

# Hacking Security

**Ruchi Bajaj**  
M.E. (I.T), U.I.E.T  
Panjab University, Chandigarh  
[ruchibajaj7@gmail.com](mailto:ruchibajaj7@gmail.com)

**Veenu Mangat**  
Lecturer, U.I.E.T  
Panjab University, Chandigarh  
[veenumangat@yahoo.com](mailto:veenumangat@yahoo.com)

***Abstract: Hacking, cracking, and cyber crimes are hot topics these days regarding information security and will continue to be in near future. When the World Wide Web was mainly used to send e-mail and view remote data, the main concern was amateur hackers devising ways to break into large systems for bragging rights. Hackers are almost impossible to eliminate. As one group is caught, another replaces them. In this paper, I will briefly explain some of the ways hackers use to breach security***

## I. INTRODUCTION

Hacking, cracking, and cyber crimes are hot topics these days and will continue to be in near future. When the world wide web was mainly used to send e-mail and view remote data, the main concern was amateur hackers devising ways to break into large systems for bragging rights [1]. Hackers are almost impossible to eliminate. As one group is caught, another replaces them [2].

There are steps one can take to reduce threat level. [3]

- 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.

The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders as of the year 2000 categorized following five offenses as cyber-crime [4]:

1. Unauthorized access
2. Damage to computer data or programs
3. Sabotage to hinder the functioning of a computer system or network
4. Unauthorized interception of data to, from and within a system or network
5. And computer espionage

“Hackers are computer professionals, with skills... Hackers built the Internet. A person who breaks into other people's computer systems to get a kick out of it or who intent to cause harm is a “cracker” [4].

A hacker is a very talented programmer, respected by his peers. A true hacker can find plenty of useful projects to work on; breaking things is more a characteristic of children of any age. The basic difference is this: hackers build things; crackers break them. Many journalists and writers have been fooled into using the word “hacker” to describe “crackers” [4]

‘Hacking’ here in this document actually means cracking. Rogers discusses types of hackers, classifying them into groups ranging from novice hackers, to disgruntled ex-employees, to professional criminals, to cyber-terrorists high tech crimes such as phishing and pharming attacks are generally committed by professional hackers. [5] There’s ‘pharming’, where hackers attack the server computers where legitimate Web sites are housed. Type in the address of the legitimate site and you are redirected to a look-alike. Government websites are the hot targets of the hackers due to the press coverage, it receives.

## II. WHAT IS HACKING?

Hacking in simple terms means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use readymade computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Hackers are classified into groups ranging from novice hackers, to disgruntled ex-employees (the group that commits most computer crime), to professional criminals, to cyber-terrorists [10]. High tech crimes such as phishing and pharming attacks are generally committed by professional hackers [5]. There’s ‘pharming,’ where hackers attack the server computers where legitimate Web sites are housed. Type in the address of the legitimate site and you are redirected to a look-alike [11].

*Why hacking? : “Motive behind the Crime” [4]*

- Greed: Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.
- Power
- Publicity Hackers enjoy the media coverage.

- Revenge
- Adventure
- Desire to access forbidden information
- Destructive mindset Wants to sell n/w security services

### III. HOW IS HACKING ORGANIZED: THE SEVEN STEPS FOLLOWED FOR HACKING

In general, these procedures fall in one of the following seven steps [10]: reconnaissance, probe, toehold, advancement, stealth, listening post, and takeover, where each step is enabled or helped by its previous steps and prepares for its following steps. These seven steps can serve as a procedural classification of hacking techniques because the hacking techniques used in each step are for the same purpose and share many common characteristics.

1. reconnaissance: to gather information of the target
2. probe: is to detect the weakness of target system in order to deploy hacking tools
3. toehold: to exploit security weaknesses and gain entry into the system
4. advancement: to advance from an unprivileged account to a privileged one
5. stealth: is to hide the penetration tracks
6. listening post: is to install back doors to establish a listening post
7. takeover: is to expand control from one host to other hosts in the network

### IV. SOME COMMON WAYS OF BREACHING SECURITY

The 10 most common ways used to breach security are Stealing Passwords, Trojan Horses, Exploiting Defaults, Man-in-the-Middle Attacks, Wireless Attacks, Doing their Homework, Monitoring Vulnerability Research, Being Patient and Persistent, Confidence Games, Already Being on the Inside.[3]

#### A.. STEALING PASSWORDS

Computers have increased in complexity and ability, but humans have not responded the same way. It is relatively easy for an administrator to increase the security a system, but it is difficult for an administrator to make users act in a more secure manner. Mechanisms like increasing password complexity requirements often only lead to users writing down password and reusing the same password on multiple systems. [9]

Security experts have been discussing the problems with password security for years. If you control authentication using passwords only, it is at greater risk for intrusion and hacking attacks than those that use some form of multifactor 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.

The perfect user will have different passwords for each different account, and he or she will be able to remember 8 to 10 character length passwords with uppercase, lowercase, special characters, and numbers. If this is the case, the perfect user is not realistically human. [9]

Therefore users perform various techniques to help themselves:

- Writing the passwords down on paper
- Saving them in a text file on their computer
- Using the same password for multiple systems
- Creating password patterns.

This helps the user, but it also helps an attacker trying to break the same passwords. If an attacker compromises a computer and discovers an unencrypted text file containing passwords to that user's various accounts, complete identity theft can occur. The same can also happen to users who write down their passwords on paper and lose it. [9].

Requiring ever longer passwords causes a reversing of security due to the human factor. 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.
- 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.

#### B. TROJAN HORSES

Criminal computer attacks grew at an alarming rate in 2004 [8]. In their 2005 Internet security threat report [6]. Symantec reported that out of the top ten

spyware programs, six were bundled with other programs [7].

A Trojan horse is a malicious payload surreptitiously delivered inside a benign host. 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. The malicious payload of a Trojan horse can be 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 even 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 can be delivered via e-mail as an attachment, it can be presented on a Web site as a download, or it can 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.

### *C. 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 one 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 user responsibility to know about the defaults of the products he deploy and make an effort to change those defaults.

But it is not just account and password defaults one need to be concerned with, there are also the installation defaults such as path names, folder names, components, services, configurations, and settings. 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 one can customize the installations, configurations, and settings, the more his system will be incompatible with attack tools and exploitation scripts.

### *D. 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.

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.

### *E. 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. 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 low cost 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 or with a dedicated hand-held device.

#### *F. DOING THEIR HOMEWORK*

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. 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. Most organizations 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 top executives and any flashy employees you have by perusing your archive of press releases.
- The address, phone number, and fax number from domain name registration.
- 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.

There is no end to the information that a hacker can obtain from public open sources. 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, one is ultimately at a loss - mainly because it is already too late. Once information is out on the Internet, it is always out there. One can obviously clean up and sterilize any information resource currently under the direct control. One 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. One can also control or limit the output of information in the future by being more discrete in announcements, product details, press releases, etc made.

However, it is the information that one can't change or remove from the Internet that will continue to erode security. The only way to manage uncontrollable information is to alter one's 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.

#### *G. MONITORING VULNERABILITY RESEARCH*

Hackers have access to the same vulnerability research that someone else can 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.

#### *H. BEING PATIENT AND PERSISTENT*

Hacking is not typically an activity someone undertakes and completes in a short period of time. Hackers often research their targets for weeks or months. And even then, their initial activities are mostly subtle probing to verify the data they gathered through their intensive "offline" research. In most cases, 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 patience and persistence. One must be able to watch even the most minor activities on your network with standard auditing processes as well as an automated 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

### *I. 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.

### *J. 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 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

In this paper, we discussed some common ways hackers use to breach security and some of the preventive techniques to protect ourselves from getting hacked

### REFERENCES

- [1] Determining the Proper Response to Online Extortion  
Anne Payton, Kennesaw State University, USA
- [2] PROBLEMS, KNOWLEDGE, SOLUTIONS:  
SOLVING COMPLEX PROBLEMS  
Enid Mumford, Emeritus Professor, Manchester Business School, United Kingdom
- [3] Ten Ways Hackers Breach Security
- [4] Hacking And Cybercrime  
Nataliya B. Sukhai, ACM, InfoSecCD Conference'04, October 8, 2004, Kennesaw, GA, USA
- [5] Identity Fraud Profiles: Victims and Offenders  
Wagner, Nicole; Management of eBusiness, 2007. WCMeb 2007.11-13 July 2007 Page(s):22 - 22
- [6] Symantec. Symantec internet security threat report, trends, january 05 - june 05, 2005.
- [7]Hunting Trojan Horses  
Micha Moffie, Winnie Cheng, David Kaeli, Qin Zhao, ACM ASID'06 October 21, 2006, San Jose, California, USA.
- [8] Bruce Schneier. **Attack trends** 2004 and 2005. In ACM, Queue vol. 3, no. 5. ACM, Jun. 2005.
- [9] A Global Look at Authentication  
Hamilton, Stephen S.; Carlisle, Martin C.; Hamilton, John A., IEEE SMC, 20-22 June 2007 Page(s):1 - 8