**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

Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to a system's resources. A hacker is a person who breaks into a system or network without authorization for malicious intent.

### 1.4.1 Hacker Classes

- Black Hats: Bad guys
- White Hats: Good guys
- Gray Hats: In between good/bad
- Suicide Hackers: Do not care if they get caught
- Script Kiddies: Unskilled, uses prebuilt tools
- Cyber Terrorists: Religious or political, cause fear.
- State-sponsored hackers: Employed by the government.
- Hacktivist: Promote political agenda

### 1.4.2 Hacking Phases

There are 5 general phases of hacking:

1. Reconnaissance
   Preparation phase to gain as much information about the target as possible prior to launching an attack.
   - Passive: Attacker does not interact with the target directly, relies on publicly available information.
   - Active: Direct interaction with the target. Using tools to scan for open ports, hosts, router locations, network mapping, operating system details, and applications.
2. Scanning (enumeration)
   Uses details from reconnaissance to scan the network for specific information. Scanning is a logical extension of active reconnaissance and often lumped with the reconnaissance phase.
3. Gaining access
   Attacker gains access to the operating system or applications on the network. Examples are password cracking, buffer overflows, denial of service, and session hijacking.
4. Maintaining access
   Attacker tries to retain ownership (root level access) of the system by installing backdoors, rootkits and trojans.

5. Clearing tracks
   Erasing evidence of malicious activities, remain unnoticed and uncaught. Overwrite server, system and application logs to avoid suspicion.

## 1.5 Ethical Hacking Concepts

Ethical hackers follow similar processes as malicious hackers. Ethical hackers are employed to assist organizations in testing network security for possible loopholes and vulnerabilities. The noun hacker refers to a person who enjoys learning the details of computer systems and stretching their capabilities. The verb to hack describes the rapid development of new programs or the reverse engineering of existing software to make it better or more efficient in new and innovative ways. The terms cracker and attacker refer to the persons who employ their hacking skills for offensive purposes. The distinction between ethical hackers and crackers is consent.

### 1.5.1 Why is ethial hacking neccessary

- Prevent hackers from gaining access.
- Uncover vulnerabilities.
- Strengthen security.
- Preventative measures.
- Safeguard data.
- Enhance security awareness.
- What can an intruder see?
- what can an intruder do?
- Does anyone notice?
- Are all components accounted for and patched?
- How much effort would it take to protect the system?
- Are the security measures compliant with legal standards?

### 1.5.2 Scope and limitations

- Scope
  - Risk assessment

  - auditing
  - counter fraud
  - security best practices.
  - highlight remedial actions.
- Limitations
  - Not much to gain without cause.
  - Can only help the organization understand its security system. (Up to organization to implement remediation's).

### 1.5.3 Skills of an Ethical Hacker

- Technical Skills
  - operating systems.
  - networking concepts
  - Computer expert
  - Security areas and related issues
  - How to launch sophisticated attacks.
- Non-technical skills
  - Quickly learn and adapt
  - String work ethic
  - problem solving skills
  - Commitment to organizations security policies
  - Awareness of local standards and laws.

## 1.6 Information security controls

Security controls prevent the occurrence of unwanted events and reduce risk to assets. Basic security concepts are Confidentiality, Integrity, Availability (CIA). Concepts related to users accessing information are authentication, authorization, and non-repudiation. This section covers Information Assurance (IA), defence in depth, risk management, cyber threat intelligence, threat modeling, incident management and AI and ML concepts.

### 1.6.1 Information Assurance (IA)

Assurance of Confidentiality, availability, integrity and authenticity of information and information systems is protected during the usage , processing, storage and transmission of information.

- Develop local policies, processes and guidance.
- Designing network and user authentication strategies.
- Identifying network vulnerabilities and threats.
- Identifying problem and resource requirements.
- Creating plans for identified resource requirements.
- Applying appropriate information assurance controls.
- Performing certification and accreditation
- Providing information assurance training.

### 1.6.2 What is Risk?

Degree of uncertainty or expectation that an adverse event may cause damage to the system. Risks are categorized into different levels according to their estimated impact on the system. A risk matrix is used to scale risk according to the probability, likelihood, and consequence or impact of the risk.

- Probability of the occurrence of a threat or and event that will damage the organization.
- Possibility of a threat acting upon internal or external vulnerability and causing harm to a resource.
- The product of the likelihood that an event will occur and the impact that the event might have on an information technology asset.

$$\text{RISK} = \text{Threats} \times \text{vulnerabilities} \times \text{Impact}$$

The impact of and event on an information asset is the product of vulnerability in the asset and the asset's value to it's stakeholders. IT risk can be expanded to:

$$\text{RISK} = \text{Threat} \times \text{Vulnerability} \times \text{Asset Value}$$

$$\text{Level of Risk} = \text{Consequence} \times \text{Likelihood}$$

| Risk Level | Consequence | Action |
|---|---|---|
| **Extreme or High** | Serious or imminent danger | • Immediate measures are required to combat the risk<br>• Identify and impose controls to reduce the risk to a reasonably low level |
| **Medium** | Moderate danger | • Immediate action is not required, but action should be implemented Quickly<br>• Implement controls as soon as possible to reduce the risk to a reasonably low level |
| **Low** | Negligible danger | • Take preventative steps to mitigate the effects of risk |

# 2 Definitions

## 2.1 General / Unsorted

- CIA Triad:
  - Confidentiality: unauthorized access to information.
  - Integrity: Trustworthiness of data
  - Availability: accessible when required
  - (Other) Non-repudiation: Sender of a message cannot deny having sent the message, same for receiver.
  - (Other) Authenticity: quality of being genuine
- OSI model - Open System Interconnection model
- Local Area Network (LAN): Computer network that connects two or more computers within a limited area.
- Virtual Local Area Network (VLAN): Broadcast domain that is divided in a computer network at the data link layer (OSI layer 2).
- Wide Area Network (WAN): Covers larger area than a LAN, typically involves telecommunication circuits for a special purpose, ie: banking network. Nodes are more than 10 miles apart.
- Time to live (TTL): time period a message can live on the network before it is discarded. (8-bits). Number of seconds or number of hops?
- User Datagram Protocol (UDP): light weight communication protocol that gives no assurance of delivery. If the application receives out of order packets they are destroyed rather than worrying about reordering them.
- Transmission Control Protocol (TCP):
- Internet of Things (IoT): Devices with embedded software and network access.
- Malware: software created to harm or infiltrate a computer system without the owners consent.
  - Virus: Create copies of themselves in other programs and activate from a trigger event.
  - Worm

  - Spyware
  - Trojan
- Information Security Policy: set of rules sanction by an organization to ensure that user of networks abide by the prescriptions regarding the security of data stored within the boundaries of the organization.
- Event: Something that happens that is detectable
- Incident: an event that violates policy.
- Certificate Authority: Organization that issues digital certificates.
- Vulnerability Scanner: Computer program designed to assess computer systems, network or applications for known weaknesses.
- Uniform Resource Locator (URL): reference to a web resource. Is a specific type of URI.
- Uniform Resource Identifier (URI): Unique sequence of characters that identifies a logical or physical resource used by web technologies. the `http://` part of the url.
- DNS Zone transfer: Used to duplicate or make copies of DNS data across a number of DNS servers or to back up DNS files.
- Open-source intelligence: to describe identifying information about a target using freely available sources.
- Defence in breadth: planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle.
- Defence in depth (DiD): Information security approach in which a series of security mechanisms and controls are layered throughout a computer network.
- Lawful Interception: Process of legally intercepting communications betwen two or more parties for surveillance on telecommunications, VoIP, data, and multiservice networks.
- Internet Zones
  - Internet (uncontrolled zone): outside the boundary of your organization.
  - Internet DMZ (controlled zone): Internet-facing controlled zone that contains components in which clients may directly communicate with. Usually buffered

by two firewalls one from internet to DMZ and one from DMZ to the internal network.

  - Production network (restricted zone): A restricted zone supports functions to which access must be strictly controlled; direct access from an uncontrolled network should not be permitted. In a large enterprise, several network zones might be designated as restricted. As with an internet DMZ, a restricted zone is typically bounded by one or more firewalls that filter incoming and outgoing traffic.

  - Intranet (controlled zone): is not heavily restricted in use, but an appropriate span of control is in place to assure that network traffic does not compromise the operation of critical business functions.

  - Management network (secured zone): In a secured zone, access is tightly controlled and available to only to a small number of authorized users. Access to one area of the zone does not necessarily apply to another area of the zone.

## 2.2 Attacks

- SQL Injection:
  - In-band SQL Injection: Attacker uses the same communication channel to launch the attack and gather results. (error-based and union-based SQL injection).
- Bluetooth
  - Bluesnarfing: Theft of information from a target device using a bluetooth connection.
  - Bluejacking: Transmission of data to a target device using a bluetooth connection.
- Operating System Attacks
- Application-Level Attacks
- Shrink Wrap Code Attacks
- Misconfiguration Attacks
- DHCP starvation attack: Broadcasting DHCP requests with spoofed MAC addresses to expend the available address pool, denying access to new users.
- MAC flooding attack: Attacker floods the switch MAC table to push legitimate MAC addresses out of the switch. This causes significant amounts of frames to be

broadcasted to all ports.

## 2.3 Organizations

- Open Web Application Security Project (OWASP): International non-profit organization focused on web application security.
- Federal Risk and Authorization Management Program (FedRAMP): Cloud computing regulatory effort, government-wide, delivers systemized approach to security assessment, authorization, and continuous monitoring of cloud products and services.

## 2.4 Cloud computing

- Platform as a service (PaaS): Third-party provider delivers hardware and software tools to users over the internet. PaaS frees developers from having to install in-house hardware and software to develop or run a new application.
- Infrastructure as a Service (IaaS):
- Hardware as a Service (HaaS):
- Software as a Service (SaaS):
- Models:
  - Private
  - Public
  - Community: Infrastructure is shared by several organizations, usually with the same policy and compliance considerations.
  - Hybrid

## 2.5 Cryptography

- Ciphers
  - Symmetric Ciphers: Single key is used for encryption and decryption
    - Data Encryption Standard (DES): Symmetric-key block cipher with key size of 56-bits
    - Triple Data Encryption Algorithm (3DES, TDES, TDEA): Applies the DES algorithm 3 times to each data block. Key length of $56 \times 3 = 168$ bits when 3 independent keys are used, or 112 when two keys are independent.

– Asymmetric Ciphers (Public key cryptography): One key can encrypt and one key can decrypt.

    *

# 3 Review Questions

## 3.1 TCP Scanning

- In the SYN scan; Nmap will send a SYN message to the target. What is the response if the port is open or closed?

    1. Open: A SYN/ACK packet
    2. Closed A RST packet
    3. Filtered: No response given

## 3.2 General

- Where does Microsoft Windows store authentication credentials and passwords?

    1. `C:\windows\system32\config`

- What netstat command will you use if you want to display all connections and listening ports, with addresses and port numbers in numerical form?

    1. `netstat -an`

- What type of rootkit uses system-level calls to hide their existence?

    1. Library Level rootkit (user-level), replaces or modifies the functionality of system calls to the operating system.