Penetration Testing Basics

1.What is the difference between VA(Vulnerability Assignment) and PT(Penetration Testing)?

ANS:

Aspect	**Vulnerability Assessment (VA)**	**Penetration Testing (PT)**
Purpose	Identifies and lists vulnerabilities.	Exploits vulnerabilities to assess real impact.
Approach	Automated scanning and reporting.	Manual + automated exploitation.
Depth	Surface-level identification.	Deep exploitation and proof of concept.
Goal	To know *what* vulnerabilities exist.	To know *how dangerous* they are.
Example	A scan finds open port 22 (SSH).	A pentest tries weak SSH credentials to gain access.

2 What is the difference between HIDS and NIDS?

ANS:

Type	**HIDS (Host-based IDS)**	**NIDS (Network-based IDS)**
Location	Installed on individual hosts or servers.	Deployed on network devices (e.g., routers, switches).
Monitors	System logs, file integrity, process activity.	Network traffic and packet data.
Scope	Single device.	Entire network segment.
Example Tools	OSSEC, Tripwire.	Snort, Suricata.

3. What is a Brute Force Attack? How can you prevent it?

ANS: A brute-force attack tries **every possible password or key combination** until it finds the correct one.

- **Example:**
  Trying many login attempts on an SSH or web login page.
- **Prevention:**

- Use **strong passwords** and **multi-factor authentication (MFA)**.
- **Account lockout** after several failed attempts.
- **CAPTCHA** to block bots.
- Use **fail2ban** or firewall rate-limiting.

4. Explain MITM attack and how to prevent it?

ANS: An attacker secretly intercepts or alters communication between two parties without their knowledge.

- **Example:**
  Intercepting data on a public Wi-Fi to steal login credentials.
- **Prevention:**
  - Use **HTTPS** and **SSL/TLS encryption**.
  - Avoid using public Wi-Fi without a **VPN**.
  - Use **certificate pinning** in applications.
  - Enable **ARP inspection** and **DNSSEC**.

5. Explain XSS attack and how to prevent it?

ANS: XSS allows attackers to **inject malicious JavaScript code** into a trusted website viewed by others.

- **Example:**
  Posting <script>alert("Hacked")</script> in a comment box that executes when someone views the page.
- **Prevention:**
  - **Validate and sanitize** user input.
  - Use **Content Security Policy (CSP)**.
  - Encode outputs (HTML, JS, URL encoding).
  - Use frameworks that auto-escape inputs.

6. What is a Botnet?

ANS: A **network of compromised computers (bots)** controlled by an attacker (botmaster).

Usage:
- Launch **DDoS attacks**.
- Send **spam emails**.
- Spread **malware** or perform crypto-mining.

Prevention:
- Keep systems updated.
- Use firewalls and antivirus.
- Monitor for unusual outbound traffic.

7. What is a DDoS attack and how does it work?

ANS: A DDoS attack floods a target server or network with **massive traffic** from many infected systems (botnets), making it **unavailable to users**.

How it Works:

1. Attacker builds a botnet.
2. Commands all bots to send traffic to the target.
3. The server becomes overloaded and stops responding.

Prevention:

- Use **CDNs or load balancers**.
- **Rate limit** incoming traffic.
- Use **firewall and IDS/IPS**.
- Deploy **anti-DDoS services** (e.g., Cloudflare).

8. What is a zero-day vulnerability?

ANS: A **newly discovered software flaw** that has **no patch or fix available**, and is exploited before the developer becomes aware of it.

Example:
A browser exploit discovered and used before an update is released.

Prevention:

- Regular updates and patching.
- Use intrusion detection systems.
- Monitor threat intelligence feeds.

9. What is network sniffing

ANS: Capturing and analyzing network packets to monitor or steal data.

Used For:

- Legitimate: network troubleshooting, monitoring.
- Malicious: capturing passwords, cookies, or private data.

Tools: Wireshark, tcpdump, Ettercap.
Prevention:

- Use **encrypted protocols** (HTTPS, SSH).
- Use **switches** instead of hubs.
- Use **VPNs** to encrypt traffic.

10. What is the difference between IDS and IPS?

ANS:

Type	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Function	Detects and alerts suspicious activity.	Detects and actively blocks malicious activity.
Action	Passive — sends alerts only.	Active — drops or rejects malicious packets.
Placement	Out-of-band (monitors traffic).	Inline (sits in the data path).
Goal	Identify and report.	Identify and stop.