ports are
- open
- closed
- filtered

This information can be used by attackers to identify potential entry points into a system & launch targeted attacks.

Nmap (Network Maps)

It is a popular open source tool used for network discovery & security auditing.

It can be used to
- scan networks
- identify hosts
- discover services running on these hosts.
- determine which ports are open

Nmap offers a wide range of scanning techniques & options, making it a versatile tool for both reconnaissance & vulnerability assessment.

(3) Pretty Good Privacy (PGP) is a data encryption & decryption program that provides cryptographic privacy & authentication for data communication

It is commonly used for securing email communications.

PGP works by using a PKI to encrypt messages

Each user has a pair of keys
- Public key (to encrypt)
- Private key (to decrypt)

Users can share their public key with others, allowing them to send encrypted messages that only the intended recipient can

decrypt using their private key
PGP also provides digital signatures, allowing users to verify the authenticity of messages & ensure they have not been tampered

(4) Firewall

A firewall is a network security device that monitors & controls incoming & outgoing network traffic based on predetermined security rules.
It acts as a barrier between a trusted internal network & untrusted external networks.
Types of firewalls :
(a) Packet Filtering Firewalls
(b) Stateful Inspection Firewalls
(c) Proxy Firewalls
(d) Application Aware Firewalls
(e) Cloud Firewalls

Intrusion Detection System (IDS)

An IDS is a security tool designed to monitor network/system activities for malicious activities or policy violations
It analyzes network traffic, system logs & other data sources to identify signs of unauthorized access, misuse or security breach
IDS can detect various types of attacks including
- malware infections
- network scanning
- unauthorized access attempts
& alert administratars to take appropriate actions

DATE:

IS Assignment 2

Kreena Shah
60004210243
C'32

(1) Malware, short for malicious software, refers to any software intentionally designed to cause damage to a computer, server, network or user.

There are several types of malware, each with its own characteris & methods of propogation

Here are some common types

(a) Viruses
(b) Worms
(c) Trojans
(d) Ransomware
(e) Spyware
(f) Adware
(g) Rootkits
(h) Keyloggers
(i) Backdoors
(j) Botnets
(k) Exploit Kits

(2) Cross Site Scripting (XSS)

XSS is a type of security vulnerability commonly found in web applications.

It occurs when an attacker injects malicious scripts into web page viewed by other users.

These scripts are then executed in the context of the victim's browser, allowing the attacker to steal sensitive information, hijack sessions, or deface websites

Illustration :

Suppose there is a web application that allows users to post comments on a forum.

The application fails to properly validate & sanitize user input, allowing an attacker to inject malicious javascript code into a comment

When other users view the infected comment, the malicious code executes in their browsers, enabling the attacker to steal their session cookies or perform actions on their behalf

(3) DoS (Denial of Service)

A DoS attack is a cyber attack aimed at disrupting the normal functioning of a target system, network or service by overwhelming it with a large volume of traffics, requests, or malicious activity.

The goal of DoS attack is to make the target resource unavailable to legitimate users, thereby causing disruption, downtime, or financial losses

DoS attacks can take various forms, including

(a) Network based DoS

(b) Application layer DoS

(c) Distributed Denial of Service (DDoS)