ASSIGNMENT 2

Q1] What is NMap? What is port scanning?

- NMap:

Nmap (Network Mapper) is an open source network discovery & security auditing tool. It is widely used for network exploration, identifying devices, and scanning for open ports on a network. Nmap can detect hosts and services, operating systems, and vulnerabilities on the network, making it essential for network admins and cybersecurity professionals.

- Host Discovery: Nmaps helps identify devices on network.
- Port Scanning: It helps finding open and close ports on a target machine.
- Version Detection: Identifies versions of services running on open ports.
- OS Detection: Determining the operating system of a target machine.
- Vulnerability Detection: Finding potential security flaws in services.

Nmap supports various scan types, including TCP SYN, UDP, ACK, & more, allowing flexibility how it probes a network.

- Port Scanning:

Port scanning is the process of probing a network device for open or closed communication channels, known as ports. These ports are the endpoints through which devices on a network communicate using various protocols By scanning these ports, one can determine which services or applications are running on the target devices.

- Open Ports: Indicate that the port is active & accepting connections, which could mean a service is running on that port.
- Closed Ports: The port is reachable but not currently accepting connections.
- Filtered ports: The port is blocked by a firewall or security configuration, making it impossible to determine its state.

Port scanning helps in:

- Network Security: Identifying vulnerable open ports that attackers could exploit.
- Network Troubleshooting: Diagnosing connectivity issues by checking which ports are open or closed.
- Service Discovery: Mapping services running on a device for further analysis.

Q2) Explain OS Fingerprinting.

- OS Fingerprinting is a network scanning technique used to determine the OS of a remote device or system. This is accomplished by analyzing the unique characteristics in the responses of the target system to network probes or packets. OS fingerprinting helps identifying the exact OS or OS family running on the target machine.

There are two types of OS Fingerprinting:

① Active OS Fingerprinting

② Passive OS Fingerprinting

① Active OS Fingerprinting:

- In active OS fingerprinting, the attacker or network analyzer sends specially crafted packets to the target machine & analyzes the responses. The goal is to achieve / observe how the system reacts to different types of traffic. The differences in how various OS handle these packets help to identify the target OS.

• Process:

① Packet Crafting: Special packets are sent with unusal flags or malformed data. These packets can include SYN/ACK, FIN or fragmented packets.

② Response Analysis: The target system's responses are analyzed based on factors such as TTL (Time-to-live), windows size, TCP options & other networking behaviour.

③ Signature Matching: The gathered information is compared against a database of known OS signatures to identify the OS.

② Passive OS Fingerprinting:

- In Passive OS Fingerprinting, no probes are sent to the target. Instead, the analyst captures & analyzes traffic that is already passing through the network, using a packet sniffer. This method examines the traffic between the target device & other system, focusing on the characteristics of packets & the flags used in the packets.

• Process:

① Traffic Capture: The tool or analyst passively listens to traffic on the networking using tools like Wireshark or tcpdump.

② Analysis: The packets generated by the target system are analyzed based on factors such as TCP/IP stack behaviour & other subtle behaviours.

③ Identification: The results are compared to known OS signatures, much like in active fingerprinting.

Q3] Describe Keylogger attack.

- A keylogger attack is a form of cyberattack where malicious software or hardware is used to record the keystrokes made by a user on a keyboard. This allows attackers to capture sensitive information. The captured data is often transmitted to the attacker without the user's knowledge.

Key logger attacks can be carried out in two ways:

① Software Keyloggers 11

- They are programs installed on a computer, typically without user's consent, or knowledge. They run in the background & monitor all keystrokes typed on the keyboard. Some advanced versions can also capture screenshots, log clipboard activity, & record system activity.
- The software intercepts keyboard signals at various levels. Once the keystrokes are logged, the data is either stored locally or sent to the attacker's server.

- Software keyloggers can be spread through phishing emails, malicious downloads or by exploiting vulnerabilities in software.
- Examples:

i] Spyware: Malware designed to track user activity, including keystrokes.

ii] Trojan keyloggers: Installed when the victim unknowingly runs a trojan-infected program.

② Hardware keyloggers:

- They are physical devices that are attached to a computer to capture keystrokes. They are often placed between the keyboard & the computer. Unlike software keyloggers, hardware keyloggers do not rely on the system's software and can be often bypass detection by antivirus program.

- The devices record the electrical signals generated when a key is pressed & store the data locally. The attacker later retrieves the device to collect the logged information.
- They are more likely to be used in targetted attacks, especially in environments where physical access to the system is possible.
- Examples:

i] USB Keylogger: A small device that fits between the keyboard's USB plug & the computer.

ii] Keyboard-level Keylogger: These are embedded inside the keyboard itself.

Q4] Explain in detail DOS Attack.

- It is a type of cyberattack where an attacker aims to make a machine, network, or service unavailable to its intended users by overwhelming the target with a flood of illegitimate requests, excessive data. This overloads the system's resources, causing it to slow down significantly or crash entirely. The primary goal of DOS attack is to disrupt normal services, denying legitimate users access to a website or online services.

In typical DOS attacks, only one machine & one internet connection are used to flood the target with requests.

Following are the types of DOS Attacks:

① Flood Attacks:

- Flooding attacks occur when an attacker sends an overwhelming no. of requests or data packets to a target server, exhausting its resources.

• ICMP Flood: The attack floods the target with ICMP echo requests packets. When the target attempts to respond to each ping request, it becomes overwhelmed.

• UDP Flood: The attacker sends numerous UDP packets to random ports on the target, causing the target system to check for non-existent apps on those ports.

② Resource Exhaustion Attacks:

- This attack targets system resources such as memory, CPU, or disk usage space by overwhelming the target with resource-heavy requests.

- HTTP Flood: The attacker sends a high volume of HTTP requests to a web server, forcing it to handle multiple complex requests.
- Slowloris: This attack keeps many HTTP connections to the target server open by sending partial requests but never completing them.

③ Application - Layer Attacks:

- These attacks focus on the application layer of the OSI model & exploit weakness in the application to crash the service or make it unavailable.
- DNS Flood: The attacker sends a large no. of requests to the DNS server, asking it to resolve domain names to IP address, overwhelming it.
- layer 7 DOS: It targets the application layer, such as HTTP, SMTP or FTP services, to overwhelm the application layer directly rather than the server itself.

- A more severe form, Ddos (Distributed Denial of Service) is an advanced version of DOS attack in which multiple systems are used to flood the target with traffic or requests. These systems are typically compromised machines under the control of attacker.

Q5] Describe IPSec

- IPSec (Internet Protocol Security) is a comprehensive framework of protocols used to secure Internet Protocol communications by authenticating & encrypting each IP packet in data stream. It operates at the network layer of OSI model, ensuring that communications over IP

IP networks. It provides a set of security services such as data confidentiality, integrity, authentication & replay protection, making it essential for secure communication between devices, specially in VPN solutions.

- Confidentiality:

- It encrypts the data being transmitted over the network to ensure that unauthorized parties cannot read the contents. The encryption transforms readable data into an unreadable format using algorithms like AES, DES.

- Authentication:

- It verifies the identification of the communicating parties to ensure that the data is being sent & recieved by trusted sources. It uses mechanisms like pre-shared keys, digital certificates, etc.

- Integrity:

- It ensures that the data is not altered during transmission; Any changes made to the data can be detected by verifying message integrity using hashing algorithms such as HMAC (Hash Message Authentication Code).

- Replay Protection:

- It prevents attackers from capturing & resending legitimate packets to decieve the reciever. It uses sequence numbers to ensure that each packet is unique & delivered in the correct order.

Q6] Describe Email Security.

- It refers to the techniques and measures taken to protect email communication from unauthorized access, loss of confidentiality, integrity breaches, & other cyber threats. Since emails are a primary source/means of communications for individuals & organizations, they are also common target for cyberattacks such as phishing, spam, malware. Ensuring the security of emails is crucial to prevent data breaches, financial losses & other forms or damage.

- Encryption:
  - Encryption ensures that only the intended reciepent can read the email content by converting readable text into unreadable code.
- Authentication:
  - Email authentication techniques prevent spoofing and impersonation by verifying the identity of the sender.
- Anti-Phishing:
  - Anti-Phishing scan incoming emails for signs of phishing attempts, malicious links, or unsolicated content.
- Anti-Malware Protection:
  - Email security gateways & anti-virus software scan emails attachment and links for malware, preventing them from reaching the user's inbox.
- Data loss Prevention (DLP):
  - DLP tools prevent sensitive information, such as personally identifiable information (PII) or financial data, from being sent via email.

- Common Threats:

① Phishing:

- Emails designed to decieve recipients into sharing sensitive information.

② Spam:

- Unwanted and Unsolicitated emails that can carry malicious content or phishing attempts.

③ Email Spoofing:

- Sending emails from a forged address to mislead recipients.

④ Man-In-The-Middle Attack:

- Intercepting email communications during transmission.