



Certified Ethical Hacking

The 5 Phases Every Hacker Must Follow

The 5 Phases Every Hacker Must Follow

Originally, to “hack” meant to possess extraordinary computer skills to extend the limits of computer systems. Hacking required great proficiency. However, today there are automated tools and codes available on the Internet that makes it possible for anyone with a will and desire, to hack and succeed.

Mere compromise of the security of a system does not denote success. There are websites that insist on “taking back the net” as well as those who believe that they are doing all a favor by posting the exploit details. These can act as a detriment and can bring down the skill level required to become a successful attacker.

The ease with which system vulnerabilities can be exploited has increased while the knowledge curve required to perform such exploits has shortened. The concept of the elite/super hacker is an illusion.

However, hackers are generally intelligent individuals with good computer skills, with the ability to create and explore into the computer’s software and hardware. Their intention can be either to gain knowledge or to dig around to do illegal things. Attackers are motivated by the zeal to know more while malicious attackers would intend to steal data. In general, there are five phases in which an intruder advances an attack:

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Covering Tracks

Phase 1—Reconnaissance

Reconnaissance refers to the preparatory phase where an attacker gathers as much information as possible about the target prior to launching the attack. Also in this phase, the attacker draws on competitive intelligence to learn more about the target. This phase may also involve network scanning, either external or internal, without authorization.

This is the phase that allows the potential attacker to strategize his/her attack. This may take some time as the attacker waits to unearth crucial information. Part of this reconnaissance may involve “social engineering.” A social engineer is a person who smooth-talks people into revealing information such as unlisted phone numbers, passwords, and other sensitive information.

Another reconnaissance technique is “dumpster diving.” Dumpster diving is the process of looking through an organization’s trash for discarded sensitive information. Attackers can use the Internet to obtain information such as employee’s contact information, business partners, technologies in use, and other critical business knowledge, but “dumpster diving” may provide them with even more sensitive information such as username, password, credit card statement, bank statement, ATM slip, social security number, telephone number, etc..

For example, a Whois database can provide information about Internet addresses, domain names, and contacts. If a potential attacker obtains DNS information from the registrar, and is able to access it, he/she can obtain useful information such as the mapping of domain names to IP addresses, mail servers, and host information records. It is important that a company has appropriate policies to protect its information assets, and also provide guidelines to its users of the same. Building user awareness of the precautions they must take in order to protect their information assets is a critical factor in this context.

Reconnaissance Types

Reconnaissance techniques can be categorized broadly into active and passive reconnaissance.

When an attacker approaches the attack using passive reconnaissance techniques, he/she does not interact with the system directly. He uses publicly available information, social engineering, and dumpster diving as a means of gathering information.

When an attacker employs active reconnaissance techniques, he/she tries to interact with the system by using tools to detect open ports, accessible hosts, router locations, network mapping, details of operating systems, and applications.

The next phase of attacking is scanning, which is discussed in the following section. Some experts do not differentiate scanning from active reconnaissance. However, there is a slight difference as scanning involves more in-depth probing on the part of the attacker. Often reconnaissance and scanning phases overlap, and it is not always possible to demarcate these phases as watertight compartments.

Active reconnaissance is usually employed when the attacker discerns that there is a low probability that these reconnaissance activities will be detected. Newbies and script kiddies are often found attempting this to get faster, visible results, and sometimes just for the brag value they can obtain.

As an ethical hacker, you must be able to distinguish among the various reconnaissance methods, and be able to advocate preventive measures in the light of potential threats. Companies, on their part, must address security as an integral part of their business and/or operational strategy, and be equipped with proper policies and procedures to check for such activities.

Phase 2 - Scanning

Scanning is the method an attacker performs prior to attacking the network. In scanning, the attacker uses the details gathered during reconnaissance to identify specific vulnerabilities. Scanning can be considered a logical extension (and overlap) of the active reconnaissance. Often attackers use automated tools such as network/host scanners, and war dialers to locate systems and attempt to discover vulnerabilities.

An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as Traceroute. Alternatively, they can use tools such as Cheops to add sweeping functionality along with what Traceroute renders.

Port scanners can be used to detect listening ports to find information about the nature of services running on the target machine. The primary defense technique in this regard is to shut down services that are not required. Appropriate filtering may also be adopted as a defense mechanism. However, attackers can still use tools to determine the rules implemented for filtering.

An attacker follows a particular sequence of steps in order to scan any network. Though a generic approach has been presented, the scanning methods may differ based on the attack objectives, which are set up before the attackers actually begin this process.

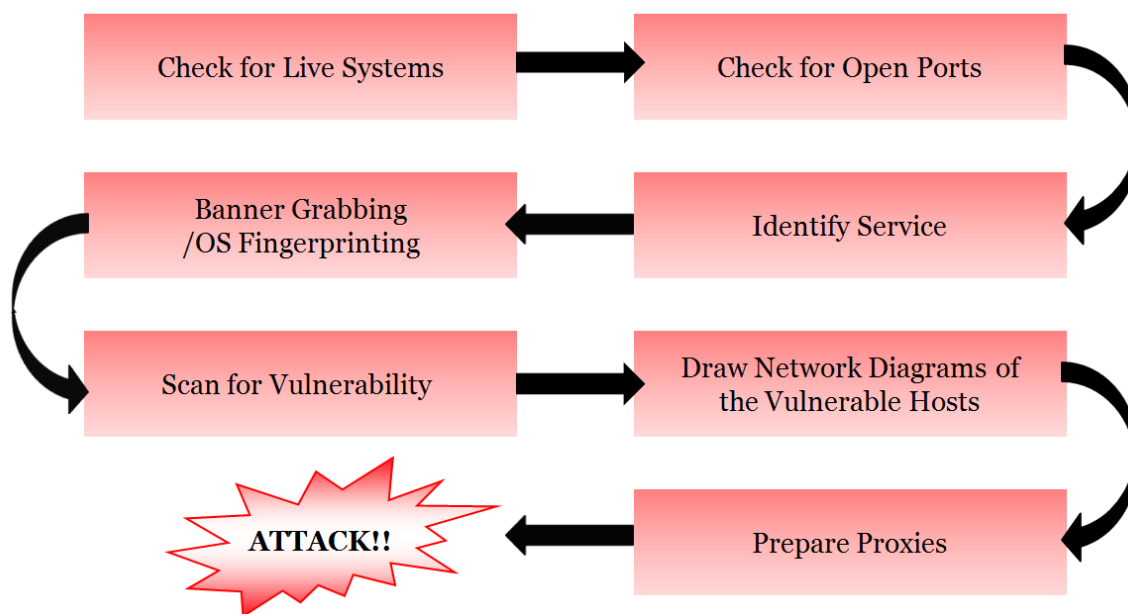


Figure: CEH Scanning Methodology

The most commonly used tools are vulnerability scanners that can search for several known vulnerabilities on a target network, and can potentially detect thousands of vulnerabilities. This gives the attacker the advantage of time because he/she only has to find a single means of entry while the systems' professional has to secure many vulnerable areas by applying patches. Organizations that deploy intrusion detection systems still have reason to worry because attackers can use evasion techniques at both the application and network levels.

Phase 3 - Gaining Access

Gaining access is the most important phase of an attack in terms of potential damage. Attackers need not always gain access to the system to cause damage. For instance, denial-of-service attacks can either exhaust resources or stop services from running on the target system. Stopping of service can be carried out by killing processes, using a logic/time bomb, or even reconfiguring and crashing the system. Resources can be exhausted locally by filling up outgoing communication links.

The exploit can occur locally, offline, over a LAN or the Internet as a deception or theft. Examples include stack-based buffer overflows, denial-of-service, and session hijacking. Attackers use a technique called spoofing to exploit the system by pretending to be strangers or different systems. They can use this technique to send a malformed packet containing a bug to the target system in order to exploit vulnerability. Packet flooding may be used to remotely stop availability of the essential services. Smurf attacks try to elicit a response from the available users on a network and then use their legitimate address to flood the victim.

Factors that influence the chances of an attacker gaining access into a target system include the architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained. The most damaging type of the denial-of-service attacks can be distributed denial-of-service attacks, where an attacker uses zombie software distributed over several machines on the Internet to trigger an orchestrated large scale denial of services.



Phase 4 - Maintaining Access

Once an attacker gains access to the target system, the attacker can choose to use both the system and its resources, and further use the system as a launch pad to scan and exploit other systems, or to keep a low profile and continue exploiting the system. Both these actions can damage the organization. For instance, the attacker can implement a sniffer to capture all network traffic, including telnet and ftp sessions with other systems.

Attackers, who choose to remain undetected, remove evidence of their entry and use a backdoor or a Trojan to gain repeat access. They can also install rootkits at the kernel level to gain super user access. The reason behind this is that rootkits gain access at the operating system level while a Trojan horse gains access at the application level. Both rootkits and Trojans depend on users to install them. Within Windows' systems, most Trojans install themselves as a service and run as local system, which has administrative access.

Attackers can use Trojan horses to transfer user names, passwords, and even credit card information stored on the system. They can maintain control over "their" system for a long time by "hardening" the system against other attackers, and sometimes, in the process, do render some degree of protection to the system from other attacks. They can then use their access to steal data, consume CPU cycles, and trade sensitive information or even resort to extortion.

Organizations can use intrusion detection systems or deploy honeypots and honeynets to detect intruders. The latter though is not recommended unless the organization has the required security professional to leverage the concept for protection.



Phase 5 - Covering Tracks

An attacker would like to destroy evidence of his/her presence and activities for various reasons such as maintaining access and evading punitive action. Erasing evidence of a compromise is a requirement for any attacker who would like to remain obscure. This is one of the best methods to evade trace back. This usually starts with erasing the contaminated logins and any possible error messages that may have been generated from the attack process, e.g., a buffer overflow attack will usually leave a message in the system logs. Next, the attention is turned to effecting changes so that future logins are not logged. By manipulating and tweaking the event logs, the system administrator can be convinced that the output of his/her system is correct, and that no intrusion or compromise has actually taken place.

Since, the first thing a system administrator does to monitor unusual activity, is to check the system log files, it is common for intruders to use a utility to modify the system logs. In some extreme cases, rootkits can disable logging altogether and discard all existing logs. This happens if the intruders intend to use the system for a longer period of time as a launch base for future intrusions. They will then remove only those portions of logs that can reveal their presence.

It is imperative for attackers to make the system look like it did before they gained access and established backdoors for their use. Any files, which have been modified, need to be changed back to their original attributes. Information listed, such as file size and date, is just attribute information contained within the file.

Trojans such as ps or netcat come in handy for any attacker who wants to destroy the evidence from the log files or replace the system binaries with the same. Once the Trojans are in place, the attacker can be assumed to have gained total control of the system. Rootkits are automated tools that are designed to hide the presence of the attacker. By executing the script, a variety of critical files are replaced with trojanned versions, hiding the attacker with ease.

Other techniques include: Steganography and tunneling. Steganography is the process of hiding the data— for instance in images and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another. Even the extra space (e.g. unused bits) in the TCP and IP headers can be used for hiding information. An attacker can use the system as a cover to launch fresh attacks against other systems or use it as a means of reaching another system on the network without being detected. Thus, this phase of attack can turn into a new cycle of attack by using reconnaissance techniques all over again.

Other Resources:

HackerJournals

HACKER JOURNALS
NEWSPAPER

HackerJournals Whitepapers
Computer Security Knowledge base Portal

HackerJournals Vulnerabilities

HackerJournals Magazine 

HackerJournals Blogs

HackerJournals Video



HackerJournals Calendar



CodeRed Center

CEHBLOG

Newsletters