GCIA Practical Assignment

Version 3.2

By Philip LJUNGBERG

July 1, 2002

Table of Contents

1 Assignment # 1 : Describe the State of Intrusion Detection – The Market of Intrusion Detection Systems 5

1.1 Definition of intrusion detection systems 5
1.2 Classification of intrusion detection systems 5
1.2.1 Sources of input 5
1.2.1.1 Host-based Intrusion Detection Systems 6
1.2.1.2 Network-based Intrusion Detection Systems 6
1.2.1.3 Hybrid Intrusion Detection Systems 8
1.2.2 Architecture of intrusion detection systems 8
1.2.3 Granularity of data processing 9
1.2.4 Methods of analysis 9
1.2.4.1 Anomaly Detection Model 10
1.2.4.2 Misuse Detection Model 10
1.2.5 Generated output of Intrusion Detection Systems 11
1.2.5.1 Passive Intrusion Detection Systems 11
1.2.5.2 Reactive Intrusion Detection Systems 11
1.3 Conclusion 12
1.4 Appendix A 12
1.5 References 14

2 Assignment # 2 : Network Detects 15

2.1 Detection # 1 : WEB-MISC cisco /%% DOS attempt 15
2.1.1 Detection data 15
2.1.2 Source of the trace 17
2.1.3 Detect was generated by 17
2.1.4 Probability the source address was spoofed 17
2.1.5 Description of the attack 17
2.1.6 Attack mechanism 17
2.1.7 Correlations 18
2.1.8 Evidence of active targeting 18
2.1.9 Severity 18
2.1.10 Defensive recommendations 19
2.1.11 Multiple choice test question 19
2.1.12 Incidents.org Questions 19
2.1.13 References 20
2.2 Detection # 2 “FTP wu-ftp file completion attempt” 21
2.2.1 Detection data 21
2.2.2 Source of the trace 24
2.2.3 Detect was generated by 24
2.2.4 Probability the source address was spoofed 24
2.2.5 Description of the attack 24
2.2.6 Attack mechanism 24
2.2.7 Correlations 25
2.2.8 Evidence of active targeting 25
2.2.9 Severity 26
2.2.10 Defensive recommendations 26
2.2.11 Multiple choice test question 26
2.2.12 Incidents.org Questions 26
2.2.13 References 27
2.3 Detection # 3 : “SOCKS scan” 28
2.3.1 Detect data 28

2.3.2 Source of the trace 28
2.3.3 Detect was generated by 29
2.3.4 Probability the source address was spoofed 29
2.3.5 Description of the attack 29
2.3.6 Attack mechanism 29
2.3.7 Correlations 29
2.3.8 Evidence of active targeting 30
2.3.9 Severity 30
2.3.10 Defensive recommendations 30
2.3.11 Multiple choice test question 31
2.3.12 Incidents.org questions 31
2.3.13 References 31

3 Assignment # 3: Analyze This 32

3.1 Executive Summary 32
3.2 List of Files 32
3.3 Network infrastructure 32
3.4 List of detects 33
3.5 Description of detects 36
3.5.1 Suspicious traffic 36
3.5.1.1 Suspicious host traffic 36
3.5.1.2 Watchlist 000220 IL-ISDNNET-990517 and 000222 NET-NCFC 36
3.5.1.3 MISC source port 53 to <1024 37
3.5.1.4 UDP SRC and DST outside network 37
3.5.1.5 Connect to 515 from outside 38
3.5.1.6 X11 Outgoing 38
3.5.1.7 Beetle.ucs 38
3.5.1.8 AFS – Off-campus activity 38
3.5.1.9 Tiny Fragments – Possible Hostile Activity 38
3.5.2 CS WEBSERVER – external web/ftp traffic 39
3.6 Information gathering attempts 39
3.6.1 SMB Name Wildcard 39
3.6.2 Netbios NT Null Session 39
3.6.3 SNMP Public Access 39
3.6.4 Incomplete packet fragments discarded 39
3.6.5 Scans 40
3.6.5.1 Queso fingerprint 40
3.6.5.2 NMAP TCP ping! 40
3.6.5.3 SCAN Proxy attempt 40
3.6.5.4 Null Scan! and Xmas Scan 40
3.6.5.5 INFO – Possible Squid Scan 40
3.6.5.6 Synscan Portscanning ID 19104 40
3.6.5.7 Scan Fin 41
3.6.6 ICMP messages 41
3.6.6.1 ICMP Echo Requests 41
3.6.6.2 ICMP Destination Unreachable 42
3.6.6.3 ICMP Router Selection 43
3.6.6.4 ICMP Source Quench 43
3.6.6.5 MISC and ICMP traceroute 44
3.6.6.6 ICMP Redirect 44
3.6.6.7 ICMP Fragment Reassembly Time Exceeded 44
3.6.6.8 ICMP Address Mask request 44
3.7 P2P and chatters 44
3.7.1 INFO Inbound GNUTella Connect request / accept and INFO Outbound GNUTella Connect request / Accept 44
3.7.2 INFO Napster Client Data 45

3.7.3 INFO MSN IM Chat Data 45
3.7.4 INFO Possible IRC Access 45
3.7.5 IRC evil – running XDCC 45
3.8 Viruses, worms and trojans 45
3.8.1 High port 65535 udp/tcp – possible Red Worm - traffic 45
3.8.2 NIMDA – Attempt to execute cmd from campus host 45
3.8.3 Virus - Possible pif Worm / Possible scr Worm 46
3.8.4 Possible Trojan server activity 46
3.8.5 Back Orifice 46
3.8.6 BACKDOOR Netmetro Incoming traffic 46
3.9 WEB alerts 46
3.9.1 Spp_http_decode:IIS Unicode attack detected 46
3.9.2 Spp_http_decode: CGI Null Byte attack detected 47
3.9.3 IDS552/web-iis_IIS ISAPI Overflow ida nosize 47
3.9.4 WEB-CGI alerts 47
3.9.5 WEB-FRONTPAGE alerts 48
3.9.6 WEB-IIS alerts 48
3.9.7 WEB-MISC alerts 49
3.10 FTP alerts 49
3.10.1 INFO FTP anonymous FTP 49
3.10.2 FTP DoS ftpd globbing 50
3.10.3 TFTP 50
3.11 Other System Integrity Attempts 50
3.11.1 MS-SQL xp_cmdshell – program execution 50
3.11.2 SMB C Access 50
3.11.3 MISC PCAnywhere Startup 50
3.11.4 SMTP chameleon overflow 50
3.11.5 EXPLOITS 51
3.11.6 MISC Large ICMP / UDP Packet 51
3.11.7 Port 55850 tcp/udp – Possible myserver activity – ref. 010313-1 51
3.11.8 SUNRPC highport access! 52
3.11.9 RPC tcp traffic contains bin_sh 52
3.12 Analysis identifying relationships 52
3.13 "Top talkers" List 52
3.13.1 Top 10 alerts 52
3.13.2 Top 10 Portscans 54
3.14 List of external addresses and registration information 55
3.14.1 Reasons for selection 55
3.14.2 Registration information 55
3.15 Link graph and analysis 60
3.16 Insights into internal machines 64
3.17 Defensive recommendations 66
3.18 Description of the analysis process 66
3.19 References and correlations with other students' practicals 67

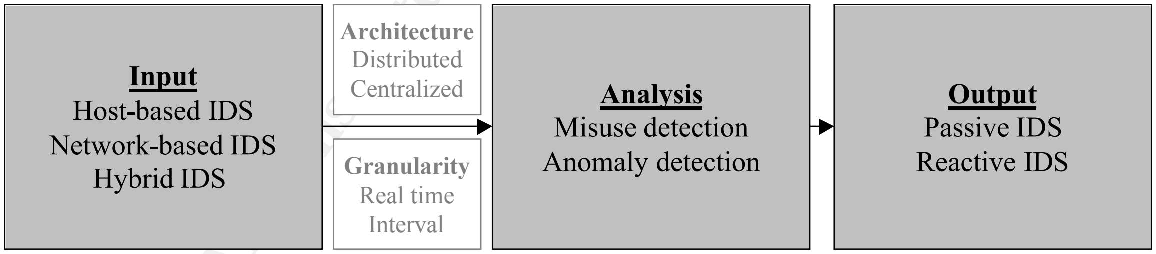
1 Assignment # 1: Describe the State of Intrusion Detection – The Market of Intrusion Detection Systems

Intrusion detection systems (IDSs) are becoming a necessary complement of every organization's security infrastructure. The question is therefore not whether to implement an intrusion detection system but which type of IDS is going to be implemented. In this paper we will explain the concept of intrusion detection and describe the different kinds of IDSs currently available on the market. At the end we will position the vendors included in Gartner's magic quadrant in a table based on criteria which will be explained throughout the paper.

1.1 Definition of intrusion detection systems

An intrusion detection system is software or a combination of both software and hardware that automates the process of monitoring a system or a network and analyzes the resulting data for signs of intrusions. IDSs can be distributed into three components : input, analysis and output (see Figure 1). The input is generated by sensors, which can be distributed over the network of the organization or centralized on a single host. The sensors collect the information from the networking equipment and applications and forward it to the analysis engines. The analyzer is responsible for determining if an intrusion has occurred – which is done by examining all the events added to the database by the sensors – and results in an assessment of the state of security. The output of the analyzer can provide some guidance about what actions have to be taken by the security administrators as a result of the intrusions or may include evidence supporting the conclusion that an intrusion has occurred. [1]

Figure 1 : The Classification of Intrusion Detection Systems



Source : Own production.

1.2 Classification of intrusion detection systems

The classification of intrusion detection systems is rather a hard topic, because many of the IDSs are based on more than one approach. In this paper, the classification is based on the distribution of the IDSs into three components – input, analysis and output – which have already been pointed out in Figure 1.

1.2.1 Sources of input

The first and most common way to classify the techniques of intrusion detection is to group them by their sources of input. Based on the used type of input, three types of

IDSs can be differentiated : a host-based IDS, a network-based IDS and a hybrid IDS.

1.2.1.1 Host-based Intrusion Detection Systems

The first intrusion detection systems, developed in 1988, were host-based IDSs. They monitored the activity on a single host through a piece of software that was installed on the system. Application-based IDSs are a special subset of host-based intrusion detection systems and are designed to protect specific applications (such as webservers, databases, etc.) [2]

Host-based IDSs can determine exactly which users and processes are subject to the intrusion because decisions are based on information that is generated by the operating system audit trails and the system logs of the monitored host itself. This makes host-based IDSs more effective than network-based IDSs, if the rules are properly tuned.

Since the sensors and parts of the analysis engines of the host-based IDSs are installed on the host itself they are the first target for potential intruders who can delay and/or change the generated logs or even disable the entire IDS by denial of service attacks, which makes it less reliable than network-based IDS. [1] Another disadvantage of host-based IDSs is the fact that by residing on the monitored server itself they consume some of its processing power, disk storage and memory. If the IDS appears to get in the way of production software, very often the IDS sensor will be disabled because of its use of vital computing resources. [3]

Most of the host-based IDSs are designed to work as a standalone product, which makes them harder to manage than network-based IDSs. Nevertheless, a few of them can be monitored via a centralized IDS management infrastructure, while others generate messages in a data format that can be interpreted by a network management system. [1]

Examples of Host-based IDS are Dragon Squire (Enterasys Networks), Intruder Alert (Symantec), Entercept (Entercept), Kane Security Analyst (Intrusion.com), NetIQ Security Manager (NetIQ) and Tripwire (Tripwire).

1.2.1.2 Network-based Intrusion Detection Systems

Nowadays, because of the explosive growth of networking, the majority of commercial IDSs are network-based IDSs. These network-based IDSs, developed at the beginning of the 90s, use network packets read directly off the network and gathered by sensors as an information source for their analysis. [4].

The implementation of network-based IDSs has little or no impact on the organization’s servers because they are standalone, passive devices. Above all this, they can run in some sort of ‘stealth’ mode by encrypting the communication between the sensors and the analysis engine. A stealthed IDS is very hard to disable, but it can still be located by the attackers because the IP headers are not encrypted (thus the IP addresses are readable) and the ports are not HTTPS or SSH (e.g. Realsecure uses port 9002).

It is not very easy to implement a network-based IDS in a switched environment, because all the traffic from a specific segment goes through one port of the switch. This way it is impossible to monitor this segment because all of its traffic is being separated from the other segments. This problem can be solved through the use of 'port mirroring'. "Port mirroring is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied." [5] Since port mirroring consumes a lot of CPU resources, some vendors have proposed alternative solutions like taps and IDSs embedded on the switch. Cisco is for example a vendor that offers IDSs directly embedded on the backplane of the switch via a specially developed card. [6] Taps are network monitoring boxes that can be connected directly between the router and the switch, between two switches or between the switch and a host. This way it is very easy to plug into the network – without any fear of being noticed by the target being monitored – because the traffic on every port of the tap is being mirrored to another dedicated port. More information about taps can be found at www.shomiti.com. [7] However, both solutions will start dropping packets when they are confronted with a huge amount of traffic.

Intrusion detection systems must be able to keep up with the information generated by a lot of hosts. In periods of high traffic the IDS may have difficulties handling so much data, which can result in dropping packets. This is why the amount of packets that can be handled by an IDS is more important than the amount of bits per second. Most vendors promote their IDS being able to easily handle the amount of packets sent over a 100 Mbps connection. In reality, these vendors are referring to packets of 1.500 byte, but the average website generates about 50.000 packets of 180 bytes per packet per second on a 100 Mbps connection. Practice shows that IDSs start dropping packets when they are confronted with 60-byte packets. In addition, they have to maintain a connection state table for an enormous amount of TCP connections, which requires an extensive amount of memory. Not all IDSs are stateful though and most of them that are can be configured to not keep state (such as Snort). The latter is not recommended because essential information will be lost. Even if the connection with the client or the server has been closed, statefull IDSs have to save connection information, because intruders can hijack these 'closed' sessions. Since the process of monitoring and analyzing events asks so much processing power, vendors are looking to detect attacks with less computing power or just to detect fewer attacks, which will reduce the effectiveness of the IDS. Another major disadvantage of network-based IDSs is that they cannot tell if a detected intrusion has indeed been successful. Security administrators have to check each host individually to verify if they have been corrupted by intruders or not. Some IDS analysts also run a sniffer alongside the NIDS sensor. This way, if a serious attack is detected, the sniffer logs can be queried and the analyst can determine if the attack was successful. This is almost not feasable on high bandwidth networks, but it is quite effective on small to medium sized ones. Above all this, network-based IDSs have also difficulties with the handling of fragmented packets and the analysis of encrypted information. Especially the latter disadvantage makes a NIDS in today's organizations of a lesser value, because more and more traffic is encrypted. [1] However, if the traffic is SSL, a load balancer with an SSL accelerator card (e.g. F5 Big-IP) can decrypt the traffic for analysis by the IDS. [10]

Examples of network-based IDSs are Cisco Secure IDS (Cisco), BlackICE Sentry and BlackICE Gard (both ISS), Dragon Sensor (Enterasys Networks), Net Prowler (Symantec), SecurenetPro (Intrusion.com), NFR NID (NFR Security), SilentRunner (Raytheon), NetDetector (Niksun), ManTrap (Recourse Technologies) and Snort.

1.2.1.3 Hybrid Intrusion Detection Systems

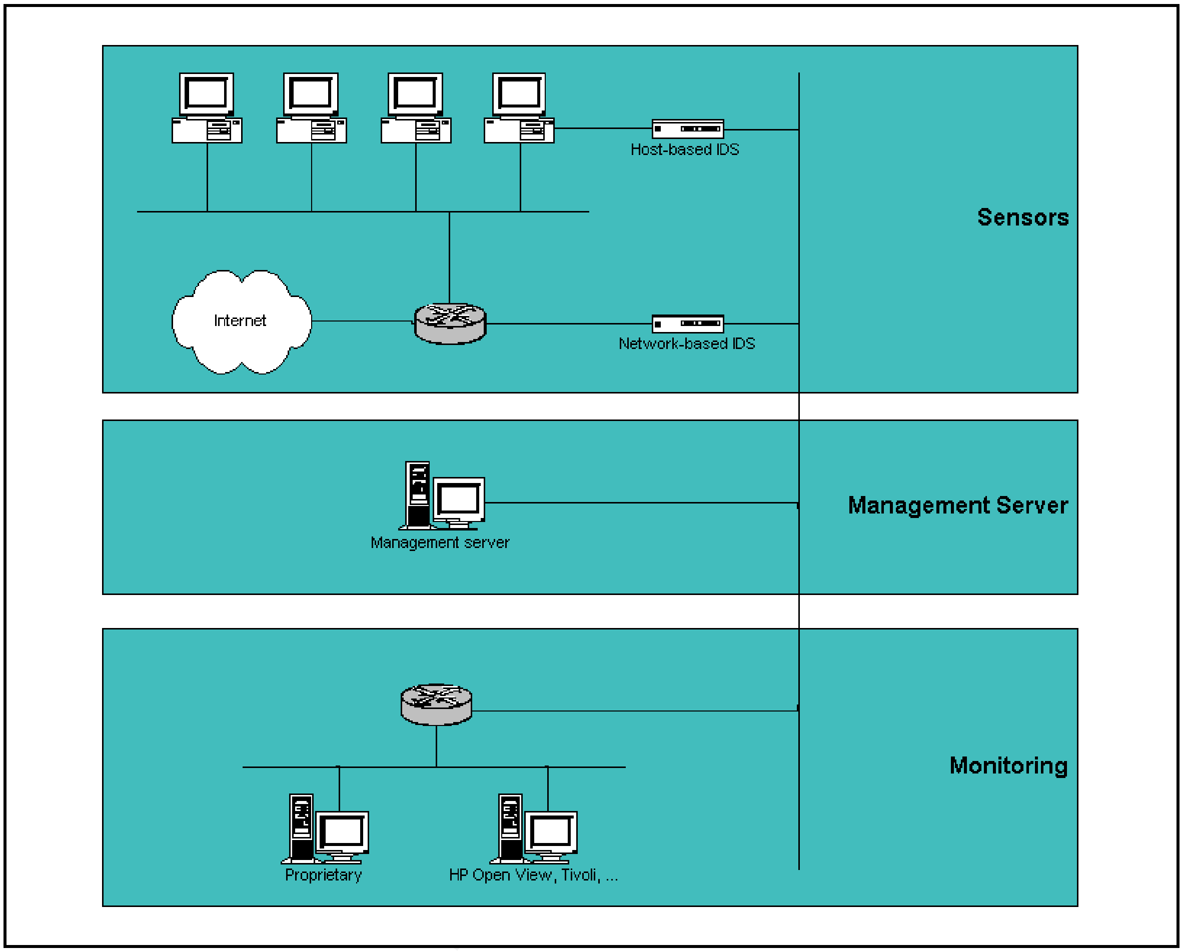
Both host-based and network-based IDSs have their pros and cons and a truly effective IDS will use a combination of both, known as a hybrid IDS. Gartner suggests to use network-based intrusion detection at the boundaries of the network and host-based IDS only on servers of high value to the organization. [8]

Recently, a few vendors have developed a new type of hybrid IDS solution, called network node IDS. "Network node IDSs delegate the new IDS function down to individual hosts, alleviating the problems of both high speeds and switching." This means that a network node IDS sensor is installed on every server that has to be protected. This sensor will only listen to the network packets that are sent to the host it resides on (it acts as a firewall) and is therefore much faster than network-based IDSs. [2]

1.2.2 Architecture of intrusion detection systems

The most important architectural components of IDSs are the host (this is the system where the IDS is running on) and the target (this is the system that the IDS monitors). In the 80's most of the IDSs where running on the same machines as they were monitoring, since the high cost of hardware made it too expensive to install the IDS on a separate system. This was a severe security problem because any intruder attacking the target system was also attacking the IDS and could simply disable it. This is why there was an evolution to the separation of the host and the target as hardware got cheaper, eventually resulting in the development of appliances (i.e. a specially developed combination of hardware and software for the execution of a specific task). In a separated environment the IDS is a lot harder to find, especially when encryption is used for the communication between the sensors and the analysis engine. [1] Most of the current vendors provide an IDS solution with a three-tiered architecture, consisting of the sensors, a management server and a system to monitor the IDS (see Figure 2). However, it is possible that the management and the monitoring systems are the same.

Figure 2 : Three-tiered IDS architecture



Source : Own production.

1.2.3 Granularity of data processing

The elapsed time between the capture of the events by the sensors and the analysis of these events varies among different IDSs. Sensors can send the events in real-time or with an interval to the analysis engines. In the early systems mostly interval-based solutions where used. However, because of the need for a fast response of the IDS and the growing success of network-based IDSs the majority of the current IDSs use a continuous flow between the sensors and the analyzers. [1]

1.2.4 Methods of analysis

The classification of IDSs by methods of analysis can be divided into anomaly detection and misuse detection. Anomaly detection systems detect intrusions by looking for activities that are different from the normal behavior of the users or systems. This method is still part of a great deal of research and is mostly used in non-commercial projects. Misuse detection systems look for activities that correspond to known intrusion techniques or system vulnerabilities and are mostly used in commercial IDSs. Both anomaly detection and misuse detection have their pros and cons and the most effective IDSs use a combination of both. [1]

1.2.4.1 Anomaly Detection Model

Anomaly detection systems react on abnormal behavior from a user or a system. Every behavior that does not fit into the profile of these users or systems is identified as an intrusion. The profiles, created for this purpose, are constructed from historical data collected over a period of time where the system has operated in normal conditions.

Anomaly detection systems still generate a lot of false positives (i.e. false alarms), due to the unpredictable behaviour of the users and the systems. A large number of these false positives can lead to the fact that real intrusions go unnoticed by the security administrators of the organization. Decreasing the number of these false positives can be done through extensive training of the anomaly detection system, but this has to be done in situations of normal behavior.

The fact that anomaly detection systems can detect unusual behavior and thus have the ability to detect an intrusion without the existence of a known signature of the attack is one of the most important advantages of these systems. These new attacks can then be used as input for misuse detection systems and can be added to its signature database. The anomaly detection system can for example generate a figure representing the normal use of CPU load by a user. The misuse detection system can then use this figure as part of a signature to trigger an alarm if the user exceeds this figure.

Anomaly detection is still subject of a lot of research and this is why it is not used in commercial intrusion detection systems yet. There are a few IDSs though where anomaly detection is used in a limited form, in conjunction with misuse detection systems. [1]

1.2.4.2 Misuse Detection Model

Misuse detection systems analyze potential intrusions based on signatures. These signatures are “events or sets of events that match a predefined pattern of events which describe a known attack”. Most of the misuse detection systems used in commercial products compare a single intrusion attempt with a unique signature. The more sophisticated systems, called state-based systems, can relate different intrusion attempts as a single intrusion based on leveraging a single signature.

Misuse detection systems do not generate a lot of false positives what makes them a lot more effective than anomaly detection systems. They generate quick and reliable diagnoses of attacks, which can be used by the security administrators to prioritize countermeasures against specific, dangerous intrusions.

One of the most important disadvantages of misuse detection systems is the fact that they can only detect the intrusions they know about. This is the reason why the database of known signatures has to be constantly updated with new signatures. This updating process makes a large difference between different commercial products. Variants of known attacks also go undetected by misuse detection systems if the signatures are too tightly defined. State-based systems are not affected by this problem but they are not commonly used in commercial intrusion detection systems. [1]

1.2.5 Generated output of Intrusion Detection Systems

Intrusion detection systems generate a response after capturing and analyzing the events. Some IDSs just generate a report while others take action and for example redefine the rules in the firewalls. Therefore, a distinction can be made between passive and reactive IDSs. In a few occasions a combination of both systems is being used.

1.2.5.1 Passive Intrusion Detection Systems

Passive intrusion detection systems imply that the systems generate reports and send them to the security administrators. It is then up to them to take the appropriate actions.

Most commercial passive intrusion detection systems generate alarms and offer the possibility to determine who receives the alarms and when and how they are generated. A popup window or an onscreen alert is the most common form of alarm that is used by these IDSs. The details of the generated output vary widely from very detailed to a simple message that an intrusion has occurred. Some IDSs offer even the possibility to send an alarm to a pager or a mobile phone carried by the security administrators. Systems that send an e-mail as an alert cannot be trusted though because these mails can get forged or blocked by the intruders. Some passive intrusion detection systems can send an alarm or alert to network management systems. These systems send SNMP traps to central management consoles where they are displayed to the security administrators. The output generated by most of the passive IDSs can be transformed in a standard format to integrate them in a database system. This way statistics over a particular period can be generated.

An important feature of intrusion detection systems is the way in which alerts are generated. If they react to an intrusion by broadcasting alarms and alerts in plain text over the network the intruder(s) will probably detect the IDS. In the worst scenario the attackers will even attack the IDS itself. This makes the encryption of the communication of IDSs a necessity to ensure their reliability. [1]

1.2.5.2 Reactive Intrusion Detection Systems

Reactive IDSs detect, log and alert but also respond to intrusions. An intrusion detection system can react in three different ways [7]:

- Collection of additional information: The collection of additional information is done by turning on more logs and thus more information sources. This additional information can then be used to support further investigation to arrest the intruders.

- Changing the environment: The IDS can block the IP-addresses from which the intruders are coming. Reconfiguration of the routers and firewalls by the reactive IDSs are also an option.
- Taking actions against the intruder(s): The intrusion detection systems could send the intruder a warning e-mail or they could even launch a denial-of-service attack against him. These actions don't raise a problem if the intrusion detection thresholds are very finely tuned to minimize the occurrence of a false positive. Questions are raised though about the legal aspects of these IDSs and legal advice should be obtained before pursuing any 'strike-back' option.

1.3 Conclusion

The classification of intrusion detection systems is a difficult task, because many IDSs are based on a different approach. In this paper a distinction has been made between three components resulting in following classification:

- Input: host-based, network-based and hybrid IDSs,
- Analysis: anomaly detection and misuse detection,
- Output: passive and reactive IDSs.

Nowadays, most of the sensors send the data in real-time to the analysis engines, but in the early days of intrusion detection a distinction could be made between sensors that transmitted the data in real-time or with an interval to the analyzers. Some IDSs have both the input and analysis components installed on one host and work as a standalone system while others employ a three-tiered architecture with separate sensors, management servers and a monitoring system.

The best intrusion detection system is a hybrid IDS (with sensors on the boundaries of the network and on the most important servers), that employs a combination of both anomaly and misuse detection, that provides the security administrators with real-time information about the intrusions while blocking them and that can be monitored via the enterprise's central management system.

1.4 Appendix A

As a way of testing the model in Figure 1 I have included an overview of all the IDS vendors mentioned in Gartner's magic quadrant. This table will give you a first impression about the most important IDS vendors and which products they offer. As I tried to fill in the entire table, lots of questions could not be answered because of lack of the right information on the vendor's websites (especially the methods of response of the IDSs is rarely mentioned).

I solely searched on the vendor's website to get the information for the table. This information can be outdated at the time of reading this paper. Gartner's magic quadrant is online available at http://www.allasso.pt/base/docs/11022985137.pdf.

	Vendor	Product	Sensors						Granularity		Management	Analysis		Passive Response				Active Response		
			Host-based IDS	Application-based IDS	Network-based IDS	Hybrid	Network node IDS	Appliances	Real-time	Interval	Mgmt. of the sensors	Misuse Detection	Anomaly Detection	Passive	SMTP	Paging	SNMP	(Re)active	OPSEC	Cisco Routers
Leaders	Cisco www.cisco.com	Cisco Secure IDS	[1]		C			4210 : 45 Mbps 4230 : 100 Mbps 4250 : 500 Mbps	X	-	Cisco Secure IDS Director Cisco Secure Policy Manager	X	-	X			HP	X	Via PentaSafe	X
	ISS www.iss.net	RealSecure				C		RealSecure for Nokia	X	-	Workgroup Manager	X	-	X	X	X	X	X	X	?
		RealSecure Server Sensor					C													?
		BlackICE Agent					C	None			ICEcap Manager	X	-	X	X	X	X	X	-	?
		BlackICE Sentry (Gigabit)			C															?
		BlackICE Guard			C															?
	Enterasys Networks www.enterasys.com	Dragon Squire	C						X	-	Dragon Server	X	-	?	?	?	?	X	X	X
		Dragon Sensor			C			Dragon Sensor												
Challengers	Symantec www.symantec.com	Intruder Alert	C					None	X	-	Manager	?	?	X	?	?	Tivoli BMC Patrol HP Open View	?	-	?
		Net Prowler			C															
Visionaries	Entercept www.entercept.com	Entercept	C		[2]			None	X	-	Console	X	X	X	X	X	X	X	X	-
		Entercept Web Server		C																
	Intrusion.com www.intrusion.com	Kane Security Analyst	C					None	X	-	Kane Secure Enterprise	X	-	?	?	?	?	?	-	X
		SecurenetPro			C			SecureNet PDS 2000 SecureNet PDS 5000 SecureNet Gig			SecureNet 8001 SecureNet Provider	X	-	?	?	?	?	X	X	?
	NFR Security www.nfr.com	NFR NID			C			NFR NID-200	X	-	NFR Central Management Server Anzen Flight Jacket	X	X	X	X	?	?	X	X	?
Niche Players	NetIQ www.netiq.com	NetIQ Security Manager	C					None	X	-	Security Manager	?	?	?	?	?	?	?	-	?
	Tripwire www.tripwire.com	Tripwire	C/F					None	X	-	Tripwire Manager	File Integrity Checker		-	-	-	X	X	X	?
	Raytheon www.raytheon.com	SilentRunner			C			None	X	-	Manager	?	?	?	?	?	?	-	-	?
	Niksun www.niksun.com	NetDetector			C			NetDetector 2400 NetDetector 5400/5600	X	-	Manager	-	X	X	?	?	?	X	-	X
	Recourse Technologies www.recourse.com	ManTrap			C			ManHunt nodes	X	-	ManHunt Manager	X	X	X	X	?	?	X	X	X
Freeware	Snort www.snort.org	Snort			F			None	X	-	IDS Policy Manager	X	X	X	X	-	X	X	-	-

- = Not available, ? = No information available, X = available, C = Commercial, F = Freeware

[1] Cisco IDS host sensor is provided in partnership with Entercept Software and PentaSafe Vigilent Security Agent.

[2] Via Cisco's Secure IDS

1.5 References

1. R. Bace, P. Mell, 26 July 2002, NIST Special Publication on Intrusion Detection Systems, On-line available at http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf.

2. A. Cliff, 19 July 2001, IDS Terminology, Part Two : H-Z, On-line available at http://online.securityfocus.com/infocus/1214.

3. G. Arcuri, 23 January 2001, Intrusion Detection (IDS): Perspective, Gartner.

4. P. Astithas, 1999, Intrusion Detection Systems, On-line available at http://www.daemonnews.org/199905/ids.html.

5. Whatis.com, 6 January 2001, Port mirroring, On-line available at http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci511650,00.html.

6. R. Graham, 21 March 2000, FAQ: Network Intrusion Detection Systems, On-line available at http://www.robertgraham.com/pubs/network-intrusion-detection.html.

7. K. van Wyk and R. Forno, August 2001, Incident Response : Chapter 7 : Tools of Trade, On-line available at http://www.oreilly.com/catalog/incidentres/chapter/ch07.html.

8. R. Stiennon, 19 October 2001, Intrusion Detection Market Magic Quadrant 2H01, On-line available at http://www.allasso.pt/base/docs/11022985137.pdf.

9. Network Security Resource, 26 July 2002, Topics > Intrusion Detection Systems, On-line available at http://www.gslis.utexas.edu/~netsec/ids.html#reac.

10. F5, 28 August 2002, SSL Accelerator 400/800, On-line available at http://secure.f5.com/f5products/bigip/sslaccelerator/index.html.

2 Assignment # 2: Network Detects

2.1 Detection # 1: WEB-MISC cisco /%% DOS attempt

2.1.1 Detection data

The alerts that were triggered by the Snort rule are:

```
06/07-21:14:44.524488  [**] [1:1546:4] WEB-MISC cisco /%% DOS attempt [**] [Classification: Web Application Attack]
[Priority: 1] {TCP} 46.5.180.250:64347 -> 132.235.74.123:80

07/09-16:15:03.504488  [**] [1:1546:4] WEB-MISC cisco /%% DOS attempt [**] [Classification: Web Application Attack]
[Priority: 1] {TCP} 46.5.180.250:61955 -> 66.54.32.235:80

07/09-16:15:03.574488  [**] [1:1546:4] WEB-MISC cisco /%% DOS attempt [**] [Classification: Web Application Attack]
[Priority: 1] {TCP} 46.5.180.250:61955 -> 66.54.32.235:80
```

The Snort rule that triggered these specific alerts is:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC cisco /%% DOS attempt";
flow:to_server,established; uricontent:"/%%"; classtype:web-application-attack; sid:1546; rev:4;)
```

The Snort output in packet logger mode was as follows:

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

06/07-21:14:44.524488 46.5.180.250:64347 -> 132.235.74.123:80
TCP TTL:124 TOS:0x0 ID:7980 IpLen:20 DgmLen:77 DF
***AP*** Seq: 0xA0E5C06E  Ack: 0xB0E4428  Win: 0x4356  TcpLen: 20
9E 2F 25 25 65 AF 42 EE FF 67 DD 31 F5 3A 3E 00  ./%%e.B..g.1.:>.
01 05 02 0E 00 00 00 CA 18 C0 A8 7B 96 28 03 00  ...........{.(..
00 27 3C 00 00                                   .'<..

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

06/07-21:14:44.924488 46.5.180.250:64347 -> 132.235.74.123:80
TCP TTL:124 TOS:0x0 ID:7993 IpLen:20 DgmLen:90 DF
***AP*** Seq: 0xA0E5C7E8  Ack: 0xB0E55D0  Win: 0x4117  TcpLen: 20
3E 97 CE C0 F0 8A EB AC 73 CA B0 D1 2C 9E 54 25  >.......s...,.T%
80 01 06 1B 00 00 00 00 00 61 74 74 61 63 6B 20  .........attack
6F 66 20 74 68 65 20 63 6C 6F 6E 65 73 20 61 76  of the clones av
69 00                                            i.

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

…

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

07/09-16:15:03.504488 46.5.180.250:61955 -> 66.54.32.235:80
TCP TTL:124 TOS:0x0 ID:43075 IpLen:20 DgmLen:608 DF
***AP*** Seq: 0xAA2649  Ack: 0x967AF474  Win: 0x2058  TcpLen: 20
47 45 54 20 2F 52 65 61 6C 4D 65 64 69 61 2F 61  GET /RealMedia/a
64 73 2F 63 6C 69 63 6B 5F 6C 78 2E 63 67 69 2F  ds/click_lx.cgi/
77 77 77 2E 75 73 61 74 6F 64 61 79 2E 63 6F 6D  www.usatoday.com
2F 64 6F 75 62 6C 65 74 72 65 65 2F 6C 6F 61 64  /doubletree/load
73 2E 68 74 6D 2F 25 25 52 41 4E 44 25 25 2F 53  s.htm/%%RAND%%/S
70 65 63 69 61 6C 31 2F 32 30 31 36 34 5F 44 6F  pecial1/20164_Do
75 62 6C 65 74 72 65 65 5F 53 77 65 65 5F 32 33  ubletree_Swee_23
36 36 2F 63 6C 65 61 72 2E 67 69 66 2F 25 00 25  66/clear.gif/%.%
20 45 52 25 25 20 48 54 54 50 2F 31 2E 31 0D 0A   ER%% HTTP/1.1..
41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 41 63 63  Accept: */*..Acc
65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20 65 6E  ept-Language: en
2D 75 73 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F  -us..Accept-Enco
64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65 66 6C  ding: gzip, defl
61 74 65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A  ate..User-Agent:
20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F   Mozilla/4.0 (co
6D 70 61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35  mpatible; MSIE 5
2E 35 3B 20 57 69 6E 64 6F 77 73 20 4E 54 20 34  .5; Windows NT 4
2E 30 29 0D 0A 48 6F 73 74 3A 20 61 64 2E 75 73  .0)..Host: ad.us
61 74 6F 64 61 79 2E 63 6F 6D 0D 0A 43 6F 6E 6E  atoday.com..Conn
65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69  ection: Keep-Ali
76 65 0D 0A 43 6F 6F 6B 69 65 3A 20 52 4D 49 44  ve..Cookie: RMID
3D 61 61 38 31 33 32 37 38 33 61 66 37 30 66 63  =aa8132783af70fc
30 3B 20 55 53 41 54 55 49 44 3D 61 61 38 31 33  0; USATUID=aa813
32 37 38 33 62 62 39 64 64 37 38 3B 20 70 65 72  2783bb9dd78; per
73 6F 6E 61 6C 3D 25 33 46 7A 69 70 25 33 44 31  sonal=%3Fzip%3D1
31 37 32 39 25 32 36 77 6D 6F 25 33 44 37 32 35  1729%26wmo%3D725
30 33 35 25 32 36 77 63 69 74 79 25 33 44 49 73  035%26wcity%3DIs
6C 69 70 25 32 36 77 73 74 61 74 65 25 33 44 4E  lip%26wstate%3DN
59 25 32 36 7A 63 69 74 79 25 33 44 44 65 65 72  Y%26zcity%3DDeer
25 32 35 32 30 50 61 72 6B 25 32 36 7A 73 74 61  %2520Park%26zsta
74 65 25 33 44 4E 59 3B 20 41 46 46 49 4C 49 41  te%3DNY; AFFILIA
54 45 5F 43 4F 44 45 3D 75 73 61 3B 20 56 45 52  TE_CODE=usa; VER
54 49 43 41 4C 5F 43 4F 44 45 3D 6E 61 74 69 6F  TICAL_CODE=natio
6E 61 6C 3B 20 55 53 41 54 49 4E 46 4F 3D 55 49  nal; USATINFO=UI
44 25 33 44 61 61 38 31 33 32 37 38 33 61 66 37  D%3Daa8132783af7
30 66 63 30 0D 0A 0D 0A                          0fc0....
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
07/09-16:15:03.574488 46.5.180.250:61955 -> 66.54.32.235:80
TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:607
***AP*** Seq: 0x967AF575  Ack: 0xAA2882  Win: 0x25BC  TcpLen: 20
47 45 54 20 2F 52 65 61 6C 4D 65 64 69 61 2F 61  GET /RealMedia/a
64 73 2F 63 6C 69 63 6B 5F 6C 78 2E 63 67 69 2F  ds/click_lx.cgi/
77 77 77 2E 75 73 61 74 6F 64 61 79 2E 63 6F 6D  www.usatoday.com
2F 64 6F 75 62 6C 65 74 72 65 65 2F 6C 6F 61 64  /doubletree/load
73 2E 68 74 6D 2F 25 25 52 41 4E 44 25 25 2F 53  s.htm/%%RAND%%/S
70 65 63 69 61 6C 31 2F 32 30 31 36 34 5F 44 6F  pecial1/20164_Do
```

2.1.2 Source of the trace

This trace is taken from a post at http://www.incidents.org/logs/Raw/. There was no information available about the network infrastructure.

2.1.3 Detect was generated by

The raw tcpdump log files provided at http://www.incidents.org/logs/Raw/ were generated by the Snort Intrusion Detection System (http://www.snort.org).

2.1.4 Probability the source address was spoofed

The probability that the source was spoofed is very low. All the detected packets are TCP packets which require a three-way handshake for the connection to become established. Spoofing is still possible though, but it would have to be a complicated man in the middle attack.

2.1.5 Description of the attack

The "WEB-MISC cisco /%% DOS attempt" alert is triggered for a potential denial of service attack against Cisco routers. This vulnerability appears in multiple releases of Cisco's IOS software. A hacker can run a buffer overflow against Cisco routers with the web configuration enabled. When the attack is successful the router will reboot and stay unavailable, resulting in a DoS.

2.1.6 Attack mechanism

This DoS attack is only possible under the condition that the IOS HTTP server is enabled on the Cisco router or switch. This server is enabled on all Cisco 1003, 1004 and 1005 routers by default. On all the other Cisco routers the HTTP server must explicitly be enabled. As of IOS release 11.1 and 11.2 the HTTP server got vulnerable for this attack. Starting from these versions of the IOS software, a function was added that parses special characters in a URI (Uniform Resource Identifier) of the format "%nn" where each "n" represents a hexadecimal character. This attack is very easy to execute when previous condition is met. The hacker just has to browse to http://<router-ip>/%% and the router or switch will halt and reboot because it has incorrectly parsed the "%%" and enters in an infinite loop. In some exceptional cases the router fails to reload and stays halted.

There is something unusual though about this alert. If we take a look at all the other alerts which were triggered for 46.5.180.250 we see that these are all WEB alerts (Table 1). This has to be an internal machine (maybe an http-proxy) generating lots of (false) alerts.

When we look at the Snort output in packet logger mode we see:

- For the first alert that someone is looking for an avi file named 'attack of the clones' on 132.235.74.123.
- For the second and the third alert that someone is browsing to http://www.usatoday.com/doubletree/loads.htm/%%RAND%%/Special1/20164_ Doubletree_Swee_2366/clear.gif.

These alerts are definitely examples of a false positive (i.e. an alert caused by a non-malicious event).

Table 1 : Other alerts triggered by 46.5.180.250

SRC IP	Alerts	Number of alerts
46.5.180.250	[1:895:5] WEB-CGI redirect access	145
46.5.180.250	[1:1113:4] WEB-MISC http directory traversal	101
46.5.180.250	[1:873:5] WEB-CGI scriptalias access	27
46.5.180.250	[1:1425:6] WEB-PHP content-disposition	11
46.5.180.250	[1:1333:4] WEB-ATTACKS id command attempt	11
46.5.180.250	[1:1497:6] WEB-MISC cross site scripting attempt	4
46.5.180.250	[1:882:4] WEB-CGI calendar access	3
46.5.180.250	[1:1767:2] WEB-MISC search.dll access	3
46.5.180.250	[1:1546:4] WEB-MISC cisco /%% DOS attempt	3
46.5.180.250	[1:1010:5] WEB-IIS encoding access	3
46.5.180.250	[1:1287:5] WEB-IIS scripts access	2
46.5.180.250	[1:1112:4] WEB-MISC http directory traversal	2
46.5.180.250	[1:1561:4] WEB-MISC ?open access	1
46.5.180.250	[1:1560:4] WEB-MISC /doc/ access	1

2.1.7 Correlations

No correlations were found, although Cisco described this vulnerability at http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml.

2.1.8 Evidence of active targeting

These attacks are not actively targeted since the alerts were false positives.

2.1.9 Severity

The severity formula is not essential here because this is a false positive. In case this was no false positive the formula would be:

The severity formula is:

(criticality + lethality) – (system countermeasures + network countermeasures)

Each of the above variables has a value ranging from 1 (lowest) to 5 (highest)

Values of the variables for this alert:

- Criticality: 5, the destination router seems to be targeted.
- Lethality: 1, if the destination router had the IOS HTTP server running without restrictions it could have been vulnerable for this attack. The right conditions for this attack are very rare though.
- System countermeasures: 1, the IOS will halt and boot the router. This value will be 1 if no countermeasures are taken and 4 or 5 if ACLs, password protection, etc. are implemented.
- Network countermeasures: 1, if this a router connected to the Internet no network countermeasures are present.

Severity = (5 + 1) – (1 + 1) = **4**

2.1.10 Defensive recommendations

If this was a genuine "WEB-MISC cisco /%% DOS attempt" alert:

- Disable the IOS HTTP server on the router.
- Upgrade the IOS to the most recent version.
- Use an access list to prevent unauthorized access to the router.
- Apply an access-class option directly to the HTTP server itself.

As this was a false positive no defensive recommendations are made.

2.1.11 Multiple choice test question

You can identify an operating system on:

A. ttl, ID, window size and initial sequence number
B. ttl, window size, DF bit set and TOS settings
C. ttl, window size, DF bit set and ID
D. ttl, window size and ID

Answer is B.

2.1.12 Incidents.org Questions

1. Posted by Jon Warchild

   "You may want to clarify what you mean here based on the data you were given. Just because this was TCP traffic and TCP traffic requires a 3-way handshake, does not mean that it wasn't spoofed. Take a peek at the Sequence and Acknowledge values in the packets -- with a quick reference to the TCP RFC, you can give a good probabalistic analysis of whether or not some or all of the attack was spoofed."

Answer:

	Seq HEX	Seq DEC	Ack HEX	Ack DEC
Alert 1 – 1	0xA0E5C06E	2699411566	0xB0E4428	185484328
Alert 1 – 2	0xA0E5C7E8	2699413480	0xB0E55D0	185488848
Alert 2 – 1	0xAA2649	11150921	0x967AF474	2524640372
Alert 2 – 2	0x967AF575	2524640629	0xAA2882	11151490

Alert 1-1 and 1-2 have a normal flow, but it seems that the seq and ack number have switched for alerts 2-1 and 2-2.

2. Posted by Donald Smith

“While probably not spoofed look at the ttls. What kind of system might have changed ttls like that? They go from 124 to 240! Assuming the 124 started as 128 that makes this machine 4 hops away from the detector. But then the 240 which probably started at 255 is 15 hops away. Could the network change THAT much between these packets?”

Answer:

There is indeed something strange about the last packet though. When we take a look at the TTL, the window size, the DF bit, the TOS, the ID and the DgmLen we see that:

	Packet 1	Packet 2
TTL	124 (4 hops away)	240 (15 hops away)
Window	0x2058 (8280)	0x25BC (9660)
DF	Set	Not set
TOS	0x0 (0)	0x10 (16)
ID	43075	0
DgmLen	608	607
	Win 9*/NT	Maybe Cisco IOS 12.0

Maybe 46.5.180.250 is a http proxy.

2.1.13 References

Cisco, 11th March 2002, Cisco IOS HTTP Server Vulnerability, Revision 1.1, On-line available at http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml.

2.2 Detection # 2 “FTP wu-ftp file completion attempt”

2.2.1 Detection data

The Snort rule that triggered this specific alert is:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP wu-ftp file completion attempt [";
flow:to_server,established; content:"~"; content:"["; reference:cve,CAN-2001-0886; reference:bugtraq,3581;
classtype:misc-attack; sid:1377; rev:7;)
```

The alerts that were triggered by the previous Snort rule are:

```
07/07-00:51:38.004488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2103 -> 46.5.180.133:21
07/07-00:51:38.164488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2103 -> 46.5.180.133:21
07/07-00:52:00.014488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2104 -> 46.5.180.151:21
07/07-00:52:00.184488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2104 -> 46.5.180.151:21
07/07-00:52:22.034488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2105 -> 46.5.180.153:21
07/07-00:52:22.204488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2105 -> 46.5.180.153:21
07/07-00:52:44.044488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2106 -> 46.5.180.135:21
07/07-00:52:44.214488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2106 -> 46.5.180.135:21
07/07-00:53:06.044488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2108 -> 46.5.180.153:21
07/07-00:53:06.214488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2108 -> 46.5.180.153:21
07/07-00:53:28.054488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2109 -> 46.5.180.151:21
07/07-00:53:28.224488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2109 -> 46.5.180.151:21
07/07-00:53:50.084488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2110 -> 46.5.180.134:21
07/07-00:53:50.254488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2110 -> 46.5.180.134:21
07/07-00:54:12.074488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2111 -> 46.5.180.133:21
07/07-00:54:12.244488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2111 -> 46.5.180.133:21
07/07-00:54:34.094488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2112 -> 46.5.180.135:21
07/07-00:54:34.264488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2112 -> 46.5.180.135:21
07/07-00:54:56.124488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2113 -> 46.5.180.134:21
07/07-00:54:56.294488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 134.126.133.162:2113 -> 46.5.180.134:21
07/07-13:27:56.104488  [**] [1:1378:7] FTP wu-ftp file completion attempt { [**] [Classification: Misc Attack] [Priority: 2]
{TCP} 192.115.133.250:1627 -> 46.5.180.133:21
```

The Tcpdump output is as follows :

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

07/07-00:51:59.974488 134.126.133.162:2104 -> 46.5.180.151:21
TCP TTL:51 TOS:0x0 ID:43646 IpLen:20 DgmLen:560 DF
***AP*** Seq: 0xBD48957C  Ack: 0x86A4E439  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 30357850 6751786
43 57 44 20 30 30 30 30 30 30 30 30 30 30 30 30  CWD 000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 F0 FC 40 31 07 08 98 5F 08 08 EB 0C  0000..@1..._....
EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C  ................
EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C  ................
EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C  ................
EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C  ................
EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C  ................
EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C  ................
EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C  ................
EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C  ................
EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C  ................
EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C EB 0C  ................
EB 0C EB 0C 90 90 90 90 90 90 90 90 90 90 90 90  ................
31 DB 43 B8 0B 74 51 0B 2D 01 01 01 01 50 89 E1  1.C..tQ.-....P..
6A 04 58 89 C2 CD 80 EB 0E 31 DB F7 E3 FE CA 59  j.X......1.....Y
6A 03 58 CD 80 EB 05 E8 ED 0A CA 59 6A 03 58 CD  j.X........Yj.X.
80 EB 05 E8 ED FF FF FF FF FF FF 0A              ............

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

07/07-00:52:00.014488 134.126.133.162:2104 -> 46.5.180.151:21
TCP TTL:51 TOS:0x0 ID:43647 IpLen:20 DgmLen:68 DF
***AP*** Seq: 0xBD489778  Ack: 0x86A4E642  Win: 0x1920  TcpLen: 32
TCP Options (3) => NOP NOP TS: 30357855 6751789
43 57 44 20 7E 2F 7B 2E 2C 2E 2C 2E 2C 2E 7D 0A  CWD ~/{.,.,.,.}.

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

07/07-00:52:00.184488 134.126.133.162:2104 -> 46.5.180.151:21
TCP TTL:51 TOS:0x0 ID:43655 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0xBD4897E0  Ack: 0x86A4E779  Win: 0x1920  TcpLen: 32
TCP Options (3) => NOP NOP TS: 30357872 6751807
43 57 44 20 7E 7B 0A                             CWD ~{.

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

07/07-00:52:21.994488 134.126.133.162:2105 -> 46.5.180.153:21
TCP TTL:51 TOS:0x0 ID:42562 IpLen:20 DgmLen:560 DF
***AP*** Seq: 0xBEDDE7A6  Ack: 0x88951CBD  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 30360052 6753987
43 57 44 20 30 30 30 30 30 30 30 30 30 30 30 30  CWD 000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
```

2.2.2 Source of the trace

This trace is taken from a log file at http://www.incidents.org/logs/Raw/. There was no information available about the network infrastructure.

2.2.3 Detect was generated by

The raw tcpdump log files provided at http://www.incidents.org/logs/Raw/ were generated by the Snort Intrusion Detection System (http://www.snort.org).

2.2.4 Probability the source address was spoofed

It is quite unlikely that the source address was spoofed because an FTP connection requires an established connection via a three-way handshake. It is possible though that the host of which we see the incoming IP address is compromised. The hacker will use this compromised host while hacking someone's network and thereby hides his own source IP address. It is certainly essential though that an active FTP session has been established because the hacker needs to logon and send his or her rootkit to the FTP server. This way we conclude that the chance of this being a spoofed IP address is very low.

2.2.5 Description of the attack

The Wu-ftpd is an FTP server based on the BSD ftpd developed by the Washington University. This FTP daemon has a buffer overflow that can be used by a remote attacker to execute arbitrary code on the server with root permissions.

Exploits for this attack were found at

- CVE: CAN-2001-0886 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0886)
- Bugtraq: 3581 (http://online.securityfocus.com/bid/3581)

2.2.6 Attack mechanism

To exploit this buffer overflow, the attacker must be able to log in to the FTP daemon with an account or the anonymous account. Clients can use "file globbing"patterns for organizing their files with Wu-FTP. Wu-FTP creates a list of the matching files while processing the globbing pattern. If an error occurs during the processing there will be no memory allocated. Under certain circumstances Wu-FTP will free some memory though and it is at this moment that a hacker can enter data which can lead to the execution of arbitrary commands. A more detailed description, a list of affected systems and also a corroboration can be found at http://aris.securityfocus.com/alerts/wuftpd/011128-Alert-wuftpd.pdf.

2.2.7 Correlations

The “FTP wu-ftp file completion attempt {“ alert is apparently a very common alert as it was mentioned on multiple sites. One of these postings caught my attention though. The following Snort information was reported by Gideon Lenkey on 10th January 2002 at http://online.securityfocus.com/archive/75/249597.

```
SNORT reports a buffer overflow:
- ------------------------------------------------------------------------
attacks  from             to              method
===========================================================================
   420    134.184.43.10    1.1.1.1    FTP EXPLOIT stat overflow : {TCP}
   420    134.184.43.10    1.1.1.1    FTP wu-ftp file completion attempt { {TCP}
     1    134.184.43.10    1.1.1.1    FTP wu-ftp file completion attempt [ {TCP}
```

This information was gathered when Gideon’s Linux box was compromised with an ftp buffer overflow. After this intrusion a file integrity checker was run on the machine. The output of this check showed anomalies in the file system, but according to Gideon, there were no signs of a Trojan (perhaps he overlooked the “`added:/lib/libZ.a/log/sniff`” alert). The output of the checker was double checked with the same results. Finally the machine was “shutdown and booted from a jump kit CD and the root partition system was mounted from a different mount point.” Apparently the root kit hides the hacker by preloading a shared library. The root kit itself contains a sniffer, an sshd and a cron process to keep the sshd and the sniffer alive.

When we take a look at the other alerts that were triggered by 134.126.133.162 we see that this host also triggers the “FTP EXPLOIT CWD overflow” alert on the same targets as for the “FTP wu-ftp file completion attempt {“ alert as we can see in Table 2. It is certainly advised to check the destinations (i.e. 46.5.180.x) for a possible installation of a rootkit.

Table 2 : Other alerts for 134.126.133.162 and 192.115.133.250

SRC IP	Alerts	# Alerts	DST IP
134.126.133.162	[1:1378:7] FTP wu-ftp file completion attempt {	4	46.5.180.153
134.126.133.162	[1:1378:7] FTP wu-ftp file completion attempt {	4	46.5.180.151
134.126.133.162	[1:1378:7] FTP wu-ftp file completion attempt {	4	46.5.180.135
134.126.133.162	[1:1378:7] FTP wu-ftp file completion attempt {	4	46.5.180.134
134.126.133.162	[1:1378:7] FTP wu-ftp file completion attempt {	4	46.5.180.133
134.126.133.162	[1:1630:3] FTP EXPLOIT CWD overflow	2	46.5.180.153
134.126.133.162	[1:1630:3] FTP EXPLOIT CWD overflow	2	46.5.180.151
134.126.133.162	[1:1630:3] FTP EXPLOIT CWD overflow	2	46.5.180.135
134.126.133.162	[1:1630:3] FTP EXPLOIT CWD overflow	2	46.5.180.134
134.126.133.162	[1:1630:3] FTP EXPLOIT CWD overflow	2	46.5.180.133
192.115.133.250	[1:1378:7] FTP wu-ftp file completion attempt {	1	46.5.180.133

2.2.8 Evidence of active targeting

In Table 2 you can see that the hacker at 134.126.133.162 first tries two 46.5.180.15* addresses and a second later he has a try on 3 consecutive 46.5.180.13* addresses. The attacker at the 134.126.133.162 host is not scanning for FTP-servers so we can conclude that the attacker was just trying out a few addresses. At the moment of writing this paper none of the above destination IP addresses were alive and thus not accepting incoming FTP sessions.

2.2.9 Severity

The severity formula is:

(criticality + lethality) – (system countermeasures + network countermeasures)

Each of the above variables has a value ranging from 1 (lowest) to 5 (highest)

Values of the variables for this alert:

- Criticality: 4, the hacker was trying a buffer overflow on internal hosts which were running an FTPd.
- Lethality: 5, the destinations are or could have been compromised.
- System countermeasures: 1, no countermeasures by the FTPd, anonymous users are probably allowed.
- Network countermeasures: 1, the traffic was not blocked by a firewall (although I have not seen any traffic sent back to the source Ip address).

Severity = (4 + 5) – (1 + 1) = **7**

2.2.10 Defensive recommendations

If your FTPserver runs the Wu-FTPd and you receive the "FTP wu-ftp file completion attempt" alert you should run a file integrity checker on the server. If there are additional files installed on your system, it is likely that a rootkit has been installed on it. If you are running wu-FTP you should certainly upgrade to the most recent version or consider disabling or removing the software. It is also advisable that access to anonymous FTP servers is limited (or even blocked) at the border routers and/or on the firewalls.

2.2.11 Multiple choice test question

Where is the "CWD ~" command used for?

A. It is used to go to the directory called "~", which is often used to hide files.
B. It is used to determine the existence of a user on the remote system by issuing the command CWD ~<username>
C. It stands for Current Working Directory and it is used to see in which directory you are working.
D. It stands for Copy Working Directory and it is used to copy files between directories. CWD ~ is used to copy a file to the parent directory.

Answer is B.

2.2.12 Incidents.org Questions

Posted by Robert Wagner: “FTP server allowing anonymous connections?? What privileges Read or RW?”

Answer: When you login with the anonymous username most of the time you've got only read access, if you run the buffer overflow you get rw access and can install a rootkit. There are also anonymous FTP servers granting rw access. They can be found using the tool Grim’s Ping (at http://grimsping.cjb.net/).

Posted by Robert Wagner: “Do you recommend just removing the new files or rebuild the server?”

Answer: What if an existing file has been changed and for some reason the filesize stays the same? I think we should rebuild the server. It will take more time (not if sufficient back-ups have been made) but it is much safer.

Posted by Robert Wagner: “Was the IDS on the compromized server or picking up traffic in parrellel to it (can the IDS be trusted)? Should all traffic going to and from the compromized server be monitored (log every connection + details)?”

Answer: All the traffic *to* the server should get monitored for anonymous logins. All the traffic *from* the server should get monitored for suspicious port activity (ssh connections). I don't think the sensor of the IDS was on the server itself. This would be very unsafe. I guess it was on a separate server sending all the logs to a separate, safe server.

Posted by Donald Smith: What OS was affected in Gideon’s detect?

Answer: Red Hat 7.0

2.2.13 References

ARIS Predictor, Securityfocus, 28 November 2001, Wu-ftpd Incident Alert, On-line available at http://aris.securityfocus.com/alerts/wuftpd/011128-Alert-wuftpd.pdf.

G. Lenkey, 10 January 2002, ld.so.preload Root Kit, On-line available at http://online.securityfocus.com/archive/75/249597.

2.3 Detection # 3 : “SOCKS scan”

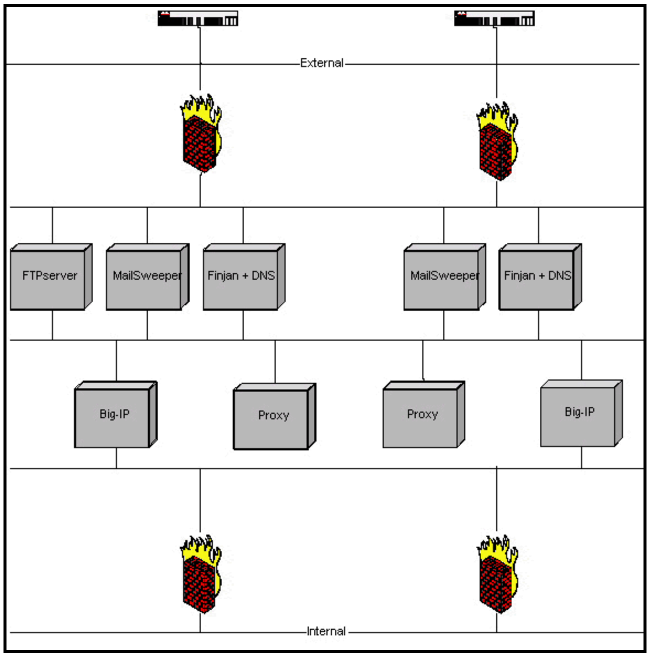
2.3.1 Detect data

```
01:05:55.435464 I x.47.146.102.2721 > MY.NET.147.socks: S 446231048:446231048(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
01:05:58.647048 I x.47.146.102.2721 > MY.NET.147.socks: S 446231048:446231048(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
01:06:05.209608 I x.47.146.102.2721 > MY.NET.147.socks: S 446231048:446231048(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
01:12:01.635613 I x.47.146.102.1951 > MY.NET.240.socks: S 683089364:683089364(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
01:54:15.257547 I x.47.146.102.3990 > MY.NET.145.socks: S 2314052035:2314052035(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
02:10:59.325879 I x.47.146.102.4730 > MY.NET.202.socks: S 2960499149:2960499149(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
02:11:02.566973 I x.47.146.102.4730 > MY.NET.202.socks: S 2960499149:2960499149(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
02:11:09.130677 I x.47.146.102.4730 > MY.NET.202.socks: S 2960499149:2960499149(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
03:13:23.725914 I x.47.146.102.1279 > MY.NET.247.socks: S 1074348904:1074348904(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
03:13:26.904549 I x.47.146.102.1279 > MY.NET.247.socks: S 1074348904:1074348904(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
03:13:33.466285 I x.47.146.102.1279 > MY.NET.247.socks: S 1074348904:1074348904(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
03:15:04.920250 I x.47.146.102.2122 > MY.NET.216.socks: S 1138927662:1138927662(0) win 60352 <mss
1460,nop,wscale 2,nop,nop,sackOK> (DF)
```

2.3.2 Source of the trace

This trace was taken on the external firewalls of our corporate’s internet infrastructure (see Figure 3).

Figure 3 : Corporate network



2.3.3 Detect was generated by

The log file was captured via a tcpdump filter on the firewall. This attack was captured 'by accident' while I was experimenting with the syntax of tcpdump. The rule dropped all traffic for the ports 25 (SMTP), 53 (DNS), 80 (HTTP) and 443 (HTTPS) and all traffic sent to a multicast address used by our firewall's redundancy mechanism. I wrote this rule to see if there were a lot of scans aimed at our infrastructure. I captured on average one scan per day (most of them were 'plain' IP scans or port scans).

2.3.4 Probability the source address was spoofed

The propability that the source was spoofed is reasonable. If the attacker is sniffing the network of the spoofed IP he will still be able to see the reply packets sent by the firewall to the spoofed IP.

2.3.5 Description of the attack

This attack is initiated by a hacker looking for open SOCKS ports. The SOCKS server is a server that is usually lined up parallel to the http and ftp proxy and handles all the connections that are not forwarded by the latter proxies.

2.3.6 Attack mechanism

The hacker is just doing a little reconnaissance here. In case he finds a listening port (a SOCKS server usually listens on port 1080 but this can be altered by the sysadmin). SOCKS are 'widely' used to obfuscate IP addresses. When a hacker (or shall I call him a spammer) finds an open SOCKS server he can use this server for example to proxy his spam because the source IP address will be the one of the SOCKS server. The log files of proxy servers are usually kept for a few months or years so eventually it will be possible to track the real source address of the attacker. However, it is also possible that the attacker uses a chain of proxy servers to obfuscate his address which makes it very difficult and time-consuming to detect the real source address.

According to the ports database on http://www.iss.net/security_center/advice/ Exploits/Ports/ most hackers scanning for port 1080 are looking for Wingate, which is a proxy for Windows. Bugtraq id 509 “Qbik WinGate Buffer Overflow DoS Vulnerability” (or CVE entry CVE-1999-0441) tells about a very easy exploit for Wingate. You have just got to telnet to port 2080 (I think this a typo in Bugtraq?) and send 1.079 characters. It will result in a crash of the Wingate server.

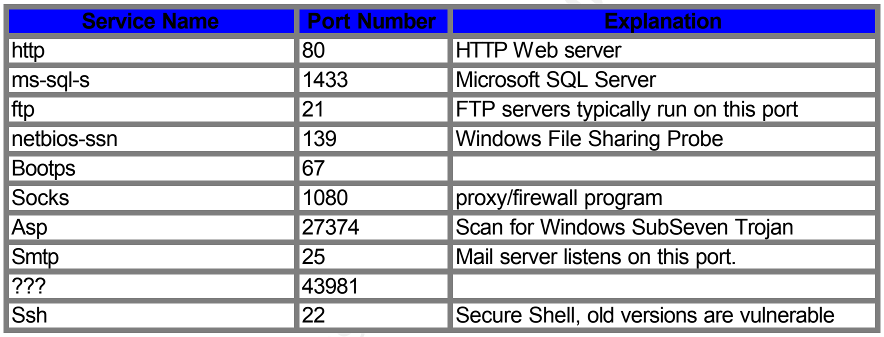
2.3.7 Correlations

Socks scans are very common these days.

In http://www.incidents.org/archives/y2k/0115stutzman.htm Jeff Stutzman states that SOCKS scanning is the second most scanned port.

At incidents.org the SOCKS port is at the sixth place of most scanned ports (See Table 3).

Table 3 : Top 10 ports at incidents.org



Service Name	Port Number	Explanation
http	80	HTTP Web server
ms-sql-s	1433	Microsoft SQL Server
ftp	21	FTP servers typically run on this port
netbios-ssn	139	Windows File Sharing Probe
Bootps	67	
Socks	1080	proxy/firewall program
Asp	27374	Scan for Windows SubSeven Trojan
Smtp	25	Mail server listens on this port.
???	43981	
Ssh	22	Secure Shell, old versions are vulnerable

Source: http://isc.incidents.org/top10.html

2.3.8 Evidence of active targeting

There is no SOCKS server present in our network, so the hacker is definitely scanning our network. The IP addresses he scanned were not actively used so he is just guessing. I don’t think he is using some sort of scanning tool because there is a random interval from several seconds (even minutes) between two scanned destinations. It could be a slow scan, but no other activity from this source IP address was noticed in the logging for the rest of the week (and it was captured at the beginning of the week).

2.3.9 Severity

The severity formula is:

(criticality + lethality) – (system countermeasures + network countermeasures)

Each of the above variables has a value ranging from 1 (lowest) to 5 (highest)

Values of the variables for this alert:

- Criticality: 1, the hacker was just scanning at random for SOCKS servers.
- Lethality: 1, there is no active SOCKS server present on our network.
- System countermeasures: 5, there is no active SOCKS server present on our network.
- Network countermeasures: 5, the traffic was blocked by the firewalls.

Severity = (1 + 1) – (5 + 5) = **-8**

2.3.10 Defensive recommendations

As long as this traffic is blocked at the firewalls or the border routers this scan should be harmless.

2.3.11 Multiple choice test question

What is the difference between "reconnaissance through indirect observation" and "advanced reconnaissance through indirect observation"?

A. The hacker uses a more advanced scanner with lots of functionalities (e.g. Nmap) instead of a simple script.
B. The hacker uses public IP addresses instead of private IP addresses.
C. The hacker uses multiple compromised hosts which are used to observe the response and forward it to the hacker.
D. The hacker is hiding his other activities by sending multiple packets with different spoofed source IP addresses.

Answer is C. The advanced part implies on the fact that the attacker uses multiple compromised hosts for the reconnaissance. More information can be found at http://www.sans.org/newlook/resources/IDFAQ/spoofed_IP.htm.

2.3.12 Incidents.org questions

Posted by Jon Warchild: "Spoofing a scan can have a pretty large impact on the overall attack, as the baskscatteris often easy to spot. Additionally, point out what the snort rule is looking for in this case – port 1080, SYN – and how easy it is to pass a spoofed packet like this through every firewall/filtering device in existence."

Answer: I've got to disagree about the last one. If a (personal) firewall is misconfigured passing all the traffic from and to the Internet (instead of only to the Internet) it is easy to pass the firewall. If a stateful packet filter does not allow incoming connections via port 1080, you will not pass, even if it is a spoofed packet.

2.3.13 References

Everything2, 9th July 2000, Socks, On-line available at http://www.everything2.com/ index.pl?node=Socks.

3 Assignment # 3: Analyze This

A University has asked me to perform an audit on log data files of five consecutive days, which they provided. The purpose of this assignment is to produce an analysis report with special attention on signs of compromised systems or other network problems.

3.1 Executive Summary

In order to conduct this audit, network logs from 5 consecutive days were downloaded from the University's ftp-site. Each log was analyzed in order to get an understanding of the type of specific alerts noted during this time-period.

Millions of alerts were investigated for this short period, which can only mean that the university is crowded with criminals or that the rules from the intrusion detection sensors should be tuned. It is impossible to generate so much 'illegal' traffic in such a short period of time, the network I think the latter is the case. All the different alerts are described in detail in 3.4.

As it was very difficult to focus on the real security issues with all the false alerts, I think the network of the University is quite secure. Nevertheless, a number of compromised hosts could be identified, which are described in more detail in 3.15.

3.2 List of Files

The University provided me with several log files in Snort format which can be found on www.incidents.org/logs. I selected the log files from 14 till 18 June (see Table 4) and downloaded them from the website. I added 3 extra oos_files because the files from 16 till 18 June were lacking.

Table 4: List of files

Friday	14 June 2002	Alert.020614.gz 19,349,046	Scans.020614.gz 26,575,222 bytes	Oos_Jun.14.2002.gz 2,790 bytes
Saterday	15 June 2002	Alert.020615.gz 10,439,117	Scans.020615.gz 17,422,461 bytes	Oos_Jun.15.2002.gz 846 bytes
Sunday	16 June 2002	Alert.020616.gz 12,851,421	Scans.020616.gz 19,927,071 bytes	N/A
Monday	17 June 2002	Alert.020617.gz 9,744,658	Scans.020617.gz 12,640,396 bytes	N/A
Tuesday	18 June 2002	Alert.020618.gz 97,615,869	Scans.020618.gz 7,510,245 bytes	N/A
Wednesday	-	-	-	Oos_Jun.19.2002.gz 142,062 bytes
Thursday	-	-	-	Oos_Jun.20.2002.gz 317,171 bytes
Friday	-	-	-	Oos_Jun.21.2002.gz 368,944 bytes

3.3 Network infrastructure

Before I started to analyze the log-files I had to get a picture of the network infrastructure.

I did this by identifying the routers and the gateways of the university's network. These routers and gateways are the boarder between the university and the network and will pass the hostile traffic or will be subject of an attack.

First I identified the university's private range of IP addresses. Since the range 130.85.0.0 appeared the most in the log files I did an nslookup on one of these addresses. I took 130.85.53.51 and it resolved as ecs021pc21.ucslab.umbc.edu. I surfed to the www.umbc.edu website and it appears to be the University of Maryland, Baltimore County. According to the Arin website (www.arin.net) the University of Maryland, Baltimore Country is owner of the 130.85.0.0 segment.

```
University of Maryland Baltimore County (NET-UMBCNET)
        UMBC University Computing
        Baltimore, Maryland 21250
        US

        Netname: UMBCNET
        Netblock: 130.85.0.0 - 130.85.255.255

        Coordinator:
           Suess, John J.  (JJS41-ARIN)  jack@UMBC.EDU
           (410)455-2582

        Domain System inverse mapping provided by:

        UMBC5.UMBC.EDU               130.85.1.5
        UMBC4.UMBC.EDU               130.85.1.4
        UMBC3.UMBC.EDU               130.85.1.3

        Record last updated on 17-Mar-2000.
        Database last updated on  21-Jul-2002 20:00:38 EDT.
```

In Table 5 I played a little bit with nslookup and tracert.

Table 5 : Nslookup and Tracert results

	Name	IP address	Last but one hop	Last hop
Nameservers	UMBC3.UMBC.EDU	130.85.1.3	131.118.255.18	130.85.16.6
	UMBC4.UMBC.EDU	130.85.1.4	131.118.255.18	130.85.16.6
	UMBC5.UMBC.EDU	130.85.1.5	131.118.255.18	130.85.16.45
Webserver	www.umbc.edu	130.85.253.114	131.118.255.18	130.85.16.45
SMTP servers	mx1out.umbc.edu	130.85.253.51	131.118.255.18	130.85.16.6
	mx2out.umbc.edu	130.85.253.52	131.118.255.18	130.85.16.6
	mx3out.umbc.edu	130.85.253.53	131.118.255.18	130.85.16.45
POP3 servers	mr4.umbc.edu	130.85.60.10	131.118.255.18	130.85.16.6
	amidala.umbc.edu	130.85.6.39	131.118.255.18	130.85.16.45
	mr2.umbc.edu	130.85.6.44	131.118.255.18	130.85.16.45
	mr3.umbc.edu	130.85.6.59	131.118.255.18	130.85.16.45

I have a first picture now of some of the University's servers with a connection to the Internet.

3.4 List of detects

Because the same information from the scans- and oos-files is included in the alert-files, only the alert-files are used for the generation of the list of detects (see Table 6). The list contains 105 different kinds of alerts!

Table 6 : Alerts sorted by frequency

Number of alerts	Alert
886836	suspicious host traffic
54218	SMB Name Wildcard
33028	SNMP public access
27492	MISC Large UDP Packet
22441	spp_http_decode: IIS Unicode attack detected
18685	ICMP Echo Request L3retriever Ping
13723	INFO Inbound GNUTella Connect request
6665	MISC traceroute
6414	INFO MSN IM Chat data
6039	ICMP Destination Unreachable (Communication Administratively Prohibited)
5925	ICMP Destination Unreachable (Host Unreachable)
4153	WEB-MISC prefix-get //
4110	CS WEBSERVER - external web traffic
3762	AFS - Off-campus activity
3619	MISC source port 53 to <1024
2679	UDP SRC and DST outside network
2455	ICMP Echo Request Nmap or HPING2
1557	High port 65535 udp - possible Red Worm - traffic
1387	WEB-MISC Attempt to execute cmd
1281	ICMP Echo Request Windows
1141	ICMP Echo Request BSDtype
1007	ICMP Fragment Reassembly Time Exceeded
926	FTP DoS ftpd globbing
845	Watchlist 000222 NET-NCFC
690	INFO FTP anonymous FTP
672	MISC Large ICMP Packet
663	ICMP Router Selection
595	Watchlist 000220 IL-ISDNNET-990517
557	WEB-IIS view source via translate header
439	SMB C access
392	Queso fingerprint
370	SCAN Proxy attempt
359	Null scan!
356	IDS552/web-iis_IIS ISAPI Overflow ida nosize
256	High port 65535 tcp - possible Red Worm - traffic
215	NIMDA - Attempt to execute cmd from campus host
214	INFO Outbound GNUTella Connect request
150	CS WEBSERVER - external ftp traffic
146	ICMP Source Quench
142	Port 55850 tcp - Possible myserver activity - ref. 010313-1
101	INFO - Possible Squid Scan
96	SUNRPC highport access!
95	ICMP traceroute
93	ICMP Destination Unreachable (Fragmentation Needed and DF bit was set)
68	WEB-MISC http directory traversal
65	Possible trojan server activity
59	EXPLOIT x86 NOOP
57	INFO Possible IRC Access
57	WEB-FRONTPAGE _vti_rpc access
54	WEB-IIS _vti_inf access
54	ICMP Destination Unreachable (Network Unreachable)
54	Attempted Sun RPC high port access

51	spp_http_decode: CGI Null Byte attack detected
47	NMAP TCP ping!
47	WEB-MISC count.cgi access
37	WEB-MISC compaq nsight directory traversal
34	INFO Napster Client Data
32	Incomplete Packet Fragments Discarded
26	WEB-MISC Lotus Domino directory traversal
23	WEB-CGI formmail access
22	WEB-MISC 403 Forbidden
22	WEB-MISC whisker head
19	WEB-CGI rsh access
17	INFO Outbound GNUTella Connect accept
15	ICMP Address Mask Request
13	BACKDOOR NetMetro Incoming Traffic
13	EXPLOIT x86 setgid 0
13	SCAN Synscan Portscan ID 19104
12	ICMP Echo Request CyberKit 2.2 Windows
11	WEB-CGI redirect access
10	EXPLOIT x86 setuid 0
8	ICMP Destination Unreachable (Protocol Unreachable)
8	WEB-IIS Unauthorized IP Access Attempt
8	NETBIOS NT NULL session
7	WEB-CGI csh access
6	connect to 515 from outside
6	EXPLOIT NTPDX buffer overflow
6	Port 55850 udp - Possible myserver activity - ref. 010313-1
6	WEB-CGI finger access
5	MS-SQL xp_cmdshell - program execution
5	X11 outgoing
4	beetle.ucs
4	RPC tcp traffic contains bin_sh
4	Back Orifice
3	WEB-CGI ksh access
3	INFO Inbound GNUTella Connect accept
3	SCAN FIN
2	Tiny Fragments - Possible Hostile Activity
2	WEB-FRONTPAGE fpcount.exe access
1	WEB-IIS .cnf access
1	WEB-CGI glimpse access
1	WEB-MISC ~root
1	EXPLOIT x86 stealth noop
1	Virus - Possible pif Worm
1	TFTP - Internal UDP connection to external tftp server
1	TFTP - External UDP connection to internal tftp server
1	SMTP chameleon overflow
1	SCAN XMAS
1	MISC PCAnywhere Startup
1	IRC evil - running XDCC
1	ICMP Redirect (Network)
1	Virus - Possible scr Worm

3.5 Description of detects

I divided the detects in 7 parts:

- Suspicious traffic: traffic that could be harmless, but must be watched.
- Information gathering attempts: traffic that is meant to gain information about the University's network.

- P2P and chatters: traffic that can result in massive bandwidth utilization and the exchange of infected files.
- Viruses, worms and Trojans: little programs with big consequences
- Web alerts: abnormal, suspicious traffic destined for the webservers
- FTP alerts: anormal, suspicious traffic destined for the FTP servers
- Other system integrity attempts : abnormal, suspicious traffic destined for other servers or hosts (SQL servers, SMTP servers, hosts, …)

The above break up has not been consequently followed throughout this paper. There were alerts belonging to a category of rules (e.g. ICMP) were some of the exploits can be used to run a denial of service attack while others are used for information gathering. These alerts were not split up from their category.

3.5.1 Suspicious traffic

3.5.1.1 Suspicious host traffic

I couldn't find any correlations for this specific alert on the Internet. As the title of the alert mentions it is a very general alert. I checked the log again for destination IP and destination port and it revealed some interesting scans:

- IP scans against hosts from the 18.29.100.0, 18.29.113.0, 18.29.114.0, 18.29.115.0, 18.29.116.0, 18.29.117.0, 18.29.118.0 and 18.29.119.0 segment on destination port 80. These hosts were all scanned by one internal host, i.e. 130.85.157.248. This host or the user of this host should definitely be checked.
- Various port scans initiated by a pretty large number of different source IP addresses against the hosts (i.e. distributed port scans):

130.85.75.102	port 1789 → 3801
130.85.5.44	port 1082 → 4985
130.85.158.75	port 35714 → 42399
130.85.157.253	port 2805 → 4510
130.85.157.252	port 1080 → 3899
130.85.157.248	port 1027 → 4985
130.85.157.247	port 1079 → 2197
130.85.157.243	port 1063 → 2094
130.85.157.242	port 1073 → 4886

3.5.1.2 Watchlist 000220 IL-ISDNNET-990517 and 000222 NET-NCFC

The watchlists 000220 IL-ISDNNET-990517 and 000222 NET-NCFC were also mentioned in the paper from my colleague Hee So. Both watchlists are monitoring the traffic generated by two sources:

- Watchlist 000220 IL-ISDNNET-990517: ISDN Net Ltd. (212.179.0.0/16)
- Watchlist 000222 NET-NCFC: Institute of Computing Technology Chinese Academy of Sciences, Bejing China (159.226.0.0/16)

The 212.179.0.0 segment belongs to Bezeq International, an Israeli phone company. Herd Beast writes in Phrack Magazine about Bezeq: “As you might have understood, up until lately, the Israeli phone company (Bezeq) wasn't very aware of security and boring stuff like that. Now it's becoming increasingly aware, although not quite enough. The notion in Israel is that hackers are like computer geniuses who can get into ANYWHERE, and when last did you see someone like that? So basically, corporate security is lax (does "unpassworded superuser account" ring a bell?), although not always that lax.” I think this statement says enough. All destination hosts targeted by these well known attack sites should be carefully checked.

3.5.1.3 MISC source port 53 to <1024

This alert is triggered when an external host tries to connect with source port 53 (i.e. DNS) to a privileged port on an internal server. Stateless firewalls may pass this traffic assuming that this is a response to a legitimate DNS query.

With BIND version 4 and lower the source and destination ports are both set to 53 by default as this is the case with almost all the “MISC source port 53 to < 1024” alerts. If the source hosts use Bind version 4 or lower this would mean that the alert is a false positive. BIND 8 and later uses an ephemeral port.

3.5.1.4 UDP SRC and DST outside network

99 % of the “UDP SRC and DST outside network” are triggered with the destination host 229.55.150.208 (which is a multicast address) and destination port 1345. I looked for port 1345 in the Snort port database and it says that it is used for vpjp. When I was looking for vpjp on Google I stumbled on a posting from Jacco Braat at http://cert.uni-stuttgart.de/archive/incidents/2000/11/msg00022.html. He was having the same problem: hosts that were connecting to 229.0.0.0 addresses via port 1345, except that his source addresses were internal. It was in one of the replies to this posting that I found the solution. Peter Freeman wrote at http://cert.uni-stuttgart.de/archive/incidents/2000/11/msg00136.html : “I had the same problem with my machine; I tracked it down to ngctw32.exe which was started from runservice on my Win98 machine. Deleting that registry key solved the problem, and it never happened again. Ngctw32.exe was installed with Norton Ghost, the properties of the exe describe it as Norton Ghost Client Agent. If anyone can tell me what it was reporting to ip 229.55.150.208 and why, it would be nice.” I double-checked this via a search on Google and it was confirmed on a website of Symantec (http://service2.symantec.com/SUPPORT/ghost.nsf/docid/1999033015222425). This way we can conclude that these alerts are all false positives.

3.5.1.5 Connect to 515 from outside

There are just a few connections initiated by the source IP address 255.255.255.255 against port 515. This port is used by Linux systems for network printing and is quite unusual if the connection is initiated from external sources (especially when the source IP address is 255.255.255.255, i.e. spoofed). It is advisable to check the destination hosts for the vulnerabilities IDS 456 and 457 listed on arachnids which can be used against port 515. The source port 31337 is also quite unusual because it stands for 'elite' in hackers language. A correlation was found on http://cert.uni-stuttgart.de/archive/incidents/2001/07/msg00026.html.

3.5.1.6 X11 Outgoing

This alert indicates that an Xterm session was initated, sending output to an external x-server. Exploit IDS 126 was found on arachnids which states that this is insecure traffic since it is often a sign of compromise.

3.5.1.7 Beetle.ucs

Again a strange alert. A search on Google brought me to the GCIA practical of Edward Peck. He says that "This alert indicates that users are copying information from the Internet and saving it to a CD-R". A search on Google for beetle on the .edu domain gives me the following information "How do I ... burn a CD? beetle.ucs.umbc.edu is located in ECS 125A. Put a blank CD-R disc in the external drive, log on, and then (as root) run the command cdrecord dev=/dev/sga speed=4 /this/is/the/path/to/my/cd-image.iso. It should take approximately fifteen minutes to burn a CD." This proves Edward's explanation.

3.5.1.8 AFS – Off-campus activity

At first I didn't find any information about this specific alert on the Internet. All the connections are made to destination port 7001 though. According to the Snort port database, this port is used for "afs3-callback, callbacks to cache managers". AFS – or the Andrew File System – "is a location-independent file system that uses a local cache to reduce the workload and increase the performance of a distributed computing environment. A first request for data to a server from a workstation is satisfied by the server and placed in a local cache. A second request for the same data is satisfied from the local cache." CVE-2000-1174, CAN-2001-1279, CAN-2002-0575 and CAN-2002-0822 are all CVE entries for AFS exploits (most of them are buffer overflows).

3.5.1.9 Tiny Fragments – Possible Hostile Activity

Someone at 68.37.185.113 is sending fragments that are smaller than the normal 256 bytes. This could be a hacker using an nmap, fragrouter or even GNUTella. Because of the small number of alerts (i.e. 2) and because these were the only alerts generated by this source it is of no great importance, unless the number of alerts increases in the future.

3.5.2 CS WEBSERVER – external web/ftp traffic

All of the alerts are generated for the destination 130.85.100.165, which is the webpage for the Computer Science and Electrical Engineering department of the UMBC at http://www.umbc.edu/engineering/csee/. I guess that this is a rule to show all IP addresses of the external hosts which are connecting to the CS (Computer Science) web- or FTPserver.

3.6 Information gathering attempts

3.6.1 SMB Name Wildcard

The SMB (Server Message Block) protocol indicates a Netbios name table retrieval query. This enables Microsoft Windows and Unix computers to share files and printers over a network when only IP addresses are known. Using the program 'nbtstat' a hacker may gain lots of information about (remote) MS Windows hosts. As this can be regarded as a reconnaissance effort all incoming Netbios traffic (ports 137-139) should be blocked at the perimeter of your network. There are numerous external hosts which are trying to connect to port 137 of internal hosts.

3.6.2 Netbios NT Null Session

This alert indicates that somebody tried to login to a Windows NT host as "Nobody". In normal situations this is used to enable enumeration of users and shares. If exploited it can reveal this information to the hacker.

3.6.3 SNMP Public Access

SNMP (Simple Network Management Protocol) is used for network management and monitoring. The sensitive information provided by the network devices via SNMP is only protected by a community string (login + password together). On most of the network devices SNMP is enabled by default with default community strings, which can be easily guessed by hackers. This way hackers can get access to information like the users, shares, domains, running services, etc. All IP addresses that triggered this alert were internal addresses, which is good. Any SNMP traffic that is not explicitly required should be disabled and all inbound traffic to internal SNMP-enabled servers should be blocked on the border routers. More information about the numerous SNMP-exploits can be found at http://www.cert.org/advisories/CA-2002-03.html.

3.6.4 Incomplete packet fragments discarded

This event describes that an IP datagram was fragmented and not all fragments did arrive. This could be harmless or it could indicate that an attacker is checking out some hosts on your network. As the source and destination ports are both zero for all the alerts triggered I think it will be the latter.

3.6.5 Scans

3.6.5.1 Queso fingerprint

This alert tells us that someone has used Queso – which is used for OS fingerprinting –

against the University’s network. A detailed explanation of the Queso fingerprint can be found at http://online.securityfocus.com/infocus/1225.

Lots of false positives are generated by ECN enabled Linux-hosts. It is very simple though to exclude the false positives from the real alerts, as Queso has an initial TTL of 255 and Linux uses an initial TTL of 64. Queso has also a predictable TCP window size but it is not feasable to include this in a Snort signature.

3.6.5.2 NMAP TCP ping!

Someone using the Nmap portscanning tool pinged a host on our network to check if it is reachable. A detailed explanation of the Nmap fingerprint can be found at http://online.securityfocus.com/infocus/1225.

3.6.5.3 SCAN Proxy attempt

This alert means that someone was scanning for port 8080[3]. Hackers are not looking to compromise proxies; they just want to bounce their traffic to erase his/her tracks.

3.6.5.4 Null Scan! and Xmas Scan

With a null scan not one of the available flags in the TCP header is set, look at the source, in comparison to the XMAS scan where all flags are set. Xmas packets have a sequence number of zero. These packets should never be seen in normal TCP operation. There is one Xmas-scan initiated by 65.69.223.128 with destination 130.85.153.178 and destination port 7001. it should be mentioned that most of the connections that triggered the “Null scan!” alert had source and destination port set to zero.

3.6.5.5 INFO – Possible Squid Scan

Squid is a freeware proxy that listens on port 3128. IDS 552 mentions an exploit for Squid and warns for the possibility that hackers use Squid for bouncing their http traffic.

3.6.5.6 Synscan Portscanning ID 19104

This event indicates that an intruder may be using the Synscan tool to portscan your computer. This probe is used to gather information that can be useful in an attack. It is very widely used as a scanner and vulnerability tester for ramen, canserserver and t0rnscan. Donald Smith describes the signatures of Synscan and some other scanners in an excellent way in his GCIA paper.

3.6.5.7 Scan Fin

This event indicates that someone has sent a bare TCP packet where only the FIN flag was set. Fin-scanning can be used in stealth portscanning and is not effective against

[3] According to Snort rule set 1.9, but in this rule port 1080 seems to be added.

Windows machines. The scans were run against the same machine and port (port 0 !), but with a different source port.

3.6.6 ICMP messages

3.6.6.1 ICMP Echo Requests

These alerts are triggered because ICMP echo requests can be misused to map a company's network. The ICMP Echo Request alerts mention the operating systems or tools used by the scanners (See Table 7).

Table 7 : ICMP Echo Request

ICMP Echo Request L3retriever Ping	L3 "Retriever 1.5" security scanner
ICMP Echo Request Nmap or HPING2	Nmap or HPING2
ICMP Echo Request Windows	Microsoft Windows
ICMP Echo Request CyberKit 2.2 Windows	CyberKit 2.2 on Windows
ICMP Echo Request BSDtype	BSD/OS, FreeBSD, NetBSD, OpenBSD 2.5, Linux, or Solaris 2.5-2.7

According to the Whitehats-website the ICMP Echo Request L3retriever Ping alert should be rare, but more than 18.685 alerts were generated by this scanner. When we take a closer look at these alerts we can see that most of these alerts are generated by internal hosts on the 130.85.152.0 segment with 130.85.11.5 (fs1.ad.UMBC.EDU), .6 (dc1.ad.UMBC.EDU) and .7 (dc2.ad.UMBC.EDU) as destination. It is known that the L3retriever alert generates false positives for Win2K hosts connecting to their Win2K domain controllers. As you can see, the resolved names imply that the 3 destinations are part of Win2K Active Directory (hence ad.umbc.edu). When we filter all the 130.85.0.0 source hosts out of the list with "ICMP Echo Request L3retriever Ping" alerts we get a much smaller list.

We can conclude the same for the "ICMP Echo Request Nmap or HPING2" alerts. Lots of alerts are generated by the 130.85.152.0 segment with destination 130.85.11.5, .6 and .7. When we filter all the 130.85.0.0 source hosts out of the list with "ICMP Echo Request Nmap or HPING2" alerts we get a much smaller list

From the 1.281 "ICMP Echo Request Windows" alerts 1.108 were generated by one IP address, i.e. 68.55.192.27 (pcp295007pcs.owngsm01.md.comcast.net) with 130.85.70.225 (kooshofdeath.ucs.umbc.edu :->) as destination. All these pings were generated on 18 June between 20:39 and 21:28. This alert is probably harmless, but on the paranoid side it could also be a convert channel. It should be mentioned though that is one of the rare hosts which is pingable over the Internet and above all that, it is also accessible via HTTP (it is a website promoting Sambar server V4.4 Beta 6).

The "ICMP Echo Request CyberKit 2.2 Windows" alert is a little bit more suspicious because these alerts are generated by one internal IP address, i.e. 130.85.153.157 and it is trying to ping two external IP addresses, 204.71.200.33 (ns1-old.yahoo.com) and 66.218.71.63 (ns1.yahoo.com). It is possible that 130.85.153.157 is compromised but since the destination IP addresses are Yahoo's I think it will be more likely that someone is trying to see if he can still connect to the Yahoo nameservers.

There are companies which are using the ICMP Echo Request BSDtype to detect the closest webserver for large corporate sites and are therefore generating false positives. One such company is Speedera. An overview of the pings the University received from servers from Speedera is listed in Table 8. The destination host for this scan alays stays the same, 130.85.5.82 which resolves as grain.noc.umbc.edu.

Table 8 : ICMP Echo Request BSDtype from Speedera

Alert	SRC IP	DST IP	Number of alerts
ICMP Echo Request BSDtype	193.214.57.194	130.85.5.82	11
ICMP Echo Request BSDtype	193.45.3.130	130.85.5.82	20
ICMP Echo Request BSDtype	202.130.158.130	130.85.5.82	8
ICMP Echo Request BSDtype	203.197.173.129	130.85.5.82	17
ICMP Echo Request BSDtype	203.197.88.130	130.85.5.82	19
ICMP Echo Request BSDtype	203.89.210.82	130.85.5.82	18
ICMP Echo Request BSDtype	204.71.35.136	130.85.5.82	26
ICMP Echo Request BSDtype	205.158.108.194	130.85.5.82	20
ICMP Echo Request BSDtype	208.185.54.14	130.85.5.82	20
ICMP Echo Request BSDtype	209.240.77.130	130.85.5.82	14
ICMP Echo Request BSDtype	209.68.217.194	130.85.5.82	14
ICMP Echo Request BSDtype	209.83.178.130	130.85.5.82	12
ICMP Echo Request BSDtype	211.169.245.98	130.85.5.82	20
ICMP Echo Request BSDtype	212.62.17.145	130.85.5.82	13
ICMP Echo Request BSDtype	216.117.57.66	130.85.5.82	18
ICMP Echo Request BSDtype	216.148.216.2	130.85.5.82	20
ICMP Echo Request BSDtype	216.74.133.194	130.85.5.82	16
ICMP Echo Request BSDtype	64.0.96.12	130.85.5.82	14
ICMP Echo Request BSDtype	64.14.117.10	130.85.5.82	12
ICMP Echo Request BSDtype	64.28.86.226	130.85.5.82	18
ICMP Echo Request BSDtype	64.41.192.103	130.85.5.82	21

3.6.6.2 ICMP Destination Unreachable

The ICMP Destination Unreachable messages are generated by routers to inform the host that the destination address is unreachable due to specific circumstances (See Table 9).

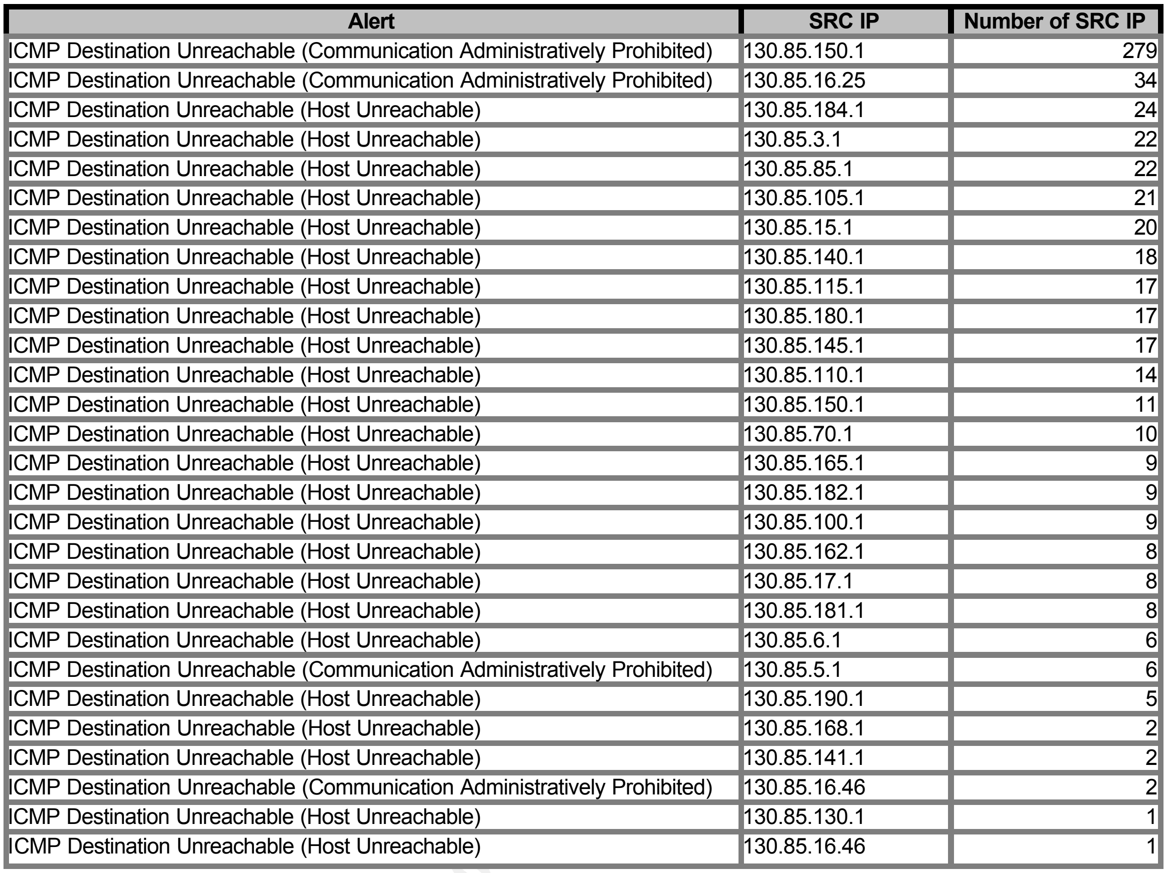
Table 9 : ICMP Destination Unreachable Messages

Message	Explanation
Network Unreachable	The network is unreachable.
Host Unreachable	The host is unreachable.
Protocol Unreachable	The designated transport protocol is not supported.
Fragmentation Needed and DF bit was set	The datagram is too big. Packet fragmentation is required but the DF bit in the IP header is set.
Communication Administratively Prohibited	This is triggered when a router cannot forward a packet due to administrative filtering.

Source : `http://www.networksorcery.com/enp/protocol/icmp/msg3.htm`

In Table 10 you see the routers that are active on the University's network and have sent an ICMP Destination Unreachable message.

Table 10 : Routers on the University's network that have sent an ICMP Destination Unreachable message



Alert	SRC IP	Number of SRC IP
ICMP Destination Unreachable (Communication Administratively Prohibited)	130.85.150.1	279
ICMP Destination Unreachable (Communication Administratively Prohibited)	130.85.16.25	34
ICMP Destination Unreachable (Host Unreachable)	130.85.184.1	24
ICMP Destination Unreachable (Host Unreachable)	130.85.3.1	22
ICMP Destination Unreachable (Host Unreachable)	130.85.85.1	22
ICMP Destination Unreachable (Host Unreachable)	130.85.105.1	21
ICMP Destination Unreachable (Host Unreachable)	130.85.15.1	20
ICMP Destination Unreachable (Host Unreachable)	130.85.140.1	18
ICMP Destination Unreachable (Host Unreachable)	130.85.115.1	17
ICMP Destination Unreachable (Host Unreachable)	130.85.180.1	17
ICMP Destination Unreachable (Host Unreachable)	130.85.145.1	17
ICMP Destination Unreachable (Host Unreachable)	130.85.110.1	14
ICMP Destination Unreachable (Host Unreachable)	130.85.150.1	11
ICMP Destination Unreachable (Host Unreachable)	130.85.70.1	10
ICMP Destination Unreachable (Host Unreachable)	130.85.165.1	9
ICMP Destination Unreachable (Host Unreachable)	130.85.182.1	9
ICMP Destination Unreachable (Host Unreachable)	130.85.100.1	9
ICMP Destination Unreachable (Host Unreachable)	130.85.162.1	8
ICMP Destination Unreachable (Host Unreachable)	130.85.17.1	8
ICMP Destination Unreachable (Host Unreachable)	130.85.181.1	8
ICMP Destination Unreachable (Host Unreachable)	130.85.6.1	6
ICMP Destination Unreachable (Communication Administratively Prohibited)	130.85.5.1	6
ICMP Destination Unreachable (Host Unreachable)	130.85.190.1	5
ICMP Destination Unreachable (Host Unreachable)	130.85.168.1	2
ICMP Destination Unreachable (Host Unreachable)	130.85.141.1	2
ICMP Destination Unreachable (Communication Administratively Prohibited)	130.85.16.46	2
ICMP Destination Unreachable (Host Unreachable)	130.85.130.1	1
ICMP Destination Unreachable (Host Unreachable)	130.85.16.46	1

3.6.6.3 ICMP Router Selection

This message is most commonly generated by hosts running Win9* or Win2K, because IRDP (ICMP Router Discovery Protocol) comes enabled by default on the DHCP clients on these operating systems. A hacker can exploit this by remotely adding a default route on the system which will be preferred over the default route obtained from the DHCP server. All the alerts were triggered by internal hosts with destination a multicast address (224.0.0.2) which seems normal traffic to me.

3.6.6.4 ICMP Source Quench

When a system receives packets at a rate that is too fast to be processed it may (= not required) send an ICMP source quench to the source host telling it to reduce the pace at which it is sending packet to the destination host. Source hosts that are causing this alert are running the destination host out of buffers and are probably trying to run a Denial of Service attack. Because of the low number of this kind of alert it is not likely that these external hosts are trying to DoS a host on the University's network.

3.6.6.5 MISC and ICMP traceroute

Traceroute is a tool commonly used to track the route packets take to reach a host. The "ICMP traceroute" alert tells us that someone is using a traceroute to detect the hops connecting the source host with the destination host.

3.6.6.6 ICMP Redirect

An ICMP Redirect message is used by routers to tell hosts that they are using a non-optimal or non-existing route to their destination. A hacker can exploit this by using crafted ICMP Redirect packets causing traffic to flow via an alternative path bypassing the security of the host. It is also used for denial of service attacks by sending a message that the victim can no longer access a particular network.

There is only one "ICMP Redirect" alert triggered by 213.142.4.4 with destination 130.85.5.82. Hence this alert, the routing table from host 130.85.5.82 has to be checked for irregular routes.

3.6.6.7 ICMP Fragment Reassembly Time Exceeded

When fragmented packets arrive at the destination host it is possible that some of the fragmented packets get lost. The packets that already have arrived at the destination will be kept in a buffer that will discard these packets if a timer has been exceeded. This method can be used by a hacker who is trying to fill these buffers. These alerts are mainly generated by host 130.85.153.169 which is sending some of these messages to hosts on the 211.233.25.0 segment. The number of generated alerts is too low for a buffer overflow I think.

3.6.6.8 ICMP Address Mask request

When a diskless system tries to obtain its subnet mask at bootstrap time it will trigger an ICMP address mask request. This ICMP message can be used to obtain the netmask of a particular device. There were 15 alerts from 194.106.18.32 to destination host 130.85.1.200.

3.7 P2P and chatters

3.7.1 INFO Inbound GNUTella Connect request / accept and INFO Outbound GNUTella Connect request / Accept

GNUTella is a file sharing system where individual users are client as well as server. The default port used by Gnutella is 6346, but this can be altered. As all kind of files can be exchanged (included viruses) this is a serious security threat.

3.7.2 INFO Napster Client Data

Napster is (or was) a peer to peer file (MP3's to be more specific) sharing network. Ports 6699 and 7777 are both used by Napster. Home users who are using Hybrid Network's cable modems are particularly vulnerable because of the lack of authentication for the remote configuration system on these modems. Bugtraq dedicated id 695 to this vulnerability.

3.7.3 INFO MSN IM Chat Data

The alert is triggered by the Microsoft Instant Messenger. Users can chat with each other and check if their friends are online. All the Instant Messenger data seems to be exchanged between the internal network and the 64.4.12.0 segment, which is the msgr.hotmail.com domain. This traffic looks normal to me.

3.7.4 INFO Possible IRC Access

Most of the alerts are triggered by internal users who are using IRC (Internet Relay Chat). This can be in conflict with the university's policy.

3.7.5 IRC evil – running XDCC

An XDCC server is a feature of IRC (Internet Relay Chat) and allows others to get files on computers running the XDCC server. The XDCC server can be used by software pirates in conjunction with backdoors to offer their "warez" on underground file-sharing networks via someone else's hardware. Eventually this will result in an enormous bandwidth utilization of the compromised network.

3.8 Viruses, worms and trojans

3.8.1 High port 65535 udp/tcp – possible Red Worm - traffic

Probably someone has noted UDP and TCP traffic on port 65535 in the past and associated it with Red Worm. The Red Worm – now known as Adore – is a worm that scans Linux hosts for exploits in LPRng, rpc-statd, wu-ftpd and Bind. If the exploit is successful the compromised server will send an e-mail to a number of known e-mailaddresses. Apparently the rule is triggered for a number of high destination ports:

- port 65000 Devil, Sockets des Troie, Stacheldraht
- port 65432 The Traitor (= th3tr41t0r)
- port 65432 (UDP) - The Traitor (= th3tr41t0r)
- port 65534 /sbin/initd
- port 65535 RC1 trojan

3.8.2 NIMDA – Attempt to execute cmd from campus host

This alert is triggered when a host on the internal network tries to connect to port 80 on a variety of (consecutive) destinations looking for IIS webservers. If a vulnerable IIS server is found the Unicode Web Traversal exploit will be used against it. 130.85.157.250 is certainly scanning here and should be checked for the presence of Nimda.

3.8.3 Virus - Possible pif Worm / Possible scr Worm

These alerts were both mentioned in a posting from John Ruff at http://archives.neohapsis.com/archives/snort/2001-08/0543.html. This alert tells you that an e-mail was sent with a .scr (a Windows screensaver) or a .tif (Tagged Image File Format) attachment. Where the alerts appear 3.600 times in John's logging, we've got only one alert of each. Although this rule is known to trigger a lot of false positives (it is excluded from the 1.8.1-RELEASE), it is safer to check 130.85.6.7, 130.85.150.131 and 130.85.88.235 with a virus scanner.

3.8.4 Possible Trojan server activity

The hosts for which this alert was triggered either listen on port 27374 or send packets to port 27374. This port is used by SubSeven, a famous Trojan. Hosts listening on port 27374 (130.85.5.88) should be checked for a SubSeven Trojan.

3.8.5 Back Orifice

Someone on the internal network is looking for a connection with the trojan Back Orifice (listens on port 31337) on a few internal machines. The destination machines (130.85.153.148, 130.85.153.167, 130.85.153.160 and 130.85.152.166) should get checked for Back Orifice. Although there are two source IP addresses the source port is the same (26465) for most of the connection attempts.

3.8.6 BACKDOOR Netmetro Incoming traffic

This alert is quite confusing about the port the Trojan listens on. Arachnids indicates that Netmetro listens on port 1024. The Snort rule is triggered when someone connects to a server listening on port 5032. The alert in this log file was triggered on port 5031 ! Anyway, the destination host (130.85.253.43) must be checked for the presence of Netmetro.

3.9 WEB alerts

3.9.1 Spp_http_decode:IIS Unicode attack detected

This event indicates that someone has sent UNICODE representations of shell metacharacters to the IIS webservers. A search on arachnids tells me that there are different kinds of Unicode attacks (search for IDS 432, IDS 433, IDS 434, IDS 452 on www.whitehats.com for more information). All the alerts are outbound which indicates that no internal webserver was targeted for this specific alert.

3.9.2 Spp_http_decode: CGI Null Byte attack detected

At first I didn't find much information about this alert, but then I stumbled on a paper written by Tom Rodriguez about "Understanding IIS Unicode

Vulnerabilities”. Tom explains the CGI Null Byte attack as follows: “When IIS receives a request referring to a script or executable, it performs URL decoding (converting %hh characters to their ASCII representations) and then performs a security check to ensure that the resulting script or executable path does not attempt to migrate out of the base share. Unfortunately, a second (unnecessary) URL decoding pass is then performed after this check. By specially crafting the URL, it is possible to essentially bypass the security check. For example, the following URL after initial URL decoding ("%25" converts into `%') results in:

http://www.example.com/scripts/..%5c../winnt/system32/attrib.exe?c:\*.*

This is passed to the security check, and it passes. Unfortunately, a second URL decode then occurs (converting the "%5c" into `\') resulting in the following URL getting processed:

http://www.example.com/scripts/..\../winnt/system32/attrib.exe?c:\*.*

This works because the IIS server first determines that the executable file is located under an executable share (ostensibly under the "/scripts" share). However, it is incorrect in this assessment, since the "..\.." portion of the URL indicates utilizing a parent share (the root share in this case) followed by the actual path to the executable. Nevertheless, it works. At this point the attacker can see all files in the C:\ directory, whether hidden or not. This mechanism therefore (again!) allows an attacker to run any arbitrary executable on the target system, even if the executable is outside of the public web directories. This vulnerability is described in CVE-2001-0333 [5], and further analysis has been performed by NSFocus [6] and Microsoft [7] ... However, only some versions of the IIS/PWS Escaped Character Decoding Command Execution vulnerability were recognized (and these were alerted as "CGI Null Byte attack detected", a confusing misdirection).” All these alerts are outbound though indicating that no internal webserver was targeted for this specific alert.

3.9.3 IDS552/web-iis_IIS ISAPI Overflow ida nosize

At first I didn’t find very much information about this one. In the practical assignments from R.W. Yuen and G. Lajon it is stated that Nimda and Code Red trigger these alerts. This explanation was kind of vague so I searched some more. I remembered that Arachnids alerts start with IDS so when I checked the Whitehats website I found the vulnerability the alert was referencing to. Apparently “an unchecked buffer in the Microsoft IIS Index Server ISAPI Extension could enable a remote intruder to gain SYSTEM access to the web server.”

3.9.4 WEB-CGI alerts

Most of the websites on the Internet contain a CGI bin directory where scripts are located that are run by general-purpose interpreters (e.g. csh, ksh, rsh,…). When these interpreters can be accessed directly by the hacker - because the interpreters are located in the cgi bin directory – the hacker will be able to execute arbitrary commands on the Web server system. All the “WEB-CGI”alerts are recurring for the same destination IP addresses (130.85.100.165, 130.85.253.125 and 130.85.6.7), which implies that they should be checked for accessibility of the interpreters. Tom Christiansen provides a script on his web page http://perl.com/perl/news/latro-announce.html to test for it.

It is not only possible though to access interpreters via the cgi bin directory. Other programs are also accessible via the cgi bin directory, like:

- the finger gateway which is used for information gathering,
- the formmail program which is used to create submission web pages. This program can be used to execute arbitrary commands on the webserver.
- the Glimpse programs (WebGlimpse and GlimpseHTTP) : they are used for web indexing and search engines. These programs can be used to execute arbitrary commands on the webserver.
- The Allaire ClusterCATS program which is used for URL redirecting. It can return sensitive information.

If one of the programs mentioned in the list above should be running on the destination hosts, the host should be checked for this vulnerability.

3.9.5 WEB-FRONTPAGE alerts

If Front Page Server Extensions (FPSE, handles the processing of web forms) is installed on one of the destinations of this alert it should be considered vulnerable for the "WEB-FRONTPAGE _vti_rpc access alert". Hackers can DoS the destination hosts simply by sending malformed data.

There were also 2 "WEB-FRONTPAGE fpcount.exe" alerts for destination 130.85.253.125. If the fpcount.exe program is installed on this server a hacker can run a buffer overflow on it and execute arbitrary commands. The destination should be checked for the presence of the fpcount.exe program.

3.9.6 WEB-IIS alerts

.cnf : someone is looking for configuration files on your IIS-webserver. Only one alert was triggered from 66.196.72.60 to 130.85.6.14.

_vti_inf : If you see this WEB-IIS alert someone is looking for the _vti_inf.html file on your IIS server. This file contains the version of the FrontPage extensions and the path on the server where the extensions are located.

Unauthorized IP Access Attempt: This event alerts to the fact that a user has tried to access a protected file or folder. The file or folder is usually protected through access controls. Usually this alert goes hand in hand with the "WEB-MISC 403 Forbidden" alert. These alerts do not generate a security threat.

View source via translate header: Someone was trying to view the source of the scripts on the IIS webserver. The dedicated scripting engine on the IIS webserver handles the requests for advanced file types such as ASP, HTR,…, processes them and executes them on the server. If a hacker adds "translate: f/" in his HTTP GET request, the scripting engine will locate the file and will send the file source to the client. 88 % of the alert messages are targeted to the 130.85.5.96 webserver. This server should get checked for this vulnerability.

3.9.7 WEB-MISC alerts

~root: someone is looking for the root directory. Only one alert was triggered by 64.218.40.7 trying to access 130.85.6.7.

403 Forbidden: users tried to access an access-controlled file on external webservers (also see 3.9.6, Unauthorized IP Access Attempt).

Attempt to execute cmd: someone added cmd.exe in the URL.

Count.cgi access: This alert indicates that a user tried to exploit a vulnerability on CGI script called "phf". If the script installed on your webserver seems vulnerable, the attacker can use this to run arbitrary commands. It appears that most of these alerts are triggered against 130.85.6.14.

http directory traversal: Most webservers allow access to a particular part of the filesystem. Sometimes a user can add a ".." to the path allowing access to parent directories. There are many other Bugtraq and CVE entries for this attack. Two other directory traversal alerts appeared in the alerts list:

- **Compaq nsight directory traversal**: directory traversal vulnerability for the Compaq Web Management Agent. The destination port for the Compaq HTTPd is 2301.
- **Lotus Domino directory traversal**: directory traversal vulnerability for the Lotus Domino server. All these alerts were triggered against destination 130.85.6.7.

Prefix-get //: This alert is triggered when someone adds a second slash after the TLDN when browsing. All these alerts are destined for 130.85.253.114, except for a few connections to the 130.85.99.85 address, which is not even a webserver.

Whisker head: Whisker is an anti-IDS tool, it crafts a request so much that the IDS will get confused, though the webserver will still be able to understand and respond to the request. There is only one external IP address triggering this alert, i.e. 203.148.192.200 with destination 130.85.253.125. The 203.148.192.200 belongs to the Christian College in Thailand, which is suspicious. This alert should be watched in the future.

3.10 FTP alerts

3.10.1 INFO FTP anonymous FTP

This alert indicates that someone logged into an FTP server with the username “anonymous”. This is a security issue since lots of FTP attacks take advantage of this “anonymous” username.

3.10.2 FTP DoS ftpd globbing

This alert is triggered when a hacker tries to crash the FTP server by sending a wildcard request to create a denial of service on vulnerable FTP servers. Most of these alerts are triggered for the destination host 130.85.153.179.

3.10.3 TFTP

TFTP (Trivial File Transfer Protocol) is the easier to use but more insecure version of FTP because of its lack of user authentication and its use of UDP instead of TCP.

At the CERT website I found out that the Nimda virus uses TFTP to transfer a copy of its code to a vulnerable IISserver. There are not enough alerts though for a host to be infected.

If TFTP is needed in the network configuration it should upgraded. TFTP is rarely needed in a network though and should be disabled.

3.11 Other System Integrity Attempts

3.11.1 MS-SQL xp_cmdshell – program execution

This alert could be triggered by a worm looking for vulnerable MS-SQL servers to initiate a series of ‘exec xp_cmdshell ‘xxx’’ commands. The worm is only successful on hosts where MS-SQL has the default installation and where the Administrator account has no password.

3.11.2 SMB C Access

This alert is triggered when a hacker tries to access the default administrative share c$ on your computer via Netbios on port 139. If this kind of traffic is allowed the hacker can access the c: filesystem. Just a few of these alerts were triggered by an external host (144.138.31.41) for a few internal destinations.

3.11.3 MISC PCAnywhere Startup

PCAnywhere is a remote control software for Windows servers. If the PCAnywhere software on the server is not secured by a password and an IP access list it is quite easy to gain access to this server. 68.55.195.120 tries to access 130.85.135.10.

3.11.4 SMTP chameleon overflow

This alert is triggered when someone sends a long “help” command to the Chameleon

SNMPd trying to overflow the buffers. There is only one alert initiated from 205.150.6.35 with destination 130.85.253.41. There is evidence for false positives reported at the Whitehats.com website, though little information is given.

3.11.5 EXPLOITS

Following EXPLOIT alerts were noticed.

- EXPLOIT x86 NOOP: A string of the character 0x90 (i.e. no op in x86 machine code) was detected. NOOPs are sent by remote overflow exploits to pad their chances of successful exploitation.
- EXPLOIT x86 stealth noop: An attacker might have tried to overflow one of the daemons with jmp 0x02 "stealth noops".
- EXPLOIT x86 setgid 0: An attacker sent the setgid 0 system call for the x86 platform. This signature is the most effective when monitoring protocols that usually consist of plaintext printable ASCII to catch remote x86 exploits.
- EXPLOIT x86 setuid 0: An attacker sent the setuid 0 system call for the x86 platform. This signature is the most effective when monitoring protocols that usually consist of plaintext printable ASCII to catch remote x86 exploits.
- EXPLOIT NTPDX buffer overflow: An UDP packet of more than 128 bytes was send to a server running the NTPd (Network Time Protocol). This is an attempt to overflow the buffers.

3.11.6 MISC Large ICMP / UDP Packet

This alert indicates that a large UDP or ICMP has been sent to a host. The normal size of the payload for UDP messages is not more than 10 bytes, for ICMP messages it doesn't exceed 64 to 128 bytes.

There are lots of different destination ports for the "MISC Large UDP Packet" alert. According to the Snort port database these ports are used for:

- 1336: Instant Service Chat
- 2469: MTI-TCS-COMM
- 1593: mainsoft-lm
- 2611: lionhead
- 2805: WTA WSP-S

Because of the large number of alerts for the "MISC Large UDP Packet"message it is also possible that there was an error in the rule itself. More information about this error can be found at http://archives.neohapsis.com/archives/snort/2000-06/0335.html. It is also possible that the threshold for detection of large packets is set to small. The Snort rule that triggered this alert should be checked.

The large ICMP packets can be used by hackers for MTU discovery or a denial of service attack (ping-of-death).

3.11.7 Port 55850 tcp/udp – Possible myserver activity – ref. 010313-1

MyServer is a simplistic DdoS (Distributed Denial of Service) and scanning tool that usually communicates via TCP or UDP to port 55850. A very thorough description about this alert can be found at www-net.cs.umass.edu/~brian/cs515/515-incident.ppt (this is a Powerpoint presentation: the description of myserver starts at slide 23). In Thomas Shepherd’s GCIA paper I found out that myserver activity could result in mail traffic to the attacker’s site (for sending system information back to the attacker).

3.11.8 SUNRPC highport access!

This alert is triggered by successful access to the RPC ports 32771 and higher. The rpcbind and portmapper facilities have numerous vulnerabilities that can allow root access. I checked Arachnids and found the following vulnerabilities:

- IDS241/rpc.ttdbserv-solaris-kill [*TCP any -> 32771:34000*]
- IDS242/rpc.ttdbserv-solaris-overflow [*TCP any -> 32771:34000*]
- IDS26/nfs-showmount [*TCP any -> 32771:*]
- IDS429/portmap-listing-32771 [*TCP any -> 32771*]
- IDS544/rpc_udp_traffic_contains_bin_sh [*UDP any -> 32771:*]
- IDS545/rpc_tcp_traffic_contains_bin_sh [*TCP any -> 32771:*]
- IDS546/rpc.sadmind-overflow [*UDP any -> 32771:34000*]

3.11.9 RPC tcp traffic contains bin_sh

This alert is triggered when someone is trying to open a root shell on a host.

3.12 “Top talkers” List

3.12.1 Top 10 alerts

In Table 11 you can see a list of the top 10 inbound security alerts. No information was found at Dshield.org concerning this top 10 of external attackers. Some facts about Table 11:

- the first 8 IP addresses and the last one trigger only one rule, i.e. “suspicious host traffic”
- 202.102.249.118 triggers 2 different alerts, i.e. “MISC Large UDP Packet and AFS – Off-campus activity

Table 11 : Top 10 Talkers external SRC IP

SRC_IP	Number of DST IP scanned	nslookup
65.120.161.122	239213	Mail.inkfirm.com
65.114.45.134	235549	< not found >
67.68.163.9	134856	Toronto-HSE-ppp3765268.sympatico.ca
80.143.254.161	85729	p508FFEA1.dip.t-dialin.net
66.130.11.113	80831	modemcable113.11-130-66.mtl.mc.videotron.ca
212.23.162.52	54631	alouette.passereaux.jmsp.net
140.142.8.72	12708	media-wm-2.cac.washington.edu
80.13.247.134	8756	ANancy-102-1-4-134.abo.wanadoo.fr

202.102.249.118	5958	< not found >
207.162.20.121	5317	Cab121.UQAT.UQuebec.Ca

The top 10 destination ports can be found in Table 12.

Table 12 : Top 10 destination ports

DST Port	Number of alerts	Port is used for
30200	474618	?
1082	134753	AMT-ESD-PROT
2020	80811	XINUPAGESERVER
137	54191	Netbios
80	35664	HTTP
161	33030	SNMP
69	18280	TFTP
6346	13216	GNUTella
1336	12695	Instant Service Chat
1117	8757	ARDUS MULTICAST TRANSFER

Almost 500.000 alerts were triggered for connections to port 30200. I didn't find any information about this port being used for a Trojan, …, but when I did a query on this port (see Table 13) it revealed some interesting information. There are a huge number of connections from 65.114.45.134 and 65.120.161.122 to 130.85.157.248. In 3.5.1.1 I already warned for this host because it was scanning a lot of external hosts. This host is definitely compromised. The "Bulletin hebdomadaire du CERT Renater" at http://www.up.univ-mrs.fr/wcri/d_serv/d_reseau/d_cert/certmsgSTAT023 tells about a compromised Red Hat box listening for incoming SSH sessions on port 30200. Their host was compromised via the installed Wu-FTPd.

Table 13 : port 30200

SRC IP	DST IP	Number of alerts	DST Port
65.120.161.122	130.85.157.248	239162	30200
65.114.45.134	130.85.157.248	235415	30200
217.128.157.220	130.85.157.248	39	30200
64.4.12.205	130.85.157.248	1	30200
212.23.162.52	130.85.157.248	1	30200

Almost 135.000 alerts were triggered against port 1082 from 67.68.163.9 to 130.85.157.252. A huge amount of connections is made to this destination host to a number of strange destination ports (see Table 14). Ports 2020 and 1117 are other ports in Table 12 which generate a lot of alerts for 130.85.157.252. Without knowing what kind of server this is, this should be further investigated.

Table 14 : Port 1082

SRC IP	DST IP	Number of alerts	DST Port	
67.68.163.9	130.85.157.252	134750	1082	AMT-ESD-PROT
66.130.11.113	130.85.157.252	80797	2020	XINUPAGESERVER
80.13.247.134	130.85.157.252	8755	1117	ARDUS MULTICAST TRANSFER
207.162.20.121	130.85.157.252	5312	3899	-
195.54.102.4	130.85.157.252	3005	2276	-
66.130.204.176	130.85.157.252	25	33354	-
195.54.102.4	130.85.157.252	18	1379	DBREPORTER
193.110.95.1	130.85.157.252	11	1760	WWW-LDAP-GW
65.216.154.252	130.85.157.252	5	2533	SNIFFERSERVER

67.68.163.9
130.85.157.252
4
1472
CSDM

As you can see in large UDP packets are sent from 140.142.8.72 to 130.85.153.157 on port 1336 (Instant Service Chat). This could be a DoS attack, although 130.85.153.157 is no critical server for the University.

Table 15 : Port 1336

SRC IP	DST IP	Number of alerts	DST Port
140.142.8.72	130.85.153.157	12693	1336

In Table 16 you can find the top 10 of internal destinations. This can give a good overview of which internal machines are subject of attacks. As you can see, 130.85.157.248 receives by far the most alerts.

Table 16 : Top 10 internal destinations

DST IP	Number of alerts
130.85.157.248	477777
130.85.157.252	232725
130.85.157.242	92591
130.85.157.243	56815
130.85.11.7	20301
130.85.11.6	17028
130.85.150.195	16049
130.85.153.157	12902
130.85.157.247	10661
130.85.140.9	7247

3.12.2 Top 10 Portscans

Although portscans are not destructive, they can be a forerunner for more evil to come. A distinction was made between scans initiated by external hosts (inbound) and scans initiated by internal hosts (outbound).

In Table 17 you can see that there are 5 out of the top 10 scans initiated by IP addresses in the 205.188.228.0 range. A search on Google revealed that spinner.com is an Internet music service. Above all that 93 % of the portscans initiated by 205.188.228.17 are scans for port 6970 (the other scanned ports are between 6972 and 7082). Ports 6970 to 6999 are used by RTP (Real-time Transport Protocol). The destinations of these portscans are probably just listening to an on-line radio channel (the University has its own internet radio station "WMBC Freeform Radio" at 130.85.179.80). This could be harmless but it is consuming a large amount of bandwidth.

Table 17 : Top 10 Inbound portscans

SRC_IP	Number of DST IP scanned	Dshield.org information			
		Nslookup	Total records against IP	Number of targets	Date range
12.151.57.37	30381	< Not found >	23	15	2002-07-26 to 2002-07-26
212.182.119.141	19705	< Not found >	< none >	< none >	< none >
132.235.75.1	17875	woubenr.rtvc.ohiou.edu	< none >	< none >	< none >
205.188.228.17	17580	mslb2.spinner.com	**540**	**275**	**2002-08-02 to 2002-08-02**

205.188.228.145	11482	mslb7.streamops.aol.com	**304**	**195**	**2002-08-02 to 2002-08-02**
205.188.228.1	10309	mslb1.spinner.com	**583**	**309**	**2002-08-02 to 2002-08-02**
63.215.70.142	9684	unknown.Level3.net	< none >	< none >	< none >
205.188.228.33	9600	mslb3.spinner.com	**505**	**265**	**2002-08-02 to 2002-08-02**
205.188.228.129	8773	mslb6.streamops.aol.com	**568**	**307**	**2002-08-02 to 2002-08-02**
63.210.46.141	3797	wm1.ash.smc.net	4	4	2002-07-04 to 2002-07-04

Table 18 : Top 10 Outbound portscans

SRC_IP	Number of DST IP scanned	Dshield.org information			
		Nslookup	Total records against IP	Number of targets	Date range
130.85.5.89	398054	Ciscoworks.noc.umbc.edu	< none >	< none >	< none >
130.85.60.43	261701	Biggs.umbc.edu	< none >	< none >	< none >
130.85.253.10	37698	Basilisk.umbc.edu	< none >	< none >	< none >
130.85.6.49	27314	Hfs2.afs.umbc.edu	< none >	< none >	< none >
130.85.6.45	19409	Wedge.umbc.edu	< none >	< none >	< none >
130.85.6.52	18923	Hfs5.afs.umbc.edu	< none >	< none >	< none >
130.85.6.50	10033	Hfs3.afs.umbc.edu	< none >	< none >	< none >
130.85.6.48	9486	Hfs1.afs.umbc.edu	< none >	< none >	< none >
130.85.6.60	9466	Hfs7.afs.umbc.edu	< none >	< none >	< none >
130.85.11.7	8433	Dc2.ad.umbc.edu	< none >	< none >	< none >

In Table 19 you can find the top 5 of the most scanned ports.

Table 19 : Top 5 most scanned ports

DST_Port		Number of alerts
161	Snmp	396605
80	http	148122
7001	Afs3-callback	62928
6970	Rtp	58741
53	Dns	49635

3.13 List of external addresses and registration information

3.13.1 Reasons for selection

I selected

- 65.114.45.134, 65.120.161.122 and 217.128.157.220 because they are connecting to the compromised host 130.85.157.248.
- 12.151.57.37 and 212.182.119.141 because they scanned an enormous part of the University's network.

3.13.2 Registration information

65.114.45.134

```
Qwest Communications (NETBLK-NET-QWEST-BLKS-4)
   950 17th St. Suite 1900
   Denver, CO 80202
   US

   Netname: NET-QWEST-BLKS-4
   Netblock: 65.112.0.0 - 65.127.255.255
   Maintainer: QWST
   Coordinator:
      Qwest, NOC  (QN-ARIN)  DIAProdMaint@qwestip.net
      1-703-363-3001 (FAX) 1-703-363-3177

   Domain System inverse mapping provided by:

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

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
   NOTE: For abuse issues, please email abuse@qwest.net.

   Record last updated on 12-Jul-2002.
   Database last updated on  3-Aug-2002 20:00:01 EDT.

----------

SELWAY PARTNERS (NETBLK-Q1105-65-114-45-128)
   52 FOREST AVE 2ND FLOOR
   PARAMUS, NJ 07652
   US

   Netname: Q1105-65-114-45-128
   Netblock: 65.114.45.128 - 65.114.45.159

   Coordinator:
      Paulison, Harry  (HP178-ARIN)  kristeena@comserv1.com
      973-812-3832

   Record last updated on 06-Nov-2001.
   Database last updated on  3-Aug-2002 20:00:01 EDT.
```

65.120.161.122

```
Qwest Communications (NETBLK-NET-QWEST-BLKS-4)
   950 17th St. Suite 1900
   Denver, CO 80202
   US

   Netname: NET-QWEST-BLKS-4
   Netblock: 65.112.0.0 - 65.127.255.255
   Maintainer: QWST

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

   Domain System inverse mapping provided by:

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

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
   NOTE: For abuse issues, please email abuse@qwest.net.

   Record last updated on 12-Jul-2002.
   Database last updated on  3-Aug-2002 20:00:01 EDT.
```

```
----------

CENTRAL DISTRIBUTION INC (NETBLK-Q0115-65-120-161-0)
   2832 ROE LANE
   KANSAS CITY, KS 66103
   US

   Netname: Q0115-65-120-161-0
   Netblock: 65.120.161.0 - 65.120.161.127

   Coordinator:
      Donakey, Coy  (CD733-ARIN)  coy.donakey@centraldistribution.com
      913-677-1666

   Record last updated on 16-Jan-2002.
   Database last updated on  3-Aug-2002 20:00:01 EDT.
```

217.128.157.220

```
inetnum:      217.128.157.0 - 217.128.157.255
netname:      IP2000-ADSL-BAS
descr:        France Telecom IP2000 ADSL BAS
descr:        BSBOR103 Bordeaux Bloc1
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
remarks:      for ANY problem send mail to
gestionip.ft@francetelecom.com
mnt-by:       FT-BRX
changed:      gestionip.ft@francetelecom.com 20010605
changed:      gestionip.ft@francetelecom.com 20020522
source:       RIPE

route:        217.128.0.0/16
descr:        RAIN
descr:        Reseaux d'Acces a l'INternet
remarks:      -------------------------------------------
remarks:      For Hacking, Spamming or Security problems
remarks:      send mail to abuse@wanadoo.fr postmaster@wanadoo.fr
ONLY
remarks:      -------------------------------------------
origin:       AS3215
mnt-by:       FT-BRX
mnt-by:       RAIN-TRANSPAC
changed:      karim@rain.fr 20010611
changed:      karim@rain.fr 20011126
source:       RIPE

role:         Wanadoo Interactive Technical Role
address:      WANADOO INTERACTIVE
address:      48 rue Camille Desmoulins
```

```
address:        92791 ISSY LES MOULINEAUX CEDEX 9
address:        FR
phone:          +33 1 58 88 50 00
e-mail:         abuse@wanadoo.fr
e-mail:         postmaster@wanadoo.fr
admin-c:        FTI-RIPE
tech-c:         TEFS1-RIPE
nic-hdl:        WITR1-RIPE
notify:         gestionip.ft@francetelecom.com
mnt-by:         FT-BRX
changed:        gestionip.ft@francetelecom.com 20010504
changed:        gestionip.ft@francetelecom.com 20010912
changed:        gestionip.ft@francetelecom.com 20011204
source:         RIPE
```

12.151.57.37

```
AT&T ITS (NET-ATT)
   200 Laurel Avenue South
   Middletown, NJ 07748
   US

   Netname: ATT
   Netblock: 12.0.0.0 - 12.255.255.255
   Maintainer: ATTW

   Coordinator:
      Kostick, Deirdre  (DK71-ARIN)  help@IP.ATT.NET
      1-919-319-8249

   Domain System inverse mapping provided by:

   DBRU.BR.NS.ELS-GMS.ATT.NET 199.191.128.106
   DMTU.MT.NS.ELS-GMS.ATT.NET 12.127.16.70
   CBRU.BR.NS.ELS-GMS.ATT.NET 199.191.128.105
   CMTU.MT.NS.ELS-GMS.ATT.NET 12.127.16.69

   For abuse issues contact abuse@att.net

   Record last updated on 06-Nov-2000.
   Database last updated on  3-Aug-2002 20:00:01 EDT.

----------

LIGHT SPEED (NETBLK-A-LIGHT112-56)
   4300 BRIGHTON BOULEVARD
   DENVER, CO 80216
   US

   Netname: A-LIGHT112-56
   Netblock: 12.151.56.0 - 12.151.63.255
   Maintainer: LSPD

   Coordinator:
      McCoy, Jeff  (JM2923-ARIN)  jmccoy@atlightspeed.com
      720-264-2029
   Record last updated on 21-Jun-2002.
   Database last updated on  3-Aug-2002 20:00:01 EDT.
```

212.182.119.141

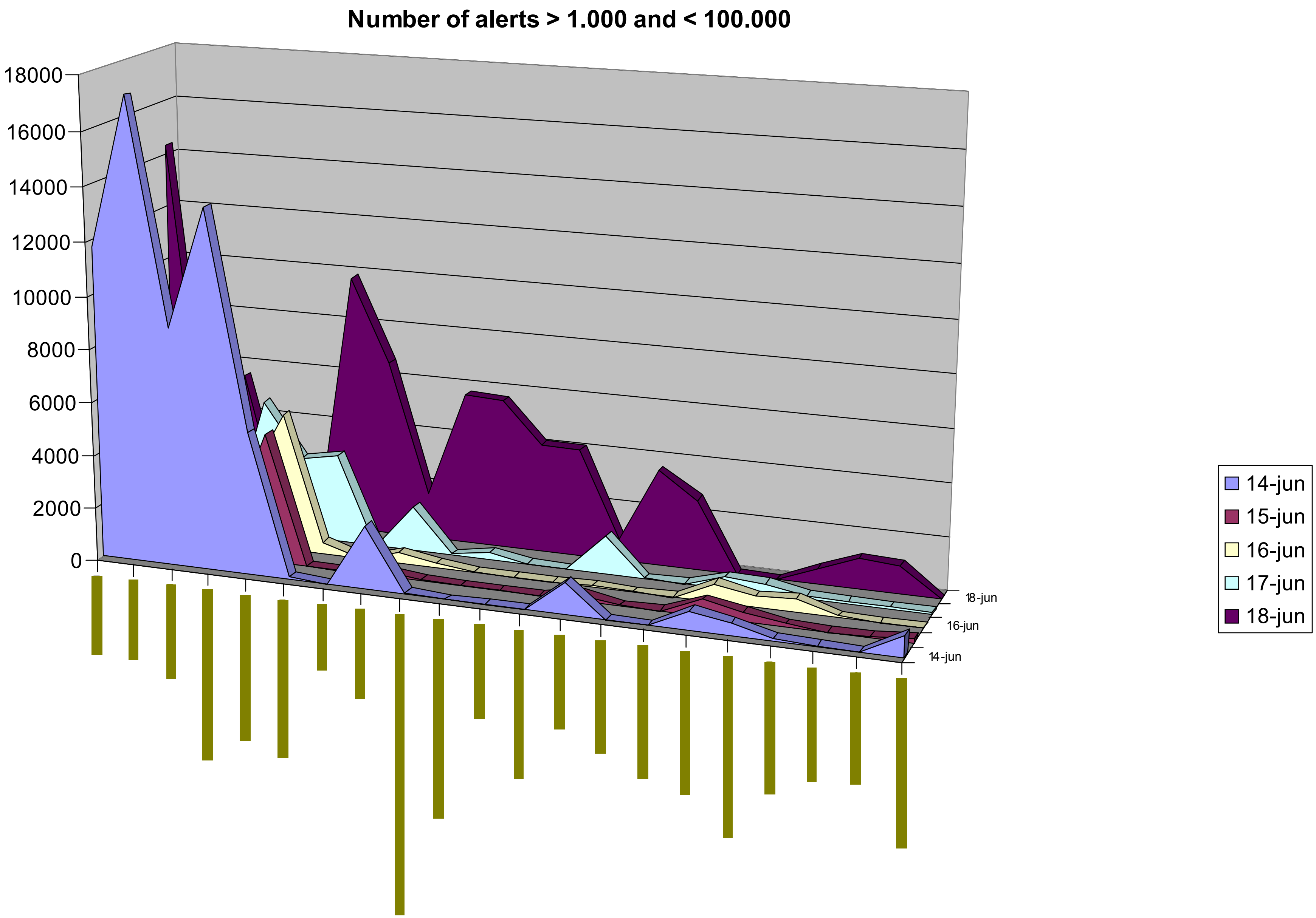
```
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:      212.182.119.136 - 212.182.119.143
netname:      LUB-FIBREX
descr:        Przedsiebiorstwo Wdrozeniowo-Uslugowe "FIBREX" Sp. z
o.o.
descr:        Lublin, Poland
country:      PL
admin-c:      AR1187-RIPE
tech-c:       AR1187-RIPE
tech-c:       AU229-RIPE
status:       ASSIGNED PA
notify:       lir@admins.man.lublin.pl
mnt-by:       PL-LUBMAN-MNT
mnt-lower:    PL-LUBMAN-MNT
changed:      Andrzej.Resztak@admins.man.lublin.pl 20001003
source:       RIPE

route:        212.182.96.0/19
descr:        non-academic part of Lublin MAN, Poland
origin:       AS12346
cross-nfy:    AR1187-RIPE
notify:       lir@admins.man.lublin.pl
mnt-by:       PL-LUBMAN-MNT
changed:      Andrzej.Resztak@admins.man.lublin.pl 19990326
source:       RIPE

person:       Andrzej Resztak
address:      ZIO UMCS
address:      Pl. Marii Curie-Sklodowskiej 1
address:      20-031 Lublin
address:      POLAND
phone:        +48 81 537 6240
phone:        +48 81 537 6192
fax-no:       +48 81 537 6295
e-mail:       Andrzej.Resztak@admins.man.lublin.pl
nic-hdl:      AR1187-RIPE
notify:       Andrzej.Resztak@admins.man.lublin.pl
mnt-by:       PL-LUBMAN-MNT
changed:      resz@helios.man.lublin.pl 19980515
changed:      Andrzej.Resztak@admins.man.lublin.pl 20010718
source:       RIPE

person:       Artur Urbanowicz
address:      ZIO UMCS
```

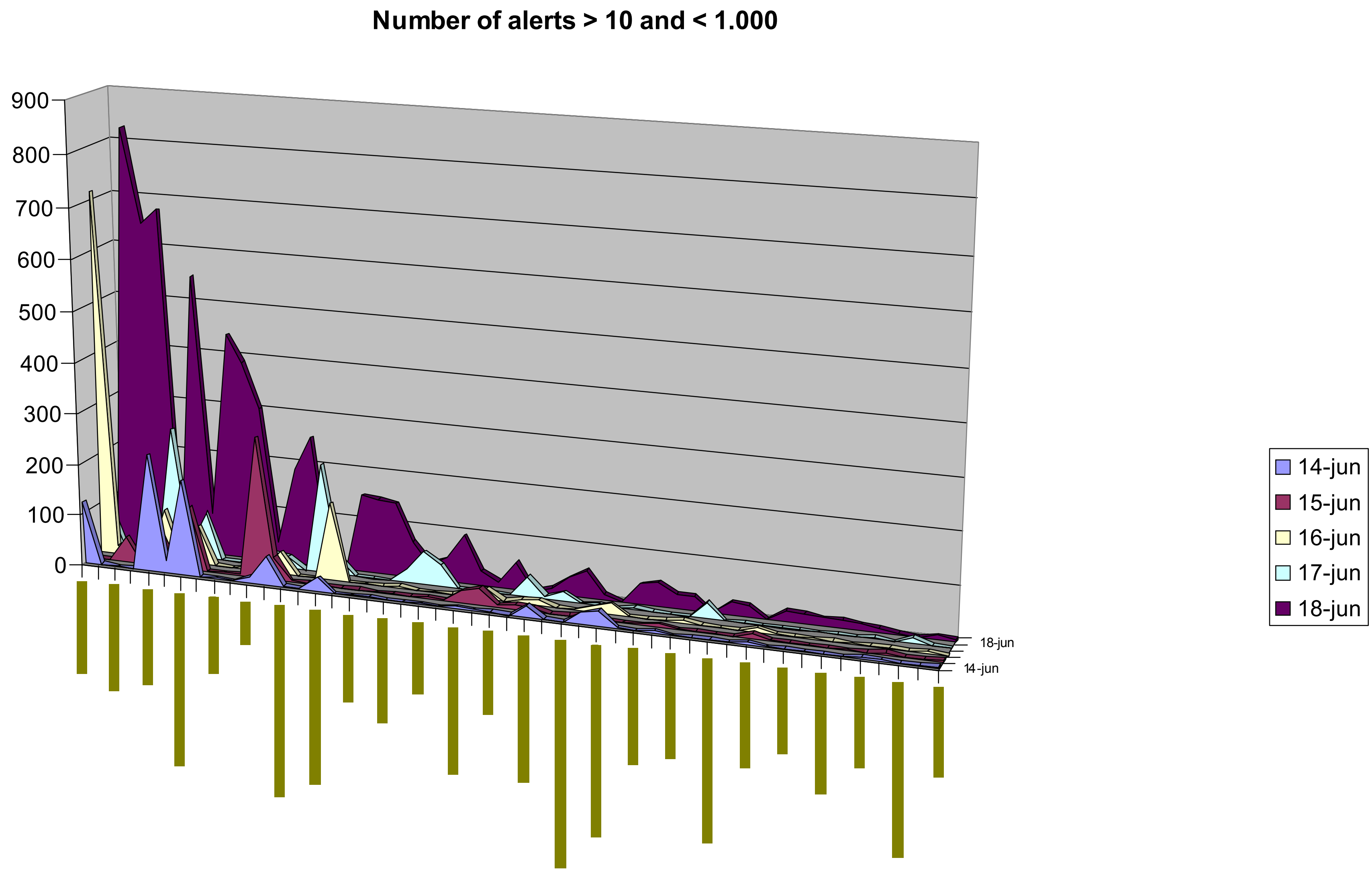
```
address:       Pl. Marii Curie-Sklodowskiej 1
address:       20-031 Lublin
address:       POLAND
phone:         +48 81 537-6209
fax-no:        +48 81 537-6295
e-mail:        lan-admin@umcs.lublin.pl
nic-hdl:       AU229-RIPE
remarks:       e-mail address used for maintaining UMCS network
notify:        lan-admin@umcs.lublin.pl
changed:       artur@golem.umcs.lublin.pl 19990322
source:        RIPE
```

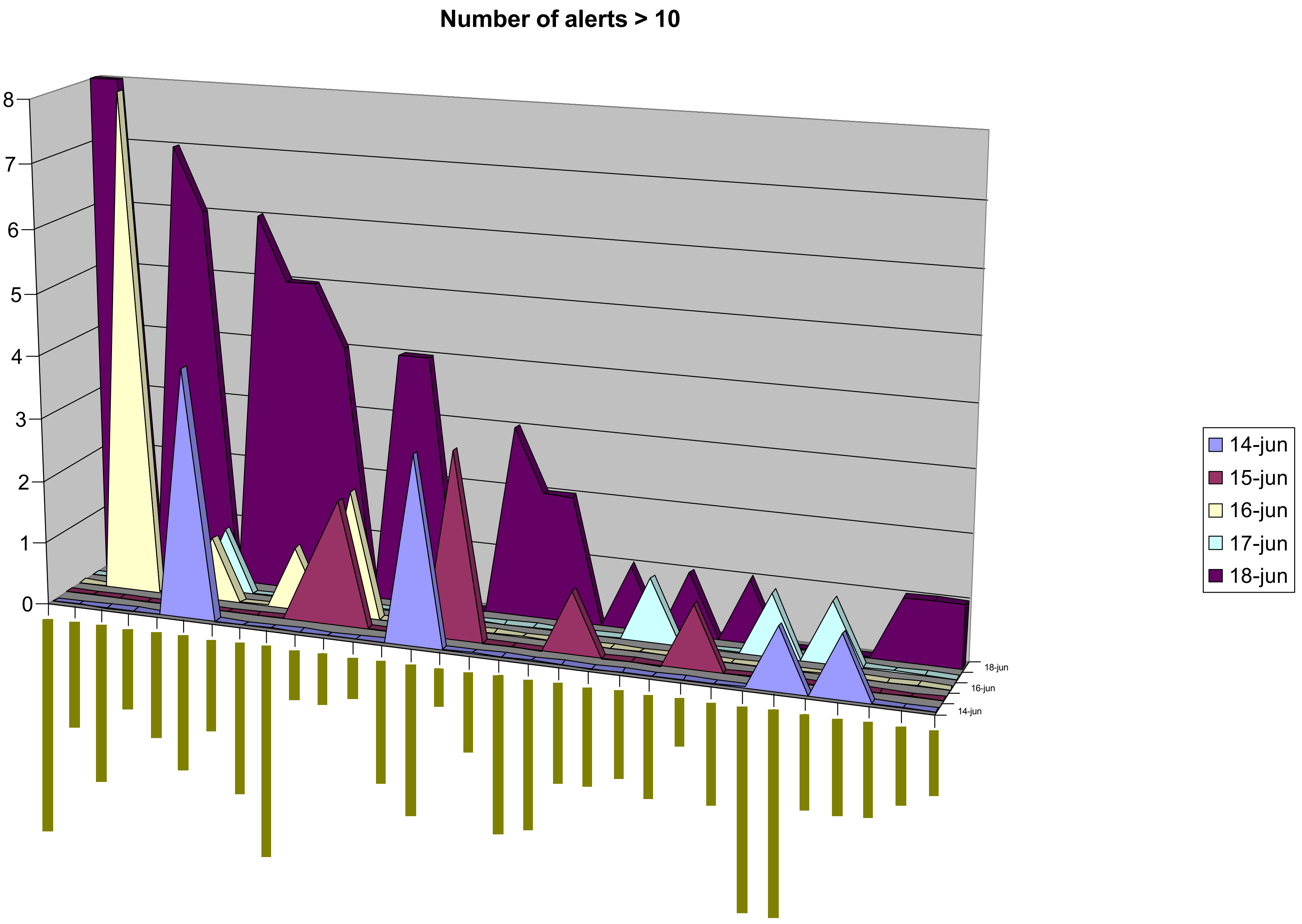
3.14 Link graph and analysis

I wanted to know if there was a difference between the different kinds of alerts the University receives per day so I made a graph of it. To make the graph interpretable I divided it into 3 parts. The first part has all the alerts occurring more than a 1.000 times, the second part has the alerts occurring between 10 and 1.000 times and the final graph has all the alerts occurring less than 10 times.

It is quite strange that there are a lot of new alerts on Tuesday. The line of Tuesday is almost the inverse of the lines of the previous days.


Number of alerts > 1.000 and < 100.000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
18-jun
16-jun
14-jun
14-jun
15-jun
16-jun
17-jun
18-jun


Number of alerts > 10 and < 1.000
900
800
700
600
500
400
300
200
100
0
18-jun
14-jun
14-jun
15-jun
16-jun
17-jun
18-jun

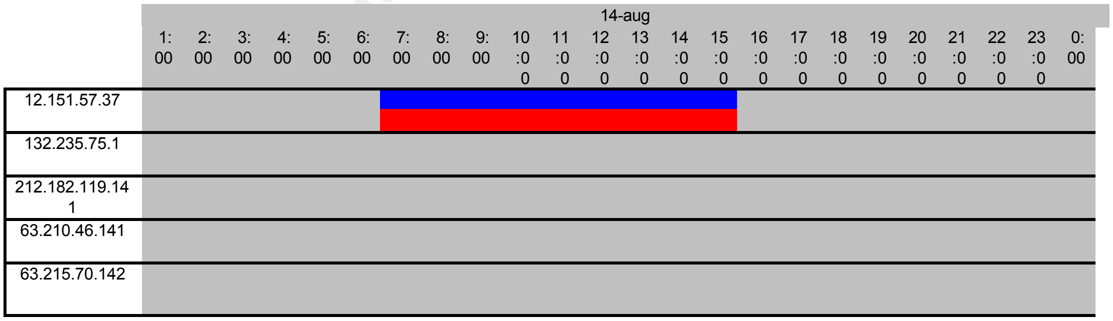

Number of alerts > 10
8
7
6
5
4
3
2
1
0
18-jun
16-jun
14-jun
14-jun
15-jun
16-jun
17-jun
18-jun

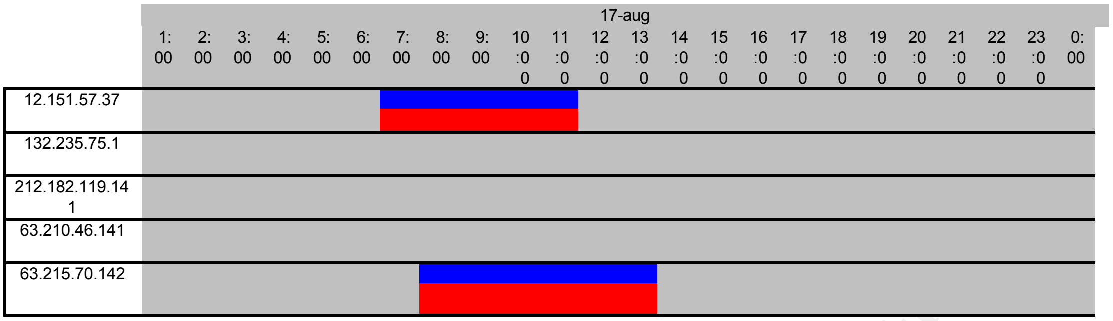
3.15 Insights into internal machines and analysis identifying relationships

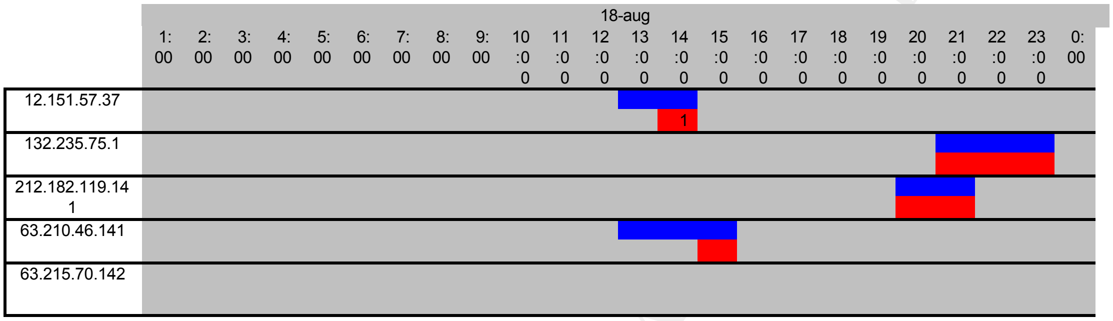
First I checked if the top 10 of the portscanners also generated other alerts.

SRC IP	Nslookup	Number of alerts	Alert
12.151.57.37	< not found >	1179	AFS - Off-campus activity
12.151.57.37		1	Attempted Sun RPC high port access
12.151.57.37		4	EXPLOIT NTPDX buffer overflow
12.151.57.37		199	High port 65535 udp - possible Red Worm - traffic
12.151.57.37		1	TFTP - External UDP connection to internal tftp server
132.235.75.1	woubenr.rtvc.ohiou.edu	1	beetle.ucs
132.235.75.1		5	MISC traceroute
132.235.75.1		28	suspicious host traffic
132.235.75.1		230	WEB-MISC Attempt to execute cmd
212.182.119.141	< not found >	1	beetle.ucs
212.182.119.141		1	CS WEBSERVER - external web traffic
212.182.119.141		1	SMB Name Wildcard
212.182.119.141		39	suspicious host traffic
212.182.119.141		219	WEB-MISC Attempt to execute cmd
63.210.46.141	wm1.ash.smc.net	1	MISC source port 53 to <1024
63.215.70.142	swin13.lax.streamos.com	922	AFS - Off-campus activity
63.215.70.142		91	High port 65535 udp - possible Red Worm - traffic
63.215.70.142		1	TFTP - Internal UDP connection to external tftp server

I found out that there were a few external IP addresses generating multiple alerts. Two of them caught my eye because they had a similar pattern : AFS and TFTP activity and a possible Red worm infection. Then, I placed the portscans and the occurrence of the other alerts in a timeline. It seems that both the scans and the other alerts are triggered at the same time.







Finally I checked if there was traffic 130.85.151.95 and 130.85.88.245 back to the external attackers. There were a few alerts triggered for "fragment reassembly time excession".

Alert	SRC IP	DST IP	Number of alerts
ICMP Fragment Reassembly Time Exceeded	130.85.151.95	63.215.70.142	1
ICMP Fragment Reassembly Time Exceeded	130.85.88.245	12.151.57.37	44

Although this pattern is very interesting I didn't find any information neither on the Internet nor via multiple postings on the incidents.org mailing list. This could be normal traffic but further investigation is certainly required.

130.85.6.49 seems to be infected with multiple worms and Trojans (Back Orifice, Red Worm and Myserver) and should be cleaned or removed from the network. The hosts infected with Red Worm all seem to generate "ICMP echo request L3retriever Ping", "ICMP echo request Nmap or HPING2" and "SMB Name Wildcard" alerts. It is appealing that all these hosts are situated on the 130.85.152.0 segment, which is a segment with Win2K computers (see 3.6.6.1).

3.16 Defensive recommendations

Hundreds of thousands alerts were generated each day of which most of them are just false positives. All these false positives make it almost unfeasible to have a clear view on the real security threats. Hence, my first recommandation is to tune the rulebase of the intrusion detection sensors to reduce the false positives to a strict minimum.

Then I would suggest to replace the hosts that show signs of infection by a Trojan or backdoors like NetMetro, Back Orifice, Myserver, … These hosts have to be cleaned up by formatting the hard disk and rebuilding the host by a back-up or by a very powerfull shareware tool called “The Cleaner” (available at http://www.moosoft.com).

My third recommandation would be to block all the bandwidth consuming activities like Napster, GNUTella, on-line gaming, chatting, … Therefore the IP security policy should be altered. If no security policy exists I suggest that you draft one as soon as possible.

My final recommendation would be for the system administrators to download a copy of nmap and run it against the entire network to see what sort of information the attackers might have gained. This will also help them prioritize their list of patches and fixes to apply.

3.17 Description of the analysis process

I searched for a data analysis tool on the Snort-site where I found Snortsnarf. I installed it on my system and ran it on the first alert-file but it got stuck after half an hour.

Because of this experience with Snortsnarf I decided to write a Perl script (See Script 1) which converts the ASCII-alerts into CSV format. This way I can import all the data in an Access-database. Because all the portscans were included in the scans-files I excluded the spp_portscans out of the data. It is also necessary to run an nl on the logfile before executing this script.

Script 1 : ASCII - CSV converter

```
#!/usr/bin/perl

# Script Philip Ljungberg 18-07-2002
# Try to analyse ASCII Snort DATA
# Script to convert ASCII to CSV for import in Access/Excell

# Variables
$infile="1000alerts";
$outfile="signatures";

# Program

if (defined ($ARGV[1])) {
  $infile = $ARGV[0]; $outfile = $ARGV[1]
  } else { print "Usage: ./convert.pl <inputfile> <outputfile>\n"; exit 0 }

open (ASCII,"<$infile") || die { print "Error opening $infile\n" };
open (CSV,">$outfile") || die { print "Error opening $outfile\n" };
while (<ASCII>) {
  chomp;
  @line=split(/\s?\[\*\*\]\s?/);
  if ($line[0] =~ /\s*(\d+)\s+(.*)/) { $f1 = $1; $f2 = $2 } else { print "Error in
     patternmatching $line[0] $line[1] $line[2]\n" }
  if ($line[2] =~ /(\d+\.\d+\.\d+\.\d+)\:*(\d*)\s\-\>\s(\d+\.\d+\.\d+\.\d+)\:*(\d*)/) {
    $f4 = $1; $f5 = $2; $f6 = $3; $f7 = $4 } else { $f4 = ""; $f5 = ""; $f6 = ""; $f7 = ""
  }
  $f3 = $line[1];
  print CSV "$f1;$f2;$f3;$f4;$f5;$f6;$f7\n";
}
close (ASCII);
close (CSV);
```

Besides this script I used some common Unix-commands like grep, cat, nl, etc.

3.18 References and correlations with other students' practicals

H, So, 16 February 2001, GIAC Intrusion In Depth, On-line available at http://www.giac.org/practical/Hee_So_GCIA.doc.

H. Beast, 17 November 1993, The Israeli Scene, On-line available at http://www.phrack.com/show.php?p=44&a=26.

Arachnids, 26 July 2002, IDS7/SOURCEPORTTRAFFIC-53-TCP, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids7&view=research

J. Braat, 2 November 2000, UDP port 1345 (VPJP ??), On-line available at http://cert.uni-stuttgart.de/archive/incidents/2000/11/msg00022.html.

P. Freeman, 16 November 2000, Re: UDP port 1345 (VPJP ??), On-line available at http://cert.uni-stuttgart.de/archive/incidents/2000/11/msg00136.html.

Symantec, 26 July 2002, How Ghost Multicasting communicates over the network, On-line available at http://service2.symantec.com/SUPPORT/ghost.nsf/docid/1999033015222425.

ISS, 26 July 2002, Port 515 lp, lpr, line printer, On-line available at http://www.iss.net/security_center/advice/Exploits/Ports/515/default.htm.

Arachnids, 26 July 2002, IDS126/X11 OUTGOING XTERM, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids126&view=event.

Martin Roesch, 14 May 2000, Re: [snort] Tiny Fragments, On-line available at http://archives.neohapsis.com/archives/snort/2000-05/0103.html

ISS, 26 July 2002, nt-netbios-nullsession (170), On-line available at http://www.iss.net/security_center/static/170.php.

Whatis.com, 16 August 2001, Simple Network Management Protocol, On-line available at http://searchnetworking.techtarget.com/sDefinition/ 0,,sid7_gci214221,00.html.

Ki.sei.cmu.edu, 27 July 2002, SNMP grabbing, On-line available at http://ki.sei.cmu.edu/idar/drill_attack.cfm?attack=SNMP%20Grabbing.

Arachnids, 26 July 2002, IDS29/SCAN PROBE-QUESO FINGERPRINT ATTEMPT, On-line available at http://www.whitehats.com/IDS/29

Anarchids, 26 July 2002, IDS28/PROBE-NMAP TCP PING, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids28&view=event.

R. Graham, 20 June 2000, FAQ: Firewall Forensics (What am I seeing ?), On-line available at http://www.robertgraham.com/pubs/firewall-seen.html#irc-probes.

Anarchids, 26 July 2002, IDS30/PROBE-XMAS-SCAN, On-line available at http://www.whitehats.com/info/IDS30

Synnergy Networks, 26 July 2002, Examining port scan methods - Analysing Audible Techniques, On-line available at http://www.synnergy.net/downloads/papers/ portscan.txt

Arachnids, 26 July 2002, IDS554/SQUID CACHEMGR.CGI CONNECTION, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids554&view=research.

Arachnids, 26 July 2002, IDS521/SCAN PROBE-SYNSCAN-PORTSCAN-ID-19104, http://www.whitehats.com/info/IDS521

Arachnids, 26 July 2002, IDS27/PROBE-FIN SCAN, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids27&view=research.

Arachnids, 26 July 2002, IDS159/ICMP PING MICROSOFT WINDOWS, On-line available at http://www.whitehats.com/info/IDS159.

Arachnids, 26 July 2002, ID/ICMP PING CYBERKIT 2.2 WINDOWS, On-line available at http://www.whitehats.com/info/IDS154.

Arachnids, 26 July 2002, IDS152/ICMP PING BSDTYPE, On-line available at http://www.whitehats.com/info/IDS152.

W. Walker, 2001, GCIA Practical Assignment v3.0, On-line available at http://www.giac.org/practical/Wade_Walker_GCIA.doc

Arachnids, 26 July 2002, IDS174/ICMP_IRDP_ROUTER_SELECTION, On-line available at http://www.whitehats.com/info/IDS174

Arachnids, 26 July 2002, IDS118/SCAN_TRACEROUTE ICMP, On-line available at http://www.whitehats.com/info/IDS118

Jeff Zahr, 15 november 2001, SANS GIAC Intrusion Detection In Depth Certification (GCIA) ..., On-line available at http://www.giac.org/practical/Jeff_Zahr_GCIA.doc

Bugtraq, 5 October 1999, Hybrid Cablemodem Remote Configuration Vulnerability, On-line available at http://online.securityfocus.com/bid/695/discussion/.

ISS, 3 May 2002, Increased Hacking Activity Associated with Underground File-Sharing Networks, On-line available at http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?id=advise117

J. von Braun, 2 September 2001, What port numbers do well-known trojan horses use?, On-line available at http://www.sans.org/newlook/resources/IDFAQ/oddports.htm.

CERT, 17 January 2002, CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL, On-line available at http://www.cert.org/advisories/CA-2001-19.html.

Geoffron, 13 August 2001, RE: [Snort-users] pif WORM?, On-line available at http://archives.neohapsis.com/archives/snort/2001-08/0543.html

E. Adams, 20 August 2001, RE: [Snort-users] pif WORM?, http://archives.neohapsis.com/archives/snort/2001-08/0835.html

P. Rottz, 20 August 2001, RE: [Snort-users] pif WORM?, http://archives.neohapsis.com/archives/snort/2001-08/0836.html

Arachnids, 26 July 2002, IDS79/Trojen_Trojan-Active-Netmetro, On-line available at http://www.whitehats.com/info/IDS79.

T. Rodriguez, 15 November 2001, Understanding IIS Unicode Vulnerabilities, On-line available at http://www.infosecalliance.com/resources/whitepapers/iis-unicode-vuln.pdf.

R. W. Yuen, 11 October 2001, SANS Parliament Hill 2001, On-line available at http://www.giac.org/practical/Rick_Yuen_GCIA.doc

G. Lajon, 14-18 August 2001, Assignment 1 – Describe the State of Intrusion Detection, On-line available at http://www.giac.org/practical/Gregory_Lajon_GCIA.doc

Arachnids, 26 July 2002, IDS552/WEB-IIS_IIS_ISAPI_OVERFLOW_IDA, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids552&view=event.

CERT, 24 September 1997, CERT® Advisory CA-1996-11 Interpreters in CGI bin Directories, On-line available at http://www.cert.org/advisories/CA-1996-11.html.

Arachnids, 27 July 2002, IDS221/WEB-CGI_HTTP-CGI-FINGER, On-line available at http://www.whitehats.com/info/IDS221.

Arachnids, 27 July 2002, IDS226/WEB-CGI_HTTP-CGI-FORMMAIL, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids226&view=research.

Bugtraq, 3th July 1996, GlimpseHTTP and WebGlimpse Piped Command Vulnerability, On-line available at http://online.securityfocus.com/bid/2026/discussion/.

Bugtraq, 8th May 2000, Allaire ClusterCATS URL Redirect Vulnerability, On-line available at http://online.securityfocus.com/bid/1179.

Bugtraq, 22nd December 2000, Microsoft IIS Front Page Server Extension DoS Vulnerability, On-line available at http://online.securityfocus.com/bid/2144/info/

Bugtraq, 14th January 1999, IIS 4.0 fpcount.exe Buffer Overflow Vulnerability, On-line available at http://online.securityfocus.com/bid/2252/discussion/

M. Kettler, 15 March 2002, Re: [Snort-users] WEB-IIS MISC forbidden, On-line available at http://www.neod.net/lists/snort/0926.html.

Arachnids, 26 July 2002, IDS305/WEB-IIS_HTTP-IIS_TRANSLATE_F, On-line available at http://www.whitehats.com/info/IDS305.

G. Lajon, 14 – 18 August 2001, GIAC Intrusion Detection In Depth, On-line available at http://www.giac.org/practical/Gregory_Lajon_GCIA.doc

Sans Institute, 3 October 2001, Nimda Worm/Virus Report – Final, On-line available at http://www.incidents.org/react/nimda.pdf

Anarchids, 26 July 2002, IDS128/WEB-CGI_HTTP-CGI-PHF, On-line available at http://www.whitehats.com/info/IDS128.

Arachnids, 26 July 2002, IDS298/HTTP-DIRECTORY-TRAVERSAL2, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids298&view=research.

Rain Forest Puppy, 24 December 1999, A look at whisker's anti-IDS tactics, On-line available at www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html

Arachnids, 26 July 2002, IDS244/HTTP-COMPAQ-INSIGHT-DOT-DOT, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids244&view=event

Arachnids, 26 July 2002, IDS487/FTP_DOS-FTPD-GLOBBING, On-line available at http://www.digitaltrust.it/arachnids/IDS487/event.html

Whatis.com, 14 April 2001, Trivial File Transfer Protocol, On-line available at http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci214177,00.html

ISS, 1 October 1989., linux-tftp (308), On-line available at http://www.iss.net/security_center/static/308.php

CERT, 25 September 2001, CERT® Advisory CA-2001-26 Nimda Worm, On-line available at http://www.cert.org/advisories/CA-2001-26.html.

Arachnids, 26 July 2002, IDS339/NETBIOS NETBIOS SMB C$ACCESS? On_line available at http://www.whitehats.com/IDS/339

Mark Gibbs, February 12, 1999, Opinion: Difficult to become a hacker? It's easier than you think - With Symantec's Web client for pcANYWHERE, you can hack away without really trying, On-line available at http://www.cnn.com/TECH/computing/9902/12/hack.idg/

Arachnids, 26 July 2002, IDS266/SMTP-CHAMELEON-OVERFLOW, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids266&view=research.

Arachnids, 26 July 2002, IDS492/NTPDX-BUFFER-OVERFLOW, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids492&view=research.

Arachnids, 26 July 2002, IDS436/SHELLCODE-X86-SETUID0-UDP, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids283&view=research.

Arachnids, 26 July 2002, IDS284/SHELLCODE-X86-SETGID0, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids284&view=research.

Arachnids, 26 July 2002, IDS181/SHELLCODE-X86-NOPS, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids181&view=research.

Arachnids, 26 July 2002, IDS291/SHELLCODE_SHELLCODE-X86-STEALTH-NOP, On-line available at http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids291&view=research.

E. Meier, 30 June 2000, Re: [snort] Large packet alerts, On-line available at http://archives.neohapsis.com/archives/snort/2000-06/0335.html.

J. Treurniet, 22 September 2000, Joanne Treurniet's GIAC CIA Practical Exam, On-line available at http://www.sans.org/y2k/practical/JoanneTreurniet.html.

E.T. Peck, 30 July 2001, Sans Giac, On-line available at http://www.giac.org/practical/Edward_Peck_GCIA.doc.

W.R. Stevens, TCP/IP Illustrated, Volume 1 (Addison-Wesley)

M. Vision, 28 August 2002, Re: Possible Queso Fingerprint attempt?, On-line available at http://archives.neohapsis.com/archives/snort/2001-03/0317.html.

Symantec, 15 April 2002, W32.Cblade.Worm, On-line available at http://securityresponse.symantec.com/avcenter/venc/data/w32.cblade.worm.html.