Introduction to Ethical Hacking

Information Security Overview

System security consists of methods and processes used for protecting information and information systems from unauthorized access, disclosure, usage, or modification.

Information security ensures the confidentiality, integrity and availability of information.

Implementing a security policy that is effective and efficient, rather than consisting of unnecessary security implementations that can result in a waste of resources and create loopholes for threats, is a continual challenge.

Security Concept Terminologies

Hack Value: refers to the attractiveness, interest, or thing of worth to the hacker. The value describes the target's level of attractiveness to the hacker.

Zero-Day Attack: exploit the victim before the developer identifies or addresses them and releases a patch for them.

Vulnerability: refers to a weak point or loophole in any system or network that can be helpful and utilized by attackers to hack into the system. Any vulnerability can be an entry point from which they can reach their target.

Security Concept Terminologies

- **Daisy Chaining:** is a sequence of hacking or attacking attempts to gain access to a network or system, one after another, using the same information and the information obtained from the previous attempt.

- **Exploit:** is a breach of a system's security through vulnerabilities, Zero-Day Attacks, or any other hacking technique.

- **Doxing:** means publishing information, or a set of information, associated with an individual. This information is collected from publicly available databases, mostly social media, and similar sources.

Security Concept Terminologies

- **Payload:** refers to the actual section of information or data in a frame as opposed to automatically generated metadata. In information security, a payload is a section or part of a malicious and exploited code that causes potentially harmful activities and actions such as exploiting, opening backdoors, and hijacking.

- **Bot:** is software that controls the target remotely and executes predefined tasks. It is capable of running automated scripts over the internet. Bots are also known as Internet Bots or Web Robots. These Bots can be used for social purposes, for example, chatterbots and live chats. Furthermore, they can also be used for malicious purposes in the form of malware. Hackers use Malware bots to gain complete authority over a computer.

Elements of Information Security (CIA)

Confidentiality - The National Institute of Standards and Technology (NIST) defines confidentiality as "*Preserving authorized restrictions on information access and disclosure while including means for protecting personal privacy and proprietary information*".

Integrity - The NIST defines integrity as "Guarding against improper information modification or destruction; this includes ensuring information non-repudiation and authenticity".

Availability - Ensuring timely and reliable access to and using information applied to systems and data is termed as Availability.

Elements of Information Security

CIA	Risk	Control
Confidentiality	Loss of privacy, Unauthorized access to information & Identity theft	Encryption, Authentication, Access Control
Integrity	Information is no longer reliable or accurate, Fraud	Maker/Checker, Quality Assurance, Audit Logs
Availability	Business disruption, Loss of customer confidence, Loss of revenue	Business continuity, Plans and tests, Backup storage, Sufficient capacity

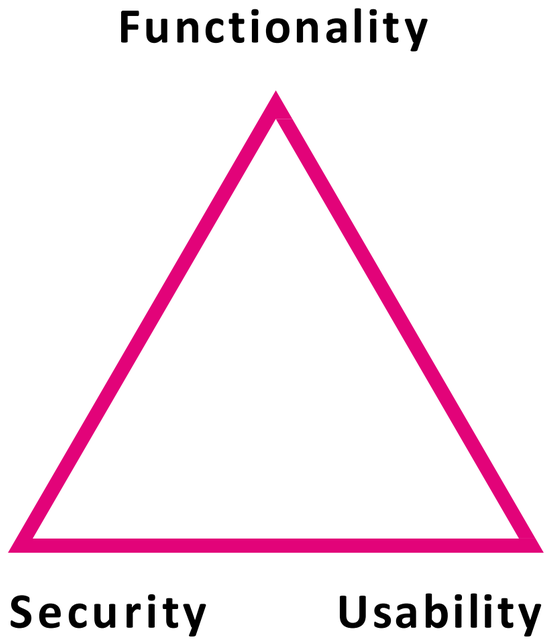
Elements of Information Security

Non-repudiation - is one of the Information Assurance (IA) pillars. It guarantees the transmission and receiving of information between the sender and receiver via different techniques

The Security, Functionality, and Usability Triangle

strength of a system's Security Functionality and Usability These three components form the Security, Functionality, and Usability triangle.

Consider a ball in this triangle—if the ball is sitting in the center, it means all three components are stronger. On the other hand, if the ball is closer to Security, it means the system is consuming more resources for Security, and the system's Function and Usability require attention.



Threats and Cyber Attack Components

Motives, Methods, and Vulnerabilities

An attacker targets a system to compromise information security based on three key components: **motive (objective), method, and vulnerability**.
These components represent the fundamental elements upon which an attack is planned and executed.

Motive (Objective): The reason or goal that drives an attacker to target a specific system (e.g., financial gain, espionage, disruption).
Method: The technique or approach used by the attacker to gain unauthorized access or carry out the attack (e.g., phishing, malware, SQL injection).
Vulnerability: A weakness or flaw in a system that can be exploited by an attacker to achieve their objective.

An attacker's motive often involves gaining access to something valuable stored within the target system, such as data, credentials, or services. The attack itself is generally **malicious and unauthorized**, although similar techniques may be used ethically in controlled environments such as **penetration testing**.

Cybersecurity Threats and Attack Types

Examples of Modern Cyber Threats

Cloud Computing Threats

Cloud computing has become widely adopted across organizations. However, its extensive use has introduced several security challenges. These threats include data breaches, misconfigured cloud settings, insecure APIs, and unauthorized access. While many of these risks are similar to traditional IT environments, the scale and shared responsibility model in cloud computing make security more complex. Therefore, securing cloud environments is essential to protect sensitive and confidential data

Advanced Persistent Threats

An Advanced Persistent Threat (APT) is a sophisticated and long-term targeted attack in which an attacker gains unauthorized access to a system and remains undetected for an extended period. APTs are typically carried out by highly skilled attackers and often target organizations to steal sensitive information, disrupt operations, or achieve strategic objectives. These attacks are persistent, meaning the attacker continuously monitors and exploits the system over time.

Cybersecurity Threats and Attack Types

Viruses and Worms

The term virus in network and information security describes malicious software. This malicious software is designed to spread by attaching itself to other files. Attaching itself to other files helps it to transfer onto other systems.

Mobile Threats

Emerging mobile phone technology, especially smartphones, has raised the focus of attacks on mobile devices. The most common threats to mobile devices are:

- Data leakage
- Unsecured Wi-Fi
- Network spoofing
- Phishing attacks
- Spyware
- Broken Cryptography

Cybersecurity Threats and Attack Types

Insider Threat

An **insider threat** occurs when an individual within an organization (e.g., employee, contractor, or partner) misuses their authorized access to compromise systems or data. Insiders typically have legitimate privileges, which makes detecting such threats more difficult. These actions may be intentional (malicious) or unintentional (negligent).

Botnets

A **botnet** is a network of compromised devices (called *bots* or *zombies*) that are controlled remotely by an attacker (botmaster). These devices are typically infected with malware and are used to perform coordinated malicious activities such as: Distributed Denial-of-Service (DDoS) attacks, Sending spam emails, Data theft, Cryptomining

Botnets operate without the knowledge of the device owners and are a major threat to internet security.

Threat Categories

Network Level Threats

The primary components of network infrastructure are routers, switches, and firewalls. These devices perform routing and other network operations and control and protect the running applications, servers, and devices from attacks and intrusions. Top network-level threats include

- Scanning
- Sniffing and eavesdropping
- Spoofing
- Session Hijacking
- Man-in-the-middle attack
- DNS and ARP

Threat Categories

Host Level (Operating System) Threats

Host-level threats target vulnerabilities in the operating system and local system environment, including unpatched systems, insecure configurations, and software flaws. Host Level Threats include:

- Malware
- Password Attacks
- Arbitrary Code Execution
- Login bypass
- Privilege Escalation
- Backdoors

Threat Categories

Application-Level Threats

The best practice to analyze application threats is by organizing them into application vulnerability categories. The main threats to the application are

- Improper Input Validation
- Broken authentication and authorization
- Security Misconfiguration
- SQL injection
- Broken Session Management
- Buffer Overflow Issues
- Cryptography Failures
- Improper error handeling and Exception Management

Software Exploitation Techniques

Shrink-Wrap Code Exploits

Shrink-wrap code refers to widely distributed, off-the-shelf software that may contain known vulnerabilities.
Attackers exploit these **publicly available vulnerabilities-**especially in unpatched systems-to gain unauthorized access.

These attacks typically target:
•Unpatched operating systems
•Commercial off-the-shelf (COTS) software
•Poorly designed or outdated applications

Information Warfare

Information warfare refers to the use and management of information and information systems to gain a strategic advantage over an adversary.

Defensive Information Warfare

Defensive information warfare involves actions taken to **protect information systems and data** from attacks, unauthorized access, and disruptions. This includes measures such as security controls, monitoring, and incident response.

Offensive Information Warfare

Offensive information warfare involves **proactive actions taken against adversaries** to disrupt, manipulate, or destroy their information systems and operations.