Hacking

Sagar More
Department of MCA, PK Technical Campus
MCA 2nd year student.
snmore1990@gmail.com
9970565243

Abstract- *Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose. A hacker is basically someone who breaks into computer networks or standalone personal computer. The Internet allows the hackers to take files, programs, passwords, and other information from users that are using it. They use this as a tool to make it easier to beat a system. Most hackers start hacking as a way to create mischief and to have fun, but with time it may become an addiction and may cause serious damage opposing to the law.*

There are three types of hackers described in the information, white hat, black hat, and gray hat hackers. This paper outlines the differences and social structures of each type. This paper explains that hacking is unauthorized use or attempt to circumvent or bypass the security mechanisms of an information system or network for the thrill of learning and "looking around" or for the malicious intent of gathering information for gain, data corruption, or access to a system. The information used illustrates what cautions and actions used by companies to prevent attacks and security breaches. The research paper concludes on a note that good auditing and consideration of security measures from time to time and vigilance intrusion detecting and good systems administration can be very effective ways of securing and fortifying the company's network.

1. Introduction

Hacking is unauthorized use of computer and network resources. The process of attempting to gain or successfully gaining, unauthorized access to computer resources for the purpose of help or break system is called hacking.

The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. As with most technological advances, there is also a dark side: criminal hackers. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo, hack their website, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. With these concerns and others, the ethical hacker can help.

Companies lose millions of dollars due to bad security practices. More and more users are using the Internet every day and a very small percentage of them know how to defend themselves. It is important to understand how hackers get into systems in order to beat them at their own game. By knowing the tools and tricks of the trade that hackers use, one is better able to defend against an attack. This paper will also talk about a standard attack plan that most attackers follow, defensive programs, how to maximize security, and also how the law punishes convicted offenders of hacking.

2. Types of Hacking

1) Inside Jobs - Most security breaches originate inside the network that is under attack. Inside jobs include stealing passwords (which hackers then use or sell), performing industrial espionage, causing harm (as disgruntled employees), or committing simple misuse. Sound policy enforcement and observant employees who guard their passwords and PCs can thwart many of these security breaches.

2) Rogue Access Points - Rogue access points (APs) are unsecured wireless access points that outsiders can easily breech. (Local hackers often advertise rogue APs to each other.) Rogue APs are most often connected by well-meaning but ignorant employees.

3) Back Doors - Hackers can gain access to a network by exploiting back door administrative shortcuts, configuration errors, easily deciphered passwords, and unsecured dial-ups. With the aid of computerized searchers (bots), hackers can probably find any weakness in your network.

4) Viruses and Worms - Viruses and worms are self-replicating programs or code fragments that attach themselves to other programs (viruses) or machines (worms). Both viruses and worms attempt to shut down networks by flooding them with massive amounts of bogus traffic, usually through e-mail.

5) Trojan Horses - Trojan horses, which are attached to other programs, are the leading cause of all break-ins. When a user downloads and activates a Trojan horse, the hacked software (SW) kicks off a virus, password gobbler, or remote-control SW that gives the hacker control of the PC.

6) Denial of Service - DoS attacks give hackers a way to bring down a network without gaining internal access. DoS attacks work by flooding the access routers with bogus traffic (which can be e-mail or Transmission Control Protocol, TCP, packets).
Distributed DoSs (DDoS5) are coordinated DoS attacks from multiple sources. A DDoS is more difficult to block because it uses multiple, changing, source IP addresses.

7) Anarchists, Crackers, and Kiddies -
Anarchists are people who just like to break stuff. They usually exploit any target of opportunity. Crackers are hobbyists or professionals who break passwords and develop Trojan horses or other SW (called warez). They either use the SW themselves (for bragging rights) or sell it for profit. Script kiddies are hacker wannabes. They have no real hacker skills, so they buy or download warez, which they launch.
8) Sniffing and Spoofing - Sniffing refers to the act of intercepting TCP packets. This interception can happen through simple eavesdropping or something more sinister.
Spoofing is the act of sending an illegitimate packet with an expected acknowledgment (ACK), which a hacker can guess, predict, or obtain by snooping.

3. Hacker versus Cracker

Hacker : A Hacker is a person who is interested in the working of any computer operating system. Most often, Hackers are programmers. Hackers obtain advanced knowledge of operating systems and programming languages. They may know various security holes within systems and the reasons for such holes. Hackers constantly seek further knowledge, share what they have discovered, and they never have intentions about damaging or stealing data.

Cracker: A Cracker is a person who breaks into other people systems, with malicious intentions. Crackers gain unauthorized access, destroy important data, stop services provided by the server, or basically cause problems for their targets. Crackers can easily be identified because their actions are malicious. Whatever the case, most people give Hacker a negative outline. Many malicious Hackers are electronic thieves. Just like anyone can become a thief, or a robber, anyone can become a Hacker, regardless of age, gender, or religion. Technical skills of Hackers vary from one to another. Some Hackers barely know how to surf the Internet, whereas others write software that other Hackers depend upon.

4. Types of Hackers on the basis of activities performed by them:

White Hat Hacker: A White Hat Hacker is computer guy who perform Ethical Hacking. These are usually security professionals with knowledge of hacking and the Hacker toolset and who use this knowledge to locate security weaknesses and implement countermeasures in the resources. They are also known as an Ethical

Hacker or a Penetration Tester. They focus on Securing and Protecting IT Systems.

Black Hat Hacker: A Black Hat Hacker is computer guy who performs Unethical Hacking. These are the Criminal Hackers or Crackers who use their skills and knowledge for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote machines, with malicious intent. These are also known as an Unethical Hacker or a Security Cracker. They focus on Security Cracking and Data stealing.

Grey Hat Hacker: A Grey Hat Hacker is a Computer guy who sometimes acts legally, sometimes in good will, and sometimes not. They usually do not hack for personal gain or not have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits. They are hybrid between White Hat and Black Hat Hackers.

Hactivism: Another type of Hackers are Hacktivists, who try to broadcast political or social messages through their work. A Hacktivist wants to raise public awareness of an issue. Examples of hacktivism are the Web sites that were defaced with the Jihad messages in the name of Terrorism.

Cyber Terrorist: There are Hackers who are called Cyber Terrorists, who attack government computers or public utility infrastructures, such as power stations and air-traffic-control towers. They crash critical systems or steal classified government information. While in a conflict with enemy countries some government start Cyber war via Internet.

Ethical Hacking: Ethical Hacking is testing the resources for a good cause and for the betterment of technology. Technically Ethical Hacking means penetration testing which is focused on Securing and Protecting IT Systems. Ethical Hacking also known as Penetration Testing or White-Hat Hacking involves the same Tools, Tricks and Techniques that Hackers use, but with one major difference: Ethical hacking is Legal. Ethical hacking is performed with the target's permission. The intent of Ethical Hacking is to discover vulnerabilities from a Hacker's viewpoint so systems can be better secured. Ethical Hacking is part of an overall information Risk Management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

5. Why Hackers Hack?

The main reason why Hackers hack is because they can hack. Hacking is a casual hobby for some Hackers, they just hack to see what they can hack and what they can't hack, usually by testing their own systems. Many Hackers are the guys who get kicked out of corporate and government IT and security organizations. They try to bring down the status of the organization by attacking or stealing information. The knowledge that malicious Hackers gain and the ego that comes with that knowledge is like an addiction. Some Hackers want to make your life miserable, and others simply want to be famous. Some common motives of malicious Hackers are revenge, curiosity, boredom, challenge, theft for financial gain, blackmail, extortion, and corporate work pressure.

Steps Performed by Hackers

- Performing Reconnaissance
- Scanning and Enumeration
- Gaining access
- Maintaining access and Placing Backdoors
- Covering tracks or Clearing Logs

Phase I: Reconnaissance

Reconnaissance can be described as the pre-attack phase and is a systematic attempt to locate, gather, identify, and record information about the target. The Hacker seeks to find out as much information as possible about the target.

Phase II: Scanning and Enumeration

Scanning and enumeration is considered the second pre-attack phase. This phase involves taking the information discovered during reconnaissance and using it to examine the network. Scanning involves steps such as intelligent system port scanning which is used to

determine open ports and vulnerable services. In this stage the attacker can use different automated tools to discover system vulnerabilities.

Phase III: Gaining Access
This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the Hacker uses for an exploit can be a local area network, local access to a PC, the Internet, or offline. Gaining access is known in the Hacker world as owning the system. During a real security breach it would be this stage where the Hacker can utilize simple techniques to cause irreparable damage to the target system.

Phase IV: Maintaining Access and
Placing Backdoors Once a Hacker has gained access; they want to keep that access for future exploitation and attacks. Sometimes, Hackers harden the system from other Hackers or security personnel by securing their exclusive access with Backdoors, Rootkits, and Trojans. The attacker can use automated scripts and automated tools for hiding attack evidence and also to create backdoors for further attack.

Phase V: Clearing Tracks
In this phase, once Hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. At present, many successful security breaches are made but never detected. This includes cases where firewalls and vigilant log checking were in place.

Working of an Ethical Hacker :
Obeying the Ethical Hacking Commandments:
Every Ethical Hacker must follow few basic principles. If he do not follow, bad things can happen. Most of the time these principles get ignored or forgotten when planning or executing ethical hacking tests. The results are even very dangerous.

Working ethically:
The word ethical can be defined as working with high professional morals and principles. Whether you're performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical Hacker must be approved and must support the company's goals. No hidden agendas are allowed!
Trustworthiness is the ultimate objective. The misuse of information is absolutely not allowed. That's what the bad guys do.

Respecting privacy:
Treat the information you gather with complete respect. All information you obtain during your testing from Web-application log files to clear-text passwords must be kept private.

Executing the plan:
In Ethical hacking, Time and patience are important. Be careful when you're performing your ethical hacking tests. A Hacker in your network or an employee looking over your shoulder may watch what's going on. This person could use this information against you. It's not practical to make sure that no Hackers are on your systems before you start. Just make sure you keep everything as quiet and private as possible.
This is especially critical when transmitting and storing your test results. You're now on a reconnaissance mission. Find as much information as possible about your organization and systems, which is what malicious Hackers do. Start with a broad view of mind and narrow your focus. Search the Internet for your organization's name, your computer and network system names, and your IP addresses. Google is a great place to start for this.
Don't take ethical hacking too far, though. It makes little sense to harden your systems from unlikely attacks. For instance, if you don't have a internal Web server running, you may not have to worry too much about. However, don't forget about insider threats from malicious employees or your friends or colleagues!

6. Prevention from Hackers

Q. What can be done to prevent Hackers from finding new holes in software and exploiting them?

Ans: Information security research teams exist to try to find these holes and notify vendors before they are exploited. There is a beneficial competition occurring between the Hackers securing systems and the Hackers breaking into those systems. This competition provides us with better and stronger security, as well as more complex and sophisticated attack techniques

Defending Hackers create Detection Systems to track attacking Hackers, while the attacking Hackers develop bypassing techniques, which are eventually resulted in bigger and better detecting and tracking systems. The net result of this interaction is positive, as it produces smarter people, improved security, more stable software, inventive problem-solving techniques, and even a new economy.

Now when you need protection from Hackers, whom you want to call? Answer is "The Ethical Hackers". An Ethical Hacker possesses the skills, mindset, and tools of a Hacker but is also trustworthy. Ethical Hackers perform the hacks as security tests computer systems. As Hackers expand their knowledge, so should you. You must think like them to protect your systems from them. You, as the ethical Hacker, must know activities Hackers carry out and how to stop their efforts. You should know what to look for and how to use that information to thwart Hackers' efforts. You don't have to protect your systems from everything. You can't.

The only protection against everything is to unplug your computer systems and lock them away so no one can touch them—not even you.

That's not the best approach to information security. What's important is to protect your systems from known Vulnerabilities and common Hacker attacks. It's impossible to overcome all possible vulnerabilities of your systems. You can't plan for all possible attacks especially the ones that are currently unknown which are called Zero Day Exploits. These are the attacks which are not known to the world. However in Ethical Hacking, the more combinations you try — the more you test whole systems instead of individual units — the better your chances of discovering vulnerabilities.

7. Safety Tips

Here are five simple tips that will help Protect Your Online Accounts

a. Use strong passwords: Using strong passwords is the best way to ensure your social media accounts don't get hacked by a spammer or someone who wants to embarrass you. That's why it's so important to have a unique password for each of your accounts. Creating strong passwords is fairly easy – just remember to combine letters, numbers and symbols that require pressing the Shift key. It's also a good idea to change your passwords once in a while, like every two months.

Using strong passwords to **protect your online accounts** is a good start, but it will not protect you from serious hackers that rely on malware like keyloggers to steal your data. If your computer is infected with a keylogger, the hacker will have access to everything you type, including your passwords. Protecting your computer will help. You can also use strong passwords when protecting your home wireless connection.

Include post letters and numbers interchanged Try not to have "dictionary words." Basically try to have a random set of letters, like cga57g. If your password is made up of all words you can search for in the dictionary and find, someone can get your password using a dictionary hack.

- Make sure your password is long, about 15 characters in length. Otherwise, a hacker could use a brute force hack to get into your account.
- Spaces help, a lot. Even if your password is "theacp", making it "the acp", will increase the strength of it ten-fold.
- Don't use the same password for multiple accounts. Put a different number or symbol for each account added onto a base password if you can't remember different passwords. For

example, "theacp" could turn into: theacp1,the@acp, the*acp, theacp!, etc…….

- Never enter your password into a page someone links you to, it may be a phishing site. Instead, make sure you go to the correct web page to be certain that your account information is secure.

b. Protect your computer

Protecting your computer is a vital part of securing your online accounts. You need to have solid security software to prevent more advanced hackers from accessing your online accounts and other sensitive data. There are many security suites available today, both paid and free. As a rule, it's best to have a couple of different security programs installed on your computer, for example an anti-virus and an antimalware application. In addition to that, it's always good to replace the Windows firewall with a more advanced one. Remember that you shouldn't have two anti-virus programs installed at once because they might conflict with each other. Update your security software daily and scan your computer weekly to make sure there are no infections. Protect your online accounts include protecting your computer as they both rely on each other for safety.

c. Keep an eye on running processes

Every single program, whether visible or hidden, launches a process that is displayed in the Windows Task Manager. So if you think that your computer is infected, you should check running processes. It's also good to monitor running processes on a regular basis.

Windows 7 has a pretty decent task manager (press Ctrl+Shift+Esc to open it), but it's still best to use a third party application, such as the free Sysinternal's Process Explorer or Auslogics Task Manager. These programs provide more details than the built-in task manager and can help you nip malware in the bud.

Some infections have a habit of masking themselves as Windows processes, such as svchost.exe and lsass.exe. So it's always good to check your processes on Fileinspet.com, a Windows process library, and check their path.

c. Download with care : Do you like downloading free stuff from the Internet? I bet you do. But sometimes downloading free stuff can be dangerous. While a lot of free downloads are perfectly fine and come from legitimate sources, many are infected. They are designed to wreak your computer and steal your data. Never download anything that looks suspicious and stick to legitimate free downloads, be it software, songs, or videos.

d.Be careful when using unprotected public networks

We all love using free Wi-Fi in cafes and libraries. While they are great for browsing the web and reading the news, it's not a good idea to use them for online banking, shopping and sometimes even email. These networks are unprotected, which means that a hacker sitting in the same cafe can easily access all of your open accounts and steal your passwords using special software. That's why you should always take extra care and watch out for any strange activity. GMail users are lucky, because GMail tells you if more than two computers are using your account at the same time – just look below your messages to access this information.

Acknowledgement
We are thankful to Dr. Manoj Devare, Head of MCA department at PK Technical campus, Chakan, Pune. Without his guidance, motivation and support we would not have submitted this paper to EITBM 2012.

References:

[1] http://en.wikipedia.org/wiki/Hacker_%28computer_security%29
[2] http://en.wikipedia.org/wiki/Hacker
[3] www.secpoint.com/types-of-hacker.html
[4]www.myipaddressinfo.com/typeofhacking.htm