Introduction to Ethical Hacking

Hacking:-

compromise or gaining un-authorized access to digital devices, such as computers, smartphones, tablets, and even entire networks.

Ethical Hacking:-

Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows Cyber Security experts to perform such activities in order to test the system's defenses. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.

Terminologies:

Attack :- An attack is an action that is done on a system to get its access and extract sensitive data

Vulnerability :-weakness in a system eg: in hardware or software

Exploit :- A method to intrude or penetrate in a system

Payload :- Malicious code inside the exploit is called payload

Malware :- Malware is malicious(intent ended to do harm) software which when enters the target host, gives an attacker full or limited control over the target

Backdoor :- A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections

Hack value :- The notion among hackers that something is worth doing. It is the reputation of the hackers (i.,e) how good he is in hacking

Zero day attack when a hacker finds a new vulnerability in a system and no one others know about it , that vulnerability or exploit is called zero day attack

Firewall:-A firewall is a network security device that monitors traffic to or from your network. It allows or blocks traffic based on a defined set of security rules

Intrusion Detection & Intrusion Prevention system:-

IDS/IPS compare network packets to a cyberthreat database containing known signatures of cyberattacks. The main difference between them is that IDS is a monitoring system, while IPS is a control system

Elements of Information Security

Confidentiality:-It protects against disclosure of sensitive information to the unintended recipients

Integrity:- the Trustworthiness of data or resources In terms of preventing improper or un-authorized changes.

Availability:-

An information system to be useful it must be available to authorized users.

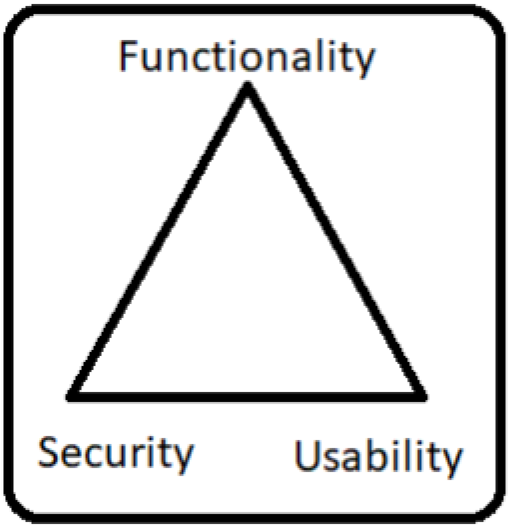
Authenticity:-

It verifies and confirms the user identity and It will manage the user access after login to any particular system.

Non-repudiation :-

Non-repudiation is the assurance that someone cannot deny the validity of something.

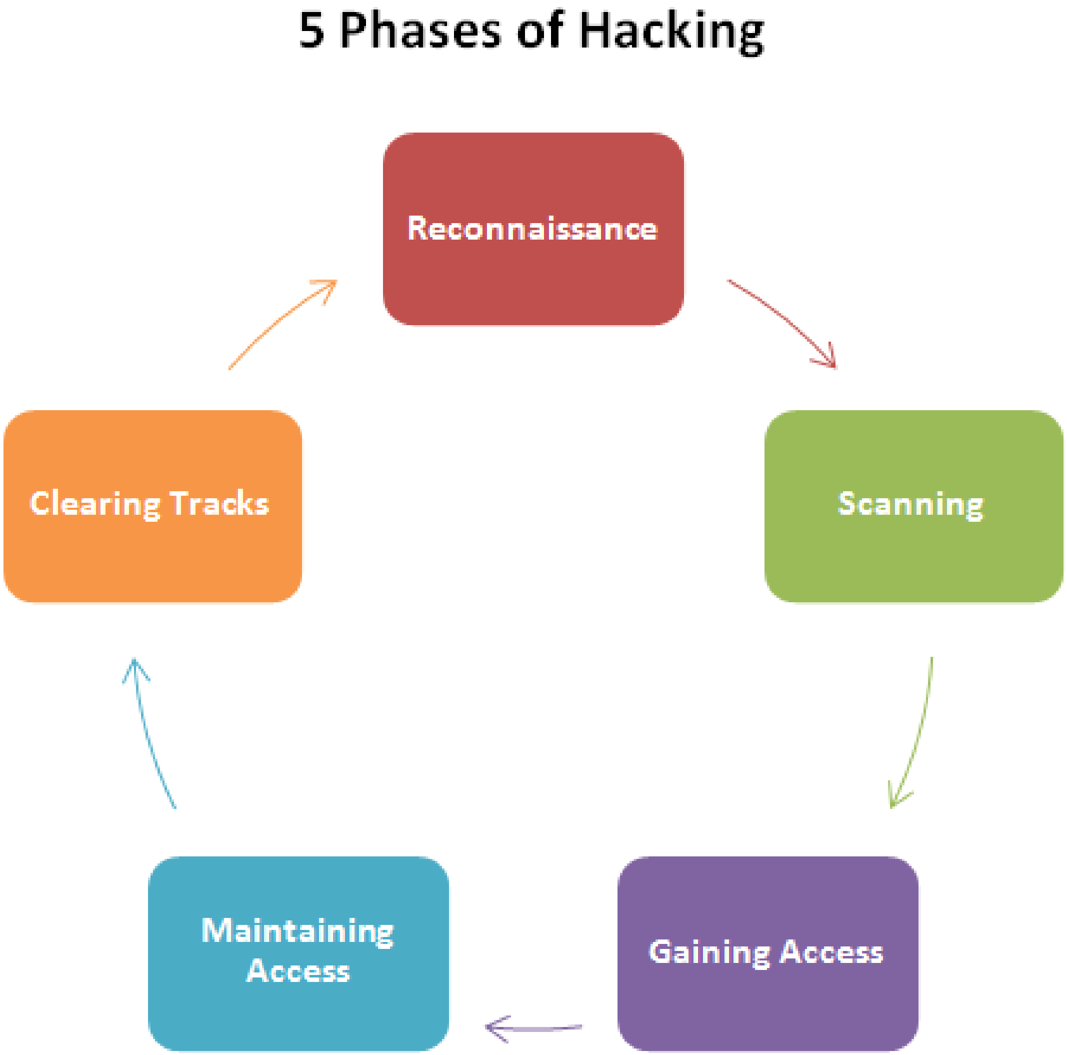
The security, functionality and usability Triangle



TYPES OF HACKERS:-

- Black hat Hackers.
- White hat Hackers.
- Grey hat Hackers.
- Script Kiddie
- Green Hat
- Red Hat
- Blue Hat
- Suicide hackers
- Hacktivist
- Cyber Terrorist

<u>Phases of Hacking:-</u>


5 Phases of Hacking
Reconnaissance
Scanning
Gaining Access
Maintaining Access
Clearing Tracks