**Module 1: Introduction to Echical Hacking**

**Essential Terminology**

* **Hack Value:** A notion among hackers that something is worth doing or is interesting.
* **Vulnerability:** Existence of a weakness, design, or implementation error that can lead to an unexpected event compromising the security of the system.
* **Exploit:** A breach of IT system security through vulnerabilities.
* **Payload:** Payload is the part of an exploit code that performs the intended malicious action, such as destroying, creating backdoors, and hijacking computer.
* **Zero-Day Attack:** An attack that exploits computer application vulnerabilities before the software developer releases a patch for the vulnerability.
* **Daisy Chaining:** It involves gaining access to one network and/or computer and then using the same information to gain access to multiple networks and computers that contain desirable information.
* **Doxing:** Publishing personally identifiable information about an individual collected from publicly available databases and social media.
* **Bot:** A "bot" is a software application that can be controlled remotely to execute or automate predefined tasks.

**Information Security**

The information security is a state of well-being of information and infrastructure in which the possibility of theft, tampering , and disruption of information and services is kept low or tolerable.

**Elements of Information Security**

**CIA triad**

* **Confidentiality:** Assurance that the information is accessible only to those authorized to have access.
* **Integrity:** The trustworthiness of data or resource in terms of preventing improper and unauthorized changes.
* **Availability:** Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users.

**Other**

* **Authenticity:** Authenticity refers to the characteristic of a communication, document or any data that ensures the quality of being genuine.
* **Non-Repudiation:** Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

**The Security, Functionality, and Usability triangle**

**Security**: Restrictions imposed on accessing the components of the system (restrictions).

**Functionality**: The set of features provided by the system (features).

**Usability**: The GUI components used to design the system for ease of use (GUI).

**Information Security Attacks and Attack Vectors**

* Attacks = Motive (Goal) + Method + Vulnerability
* A motive originates out of the notion that the target system stores or process something valuable and this leads to threat of an attack on the system
* Attackers try various tools and attacks techniques to exploit vulnerabilities in a computer system or security policy and controls to achieve their motives

**Motives behind attacks:**

* Disrupting business continuity
* Information theft and manipulating data
* Creating fear and chaos by disrupting critical infrastructures
* Financial loss to the target
* Propagating religious or political beliefs
* Achieving state's military objectives
* Demanding reputation of the target
* Taking revenge
* Demanding ransom

**Top InfoSec Threats**

* Cloud Computing Threat
* Advanced Persistent Threats (APT): stealing information from the victim machine without the user being aware of it
* Viruses and Worms
* Ransomware
* Mobile Threats

**Top InfoSec vectors:**

* Botnet
* Insider Attack
* Phishing
* Web Application Threat
* IoT Threats

**InfoSec Threats categories:**

* Network Threats (spoofing, sniffing, ...)
* Host Threats (malware, dos, ...)
* Application Threats (auth attacks, SQL injection, ...)

**Type of Attacks on a System:**

* Operating System Attacks (OS vulnerabilities)
* Misconfiguration Attacks
* Application-Level Attacks (exploit the application)
* Shrink-Wrap Code Attacks (exploit the common vulnerable libraries)

**ICT** : Information and Communication Technologies

**Classification of Attacks**

* **Passive Attacks:** Do not tamper with the data and involve intercepting and monirotring network traffice and data flow on the target network. Such as sniffing and eavesdropping.
* **Active Attacks:** Tampter with the data in transit or disrupting the communication or services, such as DoS, MitM, Session Hijacking.
* **Close-in Attacks:** The attacker is in close physical proximity with the target, such as social engineering attack.
* **Insider Attacks:** Using privileged access to violate rules or intentionally cause a threat to…. Such as theft of devices, keyloggers, backdoor…
* **Distribution Attacks:** Attachers tamper with hardware or software prior to installation. Such as modification of software or hardware during production or distribution.

**Cyber Kill Chain Methodology**

* **Reconnaissance:** Gather data on the target to probe for weak points
* **Weaponization:** Create a deliverable malicious payload using an exploit and a backdoor
* **Delivery:** Send weaponized bundle to the civtim using email, USB, etc.
* **Exploitation:** Exploit a vulnerability by executing code on the victim’s systerm
* **Installation:** Install malware on the target system
* **Command and Control:** Create a command and control channel to communicate and pass data back and forth
* **Actions on Objectives:** Perform actions to achieve intended objectives.

**Water hole attack**: Watering hole is a computer attack strategy in which an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware.

**TTPs:** Patterns of activities and methods associated with specific threat actors or groups of threat actors.

* **Tactics:** Guidelines that describe the way an attacker performs the attack from beginning to the end.
* **Techniques:** Technical methos used by an attacker to achieve intermediate results during the attack.
* **Procedues:** Organizational approaches that threat actos follow to launch an attack.

**Adversary Behavioral Identification**

* Internal Reconnaissance
* Use of PowerShell
* Unspecified Proxy Activities
* Use of Command-Line Interface
* HTTP User Agent
* Command and Control Server
* Use of DNS Tuneling
* Use of Web Shell
* Data Staging

**Indicators of Compromise (IoCs):** Clues, artifacts, and pieces of forensic data found on the network or OS of an organization that…

**Hacker Classes:**

Black Hats, White Hats, Gray Hats, Suicide Hackers, Script Hiddies, Cyber Terrorists, State-Sponsored Hackers, Hacktivist (Individuals who promote a political agenda by hacking…)

**Hacking Phase:** Reconnaissance, Scanning, Gaining Access, Maintaining Access, Clearing Tracks

* **Reconnaissance:** Passive Reconnaissance and Active Reconnaissance. PR involves acquiring info without directly interacting with the target such as searching public records or news releases, AR involves directly interacting with the target by any means such as telephone calls.
* **Scanning:** Pre-attack phase. Port Scanner, Extract Info.
* **Gaining Access:** The atttacker obtains access to the OS or App on the target. Such as escalating privileges, password cracking, buffer overflow, DoS, Session Hijacking
* **Maintaining Access:** The attacker tries to retain their ownship of the system. Use the compromised system to launch further attacks
* **Clearing Tracks:** Hide malicious acts,overwrite the server, system, and application logs to avoid suspicion.

**Information Assurance (IA):** Assurance that integrity, availability, confidentiality and authenticity of info…

**Defense-in-Depth:** A security strategy in which several protection layers are placed throughout an information system. Prevent direct attacks

**Risk:** Degree of uncertainty or expectation that an adverse event may cause damage to the system.

* **RISK**= Threat x Vulnerabilities x Impact
* **RISK**= Threat x Vulnerabilities x Asset Value
* **Level of Risk**= Consequence x Likelihood
* **Likelihood:** The chance of the risk occurring
* **Consequence:** The severity of a risk event that occurs

**Risk Management**

**Phase:**

* **Risk Identification:** Identifies the sources…
* **Risk Assessment:** Assess the organization’s risk…
* **Risk Treatment:** Selects and implements appropriate controls…
* **Risk Tracking:** Ensures appropriate controls are implemented…
* **Risk Review:** Evaluate the performance…

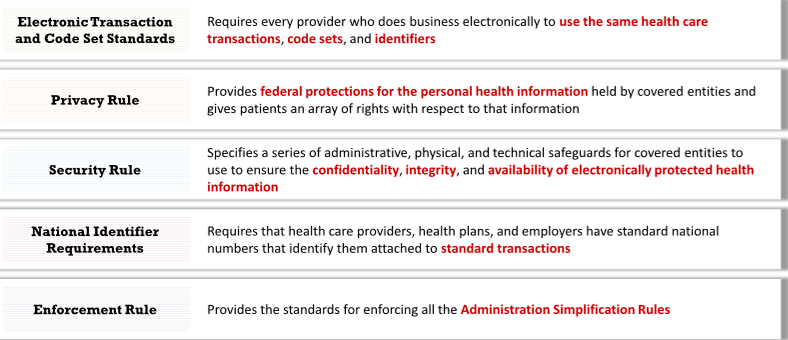
**Cyber Threat Intelligence (CTI):** Collection and analysis of info about threats and adversaries…

* **Types:** Strategic, Tatical, Operational, Taechnical
* **Threat Modeling:** A risk assessment approach
* **Process:** Identify security objectives, application overview, decompose the application, identify threats, identify vulnerbilities.
* **Incident Management:** A set of defined processes to identify, analyze, prioritize, and resolve security incidents…
* **Incident Handling and Response (IH&R):** The process of taking organized and careful steps when reacting to a security incident or cyberattack

**PCI DSS (Payment Card Industry Data Security Standard):** A proprietary information security standard for org that handle cardholder info….Apply to all entities involved in payment card processing.

**ISO/IEC 27001:2013:** Specifiy the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization

**HIPAA (Health Insurance Portability and Accountability Act):**



**SOX (Sarbanes Oxley Act):** Protect investors and the public by increasing the accuracy and reliability of corporate disclosures.

**DMCA (The Digital Millennium Copyright Act):** A United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization (WIPO)**. Define the legal prohibitions against the…

**FISMA (Federal Information Security Management Act):** Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operatrions and assets.

**GDPR (General Data Protection Regulation):** One of the most stringent privacy and security laws globally. Lecy harsh fines against those who violate its pricacy…

**DPA (Data Protection Act 2018):** Set out the framework for data protection law in the **UK.** Protect individuals concerning the processing of personal data.