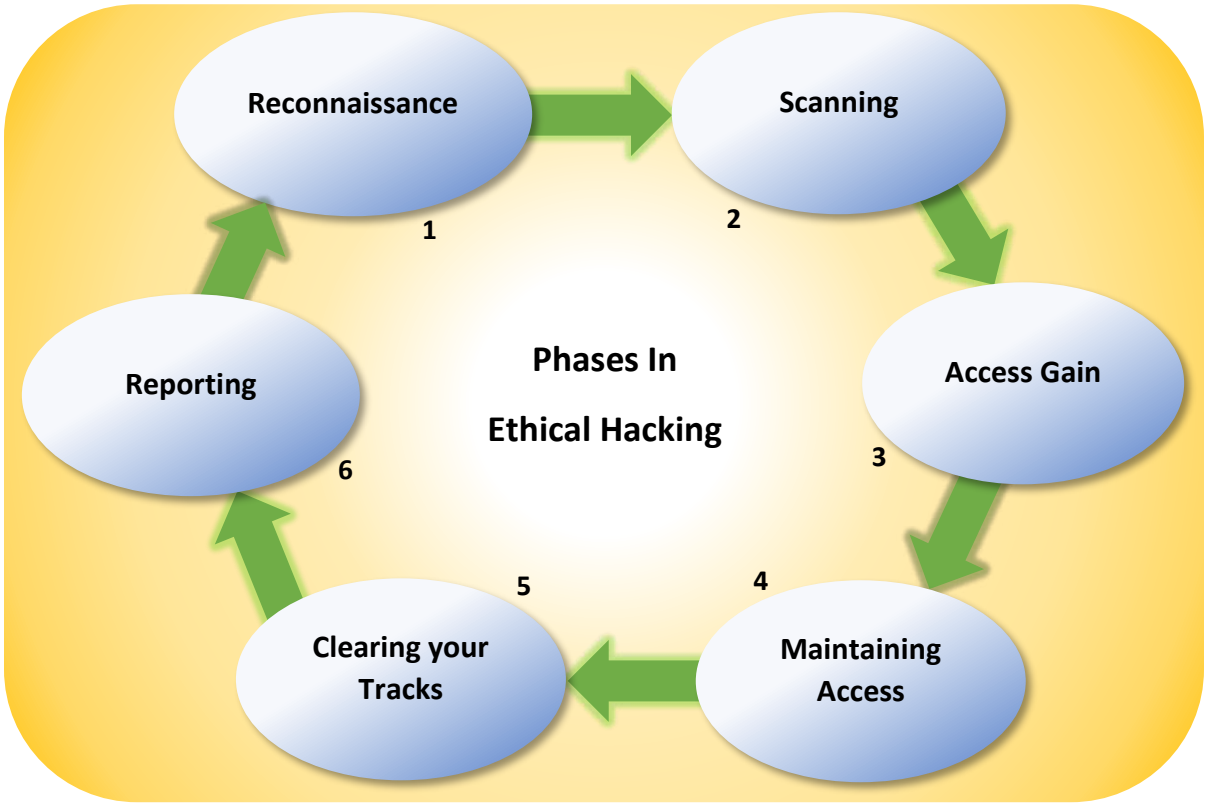
ETHICAL HACKING PROCESS

In Short, Ethical hacking, performed by white hat hackers, is a term used to describe defense hacking for companies and organization, which involves the identification of potential threats on a computer or network.

Like all good projects, ethical hacking too has a set of distinct phases. It helps hackers to make a structured ethical hacking attack.

Different security training manuals explain the process of ethical hacking in different ways, but in my experience, the entire process can be categorized into the following six phases;

1. Reconnaissance.
2. Scanning.
3. Access Gain.
4. Maintain the Access.
5. Clearing your Tracks.
6. Reports.



RECONNAISSANCE

What is Reconnaissance?

From the dictionary meaning, ***Reconnaissance*** is a preliminary survey to gain information; especially: an exploratory military survey of enemy territory. In Cyber-security reconnaissance is a way of gathering targets information using different methods.

When performing a recon exercise on a target there are three main information that ethical hackers make use of;

1. The Network.
2. The Host.
3. Users/People involved.

Steps in Performing a Reconnaissance Exercise.

Information Gathering and getting to know the target systems is the first process in ethical hacking. Reconnaissance is a set of processes and techniques; Foot-printing, Scanning & Enumeration used to discover and collect information about a target.

In recon exercise/phase, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below;

1. Collecting first information.
2. Determine the range of network.
3. Identify active machines.
4. Discover available open ports as well as Aps (Access Points).
5. Fingerprint the Operating System.
6. Look out for services running on various ports.
7. Network Mapping.

Reconnaissance is basically divided into two major parts.

1. **Active Reconnaissance:** Active reconnaissance, involves a direct contact with your target's computer system to gain information and information gotten directly are actually accurate. There's the risk of being caught in the process of active recon without permission. But most hacking activities, require active recon.
2. **Passive Reconnaissance:** In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

Foot-Printing

Foot-printing is more of an effort to map out, at a high level, what the landscape looks like. They are interchangeable terms in CEH parlance, but if you just remember that foot-printing is part of reconnaissance, you'll be fine. During the foot-printing stage, you're looking for any information that might give you some insight into the target, no matter how big or small. Of particular importance are things such as the high-level network architecture (what routers are they using and what servers have they purchased?), the applications and websites (are they public facing?), and the physical security measures (what type of entry control systems present the first barrier, and what routines do the employees seem to be doing daily?). Of course, anything providing information on the employees themselves is always great to have, because the employees represent a gigantic target for you later in the test. Although some of this data may be a little tricky to obtain, most of it is relatively easy to get and is right there in front of you, if you just open your virtual eyes. Just like reconnaissance, foot-printing is of two types; ***Active and Passive Foot-printing.***

During the process, hackers also look out for the following things;

1. Domain Name.
2. IP addresses.
3. Namespaces.
4. Employee Information.
5. Phone Numbers.
6. E-mails.
7. Job Information.

In my next write-up, I will discuss foot-printing in details.

Enumeration

Enumeration in the actual sense is the complete listing of things in an orderly manner with regards to items in a collection. Enumeration is the act of making a list of policies, user accounts, shares and other resources. This step happens just before vulnerability assessment and after scanning. This helps the attacker put together the best strategy for gaining access.

Enumeration can be used to gain information on;

1. Users and Groups
2. Networks and shared paths
3. Hostnames
4. Route Tables
5. Service Settings
6. SNMP port scanning
7. DNS Details Applications and Banners.

Enumeration can be done with the following tools.

In windows Operating System, the use of many tool is done to enumerate NetBIOS names with commands like;

- Net accounts,
- Net config server,
- Net config workstation,
- Net view.

And so much more.

In my next write-up, I will discuss enumeration in detail.

Scanning

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

Gaining Access

In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

Maintaining Access

It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.

Clearing Tracks

This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.

Reporting

Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

This write-up is a definition. The processes will be discussed in details in the coming write-ups