●Web Based Hacking

1. What is Session Hijacking Explain with Techniques?

ANS: Session hijacking involves an attacker using captured brute forced or reverse-engineered session IDs to seize control of a legitimate user’s session while that session is still in progress.

2. Find DoS/DDoS Attack Tools

ANS: Many DDoS Attack tools as HTTP unbearable load king HULK, Slowloris, PyLoris, DAVOSET, GodenEye open web application security, project, HTTP post, LOW ORBIT ION Cannon High Orbit ION RUDY freely available.

3. Explain SYN Flooding Attack with example

ANS: A SYN flood attack is a type of denial-of-service DOS attack that exploit the TCP three-way handshake process by sending a large volume of SYN packets to a handshake effectively from establishin connections.

4. List of Web App Hacking Methodology

ANS: DNS, NMAP, HTTP, WAF SSL/TLS, advanced serch quries, phishing, OSINT , WSTG, PTES, OWASP, WASC.

5. SQL Injection Methodology

ANS: identify potential SQL injection, analyze the web application DBMS, OR 1=1 UNION SELECTION SELETION \* FROM, Classic SQL injection, Blind SQL injection, Time based blind SQL injection, out of band SQL injection.

6. Explain sql injection with any tool

ANS: SQL injection is a type of web application security vulnerability that allows an attacker to inject malicious SQL code into a web application database, set up burp suite, identify a vulnerable web application, send a malicious request, analyze the response.

7. Explain deference between VA And PT

ANS: VA vulnerability assessment and PT penetration testing are two related but distinct concepts in the field of cybersecurity,

VA typically, network scanning, vulnerability, configuration review, risk assessment, PT is to, reconnaissance, exploitation, reporting.

8. How to write vulnerability assessment Report

ANS: The process of identifying classifying and reporting vulnerability that are present in application networks and other digital assets, select a temple the right template sets the foundation for a comprehensive vulnerability assessment report.

9.Explain the Zero Day Attacks .

ANS: A zero day attacks is a cyber attack that exploits a previously unknown vulnerability in software or hardware computer system unknown to its owners developers or anyone capable of mitigating it.