MODULE no:- 1

**INTRODUCTION TO ETHICAL HACKING**

**Informtion security Overview**

**Element of Information security**

Element of Information is explained in three word *Confidentiality , Integrity , Availability .* which is popularly known as CIA triad.

**Confidentiality**:- Confidentiality is the assurance that the information is accessible to authorize person.

**Integrity** :- in this term, protect the data from deletion or modification by intruder .

After keeping the data confidential and integrity , than also data is useless unless it is not accessible , so here our third term come

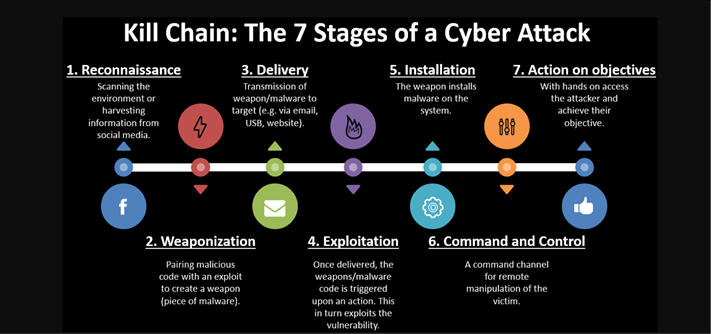
**Availability** :- Data must be available to authorize user only.

**Cyber Kill Chain**

A commonly referred-to framework in the information security space is the cyber kill chain. It gives information How an attacker or intruder attack the Organization . It also reveal all the possibility of threats and attack of every point, and how to defend that attack.

**Cyber kill chain Methodology**

Cyber kill chain methodology is step by step method how an attack is prepared by attacker , and How organization prepare to defense themselves.



**Just think of that , Before going to a WAR , what methodology is importan**t ,

• you must know the weakness of the opponent

• You must have weapon for fight . without weapon you are useless.

• You must have way to inter the battle and pierce the opponent army shield .

• After enter you need to attack them with full power

• Conquer the Battle and achieve the win

Same methodology is used by attacker

**Methodology**

**Reconnaisssance :-**  This is most important stage of Hacking , where we collect information. Further we will see it in depth .

So the attacker gather information of organization like policy, system information, network information ,specific Ip address, employee detail .

**Weaponization :-**  After collecting all type of information , attacker analyze the vulnerability , than he create the technique to exploit and gain access of target organization . So know he create the malicious script ,payload , worms , trojans according to vulnerability.

This is weaponization and all type of script is weapon of attacker .

**Delivery:-**  Know after creating weapon (payload) , It’s time to deliver it . attacker use various way to deliver the payload like through email, malicious link , vulnerable web application and usb. All this type of method is popularly known as Social Engineer.

**Exploitation :-**  know the attacker exploit his code and gain remote access to the organization system .

**Installation:-** At this stage attacker will install more malicious payload to maintain the access and gain full remote access to the target system.

**Command and control:-**  At this stage attacker will do monopoly , they will leverage the web traffic , read all email , access sensitive file . They will escalate the previllage . Hide all evidence of compromise process by the help of encryption.

**Action on Objectives:-**  After gaining full remote access of victim , know the attacker complete his goal . If they want to harm the system ,they will or if they want sensitive file , they will achieve it. So Here attacker complete his Goal.

**Tactics ,Techiniques and Procedure (TTPs)**

**Tactics :-**  Tactics is the procedure , where attacker create his methodology or we can say way of attack ,attacker perform the attack. How the attacker gather information , previllage the escalation and deploy the system.

**Techniques:-** Techniques is the info about attacker how they gain access through the intermediate level . How they do initial attcks and how he maintain the access.

**Procedure :-**  In procedure all the task are clarified step by step how attacker or cyber criminal follow the step of TACTICS and TECHNIQUES . These are the specific pre-configured step to be used by intruder , cyber criminal or attacker to ensure that they achieve their goal.

Before going to understand what is hacking lets know How hacking come and Person who did hacking and earn name in the field of Hacking

# John Draper

He was the programmer . He is also known as the captain crunch

Actually he did phone phreaking with the help of wishtle . He actually blow the wishtle at the frequency of 2600hertz, so by doing this process he found that call become free. So he invented the phone phreaking hack.

Later on a device was invented for creating a same frequency sound to make call free, which is known as BLUE BOX . It was designed and built by STEVE WOZNAIK and sold by steve jobs

# Kevin Mitnick

He is the former hacker in previous days . He is known as Father of social engineer . At child hood he found vulnerability in bus ticket system and make himself ticket free for life time . He was so creative mindset person.

**Many hacker arise and earn name ,some hacker earn fame also by doing good workd.**

**What is Ethical Hacking?**

Before understanding , what is ethical Hacking lets understand what is hacking and who is hacker .

Hacking is the term which refers the exploitation of vulnerable system , compromised the security to gain access unauthorize way.

Hacker is the person who can exploit the vulnerability , he is able to see the vulnerability which common people cannot see it. He can exploit system or destroy the security without authorization , steal sensitive data.

Topic is revealing most of the thing . Information security is the term where protection and safeguarding is given to the Data of information.

Know understand the ethical hacking , this is legalise action means all type of action taken by hacker are with permission by organization.

**It is necessary for technical field to secure the data of organization.**

**Types of Hackers**

* **Black Hat** - Hackers that seek to perform malicious activities.
* **Gray Hat** - Hackers that perform good or bad activities but do not have the permission of the organization they are hacking against.
* **White Hat** - Ethical hackers; They use their skills to improve security by exposing vulnerabilities before malicious hackers.

**Hacking Vocabulary**

* **Hack value** - Perceived value or worth of a target as seen by the attacker.
* **Vulnerability** - A system flaw, weakness on the system (on design, implementation etc).
* **Threat** - Exploits a vulnerability.
* **Exploit** - Exploits are a way of gaining access to a system through a security flaw and taking advantage of the flaw for their benefit.
* **Payload** - Component of an attack; is the part of the private user text which could also contain malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.
* **Zero-day attack** - Attack that occurs before a vendor knows or is able to patch a flaw.
* A **zero-day vulnerability** is a software vulnerability discovered by attackers before the vendor has become aware of it. Because the vendors are unaware, no patch exists for zero-day vulnerabilities, making attacks likely to succeed.
* A **zero-day exploit** is the method hackers use to attack systems with a previously unidentified vulnerability.
* A **zero-day attack** is the use of a zero-day exploit to cause damage to or steal data from a system affected by a vulnerability.
* **Daisy Chaining / Pivotting** - It involves gaining access to a network and /or computer and then using the same information to gain access to multiple networks and computers that contains desirable information.

.

**Attack Vectors**

*Path by which a hacker can gain access to a host in order to deliver a payload or malicious outcome*

* **APT - Advanced Persistent Threats**

Advanced persistent threat is a targeted cyber attack , in which intruder gain access to a network and remain undetected for a certain period of time.

Example zero-day attack

* **Cloud computing / Cloud based technologies**

Hacker gain access on computer or network and he deliever the malicious script .

* + Flaw in one client's application cloud allow attacker to access other client's data
* **Viruses, worms, and malware**
  + Viruses and worms are the most prevalent networking threat that are capable of infecting a network within seconds.
* **Ransomware**
  + Restricts access to the computer system's files and folders and demands an online ransom payment to the attacker in order to remove the restrictions.
  + Huge network of compromised systems used by an intruder to perform various network attacks.
* **Insider attacks**
  + Disgruntled employees can damage assets from inside.
  + Huge network of compromised hosts. (used for DDoS).
* **Phishing attacks**
* **Web Application Threats**
  + Attacks like SQL injection, XSS (Cross-site scripting)...

## Vulnerabilities

**CVSS - Common Vulnerability Scoring System** –

-Places numerical score based on severity

**CVE – Common Vulnerabilities and Exposures**

**-** Is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE

## The Five Stages of Ethical Hacking

### **Reconnaissance**

Information gathering about victim is known as Reconnaissance.

Gathering evidence about targets; There are two types of Recon:

* **Passive Reconnaissance**: Gain information about targeted computers and networks **without direct interaction with the systems**.
  + e.g: Google Search, Public records, New releases, Social Media, Wardrive scanning networks around , who is , ns look up, google dork,
* **Active Reconnaissance**: Envolves direct interaction with the target.
  + e.g: Make a phone call to the target, Job interview; tools like Nmap, Nessus, OpenVAS, Nikto, and Metasploit can be considered as Active Recon.

### 2. **Scanning & Enumeration**

Obtaining more in-depth information about targets.

* e.g: Network Scanning, Port Scanning, Which versions of services are running.

(Depth info in scanning module)

### 3. **Gaining Access**

Attacks are leveled in order to gain access to a system.

* e.g: Can be done locally (offline), over a LAN or over the internet.
  + e.g(2): Spoofing to exploit the system by pretending to be a legitimate user or different systems, they can send a data packet containing a bug to the target system in order to exploit a vulnerability.
  + Can be done using many techniques like command injection, buffer overflow, DoS, brute forcing credentials, social engineering, misconfigurations etc.

### 4. **Maintaining Access**

Items put in place to ensure future access.

* e.g: Rookit, Trojan, Backdoor can be used.

### 5. **Covering Tracks**

Steps taken to conceal success and intrusion; Not be noticed.

* e.g: Clear the logs; Obfuscate trojans or malicious backdoors programs.

**What is Risk ?**

Word of Risk is predefined by itself . In cybersecurity Risk refer to potential damage of system and data or its resources. Risk gave loss on the organization from internal and external resources.

In simple way we can say that it breaks the policy of CIA triad . Generally risk occur due to threats .

There is relation between threats , vulnerability , impact

**RISK = Threats × vulnerability × Impact**

### **Risk Management**



Risk management is the process of identifying the risk , than analyze the impact of risk , how much it is critical and about vulnerability . So it help the organization to develop the better risk management afterward they control the risk and mitigate its effect.

### Phases of Risk Management

* **Risk Identification :-** First identify the cause , consequences , sources of Risk. For identification of Risk ,its depend on the skill of identifier(people)
* **Risk Assessment:-** After identification of Risk it must me analyze to know the severity and seriousness of the risk.
* **Risk Treatment :-**  After knowing the seriousness of risk , it must eliminate. And check that it wont affect again .
* **Risk Tracking:-**  After Treatment of Risk , ensure that it should be handle appropriately so it can be controlled and Identifies the chance of new risk.
* **Risk Review**:- Evaluates the performance of the implemented risk management strategies

## Threat Modeling

## What is threat?

## The threat that harm the computer system or compromised the system and harm the system , sensitive data

## So threat modeling is the method of identifying the threat , identify the key vulnerabilities and improve the security design.

## Five step of Threat Modeling

## Identify :- Identify the threat , how much effort is required to remove the threat. Identify security objective like what dara should be protected , are there specific quality of service requirements etc

## Application Overview -

## End to end deployment

## Logical Layers

## Key component

## Communication ports and protocols

## Decompose the Application

## In this step the administrator breaks down the application to identify the trust boundries , data flow , entry points, and exit points

## Identify the threats:-

## The administrator should identify the threats to control the scenario and context using the iformation obtained in the application overview

## Identify Vulnerabilities

## A vulnerability is a weakness in application that allows attacker exploitation . Security Administrator should Identify any weakness related to threats

## Role of AI()Ariticial Intelligence and ML(Machine Learning) in Cyber Security

## Today’s world , artificial intelligence is getting popular include with machine learning in various field and various organization , due to increase in computing power.

## Technology Advancements in AI gone so far that automated car are developed with the help of AI , But threats are also composed by AI like botnet , malware, phising .

## What are AI and ML?

## As day by day technology are becoming advanced in AI that there is only solution to defend network against the various attacks that an antivirus scan cannot detect .

## ML , machine learning is a branch of artificial intelligence , which has ability of self learning without making program to understand in simple manner , it itself aquire many things

## Self learning system is used to explain the normal network along with its device . It analyze set of security event to identify the way or method of malicious activity and pattern also .

## Information Security Law and Standards

## There are some Laws , rules and guidelines in cybersecurity for country and community to govern behavior.

## ISO/ISE 27001:2013

## There are some rules and guidline are there so fraud and CIA loose problem should be handle .

## This regulation is use within organization to formulate security requierement and objectives and to ensure that security risk are cost-affective managed

## Lets see some rules

## Health Insurance Portability and Accountability Act (HIPAA)

## This law and act address that no one can reveal your health condition or any report , basically it protect the health information to disclose .

## Sarbanes Oxley Act

## SOX act is introduce for invester to protect from fraudlent accounting by corporation.