Ethical Hacking

- Ethical hacking also known as penetration testing or white-hat hacking
- It involves the same tools, tricks, and techniques that hackers use
- It is legal
- Used to find flaws in the system in order to take appropriate security measures to protect the data and maintain functionality
- Neither damage the target systems nor steal information
- Evaluate target systems security and report back to owners about the bugs found

What is Penetration Testing?

- An authorized simulated cyber attack on a computer system, performed to evaluate the security of the system
- It is conducted to find the security risk which might be present in the system
- If a system is not secured, then any attacker can disrupt or take authorized access to that system
- Security risk is normally an accidental error that occurs while developing and implementing the software
    - For example, configuration errors, design errors, and software bugs, etc.

Why is Penetration Testing Required?

- Penetration testing is essential because :
  - It identifies a simulation environment i.e., how an intruder may attack the system through white hat attack
  - It helps to find weak areas where an intruder can attack to gain access to the computer’s features and data
  - It supports to avoid black hat attack and protects the original data
  - It estimates the magnitude of the attack on potential business
  - It provides evidence to suggest, why it is important to increase investments in security aspect of technology

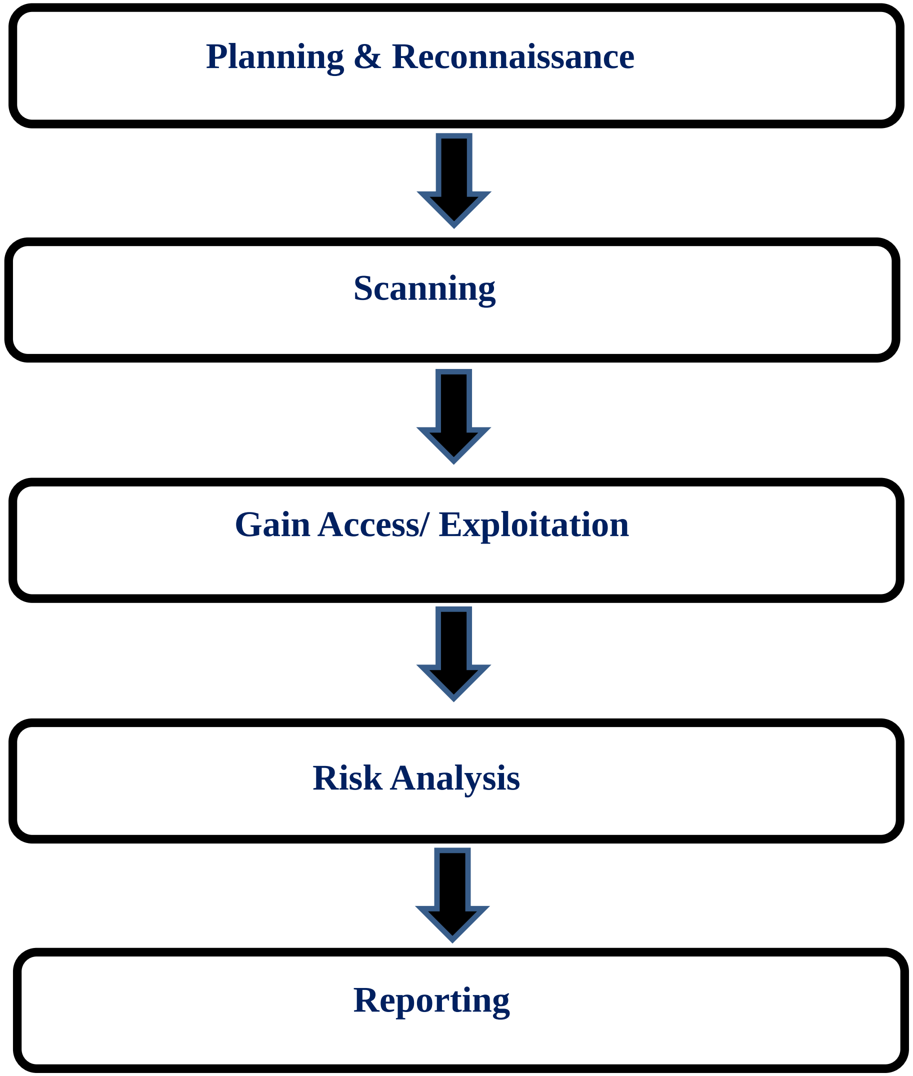
When to Perform Penetration Testing?

- Penetration testing is an essential feature that needs to be performed regularly for securing the functioning of a system
- It should be performed whenever :
  - Security system discovers new threats by attackers
  - You add a new network infrastructure
  - You update your system or install new software
  - You relocate your office
  - You set up a new end-user program/policy

Penetration Testing - Method

- Penetration testing is a combination of techniques that considers various issues of the systems and tests, analyzes, and gives solutions
- It is based on a structured procedure that performs penetration testing step-by-step

Phases of Ethical Hacking / Penetration Testing



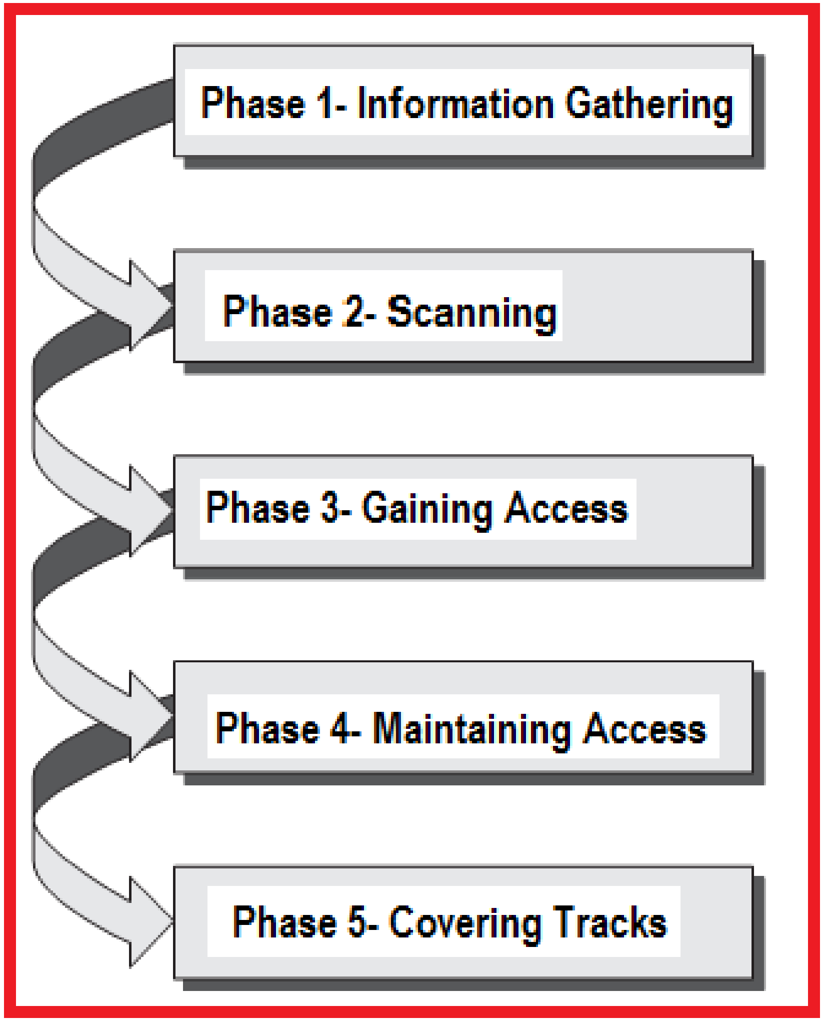
Planning & Reconnaissance

Scanning

Gain Access/ Exploitation

Risk Analysis

Reporting



Phase 1- Information Gathering

Phase 2- Scanning

Phase 3- Gaining Access

Phase 4- Maintaining Access

Phase 5- Covering Tracks

Phases of Ethical Hacking / Penetration Testing

Collecting information: We collect all the information relevant for an attack and examine the company from the perspective of an external attacker.

Identifying vulnerabilities: We determine potential weak points in networks, infrastructure components, mobile end devices and applications.

Exploiting vulnerabilities: We attempt access in the role of an external or internal attacker.

Reporting: We document and analyze the vulnerabilities identified.

Countermeasures: We recommend suitable protective measures and explain the next steps.

Hacking Process

- Footprinting
- Scanning
- Gaining Access
- Maintaining Access

Footprinting

- Also known as **reconnaissance**
- It is the technique used for gathering information about computer systems and the entities they belong to.
- A hacker might use various tools and technologies to get this information
  - **Whois Lookup**
  - **NS Lookup**
  - **IP Lookup**

Scanning

- A set of procedures for identifying live hosts, ports and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network
  - **Port Scanning**
  - **Network Scanning**
  - **Finger Printing**
  - **Fire Walking**

Gaining Access

- Gaining Access also called “**Hacking into the system**”
- It is the process exploiting the loopholes and vulnerabilities in order to breaking the system
  - **Password Attacks**
  - **Social Engineering**
  - **Viruses**

Maintaining Access

- Once an attacker Gaines access into the target system, he can choose to use both the system and the resources as a launched pad to scan and exploit other system
  - **Os BackDoors**
  - **Trojans**
  - **Clears Tracks**

Ethical Hacking Vs. Penetration Testing Vs. Vulnerability Assessment

- Generally, these terms are used interchangeably by many people, either because of misunderstanding or marketing hype
- These terms are different from each other in terms of their objectives and other means
- However, before describing the differences, let us first understand both the terms one-by one

Ethical Hacking Vs. Penetration Testing

Penetration Testing	Ethical Hacking
A narrow term focuses on penetration testing only to secure the security system.	A comprehensive term and penetration testing is one of its features.
A tester needs to have a good knowledge and skills only in the specific area for which he conducts pen testing.	An ethical hacker needs to have a comprehensive knowledge of various software programming and hardware techniques.
Anyone who is familiar with penetration testing can perform pen tests	Usually it required an obligatory certification of ethical hacking
Paper work is less compared to Ethical hacking.	A detailed paper works are required, including legal agreement etc.
To perform this type of testing, less time required.	Ethical hacking involves lot of time and effort compared to Penetration testing.
Access is required only to those systems on which the pen testing will be conducted	Access is required to a wide range of computer systems throughout an IT infrastructure

Penetration Testing Vs. Vulnerability Assessment

Penetration Testing	Vulnerability Assessments
Determines the scope of an attack.	Makes a directory of assets and resources in a given system.
Tests sensitive data collection.	Discovers the potential threats to each resource.
Gathers targeted information and/or inspect the system.	Allocates quantifiable value and significance to the available resources.
Cleans up the system and gives final report.	Attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
It is non-intrusive, documentation and environmental review and analysis.	Comprehensive analysis and through review of the target system and its environment.
It is ideal for physical environments and network architecture.	It is ideal for lab environments.
It is meant for critical real-time systems.	It is meant for non-critical systems.

Hacker and Ethical Hacker

- Hacker
  - Access computer system or network without authorization
  - Breaks the law
- Ethical Hacker
  - Performs most of the same activities but with owner’s permission
  - Employed by companies to perform Penetration Tests

Types of Hackers

- Black Hat Hacker
  - Bad guys
  - Use their skill maliciously for personal gain
  - Hack banks, steal credit cards and deface websites
- White Hat Hacker
  - Good guys
  - Don’t use their skill for illegal purpose
  - Computer security experts and help to protect from Black Hats
- Grey Hat Hacker
  - It is a combination of White hat and Black Hat Hackers
  - Goal of Grey hat hackers is to provide national security

Various Qualities a Hacker Should Posses

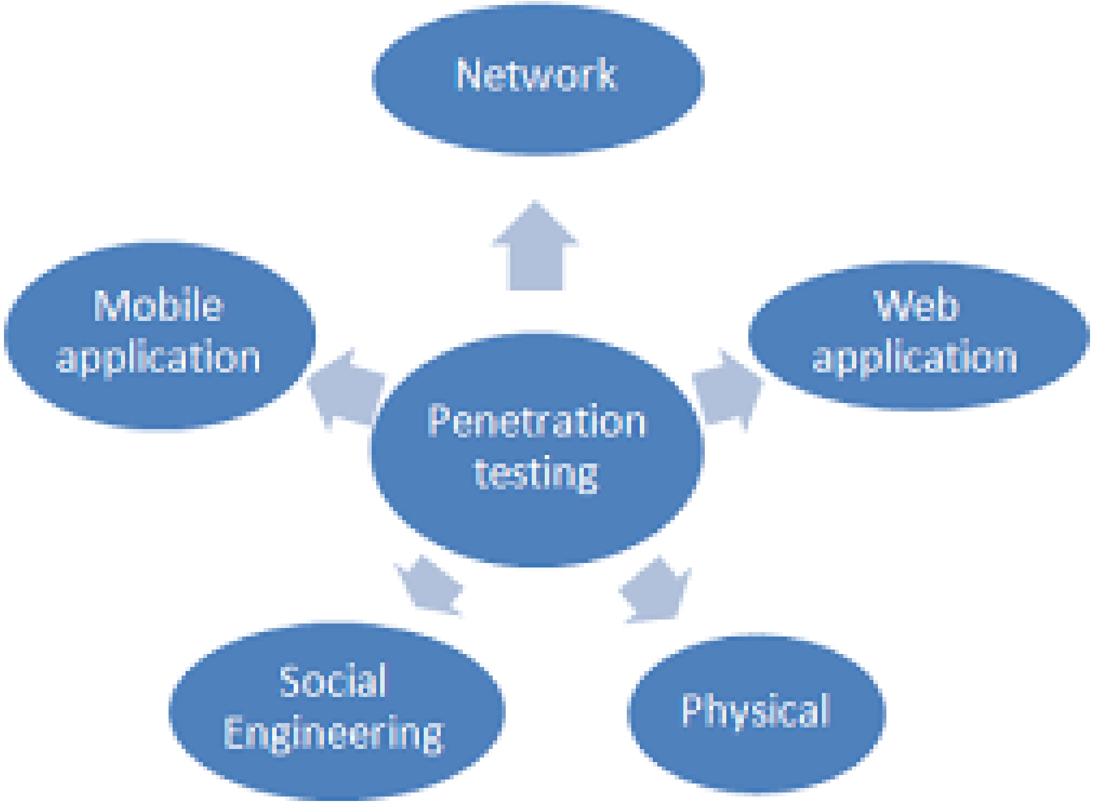
- Good coder
- Well knowledgeable person both hardware as well as software
- Should have knowledge on security system
- Trusted Person

Types of Penetration Testing

- The type of penetration testing normally depends on the scope and the organizational wants and requirements

- Following are the important types of pen testing –
  - Black Box
  - White Box
  - Grey Box

Penetration Testing Services



Penetration Testing - Tools

Tool Name	Purpose	Portability	Expected Cost
Hping	Port Scanning Remote OS fingerprinting	Linux, NetBSD, FreeBSD, OpenBSD, Solaris, Mac OS X, Windows	Free
Nmap	Network Scanning Port Scanning OS Detection	Linux, Windows, FreeBSD, OS X, HP-UX, NetBSD, Sun, OpenBSD, Solaris, IRIX, Mac, etc.	Free
SuperScan	Runs queries including ping, whois, hostname lookups, etc. Detects open UDP/TCP ports and determines which services are running on those ports.	Windows 2000/XP/Vista/7	Free

Penetration Testing – Tools cont.

Tool Name	Purpose	Portability	Expected Cost
p0f	OS fingerprinting Firewall detection	Linux, FreeBSD, NetBSD, OpenBSD, Mac OS X, Solaris, Windows, and AIX	Free
Xprobe	Remote active OS fingerprinting Port Scanning TCP fingerprinting	Linux	Free
Httprint	Web server fingerprinting SSL detection Detect web enabled devices (e.g., wireless access points, switches, modems, routers)	Linux, Mac OS X, FreeBSD, Win32 (command line & GUI)	Free
Nessus	Detect vulnerabilities that allow remote cracker to control/access sensitive data	Mac OS X, Linux, FreeBSD, Apple, Oracle Solaris, Windows	Free to limited edition

Penetration Testing – Tools Cont.

Tool Name	Purpose	Portability	Expected Cost
GFI LANguard	Detect network vulnerabilities	Windows Server 2003/2008, Windows 7 Ultimate/ Vista, Windows 2000 Professional, Business/XP, Sever 2000/2003/2008	Only Trial Version Free
Iss Scanner	Detect network vulnerabilities	Windows 2000 Professional with SP4, Windows Server 2003 Standard with SO1, Windows XP Professional with SP1a	Only Trial Version Free
Shadow Security Scanner	Detect network vulnerabilities, audit proxy and LDAP servers	Windows but scan servers built on any platform	Only Trial Version Free
Metasploit Framework	Develop and execute exploit code against a remote target Test vulnerability of computer systems	All versions of Unix and Windows	Free
Brutus	Telnet, ftp, and http password cracker	Windows 9x/NT/2000	Free

Penetration Testing
Top Tools for Cyber Security Engineers

- Wireshark
- Nmap
- Ncat (Previously Netcat)
- Metasploit
- Nikto
- Burp Suite
- John the Ripper
- Aircrack-ng
- Nessus
- Snort

How to Become a Penetration Tester?

- Stay up to date on recent developments in computer security, reading newsletters and security reports are a good way to do this
- Becoming proficient with C/C++ and a scripting language such as PEARL
- Microsoft, Cisco, and Novell certifications
- Penetration Testing Certifications
    - Certified Ethical Hacker (CEH)
    - GIAC Certified Penetration Tester (GPEN)

Role of a Penetration Tester

- Identify inefficient allocation of tools and technology
- Testing across internal security systems
- Pinpoint exposures to protect the most critical data
- Discover invaluable knowledge of vulnerabilities and risks throughout the infrastructure
- Reporting and prioritizing remediation recommendations to ensure that the security team is utilizing their time in the most effective way, while protecting the biggest security gaps

How to protect the system?

- Patch security hole often
- Encrypt important data (Ex: pgp, ssh)
- Do not run unused daemon
- Remove unused program
- Setup loghost
- Backup the system often
- Setup firewall
- Setup IDS (Ex: snort)

Data Security & Protection

- Data Security technologies includes:
  - Disk Encryption
  - Backups
  - Data Masking
  - Data erasure
- Creating Strong Passwords

What should do after hacked?

- Shutdown or turn off the system
- Separate the system from network
- Restore the system with the backup or reinstall all programs
- Connect the system to the network
- It can be good to call the police