this has to make sure that the patched up version formmail.pl is used. Since I am not sure that this has been done on the server, I will be giving lower points to it.

Network Countermeasures=2.The Network countermeasure here would be to have ACL or Firewall to restrict only the port 80 traffic from the web server, if there is no mailing has to take place from the web server. Since I am not sure whether this has been implemented, I would be giving it low points.

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

### 2.3.12 Defensive Recommendation

1] Make sure your Web server does not have any sample scripts or unnecessary scripts or files that can leak precious information. Install only what is necessary. The default scripts that come along with web servers should be deleted. Scripts downloaded from popular sites should not be used and if new scripts are being written, the security of these scripts should be thoroughly checked. In this particular case, if formmail.pl is not required, it should be deleted.

2] If formmail.pl has to be used make sure the patched version is used and if possible Hard code the recipient's email address in the formmail.pl program. Do not rely on the address submitted by the user.

3] Use tools like Whisker to periodically check for existing vulnerable CGI scripts. It would be advisable to implement auditing applications like Enterprise Security Manger from Symantec to automate the auditing for Vulnerabilities like existence of vulnerable CGI scripts for critical servers.

4]Make sure that proper ACLs are implemented at the gateway and perimeter level to prevent any unauthorized traffic from going across the perimeter.

5]Make sure that security reference sites like bugtraq and CVE is periodically checked to get the latest information on latest vulnerabilities.

### 2.3.13 Multiple Choice Test Question

Which pre-processor module must be enabled in the snort.conf to detect the URI content "/formmail" in the above detect?

A]http_decode.

B]stream4.

C]frag2

D]minfrag.

Correct Answer: A.

# ASSIGNMENT #3: Analyze This

## Executive Summary:

This is a security audit for a university covering five consecutive days of events. The data was broken up into three different kinds of information generated using the popular Snort IDS. Alert files consisting of snort alert information were supplemented by Scan files, which were Snort scan reports. In addition the university provided information regarding Out of Spec packets that were detected on their network.

The following table lists the files selected for analysis:

| | | |
|---|---|---|
| alert.021024 | OOS_Report_2002_10_24_13248.txt | scans.021024 |
| alert.021025 | OOS_Report_2002_10_25_1543.txt | scans.021025 |
| alert.021026 | OOS_Report_2002_10_26_18726.txt | scans.021026 |
| alert.021027 | OOS_Report_2002_10_27_362.txt | scans.021027 |
| alert.021028 | OOS_Report_2002_10_28_28192.txt | scans.021028 |

After analyzing the files, it can be concluded that University has to improve on their perimeter protection including ACL`s on Router, Rulesets of firewall, Potential networkproblems, Antivirus protection, stricter enforcement of policies as to application and services loaded on user workstations, finetuning of the IDS signatures etc. These are explained in detail along with Top Ten alerts, Scans and OOS Top talker's discussion given below. The analysis could have been more comprehensive if the University had provided the actual ruleset used by Snort, a detailed networked diagram showing their critical servers, a list of applications authorized to run on the Internal network. To overcome this limitation of not being provided the complete network diagram, the Alert, Scan and OOS files were referenced for traffic through server ports and the following mapping was done.

MY.NET.100.158 (FTP server)
MY.NET.6.40 (E-Mail Server)
MY.NET.100.217 (E-Mail Server

MY.NET.137.7 ( DNS Server)

MY.NET.134.11 (Web Server)
MY.NET.150.83 (Web Server)
MY.NET.137.66 (Web Server)
MY.NET.84.173 (Web Server)

MY.NET.132.22(Windows DC)

### Top Ten Alerts :

From our analysis of the alert logs it was evident that 213959 alerts occurred while the logs were being created. A breakdown of attacks is as follows

| Signature | # Alerts | # Sources | # Dests |
|---|---|---|---|
| Back Orifice | 1 | 1 | 1 |
| spp_http_decode: IIS Unicode attack detected [**] MY.NET.153.17010/25-15:31:38.515640 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |
| Queso fingerprint [**] 66.28.100.19610/28-21:52:34.348327 [**] Queso fingerprint | 1 | 1 | 1 |
| Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.83.13310/28-16:03:39.527581 [**] SMB Name Wildcard | 1 | 1 | 1 |
| spp_http_decode: IIS Unicode attack detected [**] MY.NET.53.15010/24-16:04:03.694936 [**] SMB Name Wildcard | 1 | 1 | 1 |
| Queso fingerprint [**] 66.28.100.19710/28-17:08:51.394668 [**] Queso fingerprint | 1 | 1 | 1 |
| SMB Name Wildcard [**] 217.98.68.1010/28-15:55:32.348284 [**] Queso fingerprint | 1 | 1 | 1 |
| SMB Name Wildcard [**] 210.180.195.12910/28-22:54:05.233414 [**] spp_http_decode: CGI Null Byte attack detected | 1 | 1 | 1 |
| spp_http_decode: IIS Unicode attack detected [**] MY.NET.88.15010/28-18:32:39.380254 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |
| SMB Name Wildcard [**] 200.207.4.21310/25-17:56:33.486418 [**] FTP DoS ftpd globbing | 1 | 1 | 1 |
| SMB Name Wildcard [**] 128.59.58.19610/28-11:16:29.060384 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |
| Queso fingerprint [**] 66.28.100.19910/28-22:38:20.219506 [**] Queso fingerprint | 1 | 1 | 1 |
| spp_http_decode: IIS Unicode attack detected [**] MY.NET.91.10010/24-15:05:29.775222 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |
| Watchlist 000222 NET-NCFC [**] 159.226.23.49:3029 -> MY.NET.132.2210/24-10:54:47.797271 [**] Watchlist 000222 NET-NCFC | 1 | 1 | 1 |
| Queso fingerprint [**] 66.28.100.196:55802 -> MY.NET.140.210/28-21:26:28.543072 [**] Queso fingerprint | 1 | 1 | 1 |
| spp_http_decode: IIS Unicode attack detected [**] MY.NET.153.16510/25-13:38:22.218618 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |

| | | | |
|---|---|---|---|
| SMB Name Wildcard [**] 212.19.4.19010/28-19:09:10.372031 [**] Queso fingerprint | 1 | 1 | 1 |
| SMB Name Wildcard [**] 218.163.73.4210/24-10:44:51.920844 [**] Watchlist 000222 NET-NCFC | 1 | 1 | 1 |
| Watchlist 000222 NET-NCFC [**] 159.226.23.4910/24-10:54:14.120393 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |
| Queso fingerprint [**] 66.28.100.19810/28-21:49:47.929542 [**] Queso fingerprint | 1 | 1 | 1 |
| Queso fingerprint [**] 66.28.100.20810/28-20:15:34.438668 [**] SMB Name Wildcard | 1 | 1 | 1 |
| SMB Name Wildcard [**] 211.162.214.11310/24-23:21:07.764358 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |
| IDS552/web-iis_IIS ISAPI Overflow ida nosize [arachNIDS] | 1 | 1 | 1 |
| SMB Name Wildcard [**] 65.238.23.3810/26-12:42:16.577379 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |
| Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.83.13310/28-14:50:21.115013 [**] Queso fingerprint | 1 | 1 | 1 |
| SMB Name Wildcard [**] 193.253.205.11110/25-16:54:36.494846 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |
| SMB CD... | 1 | 1 | 1 |
| Queso fingerprint [**] 66.28.100.19710/28-23:46:21.994466 [**] Queso fingerprint | 1 | 1 | 1 |
| spp_http_decode: IIS Unicode attack detected [**] MY.NET.153.45:2180 -> 211.233.29.11210/24-10:48:49.613977 [**] Watchlist 000222 NET-NCFC | 1 | 1 | 1 |
| spp_http_decode: IIS Unicode attack detected [**] MY.NET.108.3410/28-09:30:02.343453 [**] FTP DoS ftpd globbing | 1 | 1 | 1 |
| SMB Name Wildcard [**] 210.180.195.12910/28-22:54:07.955506 [**] spp_http_decode: CGI Null Byte attack detected | 1 | 1 | 1 |
| spp_http_decode: IIS Unicode attack detected [**] MY.NET.106.10810/24-11:01:43.914773 [**] Watchlist 000222 NET-NCFC | 1 | 1 | 1 |
| spp_http_decode: CGI Null Byte attack detected [**] MY.NET.153.20810/24-15:38:16.778226 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |
| SMB Name Wildcard [**] 156.17.95.7810/28-19:54:20.493490 [**] Queso fingerprint | 1 | 1 | 1 |
| spp_http_decode: IIS Unicode attack detected [**] MY.NET.145.19710/25-09:09:10.316573 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |

| | | | |
|---|---|---|---|
| Queso fingerprint [**] 66.28.100.19910/28-22:26:08.780591 [**] Queso fingerprint | 1 | 1 | 1 |
| Queso fingerprint [**] 66.28.100.19910/28-22:44:28.118109 [**] SMB Name Wildcard | 1 | 1 | 1 |
| DDOS mstream handler to client | 1 | 1 | 1 |
| Queso fingerprint [**] 66.28.100.20310/28-20:57:53.399508 [**] Queso fingerprint | 1 | 1 | 1 |
| SMB Name Wildcard [**] 210.123.3.20710/24-19:36:22.498365 [**] SMB Name Wildcard | 1 | 1 | 1 |
| SMB Name Wildcard [**] 202.211.69.8610/25-15:54:04.921401 [**] Tiny Fragments - Possible Hostile Activity | 1 | 1 | 1 |
| Queso fingerprint [**] 66.28.100.197:59272 -> MY.NET.140.210/28-21:27:19.417902 [**] spp_http_decode: IIS Unicode attack detected | 1 | 1 | 1 |
| SMB Name Wildcard [**] 10.1.171.2110/28-22:30:11.835213 [**] Queso fingerprint | 1 | 1 | 1 |
| SMB Name Wildcard [**] 61.220.253.8910/27-12:18:09.691512 [**] Watchlist 000220 IL-ISDNNET-990517 | 1 | 1 | 1 |
| EXPLOIT x86 stealth noop | 2 | 2 | 2 |
| HelpDesk MY.NET.70.49 to External FTP | 2 | 1 | 1 |
| Probable NMAP fingerprint attempt | 2 | 1 | 1 |
| SYN-FIN scan! | 3 | 3 | 3 |
| NIMDA - Attempt to execute cmd from campus host | 4 | 4 | 2 |
| HelpDesk MY.NET.83.197 to External FTP | 4 | 1 | 2 |
| External FTP to HelpDesk MY.NET.83.197 | 4 | 3 | 1 |
| TFTP - External UDP connection to internal tftp server | 6 | 6 | 6 |
| Attempted Sun RPC high port access | 6 | 3 | 4 |
| External FTP to HelpDesk MY.NET.70.49 | 6 | 3 | 1 |
| HelpDesk MY.NET.70.50 to External FTP | 6 | 1 | 2 |
| External FTP to HelpDesk MY.NET.70.50 | 7 | 4 | 1 |
| Bugbear@MM virus in SMTP | 11 | 11 | 4 |
| EXPLOIT NTPDX buffer overflow | 14 | 11 | 10 |
| RFB - Possible WinVNC - 010708-1 | 19 | 11 | 11 |
| TCP SRC and DST outside network | 25 | 13 | 8 |

|  |  |  |  |
|---|---|---|---|
| ICMP SRC and DST outside network | 27 | 5 | 5 |
| EXPLOIT x86 setgid 0 | 51 | 38 | 28 |
| DDOS shaft client to handler | 53 | 2 | 2 |
| EXPLOIT x86 setuid 0 | 68 | 46 | 34 |
| Port 55850 udp - Possible myserver activity - ref. 010313-1 | 69 | 14 | 11 |
| TFTP - Internal TCP connection to external tftp server | 87 | 3 | 3 |
| External RPC call | 118 | 3 | 114 |
| TFTP - Internal UDP connection to external tftp server | 133 | 9 | 13 |
| High port 65535 tcp - possible Red Worm - traffic | 160 | 24 | 27 |
| NMAP TCP ping! | 189 | 28 | 30 |
| SMB C access | 202 | 118 | 14 |
| EXPLOIT x86 NOOP | 216 | 51 | 54 |
| Possible trojan server activity | 242 | 17 | 25 |
| Port 55850 tcp - Possible myserver activity - ref. 010313-1 | 329 | 38 | 38 |
| Null scan! | 479 | 36 | 23 |
| Incomplete Packet Fragments Discarded | 808 | 22 | 16 |
| Tiny Fragments - Possible Hostile Activity | 960 | 4 | 2 |
| SUNRPC highport access! | 1209 | 35 | 37 |
| IRC evil - running XDCC | 1509 | 2 | 11 |
| High port 65535 udp - possible Red Worm - traffic | 4721 | 107 | 100 |
| Watchlist 000222 NET-NCFC | 6735 | 28 | 28 |
| spp_http_decode: CGI Null Byte attack detected | 9949 | 62 | 59 |
| FTP DoS ftpd globbing | 11316 | 14 | 2 |
| Watchlist 000220 IL-ISDNNET-990517 | 12592 | 80 | 66 |
| Queso fingerprint | 27515 | 158 | 48 |
| SMB Name Wildcard | 65910 | 1237 | 896 |
| spp_http_decode: IIS Unicode attack detected | 68147 | 717 | 1501 |

The following are the discussion on top ten alerts. There are also alerts discussed intermittently which do not figure in the Top Ten Alerts but has significance during the course of discussion.

**spp_http_decode: IIS Unicode attack detected**

**Severity:** High

**Reported:** 68147 times.

**Summary:**

An error in Microsoft's IIS 4 and 5 web server allow a crafted URL string to be sent to a web server, which give you access both files and folders anywhere on the local machine. It is possible for an attacker to increases the effectiveness of this attack by copying a cmd.exe file to local machines virtual directory. This would allow an attacker to potentially enable an ftp or telnet session on the remote machine that would allow the intruder to upload malicious code on to the web server. This vulnerability is utilized by worms like Code Red,Code Red II,Nimda and Sadmind.The HTTP_decode Snort Preprocessor is designed to look out for Unicode-encoded "\" "/" and "." Characters on common HTTP ports. Of the 717sources, nearly 380 are originating from the MY.NET network.

**Correlations:**

Tod Beardsley has discussed IIS Unicode in detail in his practical assignment GCIA 3.1 practical. On March-2002.but he could find only 76 sources from the MY.NET network while I could find around 380 such sources within the network. This indicates that University could have increased their machines running Windows in the network and also it indicates that University has not been able to eradicate this vulnerability from this network. University has to take this on priority and implement all the recommendation specified below.

**Recommendation:**

1] University has to have a serious look at their perimeter controls. They should have proper Ingress and Egress filters implemented to drop any packets containing the malicious payload. In case the university is making use of application level proxy firewalls, they can make use of the content filtering which can be configured for the HTTP rules.

2] All the suspected 380 sources should be thoroughly checked for the existence of the worms and if requires should be formatted and rebuilt.

3] University should have do serious rethinking about their Antivirus implementation. University should make sure that they are making use of Antivirus software, which can be centrally managed so as to make sure that the policies deployed are consistent across the network. Also it should be made sure that Antivirus scanning is deployed at all the HTTP, SMTP gateways to scan the traffic at the protocol layer.

4] University should make sure that all the machines in the network is making use of the patches released by Microsoft for these vulnerabilities.

5] Since most of these worms makes use of Microsoft sharing to spread itself across the network, policies should be made so as to disable the sharing of hard disks by the workstations or at least password protect this shares.

6] University should also make sure that only the required services are running on the machines. Most of the client workstations do not require to IIS services running at all. To make this happen, the University should immediately make an action plan to audit the machines in the network to remove the unwanted services. They can also make use of applications like Enterprise Security Manager to automate this process for them. (Symantec discusses Point no 5 & 6 in greater detail at the URL http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html.)

**SMB Name Wildcard:**

**Severity:** Low.

**Reported:** 65910.

**Summary:**

This is a standard netbios name table retrieval query. Windows machines often exchange these queries as a part of the filesharing protocol to determine NetBIOS names when only IP addresses are known. An attacker could use this same query to extract useful information such as workstation name, domain, and users currently logged in. Windows machines typically send these types of queries in normal operation, particularly when filesharing is active, to determine NetBIOS names when only IP addresses are known. This type of query, when originating from an external network, is usually a pre-attack probe to gather netbios name table information such as workstation name, domain, and a list of currently logged in users. There were 1237 sources for this alert and all of them were from external source creating a serious question mark on the ACL`s in place at the Universities perimeter gateways.

193.251.181.131 has 2107 instances of SMB Name Wildcard alerts and the destination IP in this case is MY.NET.132.22.The question would be why was 193.251.181.131. trying to do a netbios name table query with MY.NET.132.22.The who is lookup for 193.251.181.131 gives us the output as follows:

```
inetnum:      193.251.180.0 - 193.251.184.255
netname:      IP2000-ADSL-BAS
descr:        France Telecom IP2000 ADSL Broadband Access Servers
country:      FR
```

So this seems to be customer of France Telecom and he do not require to have netbios access to the University sever.

**Correlations:**

Bryce Alexander explains the SMB Name Wildcard in the IDS FAQ (http://www.sans.org/newlook/resources/IDFAQ/port_137.htm.)
. In this paper, he describes this alert to be caused either by a malicious user using commands like nbtstat – A to retrieve internal information or it could be because of worms like network.vbs.The payload has to be examined to get further information about the exact nature of this query.

Mark Menke has analyzed this alert in his GCIA paper (www.giac.org/practical/Mark_Menke_GCIA.doc). He encountered this alert 338 times in his analysis. He has stated that this could be a malicious traffic to the NetBios port and suggests that this could be severe if the server responds to it.

A detailed Analysis of this alert is done by Chris Grout in his GCIA submission (www.chrisgrout.com/data/chrisgrout_gcia.pdf). Here Chris suggests this alert to be either caused by using commands like nbtstat or nbmlookup. But in his case the scan was done incrementally against the entire class C network but in our case the probe was only targeted to MY.NET.132.22 .So a case of active targeting even though the frequency of probe was as high as described by Chris. . Since there were no more alerts from this source IP, MY.NET.132.22 seems not to have responded back with any critical information Looking for further alerts to MY.NET.132.22, I could find three more IP`s belonging to France telecom probing for the netbios information among 10991 instances of this alert.

**Recommendations:**

1] University has to have a serious relook on the ACL`s implemented at the perimeter gateways. Any unwanted netbios traffic should not be able to cross across the border routers. The firewalls should be check ed.for stricter access rules.

2] The destination IP`s of this alert should be cross-checked for any viral activity. It should be made sure that this machines are running current definitions of the Antivirus.Also the payload of the communication between the suspected sources of this alert and the MY.NET machines should be analyzed more thoroughly to rule out any critical happenings.

**Queso fingerprint:**

**Severity:**

Medium since this would be an attempt to know the OS in question and this information would be used later to launch a more severe attack.

Reported: 27515 times

**Summary:**

The purpose of operating system (OS) fingerprinting is to glean as much information about a remote operating system as possible. Utilities like Queso query the TCP/IP stack for such information. and have the capability of setting and sending bogus flag settings, such as a TCP SYN or TCP RST flag within the TCP header. In this case the alert was generated when Snort detected the existence of reserved bits in the packet.

**Correlation:**

1]Mark Menke discusses the Queso Fingerprint in his practical submission (www.giac.org/practical/Mark_Menke_GCIA.doc.). He has pointed out how OS fingerprinting can be done by making use of illegal flags.

But Queso is rarely used nowadays with the availability better fingerprinting tools like NMAP3.Looking at the destination on which this alert was being reported, I was interested on the machine MY.NET.185.48.This machine had as a destination

4 instances of Possible Trojan server activity

5 instances of Null scan!

52 instances of NMAP TCP ping!

178 instances of Queso fingerprint.

This machine seems to be attracting lot of scans .Now looking at the alert being generated as Queso Fingerprint, I could see that destination port was 6346 for this alert. Now this port is used by Gnutella, which is a file sharing application. One of the alert is a given below:

```
10/24-02:15:36.927154 [**] Queso fingerprint [**] 209.104.74.2:43325 -> MY.NET.185.48:6346.
```

An the corresponding OOS file indicates :

```
10/24-02:15:36.927159 209.104.74.2:43325 -> MY.NET.185.48:6346

TCP TTL:40 TOS:0x0 ID:36135 IpLen:20 DgmLen:60 DF

12****S* Seq: 0x7BA54B83  Ack: 0x0  Win: 0x16D0  TcpLen: 40
```

```
TCP Options (5) => MSS: 1460 SackOK TS: 1105249956 0 NOP WS: 0
```

But normally the initial TTL is supposed to be 255 for Queso packets while the above packets indicate a TTL of 64 and hence could be a packet from Linux machine with ECN bits set. Now this is most probably is Gnutella peer traffic going across ECN enabled routers. Looking at other alerts generated from MY.NET.185.48, the port 6346 seems to be very active and this indicates an active Gnuetella peer. Now taking into consideration the NMAP TCP Ping to MY.NET.185.48, we see that again the destination port is 6346 as seen in the alert below:

```
10/24-21:07:41.973576 [**] NMAP TCP ping! [**] 12.99.244.2:80 -> 123.123.185.48:6346.
```

This alert is generated by snort when it detects a packet with acknowledgement bit set but with acknowledgement number equal to zero. Now checking the alerts generated by 12.99.244.2, I could see the

NMAP TCP ping alert also generated for ports 8028 on MY.NET.122.96, port 6346 on MY.NET.162.198, MY.NET.140.47 on port 32821.The above probe could have been made using the "-g" option so as to make the firewalls think it to be a valid http traffic. I could not find anything interesting which can be listening on 8028 and 32821 while 6346 as we know would be port used Gnutella.This is pointing to some malicious intent from the IP 12.99.244.2.

**NMAP TCP Ping:**

**Severity:** Medium since NMAP can be use to make sure that the remote host is reachable.

**Reported:** 189 times

**Summary:**

NMAP is utility which is used for network exploration and auditing .It supports ping scanning to TCP ports to determine whether remote hosts are up, to determine which services are running on the remote machine and determining the remote machines operating system. In this case snort detected it because of the acknowledgement flag being set with acknowledgement number being zero which matches a NMAP TCP scan.

Correlations:

John Garris (www.giac.org/practical/John_Garris_GCIA.doc.) speaks about this in his practical submission and explains how NMAP is used to fingerprint OS.

The D-Shield look up on 12.99.244.2 is given below:

**IP Address:** 12.99.244.2

**HostName:** 2.muec.lsan.lsancass.dsl.att.net

**DShield Profile:**

| | |
|---|---|
| Country: | US |
| Contact E-mail: | abuse_AT_att.net (bounced) |
| Total Records against IP: | 298 |
| Number of targets: | 103 |
| Date Range: | 2002-12-09 to 2002-12-10 |

Ports Attacked (up to 10):

| Port | Attacks |
|---|---|

**Fightback:** not sent

**Whois:**

```
OrgName:    AT&T WorldNet Services
OrgID:      ATTW

NetRange:   12.0.0.0 - 12.255.255.255
CIDR:       12.0.0.0/8
NetName:    ATT
NetHandle:  NET-12-0-0-0-1
Parent:
NetType:    Direct Allocation
NameServer: DBRU.BR.NS.ELS-GMS.ATT.NET
NameServer: DMTU.MT.NS.ELS-GMS.ATT.NET
NameServer: CBRU.BR.NS.ELS-GMS.ATT.NET
NameServer: CMTU.MT.NS.ELS-GMS.ATT.NET
Comment:    For abuse issues contact abuse@att.net
RegDate:    1983-08-23
Updated:    2002-08-23
```

This IP belongs to the AT&T Worldnet Service an there should be mail send to abuse@att.net informing them about the malicious intent from 12.99.244.2.On checking the alerts involving MY.NET.122.96, I could see 3 more IP`s scanning for port 8028.University should definitely check on the machine to make sure that no Trojan is listening on port 8028.Similarly checking on MY.NET.140.47 activities along with NMAP TCP Ping, I could sense suspicious Trojan activity on this machine. It was also destination for DDOS shaft client to handler alert with 66.168.148.206 as the source and also destination for possible Trojan activity alert with MY.NET.140.47.as source and 24.103.197.64 as destination. The alerts are shown below:

```
10/28-10:39:04.674688  [**] DDOS shaft client to handler [**] 66.168.148.206:5044 ->
MY.NET.140.47:20432

10/28-14:45:28.973507  [**] Possible trojan server activity [**] MY.NET.140.47:27374 ->
24.103.197.64:7158.
```

**DDOS Shaft client to handler.**

**Severity :** High.

**Reported**: 53 times.

**Summary:**

Shaft is DDOS tool in which a client establishes a session by Telnet to masters on TCP port 20432. Client requests attack by passing masters information specifying the victims, the duration of attack and the type of attack (TCP, UDP, ICMP floods or combination of three). Masters then pass this information to daemons to perform the requested attacks. This event could be because of the control traffic from shaft master to shaft handlers. Snort generated this alert when it found TCP traffic going to port 20432.

**Correlations**: could not find much information on this.

**Recommendations:**

1]ACL should be in place to block any traffic initiating to port 20432 of the Internal network.

2] The suspected machine to be scanned for any application running any service on port 20432 and if any service is found, it should be disabled and if possible, the machine should be rebuilt.

Now there was no other alert involving 66.168.148.206.The Dshield lookup of the IP gives the output as follows :

**IP Address:** 66.168.148.206

**HostName:** lebanon-66-168-148-206.midtn.chartertn.net

**DShield Profile:**

| | |
|---|---|
| Country: | US |
| Contact E-mail: | abuse_AT_charter.net (bounced) |
| Total Records against IP: | |
| Number of targets: | |
| Date Range: | to |

Ports Attacked (up to 10):

| **Port** | **Attacks** |
|---|---|

**Fightback:** not sent

**Whois:**

```
CustName:   Charter Communications
Address:    12405 Powerscourt St. Louis MO 63131
Country:    US
RegDate:    2001-11-12
Updated:    2001-11-15

NetRange:   66.168.144.0 - 66.168.159.255
CIDR:       66.168.144.0/20
NetName:    LBN-TN-66-168-144
NetHandle:  NET-66-168-144-0-1
Parent:     NET-66-168-0-0-1
NetType:    Reassigned
Comment:
RegDate:    2001-11-12
Updated:    2001-11-15
```

The address belongs to Charter Communications. Since their contact mail has bounced, they should be informed by phone .It could be that their machine is compromised.

**Possible trojan server activity**

**Severity:** High

**Reported:** 242 times

**Summary:**

This alert indicates presence of subseven 2.1 Trojan since 27374 is the default port used by the Trojan .The alert was generated due to the TCP communication from the port 27374.This would be a response to a connection request.

Subseven is a Trojan for the Windows platform. It consists of two parts Client and server. The hacker uses client to connect to the victim machine. Once he is successful in connecting to the remote machine, he is installs the server part of the Trojan and then he is able to take control of the remote machine fully. There is also editserver.exe component, which enables the hacker to configure the parameters of the server.exe such as the port used by the server, password for server.exe and many other values. The hacker also can get notification when his victim comes online by ICQ, email or IRC.

**Correlations:**

1] http://www.sans.org/newlook/resources/IDFAQ/subseven.htm for the entire details about subseven Trojan.

2]David Oborn has analyzed Subseven in quite detail in his practical assignement at

(www.giac.org/practical/David_Oborn_GCIA.html). In this analyze he has detected a scan from external source to see whether Subseven exists in the machine. But in this case the traffic is taking place from port 27374 indicating that the host MY.NET.140.4 could be compromised.

**Recommendations:**

1] The machine should be looked for existence of Trojan files and if found, the specific entries should be removed. Preferably the machine should be rebuilt from scratch to avoid having any other unknown backdoors in the system.

2] Again a relook in the ACL implemented at the router and firewall should be done to block traffic to and fro unwanted ports.

3] The antivirus policies should be rethinked upon. The best way to detect such Trojans is to have the antivirus running the latest definitions protecting the affected machines.

The IP 24.23.106.20 requires further investigation. The Who is lookup of this IP provides me with the following information. This IP seems to be a customer of Rogers Cable.

**Whois:**

CustName: Rogers Cable Inc. Ym

Address: 1 Mount Pleasant Road Toronto ON M4Y-2Y5

Country: CA

RegDate: 2002-09-17

Updated: 2002-09-17

```
NetRange:   24.103.196.0 - 24.103.197.255
CIDR:       24.103.196.0/23
NetName:    ON-ROG-28-YM-2
NetHandle:  NET-24-103-196-0-1
Parent:     NET-24-100-0-0-1
NetType:    Reassigned
Comment:
RegDate:    2002-09-17
Updated:    2002-09-17

# ARIN Whois database, last updated 2003-01-03 20:00
# Enter ? for additional hints on searching ARIN's Whois database.
```

To make sure that this IP is not involved in any Scan activity, I checked the scans log for any entry for 24.23.106.20 and found that there was indeed some scan activity from MY.NET.86.19 to 24.103.197.64.

```
Oct|25|21|34|36|MY.NET.86.19|1072|->|24.103.197.64|7157|SYN|******S*|
```

The destination port in this case is 7157.Now why would my internal machine go to a cable modem customers 7157 port with initial SYN packet? This warrants further investigation on MY.NET.86.19.

Looking on the alerts involving MY.NET.86.19, I could find 76 alert involving MY.NET.86.19 but none of them involving 24.103.197.64.However I could find around 10 alerts for EXPLOIT x86 setuid 0 alerts. These are normally false alerts and occurs during normal binary file transfers but the remote and local ports in this case are using unusual ports. I could find 7 such alerts from 140.117.93.65 and from ports 511,3083,4386,4530.

### EXPLOIT x86 setuid 0

**Severity**: high if it was a true exploit but this alert is normally false alert arising during some binary file transfer.

**Reported**: 68 times.

**Summary:**

This alert is generated when the attacker has sent the system call setuid(0) to the destination running on x86 platform. The alert was found when Snort found the content |b017 cd80| in the DataStream. By making use of this exploit, the hacker can create a process whose permission is based on the UID of the programs owner rather than that of user executing the program and mostly this would be root and this could lead to the security compromise of machine.

**Correlations:**

1]Ronald Ross has discussed this exploit in details in www.giac.org/practical/Ronald_Ross.doc and he has explained lot of secure way to implement Setuid.

2]Arachnids discusses the Sheelcode-x86-setuid0 in details in its write up on ID283 at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids283&view=event.

3] http://www.acm.uiuc.edu/workshops/security/setuid.html describes how to secure your setuid programs.

**Recommendations.**

1] University should have the ACL implemented at perimeter router and firewalls to prevent access to unauthorized ports.

2] The machines suspected to this exploit has to be audited for existent of backdoors implanted by making use of this exploit. Any unauthorized services should be removed. University should plan of making use of commercial tools available for such auditing process like Symantec Enterprise Security Manager for automating this auditing process and also they should implement Host based IDS for real time alerts when files are modified.

3]The programs running on the suspected machines should be cross checked to make sure that only very necessary programs requiring setuid bit set should have it enabled.

4] All the critical servers should be running the latest Antiviruses with definition updated.

**Whois** for 140.117.93.65 gives

```
 Ministry of Education Computer Center TANET-BNETA (NET-140-117-0-0-1)
                                  140.117.0.0 - 140.138.255.255
Ministry of Education Computer Center TANET-B3 (NET-140-117-0-0-2)
                                  140.117.0.0 - 140.117.255.255

# ARIN Whois database, last updated 2003-01-03 20:00
# Enter ? for additional hints on searching ARIN's Whois database
```

It seems to be some IP belonging to Taiwan and the University should take a look at the machine what was the services using this port. The port 511 is a troublesome one since T0rn rootkit bind to this.

The University should definitely look any unauthorized service running on MY.NET.86.19.

Other Interesting thing observed was there were a lot of scans on port 8995.There were

NMAP TCP Ping, Queso Fingerprint, possible Trojan activity and also watchlist access to this port.

**Possible myserver activity**

**Severity**: high.

**Reported:** 242 alerts with 17 sources and 25 destinations.

**Summary**:

MyServer is a little known DDOS agent. It binds to port 55850, and the rootkit installs Trojans of ls and ps, so it won't be seen running. Netstat has to be run on the server to check whether any services are running on this port and if some unauthorized services are running, it has to be disabled.

**Recommendations**:

1] University should have ACL implemented at the perimeter router and firewall.

2] The machines involved in the alert should be cross checked for existence of any unauthorized service or applications. If any of such services or applications are running, it should be removed.

3] All the machines should be running latest anti-vrus with updated definitions.

I could find 4 Queso fingerprinting attack on MY.NET.86.19 from 216.102.150.127.Looking for further information on 216.102.150.127, we could find that the IP is coming from Pac Bell ADSL service provider.

**Whois** information for 216.102.150.127 is as given below:

```
Pac Bell Internet Services PBI-NET-6 (NET-216-100-0-0-1)

                                  216.100.0.0 - 216.103.255.255
```

```
ADSL BASIC-lsan03 PBI-CUSTNET-7354 (NET-216-102-148-0-1)
                              216.102.148.0 - 216.102.151.255
# ARIN Whois database, last updated 2003-01-03 20:00
# Enter ? for additional hints on searching ARIN's Whois database
```

Looking at the communication from 216.102.150.127, I could find 13 Queso fingerprinting alerts with MY.NET.86.19 and MY.NET.185.48 as the destinations. The destination port for MY.NET.185.48 is 6346, which is used by file sharing application Gnutella.So this machine should be looked by University to make sure that no unauthorized services are running in this machine compromising the security of the entire University Security.

Another one of the Top Ten alerts would be FTP DoS ftpd globbing.

**FTP DoS ftpd globbing**

**Severity**: High.

**Reported**: 11321 times.

**Summary**:

DoS ftpd globbing, is an attempt to crash the server by issuing a command like “LIST */../*../*/../*/../*”. This will often overload the FTP server software, causing it to crash. The Snort rule was activated since it could find the content 2f2a in the DataStream. This alert also sometimes gives false positive if there is genuine wild card request in the FTP request. Many ftpd server versions are affected by a resource saturation attack where a user can request a long directory name that includes numerous "globbing" characters. This request could render many common ftpd servers inoperable

**Recommendation**:

1] Update the applications with the latest patches released by their respective vendors.

2] University should make sure that only the required services are running on the machine.

3] University has to double check the ACL`s implemented on the perimeter router and firewalls.

There were 253 incidents reported from 217.225.222.81 to MY.NET.100.158 and the source port remained unchanged throughout the attack. Whois lookup on this IP gives the following information:

**Whois:**

```
inetnum:     217.224.0.0 - 217.237.161.47
netname:     DTAG-DIAL15
descr:       Deutsche Telekom AG
country:     DE
admin-c:     DTIP-RIPE
tech-c:      ST5359-RIPE
status:      ASSIGNED PA
```

So the IP is coming from the Dutch Telecom  service provider.University should send information on this IP to dbd@nic.dtag.de .

**spp_http_decode: CGI Null Byte attack detected.**

**Severity**: High

**Reported**: 9956 times.

**Summary:**

It is possible to append a NULL character (%00) to the of a web request and display the contents of an arbitrary web-readable file.

Nearly all attacks are launched from the internal network to the external. It's a part of the http preprocessor. Basically, if the http decoding routine finds a %00 in an http request, it will alert with this message. Sometimes you may see false positives with sites that use cookies with urlencoded binary data, or if you're scanning port 443 and picking up SSLencrypted traffic. The content payload has to be further examined to check whether the traffic is malicious or just a false alert.

**Correlation**:

1] (http://online.securityfocus.com/bid/3810/discussion/) has a good discussion on this.

Nearly 2043 of these alerts involve MY.NET.84.173 and the port 80 of 209.10.239.135.Now checking out the whois information of 209.10.239.135,we get the output as:

```
Globix Corporation GLOBIXBLK3 (NET-209-10-0-0-1)
                    209.10.0.0 - 209.10.255.255
IFilm Corp IP007442-209-10-239 (NET-209-10-239-128-1)
                    209.10.239.128 - 209.10.239.191.
```

The IP seems to belong to the domain ifilm.com.Now content of the payload has to be further examined to cross check whether this was a valid attack by MY.NET.84.173.Now checking for any other suspicious activity from MY.NET.84.173, I could find no alerts but going through the scan log I could find it to be the destination of 27 Syn scans for its port 21,80 and 443.University should make sure that it has only the required services are enabled and have a stricter access control.

**Watchlist 000220 IL-ISDNNET-990517**

**Severity** : Medium.

**Reported** : 12592 times with 80 source IP and 66 destnation IP.

**Summary**: The watchlist is provided because of the frequency of scans that are launched from the offending network. The IL-ISDNNET indicates an ISP called ISDNNET located in Israel. It is provided as a signature, and the recommendation is to keep a close watch on the types of traffic coming into your network.

**Recommendation**:

1] If the communication is not required with this network,ACL`s should be implemented to block this IP`s.

From the above watchlist source, 2970 alert generated from the IP. Checking on the destination of this IP, we find that 540 of these alerts are directed to MY.NET.168.35.But this seems to be a harmless communication from MY.NET.168.35 to the Web Server 212.179.35.118.

Doing a reverse lookup on 212.179.35.118 we find that it maps to bzq-179-35-118.dcenter.bezeqint.net, which is the web server for imesh. However the content of the datastream should be checked for any malicious activity since the IP address is from a suspect network. Checking on whether this IP is involved in any Scans or OOS packets. The scans did show me 1823 UDP packets destined for port 1214 of 212.179.35.118 from various MY.NET machines which indicate Kaaza Traffic reiterating the fact that University has a serious problem in their hand if they do not do an immediate auditing of applications active in their network and have a stricter ACL policies.

**Watchlist 000222 NET-NCFC**

**Severity** : Medium.

**Reported** : 6735 times with 28 sources and 28 destinations.

**Summary**:

The watchlist is provided because of the frequency of scans that are launched from the offending network. This IP belongs to the block of IP assigned to Computer Network Center Chinese Academy of Sciences. It is provided as a signature, and the recommendation is to keep a close watch on the types of traffic coming into your network.

**Correlation**:

1]Lenny Zeltser has discussed about this in his SANS practical in www.zeltser.com/sans/idic-practical.

Recommendation:

1]If the communication is not required with this  network,ACL`s should be implemented to block this IP`s.

159.226.23.49 is the IP, which was involved in the maximum number of, alerts about 4798 incidents of the above alert. Looking in the alert file for the destination of this IP, I found that the IP was MY.NET.132.22 and the destination port varying between 1038,1046 and 1058 while the source port remains constant at 3092.University should look on the machine on the applications listening on this port and also should enforce stricter ACL at router and firewall level. Looking for any suspicious scans from 159.226.23.49 in the scans and OOS file, I could not find any entries.

Now checking on whether MY.NET.132.22 is compromised, we will check on the alerts involving this IP.I could not find any indications of this IP being compromised evnthough it was a target of large number of SMB wildcard alerts which was discussed above.

**High port 65535 udp - possible Red Worm – traffic**

**Severity**: High

**Reported**: 4721 with 107 sources and 100 destinations.

**Summary**:

The Adore or Red worm affects Linux systems. It is a program, which creates a backdoor in these systems and sends the information identifying the compromised system to four different e-mails in China and United States. It binds a Trojan backdoor to UDP port 65535 of the infected host. It scans the Internet for hosts vulnerable to LPRng, rpc-statd, wu-ftpd and BIND vulnerabilities. It attempts to send /etc/ftpusers,ps -aux,/root/.bash_history,/etc/hosts,/etc/shadow to adore9000@21cn.com, adore9000@sina.com, adore9001@21cn.com, adore9001@sina.com. Then a package called icmp is run setting up a port to listen and the packet length to watch for. When this information matches, a rootshell gets activated to allow connection. It also sets up a cronjob in cron daily (which runs at 04:02 local time) to run and remove all traces of its existences and then system is rebooted without removing the backdoor.

**Correlations:**

http://www.sans.org/y2k/adore.htm discusses the worm in quite detail.

Recommendations:

1] There should be ACL implemented to block traffic to unwanted ports especially to empheral ports.

2] All the systems should be verified to be running Latest Antivirus with the current definition.

3] The victim machines should be checked up for modified files or backdoors listening. And if possible the system should be rebuilt.

4] Vulnerability Assessment tools like Symantec Enterprise Security Manager should be run scheduled and run periodically to check upon vulnerable services running on critical machines.

5] Host based IDS on critical machines would have really been beneficial for the University for such attacks.

The source IP involved in maximum number of Red Worm alert is 200.153.74.218 with 29 alerts. The whois information for this IP is :

```
inetnum:     200.153.74.192/27
aut-num:     AS10429
abuse-c:     SRL145
owner:       INFORMÁTICA IGARAPAVA LTDA
ownerid:     000.943.237/0001-06
responsible: Jorge Luiz Rodrigues
address:     R. Dr Gabriel Vilela, 259,
address:     14540-000 - Igarapava - SP
phone:       (016) 31722847 []
owner-c:     IIL224
tech-c:      IIL224
created:     20020305
changed:     20020305
inetnum-up:  200.153/16

nic-hdl-br:  IIL224
person:      INFORMÁTICA IGARAPAVA LTDA
e-mail:      jorgelu@SERNET.COM.BR
address:     RUA DR. GABRIEL VILELLA, 259,
address:     14540-000 - IGARAPAVA – SP.
```

This seems to be an ISP from Brazil. Checking for other alerts originating from this IP, I found that there were around total of 55 alerts involving 200.153.74.218 and MY.NET.114.45.On looking further, MY.NET.114.45 seems to be involved in this communication with 200.153.74.218 for about 10 minutes. University should be advised immediately to have a check on this machine. Looking further for suspicious activity from MY.NET.114.45, I could find 32703 UDP scans originating from this IP with source port 2917.something is here and this machine is definitely worth checking by University.

## IRC evil - running XDCC

**Severity**: high

**Reported**: 1509 times with 2 sources and 11 destinations.

**Summary:**

XDCC is an IRC Bot client, which use the IRC facility to distribute files including movies and software. But the downside of this is that XDCC can also be remotely controlled using IRC channels. Also there could be a backdoor planted along with the Bot client which allows an intruder to access the machine with administrative privilege and hence compromising the entire network.

**Correlation**:

1] http://security.duke.edu/cleaning/xdcc.html gives the entire details of the XDCC client.

**Recommendation:**

1] University should have ACL in place, which disallows IRC communication ports used by IRC like 6666,6667,6668,6669 and 7000 at the router or firewall level if they are willing to disallow IRC as a policy.

2] A good password policy should be implemented by the University. There are numerous applications like Symantec Enterprise Security Manager which can be scheduled automatically to scan the critical machine for breach of such policies.

3] Compromised machines should be checked for alteration of critical files or addition of new files as described in the duke site.

4] Implementing host based IDS on critical machines can make sure that such backdoors will not planted on these machines and reducing the probability of compromising the network.

5] All the machines should be running the latest antivirus program with current definition.

The above alert is occurring the maximum number of 960 times between MY.NET.100.220 and 206.167.75.78. The destination port of MY.NET.100.220 is 6667 which is normally used by IRC servers but this is also used by Trojans like Dark FTP,EGO,Subseven ,Trinity,Winsatan.Looking up for the whois information on 206.167.75.78 ,we get

Reseau d'Informations Scientifiques du Quebec (RISQ Inc.) RISQ-206-72-75-C (NET-206-167-72-0-1)

206.167.72.0 - 206.167.75.255

Reseau Interordinateur Scientifique Quebecois [RISQ] RISQ-MULTI (NET-206-167-75-0-1)

206.167.75.0 - 206.167.75.255

# ARIN Whois database, last updated 2003-01-09 20:00

# Enter ? for additional hints on searching ARIN's Whois database.

Now RISQ is a non-commercial network that links universities and government institutions in Quebec. On checking on alerts generated by MY.NET.100.220, it is involved with 1475 IRC alerts to different IP.So university should immediately check on this machine and if IRC is disallowed by policy, the user should be informed of the same.

**SUNRPC highport access!**

**Severity**: high.

**Reported:** 1209 times from 35 sources and 37 destinations.

**Summary**:

This alert would be due to the source scanning the destination to check whether Sun RPC (rpcbind, portmapper) service is running. Then making use of the vulnerabilities existing with this service, the intruder can launch further attacks.

**Correlation**:

Loras Evens discusses about this in her Practical assignment in New Orleans-2001.

**Recommendation**:

1] There should be ACL implemented at the router and firewall to prevent the higher order ports like 32771 used by Ghost portmapper from being accessed by external sources.

2] Internal machines should be cross-checked by the university to confirm that no unwanted service is active on these machines. There has to be frequent auditing done on the network to check out whether unnecessary services are running in the network.

3] Machines should be running the latest software patches released by the vendors.

The source port which was involved in the above alert for maximum number of 689 from 64.28.67.98 to 2 destinations of MY.NET.55.126 and MY.NET.55.144.The whois information for 64.28.67.98 is

```
OrgName:    Cable & Wireless
OrgID:      EXCW

NetRange:   64.28.64.0 - 64.28.95.255
CIDR:       64.28.64.0/19
NetName:    BO2-1
NetHandle:  NET-64-28-64-0-1
Parent:     NET-64-0-0-0-0
NetType:    Direct Allocation
NameServer: DNS01.EXODUS.NET
NameServer: DNS02.EXODUS.NET
NameServer: DNS03.EXODUS.NET
NameServer: DNS04.EXODUS.NET
Comment:    * Rwhois reassignment information for this block is available at:
            * rwhois.exodus.net 4321
            * For abuse please contact abuse@exodus.net
RegDate:
Updated:    2002-08-21.
```

This is a customer of cable and wireless.Now the port 6667 is used by Trojans like Dark FTP,EGO,Subseven ,Trinity,Winsatan etc.So the destination of this IP should be cross checked for any compromise and if found to be compromised,the machines should be rebuilt.

**Top Ten Alert External Source Addresses**

| Source Address | Count of Source Address |
|---|---|
| 80.13.176.77 | 7689 |
| 159.226.23.49 | 4802 |
| 66.28.100.197 | 3363 |
| 66.28.100.203 | 3245 |
| 66.28.100.198 | 3215 |
| 66.28.100.199 | 3111 |
| 212.179.35.118 | 2970 |
| 66.28.100.195 | 2895 |
| 66.28.100.211 | 2436 |
| 66.28.100.207 | 2411 |

**80.13.176.77**

**Whois** :

```
inetnum:     80.13.176.0 - 80.13.176.255
netname:     IP2000-ADSL-BAS
descr:       BSBOR103 Bordeaux Bloc2
country:     FR
admin-c:     WITR1-RIPE
tech-c:      WITR1-RIPE
status:      ASSIGNED PA
remarks:     for hacking, spamming or security problems send mail to
remarks:     postmaster@wanadoo.fr AND abuse@wanadoo.fr.
```

Wanadoo is France Telecoms Internet service and the IP is one of the users of their service.

**Alerts in which the IP is involve**d:

1] FTP DoS ftpd globbing: This IP has 7689 alerts generated of FTP Dos globbing with destination as MY.NET.100.158.

**Recommendation:**

All the recommendations specified in the discussion of FTP DOS ftpd in Top alerts Section should be applicable here.

**159.226.23.49**

**Whois**:

Whois information of this IP shows that belong to The Computer Network Center Chinese Academy of Sciences, which is included in the Watchlist 000222 NET-NCFC.

**Alerts involving the IP**:

1] This IP is involved in 4802 alerts for Watchlist 000222 NET-NCFC.

**Recommendation**:

All the recommendation specified on Top Alerts section for the Watchlist 000222 NET-NCFC should be implemented and also the target of this IP, MY.NET.132.22 should be crosschecked for any compromise.

**66.28.100.195**
**66.28.100.197**
**66.28.100.198**
**66.28.100.199**
**66.28.100.203**
**66.28.100.207**
**66.28.100.211**

**Whois**:

This bunch of IP`s belong Cogent Communications.

**Alerts involving this IP**:

Collectively this IP`s are involved in 26094 alerts for Queso fingerprint alerts. The destination of this alert is MY.NET.140.2 and destination port is 3128.This port is used by Trojans like www tunnel backdoor, RingZero and also this port is used by Squid-http.
Looking at the scans originating from this IP`s there are around 21783 scans. The symptom of ringzero worm consists of probe to three ports 80,8080 and 3128 but here we could find scans only for port 3128 from cogent communications IP and hence pointing towards for a scan for open proxy for anonymous access. However University should check up the target machine to make sure.

**Recommendations**:

1] The University machines involved in this alert should be checked for any compromise.
2] These machines should be running the latest Antivirus with latest definitions.
3] The machines should be checked for any unauthorized services running particularly on port 3128 and if required these services should be disabled.
4]ACL should be crosschecked to make sure  it block access to unwanted ports of the internal machines.

**212.179.35.118**

**Whois** :

```
inetnum:      212.179.35.96 - 212.179.35.127
netname:      EPLICATION-LTD
mnt-by:       INET-MGR
descr:        EPLICATION-LTD-HOSTING
country:      IL
admin-c:      ZV140-RIPE.
```

**Summary** :

This IP is from Israel and comes under Watchlist 000220 IL-ISDNNET-990517 and is involved 2971 watchlist alert. Looking at the communication it seems to be a normal web communication but the

University machines involved with this alert should be checked up for any compromise. Also this IP is involved in1823 instances of scans to port 1214 from the University machines indicating Kaaza communication to be active.

**Recommendation:**

All the recommendation discussed in the section for Watchlist for IL-ISDNNET on Top Alerts section hold true here.

## Top Ten Alert Target Addresses

| Target Address | count of Target Address |
|---|---|
| MY.NET.140.2 | 26088 |
| MY.NET.100.158 | 11031 |
| MY.NET.132.22 | 10985 |
| 209.10.239.135 | 5463 |
| 210.219.201.2 | 4993 |
| 211.115.215.20 | 2706 |
| MY.NET.83.94 | 2311 |
| 211.239.164.180 | 1695 |
| 216.241.219.22 | 1470 |
| MY.NET.70.176 | 1362 |

**MY.NET.140.2**

**Severity**: High. Based on the alerts and scans generated involving this IP, this machine is running web server with FTP services running.

**Summary**:

There were 26089 alerts of Queso Fingerprint with MY.NET.140.2 as destination .Of this 11 alerts had the destination of port 80 which indicates that the intruders were trying to find whether port 80 was up or not. But worrying thing would be 26063 Queso Fingerprint alerts for destination ports 3128 from source IP range of 66.28.100 series, which is discussed on Top Alerts section.

**Recommendation**:

1] University should confirm whether the services including the web service, FTP service should be running on the machine. If these services are not required, University should immediately stop these services. If the services are required, University should make sure that it has all the patches released by vendors and local security like user rights are all in place. Also default passwords and default scripts used by intruders successfully should not be in the system.

2] University should make sure of the service running on Port 3128 since it is used by many Trojans as discussed on Top Alerts section and also used by Squid-Http proxy. If there is indication of Trojan, the system should be thoroughly checked for any changed system files or any backdoors planted. And preferably rebuilt. And if there is Squid Proxy running on this port, service should be stopped and if this is a required service, then all the precaution required to prevent it from being used as open proxy should be taken.

3] University should immediately create policies to block access to unwanted ports of the internal network at the perimeter level by making use of ACL at the router level and rules at the firewall level. University should make sure all the machines are running the latest Antivirus program with updated definitions. Critical servers of the University should be protected by host based IDS and policy management software's like Enterprise Security Manager to make sure that the future compromise of such machines would be minimum.

4] Notification should be send to Cogent Communication to whom which the range of IP`s 66.28.100 belongs and if the scan continues, these range of IP`s should be blocked at the router level.

**MY.NET.100.158**

**Severity**: High. Based on the alerts and scans for this IP, this machine is running the FTP server for the University.

**Summary:**
There seems to 10969 alerts for FTP DoS ftpd globbing, which is discussed on Top Alerts section.
This machine is also involved in 223 scans including port 20 and 53 as source port. This could mean that this machine is running the DNS services and University has to make sure that whether this machine is authorized to run this service or not.

**Recommendation**:
The recommendation on Top Alerts section with respect FTP Dos globbing should be implemented by the university. University also Make sure that unwanted services are not running on this machine and also ACL should be implemented at the router and firewall level to prevent access to unauthorized ports of the internal machines.

**MY.NET.132.22**

**Severity:**

From the alerts originating from this machine, it seems to be windows Domain Controller and hence severity should be high.

**Summary:**

1] The machine is target of 7917 SMB Name Wildcard alerts. This alert is discussed in detail on Top Alerts section.

2] The machine is also target of 4803 alerts for Watchlist 000222 NET-NCFC indicating that this machine is an attraction for the Ips belonging to Computer Network Center Chinese Academy of Sciences. This alert is discussed in detail on Top Alerts section

**Recommendation**:

Along with recommendations specified with above alerts discussion, for this particular machine University should make sure that:
1]ACL is implemented at the Router and Firewall level preventing access to port 137 of internal machines.
2] The IP`s belonging to the Chinese Academy of sciences should be blocked at the router level.
3] This particular machine should be checked for any compromise and the corrective action should be taken.

**209.10.239.135**

**Whois:**

Globix Corporation GLOBIXBLK3 (NET-209-10-0-0-1)
209.10.0.0 - 209.10.255.255
IFilm Corp IP007442-209-10-239 (NET-209-10-239-128-1)
209.10.239.128 - 209.10.239.191.

This IP belong to Ifilm corporation.

**Summary :**

This IP is involved in 5463 alerts of CGI Null Byte attack which is discussed in detail on Top Alerts section .

**Recommendation:**
The recommendation specified in Top Alerts section should be implemented by the University and also Ifilm corp should be notified of the malicious activity from their ip .

**210.219.201.2**
**211.115.215.20**
**211.239.164.180**

**Whois :**

```
inetnum:      210.216.0.0 - 210.219.255.255
               211.104.0.0 - 211.119.255.255
              211.232.0.0 - 211.255.255.255
netname:      KRNIC-KR
descr:        KRNIC
descr:        Korea Network Information Center
country:      KR
admin-c:      HM127-AP
tech-c:       HM127-AP
```

This IP belongs Korea Network Information Center.

**Summary:**

The IP 210.219.201.2 is involved with 4993 alerts IP 211.115.215.20 is involved in 2706 alerts and ip 211.239.164.180 is involved with 1695 alerts of IIS Unicode attack .This alert is discussed in detail on Top Alerts section .

**Recommendation** :

The recommendation suggested on Top Alerts section for this alert should be implemented by the University.

**MY.NET.83.94**

**Severity :**

This Machine does no seem to run any important service from the alert and scan logs and hence severity can be considered to be low.

**Summary:**

1] This IP is destination of 2308 Watchlist 000220 IL-ISDNNET-990517 alert. This alert is discussed in detail on Top Alerts section .In this case the source port for this alert is 1214 which is used by file sharing applications like Kazaa.

2] This IP is also a source for 78490 scans originating from port 2394 indicating that this machine could possibly compromised.

**Recommendation:**

Along with the recommendation given for the watch list alert on Top Alerts section, University should also follow the recommendation for this particular machine.

1] There should be ACL at the router and firewall level blocking the Watchlist IP`s.
2] The machine seems to be running Kazaa which is a file sharing applications and this should be blocked due to the vulnerabilities associated with it and also since they are the applications which hog the bandwidth most. This service should be removed from the machine and a policy should be implemented by University to prevent any such applications being used by users.

3] The large number of scans originating from the machine indicates that the machine could be compromised. University should make sure that machine is not compromised with no change in critical system file and no backdoors planted. The machine should be checked for the service listening on port 2394 and if any unauthorized service is running on this port, it should be removed.

**216.241.219.22**

**Whois :**

```
OrgName:    The Cobalt Group, Inc
OrgID:      THECOB

NetRange:   216.241.208.0 - 216.241.223.255
CIDR:       216.241.208.0/20
NetName:    COBALT-NET2
NetHandle:  NET-216-241-208-0-1
Parent:     NET-216-0-0-0-0
NetType:    Direct Assignment.
```

This IP belongs to the Cobalt Group.

**Summary :**

This IP is involved in 1470 alerts of CGI Null Byte attack.This alert is discussed in detail on Top Alerts section.

**Recommendation:**

University should follow the recommendation specified in Top Alerts section .

**MY.NET.70.176**

**Severity :**

The machine does not seem to run any important service from the alert and scan logs.

**Summary:**

This IP is involved in 1362 alerts of Portscan which on checking the scan logs indicated to be directed from source port 6257 to destination port 6257.This port is used by winMX which is a file sharing application,

**Recommendations:**

1] University should block all traffic to unwanted IP`s and Services of the internal network by implementing stricter ACL at the router and firewall level.

2] University should undertake an audit of the internal systems and remove all unwanted applications like winMX and the users should be educated about filesharing applications. These applications have their vulnerability associated with it and are also a source of bandwidth hog.

## SCAN LOG TOP TALKERS

**Top Ten External SCAN Source Addresses**

Top Ten External SCAN Source Addresses

| Source Address | count of Source Address |
|---|---|
| 217.225.111.151 | 27171 |
| 217.83.131.59 | 25898 |
| 149.225.38.27 | 16893 |
| 211.177.141.230 | 12555 |
| 202.109.246.4 | 11714 |
| 80.14.167.231 | 10354 |
| 80.128.113.181 | 10224 |
| 4.65.239.246 | 10022 |
| 218.28.1.44 | 9880 |
| 208.255.145.180 | 9406 |

**217.225.111.151**
**217.83.131.59**
**80.128.113.181**

**Whois :**

inetnum:      217.224.0.0 - 217.237.161.47
                    217.80.0.0 - 217.89.31.255
                      80.128.0.0 - 80.146.159.255
netname:      DTAG-DIAL15
descr:        Deutsche Telekom AG
country:      DE
admin-c:      DTIP-RIPE.

So these IP`s seem to be customers of Deutsche Telekom.

**Summary :**

The IP 217.225.111.151 is involved in 27171 scans for port 80 of the entire series of MY.NET.10 .X TO MY.NET.199.254.X and then launching 397 instances of IIS Unicode attack to the hosts who responded to this scan.

The IP 217.83.131.59 is involved in 25898 scans for port 80 of the entire series of MY.NET.15.X to MY.NET.199.254.X and 359 instances of IIS Unicode attack.

The IP 80.128.113.181 is involved in 10224 incidents of scan to port 21 of the MY.NET network and is involved in 6 attempts to do External FTP to the helpdesk machines.

**Recommendation:**

1] The destination of these scans should be checked for any compromise.

2] University should follow recommendation specified for IIS Unicode on Top Alerts section.

3] Mail should be send to Deutshe Telekom indicating the malicious intent from these IP`s.

4] There should be a stricter ACL enforced by the University to make sure only authorized service and authorized ip`s can be accessed by external ip`s.

**149.225.38.27**

**Whois :**

RIPE Network Coordination Centre RIPE-149-206-BLK (NET-149-206-0-0-1)
                              149.206.0.0 - 149.251.255.255
EUnet Deutschland GmbH CUMULUS-1 (NET-149-225-0-0-1)
                              149.225.0.0 - 149.225.255.255

**Summary :**

This IP is involved in16893 instance of scans on MY.NET network for port 80.But there was no alert generated from this IP indicating that IP did not launch any attack after he finished his scan.

**Recommendation:**

1] Eunet should be send mail informing them about the scan from their IP.

2] There should be better ACL at router and firewall level preventing access to services and IP`s not required for external access.

**211.177.141.230**

**Whois :**

inetnum: 211.172.0.0 - 211.199.255.255
netname: KRNIC-KR
descr: KRNIC
descr: Korea Network Information Center
country: KR .

So this IP belongs to Korea Network Information Center.

**Summary :**

This IP is involved in 12555 instances of scans for port 21 of the MY.NET network.There was no alert indicating that there was no attack launched at these ports by 211.177.141.230.

**Recommendation:**

1]There should be ACL implemented at router and firewall to prevent access to not needed internal services and IP`s.

**202.109.246.4**

**Whois :**

inetnum: 202.109.246.0 - 202.109.246.31
netname: FUJIAN-TSANN-LTD
descr: TSANN KVEN CHINA ENTERPRISE
country: CN
admin-c: XY39-AP
tech-c: XY39-AP
mnt-by: MAINT-CHINANET-FJ

**Summary:**

There are 11714 instances of scan for port 80 from this IP for MY.NET addresses. However there is no alert from this IP indicating that there was no attack launched by this IP after the scan.

**Recommendation:**

1]Fujian Tsann Ltd should be informed the malicious probe from their IP.

2] University should enforce stricter ACL at their perimeter to restrict traffic only to required services on required ports.

**80.14.167.231**

**Whois :**

```
inetnum:      80.14.167.0 - 80.14.167.255
netname:      IP2000-ADSL-BAS
descr:        BSSGW111 Ste Genevieve Bloc2
country:      FR
```

This IP belongs to ADSL service provider in France.

**Summary:**

This IP is involved in 11714 instances of scan of port 80 of the MY.NET network and then followed it up with 371 attacks of IIS Unicode attack on the machines which responded to the scan.

**Recommendation:**

1] The recommendation specified for IIS Unicode on Top Alerts section should be followed by the University.

2] There should be stricter ACL enforced by the university to prevent any access to the non-requires IP`s and Services.

**4.65.239.246**

**Whois :**

```
OrgName:    Genuity
OrgID:      GNTY

NetRange:   4.0.0.0 - 4.255.255.255
CIDR:       4.0.0.0/8
NetName:    GNTY-4-0
NetHandle:  NET-4-0-0-0-1 .
```

**Summary:**

This IP was involved in 10022 scans for port 80 of MY.NET network but since there is no alert involving this IP, it seems that no attack was launched by this IP.

**Recommendation:**

1] Mail should be send to Genuity informing about the portscan from their IP.

2] University should enforce stricter ACL to prevent access to unauthorized services and IP`s to the external sources.

**218.28.1.44**

**Whois :**

```
inetnum:      218.28.1.32 - 218.28.1.47
netname:      HA-ZZ-MACHINE-SCHOOL
country:      CN
descr:        Henan Machine School,
descr:        Zhengshang Road,
descr:        Zhenzhou city,
descr:        Henan Province.
```

**Summary :**

This IP is involved in 9880 incidents of scanning port 21 of the MY.NET network and then also involved in 3 alerts of External FTP to HelpDesk machines.

**Recommendation:**

1] University should enforce stricter ACL at the router and firewall level to prevent access to unauthorized services and IP.

2] Mail should be send to HA-ZZ-MACHINE-SCHOOL informing them about the malicious activity from their IP.

3] There should be an internal auditing taken by the University to make sure that no unauthorized services are running on any of the machines in the University network.

**208.255.145.180**

**Whois:**

```
OrgName:    UUNET Technologies, Inc.
OrgID:      UU

NetRange:   208.192.0.0 - 208.255.255.255
CIDR:       208.192.0.0/10
NetName:    UUNET1996B .
```

**Summary :**

This IP is involved in 9406 incidents of scan for port 80 of the internal network. But there seems to be no other alerts involving this IP indicating that no attack was launched from this IP.

**Recommendation:**

1] Mail should be send to UUNet informing about the portscan from their IP.

2] University should enforce stricter ACL to prevent access to unauthorized services and IP`s to the external sources

**Top Ten Internal SCAN Target Addresses**

| Target Address | count of Target Address |
|---|---|
| MY.NET.88.52 | 651 |
| MY.NET.151.72 | 523 |
| MY.NET.100.217 | 521 |
| MY.NET.178.41 | 518 |
| MY.NET.88.122 | 513 |
| MY.NET.53.31 | 483 |
| MY.NET.82.70 | 477 |
| MY.NET.91.87 | 463 |
| MY.NET.158.25 | 455 |
| MY.NET.163.76 | 447 |
| | |

The above report shows the top ten internal hosts that were scanned by external addresses. These hosts should be checked for signs of compromise and corrective measures should be taken.

**Top Ten Scan Destination Ports**

| Destination Port | Count | Description |
|---|---|---|
| 6257 | 2045724 | Used by WinMX which is used for FileSharing |
| 80 | 201492 | Used for HTTP and Web servers have this port open. |
| 27005 | 180349 | Used by Flex-lm |
| 22321 | 99631 | Used by Winnx |
| 1214 | 65369 | Used by Kazaa |
| 21 | 47206 | Used by FTP. |
| 53 | 41047 | Used by DNS |
| 6346 | 33656 | Used by Gnutella and BearShare |
| 3128 | 22184 | Used by Squid-HTTP . |
| 137 | 20106 | Used by Netbios name service |

On having look at the Top Destination ports, we see a lot of scan for filesharing applications like WinMX, Kazaa, Gnutella and Bearshare.University should be warned against these since these have vulnerabilities associated with them and is major cause for bandwidth hog. There are also scans for HTTP, FTP and DNS.University should be asked to apply the latest patches for these and the ACL`s and firewall rules for access to these servers should be thoroughly checked. There is also scan for netbios name service and University should cross check that there is no access to this for external sources by enabling more stricter ACL`s at router and firewall level.

## OOS Top Talkers:

.

**Top Ten External OOS Source Addresses**

Top Ten External OOS Source Addresses

| Source Address | Count of Source Address |
|---|---|
| 209.116.70.75 | 658 |
| 200.221.193.133 | 577 |
| 63.98.19.242 | 247 |
| 61.151.246.250 | 107 |
| 65.33.99.232 | 51 |
| 207.228.236.26 | 42 |
| 195.158.108.36 | 40 |
| 209.132.232.123 | 17 |
| 148.63.81.177 | 2 |
| 204.152.189.120 | 2 |

**209.116.70.75**

**Whois:**

Allegiance Telecom Companies Worldwide ALGX-ABI-BLK14 (NET-209-116-0-0-1)
209.116.0.0 - 209.119.255.255
Inflow INFLOW-RDU2-1 (NET-209-116-68-0-1)
209.116.68.0 - 209.116.71.255
Red Hat, Inc. INFLOW-18773-5591 (NET-209-116-70-64-1)
209.116.70.64 - 209.116.70.95.

So this IP belongs to Red Hat INC.

**Summary :**

This IP was involved in 658 instances of OOS packets. The packets were classified as OOS since it had the reserved bits set with Sin flag set. The destination port for these packets 25.This IP is also involved in 514 instances of Queso Fingerprint alert. The user probably was trying to check out whether the port 25 was listening by sending out the scan in stealth mode.

**Recommendation:**

Along with the recommendation specified for Queso Fingerprint attack, University should also follow the following recommendation for this specific case.

1] University should have stricter ACL policies at the router and Firewall preventing access to unauthorized services and IP`s.

2] The Destinations of these scans should be checked for compromise and corrective action taken, if any compromise is found.

3] Red Hat Inc should be notified about the malicious activity from their IP.

**200.221.193.133**

**Whois :**

owner:     Comite Gestor da Internet no Brasil
ownerid:    BR-CGIN-LACNIC.

So this IP is assigned to ISP in Brazil.

**Summary:**

This IP is involved in 577 incidents of OOS packets. This packets are classified as OOS packets since they have only the push flag set with out the acknowledgement flag. The destination port is 1214 which is used by Kaaza,a file sharing application and the traffic seems to be a normal Kazaa traffic.

**Recommendation:**

1]University should be implement stricter ACL`s at the router and firewall level to block access to unauthorized services and IP`s.

2] University should implement an immediate audit of the machines in the University network to make sure unauthorized services and applications are not running since running applications like Kazaa have vulnerabilities associated with them and also could be one of the major causes for bandwidth hog

**63.98.19.242**

**Whois :**

This IP belongs to UUNET Technologies, Inc.

**Summary :**

This IP is involved in 247 OOS packets. These packets are classified as OOS packets since they have the reserved bits set. The destination of these scans is port 113.Now Port 113 is used by ident authentication service. Since lot of ISP`s do reverse ident lookups for their e-mail sessions, this port has to be open in such cases. Because of this many firewalls do not block access to this port. The intruder here is trying to scan this port hoping that firewall allows access to this port and also he is trying to do a stealth scan by having the reserved bits set. But there seems to be no subsequent alerts from this source, indicating that probably he was not successful in getting the required information.

**Recommendation:**
1] University should implement stricter ACL at router and firewall level to block access to unauthorized IP`s and services.

2] The destination of this scan should be checked for any compromise and if the machine is found to be compromised, corrective action should be taken.

3] UUNET should be informed about the malicious activity from their IP.

**61.151.246.250**

**Whois:**

inetnum: 61.151.245.0 - 61.151.246.255
netname: STATELINE-NETWORK
descr: Stateline Network Co., Ltd. Shanghai
country: CN .

**Summary :**

This IP is involved in 107 OOS packets. These packets are classified as OOS packets since they have reserved bits set with Syn flag set. The destination port for this scan is 113, which is described in above discussion. Also this IP is involved in 47 alerts of Queso fingerprint, which is due to the existence of reserved bit along with Syn flag. This technique of scanning for port 113 involves issuing a response to the ident/auth daemon on port 113 to query the service for the owner of the running process. The main reason behind this is to find daemons running as root, obviously this result would entice an intruder to find a vulnerable overflow and instigate other suspicious activities involving this port. But since there were no other alerts involving this IP, the intruder doesn't seem to have got the desired response.

**Recommendation.**

Along with the recommendation specified on Top Alerts section for Queso Fingerprint and also the recommendation in above discussion, the Stateline-network also should be informed about malicious activity from their IP.

**65.33.99.232**

**Whois :**

rgName: ROADRUNNER-SOUTHWEST
OrgID: RRSW

NetRange: 65.32.0.0 - 65.34.31.255
CIDR: 65.32.0.0/15, 65.34.0.0/19
NetName: ROADRUNNER-SOUTHEAST

**Summary :**

This IP is involved in 51 instances of OOS packets. These packets are classified as OOS since they have the reserved bits set. The IP was scanning for ports 23,113,1080,666 &8888 probably looking for Trojans listening on this port. He is using the scan with reserved bits to make the scan stealthy. This IP is also involved in 12 alerts of queso fingerprint, which is due to the reserved bits set in the packets.

**Recommendation:**

1] There should be a stricter ACL implemented by the University at the router and firewall level to prevent access to unwanted internal IP and services.

2] The destination of this scans should be cross checked for any compromise and in case of compromise, corrective measures should be taken.

3] There should be a strict auditing taken by University on internal network to make sure that no unauthorized services or application are running in the internal network.

4] Roadrunner-Southwest should be informed of the malicious activity from their IP.

**207.228.236.26**

**Whois:**

OrgName: HopOne Internet Corporation
OrgID: HOPO

NetRange: 207.228.224.0 - 207.228.255.255
CIDR: 207.228.224.0/19 .

**Summary :**

This IP is involved in 42 incidents of OOS packets. These packets are classified as OOS since the reserved bits are set with Syn flag. The destination port is 25.This IP is also involved in 8 instances of Queso fingerprint alert. The intruder here is trying to see whether the destination is listening on port 25.He is using the scan with reserved bits for stealth scan. Since this IP is not involved in other alerts, the intruder might have not received any response from his target.

**Recommendation:**

Along with the recommendation specified for Queso Fingerprint attack, University should also follow the following recommendation for this specific case.

1] University should have stricter ACL policies at the router and Firewall preventing access to unauthorized services and IP`s.

2] The Destinations of these scans should be checked for compromise and corrective action taken, if any compromise is found.

3] Hopone should be notified about the malicious activity from their IP.

**195.158.108.36**

**Whois :**

inetnum: 195.158.96.0 - 195.158.127.255
netname: MT-TERRANET-20021024
descr: PROVIDER
descr: TerraNet Ltd
country: MT.

**Summary :**

This IP is involved in 40 instances of OOS packets. These packets are classified as OOS packets because these packets have reserved bits with Syn flag. These scans have destination port of 6346, which is used, by file sharing applications like Gnutella.

**Recommendations:**

1] University should block all traffic to unwanted IP`s and Services of the internal network by implementing stricter ACL at the router and firewall level.

2] University should undertake an audit of the internal systems and remove all unwanted applications like Gnutella and the users should be educated about filesharing applications. These applications have their vulnerability associated with it and is also a source of bandwidth hog

**209.132.232.123**

**Whois :**

Alchemy Communications ALCHEMY-NET-1 (NET-209-132-192-0-1)
209.132.192.0 - 209.132.255.255
Response Base ALCH-137 (NET-209-132-232-96-1)
209.132.232.96 - 209.132.232.127.

**Summary :**

This IP is involved in 17 incidents of OOS packets. These packets are classified as OOS packet because the reserved bits are set with Syn flag set. These packets have destination port of 25 indicating that the intruder was trying to whether SMTP port is open on this IP and then try out the different exploits associated with applications listening on the port. Alert log also indicates 10 incidents of Queso fingerprint alert associated with this IP due to the reserved bit set packets.

**Recommendation:**

1] University should implement ACL on router and firewall level restricting the communication to only authorized IP`s and services.

2] The destination of this scan should be checked for any compromise and corrective measures should be undertaken if this compromise is found to be true.
3] Alchemy communication should be notified about the malicious activity from this IP.

**148.63.81.177**

**Whois :**

OrgName: Spacenet, Inc.
OrgID: SPAN .

This IP belongs to Spacenet Inc.

**Summary :**

This IP is involved in 2 instances of OOS packets. These packets are classified as OOS packet because it has the push flag set without the acknowledgement flag set. These packets have destination port of 3442 of the Internal machine. There seems to be no specific application, which uses this port.

**Recommendation:**

1] University should check upon the destination machine of this packet for the application listening on port 3442.If this application is unauthorized, it should be removed immediately.

2] The machine should be checked for any compromise and if found, corrective action should be taken.

3] There should be ACL implemented at the router and firewall level restricting access to unwanted IP`s and services of the internal network.

**204.152.189.120**

**Whois :**

OrgName: INTERNET SOFTWARE CONSORTIUM, INC.
OrgID: V6IS

NetRange: 204.152.184.0 - 204.152.191.255
CIDR: 204.152.184.0/21 .

**Summary :**

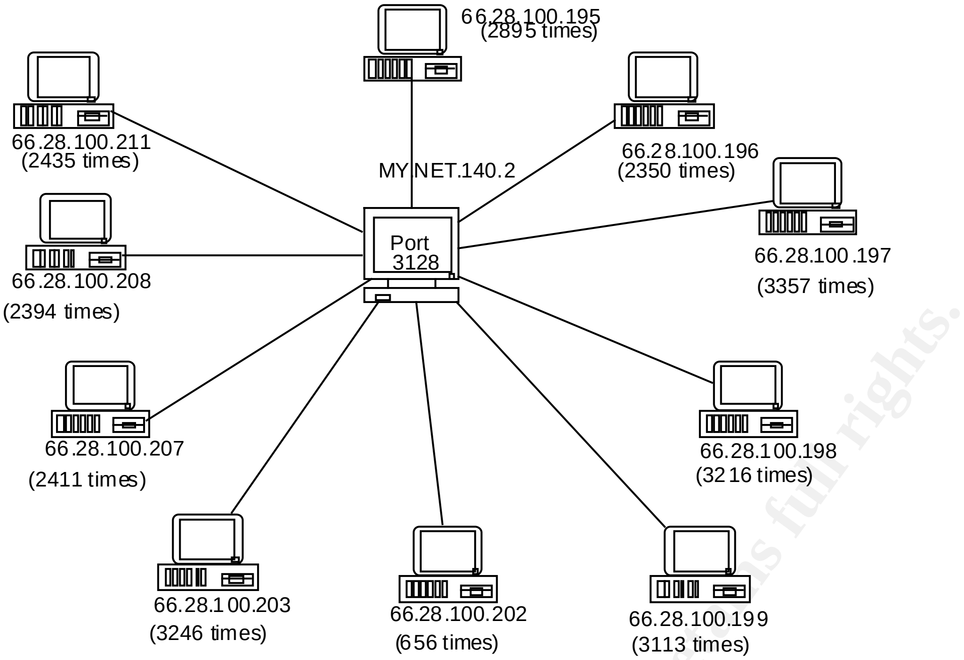
This IP is involved in 2 incidents of OOS packets. These packets are classified as the OOS packet because the reserved bits are set with Syn flag set. The destination port is 113, which is the Inetd service port and is discussed in detail on Top Alerts section.

**Recommendation:**

The same recommendation, which is specified on above section for the scan of 113. Also Internet Software Consortium should be notified about the activity from their IP.

## LINK GRAPH

Looking at the alert log files provided by the University, The interesting thing was the large Queso fingerprint attacks. This is interesting because nowadays Queso is rarely used due to the availability of more sophisticated fingerprinting tools like NMAP3.There were total of 27515 alerts generated for the Queso Fingerprint for a period and out of this 26219 alerts had MY.NET.140.2 as destination and the sources coming from 66.28.100.x network. This bunch of IP`s belong to Cogent communications. The destination port for this fingerprinting is 3128, which is associated with Trojans like Ringzero, and also it is used for squid http proxy. Since normally Ringzero Trojan scan consists of scan port 80 & 8080 along with 3128,this could be an attempt to find open proxy for anonymous proxy access. University has to have a look at the service or application listening on 3128 and if they are using squid proxy, they have to enforce necessary ACL to prevent it being used as open proxy.



## Defensive Recommendations

Each analysis of the Alert, Scan and OOS files was followed by defensive recommendation for that particular analysis. But in a nutshell the defensive recommendation for the University would be as follows:

1] University should have relook at the ACL` implemented by them at the Router and Rulesets at the Firewall level. They should make sure that these ACL`s and Rulesets should allow access only to the allowed services and IP`s in the internal network.

2] The logs suggests that file sharing applications like Kazaa, Gnutella etc are existing in the internal network. These applications have vulnerabilities associated with it and also they are primary cause for Bandwidth hogging. So the University should undertake an immediate auditing of the entire network to make sure that users are not making use any unauthorized applications which can put their entire network under compromise.

3] There seems to be unauthorized services running on the user workstations. University should make use of good port scanners to check upon ports upon critical machines and if any unwanted port is open corrective measures should be taken.

4] There seems to be numerous alerts pertaining to Trojan like activity and there were indications of worms like Nimda still active in the University network. The University should implement a good enterprise level Antivirus solution that can be centrally managed for updating the definitions for the entire network as well implementing a central policy of viruses. The solution chosen by the University should also be capable of scanning for viruses and worms and Trojans at the HTTP, SMTP gateways also. In case the University finds any of the machines compromised, they should be rebuilt the entire machine to prevent any backdoor from still existing on the machine.

5] University should protect all critical servers by host based IDS so as to prevent any attack on these servers like changing of system files.

6] University should make sure that they create a standard policy as to the patches applied, password protection, user rights etc for critical machines. They can make use of commercially available tools like Enterprise Security Manager from Symantec to automate this process.

## Brief Analysis Process

The procedure followed by me for my analysis process is as follows:

1] I created a single alert file from the five alert files downloaded from the incidents.org file. Since I was using windows 2000 platform and the size of the alert files were too large for the windows default text editor notepad.exe, I had to use the 32 bit text editor Ultredit (www.ultraedit.com) which could handle upto 2 GB of file size to club all the 5 files into one file. Then I made use of snortsnarf to get the easy to read html format. I used the command after renaming the MY.NET entries to 123.123 which was unused in the alert files (based on Lora Evens practical)

```
snortsnarf.pl -d C:\Inetpub\wwwroot\logs -dns -db C:\sno
rt\snortsnarf\ann-dir\annotation-base.xml -cgidir http://localhost\cgi C:\Inetpu
b\wwwroot\logs\alert
```

to create the html output.

2] once the html output was created, I started working with top ten alerts.

3] I again made a single file for scan and oos files.

4] I made use of ultraedit heavily to sort these files based on IP`s, based on ports, based on alerts etc. Ultraedit also had advanced sorting options where I could sort the textile based on columns and this helped to sort the text files in any way I wanted to.

5] To get the numerical counts for the Top Talkers for Scan and OOS files, I fed the single file created for each of these types to MS-ACCESS after creating the delimiter field by means of ultraedit. I then made use of the customizable query provided by MS-Access to get the output desired by me.

6] I used google extensively to search for references and correlations.

7]Dshield and www.whois.sc was used for getting information about IP and whois information.

8] http://www.neohapsis.com/neolabs/neo-ports/ was used by me to get information about different ports.

9] I made use of Lanflow (www.pacestar/lanflow) to create the link graph.