Introduction
To
Ethical Hacking

Learning Goal

- Information Security Overview
- Information Security & Attack Vectors
- Hacking Concepts, Types & Phases
- Ethical Hacking Concepts & Scope
- Information Security Controls
- Information Security Laws & Standards

Essential Terminology

Hack Value

Notion among hackers that **something worth doing**

Vulnerability

Weakness or **implementation error** that can compromise the security of the system

Exploit

A **breach** of system security through vulnerabilities

Payload

Part of an exploit code that performs the intended malicious action

Zero-Day Attack

Exploits **application vulnerabilities** before releasing a patch

Daisy Chaining

Gaining access to one network/computer & then using same information gain access to multiple network/computers

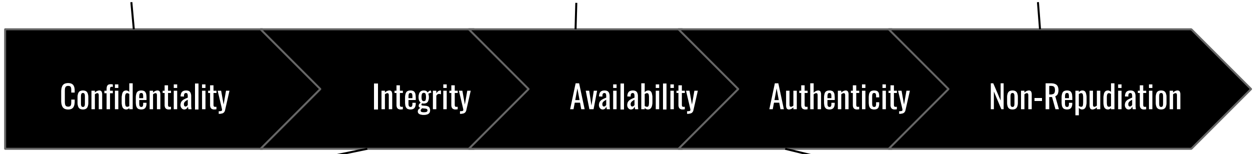
Doxing

Publishing personally identifiable information about an individual collected from public sources

Bot

Remotely controlled application to **execute or automate** predefined task

Elements of Information Security



Confidentiality

Accessible only to those who've **authorized access**

Integrity

Trustworthiness of data or resources in term of unauthorized changes

Availability

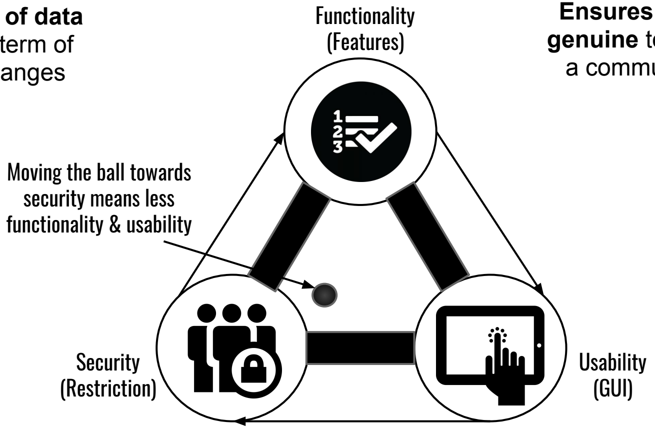
Information is accessible when **required by the authorized user**

Authenticity

Ensures the quality of being genuine to the characteristics of a communication or any data

Non-Repudiation

Guarantee the sender & recipient both **can't deny** sending & receiving the message



Functionality (Features)

Security (Restriction)

Usability (GUI)

Moving the ball towards security means less functionality & usability

Information Security Attack Vectors

- **Cloud Computing Threats**
  - **On-demand delivery of IT capabilities** where sensitive data of organizations & clients stored
- **Advanced Persistent Threats**
  - Attack that **focuses on stealing information from victim machine** without the user being aware of it
- **Viruses & Worms**
  - Most prevalent networking threat that are **capable of infecting a network within seconds**
- **Botnet**
  - A huge **network of compromised systems** used by an intruder to perform various network attacks
- **Insider Attack**
  - An **attack performed on a corporate network** or on a single computer by an **entrusted person(insider)** who has authorized access to the network

Threat Categories & Types of Attacks

Network Threats

- Information Gathering
- Sniffing & Eavesdropping
- Spoofing
- Session hijacking
- DNS & ARP Poisoning
- Password-based Attack
- DOS Attack
- Compromised-key Attack
- Firewall & IDS Attack

Host Threats

- Malware Attacks
- Footprinting
- Password Attacks
- DOS Attacks
- Arbitrary Code Execution
- Unauthorized Access
- Privilege Escalation
- Backdoor Attacks
- Physical Security Threats

Application Threats

- Improper Data/Input Validation
- Authentication & Authorization Attacks
- Security Misconfiguration
- Information Disclosure
- Broken Session Management
- Buffer Overflow
- Cryptography Attacks
- SQL Injection
- Improper Error Handling & Exception Management

Operating System Attacks

Misconfiguration Attacks

Application Level Attacks

Shrink Wrap Code Attacks

Hacking & Hackers

- Refers to **exploiting system vulnerabilities & compromising security** controls to gain unauthorized access to the system resources
- Involves **modifying system** or **application features** to achieve a goal

01
Intelligent individuals with excellent computer skills, with the ability to create & explore into the computer's software & hardware

02
For someone it is a hobby to see how many computers or networks they can compromise

03
Their intention can either be to gain knowledge or to poke around to do illegal things like stealing business data, credit card information, passwords etc

Black Hats

White Hats

Gray Hats

Suicide Hackers

Script Kiddies

Cyber Terrorists

State Sponsored

Hacktivist

Hacking Phases

- **Reconnaissance**
  - **Attacker seeks to gather information** about a target prior to launch attack
  - Noted for ease of entry for attack when the **target is known on a broad scale**
  - **Target range** may include the target organization’s clients, employees, operations, network, and systems
  - **Passive Reconnaissance**
    - Acquiring information without directly interacting with the target
  - **Active Reconnaissance**
    - Interacting with the target directly by any means

- **Scanning**
  - **Pre-Attack Phase**
    - Attacker **scans the network** for specific information on the basis of reconnaissance
  - **Port Scanner**
    - It includes the use of dialers, **port scanners**, network mappers, ping tools, vulnerability scanners, etc.
  - **Extract Information**
    - Attackers extract information such as **live machines**, port, port status, OS details, device type, **system uptime**, etc to launch attack

Hacking Phases

- **Gaining Access**
  - Attacker obtains access to the **operating system or application** on the computer or network
  - Attacker can **escalate privileges** to obtain complete control of the system
  - Attacker can gain access at the **operating system level**, **application level**, or **network level**

  Example include password cracking, buffer overflow, DOS, session hijacking etc.

- **Maintaining Access**
  - Attacker tries to retain his or her **ownership of the system**
  - Attacker may prevent the system from being owned by other attackers by securing their exclusive access with **Backdoors**, **RootKits**, or **Trojans**
  - Attacher can upload, download, or **manipulate data**, applications, and configurations on the **owned system**
  - Attacker use the compromised system to **launch further attacks**

Hacking Phases

- **Clearing Tracks**
  - **Hide malicious acts & activities** carried out by an attacker
  - **Continuing access** to the victim's system, remaining **unnoticed & uncaught**, deleting evidence that might lead to his prosecution
  - Attacker overwrites the server, system, and application logs to **avoid suspicion**

Attackers always cover tracks to hide their identity

Network Security Zoning

❑ Allows an organization **to manage a secure network environment** by selecting the appropriate security levels for different zones of internet & Intranet networks

❑ Helps in effectively monitoring & controlling **inbound and outbound traffic**

- Internet Zone
- Internet DMZ
- Production Network Zone
- Intranet Zone
- Management Network Zone

Security Policies

Promiscuous Policy

No restrictions on usage of system resource

Permissive Policy

Begins wide open & only known **dangerous services/attacks or behaviors** are blocked

Should be updated regularly to be effective

Prudent Policy

Provides **maximum security** while allowing known but necessary dangers

Blocks all services and only safe/necessary services are enabled individually

Everything is logged

Paranoid Policy

Forbids everything, no internet connection, or severely limited internet usage

Network Vulnerability Assessment Methodology

Phase I - Acquisition

- Review **laws & procedures** related to network vulnerability assessment
- **Identify and review document related to network security**
- Review the list of **previously discovered vulnerabilities**

Phase II - Identification

- Conduct **interviews with customers & employees** involved in system architecture design and implementation
- Gather **technical information about all network components**

Phase III - Analyzing

- Review interviews
- **Analyze the results** of previous vulnerability assessment
- Analyze security vulnerabilities & **identify risks**
- Perform **threat & risk analysis**
- Analyze the effectiveness of **existing security controls & policy**

Network Vulnerability Assessment
Methodology

Phase IV - Evaluation

- Determine the probability of exploitation of **identified vulnerabilities**
- Identify the gaps between **existing & required security measures**
- **Determine the controls** required to mitigate the identified vulnerabilities
- **Identified upgrades** required to the network vulnerability assessment process

Phase V - Generating Reports

- Result of analysis must be presented in a **draft report** to be evaluated for further variations
- **Report should contain**:
  - Task rendered by each team member
  - Methods used & findings
  - General and specific recommendations
  - Terms used & their definitions
  - Information collected from all the phases
- All documents must be **stored in a central database** for generating the final report

Penetration Testing

A method of evaluating the security of an information system/network by **simulating an attack to find out vulnerabilities** that an attacker could exploit

Security measures are actively analyzed for design weaknesses, technical flaws & vulnerabilities

It will **point out** the vulnerabilities and will **document** how the weaknesses can be exploited

Results are delivered comprehensively in a **report**, to execute management and technical audiences

“ Blue Teaming/Red Teaming

Blue Teaming

A set of **security responders** performs analysis of an information system to assess the adequacy and efficiency of its security controls

Has **access** to all the organizational resources and information

Detect & mitigate red team(attackers) activities and to anticipate how **surprise attack** might occur

Red Teaming

A team of ethical hackers performs penetration test on an information system with **no or a limited access** to the organization’s limited access

May be conducted **with** or **without** warning

Proposed to **detect network** & **system vulnerabilities** and **check security** from an attacker’s perspective approach to network, system or information access

Types of Penetration Testing

Black-box

No prior knowledge of the infrastructure to be tested

- Blind Testing
- Double Blind Testing

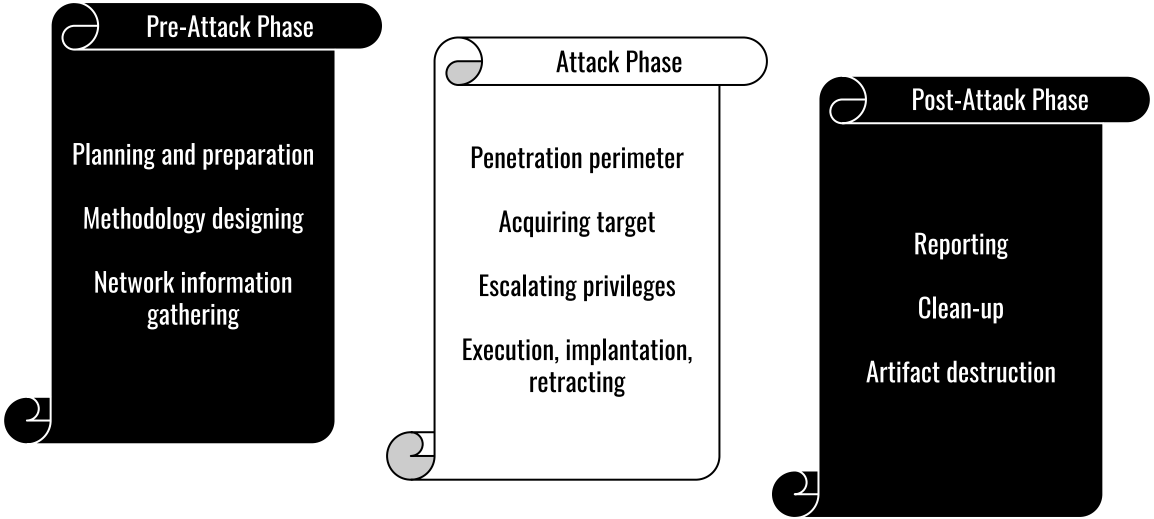
White-box

Complete knowledge of the infrastructure that needs to be tested

Grey-box

Limited knowledge of the infrastructure that needs to be tested

Phases of Penetration Testing



Pre-Attack Phase

Planning and preparation

Methodology designing

Network information gathering

Attack Phase

Penetration perimeter

Acquiring target

Escalating privileges

Execution, implantation, retracting

Post-Attack Phase

Reporting

Clean-up

Artifact destruction

THE END