Ethics in IT

Class 9

Lab 1

UNITED TRUST

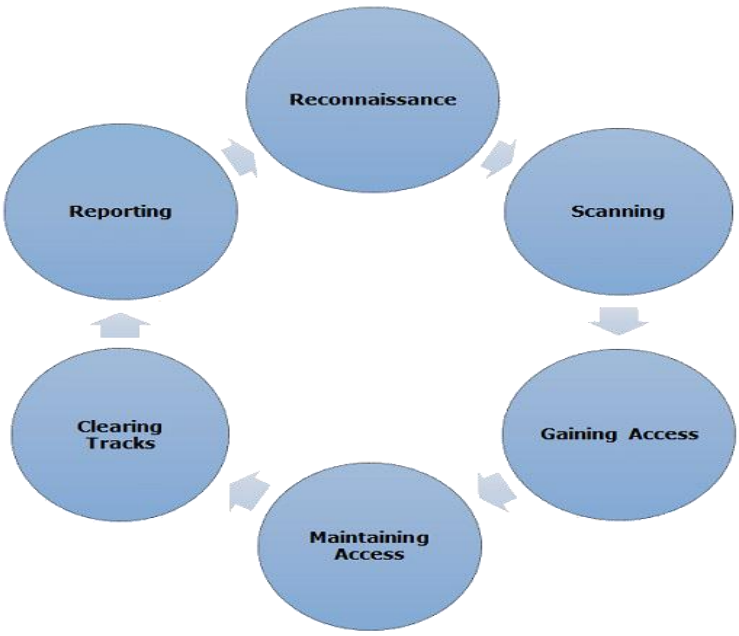
bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

Lab Objectives:

- Ethical hacking process

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 for me as a Certified Ethical Hacker, the entire process can be categorized into the following six phases.



Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means.

The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

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.

Ethical Hacking - Reconnaissance

Information Gathering and getting to know the target systems is the first process in ethical hacking.

Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system

During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below −

√ Gather initial information

√ Determine the network range

√ Identify active machines

√ Discover open ports and access points

√ Fingerprint the operating system

√ Uncover services on ports

√ Map the network

Reconnaissance takes place in two parts − Active Reconnaissance and Passive Reconnaissance.

Active Reconnaissance

In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

Domain Admins, Domain Controllers, Privileged Access, DCSync, Admin Workstations, Admin Delegations, SYSVOL, Passwords, Hashes, System Container, Trust Relationships, rootDSE, SPNs, Kerberos, NTLM, Sites, Subnets, net use, Config Partition, ACLs, Security Permissions, Effective Permissions, Privilege Escalation...

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.