Global Knowledge™

Expert Reference Series of White Papers

Ten Ways Hackers Breach Security

Ten Ways Hackers Breach Security

James Michael Steward, Global Knowledge Instructor

Introduction

Hacking, cracking, and cyber crimes are hot topics these days and will continue to be for the foreseeable future. However, there are steps you can take to reduce your organization's threat level. The first step is to understand what risks, threats, and vulnerabilities currently exist in your environment. The second step is to learn as much as possible about the problems so you can formulate a solid response. The third step is to intelligently deploy your selected countermeasures and safeguards to erect protections around your most mission-critical assets. This white paper discusses ten common methods hackers use to breach your existing security.

1. Stealing Passwords

Security experts have been discussing the problems with password security for years. But it seems that few have listened and taken action to resolve those problems. If your IT environment controls authentication using passwords only, it is at greater risk for intrusion and hacking attacks than those that use some form of multi-factor authentication.

The problem lies with the ever-increasing abilities of computers to process larger amounts of data in a smaller amount of time. A password is just a string of characters, typically only keyboard characters, which a person must remember and type into a computer terminal when required. Unfortunately, passwords that are too complex for a person to remember easily can be discovered by a cracking tool in a frighteningly short period of time. Dictionary attacks, brute force attacks, and hybrid attacks are all various methods used to guess or crack passwords. The only real protection against such threats is to make very long passwords or use multiple factors for authentication. Unfortunately, requiring ever longer passwords causes a reversing of security due to the human factor. People simply are not equipped to remember numerous long strings of chaotic characters.

But even with reasonably long passwords that people can remember, such as 12 to 16 characters, there are still other problems facing password-only authentication systems. These include:

- People who use the same password on multiple accounts, especially when some of those accounts are on public Internet sites with little to no security.
- People who write their passwords down and store them in obvious places. Writing down passwords is often encouraged by the need to frequently change passwords.
- The continued use of insecure protocols that transfer passwords in clear text, such as those used for Web surfing, e-mail, chat, file transfer, etc.
- The threat of software and hardware keystroke loggers.
- The problem of shoulder surfing or video surveillance.

Password theft, password cracking, and even password guessing are still serious threats to IT environments. The best protection against these threats is to deploy multifactor authentication systems and to train personnel regarding safe password habits.

2. Trojan Horses

A Trojan horse is a continuing threat to all forms of IT communication. Basically, a Trojan horse is a malicious payload surreptitiously delivered inside a benign host. You are sure to have heard of some of the famous Trojan horse malicious payloads such as Back Orifice, NetBus, and SubSeven. But the real threat of Trojan horses is not the malicious payloads you know about, its ones you don't. A Trojan horse can be built or crafted by anyone with basic computer skills. Any malicious payload can be combined with any benign software to create a Trojan horse. There are countless ways of crafting and authoring tools designed to do just that. Thus, the real threat of Trojan horse attack is the unknown.

The malicious payload of a Trojan horse can be anything. This includes programs that destroy hard drives, corrupt files, record keystrokes, monitor network traffic, track Web usage, duplicate e-mails, allow remote control and remote access, transmit data files to others, launch attacks against other targets, plant proxy servers, host file sharing services, and more. Payloads can be grabbed off the Internet or can be just written code authored by the hacker. Then, this payload can be embedded into any benign software to create the Trojan horse. Common hosts include games, screensavers, greeting card systems, admin utilities, archive formats, and even documents.

All a Trojan horse attack needs to be successful is a single user to execute the host program. Once that is accomplished, the malicious payload is automatically launched as well, usually without any symptoms of unwanted activity. A Trojan horse could be delivered via e-mail as an attachment, it could be presented on a Web site as a download, or it could be placed on a removable media (memory card, CD/DVD, USB stick, floppy, etc.). In any case, your protections are automated malicious code detection tools, such as modern anti-virus protections and other specific forms of malware scanners, and user education.

3. Exploiting Defaults

Nothing makes attacking a target network easier than when that target is using the defaults set by the vendor or manufacturer. Many attack tools and exploit scripts assume that the target is configured using the default settings. Thus, one of the most effective and often overlooked security precautions is simply to change the defaults.

To see the scope of this problem, all you need to do is search the Internet for sites using the keywords "default passwords". There are numerous sites that catalog all of the default user names, passwords, access codes, settings, and naming conventions of every software and hardware IT product ever sold. It is your responsibility to know about the defaults of the products you deploy and make every effort to change those defaults to non-obvious alternatives.

But it is not just account and password defaults you need to be concerned with, there are also the installation defaults such as path names, folder names, components, services, configurations, and settings. Each and every possible customizable option should be considered for customization. Try to avoid installing operating systems into the default drives and folders set by the vendor. Don't install applications and other software into their "standard" locations. Don't accept the folder names offered by the installation scripts or wizards. The more

you can customize your installations, configurations, and settings, the more your system will be incompatible with attack tools and exploitation scripts.

4. Man-in-the-Middle Attacks

Every single person reading this white paper has been a target of numerous man-in-the-middle attacks. A MITM attack occurs when an attacker is able to fool a user into establishing a communication link with a server or service through a rogue entity. The rogue entity is the system controlled by the hacker. It has been set up to intercept the communication between user and server without letting the user become aware that the misdirection attack has taken place. A MITM attack works by somehow fooling the user, their computer, or some part of the user's network into re-directing legitimate traffic to the illegitimate rogue system.

A MITM attack can be as simple as a phishing e-mail attack where a legitimate looking e-mail is sent to a user with a URL link pointed towards the rogue system instead of the real site. The rogue system has a look-alike interface that tricks the user into providing their logon credentials. The logon credentials are then duplicated and sent on to the real server. This action opens a link with the real server, allowing the user to interact with their resources without the knowledge that their communications have taken a detour through a malicious system that is eavesdropping on and possibly altering the traffic.

MITM attacks can also be waged using more complicated methods, including MAC (Media Access Control) duplication, ARP (Address Resolution Protocol) poisoning, router table poisoning, fake routing tables, DNS (Domain Name Server) query poisoning, DNS hijacking, rogue DNS servers, HOSTS file alteration, local DNS cache poisoning, and proxy re-routing. And that doesn't mention URL obfuscation, encoding, or manipulation that is often used to hide the link misdirection.

To protect yourself against MITM attacks, you need to avoid clicking on links found in e-mails. Furthermore, always verify that links from Web sites stay within trusted domains or still maintain SSL encryption. Also, deploy IDS (Intrusion Detection System) systems to monitor network traffic as well as DNS and local system alterations.

5. Wireless Attacks

Wireless networks have the appeal of freedom from wires - the ability to be mobile within your office while maintaining network connectivity. Wireless networks are inexpensive to deploy and easy to install. Unfortunately, the true cost of wireless networking is not apparent until security is considered. It is often the case that the time, effort, and expense required to secure wireless networks is significantly more than deploying a traditional wired network.

Interference, DOS, hijacking, man-in-the-middle, eavesdropping, sniffing, and many more attacks are made simple for attackers when wireless networks are present. That doesn't even mention the issue that a secured wireless network (802.11a or 802.11g) will typically support under 14 Mbps of throughput, and then only under the most ideal transmission distances and conditions. Compare that with the standard of a minimum of 100 Mbps for a wired network, and the economy just doesn't make sense.

However, even if your organization does not officially sanction and deploy a wireless network, you may still have wireless network vulnerabilities. Many organizations have discovered that workers have taken it upon themselves to secretly deploy their own wireless network. They can do this by bringing in their own wireless

access point (WAP), plugging in their desktop's network cable into the WAP, then re-connecting their desktop to one of the router/switch ports of the WAP. This retains their desktop's connection to the network, plus it adds wireless connectivity. All too often when an unapproved WAP is deployed, it is done with little or no security enabled on the WAP. Thus, a $50 WAP can easily open up a giant security hole in a multi-million dollar secured-wired network.

To combat unapproved wireless access points, a regular site survey needs to be performed. This can be done with a notebook using a wireless detector such as NetStumbler or with a dedicated hand-held device.

6. Doing their Homework

I don't mean that hackers break into your network by getting their school work done, but you might be surprised how much they learn from school about how to compromise security. Hackers, especially external hackers, learn how to overcome your security barriers by researching your organization. This process can be called reconnaissance, discovery, or footprinting. Ultimately, it is intensive, focused research into all information available about your organization from public and non-so-public resources.

If you've done any research or reading into warfare tactics, you are aware that the most important weapon you can have at your disposal is information. Hackers know this and spend considerable time and effort acquiring a complete arsenal. What is often disconcerting is how much your organization freely contributes to the hacker's weapon stockpile. Most organizations are hemorrhaging data; companies freely give away too much information that can be used against them in various types of logical and physical attacks. Here are just a few common examples of what a hacker can learn about your organization, often in minutes:

- The names of your top executives and any flashy employees you have by perusing your archive of press releases.
- The company address, phone number, and fax number from domain name registration.
- The service provider for Internet access through DNS lookup and traceroute.
- Employee home addresses, phone numbers, employment history, family members, previous addresses, criminal record, driving history, and more by looking up their names in various free and paid background research sites.
- The operating systems, major programs, programming languages, specialized platforms, network device vendors, and more from job site postings.
- Physical weaknesses, vantage points, lines of sight, entry ways, covert access paths, and more from satellite images of your company and employee addresses.
- Usernames, e-mail addresses, phone numbers, directory structure, filenames, OS type, Web server platform, scripting languages, Web application environments, and more from Web site scanners.
- Confidential documents accidentally posted to a Web site from archive.org and Google hacking.
- Flaws in your products, problems with staff, internal issues, company politics, and more from blogs, product reviews, company critiques, and competitive intelligence services.

As you can see, there is no end to the information that a hacker can obtain from public open sources. This list of examples is only a beginning. Each kernel of truth discovered often leads the hacker to unearth more. Often, a hacker will spend over 90% of their time in information-gathering activities. The more the attacker learns about the target, the easier the subsequent attack becomes.

As for defense, you are ultimately at a loss—mainly because it is already too late. Once information is out on the Internet, it is always out there. You can obviously clean up and sterilize any information resource currently

under your direct control. You can even contact third-party information repositories to request that they change your information. Some online data systems, such as domain registrars, offer privacy and security services (for a fee, of course). You can also control or limit the output of information in the future by being more discrete in your announcements, product details, press releases, etc.

However, it is the information that you can't change or remove from the Internet that will continue to erode your security. The only way to manage uncontrollable information is to alter your environment so that it is no longer correct or relevant. Think of this as a new way to deviate from defaults or at least deviate from the previous known.

7. Monitoring Vulnerability Research

Hackers have access to the same vulnerability research that you do. They are able to read Web sites, discussion lists, blogs, and other public information services about known problems, issues, and vulnerabilities with hardware and software. The more the hacker can discover about possible attack points, the more likely it is that he can discover a weakness you've yet to patch, protect, or even become aware of.

To combat vulnerability research on the part of the hacker, you have to be just as vigilant as the hacker. You have to be looking for the problems in order to protect against them just as intently as the hacker is looking for problems to exploit. This means keeping watch on discussion groups and web sites from each and every vendor whose products your organization utilizes. Plus, you need to watch the third-party security oversight discussion groups and web sites to learn about issues that vendors are failing to make public or that don't yet have easy solutions. These include places like securityfocus.com, US CERT, hackerstorm.com, and hackerwatch.org.

8. Being Patient and Persistent

Hacking into a company network is not typically an activity someone undertakes and completes in a short period of time. Hackers often research their targets for weeks or months, before starting their first tentative logical interactions against their target with scanners, banner-grabbing tools, and crawling utilities. And even then, their initial activities are mostly subtle probing to verify the data they gathered through their intensive "offline" research. Once hackers have crafted a profile of your organization, they must then select a specific attack point, design the attack, test and drill the attack, improve the attack, schedule the attack, and, finally, launch the attack.

In most cases, a hacker's goal is not to bang on your network so that you become aware of their attacks. Instead, a hacker's goal is to gain entry subtly so that you are unaware that a breach has actually taken place. The most devastating attacks are those that go undetected for extended periods of time, while the hacker has extensive control over the environment. An invasion can remain undetected nearly indefinitely if it is executed by a hacker who is patient and persistent. Hacking is often most successful when performed one small step at a time and with significant periods of time between each step attempt - at least up to the point of a successful breach. Once hackers have gained entry, they quickly deposit tools to hide their presence and grant them greater degrees of control over your environment. Once these hacker tools are planted, hidden, and made active, the hackers are free to come and go as they please.

Likewise, protecting against a hacker intrusion is also about patients and persistence. You must be able to watch even the most minor activities on your network with standard auditing processes as well as an auto-

mated IDS/IPS system. Never allow any anomaly to go uninvestigated. Use common sense, follow the best business practices recommended by security professionals, and keep current on patches, updates, and system improvements.

However, realize that security is not a goal that can be fully obtained. There is no perfectly secure environment. Every security mechanism can be fooled, overcome, disabled, bypassed, exploited, or made worthless. Hacking successfully often means the hacker is more persistent than the security professional protecting an environment. Ultimately, it is an arms race to see who blinks or falls behind first. With enough time, the right tools, sufficient expertise and skill, mounting information collection, and persistence, a hacker can and will find a way to breach any and every security system.

9. Confidence Games

The good news about hacking today is that many security mechanisms are very effective against most hacking attempts. Firewalls, IDSes, IPSes, and anti-malware scanners have made intrusions and hacking a difficult task. However, the bad news is many hackers have expanded their idea of what hacking means to include social engineering: hackers are going after the weakest link in any organization's security—the people.

People are always the biggest problem with security because they are the only element within the secured environment that has the ability to choose to violate the rules. People can be coerced, tricked, duped, or forced into violating some aspect of the security system in order to grant a hacker access. The age-old problem of people exploiting other people by taking advantage of human nature has returned as a means to bypass modern security technology.

Protection against social engineering is primarily education. Training personnel about what to look for and to report all abnormal or awkward interactions can be effective countermeasures. But this is only true if everyone in the organization realizes that they are a social engineering target. In fact, the more a person believes that their position in the company is so minor that they would not be a worthwhile target, the more they are actually the preferred targets of the hacker.

10. Already Being on the Inside

All too often when hacking is discussed, it is assumed that the hacker is some unknown outsider. However, studies have shown that a majority of security violations actually are caused by internal employees. So, one of the most effective ways for a hacker to breach security is to be an employee. This can be read in two different ways. First, the hacker can get a job at the target company and then exploit that access once they gain the trust of the organization. Second, an existing employee can become disgruntled and choose to cause harm to the company as a form of revenge or retribution.

In either case, when someone on the inside decides to attack the company network, many of the security defenses erected against outside hacking and intrusion are often ineffective. Instead, internal defenses specific to managing internal threats need to be deployed. This could include keystroke monitoring, tighter enforcement of the principle of least privilege, preventing users from installing software, not allowing any external removable media source, disabling all USB ports, extensive auditing, host-based IDS/IPS, and Internet filtering and monitoring.

Conclusion

There are many possible ways that a hacker can gain access to a seemingly secured environment. It is the responsibility of everyone within an organization to support security efforts and to watch for abnormal events. We need to secure IT environments to the best of our abilities and budgets while watching for the inevitable breach attempt. In this continuing arms race, vigilance is required, persistence is necessary, and knowledge is invaluable.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:
Essentials of Network Security
Certified Ethical Hacker (CEH)
Foundstone Essentials of Hacking
Foundstone Ultimate Hacking
Foundstone Ultimate Hacking: Expert

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

James Michael Stewart has been working with computers and technology for more than 20 years. As a Global Knowledge Instructor he has been teaching CEH and CHFI courses. He has also focused on Windows 2003/XP/2000, certification, and security in the classroom. In addition, Michael has authored numerous books on security, certification, and administration topics. He is a regular instructor at Interop. Michael holds the following certifications: CISSP, ISSAP, SSCP, MCT, CEI, CEH, CHFI, TICSA, CIW SA, Security+, MCSE+Security Windows 2000, MCSA Windows Sever 2003, MCDST, MCSE NT & W2K, MCP+I, Network+, iNet+.