**Cyber Security Viva Questions and Answers**

**Unit I: Footprinting and Reconnaissance**

**Q1: What is footprinting, and why is it important in cybersecurity?**  
**A:** Footprinting is the process of gathering information about a target system or network. It helps attackers and ethical hackers understand the security posture before launching further attacks or security assessments.

**Q2: What is Recon-ng, and how is it used?**  
**A:** Recon-ng is an open-source reconnaissance framework in Kali Linux used for automated information gathering, including domain enumeration, API-based OSINT, and web reconnaissance.

**Q3: How does the FOCA tool work in footprinting?**  
**A:** FOCA (Fingerprinting Organizations with Collected Archives) extracts metadata from documents such as PDFs and Word files to gather information about the organization’s internal structure and users.

**Q4: What is the use of Windows Command Line Utilities in reconnaissance?**  
**A:** Tools like ping, tracert, nslookup, and netstat help gather information about network connectivity, route tracing, domain name system (DNS) records, and active connections.

**Q5: How can HTTrack be used in ethical hacking?**  
**A:** HTTrack is a website copier tool that allows users to download entire websites for offline browsing and analysis.

**Unit II: Enumeration and Vulnerability Analysis**

**Q6: What is enumeration in cybersecurity?**  
**A:** Enumeration is the process of extracting user names, machine names, network resources, and other critical information from a system.

**Q7: How does Nmap help in enumeration?**  
**A:** Nmap is a powerful network scanning tool used to identify active hosts, services, open ports, and operating system details on a network.

**Q8: What is NetBIOS Enumeration, and why is it used?**  
**A:** NetBIOS enumeration is used to gather information about network shares, usernames, and workgroups in a Windows environment.

**Q9: What is Nessus, and how does it help in vulnerability analysis?**  
**A:** Nessus is a vulnerability scanner that helps detect security weaknesses, misconfigurations, and known exploits in a system.

**Q10: What is the function of OpenVAS?**  
**A:** OpenVAS (Open Vulnerability Assessment Scanner) is an open-source vulnerability scanner that helps in identifying security threats in IT systems.

**Unit III: System Hacking and Network Security**

**Q11: What is Winrtgen, and how does it help in password cracking?**  
**A:** Winrtgen is a tool used to generate rainbow tables that help in cracking hashed passwords.

**Q12: What is the purpose of PWDump?**  
**A:** PWDump is a tool used to extract password hashes from Windows systems for offline analysis.

**Q13: What is Ophcrack, and how does it work?**  
**A:** Ophcrack is a password cracking tool that uses rainbow tables to crack Windows login passwords.

**Q14: What is the significance of Wireshark in cybersecurity?**  
**A:** Wireshark is a network protocol analyzer used to capture and inspect network traffic for security analysis and troubleshooting.

**Q15: What is MAC spoofing, and how is it performed using SMAC?**  
**A:** MAC spoofing is the process of changing a device’s MAC address. SMAC is a tool that allows users to modify their MAC address to evade network security controls.

**Unit IV: Web Security and Attacks**

**Q16: What is Burp Suite, and how is it used?**  
**A:** Burp Suite is a web security testing tool that allows penetration testers to intercept, modify, and analyze HTTP requests and responses.

**Q17: What is OWASP ZAP, and how does it help in web security?**  
**A:** OWASP ZAP (Zed Attack Proxy) is a security tool used for finding vulnerabilities in web applications by performing automated and manual scanning.

**Q18: How does droidsheep work for session hijacking?**  
**A:** DroidSheep is an Android application used to capture and hijack web sessions over Wi-Fi networks.

**Q19: What is HoneyBOT, and how does it work?**  
**A:** HoneyBOT is a honeypot software used to detect and analyze malicious network activity by simulating vulnerable services.

**Q20: What is SQL Injection, and how can it be performed using Havij?**  
**A:** SQL Injection is an attack technique used to exploit vulnerabilities in SQL-based applications. Havij is an automated tool that helps attackers extract database information using SQL Injection.

**Unit V: Cryptography and Wireless Security**

**Q21: What is Aircrack-ng, and how is it used for wireless security?**  
**A:** Aircrack-ng is a suite of tools used to assess and crack Wi-Fi network security by capturing packets and analyzing encryption weaknesses.

**Q22: What is TrueCrypt, and how does it help in data security?**  
**A:** TrueCrypt is a disk encryption software that allows users to create encrypted volumes to protect sensitive data.

**Q23: What is the function of MD5 Calculator?**  
**A:** MD5 Calculator generates MD5 hashes, which help in verifying file integrity and password security.

**Q24: What is the purpose of CrypTool?**  
**A:** CrypTool is an educational tool that demonstrates cryptographic algorithms and security concepts.

**Q25: How does Advanced Encryption Package help in securing data?**  
**A:** Advanced Encryption Package provides encryption and decryption features using various algorithms like AES and RSA to protect sensitive data.

**Conclusion:**  
This document provides a comprehensive list of potential viva questions and answers based on cybersecurity tools and techniques covered in the curriculum.