Global Information Assurance Certification Paper

What's the MS04-011?

GIAC Certified Incident Handler(GCIH)
V3.0

Abstract:
I will demonstrate the ability to gain access to multiple Windows machines on the public network of a major University. The Information Technology Security Group has conducted multiple budget and strategic meetings with helpdesk, networking, and administrative groups on campus to demonstrate the need for an effective and authoritative IT Security implementation. These meetings have met with resistance from various groups for different reasons. I will use this project to demonstrate the impact to the University if IT security is not implemented correctly. This paper will demonstrate the ease of compromising faculty, staff, and student computers at this location.

SLADE GRIFFIN

Statement of Purpose

The goal of my "attack will be twofold. I will gain access to a machine that effectively mimics a great number of the fifteen thousand public IP addresses on our network. I will perform the attack from the "script kiddy" point of view to demonstrate the ease of compromising a large number of systems with limited knowledge and public information. This will demonstrate both the need for strong security policy, and the need for the proper security equipment in the network.

I will acquire SYSTEM level access to a Windows 2000 SP2 machine with an up to date antivirus package running current definitions. I will perform the attack from a fully patched Windows XP machine. Once SYSTEM privileges are obtained, I can then clear the system logs of the attack, and retain my access for the future. Once a single machine is compromised, gaining access to other machines on the same network becomes much easier. Eventually an attacker would stumble across or deliberately target a more sensitive or high availability target.

To gain access to the machine I will exploit the MS04-011 LSASS vulnerability that Microsoft made public in April 2004. The code I have chosen lets you exploit a number of services that run by default on a Microsoft Windows system. The MS04-011 security actually encompasses several vulnerabilities, but we will be focusing on the LSASS buffer overrun. LSASS and buffer overruns will be described in detail later. Exploiting the LSASS vulnerability will give the attacker a command shell with SYSTEM level privileges, which allows software installation, deleting/viewing files, and creating users.

The second, and more important goal, is to demonstrate the need for secure computing policies. As noted in previous University GCIH candidate papers[i], the concept of a free and open network is difficult to overcome. The goal is to maintain freedom and openness while providing a secure environment where grades, medical, financial, and personal data can be exchanged. There are several new technologies available that can provide this type of security. Newer firewalls and Intrusion Prevention devices can inspect the handshake during packet exchange and provide very reliable results. During the course of my attack, I tested an IPS from Tipping Point Technologies™ that effectively thwarted my attack later. This particular device claimed to be able to block an entire exploit, i.e. it has a digital vaccine to drop any traffic destined to exploit the MS03-026 DCOM RPC vulnerability. The advantage to this type of technology is that you do not need a new "signature" for every virus/worm variant. One signature covers all variants. Needles to say I was quite skeptical of the sales representative's claims and wanted to test it out myself.

Introduction

The student network at our University, ResNet, is composed of roughly 6,500 student computers. The dominant operating system among these people is, of course, Windows. I personally feel you can use this operating system in a secure manner and never be a threat to yourself or others if you just take a little time and pay attention. However, since we cannot rely on the studious young folks to maintain up-to-date virus protection and a secure patch level we need to take steps to do it "for them". The Information Technology Security Group, ITSG, was formed on this campus a little over a year ago and we have since been developing Incident response procedures and secure policy. The most recent incident was my inspiration for this proof of concept. A student who had his computer compromised decided to find out how difficult, or not, it was to compromise anyone attached to our main class b IP range. The student was able to check out a laptop from our library, download less than 1Mb worth of exploits, and obtain complete remote access to several machines. In all, this novice computer user compromised 8 machines in less than three hours and would not even qualify as a script kiddy. His knowledge or lack thereof, was astounding when he was interviewed. This novice Windows user was able to obtain a Senior Vice President's SSN, Credit card, date of birth, and travel schedule.

The Exploit

Name

I chose to exploit the Microsoft MS04-011[ii] vulnerability –CAN-2003-0533[iii]. CERT Technical Cyber Security Alert TA04-104A. I started my attack one week after the alert was first published on April 13, 2004. I quickly discovered that sixty to seventy percent of the hosts I found were vulnerable. I did not provide the full exploit code based on advice from my superiors and peers. The choice of code was very scientific; I went to http://www.google.com and searched for "Microsoft LSASS exploit". I had no less than 20 pages of wonderful information, code, to choose from. I picked a very interesting site claiming to have 0-day exploits[iv]. 0-day exploits are the newest most dangerous type as they have just been discovered.

Operating System

I chose the LSASS vulnerability because of the wide range of Microsoft™ operating systems it affects. As of April 21, 2004 this is the current list:
Microsoft Windows NT® Workstation 4.0 Service Pack 6a
Microsoft Windows NT Server 4.0 Service Pack 6a
Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, and Microsoft Windows 2000 Service Pack 4

Microsoft Windows XP and Microsoft Windows XP Service Pack 1
Microsoft Windows XP 64-Bit Edition Service Pack 1
Microsoft Windows XP 64-Bit Edition Version 2003
Microsoft Windows Server™ 2003
Microsoft Windows Server 2003 64-Bit Edition
Microsoft NetMeeting
Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME) – Review the FAQ section of this bulletin for details about these operating systems.

This is an astoundingly comprehensive list of Microsoft products. Let's take a little closer look at what this actually does.

Protocols/Services/Applications

The LSASS vulnerability attacks a service that most Windows machines run when they are booted. The Local Security Authority Service verifies user logons to your computer. The software generates the process that is responsible for authenticating users for the Winlogon service. You can see how dangerous exploiting this service could be. If there were ever a process or service that needed error checking in its program code, the one that says which users belong on your system should be it.

Once I discovered the vulnerability, it was time to perform the buffer overflow and get a command prompt. We will talk about buffers and overflows in the description portion of the paper.

Variants
None yet detected, but give it a week

Description
Oh, this is really interesting. It would appear that when the code for Active Directory® was being written that the long nights took their toll on a few coders. This exploit uses a buffer overrun to gain a command shell. A buffer overrun takes advantage of an unchecked buffer. Once the buffer is overrun, you get your command shell. Let's talk a little about what these two things are and how they work.

A buffer is an area of memory used for storing messages in a program. Buffers tend to have a set size and oftentimes they do not check to see if they are getting full. Why not? I am so glad you asked. To add the size checking to a buffer would require more work. Now, I know all of us have great jobs where we are not under pressure to produce results faster than light travels, but sometimes these programmers are really under the gun. So now after the program is written, there is a buffer between two commands in a program or service your computer uses that does not know when it is starting to get full. Normally this is not a

problem because the program itself would never fill the buffer while it worked. What happens if a bad person finds that buffer though?

Again, thank you for asking. Once a "hacker" finds out there is an unchecked buffer in a program he/she might want to see if they can overflow that buffer. Overflowing a buffer was described to me as having a bucket that will hold 10 tennis balls. To overflow that bucket (buffer) we could dump in say 14,000 tennis balls. 13,990 tennis balls just fell out of that buffer and all over the floor. The floor is the operating system of your computer and maybe, just maybe, some of those tennis balls had very specific commands. One of those commands could be something like this. "Hi, I sure would like to have complete control of this nice operating system you have here." Your computer, having an unchecked buffer and thousands of tennis balls cluttering it up says " Ok."

Signatures of the attack

As of my performing this exploit, we did not have a good signature for identifying this attack. Newer exploits and worms are making it harder to detect with older IDS type systems. Without actively looking at the handshake between the systems and inspecting the packet, a polymorphic work is very difficult to detect. I used an exploit that attacks a very general weakness, but allows the attacker a lot of flexibility on the bad person side. This means you cannot just watch for certain ports across the network. More advanced intrusion prevention devices actually guard against the entire exploit and inspect all layers of the OSI model.

The Platforms/Environments

Victim's Platform

To accurately portray the "typical" student machine on our network, I set up my victim machine with Windows 2000 patched to Service Pack 2. I chose this configuration based on the generic install of the Windows 2000 disk I purchased from the local campus computer store. This patch level is indicative of what our helpdesk technicians find when a student brings a compromised machine in for repair or rebuild. Since the majority of exploits of this type are brought in from the outside, the source and destination networks will be similar. Both networks exist on the same WAN, Wide Area Network, but can be separated logically with our switches and routers. This provides a good platform since an attack coming from the student network is similar to an attack coming form the internet.

Source network

The student network at our University is a fully switched, layer three environment. Layer 3 is the network layer of the OSI model[v]. Each building has a Layer three-uplink switch that is gigabit connected back to our core. Connected to the uplink switches are edge switches that are also layer three capable and are patched directly to the student's rooms. All edge switches are gigabit connected directly

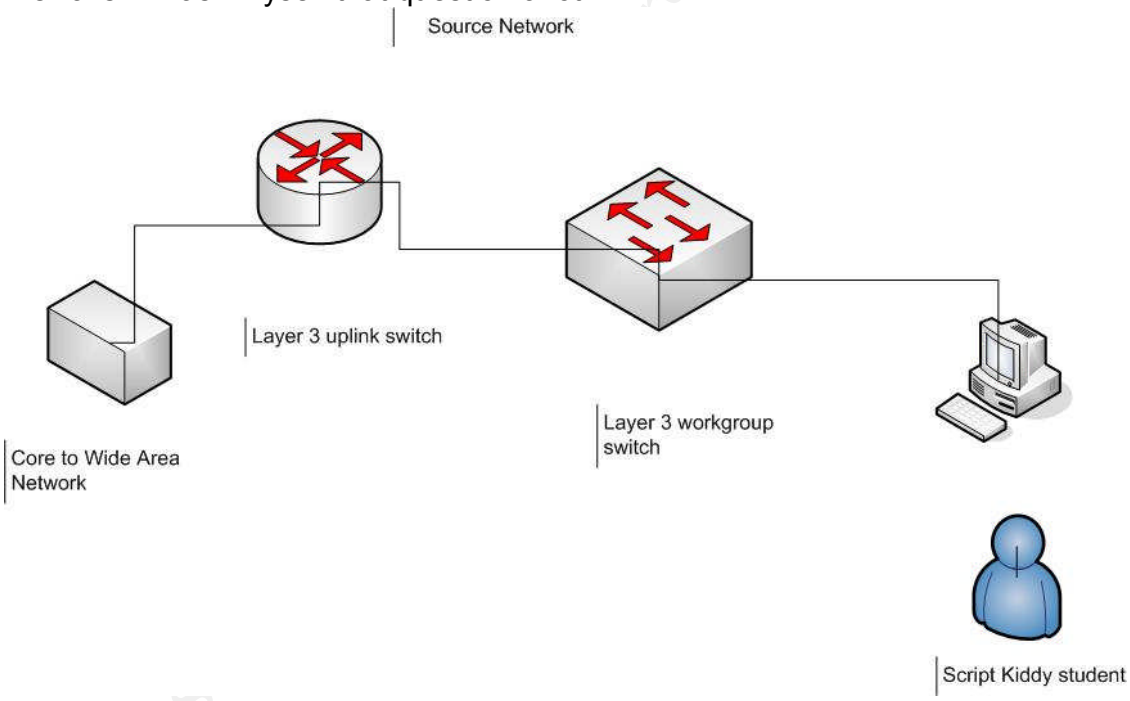
back to the respective building's uplink. This provides the students with a very robust and stable network. The edge switch is capable of layer three switching at the port level. This allows the network engineers an added layer of security and flexibility when determining how to best serve their customers.

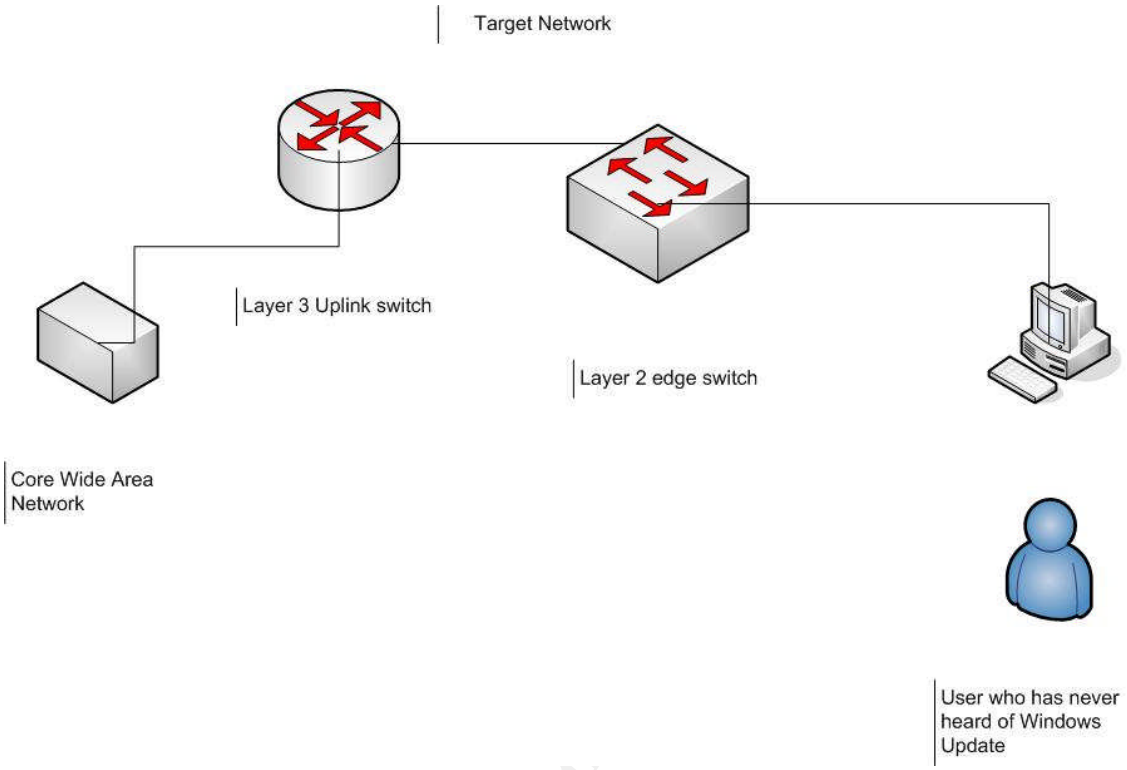
Target network

The target network will represent the older technology that is present in other parts of campus. The buildings have a similar infrastructure to the student's network, but use older equipment. Each building has a layer three uplink that is gigabit connected back to the core, and "edge" switches that are gigabit connected to the uplink. The main difference is that the edge switches outside of the student network are not layer three capable and do not offer as much security or flexibility.

Network Diagram

You may, at some point when looking at the networks, ask, "Where are the firewalls?" I ask myself that question a lot.





Stages of Attack

Reconnaissance

For the first phase of my search, I decided to gain information the old-fashioned way. I used three student workers, and myself, from the University to gain physical access to open computer labs. This physical security audit was used to bypass any existing IDS monitoring and logging capabilities on the targets. With the virus/worm outbreaks of late 2003 and 2004, we have noticed an increase in sysadmin logging and monitoring on remote hosts. While this is something the ITSG has been pushing for it did hamper my ability to perform remote scans and brute force attacks.

Penetrating facilities such as labs or the library on this campus is fairly simple. You are not asked for any identification, and monitoring is done with the use of closed circuit video and a few video cameras that FTP images to a central server. For the closed circuit video, we were able to determine that these tapes are cycled every fourteen days. This information was obtained from the person at the front desk in one of the dorms where there is a student computer lab; I offered no explanation or identification. Armed with the information obtained, I can attempt my break-in and not exploit the machine until after the fourteen-day period.

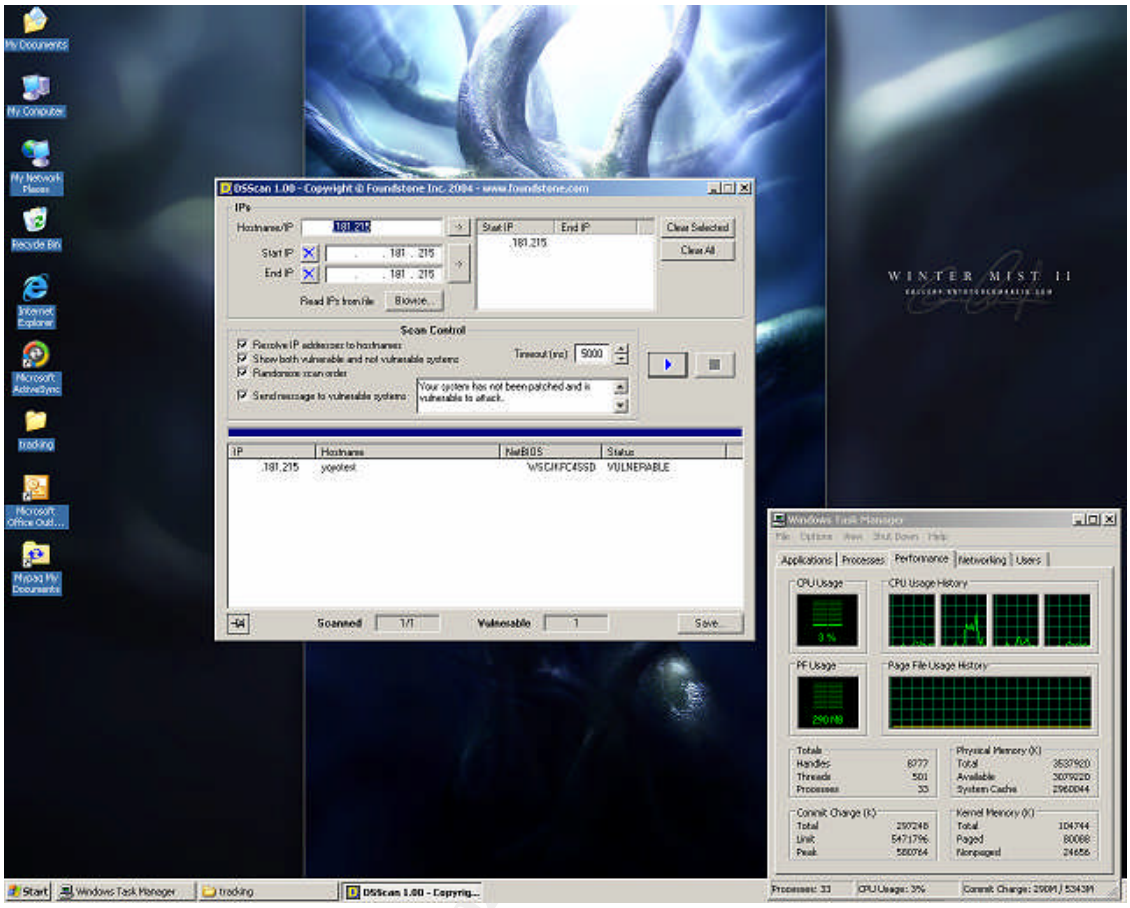
Armed with this knowledge I replicated a small portion of our network in my office. In addition, we have the core portion of the network replicated in an air-gapped network. Details of both networks will be discussed in the Incident-handling portion of the paper.

Scanning

After the physical reconnaissance, limited electronic scouting was also conducted. A brief bit of packet sniffing provided me with enough useful information to begin employing some of the better-known utilities and tools that any attacker might use. To avoid detection by our IDS and other members of the security group I used nmap to identify the correct OS and then RPCscan to determine actual vulnerability.

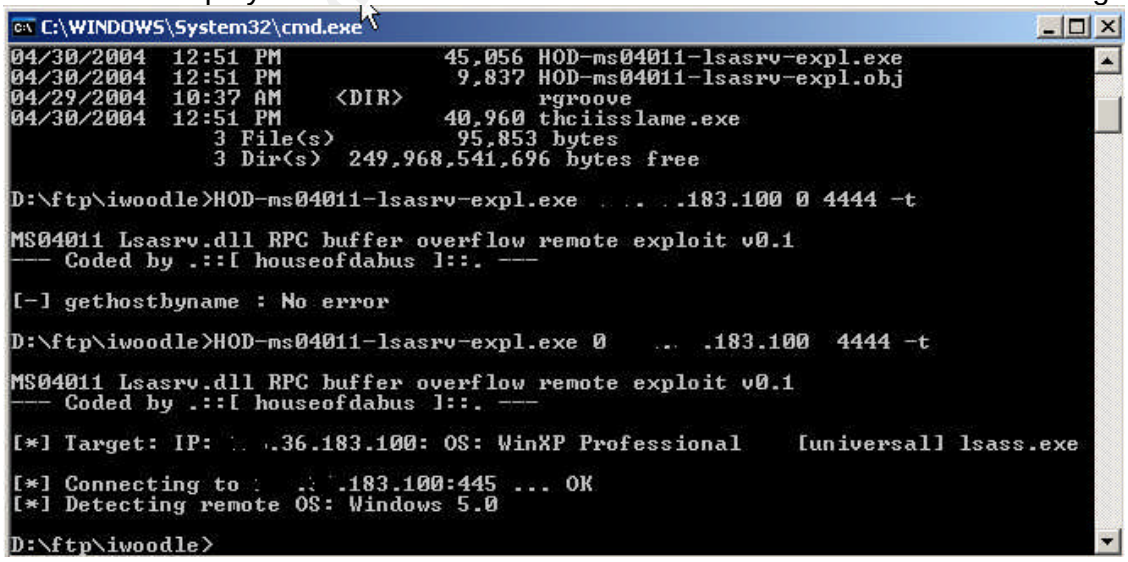
Packet sniffing and penetrating four of our student labs provided me with the class B IP range for the entire university. Visiting all of the dorms gave me the exact range for the dormitory networks, which are very conveniently numbered sequentially. After obtaining the IP range for my "targets", I used nmap for Windows to scan large blocks of IP space. A useful bit of information when conducting electronic reconnaissance on a campus is to remember that most universities provide an anonymous FTP site for downloading. Things typically available for download include the latest Linux ISOs; this will help mask your scan if you bounce through the anonymous FTP. These servers also receive so much traffic that they are ignored in most IDS logs. To fly as low under the radar as possible I used the following command: nmap –sS xxx.xxx.xxx.xxx -P0 -b xxx.xxx.xxx.xxx -T 3. The Nmap scan revealed that the victim had several listening ports. Ports on computers are like the windows on your house. You can look into a window without breaking in, if the window is open, you could reach in and see what you can grab. In some cases, you could go through the window and then walk back out the front door. This attack is similar to crawling in through a window and then walking out the front door. The only difference is that while we are inside we will be removing our "fingerprints" and making our own set of "keys".

Watching the IDS logs, the bounce scan through an open ftp server did keep my Windows machine from displaying any irregular traffic. To fully determine vulnerability I also downloaded DSScan from Foundstone[vi]. This would certainly remove all doubt, though not very stealthy.



Exploiting the System

Ok I have my exploit, and I have my target now I will do the deed. This screenshot displays the command used to determine what host we are attacking.



Very Nice! The exploit tells me the remote host is Windows 5.0, which is Windows 2000. So looking at the C code fro the exploit:

```
Targets:
*       0 [0x01004600]: WinXP Professional    [universal] lsass.exe
*       1 [0x7515123c]: Win2k Professional    [universal] netrap.dll
*       2 [0x751c123c]: Win2k Advanced Server [SP4]       netrap.dll
```

We will now use a 1 instead of the 0. We will also follow the example listed in the code.

Ex.

```
* Example:
*
* C:\HOD-ms04011-lsasrv-expl 0 192.168.1.10 4444 -t
*
* MS04011 Lsasrv.dll RPC buffer overflow remote exploit v0.1
* --- Coded by .::[ houseofdabus ]::. ---
*
* [*] Target: IP: 192.168.1.10: OS: WinXP Professional    [universal] lsass.exe
* [*] Connecting to 192.168.1.10:445 ... OK
* [*] Detecting remote OS: Windows 5.0
*
*
* C:\HOD-ms04011-lsasrv-expl 1 192.168.1.10 4444
*
* MS04011 Lsasrv.dll RPC buffer overflow remote exploit v0.1
* --- Coded by .::[ houseofdabus ]::. ---
*
* [*] Target: IP: 192.168.1.10: OS: Win2k Professional    [universal] netrap.dll
* [*] Connecting to 192.168.1.10:445 ... OK
* [*] Attacking ... OK
*
* C:\nc 192.168.1.10 4444
* Microsoft Windows 2000 [Version 5.00.2195]
* (C) Copyright 1985-2000 Microsoft Corp.
*
* C:\WINNT\system32>
```

Well before we do that let us look at our traffic in a sniffer, a program used to monitor network traffic, and see if we would be detected. Here is the relevant output.

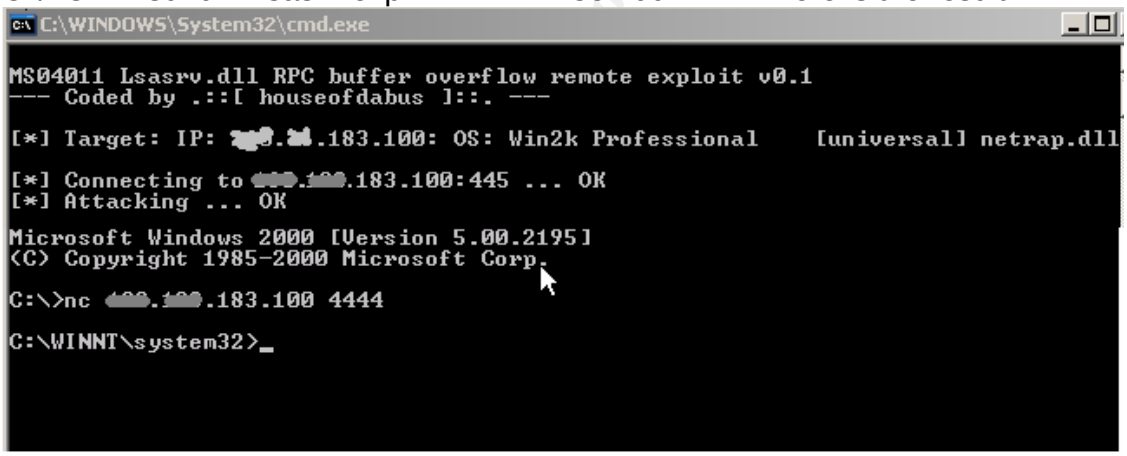
```
TCP      1892 > microsoft-ds [SYN] Seq=0 Ack=0 Win=64240 Len=0 MSS=1460
TCP      microsoft-ds > 1892 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=
TCP      1892 > microsoft-ds [ACK] Seq=1 Ack=1 Win=64240 Len=0
```

This shows us a nice TCP 3-way handshake. TCP stand for Transmission Control Protocol. It is responsible for establishing a connection and exchanging

streams of data. TCP guarantees delivery of data and guarantees that packets will be delivered in the same order in which they were sent. The SYN and ACK flags are exactly what you want to see. They are defined as:
SYN – New connection
ACK- acknowledging data

Now I noticed in the example the following line, C:\nc 192.168.1.10 4444. Apparently you need to be using netcat before you get started. Netcat is a wonderful network tool. The best definition comes straight from the author: Netcat has been dubbed the network swiss army knife. It is a simple UNIX utility, which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities. Netcat is now part of the Red Hat Power Tools collection and comes standard on SuSE Linux, Debian Linux, NetBSD and OpenBSD distributions[vii].

Fortunately I had this program installed, so I ran the exploit as instructed. C:\HOD-ms04011-lsasrv-expl 1 xxx.xxx.183.100 4444. Here is the result



Good news for us and bad news for the victim, we will ask that same command prompt on our machine what our IP address is.

```
C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Cable Disconnected

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : . . .183.100
        Subnet Mask . . . . . . . . . . . : 255.255.252.0
        Default Gateway . . . . . . . . . :    .180.1

C:\WINNT\system32>
```

We are in, we have a command shell we can do what we want. It feels god, but we are not done yet. Let us keep access and hide our tracks.

Keeping Access

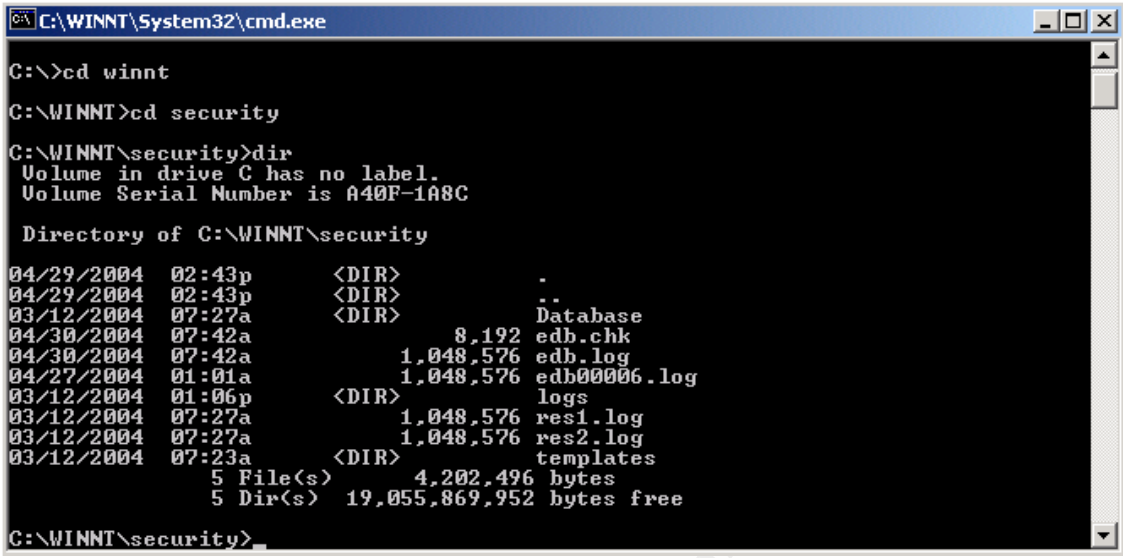
I like to keep things very simple, I think half of the hackers are caught because they try to be too fancy. Let us create our own user account from the command line. We will add a user called techsupport, this is a bit diabolical but if the user were to ever look at what users are allowed on their system techsupport should not raise any concern.

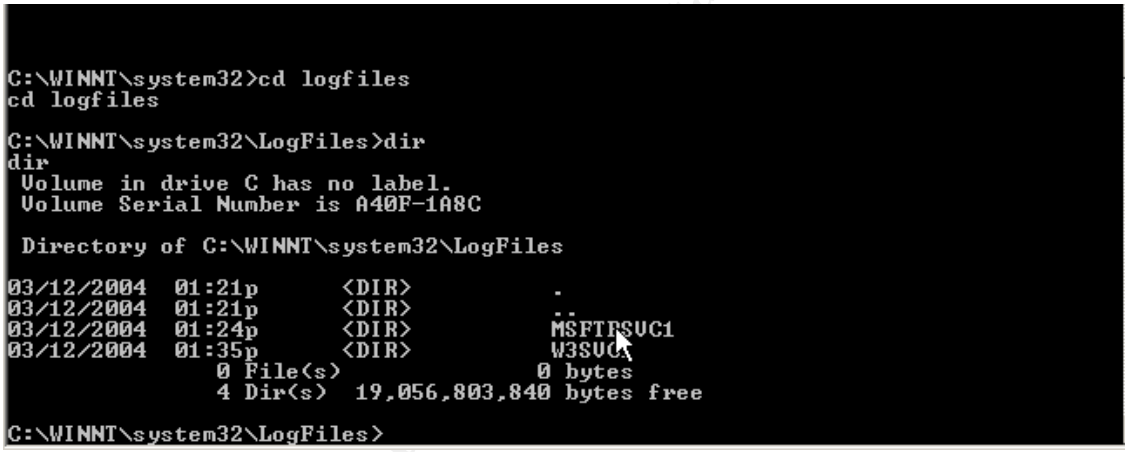
```
C:\WINNT\system32>NET USER techsupport * /add
NET USER techsupport * /add
Type a password for the user: Retype the password to confirm: The command comple
ted successfully.


C:\WINNT\system32>
```

Now they can patch and update the system and if they do not delete our user we can still get in.

Covering Tracks

Most users are not auditing logons by default but just to make sure there is no record we will check. On a Windows 2000 system these logs are kept in c:\winnt\system32\logfiles and c:\winnt\security. Let us look at what is in there.





What you can see is that the ftp service and the IIS, uck, server are logging but sadly user logons are being somewhat ignored. Now simply delete or edit it the logs in c:\winnt\security every time we access the system. We will talk about system logs in the Lessons Learned portion of the paper.

I will now wait fourteen days or more to “harvest”, or begin using, this compromised system.

The Incident handling Process

Preparation

Being prepared for an incident before it happens can save valuable time and even make the difference in obtaining the information needed to close or further pursue your case. Immediately following SANS New Orleans we formulated and Incident Response Procedure. Another invaluable tip I learned was to have a "jumpbag" prepared. It took two sizeable incidents on campus to convince people of the need for the bag but it soon demonstrated its worth.

An incident response procedure, if prepared correctly, can save you time and effort in all phases of an incident investigation. The goals of our IRP are to:

- Confirm or dispel whether an incident or abuse has occurred
- Promote the accumulation of accurate information
- Establish controls for proper retrieval and handling of evidence
- Protect privacy rights established by law and policy
- Minimize disruptions to business functions and network operations
- Allow for legal or civil recriminations against perpetrators
- Provide accurate reports and useful recommendations

Since the IRP is made available to the public, and management, we included the following definitions.

Event - An occurrence that has not been verified as an Incident

Incident - An irregular or adverse event that occurs on any part of the network. Specifically, incidents are computer intrusions, denial-of-service attacks, insider theft of information, copyright violations, and any unauthorized or unlawful activity that requires support personnel, system administrators, or computer crime investigators to respond.

ITP – The University Information Technology Policy (ITP) implements the general principles established by Fiscal Policy 135 regarding the appropriate use of equipment, software, and networks.

ITSG – The Information Technology Security Group (ITSG) is responsible for coordinating computer security efforts within the University.

SA/DCSC - System Administrators (SA) & Departmental Computer Security Contacts (DCSC) are University employees responsible for Information Systems security within a department or group. In general, the SA/DCSC is responsible for the following:

- the dissemination of University computer/information/network security

policies and guidelines to departmental faculty and staff

- the implementation of a security program specific to the designated academic department or research organization to meet the mandates and requirements of research grants and funding
- provide computer/information/network security training and assistance to department/organization members
- serve as a point of contact and liaison to the OIT security organization and other academic departments and organizations on security issues
- serve as a liaison to the University auditing department on software license compliance and other issues

Standard Operating Procedure – The Standard Operating Procedure (SOP) for Responding to ITP Abuse and Computer Security Incidents implements the general principles established by The University– Incident Response Procedure (IRP) regarding the specific procedure by which the Information Technology Security Group (ITSG) must follow when responding to an abuse or incident

Defining responsibilities during an event or incident is also helpful. There are several resources to draw from when an incident occurs and we wanted everyone to be aware of his or her responsibilities. Computer users are very effective in discovering incidents that occur. Users are responsible for monitoring unusual system behavior, which may indicate a security incident.

Users are responsible for reporting incidents to their local System Administrator (SA) or Departmental Computer Security Contact (DCSC) immediately. When the SA/DCSC is unavailable, the user should contact the Information Technology Security Group (ITSG). The user shall not reboot, disconnect, or otherwise alter the system when an event has been discovered, unless directed otherwise by a SA, DCSC, or a member of the ITSG. Otherwise, collection of valid evidence is impacted. A SA/DCSC is the first level of interaction for users experiencing security incidents. It is the SA/DCSC's responsibility to coordinate incoming information, advise users on handling security incidents, forward information to the ITSG, and disseminate information to users and other SA/DCSCs as appropriate. The SA/DCSC shall not reboot, disconnect, or otherwise alter the system when an event has been discovered, unless directed by a member of the ITSG. Otherwise, collection of valid evidence is impacted. The DCSC is responsible for monitoring the systems within their department to identify unusual behavior, which may indicate a security incident. The Information Technology Security Group (ITSG) is responsible for coordinating computer security efforts within the University. In addition, the ITSG is responsible for actively monitoring key IDS systems, assisting in vulnerability assessments, and performing forensic investigations. When necessary, the ITSG will mobilize a Computer Incident Response Team (CIRT) to review the incident and respond according to the Standard Operating Procedure. The ITSG will coordinate the response with DCSCs, security personnel, and other agencies as necessary (including but not limited to Campus Police, Student Judicial

Affairs, and the Federal Bureau of Investigation). The ITSG is also responsible for notifying the ORIT Director of Infrastructure to obtain additional direction as necessary.

The purpose of this section is to describe the roles and responsibilities that each member of the Information Technology Security Group (ITSG) has in responding to reported abuse and security incidents. It is important, therefore, that all security support personnel understand their role in relationship to this procedure.

ITSG Incident Coordinator – responsible for the gathering of all necessary information and assignment of abuse/security incident tickets to the other members of the ITSG; responsible for contacting Faculty/Staff/Students when dealing with Copyright and Commercial Use tickets; responsible for working with the ITSG Team Leader on preparing security related reports; and other assigned security related tasks assigned by the ITSG Team Leader.

ITSG Network Services Group Liaison – responsible for the enabling/disabling of network access according to procedure developed by the University – Network Services Group; responsible for establishing and maintaining open channels of communication between the ITSG and Network Services; responsible for assisting the ITSG Security Analyst's in the installation, maintenance, and management of Intrusion Detection Systems, Firewalls, and other security related infrastructure; responsible for assisting in proactive/reactive network port mapping and other security tasks assigned by the ITSG Team Leader.

ITSG Security Analyst – responsible for the installation, maintenance, and management of Intrusion Detection Systems, Firewalls, and other security related infrastructure; responsible for performing investigations and forensic analysis of critical/high profile systems; responsible for the proactive monitoring of IDS systems and firewall logs to identify network/host intrusion attempts; responsible for performing vulnerability assessments of University Systems; responsible for any other security tasks assigned by the ITSG Team Leader

ITSG Team Leader – responsible for coordination the ITSG to effectively and efficiently implement the University's Security related initiatives; responsible for interfacing with the various departments and organizational groups within the University to further security initiatives; responsible for providing timely reports to upper management on all security related events; responsible for any other tasks assigned by the Vice President of ORIT and/or his/her designates.

To maintain communications during an incident every member has a cell phone and a laminated contact list that includes several phone numbers for each team member. Other items that have been purchased but not added to the bag are USB cables, eight port hub, notebooks, and plastic baggies.

Identification

The purpose of this section is to outline the methods utilized to detect events.

Events can be detected through a variety of technical and procedural mechanisms. Technical mechanisms include intrusion detection systems (IDS) and firewalls that produce alerts when suspicious network activity occurs. Procedural mechanisms include system log reviews, observations of abnormal resource utilization and suspicious account activity. Additionally, sources external to the University may detect issues by recognizing unauthorized activity or abnormal behavior on their systems.

Typical and initial indications of security incidents include any or all of the following:

1) A system alarm or similar indication from an intrusion detection tool

2) Suspicious entries in system or network accounting (e.g., a UNIX user obtains privileged access without using authorized methods)

3) Accounting discrepancies (e.g., someone notices an 18-minute gap in the accounting log in which there is no correlation)

4) Unsuccessful logon attempts

5) New user accounts of unknown origin

6) New files of unknown origin and function

7) Unexplained changes or attempt to change file sizes, check sums, date/time stamps, especially those related to system binaries or configuration files

8) Unexplained addition, deletion, or modification of data

9) Denial of service activity or inability of one or more users to login to an account; including admin/root logins to the console

10) System crashes

11) Poor system performance

12) Unauthorized operation of a program or the addition of a sniffer application to capture network traffic or usernames/passwords

13) Port Scanning (use of exploit and vulnerability scanners, remote requests for information about systems and/or users, or social engineering attempts)

14) Unusual usage times (statistically, more security incidents occur during non-working hours than any other time)

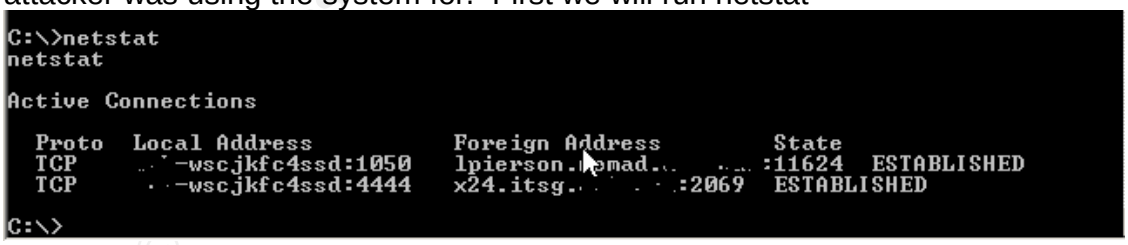
15) An indicated last time of usage of a account that does not correspond to the actual last time of usage for that account

16) Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program)

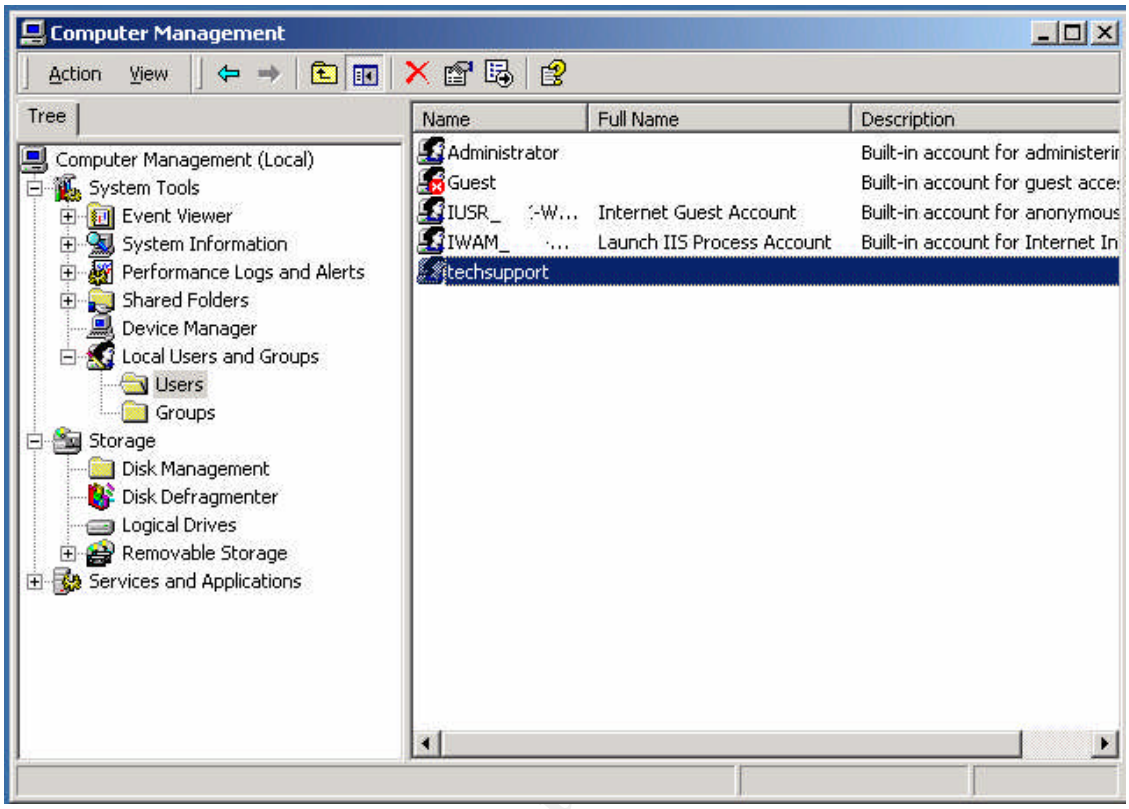
Although observing one of these symptoms is generally inconclusive, observing one or more of these symptoms is motivation for further scrutiny. Immediately informing the appropriate personnel of an event is of extreme importance. Perpetrators of computer crime are proficient at quickly destroying evidence of illegal activity. Unless evidence collection and network monitoring is immediately initiated, critical information may be destroyed before investigators have a chance to review it. Furthermore, The University also has the responsibility to inform affected individuals/organizations in a timely fashion.

In general, all users should report events to their respective SA or DCSC. The SA/DCSC will then gather the necessary information to generate a Security Event Form.

This particular exploit would have most likely been noticed by sluggish system performance, or loss of system resources. In addition to that if we can encourage our end users to maintain their anti-virus and patch levels we have a better chance of identifying the incident post compromise. Now that we are here let us see if the system is compromised. . To obtain the evidence and verify a compromise I would run netstat and view the running processes to see what the attacker was using the system for. First we will run netstat

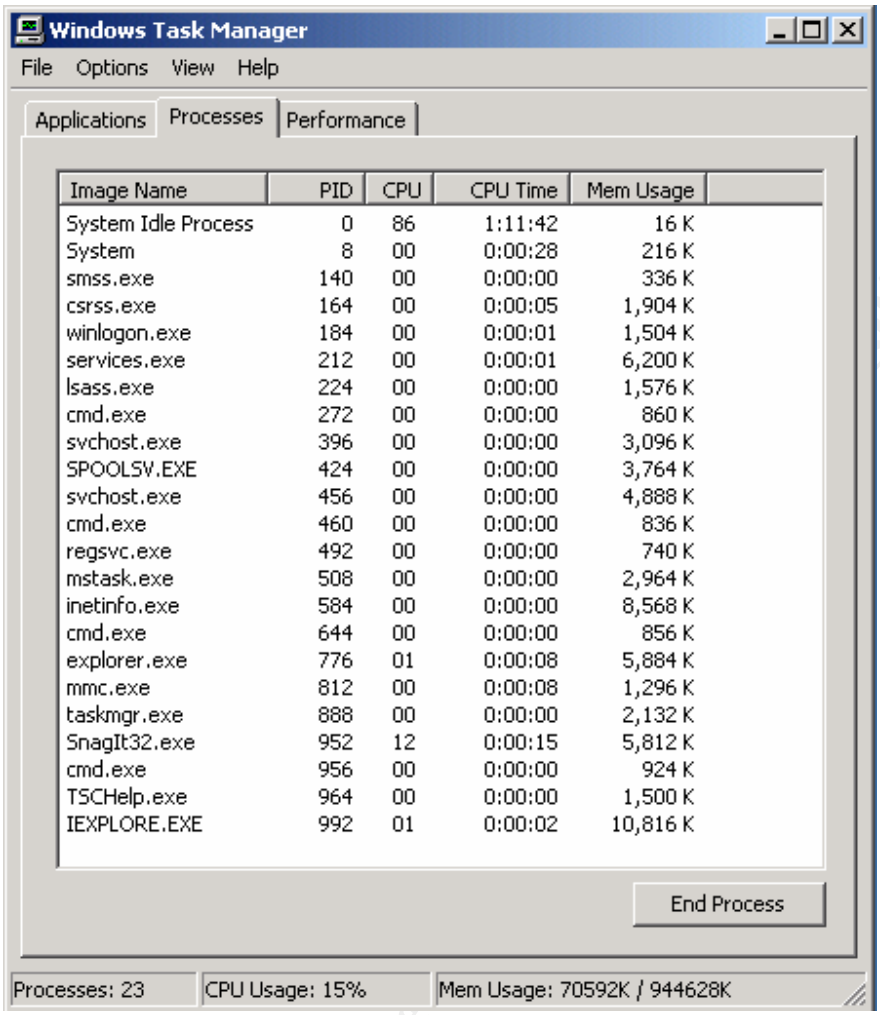


Where we notice two established connections. Netstat displays the status of network connections to the system. Seeing this is not a guarantee of a compromise. Let us see what user accounts are on the system.



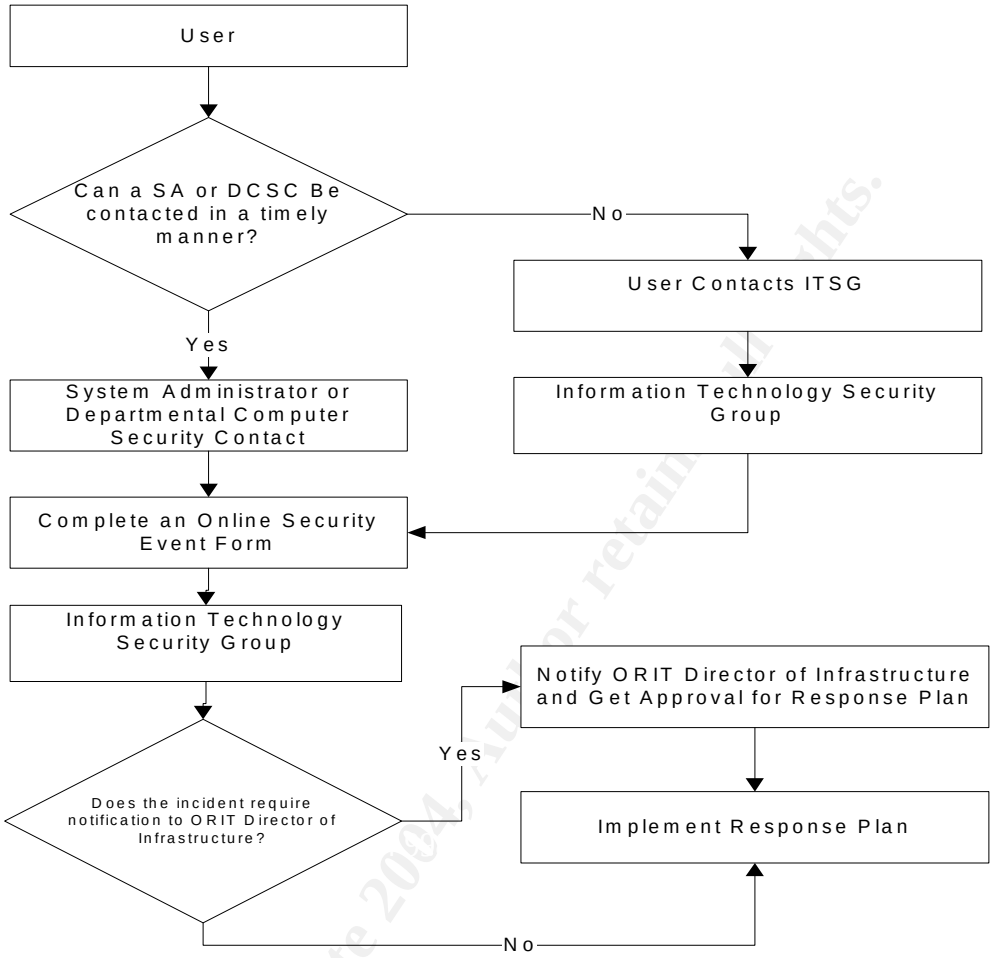
This university does not install a techsupport, or any other, account on remote machines. This is a terrible sign for the victim machine, we now need to view what processes are running, and look at the file system.

Processes are programs that are currently running on your computer. To view what is running we will hit ctrl-alt-delete and select the task manager.



Nothing suspicious here, in fact rather boring. I would say the system is compromised but not harvested for the hacker to upload his movie and game server. To be sure I would search the hard drive for files larger than 10Mb.

The following diagram outlines the notification procedure for our campus:



Containment

Containing an outbreak at the university is often difficult as we still ask users to bring us their machines for repair or rebuild. We have established general guidelines for when something can be disconnected from the network. During the Initial Response and at any time throughout the remainder of the procedure, a decision may be made to disconnect a host from the network. When the decision is made to disconnect a system from the University Network, the following procedure must be followed.

There are two guidelines for disconnecting a port from the university network. Prior to any action taken, all incidents must be reported to the ITSG. All disconnects of network service shall be performed by Network Services personnel only. The Information Technology Security Group reserves the right, in extreme cases, to initiate an immediate disconnect of any service connection.

1. Four-Hour Response - An attempt to contact the user or administrator is required, but the port can be disconnected if contact is not made within four working hours. Examples are:
   A. Stolen IP address
   B. Denial of service attack
   C. Copyright issues
   D. Someone on the campus scanning ports
   E. Second offense of the same type incident within four hours

2. Twenty-Four Hour Response - An attempt to contact the user or administrator is required, but the port can be disconnected if contact is not made within twenty-four hours. If, after investigation, the incident is determined to fit into the Four-Hour Response category, the rules of disconnect defined by the Four-Hour Response apply. Examples are:
   A. Bandwidth over subscription
   B. Virus infections
   C. Attacks against an outside source
   D. Attack on a mission critical system that requires special circumstances for a disconnection

This particular exploit, if it was even noticed, could fall under either category depending on what the attacker does once the command shell was obtained. Typically, we notice they begin scanning for other vulnerable hosts on the same network. In that case we would apply the four hour disconnect if no contact was established with the victim.

If all procedures were followed, and a live compromised system is obtained, we could find information and evidence on the victim's machine

A properly prepared jumpbag is absolutely worth its weight in gold when you are responding to an incident. Having the tools you need at your fingertips helps

reduce response time and lets you focus on what you have to do rather than looking for equipment, utilities and other items. I modeled the jumpbag at the University after the items mentioned in class. This is the current inventory:

Blank CDs	Helix (current version)
120 GB IDE Hard Drive	Static binaries (ls, dir, strings)
73 GB SCSI Hard Drive	Autopsy
Crossover Cable	The Coroner's Toolkit
Straight Through Cable	Encase™
Blank 1.44 MB Floppy Disks	Flashlight

Every member of the IT Security Group also carries a 512 MB USB thumb drive for immediate evidence collection. The contents of the jumpbag are housed is a hard sided Pullman style piece of luggage that could also accommodate clothing. Each member of the team is also responsible for maintaining their laptop as a "jumpbox" as prescribed in track 8 of the SANS curriculum. The laptops are configured with either Fedora or Red Hat™ Linux with the SANS forensics install. Unlike the SANS install we dual boot instead of using VMWare with the second operating system being Windows XP Professional™.

Because this machine was not yet harvested by the attacker we will remove it from the network and apply a hardening procedure so that the next exploit does not get to it immediately. The worst thing about this exploit is the fact that there are at least 5,000 other machines with public IP addresses vulnerable by the time I find the first one

Eradication

Removing this exploit from the system is as simple as removing the user account that I created while in the system.

Recovery

Relatively simple incidents (such as attempted but unsuccessful intrusions into systems), require only assurance that the incident did not in any way affect system software or data stored on the system. Complex incidents, such as malicious code planted by insiders, may require a complete restore operation from clean backups. It is also essential to verify that the restore operation was successful and that the system is back to its normal condition.

The importance of documenting every step taken in recovery cannot be overstated. Recovering from a system compromise can be a hectic and time-consuming process and hasty decisions are often made. Documenting the steps

taken in recovery will help prevent hasty decisions and give a record of all the steps taken to recover. This information can be referenced in the future.

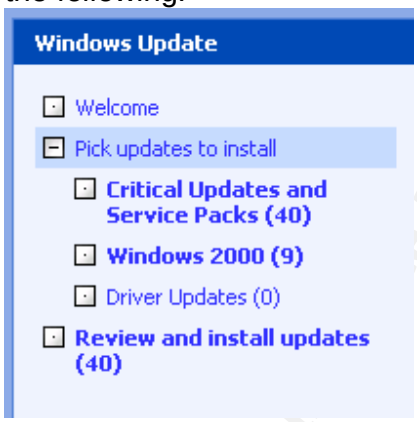
Documenting the steps taken in recovery also may be useful if there is an investigation.

Further recovery of this system will involve applying items from the Lesson Learned portion of the paper.

Lessons Learned

The past eight month shave inspired the ITSG to develop policy to protect our network and our users from exploits like this one. We have developed hardening guides and are working on secure computing policies that will hold users to a higher standard in the future. Excerpts from our Windows 2000 Hardening guide are provided in the extras section.

This incident happened because a user or sysadmin did not run know to run Windows Update regularly. It is extremely important to keep any operating system up to date. When Windows Update was run on this victim machine I got the following:



That sight can cause death in your average sysadmin or, better yet, cause them to transfer that death to the end user.

I also feel that incident like DCOM-RPC, and this one will help our University and others to begin enforcing stricter policies and maybe even patch management solutions. The amount of time and money that can be saved by implementing those two initiatives would definitely pay for the technology needed to implement them.

Finally having your system log events, preferably to a remote server, is a valuable asset when conducting forensics on a compromised machine. Had this machine been properly auditing system events and account activity there would

be more evidence. Detailed instruction on how to enable logging, and other security features is covered in the extras section. These guides and policies were written immediately upon completion of SANS New Orleans track 4 and have been invaluable.

Extras

Hardening Policy excerpts

Step 1 - Hardening the Operating Systems and Application Code

The first thing you need to do is make sure that the Operating System and Applications are up-to-date with service packs and hotfixes.

Microsoft periodically distributes large updates to its operating systems in the form of Service Packs. Service Packs include all the major and minor fixes up to the date of the service pack, and are extensively tested by Microsoft prior to release. Service Packs should be used in a test environment before being pushed into production due to the possibility of undetected bugs. If a test system is not available, wait a week or two after the release of a Service Pack, and pay attention to the Microsoft web site for potential bug reports.

Microsoft also distributes intermediate updates to their operating systems in the form of a Hotfix. These updates are usually small and address a single problem. Hotfixes can be released within hours of discovering a particular bug or vulnerability. Since they are normally released so quickly, they should be used with caution. Each Hotfix includes a description of the issue it resolves. These should be weighed to determine if the risk of installing the Hotfix is worth the risk of not installing it.

It is important to be aware that Service Packs and Hotfixes are not just applicable to operating systems. Individual applications have their own Service Pack and Hotfix requirements. The total security of the system requires attention to both Operating System and application levels.

The process of discovering which Service Pack and hotfixes are needed has been automated since the release of Windows 2000. The following steps outline the automated process of discovering and installing Service Packs and hotfixes to a Windows 2000 system.

1. Open Internet Explorer, Go to Tools-> Windows Update
2. Click on Scan for updates
3. Click on Review and install updates

During this process, if you are asked if you trust Microsoft, click yes to proceed.

Windows update will take a few moments to analyze your system. You will then be prompted with a listing of Service Packs or Hotfixes available for your system. Additionally, the following websites provide the necessary information to perform the updates manually.

Microsoft Windows Security: http://www.microsoft.com/security
Service Pack

Information: http://www.microsoft.com/windows2000/downloads/servicepacks/

Current Critical Hotfixes: http://www.microsoft.com/windows2000/downloads/critical/
Security Bulletins: http://www.microsoft.com/technet/security/

Microsoft also provides a Product Security Notification email service. The goal of this service is to provide accurate information to inform and protect their customers from malicious attacks. To subscribe to the Product Security Notification service, visit the Microsoft Profile Center at http://register.microsoft.com/regsys/pic.asp.

Step 2 - Hardening File System Security

The second thing you need to do is make sure that your hard drive partitions are formatted with NTFS (NT File System). This file system is more secure than FAT or FAT32 partition schemes. Allowed exceptions to this requirement are centrally managed servers and dual boot systems.

***To check your hard drive partitions*:**

1. Log in as Administrator.
2. Double click on My Computer
3. Right-click on each hard drive letter and choose properties.
4. The general tab will identify the File system type.
5. Click cancel to close the properties window.
6. Follow steps 1 – 5 for each drive letter, noting which ones are labeled FAT or FAT32.

Converting FAT or FAT32 partitions to NTFS:

1. Go to Start->Run

2. Type cmd and click OK.
3. At the command prompt type

convert drive /FS:NTFS /V

*Where drive = one of the drive letters you noted above.

4. Hit return to run the command
5. Follow steps 1 – 4 for each FAT or FAT32 partition.
6. Reboot the system for the changes to take effect

Disable Automated Logins:

1. Start -> Settings -> Control Panel -> Users & Passwords
2. In the Users & Passwords window, highlight user name(s)
3. Make sure there is a check in the box beside of the statement, "Users must enter a user name and password to use this computer."

Step 3 - Hardening Local Security Policies

The third thing you need to do is modify the default local security policy. Windows 2000 allows you easy access to the basic security functionality of your system.

While many system attacks take advantage of software inadequacies, many also make use of user accounts on a Windows computer. In order to prevent this sort of vulnerability, "policies" or rules define what sort of account/password "behavior" is appropriate, and what auditing behavior is required. The configuration of user account policies is inadequate or disabled in a default installation.

Account Policies answer the questions like "How often do I need to change my password?" or "How long or how complex does my password need to be?" These policies are often left disabled or weak, leaving many machines vulnerable to attack with little or no effort. Please review the OIT Password Policy located at http://x.x.x for information concerning passwords.

Auditing Policies determine what sorts of security transactions are recorded in the Security Event Log. By default, nothing is retained in the Security Event Log, so any attempts to compromise a system go completely unrecorded. Logging events is crucial for analysis in the aftermath of an intrusion incident.

The options discussed in the section can be set using the Local Security Policy editor on each individual system. Nevertheless, Group Policy configurations may override any changes made at the local level. Thus, insure that Group Policy meet the same guidelines. The following suggested changes will make your system much more secure.

To access the Local Security Policy Editor Tool:

1. Go to Start->Settings>Control Panel->Administrative Tools->Local Security Policy
2. Expand Account Policies by clicking the + box
3. Select the appropriate category
4. Double-click the individual policy settings to make the following changes:
5. When all settings have been configured, close the policy editor

Password Policy

Variable	Setting
Enforce password history	12 passwords remembered
Maximum password age	180 days
Minimum password age	0 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Account Lockout Policy

Variable	Setting
Account lockout duration	30 minutes
Account lockout threshold	7 invalid logon attempts
Reset account lockout counter after	30 minutes

Audit Policy

Variable	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No Auditing
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No Auditing
Audit system events	Success, Failure

* It is important to frequently check the Event Viewer to review log files for possible security concerns. It is optimal to log a minimum of seven days of activity in the application, system, and security logs. In order to maintain the information for seven days, users need to increase the size of the log files. You can access the Event Viewer by:

Going to Start ->Settings>Control Panel->Administrative Tools->Event Viewer

User Rights Assignment

User Right	**Domain Controller** ***Server Requirement Only***	**Standalone/ Member Server** ***Server Requirement Only***	**Windows 2000 Professional**
Access this computer from the	Domain Users	Domain Users	Remove Everyone

network			
Act as part of the operating system	None	None	None
Add workstations to domain	Administrators	None	None
Back up files and directories	Backup Operators, Administrators	Backup Operators, Administrators	Backup Operators, Administrators
Bypass traverse checking	Administrators, Server Operators, and Backup Operators	Administrators, Server Operators, and Backup Operators	Administrators
Change the system time	Administrators	Administrators	Administrators and Power Users
Create a pagefile	Domain Administrators	Administrators	Administrators
Create a token object	None	None	None
User Right	**Domain Controller** ***Server Requirement Only***	**Standalone/ Member Server** ***Server Requirement Only***	**Windows 2000 Professional**
Create permanent shared objects	None	None	None
Debug programs	None (except in off-internet development)	None (except in off-internet development)	None (except in off-internet development)
Deny access to this computer from the network	None	None	None
Deny logon as a batch job	None	None	None
Deny logon as a service	None	None	None
Deny logon locally	None	None	None
Enable computer and user accounts to be trusted for delegation	Use this right only if testing reveals it is necessary.	Use this right only if testing reveals it is necessary.	Use this right only if testing reveals it is necessary.
Force shutdown from a remote system	Administrators	Administrators	None
Generate security audits	None	None	None
Increase quotas	None	None	None
Increase scheduling priority	Administrators	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators	Administrators
Lock pages in memory	None	None	None
Log on as a batch job	None	None	None
Log on as a service	Replicators	None	None
Log on locally	Administrators, Server Operators, and Backup Operators	Administrators, Server Operators, and Backup Operators	Administrators and Authenticated Users

Manage auditing and security log ***	Administrators	Administrators	Administrators
Modify firmware environment values	Administrators, Server Operators, and Backup Operators	Administrators	Administrators
Profile single process ***	None	None	None
Profile system performance ***	None	None	None
Remove computer from docking station	None	None	None
Replace a process level token	None	None	None
User Right	**Domain Controller** ***Server Requirement Only***	**Standalone/ Member Server** ***Server Requirement Only***	**Windows 2000 Professional**
Restore files and directories	Backup Operators, Administrators	Backup Operators, Administrators	Backup Operators, Administrators
Shut down the system	Administrators and Server Operators	Administrators and Server Operators	Administrators and Authenticated Users
Synchronize directory service data	None	None	None
Take ownership of files or other objects	Administrators	Administrators	Administrators

*** Note: Service specific accounts can be granted User Rights that are necessary to perform specific user functions.

Security Options

Local Security Policy	Recommended Settings
Additional restrictions for anonymous connections	Recommended: No access with explicit anonymous permissions Minimal: Do not allow enumeration of SAM accounts and shares
Allow server operators to schedule tasks (domain controllers only)	Server Operators, Administrators
Allow system to be shut down without having to log on	Enabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	15 minutes

Audit the access of global system objects -	Enabled
Audit use of Backup and Restore privilege -	Enabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name in logon screen ###	Enabled
LAN Manager Authentication Level	Send LM and NTLM – use NTLMv2 session security if negotiated
Message text for users attempting to log on	*** * * * * * * W A R N I N G * * * * * * * * * * *** This computer system is the property of the University of . It is for authorized use only. Users have no expectation of privacy in any materials they place or view on this system. The University complies with state and federal law regarding certain legally protected confidential information, but makes no representation that any other uses of this system will be private or confidential. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized University and law enforcement personnel, as well as authorized individuals of other organizations. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized University of personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil charges/criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. **LOG OFF IMMEDIATELY** if you do not agree to the conditions stated in this warning. *** * * * * * University of * * * * * * * ***
Local Security Policy	**Recommended Settings**
Message title for users attempting to log on	Warning: This is a monitored computer system!
Number of previous logons to cache (in case domain controller is not available)	0 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Disabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon - Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders – Disabled	Disabled
Rename administrator account	Disabled (User Specific – see Step 4)
Rename guest account	Disabled (User Specific – see Step 4)
Restrict CD-ROM access to locally logged-on	Enabled (optional if remote access to CD-ROM is

user only	needed)
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Disabled
Smart card removal behavior	No Action
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled – End user system Disabled – Central server
Unsigned driver installation behavior	Warn but allow installation
Unsigned non-driver installation behavior	Silently succeed

Note: An exception to the enabling the "Do not display last user name in logon screen" is allowed for specific applications.

Step 4 - Hardening Default Accounts

The fourth thing you need to do is change the default configuration of the Administrator and Guest account. In general, a prospective user must have a username and password to access a Windows 2000 system. The default installation of Windows 2000 creates an Administrator and Guest account. By changing these accounts names, system security is greatly enhanced. The following actions should be taken:

Configuring the Administrator Account:

1. Log in as Administrator.
2. Go to Start->Settings>Control Panel->Administrative Tools->Computer Management
3. Open Local Users and Groups
4. Click on the User folder
5. Right-click the Administrator account, and choose to rename it. Make it a non-obvious name.
6. Right-click this renamed Administrator account and select "Set Password".

The Guest account is disabled in W2K by default. Enabling the guest account allows anonymous users to access the system. If you share a folder, the default permission is that "Everyone" has full control. Since the Guest account is included in "Everyone," system security is dramatically weakened. A standard practice is to always remove the

share permissions from "Everyone" and add them to "Authenticated Users." This is a much safer configuration.

Configuring the Guest Account:

1. Right-click the Guest account, and choose to rename it. Make it a non-obvious name.
2. Right-click this renamed Guest account, then select "Set Password."

SERVICE	DESCRIPTION	ACTION
Alerter	The Alerter service makes it possible for Windows 2000 computers to "alert" each other of problems. This feature is generally unused.	Disable if Unneeded
Clipbook	The Clipbook service is used to transfer clipboard information from one computer to another. This is generally only used in Terminal Services.	Disable if Unneeded
Fax Service	The Fax Service sends and receives faxes. It is generally unused.	Disable if Unneeded
Messenger	The Messenger service works in conjunction with the Alerter service.	Disable if Unneeded
NetMeeting Remote Desktop Sharing	NetMeeting users have the option to share their desktops, and allow other NetMeeting users to control their workstation.	Disable if Unneeded - **@@@**
Telnet	The Telnet service allows a remote user to connect to a machine using a command prompt. Use SSH if this functionality is needed.	Reference Telnet Policy at: http://oit..edu/infosec/

Step 6 - Prepare System for an Incident

The sixth and final thing you should do is to prepare the system for an incident. ***The information outlined in this step is for trained System Administrators only.*** It is sufficient for the general user to be aware of potential threats, to monitor the performance and functionality of your system, and to notify the ITSG if you see any unusual activities**.** ***It is recommended that all general system users contact a qualified System Administrator or the Helpdesk prior to attempting any of the activities listed in this section of the Hardening Guide.***

While the actions outlined in this guide will dramatically increase system security, system vulnerabilities may exist. New security holes are discovered regularly, thus, preparing for the worst is critical. These steps should help to facilitate identifying a system compromise, allow for forensic analysis, and enable a timely recovery.

Identifying a System Compromise

Aside from consistently watching for common indications of a system compromise (listed below), you should consider recording cryptographic checksums. By doing

so you can establish a baseline of system binaries, application code, and data. This allows you to compare the current file system against a known reliable version.

1. A system alarm or similar indication from an intrusion detection tool
2. Suspicious entries in system or network accounting (e.g., a UNIX user obtains privileged access without using authorized methods)
3. Accounting discrepancies (e.g., someone notices an 18-minute gap in the accounting log in which there is no correlation)
4. Unsuccessful logon attempts
5. New user accounts of unknown origin
6. New files of unknown origin and function
7. Unexplained changes or attempt to change file sizes, check sums, date/time stamps, especially those related to system binaries or configuration files
8. Unexplained addition, deletion, or modification of data
9. Denial of service activity or inability of one or more users to login to an account; including admin/root logins to the console
10. System crashes
11. Poor system performance
12. Unauthorized operation of a program or the addition of a sniffer application to capture network traffic or usernames/passwords
13. Port Scanning (use of exploit and vulnerability scanners, remote requests for information about systems and/or users, or social engineering attempts)
14. Unusual usage times (statistically, more security incidents occur during non-working hours than any other time)
15. An indicated last time of usage of a account that does not correspond to the actual last time of usage for that account
16. Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program)

The most commonly accepted cryptographic checksum used today is the MD5 algorithm, created by Ron Rivest of MIT and published in April 1992 as RFC 1321. To learn more about the MD5 algorithm or to download the source code visit one of the following websites:

RFC 1321: http://www.landfield.com/rfcs/rfc1321.html

MD5 Algorithm (available in the Cygwin distribution):
ftp://go.cygnus.com/pub/sourceware.cygnus.com/cygwin/cygwin-b20/full.exe

Additionally, commercial products such as Tripwire automate the process and provide a management interface for easy administration. Tripwire is available at http://www.tripwire.com.

Forensic Analysis
Forensic Analysis is the process of unearthing data of probative value from computer and information systems.

References

[i] Attack on "University "- DCOM RPC vulnerability by Alfredo Lopez
The Educational Facility' Network by Timothy C. Hall

[ii] http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

[iii] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533

[iv] http://www.k-otik.com/exploits/04292004.HOD-ms04011-lsasrv-expl.c.php

[v] http://www.webopedia.com/quick_ref/OSI_Layers.asp

[vi] http://www.foundstone.com/

[vii] http://www.atstake.com/research/tools/network_utilities/