VeriSign®

TECHNICAL BRIEF

Hacking and Network Defense

CONTENTS

Introduction

Consider the following[1]:

April 26, 2002
The Federal Aviation Administration was hacked and unpublished information on airport passenger screening activities was downloaded. The group known as "The Deceptive Duo" also publicly defaced the FAA site used by the Civil Aviation Security organization. They also used information extracted from the database to post the name of the FAA inspector, screener ID number, number of passengers screened, and any guns, explosives, or chemicals found. The duo stated this warning as their reason for the attack—"secure your systems before a foreign attacker hacks you."

November 21, 2001
Playboy.com was hacked and credit card numbers were stolen. The attacker e-mailed all of the customers claiming responsibility for the attack and provided each customer with his/her credit card number as proof.

June 3, 2001
Intruders hacked Amazon.com and download a database of 98,000 accounts including customer records, credit card information, names and addresses.

January 24, 2001
Microsoft's online services were disabled by a supposed Denial of Service attack. Further investigation by a Swedish network administrator reveals that all of Microsoft's DNS servers were behind one single network, therefore the problem was a result of poor network design.

September 11, 2000
Western Union Web site was hacked. Hackers made off with 15,700 credit and debit card numbers.

With the constant onslaught of media attention covering security breaches at even the most tightly controlled organizations, it is more important than ever to learn about hackers, their methodologies, and ways to defend your network. This paper presents profiles of hackers, describes common attacks these individuals conduct and tools they use, and presents you with several ways to defend your organization.

1. InfoWar on the World Wide Web. Various articles. http://www.infowar.com

The Hacker Profile

The idea of hacking is intriguing to many. The thought of taking on a secret persona with the superior technical skills to penetrate even the most secure network can have a spy game appeal for some. Who are these individuals? And what sets them apart from everyone else?

The term "hacker" has been exploited by the media over the years. In movies, hackers are often portrayed as greasy-haired teenagers in dark rooms hovering over computer keyboards surrounded by empty cans of soda and pizza boxes. In reality, hackers come from all walks of life. They can range from the computer programmer you work with who hacks in the evening, to a high school student who plays on the computer after he gets out of school, to almost anyone in between.

Additionally, many people do not distinguish between those who hack for fun and those who hack for far less innocent reasons. Within the security community there are both hackers and crackers. Hackers have an interest in computers and networks and actually enjoy the game of discovering vulnerabilities or holes in systems. Hackers typically like to share their findings and never intentionally damage data. Crackers, on the other hand, are focused on maliciously violating systems with criminal intent. Some people classify these people as either White Hat (good) or Black Hat (bad) hackers.

It is commonly agreed that the initial motivation for most hacking is curiosity. In these cases, exploring computers and networks creates a temptation to learn even more. This interest serves as a launch-pad for the vast majority of hackers. Some continue to explore and have fun, while others seek more challenging, and often illegal, paths. For them, attacking and outsmarting a large corporation can create a huge ego boost. Other motivations may include notoriety or showing off to increase the standing in a social group.

A growing trend for hacking motivation is revenge. With many companies experiencing significant layoffs, those who are on the receiving end of job cuts may find the motivation to seek revenge through network attacks. After all, there is no better person to target a network than someone from the "inside." A disgruntled employee may target a network simply out of revenge, causing serious damage to operations and data.

Enterprise Risks

As the information age continues to mature, more and more individuals have access to sophisticated computer and Internet technology. Today's personal computer has more power than it once took to put a man on the moon. Improved technology and lower prices allow many more people to access superior technology in their homes.

The same can be said for Internet connectivity. Many metropolitan areas now offer cable modems or DSL connectivity with 1.0MB/second access speeds for under $50 a month. Today, the power at an individual's fingertips is enough to disable a medium-sized Web hosting company. This accessibility to computer power, in part, explains the sharp rise in attacks every year. Other contributors are the increased Internet population and the availability of hacking tools.

More attacks mean increased risk. A risk is defined as a possibility of harm or loss. It is important to assess the risk your company faces as you plan and implement network security measures. Clearly, a company like Microsoft has a much greater risk than "basketsbylinda.com." Companies with more assets and intellectual capital, as well as companies with a high profile, have more to lose than others; and therefore have a much higher risk of attack.

What are the types of risks a company faces?

Disruption of Services
Many companies encounter disruption of services as a result of human error or an attack. The Denial of Service (DoS) attacks on February 7-8, 1999 against companies such as Yahoo, Buy.com, CNN, Amazon.com and Datek were aimed at disrupting the services of these companies. Most of the targeted sites were inaccessible for four hours or more. This disruption in service was not only inconvenient for customers—it led to the loss of millions of dollars in potential sales.

Damaged Reputation
Many companies fail to report security breaches because they do not want to risk public humiliation. A defaced Web site or a hacker who reveals customer credit cards can destroy a company's reputation. For example, in January of 2000 a Russian cracker stole more than 25,000 credit card numbers from CDUniverse.com. The cracker then tried to extort money from the company. When the press got wind of the incident, they published the story and caused extensive damage to CDUniverse.com's reputation in the market.

Exposure of Confidential Information
Advanced attacks involve the exposure of confidential information. Once a machine is compromised, a hacker can attack a database that may contain trade secrets, company information, or consumer information such as credit cards. On February 11, 2002 a former employee of Global Crossing was arrested for exposing employee Social Security numbers and birth dates on the Web.

Corruption of Data
Imagine the havoc that would ensue if someone hacked The NASDAQ Stock Market's www.nasdaq.com site and changed the trading prices of Intel, Microsoft, and Cisco to $.01 per share. After a hacker has compromised a machine or network, they can fairly easily tamper with the information so as to render it useless or misleading.

Liability

If a hacker uses your systems to attack another company are you equally liable for the attack? This scenario creates a situation known as downstream liability. The hacker is responsible for attacking you, but you may be responsible as well because your systems were used to attack the target. Downstream liability is currently the subject of many debates and court cases. Does your company's lack of preparedness for this type of attack indicate lack of due diligence? Does lack of due diligence bring fault upon your company?

All companies should perform their due diligence when securing their environments. Lack of a written security policy, firewalls, intrusion detection, anti-virus protection, etc. can represent a lack of due diligence on behalf of a company. The CERT® Coordination Center, part of the Carnegie Mellon University Software Engineering Center, presented a hypothetical scenario about downstream liability at the RSA 2002 conference. This white paper can be found at http://www.cert.org

Anatomy of an Attack

A hacker relies on a variety of tools as well as his or her own creativity in order to attack your network. Because every network is different, hackers employ a variety of means to breach your security. However, most hackers follow the same basic steps to perpetrate an attack:

1. Profiling
2. Scanning
3. Enumerating
4. Exploiting

1. Profiling

Profiling, or footprinting, is the process of gathering information about targets. The result is a profile of an organization's security posture, also known as the infrastructure. Profiling may also include gathering information about the physical site. Insiders (people who already work for the company) may have a significant advantage during the profiling process due to pre-knowledge of the network and physical environment. In fact, 2002 FBI statistics show that 80 percent of attacks are committed by people within the company (employees, consultants, etc).

Much of the information used for footprinting is publicly available on the Internet. Several tools and Web sites are widely available to assist in gathering this data. For example, WHOIS (www.whois.com) can reveal identities within an organization, as well as phone numbers, FAX numbers, and e-mail addresses. These e-mail addresses often represent a user's login to the domain.

Additionally, ARIN.net maintains the database of network blocks and can also be a useful tool for determining a particular company's IP addresses. This list is critical in targeting a network for attack. Netcraft.com will show you the IP address of a Web site and quite often also tells you the type and version of Web server and operating system.

Incorrectly configured DNS servers can also list a plethora of systems and their IPs for a particular network. Tools such as nslookup and dig can be used to list this information. Newswire articles commonly list employee names, which can be used to guess accounts for systems.

It is the combination of this information that allows a hacker to profile a company. It is difficult to limit dissemination of this information, but a good defense is to use alias names, generic phone numbers, and third party email addresses to deter some of this profiling activity (see Fig. 1).

```
microsoft.com
Request: microsoft.com

Registrant:
Microsoft Corporation (MICROSOFT-DOM)
   1 microsoft way
   redmond, WA 98052
   US

   Domain Name: MICROSOFT.COM

   Administrative Contact:
      Microsoft Hostmaster  (MH37-ORG)          msnhst@MICROSOFT.COM
      Microsoft Corp
      One Microsoft Way
      Redmond, WA 98052
      US
      425 882 8080
      Fax- - - .: 206 703 2641
   Technical Contact:
      MSN NOC  (MN5-ORG)                        msnnoc@MICROSOFT.COM
      Microsoft Corp
      One Microsoft Way
      Redmond, WA 98052
      US
      425 882 8080
      Fax- PATH

   Record expires on 03-May-2011.
   Record created on 02-May-1991.
   Database last updated on 31-May-2002 13:35:05 EDT.

   Domain servers in listed order:

   DNS1.CP.MSFT.NET          207.46.138.20
   DNS1.TK.MSFT.NET          207.46.232.37
   DNS3.UK.MSFT.NET          213.199.144.151
   DNS3.JP.MSFT.NET          207.46.72.123
   DNS1.DC.MSFT.NET          207.68.128.151
```

Figure 1
whois output for www.microsoft.com showing the proper use of alias information in a domain name record.

2. Scanning

After profiling a network, a hacker will then scan the network for additional information. This will allow him or her to create a list of network devices active on the network. There are several ways to complete the scanning phase. Hackers often use PING sweeps to identify what systems are active and responding on the network.

Additionally, hackers use port scanners such as nmap and 7thSphere to reveal what ports and services are available on the network devices. These scanners can also allow fingerprinting of systems. The scanner may find ports that are common to a particular network device. For example, a scanner can determine that System A is Windows 2000 (port 445), running IIS 5.0 (port 80) and FTP (port 21). A scanner can also determine that System B is a Solaris server (ports 111, 32771).

Web scans have become very popular as well. Tools such as whisker can be used to find unpatched exploits on Web servers.

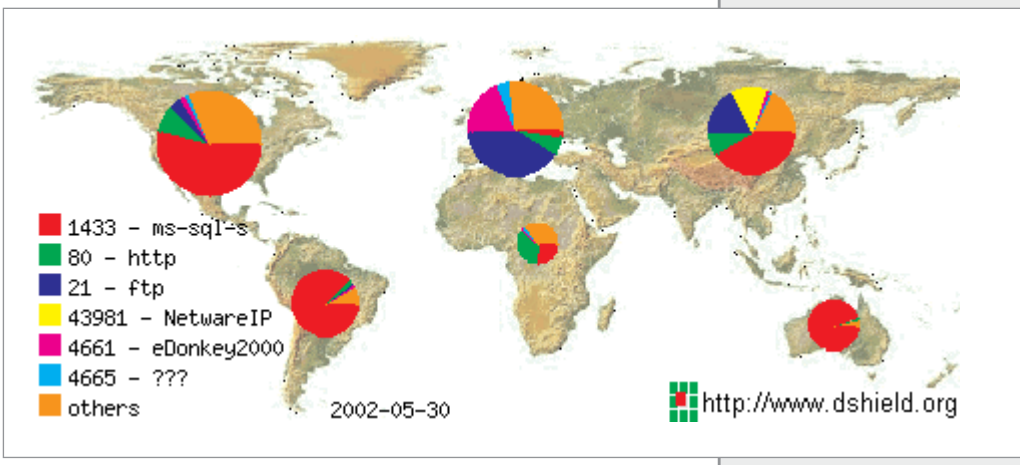

Figure 2
A snapshot of commonly scanned ports by port number and continent.

Commercial scanners such as NAI CyberCop, ISS Internet Scanner, and WebTrends Security Analyzer are typically used for legitimate scanning purposes, but are sometimes used by hackers as well. Open-source scanning tools such as nessus are publicly available to anyone, and therefore can be used by hackers during the reconnaissance phase. These scanners will scan an entire system for all vulnerabilities, not just ports and system banners. They will reveal all of the operating system and application level vulnerabilities. Examples of these much broader tools are nmap or 7thSphere.

No intrusion has occurred during the profiling and scanning phases, therefore no laws have been broken yet. Up to this point the hacker is simply checking to see which doors are unlocked but has not necessarily opened them yet. Profiling and scanning represent the initial steps leading to the attack. An intrusion detection system can assist with logging and alerting the scanning activity, as well as identifying the IP address of the attacker. This provides a proactive defense against this type of activity.

3. Enumeration

Enumeration is the intrusive process of determining valid user accounts and accessible resources such as shares. Having identified these accounts, the hacker can then guess passwords

to gain access to a system. Identifying and accessing resources might allow a way into confidential documents or even a database.

The process of enumeration requires an active connection to the machine being attacked. In addition to identifying user accounts and shared resources, a hacker may also enumerate applications and banners. By creating active connections to FTP, telnet, or Web applications, a hacker can reveal the system type and version. Anonymous accounts or accounts with easily guessable passwords may also be found. These can be identified with password grinders that use a dictionary of common passwords. Applications such as SNMP (Simple Network Management Protocol) may also leak public community strings, which can be used for system and version identification.

Please note that some of the scanners mentioned can perform scanning as well as some enumeration. In addition to software tools, there are some other means of enumerating. These are:

Social Engineering

Social engineering is essentially a confidence game, in the old fashioned sense—a "con". The goal of social engineering is to gain access to network information from the people that run the network by creating a level of trust through deceit. Social engineering takes advantage of people's natural willingness to be helpful and open. For example, an attacker may masquerade as someone else by telephone or e-mail to deceive the help desk into giving him a password or access to a system. To gain physical entry into secure areas, a hacker may simply enter a building and pass him or herself off as a visiting employee.

The notorious hacker, Kevin Mitnick, used social engineering as one of his primary weapons to gain private information. By using his skills to masquerade as an employee of a company, Mitnick was able to fool people into giving him access to physical facilities as well as unauthorized accounts. For more information about Kevin Mitnick and other hackers, view the "Hackers Hall of Fame" at http://tlc.discovery.com/convergence/hackers/bio/bio.html.

Observation

Observation can range from looking over someone else's shoulder as they login, to coming across passwords that people often keep written down on little pieces of paper hidden under keyboards or log books.

Eavesdropping

In information security, eavesdropping requires physical access to the network, and typically involves wiretaps and/or network sniffing. The process allows an attacker to capture usernames, passwords, or confidential data such as credit card numbers. Open-source tools such as Ethereal (http://www.ethereal.com) can allow anyone with a Windows NT or 2000 desktop to sniff the network.

4. Exploiting

Exploiting is the process by which the attacker gains unlawful entry to a system. At this point, the attacker would have identified vulnerabilities during the scanning and enumeration phases. The attacker can now attempt to exploit one or more of these vulnerabilities with the ultimate goal of gaining complete control of the machine.

Numerous programs exist on Web sites that provide information about automated methods of performing many exploits. One of the most popular is from Packetstorm, a non-profit organization (http://www.packetstormsecurity.org), developed to help security administrators stay current with exploit threats. The Packetstorm site features archives and links to thousands of hacker programs, and its search engine is an efficient way of locating a specific program.

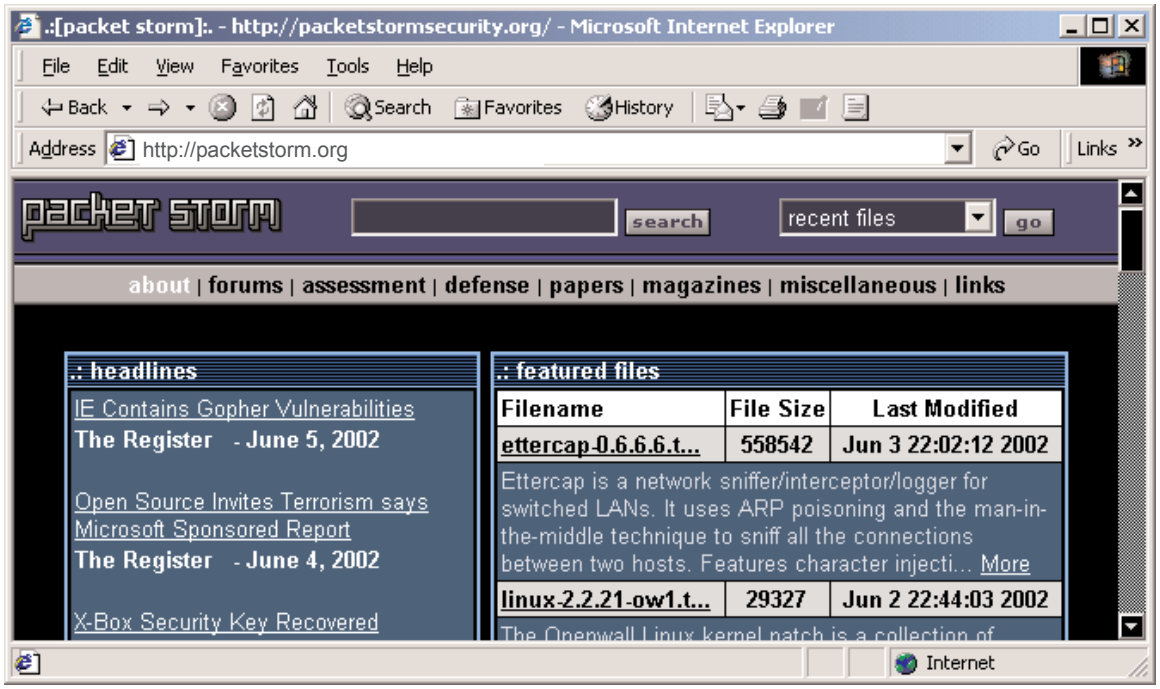

Figure 3
Packetstorm Web site.

In addition, popular books such as Hacking Exposed (Scambray, McClure, and Kurtz) detail step-by-step instructions for performing exploits on a variety of platforms and network devices. It would be impossible to create an exhaustive list of all of the known exploits—they number in the thousands. However, exploits can be categorized into some general types:

Buffer Overflows

Buffer overflows are typically a result of poor programming. Invalid input is allowed to overflow the memory buffer causing the system to crash. Advanced attacks overflow the memory buffer and allow constructed input to run on the machine, thereby exploiting the machine. To defend against this, input values provided by users should be checked by the program to determine if they are valid. In addition, programs should be limited to reasonable amount of CPU time.

Privilege Escalation

Privilege escalation occurs when a user has a local access account, or a hacker gains a local access shell through an attack, and then uses the shell to escalate his privilege to administrator or root level. There are many methods used to compromise this level including password cracking, buffer overflows, and exploitation of poor file and directory permissions.

Brute Force Attacks

Typical password brute force attacks involve trying every combination of username and password in order to break into a machine. There are a variety of brute force programs which use a list of usernames and a dictionary of passwords to try every combination. Many operating systems can "boot" a user off a machine after three or five bad login attempts. This can discourage this type of brute force activity.

Unexpected Input

Some Web pages allow users to enter usernames and passwords. These Web pages can be targeted for hacking when they allow the user to enter more characters than just a username. For example:

```
Username: jdoe; rm  -rf /
```

This might allow a hacker to remove the root file system from a UNIX Server. Programmers should limit input characters, and not accept invalid characters such as | ; < > as possible input.

Defacements

Defacements are very common to Web sites. Typically a hacker finds an exploitable vulnerability on a Web server, which allows him to upload a new home page of his choice.

Denial of Service

The anatomy of a Denial of Service (DoS) attack is somewhat complex, but its goal is disruption of network services. A DoS attack is designed to deny service to legitimate customers by flooding a network or server with so much traffic that it is rendered inaccessible. A hacker may use an army of computers to attack a large network.

Enterprise companies use very large network pipes, and in order to flood this type of network, a proportionate bandwidth or more is required. Most people at home do not have this type of bandwidth available to them, but ISPs do. To accomplish the DoS, the hacker distributes Trojan horses or zombies through e-mail and/or other means. As computers and workstations become infected, the hacker keeps track of which machines he now has control of. When he feels he has enough machines on the right networks, he wakes the zombies from sleep mode and they attack the target. This methodology protects the hacker because the attacks originated from an ISP, not his machine at home.

Launch Pad Attacks

Launch pad attacks are more and more common in today's well-connected environments. In this type of attack, your company may simply be the starting point for an attacker. Rather than use his or her own system to launch an attack, the hacker decides to use yours. Once the hacker has compromised your system, he or she uses your system (and your bandwidth) to attack a targeted network. This type of attack also raises the risk of downstream liability for the launch pad victim.

Common Hacking Tools — The Hackers Toolkit

Hackers have a variety of resources at their fingertips as they plan and execute attacks. The most common tools include the following:

Web Scanners

Web servers are common targets due to their accessibility. Web servers are usually available to the public and typically have relaxed security protection because of their location in the network. Numerous scanners exist that allow an attacker to quickly identify vulnerabilities based on common attacks. Whisker by RainForestPuppy is probably the most popular and most powerful. See http://www.wiretrip.net/rfp for more information.

Port Scanners

Port scanners allow an attacker to quickly identify available services and open ports on a server. Some even identify the operating system and version. Nmap is a very popular and powerful port scanner. See http://www.insecure.org for more information.

Password Crackers

There are many password crackers available via the Internet. Two of the most popular are L0phtcrack and John The Ripper. L0phtcrack can crack the Windows NT and 2000 SAM database to reveal passwords. It can accomplish this in two steps: first it uses a database of passwords to quickly crack commonly used passwords, then it cracks the remaining passwords via brute force. John the Ripper can be used with a variety of operating systems, such as Windows, UNIX, etc. See http://www.atstake.com or http://www.openwall.com/john/ for more information.

Password Grinders

Password grinders allow attackers to target a machine that requires a username and password login. IIS Web servers using basic authentication or FTP servers are common targets for password grinding. Common tools include webcrack and ftpcrack. See http://www.packetstormsecurity.org for more information.

War Dialers

War dialing is the art of dialing a range of phone numbers to identify modems. These modems can provide a backdoor into a network, avoiding firewalls altogether. Popular war dialers include THC-Scan, ToneLoc, and PhoneSweep. See http://www.packetstormsecurity.org or http://www.sandstorm.net for more information.

Program Password Recovery

Microsoft Word, WinZip, Adobe Acrobat, and other programs provide the means to password protect a document. Elcomsoft provides software that can crack these passwords. In fact, the Russian hacker Dimitri demonstrated the insecurities of Adobe software password protection at the DefCon 2001 conference, and was subsequently arrested by the FBI. See http://www.elcomsoft.com for more information.

Credit Card Number Generators

Validation of credit card numbers is critical to e-commerce. Many credit card number generators are in circulation and they allow a hacker to generate legitimate card numbers and names. Many of these generators are downloadable from hacker sites.

Vulnerability Scanners (broad-based)

Commercial and open source scanners provide a quick and concise way of identifying surface level vulnerabilities. They provide the means to create a baseline for an environment. Some of the most popular scanners include Nessus, ISS Internet Scanner, NAI CyberCop,

and WebTrends Security Analyzer. See http://www.nessus.org, http://www.iss.net, http://www.nai.com, or http://www.webtrends.com for more information respectively.

Packet Sniffers

Packet sniffing can allow anyone with a network connection to sniff the LAN. Capturing unencrypted packets can allow an intruder to capture usernames, passwords, and confidential data such as emails. Ethereal is a very popular open-source packet sniffer. See http://www.ethereal.com for more information.

NetBIOS Auditing Tools

NetBIOS auditing tools exist that allow an attacker to identify Windows NT and Windows 2000 user accounts with no password and available shares. Cerberus Internet Scanner has been around for years, but its simplicity makes it both useful and powerful. See http://www.cerberus-infosec.co.uk/cis.shtml for more information.

Viruses, Trojans, Worms

A computer virus attaches itself to one or more programs and modifies the original code or infects it. Advanced viruses can replicate by infecting other files.

Trojans are typically written with malicious intent and can append unauthorized code within a legitimate program. Typically the program will still perform its original functions, while also running other nefarious functions unknown to the user. Advanced Trojans such as Back Orifice and NetBus can allow complete remote control of a system by an attacker.

A worm is a computer program designed to replicate itself from one machine to another across a network or the Internet. Worms can use resources on a machine, causing significant damage. In extreme cases, servers can be set up to act as agents in distributed Denial of Service attacks. The first documented worm was the Morris Worm written by Robert Morris. In November 1988, Robert Morris was conducting research when he wrote a program that would propagate. At that time the Internet consisted of primarily academic and research centers, but his worm took out over 5000 machines. Recent worms include Code Red and Nimda.

Attack Sample

The DotDot vulnerability in many Microsoft IIS Web servers can allow an attacker to enumerate file directory structure as well as sample files and custom cgi scripts, which may also be exploitable. The root of the problem is the way Microsoft products handle Unicode. Unicode assigns a unique number for every character in every language, regardless of platform or program.

Unicode representations:

```
'/' = %c0%af
'\' = %c1%9c
```

Microsoft did not adhere to the HTTP 1.0 and 1.1 specifications and implemented the forward slash and backward slash as path separators. Therefore, IIS decodes Unicode after path checking, rather than before.

URLs such as the following can possibly list the contents of the root directory on the c:\ drive:

http://address.of.iis5.box/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\

Microsoft publishes numerous patches to counteract this type of activity. In addition, many Intrusion Detection Systems (IDS), such as ISS, provide "rskill" functions that immediately kill these types of connections. An IDS should not be used as a primary means for preventing the activity, but instead, as a means for identifying the activity and where your concerns should be focused.

Defending Against the Hack

Top Ten Ways to Secure Against Attack

Defending your network against attack requires constant vigilance and education. Although there is no recipe for guaranteeing the absolute security of your network, the following ten practices represent the best insurance for your network.

1. Keep patches up to date by installing weekly, or daily if possible.

Buffer overflow and privilege escalation attacks can usually be prevented by keeping patches up-to-date. Check your vendor's site daily for new patch releases and monitor the Computer Emergency Response Team's site, http://www.cert.org, for information on the latest vulnerabilities.

2. Shut down unnecessary services/ports.

Review your installation requirements by eliminating unnecessary services and applications. Perform a post-installation lockdown and hardening of the machine. Lance Spitzner, Senior Security Architect for Sun Microsystems, Inc. authors a useful site, http://www.enteract.com/~lspitz, with more information.

3. Change default passwords by choosing strong passwords that utilize uppercase/ lowercase/ numbers/special characters.

Some database applications create a database administrator account with no password. To protect against this vulnerability, test the accounts after install, and if no password is found on any account, disable the account or set a strong password. Weak passwords are not much better than no password at all. Examples of weak passwords include the user's name, birth date, or a dictionary word. Educate your administrators and users about the importance of strong passwords. A strong password should contain upper and lower case letters, as well as numbers and special characters (!, #, $, etc). A strong password should also be at least 7-8 characters in length, depending on operating system. Many operating systems provide means for requiring complex passwords, when enabled. More extreme countermeasures include one-time password mechanisms.

4. Control physical access to systems.

Protecting physical access to computer systems is as important as protecting computer access. Be sure employees lock down consoles when not in use—an unlocked desktop screen can instantly allow a hacker access to the network as a privileged user. A hacker may also gain access to the network via a network jack in a conference room or any non-restricted area. Data centers and network closets should be treated with vigilance as well. Even a locked door may not be enough protection in the face of a determined attacker. Alarms, video cameras, raised floors, security guards, customer accessible cages, biometric scans, and ID cards may be necessary to adequately defend against network attacks.

5. Curtail unexpected input.

Some Web pages allow users to enter usernames and passwords. These Web pages can be used maliciously by allowing the user to enter in more than just a username.

```
Username: jdoe; rm  -rf  /
```

This might allow an attacker to remove the root file system from a UNIX Server. Programmers should limit input characters, and not accept invalid characters such as | ; < > as possible input.

6. Perform backups and test them on a regular basis.

7. Educate employees about the risks of social engineering and develop strategies to validate identities over the phone, via e-mail, or in person.

8. Encrypt and password-protect sensitive data.
Data such as Web accessible e-mail should be considered sensitive data and should be encrypted. This will discourage any type of sniffer program or exposure of sensitive company data.

9. Implement security hardware and software.
Firewalls and intrusion detection systems should be installed at all perimeters of the network. Viruses, Java, and ActiveX can potentially harm a system. Anti-virus software and content filtering should be utilized to minimize this threat.

10. Develop a written security policy for the company.

Seven Questions to Test Your Security
The Computer Security Institute (CSI) conducts a computer security survey each year to evaluate the enterprise market's security posture. The 2002 survey respondents included 503 computer security practitioners from U.S. Corporations, government agencies, financial institutions, medical institutions, and universities. The responses to the questions below come from this survey. Ask yourself the following questions as you evaluate your company's network security and susceptibility to attack.

1. Why would anyone want to hack "my" site?
The motivation for access to proprietary information can vary from personal to financial to thrill-seeking. Many companies do not understand what is at risk, until it is too late. 80 percent of the respondents acknowledged financial losses due to computer breaches.

2. I've never been hacked, why should I care?
Many companies are not even aware that they have been invaded until after the fact. 90 percent of the respondents detected computer security breaches within the last twelve months.

3. How do I know if I've been hacked?
You may not know. Web defacements are commonplace, and theft of information is also very common, but rarely detected.

4. What could they possibly gain access to?
Your site could be the target of a Web defacement, vandalism, denial of service, theft, release of private information, or financial fraud.

5. How could it affect my company?
85 percent of the respondents detected computer viruses. 78 percent detected employee abuse of Internet access privileges (downloading pornography, pirated software, and inappropriate use of email systems). 98 percent of the respondents have Web sites, and 38 percent suffered unauthorized access or misuse of their Web sites within the last 12 months.

6. If I have been hacked, are my customers/clients at risk?
13 percent of attacks involved theft of transaction information—but even the theft of less vital information can damage your company's reputation and your customers' trust.

7. I have a firewall, aren't I protected?

65 percent of the interviewed companies reported attacks from inside their own company, and the remaining companies did not know the source. These insiders are often employees of the company or consultants onsite who already have access to the network.

Details of the report can be viewed at: http://www.gocsi.com/press/20020407.html.

Security Training

Reading this white paper on hacking is certainly an effective starting point for preparing against network attack. However, it is just that-a starting point. Security training is a necessary next step. Effective training can help ensure that you take a holistic approach to network security. It will teach you the proper techniques for assessing your network's security, and assist you with developing an effective security policy to manage your organization's risks. It will teach you proper deployment techniques for various security devices, provide you with the skills to audit your security measures, and help you ensure that they have been implemented and are functioning effectively and efficiently.

VeriSign's schedule of security classes is designed to cover many aspects of information security. Our Applied Hacking and Countermeasures class is a key course for security administrators and managers because it presents hacking from a hacker's perspective, and teaches you in detail how to defend against potential attacks. The five-day course is made up of approximately 70 percent labs.

Each student is provided with a laptop containing two operating systems (Windows and Linux) running simultaneously. Students learn to target a variety of systems, as well as other students in the classroom. The attacks simulate everything from reconnaissance, to building and uploading a Trojan horse, and remotely controlling the machine. The deficiencies of default installs and common exploits are explained, and the students are allowed to perform these exploits in class.

The goal is for students to understand their network's security risks by performing a week's worth of hacking in a controlled environment. Countermeasures are covered so that the student gains a better understanding of how to secure their network environment to protect against hacks. The success of this class is based on the premise that understanding how an attack is performed is the most effective way to prevent it. For more information, or to register for classes, visit http://www.verisign.com/training

The Future of Hacking

The future of hacking will be shaped by several trends:

Hacker Tools

Hacker tools are becoming more readily available through an onslaught of publicity and a number of Web sites. In addition, these tools are becoming more powerful through the development of the open-source community. In fact, some open-source tools are more powerful than their commercial counterparts.

Wireless Networks

More companies are moving to wireless networks, and in fact, 85 percent of these companies do not use the built-in encryption. This allows for sniffing outside the physical boundaries of the company and the network. Peter Shipley (http://www.dis.org) demonstrated the insecurities of wireless networks by identifying hundreds of accessible wireless networks in the San Francisco Bay area from 13 miles away.

Viruses and Worms

Viruses and worms are being designed to infect and spread attack tools. Prime examples include Code Red and NIMDA. The attack tools are becoming more stealthy and more difficult to remove once infected. Computer Economics (http://www.computereconomics.com) reported that "the worldwide impact of malicious code was $13.2 billion in the year 2001 alone, with the largest contributors being SirCam at $1.15 Billion, Code Red (all variants) at $2.62 Billion, and NIMDA at $635 million." The Cooperative Association for Internet Data Analysis (http://www.caida.org) found that the Code Red worm affected more than 359,000 servers in less than 14 hours.

Terrorism

Since the September 11, 2001 attacks, terrorism is a reality for everyone and every company. It was documented in USA Today long before the attacks that Osama Bin Laden and his network were using steganography (as defined by the FBI: "an ancient art called steganography, which means covered writing. Steganography was originally used to hide secret messages so they could not be seen. Spies used the technique to hide secret information within innocent documents, such as books or letters, in order to move information past an enemy without detection. Invisible ink is one example of a steganographic process.") to distribute plans for an attack on the U.S. This type of activity is very difficult to trace, because it is designed to be inconspicuous. Ideally, anyone scanning the data will fail to realize that it contains hidden, encrypted data.

Modern steganographers have far more powerful tools than their historic counterparts. Software allows a paranoid sender to embed messages in digitized format, typically audio, video, or still image files, in a hidden, encrypted, and password-protected format. The recipient must know which files contain hidden messages, as well as the password and decryption software to extract the hidden message. Steganography has been popularized in such movies as The Saint and Along Came a Spider. The U.S. government is also concerned about the use of steganography for corporate espionage.

Conclusion

Networks are only as secure as their administrators can make them. Administrators are responsible for the security of the devices that comprise their network. Management is equally responsible for the security of the environment. Without buy-in from executive management, administrators are left to fend for themselves.

Corporate management typically will not buy security without good reason. They need to be educated on the risks of exposure, the cost of downtime, the value of information, and the costs of damage or loss. In other words, they need a cost justification of security as an "insurance policy" or risk management tool. The return on a company's investment in security can only be calculated through a detailed risk assessment that asks and answers the questions "How much is your data worth?" and "What would it cost to restore it?" This quantification of your digital assets serves as the baseline for any future decisions about network security.

Today, there are a variety of resources to assist administrators with thwarting attackers. Many books have been published on hacking, and there are several effective security training courses and conferences available to bolster knowledge and awareness. The challenge of staying current on vulnerabilities and patches is a daunting one for administrators and security professionals; however, it is critical to the protection of data integrity in today's enterprise network. Hackers will never stop hacking. You should never stop defending yourself from attack.

For More Information

· More about VeriSign's education services is available on the VeriSign Web site at http://www.verisign.com/training, or by emailing education@verisign.com or calling 650-426-5310.

· A library of white papers, case studies, and other materials can be found at http://www.verisign.com/enterprise/library/index.html

About the Author

Michael T. Raggo, VeriSign

Michael T. Raggo, CISSP, CCSA, CCSE, CCSI, MCP, SCSA, is a Senior Security Consultant for VeriSign, Inc. As a consultant, Mr. Raggo architects and deploys firewalls, intrusion detection systems, and PKI solutions. In addition, he also performs security assessments and penetration tests. He is also an instructor for VeriSign's security classes including CheckPoint Firewall-1, Strategic E-Commerce Architecture and Security, Open Source Security Tools, and Applied Hacking & Countermeasures.

Mr. Raggo is also a guest speaker at nationwide conferences including MISTI's WebSec. Prior to joining VeriSign, Mr. Raggo was Supervisor of System Administration for www.nasdaq.com at the NASDAQ Stock Market. Mr. Raggo has 15 years experience in the information systems field including experience as a UNIX System Administrator, Network Administrator, and Firewall Administrator.

Mr. Raggo conducted graduate work in Information Systems at Johns Hopkins University. Prior to that, he earned his BSET in Electrical Engineering from the Rochester Institute of Technology.

VeriSign, Inc.
487 E. Middlefield Road
Mountain View, California 94043
http://www.verisign.com