Security Threats and Vulnerabilities

* What is Hacking ? and Method of Hacking.

=> Hacking refers to the unauthorized access or manipulation of system, network or data.

Hacker can use system or network vulnerabilities to Hack the system.

There are many type or method of Hacking.

1 Phishing:

Hacker try to get user sensitive information such as Username, password by pretending to be trustworthy entity.

2 Malware:

Malware is malicious software designed to damage, disrupt or gain unauthorized access to computer system.

3 Bait and switch:

Hackers purchase ad space on website and create attractive deceptive ads.

Users click on these ads and redirected to malicious site.

4 Cookie Theft:

Hackers exploit browser cookies, which store information like search history or password.

By stealing this cookie, attackers can impersonate the user and gain unauthorized access.

5 Denial of Service:

Hacker overload or floods the network with excessive traffic to cause a crash.

6 Keylogger:

Software that records keystrokes to capture the user sensitive information like password.

7 Brute Force:

Hacker trying all possible password combination until the correct one is found.

8 Password Cracking:

Hacker recovering password from stored or transmitted data while system has poor encryption or week password.

9 SQL Injection:

Hacker target vulnerabilities in web application and insert malicious SQL queries into input fields.

10 Man-In-Middle Attack:

Hacker intercepts communication between two party without their knowledge.

* What makes network insecure and How to identify and secure them ?

=> An Insecure network is Vulnerable to attack and unauthorized access

-> What make network Insecure ?

1 Weak or No Encryption : Data are transmitted over network without encryption that can read by Hacker.

2 Poorly Configured Firewalls : Misconfigured firewall may allow unnecessary traffic or block security updates.

3 Unpatch Software and Hardware : Outdated software and Firmware with know vulnerabilities can be explotied by attacker.

4 Weak Password Policies : Use of weak, easily gussable password or default credential can lead to unauthorized access.

5 Lack of Network Segmentation: Sensitive data and critical system are not isolated from less secure areas.

-> How to Identify

1 Vulnerability Scanning: Use tooles like Nessus or Qualys to scan the network vulnerabilities.

2 Penetration Testing: Conduct ethical hacking to simulate real-world attacks and identify weakness.

3 Network Traffic Analysis: Monitor network traffic for find unusual patterns.

4 Audit and Review Log: Regularly audit networks and system logs for suspicious activity attempts.

5 Security Assessments: Perform regular security assessment to ensure network work on best security.

=> How to Secure Network:

1 Implement Strong Encryption

2 Configure Firewalls and Intrustion Detection Systems

3 Regular Updates and Patching

4 Enforce Strong Password Policies

5 Regular Security Testing

6 Network Segmentation

7 Backup and Disater Recovery Plans.

* Explain Types of Comman Threats.

=> There are Main Four types of Comman Threats.

a) Structured Threats
b) Un structured Threats
c) Internal Threats
d) External Threats

a Structured Threats:

Structured Threats are implemented by a technically skilled person who is trying to gain access to the network.

These people are know the all types of vulnerabilities of the system.

These people are know how to implement all the types of system vulnerabilities.

They understand, develop and implement all the Hijacking Method.

These groups are often involves with the major type of Froud.

B Unstructured Threats :

Unstructured Threats are implement by non-technical person who try to gain access in your Network.

Inexperienced individual try to using the easily available hacking tooles or method.

These people does not do serious damage in the Network.

C External Threats :

Occurs when someone from Outside your Network creates a Security threats to your network.

This Threats are implemented by individuals or groups working outside of a group.

They does not have authorized access to the computer system or Network.

I) Internal Threats:

~~Our~~
Occurs when someone from inside your Network creates a security threats to your Network.

This Types of threats are more common and dangerous.

Internal attacker initiated by someone who has authorized access to the Network.

* Explain Intruders in Security.

=) Intruders is one type of Attack, in which person enters in a network places without any permission.

It breach the privacy of User and aims at stealing the Users detailes.

There are Three Types of Intruders

a) Masquerader
b) Misfeasor
c) Clandesine Users

a Masquerader :

These are not authorized to use the system but still explore User's privacy and information.

These person are ~~proce~~ processing method that given them control over the system network.

They are outsider, hence they don't have direct access to the system or Network.

B Misfeasor :

These are authorized to use the system but it is misuse the granted permission.

They take advantage of their permission and access given to them.

They are insider and they have direct access to the use of system or Network.

Page No. ______
Date :

C Clandertine User:

These are supervision/admistrative control over the system and misuse the authoritative power.

The miscontrol of power is often done by supertative authorities for gain Financial advantages.

They can be outsider or insider and they have direct / indirect access to use the system or network.