SEC 24 -- IMP Q FOR MIDSEM

1. Give difference with examples between:
   i. Brute Force Attack vs Dictionary Attack
   ii. SSL Login vs SSH Login
   iii. ARP Spoofing vs DNS Spoofing
   iv. XAAMP attack vs SQL Injection
2. NESSUS Tool's:
   i. Type of vulnerability it detects (features)
   ii. How it helps
   iii. Examples
3. NMAP Tool's:
   i. Type of vulnerability it detects (features)
   ii. How it helps
   iii. Examples
4. Metasploit Framework:
   i. Type of vulnerability it detects (features)
   ii. How it helps
   iii. Examples
5. What are payloads and its types
6. Basic Linux commands
7. Basic NMAP commands
8. Difference between 'man' and 'help' command

---

1. Differences with Examples

Brute Force vs Dictionary Attack

Comparison	Brute Force Attack	Dictionary Attack
Definition	Tries **all possible combinations** until correct password is found.	Tries passwords from a **predefined list** (dictionary).
Speed	Slower (huge combinations).	Faster (limited to known common passwords).
Example	Trying `aaaa`, `aaab`, `aaac`, etc.	Trying passwords like `password123`, `123456`, `admin` from a list.

SSL Login vs SSH Login

Comparison	SSL Login	SSH Login
Definition	Secure login over **HTTPS** using **SSL/TLS encryption**.	Secure login into **remote shell/terminal** using **SSH protocol**.
Port	Port 443 (HTTPS).	Port 22 (SSH).
Example	Logging into Gmail securely via browser.	Connecting to a Linux server using `ssh user@server`.

ARP Spoofing vs DNS Spoofing

Comparison	ARP Spoofing	DNS Spoofing
Definition	Attacker tricks network by **associating their MAC** with another device's IP (local network attack).	Attacker sends **fake DNS responses** to redirect traffic (global or local attack).
Example	Stealing login sessions on a LAN using ARP spoofing.	Redirecting facebook.com users to a fake phishing website.

XAMPP Attack vs SQL Attack

Comparison	XAMPP Attack	SQL Injection
Definition	Exploiting misconfigured or exposed XAMPP stack (Apache, MySQL, PHP, Perl) on a server.	Injecting malicious SQL code into application inputs.
Example	Accessing XAMPP dashboard remotely without authentication.	Entering `admin' --` in a login form to bypass authentication.

---

2. NESSUS Tool

Aspect	Description
Type of vulnerabilities it detects	Software bugs, misconfigurations, missing patches, weak passwords, open ports, compliance issues.
How it helps	Automated network vulnerability scanning, early identification of risks.

Examples	Detect outdated Apache server, vulnerable SSL/TLS versions, open MySQL database.

- It scan system and network for open ports services and known vulnerabilities.
- It checks software version against data bases.
- It identify the misconfiguration , missing patches ,weak passwords.
- It also generate reports with risk rotations remedial step

---

3. NMAP Tool

Aspect	Description
Type of vulnerabilities it detects	Open ports, running services, OS detection, service versions, common vulnerabilities using NSE scripts.
How it helps	Maps the attack surface, finds live hosts, weak spots, aids pentesting.
Examples	Finding open SSH port, detecting an old Samba version vulnerable to exploit, discovering web servers.

---

4. Metasploit Framework

Aspect	Description
Type of vulnerabilities it detects	Known vulnerabilities (exploits for software flaws like MS08-067, EternalBlue, weak configs).
How it helps	Automates exploitation, payload generation, post-exploitation.
Examples	Exploiting Windows XP using `ms08_067_netapi`, exploiting phpMyAdmin RCE vulnerability.

Workflow:

1. **Information Gathering** → Identify target system and services.
2. **Selecting Exploit** → Choose a suitable exploit module.
3. **Selecting Payload** → Choose the payload to deliver after exploitation.
4. **Configuration** → Set RHOSTS, LHOST, ports, and payload options.
5. **Launch Attack** → Execute the exploit to deliver payload.

6. **Post-Exploitation** → Maintain access, pivoting, data exfiltration.

---

5. What are Payloads and Their Types

Payload:

- The code that an attacker sends to a target after successful exploitation. It is responsible for giving the attacker access/control.

Types of Payloads:

- **Bind Shell**: Opens a port on the victim, attacker connects.
- **Reverse Shell**: Victim connects back to attacker's listener.
- **Meterpreter**: Advanced payload for post-exploitation (interactive control).
- **Staged vs Non-Staged**:
  - *Staged:* Small initial payload that downloads the main payload later.
  - *Non-Staged:* Full payload sent at once.

---

6. Basic Linux Commands

Command	Purpose
`ls`	List files and directories.
`pwd`	Show current directory path.
`cd`	Change directory.
`cp`	Copy files/directories.
`mv`	Move or rename files.
`rm`	Delete files or directories.
`cat`	View contents of a file.
`chmod`	Change file permissions.
`sudo`	Run commands with superuser rights.
`nano` or `vim`	Text editors inside terminal.

---

7. Basic NMAP Commands

Command	Purpose
`nmap 192.168.1.1`	Basic scan of a target.

`nmap -sS 192.168.1.1`	SYN (stealth) scan.
`nmap -p 1-1000 192.168.1.1`	Scan specific port range.
`nmap -sV 192.168.1.1`	Detect service versions.
`nmap -O 192.168.1.1`	Detect operating system.
`nmap -A 192.168.1.1`	Aggressive scan (OS, version detection, scripts).
`nmap --script vuln 192.168.1.1`	Run vulnerability detection scripts.

---

8. Difference Between ‘man’ and ‘help’ Command

Comparison	`man` Command	`help` Command
Purpose	Displays detailed manual pages for Linux commands.	Provides short help about shell built-in commands.
Example	`man ls` → full manual for `ls`.	`help cd` → shows usage info for `cd`.
Available for	System commands and installed programs.	Only built-in shell commands.