Course Notes

1 Introduction to Ethical Hacking

1.1 Module Objectives

- Understand elements of information security.
- Understand information security attacks and information warfare.
- Overview of cyber kill chain methodology, TTps, and IoCs.
- Overview of hacking concepts, types, and phases.
- Understanding ethical hacking concepts and its scope.
- Overview of information security controls.
- Overview of information security acts and laws.

1.2 Information Security Overview

1.2.1 Elements of Information Security

- **Confidentiality**
  Confidentiality is the assurance that the information is accessible only to authorized users. Control methods are data classification, data encryption, and proper disposal of equipment.
- **Integrity**
  Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes–the assurance that data is accurate. Control methods are checksums and access control.
- **Availability**
  Availability is the assurance that systems are accessible when required by authorized users. Methods to maintain data availability can include disk arrays for redundant systems and clustered machines, antivirus software to combat malware, and distributed denial-of-service (DDoS) prevention systems.
- **Authenticity**
  Authenticity refers to the characteristics of communication, documents, or any

data that ensures the quality of being genuine or uncorrupted. The major role of authentication is to confirm that the user is genuine. Control methods include biometrics, smart cards, and digital certificates.

- **Non-Repudiation**
  Non-Repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.

1.2.2 Motives, Goals and Objectives of Information Security Attacks

$$\text{Attack} = \text{Motive (Goal)} + \text{Method} + \text{Vulnerability}$$

A motive originates from the notion that the target system stores or processes something valuable, this leads to the threat of an attack on the system.

1.2.3 Motives

- Disrupt business continuity
- Perform information theft
- Manipulate data
- Create fear and chaos by disrupting critical infrastructures
- Bring financial loss to the target
- Propagate religious or political beliefs
- Achieve a state's military Objectives
- Damage the reputation of the target
- Take revenge
- Demand ransom

1.2.4 Classification of Attacks

- Passive Attacks: Monitor network traffic for reconnaissance on network activities using sniffers. used for gathering data useful in active attacks.
- Active Attacks: Tamper with data in transit or disrupt communication or services between systems to bypass or break into secured systems. Attackers launch an attack on the target system by sending traffic actively that can be detected.

- Close-in Attacks: Attacker is in close proximity to the target. Used to gather or modify information or disrupt its access.
- Insider Attacks: Performed by trusted persons who have physical access to critical assets of the target.
- Disruption Attacks: Attackers tamper with hardware or software prior to installation.

1.2.5 Information warfare

Refers to the use of information and communication technologies (ICT) for competitive advantages over an opponent.

- Command and control warfare (C2 warfare)
- Intelligence-based warfare
- Electronic warfare
- Psychological warfare
- Hacker warfare
- Economic warfare
- Cyberwarfare

1.3 Cyber Kill Chain Concepts

The cyber kill chain is a way to illustrate how attacks occur and possible threats at different stages of an attack as well as countermeasures.

1.3.1 Cyber Kill Chain Methodology

A component of intelligence based defense for the identification and prevention of malicious intrusion activities.

Attacks can happen in seven phases:

- Reconnaissance: collection of information about target to probe for weaknesses.
  - Public information on the internet
  - Network information
  - system information
  - organizational information

- Weaponization: identification of vulnerabilities based on data collected.
  - Identify appropriate malware
  - create payload
  - deliver to target
  - leverage exploits
- Delivery: Measures the effectiveness of security controls implemented by the target based on whether or not the intrusion attempt succeeds.
  - Phishing emails
  - USB drives
  - Website attacks
  - Hacking tools against operating systems, applications,...
- Exploitation: Trigger of the malicious code to exploit the vulnerability
- Installation: adversary downloads and installs more malicious software on the target system to maintain access to the network for an extended period.
- Command and Control: adversary creates a command and control channel that establishes two-way communication.
- Actions on Objectives: Adversary controls the victim system and gains access to confidential data, disrupts services or network, or destroys operational capability of the target. May use this as a launching point for new attacks.

1.3.2 Tactics, Techniques, and Procedures (TTPs)

TTPs refer to the patterns of activities and methods associated with specific threat actors.

- Tactics: The way a threat actor operates during the different phases of the attack.
- Techniques: Technical methods used by an attacker to achieve intermediate results during the attack.
- Procedures: Organizational approaches that threat actors follow to launch an attack.

TTP helps identify and profile attackers or APTs and learn more about how attacks occur.

1.3.3 Adversary Behavioral identification

Identification of the common methods or techniques followed by an adversary to launch attacks on or to penetrate an organization's network. Gives security professionals insight into upcoming threats and exploits.

- Internal Reconnaissance: Methods used once inside a target network for enumeration. Monitor activity by checking for unusual commands and packet capturing tools.
- Use of PowerShell: Automating data exfiltration. Can check the PowerShell logs or Windows Event logs.
- Unspecified Proxy activities
- Use of command-line interface
- HTTP user agent
- Command and Control server
- Use of DNS tunneling
- Use of web shell
- Data staging

1.3.4 Indicators of compromise (IoCs)

Clues, artifacts, and pieces of forensic data found on the network or operating system of an organization that indicate a potential intrusion.

- Email Indicators
  - Sender's email address
  - Email subject
  - attachments or links
- Network Indicators
  - URLs
  - Domain names
  - IP addresses
- Host-Based Indicators
  - Filenames

  - File Hashes
  - Registry keys
  - DLLs
  - Mutex
- Behavioral Indicators
  - Document executing PowerShell script
  - Remote command execution

1.3.5 Key Indicators of Compromize (IoCs)

- Unusual outbound network traffic
- Unusual activity through a privileged user account
- Geographical anomalies
- Multiple login failures
- Increased database read volume
- Large HTML response size
- Multiple requests for the same file
- Mismatched port-application traffic
- Suspicious registry or system file changes
- Unusual DNS requests
- Unexpected patching of systems
- Signs of Distributed Denial-of-Service (DDoS) activity
- Bundles of data in the wrong place
- Web traffic win superhuman behavior

1.4 Hacking Concepts