4.1. Introduction to Ethical Hacking

Ethical hackers are usually security professionals or network penetration testers who use their hacking skills and toolsets for defensive and protective purposes. Ethical hackers who are security professionals test their network and systems security for vulnerabilities using the same tools that a hacker might use to compromise the network. Any computer professional can learn the skills of ethical hacking.

The term cracker describes a hacker who uses their hacking skills and toolset for destructive or offensive purposes such as disseminating viruses or performing denial-ofservice (DoS) attacks to compromise or bring down systems and networks. No longer just looking for fun, these hackers are sometimes paid to damage corporate reputations or steal or reveal credit card information, while slowing business processes and compromising the integrity of the organization.

Hackers can be divided into three groups:

- **White Hats** -Good guys, ethical hackers
- **Black Hats** - Bad guys, malicious hackers
- **Gray Hats** -Good or bad hacker; depends on the situation

Ethical hackers usually fall into the white-hat category, but sometimes they're former gray hats who have become security professionals and who now use their skills in an ethical manner.

White Hats

White hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures. White-hat hackers are prime candidates for the exam. White hats are those who hack with permission from the data owner. It is critical to get permission prior to beginning any hacking activity. This is what makes a security professional a white hat versus a malicious hacker who cannot be trusted.

Black Hats

Black hats are the bad guys: the malicious hackers or *crackers* who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious. This is the traditional definition of a hacker and what most people consider a hacker to be.

Gray Hats

Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Gray-hat hackers may just be interested in hacking tools and technologies and are not malicious black hats. Gray hats are self-proclaimed ethical hackers, who are interested in hacker tools mostly from a curiosity standpoint. They may want to highlight security problems in a system or educate victims so they secure their systems properly. These hackers are doing their “victims” a favor. For instance, if a weakness is discovered in a service offered by an investment bank, the hacker is doing the bank a favor by giving the bank a chance to rectify the vulnerability.

Ethical hackers are motivated by different reasons, but their purpose is usually the same as that of crackers: they’re trying to determine what an intruder can see on a targeted network or system, and what the hacker can do with that information. This process of testing the security of a system or network is known as a penetration test, or pen test.

Hackers break into computer systems. Contrary to widespread myth, doing this doesn’t usually involve a mysterious leap of hackerly brilliance, but rather persistence and the dogged repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems. A pen test is no more than just performing those same steps with the same tools used by a malicious hacker to see what data could be exposed using hacking tools and techniques.

Many ethical hackers detect malicious hacker activity as part of the security team of an organization tasked with defending against malicious hacking activity. When hired, an ethical hacker asks the organization what is to be protected, from whom, and what resources the company is willing to expend in order to gain protection. A penetration test plan can then be built around the data that needs to be protected and potential risks.

Documenting the results of various tests is critical in producing the end product of the pen test: the pen test report. Taking screenshots of potentially valuable information or saving log files is critical to presenting the findings to a client in a pen test report. The pen test report is a compilation of all the potential risks in a computer or system.

Ethical Hacking Terminology

Threat - An environment or situation that could lead to a potential breach of security.

Ethical hackers look for and prioritize threats when performing a security analysis. Malicious hackers and their use of software and hacking techniques are themselves threats to an organization's information security.

Exploit - A piece of software or technology that takes advantage of a bug, glitch, or vulnerability, leading to unauthorized access, privilege escalation, or denial of service on a computer system. Malicious hackers are looking for exploits in computer systems to open the door to an initial attack. Most exploits are small strings of computer code that, when executed on a system, expose vulnerability. Experienced hackers create their own exploits, but it is not necessary to have any programming skills to be an ethical hacker as many hacking software programs have ready-made exploits that can be launched against a computer system or network. An exploit is a defined way to breach the security of an IT system through a vulnerability.

Vulnerability - The existence of a software flaw, logic design, or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to

the system. Exploit code is written to target a vulnerability and cause a fault in the system in order to retrieve valuable data.

Target of Evaluation (TOE) - A system, program, or network that is the subject of a security analysis or attack. Ethical hackers are usually concerned with high-value TOEs, systems that contain sensitive information such as account numbers, passwords, Social Security numbers, or other confidential data. It is the goal of the ethical hacker to test hacking tools against the high-value TOEs to determine the vulnerabilities and patch them to protect against exploits and exposure of sensitive data.

Attack - An attack occurs when a system is compromised based on a vulnerability. Many attacks are perpetuated via an exploit. Ethical hackers use tools to find systems that may be vulnerable to an exploit because of the operating system, network configuration, or applications installed on the systems, and to prevent an attack.

There are two primary methods of delivering exploits to computer systems:

Remote The exploit is sent over a network and exploits security vulnerabilities without any prior access to the vulnerable system. Hacking attacks against corporate computer systems or networks initiated from the outside world are considered remote. Most people think of this type of attack when they hear the term hacker, but in reality most attacks are in the next category.

Local The exploit is delivered directly to the computer system or network, which requires prior access to the vulnerable system to increase privileges. Information security policies should be created in such a way that only those who need access to information should be allowed access and they should have the lowest level of access to perform their job function. These concepts are commonly referred as “need to know” and “least privilege” and, when used properly, would prevent local exploits. Most hacking attempts occur from within an organization and are perpetuated by employees, contractors, or others in a trusted position. In order for an insider to launch an attack, they must have higher privileges than necessary based on the concept of “need to know.” This can be accomplished by privilege escalation or weak security safeguards.

The Phases of Ethical Hacking

The process of ethical hacking can be broken down into five distinct phases. Later in this book, hacking software programs and tools will be categorized into each of these steps.

An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain entry into a computer system are similar no matter what the hacker's intentions are. Figure illustrates the five phases that hackers generally follow in hacking a computer system.

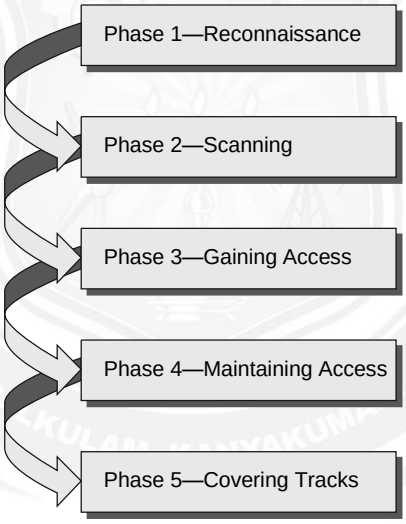

Fig : Phases of hacking

Phase 1: Passive and Active Reconnaissance

Passive reconnaissance involves gathering information about a potential target without the targeted individual's or company's knowledge. Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave. However, most reconnaissance is done sitting in front of a computer.

When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information. Social engineering and

dumpster diving are also considered passive information-gathering methods. Sniffing the network is another means of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing network traffic is similar to building monitoring: a hacker watches the flow of data to see what time certain transactions take place and where the traffic is going. Sniffing network traffic is a common hook for many ethical hackers. Once they use some of the hacking tools and are able to see all the data that is transmitted in the clear over the communication networks, they are eager to learn and see more.

Sniffing tools are simple and easy to use and yield a great deal of valuable information. Many times this includes usernames and passwords and other sensitive data. This is usually quite an eye-opening experience for many network administrators and security professionals and leads to serious security concerns.

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This process involves more risk of detection than passive reconnaissance and is sometimes called rattling the doorknobs. Active reconnaissance can give a hacker an indication of security measures in place but the process also increases the chance of being caught or at least raising suspicion. Many software tools that perform active reconnaissance can be traced back to the computer that is running the tools, thus increasing the chance of detection for the hacker.

Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. For example, it's usually easy to find the type of web server and the operating system (OS) version number that a company is using. This information may enable a hacker to find a vulnerability in that OS version and exploit the vulnerability to gain more access.

Phase 2: Scanning

Scanning involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase include

- ✓ Dialers

- ✓ Port scanners
- ✓ Internet Control Message Protocol (ICMP) scanners
- ✓ Ping sweeps
- ✓ Network mappers
- ✓ Simple Network Management Protocol (SNMP) sweepers
- ✓ Vulnerability scanners

Hackers are seeking any information that can help them perpetrate an attack on a target, such as the following:

- ✦ Computer names
- ✦ Operating system (OS)
- ✦ Installed software
- ✦ IP addresses
- ✦ User accounts

Phase 3: Gaining Access

Phase 3 is when the real hacking takes place. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline. Examples include stackbased buffer overflows, denial of service, and session hijacking. These topics will be discussed in later chapters. Gaining access is known in the hacker world as owning the system because once a system has been hacked, the hacker has control and can use that system as they wish.

Phase 4: Maintaining Access

Once a hacker has gained access to a target system, 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.

Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system.

Phase 5: Covering Tracks

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. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include

- Steganography
- Using a tunneling protocol
- Altering log files

Identifying Types of Hacking Technologies

Many methods and tools exist for locating vulnerabilities, running exploits, and compromising systems. Once vulnerabilities are found in a system, a hacker can exploit that vulnerability and install malicious software. Trojans, backdoors, and rootkits are all forms of malicious software, or malware. Malware is installed on a hacked system after a vulnerability has been exploited.

Buffer overflows and SQL injection are two other methods used to gain access into computer systems. Buffer overflows and SQL injection are used primarily against application servers that contain databases of information.

Most hacking tools exploit weaknesses in one of the following four areas:

Operating Systems : Many system administrators install operating systems with the default settings, resulting in potential vulnerabilities that remain unpatched.

Applications**:** Applications usually aren't thoroughly tested for vulnerabilities when developers are writing the code, which can leave many programming flaws that a hacker can

exploit. Most application development is “feature-driven,” meaning programmers are under a deadline to turn out the most robust application in the shortest amount of time.

Shrink-Wrap Code : Many off-the-shelf programs come with extra features the common user isn’t aware of, and these features can be used to exploit the system. The macros in Microsoft Word, for example, can allow a hacker to execute programs from within the application.

Misconfigurations : Systems can also be misconfigured or left at the lowest common security settings to increase ease of use for the user; this may result in vulnerability and an attack.

Identifying Types of Ethical Hacks

Ethical hackers use many different methods to breach an organization’s security during a simulated attack or penetration test. Most ethical hackers have a specialty in one or a few of the following attack methods. In the initial discussion with the client, one of the questions that should be asked is whether there are any specific areas of concern, such as wireless networks or social engineering. This enables the ethical hacker to customize the test to be performed to the needs of the client. Otherwise, security audits should include attempts to access data from all of the following methods.

Here are the most common entry points for an attack:

Remote Network - A remote network hack attempts to simulate an intruder launching an attack over the Internet. The ethical hacker tries to break or find vulnerability in the outside defenses of the network, such as firewall, proxy, or router vulnerabilities. The Internet is thought to be the most common hacking vehicle, while in reality most organizations have strengthened their security defenses sufficient to prevent hacking from the public network.

Remote Dial-Up Network - A remote dial-up network hack tries to simulate an intruder launching an attack against the client’s modem pools. War dialing is the process of repetitive dialing to find an open system and is an example of such an attack. Many organizations have replaced dial-in connections with dedicated Internet connections so this method is less relevant than it once was in the past.

Local Network - A local area network (LAN) hack simulates someone with physical access gaining additional unauthorized access using the local network. The ethical hacker must gain direct access to the local network in order to launch this type of attack. Wireless LANs (WLANs) fall in this category and have added an entirely new avenue of attack as radio waves travel through building structures. Because the WLAN signal can be identified and captured outside the building, hackers no longer have to gain physical access to the building and network to perform an attack on the LAN. Additionally, the huge growth of WLANs has made this an increasing source of attack and potential risk to many organizations.

Stolen Equipment - A stolen-equipment hack simulates theft of a critical information resource such as a laptop owned by an employee. Information such as usernames, passwords, security settings, and encryption types can be gained by stealing a laptop. This is usually a commonly overlooked area by many organizations. Once a hacker has access to a laptop authorized in the security domain, a lot of information, such as security configuration, can be gathered. Many times laptops disappear and are not reported quickly enough to allow the security administrator to lock that device out of the network.

Social Engineering - A social-engineering attack checks the security and integrity of the organization's employees by using the telephone or face-to-face communication to gather information for use in an attack. Social-engineering attacks can be used to acquire usernames, passwords, or other organizational security measures. Social-engineering scenarios usually consist of a hacker calling the help desk and talking the help desk employee into giving out confidential security information.

Physical Entry - A physical-entry attack attempts to compromise the organization's physical premises. An ethical hacker who gains physical access can plant viruses, Trojans, rootkits, or hardware key loggers (physical device used to record keystrokes) directly on systems in the target network. Additionally, confidential documents that are not stored in a secure location can be gathered by the hacker. Lastly, physical access to the building would allow a hacker to plant a rogue device such as a wireless access point on the network. These devices could then be used by the hacker to access the LAN from a remote location.

ROHINI COLLEGE OF ENGINEERING AND TECHNOLOGY
PALKULAM, KANYAKUMARI
OBSERVE OPTIMIZE OUTSPREAD