Cyber sicurity

CH-1.Systems Vulnerability Scanning

1. Define System and Web Vulnerability. (3 marks)
2. Explain Metasploit and OpenVAS. (4 marks)
3. Describe Nmap. Explain different functionality with its command in detail. (7 marks)
4. Define the term in briefly: (i) Open Port Identification (ii) Banner Check (3 marks)
5. What is Probe? Explain its different types. (4 marks)
6. List and explain types of Network Sniffer. List Network Sniffers and Injection tools. (7 marks)
7. Explain Ettercap and Hping Kismet. (7 marks)
8. Explain Vulnerability Scanning. (3 marks)
9. Describe Reconnaissance and Probe. (3 marks)
10. Explain Metasploit and Nmap. (7 marks)
11. Explain Injection tools like Tcpdump, Windump, and Wireshark. (7 marks)
12. Explain Ettercap and Hping Kismet. (7 marks)
13. Explain the network monitoring tool Snort. (7 marks)
14. What is OpenVAS? Write advantage and disadvantage of OpenVAS. (4 marks)
15. Describe Network Sniffers with suitable example. (3 marks)
16. Explain Wireshark and how do we use Wireshark to find a password in the network. (4 marks)
17. What is Netcat? Explain steps for File Transfer process by using Netcat in detail. (7 marks)

CH-2.Network Defense Tools

1. Define Snort. (3 marks)
2. Differentiate between Stateful and Stateless firewalls. (4 marks)
3. Explain Network Sniffers with suitable example. (7 marks)
4. Define NAT. Describe Port Forwarding with its types in detail. (7 marks)
5. Differentiate between Packet Filter and Firewall. (7 marks)
6. Explain Firewall Basics, Packet Filter Vs Firewall, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding. (7 marks)
7. What is firewall? Explain three main types of firewall. (7 marks)
8. Differentiate between Packet Filter and Firewall. (7 marks)
9. Differentiate between Stateless and Stateful Firewalls. (7 marks)

10. Define Network Address Translation. (3 marks)
11. Explain the need of Demilitarized Zone (DMZ). Explain with example. (7 marks)
12. Explain the concept of Network Address Translation (NAT) with suitable diagram. (7 marks)
13. What is Packet Filter Vs Firewall? (4 marks)

CH-3.Web Application Tools

1. Explain Curl, OpenSSL, and Stunnel. (3 marks)
2. Define Password cracking and Brute force tools. Explain any one in brief. (4 marks)
3. Describe DVWA. Explain SQL injection in DVWA with example in detail. (7 marks)
4. Explain Zed Attack Proxy. (3 marks)
5. Discuss the Web Vulnerability tools in detail. (7 marks)
6. Explain the web vulnerability tools like Nikto and W3af. (7 marks)
7. Explain DVWA and Webgoat. (7 marks)
8. Differentiate between John Ripper and HTC-Hydra. (4 marks)
9. Explain the tools for attacking wireless Networks. (7 marks)
10. Explain how SQL Injection attacks can be prevented. (7 marks)
11. Explain SQL Injection. (3 marks)
12. Explain Buffer Overflow attack in detail. (4 marks)
13. Describe DOS and DDOS attack with suitable example. (7 marks)
14. Explain Steganography with example. (3 marks)
15. Explain L0htcrack, HTC-Hydra, Pwdump. (4 marks)
16. Explain DVWA and Webgoat. (7 marks)

CH-4.Introduction to Cyber Crime and Law

1. Define Digital Forensics. (3 marks)
2. Explain types of Cyber Crimes. (4 marks)
3. Explain IT Act, 2000. List out and discuss different sections under IT Act, 2000 in detail. (7 marks)
4. Define Incident Response. (3 marks)
5. Discuss about Contaminants and Destruction of Data. (4 marks)
6. Discuss Attack vector. List out different types of Attack vector. (7 marks)
7. Write short note on Indian IT ACT 2000. (3 marks)
8. What is the difference between Threat, Vulnerability, and Risk and Computer Virus? (4 marks)
9. What do you mean by Cyber Crime? How do you relate it with Hacking? (3 marks)

10. Explain Traditional Problems Associated with Computer Crime. (4 marks)
11. Illustrate the aim and objective of Indian IT ACT 2000. (3 marks)
12. List out different types of Traditional Problems Associated with Computer Crime. (4 marks)
13. What is Incident Response? Explain its process flow with appropriate diagram. (7 marks)
14. Describe attack vector, cyberspace, and IT act 2000. (3 marks)
15. Explain hacking and its types. (4 marks)
16. Explain Incident response and digital forensics. (7 marks)
17. List three contemporary crimes. (3 marks)
18. Explain the types of cybercrimes. (4 marks)
19. What is contemporary approach in criminology in the world of computer science? (3 marks)
20. Explain in details: Hacking, Attack vectors, Cyberspace and Criminal Behavior. (7 marks)
21. What are the Cyber Crime Scenarios and explain its applicability for Legal Sections? (7 marks)
22. Define the Cyber Crime in your own words. Explain the different type of classification of Cyber Crime. (7 marks)
23. Explain passive attacks and active attacks with respect to cyber criminals. (3 marks)

CH-5.Introduction to Cyber Crime Investigation

1. Discuss Keyloggers and Spyware. (4 marks)
2. Explain Virus, Worms, Trojan Horses, and Backdoors in detail with example. (7 marks)
3. Explain Buffer Overflow attack in detail. (4 marks)
4. Describe DOS and DDOS attack with suitable example. (7 marks)
5. Explain Steganography with example. (3 marks)
6. Explain Keyloggers. Explain different types of Keyloggers. (3 marks)
7. Explain Wireshark and how do we use Wireshark to find a password in the network. (4 marks)
8. What is Hacking? Explain types of Hackers. (7 marks)
9. Explain the concept of Keyloggers and Spyware. (4 marks)
10. Explain the concept of Virus, Worms, Trojan Horses, and Backdoors. (7 marks)
11. Explain the concept of Buffer Overflow. (4 marks)
12. Explain the concept of DOS and DDOS attack. (7 marks)
13. Explain the concept of Steganography. (3 marks)
14. Explain the concept of Keyloggers. (3 marks)

15. Explain the concept of Wireshark. (4 marks)
16. Explain the concept of Hacking. (7 marks)