Resources:
E-newsletters
Discussion Center
Technical Q&A
Downloads
Books & CDs
Products & Services
Peer Directory
White Papers

Hacking the hacker: How a consultant shut down a malicious user on a client's FTP server

August 19, 2003 | John Verry | E-Mail

Rating: 4.9 / 5 | Rate this article
Discussions: 69 Post(s) | 1 NEW | View posts

This article was originally published on TechRepublic in August 2003. It was the most widely read piece of content on the site for the next three month period, and one of the most highly rated articles ever published on TechRepublic.

Ethical hacking is one of the most intriguing and exciting elements of our work. In most engagements, our efforts involve attempting to penetrate a client's network, documenting the results of our efforts, and recommending optimal strategies for mitigating the risks we have identified.

A recent engagement for a software development firm took an interesting twist at the onset of the project, as we quickly discovered the client's FTP server had already been hacked and was being used for illegal purposes. I'll describe the techniques we used to meet the client's requirements and explain how our efforts turned from hacking their network to hacking the hacker.

Late to the party

We convened with the client for a brief kickoff meeting to reconfirm the objectives of the Limited Knowledge Penetration Test (PT) and to gather sufficient information to ensure that the testing did not affect normal business operations. We began our preliminary research by reviewing publicly available information relating to the target company, including news releases, newspaper articles, annual reports, SEC filings, and the corporate Web site. Hackers commonly use these resources to gather potentially vital information relating to a company, including names of key employees, product lines/releases, key dates (such as the date a partnership was formed and a network administrator's birthday), empire locations, hardware/software used, etc.

During these operations, we discovered that an internal user at the client's organization was the leading poster of messages and/or content to a Web site that distributed illegal pornographic images. This was immediately reported to Client Management, which became increasingly concerned as it disclosed that there were multiple instances of often unexplainable periods of full utilization of the outbound Internet links during odd hours. (We are still unsure why it didn't disclose this at the kickoff meeting.)

After using nMap to footprint the external network, we focused our attention on an FTP server that was curiously installed outside the firewall. A port scan against the box returned extremely troubling results. In addition to the expected open port (port 21), we found a half dozen other open ports, including 139, 2187, 3437, and 14120.

- Port 139 was running NetBIOS and allowed extensive leaking of information via Null Session Enumeration.
- Port 2184 was running Microsoft Windows Telnet Server, which generally runs on port 23. Sometimes an admin will run this on an odd port; however, attempts to log in to Telnet with a valid username/password combination we obtained via Enumeration of port 139 would result in a hung Telnet session.
- Port 3437 was running a service that prompted for a password. We connected to it with both Telnet and NetCat. If no valid password was given for three seconds or an invalid password was given, the connection would be terminated.
- Port 14120 was running a second FTP Service.

Some key details of our FTPing the site include:

- Two users were currently connected; in the past 24 hours, 23 users had connected.
- 19 MB had been downloaded since the last time the server was restarted (earlier that morning).
- Anonymous logins were rejected and our attempts to password-guess were unsuccessful.
- Searches based on the hacker tags in the banner returned only links to listings of various hacked pubstors.
- Searching on the machine's IP address failed to reveal its public listing in any warez or pubstor directories.

Should the client prosecute?

The client's first concern was the potential correlation between the posting of messages / content to a site that housed illegal images and the distribution of large files from its FTP Server. Was an employee using their FTP server to distribute pornography?

We advised the client that if it intended to prosecute, it would need to work within the legal framework of forensic investigations. Most notably, it would be critical for the forensic data to be authenticated as genuine.

Many of the actions an individual might take, including rebooting the machine, copying files from the server, and reviewing security logs, can alter the drive data. The client's management was adamant about conducting the investigation in a manner that would provide the opportunity to prosecute if necessary. The client's lawyer also believed that by demonstrating due diligence, it would minimize the risk of a third party taking legal action against the organization as a result of the hack.

A particularly important legal case, "Gates Rubber Co. vs. Bando Chemical Indus, Ltd," helped define the mandatory legal duty of a forensic investigator with regard to creating a mirror image copy of the hard drive in a manner that maintains chain of evidence and custody. In that case, the investigator's decision to perform logical "file-by-file" copying to preserve the evidence precluded legal use of the data because the copying might have resulted in lost information and the creation of new temporary files on the media.

Assessing the hack

We used Encase software, which is used extensively by law enforcement professionals, to gather a mirrored image of the drive. We then mounted it in a Windows 2000 machine but were unable to navigate/view the directory structure of the illicit FTP Server. There are a number of ways that hackers (and Windows itself) can hide directories and files. A simple way to make folders invisible (dependent upon Explorer settings) is to set a folder's property to +s[ystem] within Windows Explorer or via DOS. For example, although users may clear their Internet History, the data is still maintained in hidden files that can be accessed by an investigator.

Other methods include using device driver names such as "prn," "con," and "com1" or a special combination of characters such as "..--1" (dot dot dash dash 1).

To access the hidden directories and determine the content being distributed, we added the drive to a Windows 2000 Server and mounted it read-only from a Red Hat 9 Linux machine.

Assessing the facts before looking at the drive, we knew the following:

- A Serv-U daemon (a rogue FTP Server) had been installed by the hacker.
- This installation would have required administrator access.
- Microsoft Telnet server was running on TCP 2184 without NTLM authentication, enabling a malicious user to gain access to the system.
- An unknown service was running on TCP 3437.
- The penetration test manager advised that they had found directories within their FTP root they could not delete.

We first viewed the FTP root of the Serv-U daemon. Three files immediately caught our attention:

- 1kbtest.ptf
- 1mbtest.ptf
- space.asp

The first two files were used by the hacker to measure the available bandwidth of the server and gauge the efficacy of using this machine to conduct other attacks. The Space.asp Active Server Page was used to enumerate drives and their free space on the server. These files illustrate the dangers of anonymous uploads.

Next, we looked at the Serv-U daemon. Normally, Serv-U is run through the information contained in an ini configuration file. We searched the drive for .ini files and examined the output. This resulted in the discovery of r_bot.ini in the system directory (E:\winnt\system32). An examination of this file revealed that the attacker was using e:\winnt\system32\inf as his base of operations on the host. It also showed that the attacker was using IRC to remotely control the machine.

Further examination of the system32 directory showed the appearance of several suspicious files, all of which appeared on Feb. 17, 2003:

- **info.exe** - An enumeration tool to detail information about the local server to the hacker
- **hlp32.exe** - A renamed version of Bouncer v1.0.RC6, which is a Proxy utility
- **jrun.exe** - A renamed version of "Netcat," the TCP/IP Swiss Army knife of hackers
- **kill.exe** - A utility to allow the hacker to terminate processes that he did not want running on the box
- **pslist** - A utility that provides Proccess IDs for running processes (UNIX-like), which was likely used in concert with kill.exe
- **wshell.exe** - A Windows shell application (Winshell) that provided the hacker with a remote graphical user interface (on TCP port 3437), which was password-protected (we cracked the password)
- **reg.exe** - A utility to make it possible to edit the machine registry from a command line (DOS)
- **service.exe** - An IRC bot used to control the machine; notify that it's online

More anomalies present in the directory were IIS log file directories for February 15 through 18. An examination of the abbreviated logfiles showed the upload of the speed test files and space.asp page on the 15th. We could also observe the creation of a directory and upload of a copy of Photoshop.

Examining the winnt\system32\inf directory, we found the home directory of the Serv-U service. We saw that the attacker had created directories for applications, movies, and games. Files in these directories included an ISO image of Windows Server 2003 and movies, including an Indiana Jones movie and the documentary Bowling for Columbine.

Another directory found in \system32 provided further detail of the intruder's activity. This directory included the following attack utilities:

- **sfind.exe** - A command-line vulnerability scanner
- **X-Scan** - A command-line and GUI scanner
- **IpcScan** - A command-line and GUI Windows account cracker

We also discovered that the attacker had removed most of the log files generated by these tools. (They had been stored in E:\!!!!\SQLEXECl.) An examination of the slack space in the drive showed that the files had been overwritten. However, the entire Class B network belonging to a significant U.S. governmental agency had been scanned for vulnerabilities.

Turning the tables

In light of the potential liability associated with the distribution of copyrighted materials and the attack on government agencies, the client authorized us to attempt to identify the source of the hack. Most notably, we recognized that the attacker was very comfortable using IRC. We examined the communications of the installed IRC bot and determined the IP Address it was connecting to.

Using the information in r_bot.ini, coupled with these potential passwords, we attempted to access the attacker's password-protected chat room. Unfortunately, our attempts to guess the password were unsuccessful. Returning to the drive, we cracked a password by using an internally developed cracker that can identify potential passwords via regular expression searching. We returned to the chat room and conducted a whois to obtain information regarding the owner / moderator of the chat room.

At this point, we knew which host the attacker was connecting from. Provided the host legally belonged to the attacker, we could obtain his identity from his ISP. From the IRC site, we identified nine additional servers that had been compromised in the same manner, including two universities and a large regional bank. (We notified the ISP and the owners of the IPs of our findings.)

We began with an attempt to verify whether this connection was being proxied. We discovered that the server at xxx.xxxxxx.xx wouldn't allow IRC connections from unsecured proxy servers. (Note: We've replaced all IP addresses with Xs.) We then probed the attacker's machine to view the available services.

We used nMap to identify the services running on the hacker's system and found that the attacker was using a Windows XP Professional machine, located in Belgium (determinable by an IP address belonging to a Belgium ISP). He was running a private Serv-U FTP Daemon on TCP 1412, as well as a publicly available Serv-U FTP service (port 21).

We could see that he employed a common tactic: By having a publicly available FTP site, loaded with his hacking tools, he could compromise a machine and download the tools and files he needed. Note the absence of any banner advising that the machine was private and that public connections were not allowed so we were not actually "hacking" the hacker.

We then proceeded to download the contents of the FTP server. Examining the files, we could piece together his attack methodology and actions:

- He scanned for machines with vulnerabilities in Microsoft SQL Server, IIS, or NetBIOS.
- Once a victim was located, he downloaded and executed a batch file, which performed numerous actions before deleting itself.
- He created an account called Admin, set the password, and added the account to the Administrator's group.
- He FTPed necessary tools to the machine, creating directories within winnt\system32 to store them.
- He configured the Microsoft Telnet Service to run on port 2184, disabling NTLM authentication.
- He installed a WinShell Service on port 3437.
- He installed the Serv-U daemon and configured directories.
- He installed an unsecured SOCKS proxy.

He then patched the machine to prevent other attackers from using the same exploits:

- He disabled WebDav on IIS HTTP.
- He set RestrictAnonymous=1 in an attempt to prevent Null Session Enumeration. (This value should be set to 2 to be effective.)
- He deleted administrative file shares.

Based upon what we found, we were able to create specific Web queries to determine the attacker's real identity. Our final report to the client included this information about the hacker:

- Full name
- Date of birth
- Town in Belgium where he lived
- E-mail address
- Photograph

Cleaning up the mess

Although the client was relieved to learn it wasn't trafficking illegal pornography, it was concerned to be trafficking intellectual property. It was also concerned that its FTP server had been used to conduct scans and/or attacks on other networks. Our report included many recommendations, most notably:

- Consult with legal counsel regarding the liability associated with the hack and current legal responsibility (a very subjective area at this time).
- Consider reporting the hack to the appropriate agencies and affected parties, including:
    - The local office of the FBI
    - The State Office of Information Technology
    - The State Police's High Technology Crimes Unit
    - CERT
    - Microsoft
    - Adobe
    - The governmental agency scanned
    - Paramount Pictures (Indiana Jones)
    - United Artists (Bowling for Columbine)
    - Clients regularly accessing the FTP server
- Rebuild the FTP server.
- Move the FTP server behind the firewall and limit traffic to the FTP server to ports 20 and 21.

Don't make it too easy

Executing on the basics of IT security is not enough to ensure that your organization will not be hacked, but it will significantly reduce the chances. Further, if you are hacked, you'll be able to recognize and remediate it before significant damage to the organization is done.

The basics for systems that need to be externally accessible (Web, e-mail, FTP) include these steps:

- Put them behind an appropriate firewall (preferably in a DMZ).
- Disable all services except those absolutely needed.
- Filter all except port-specific traffic to systems (e.g., 20/21 for FTP).
- Turn on system and firewall logs.
- Review the logs on a daily basis.
- Consider implementing intrusion prevention software for mission- critical boxes.

Although this seems like (and truly is) "Security 101," I can assure you that many organizations are not executing on the basics. Virtually all of the hacks we investigate are caused by a failure to execute on some combination of these fundamentals.

Rate | E-mail | Printer Friendly | Discuss

Discussions

- Well Written — Drivr 10k | 08/19/03
    - Agreed! — it@berlow.org 10k | 08/19/03
    - Super Ariticle — deepsix | 08/19/03
        - Excellent Article — Pr1est 5k | 08/19/03
    - Missing Details — Rui@OBS | 08/20/03
    - Excellent detective work — chucksel 5k | 08/20/03
    - I loved it! — wodenickel@hotpop.com 10k | 08/20/03
    - Wow, it can actually be done — Damo_uk23 | 08/21/03
        - The Same happened with me — Naeem Akhtar | 08/25/03
    - Great article — info@johnmichaud.com | 08/21/03
    - PrimeTime Article — Padre5 | 08/21/03
    - If you like stuff like this — LordInfidel 10k | 08/21/03
        - Two thumbs up — OzMedia 10k | 08/25/03
    - Don't rely on the FBI to assist... — KTC 5k | 08/21/03
    - Well written and defined except for — LesSalmon@Manx.Net | 08/21/03
    - "we could obtain his identity from his ISP" — dball@cityofsacramento.org 5k | 08/21/03
    - Super. 11 out of 10! — gbeck@cnginternet.com | 08/21/03
    - Couldn't agree more! — dmh1 10k | 08/27/03
    - Agreed!!! — ShockRide 10k | 08/27/03
- Fantastic Article ! A Must Read — bacchus@hush 5k | 08/20/03
    - More Like it Please — jscott310@btinternet.com | 08/21/03
        - Stealing the Network: How to own the box — LordInfidel 10k | 08/21/03
- Great article, well written — phungle@hotmail.com | 08/20/03
- I am just breatless — jleche@ocwen.com | 08/20/03
- Very Interesting — patopp@att.net 5k | 08/21/03
- DMZ ? — seanodea@hotmail.com | 08/21/03
    - Yes in a DMZ — red_wolf(at)fastmail.fm 10k | 08/21/03
- Best article I've read on TR — InquireWithin 10k | 08/21/03
- Excellent writing — larvoss@ieee.org | 08/21/03
- Good article.... but — red_wolf(at)fastmail.fm 10k | 08/21/03
- I Love A Mystery Too! — tonyfriendly@friendlybusinessgroup.com | 08/21/03
- Great article - but need more info... — sheldonmercer@ns.sympatico.ca | 08/21/03
    - Here is another — pgomez@bscinet.com 5k | 08/21/03
- How did the FTP site move? — sherpa dan | 08/21/03
    - Firewalls & the FTP Server — Catadmin 10k | 08/21/03
        - As a SOHO am I doing enough? — sherpa dan | 08/21/03
        - A router is not a firewall. — Eqwatz 5k | 08/21/03
            - Great article *NEW* — erickerin@hotmail.com | 09/02/03
- Read this Book!!!!!!!!! — LordInfidel 10k | 08/21/03
    - Am I the first to ask... — dpetrak 10k | 08/21/03
        - 60% plus all the oreos I can eat — LordInfidel 10k | 08/25/03
    - Thanks for the warning — johncymru 10k | 08/25/03
        - your not being serious???? — LordInfidel 10k | 08/25/03
- Bravo! — stuart_at_oz 10k | 08/21/03
    - Sorry, that was pgomez not LordInfidel — stuart_at_oz 10k | 08/21/03
- Brilliant A Must to Read: — jsimser@hotmail.com | 08/22/03
- Excellent! However,as to not actually "Hacking"... — packet_geek 10k | 08/22/03
- Excellent article — Elama | 08/22/03
- Thanks — sexygina@earthlink.net | 08/24/03
- Superb!! — Shinzo | 08/30/03