**PRACTICAL COMPONENT**

**List of Experiments supposed to finish in Open Lab Sessions:**

|  |  |
| --- | --- |
| **S. No** | **Title of the experiment** |
| 1 | Perform host discovery using   1. Perform host discovery using Nmap 2. Perform host discovery using Angry IP Scanner |
| 2 | Perform port and service discovery   1. Explore various Network Scanning techniques using Nmap. 2. Explore various Network Scanning techniques using Hping3. |
| 3 | Perform OS discovery   1. Perform OS discovery using Nmap Script Engine (NSE) 2. Perform OS discovery using Unicornscan |
| 4 | Footing the Web Server   1. Information Gathering using Ghost Eye 2. Footprint a web server using the httprecon Tool 3. Footprint a web server using Netcat and Telnet 4. Enumerate web server information using Nmap Scripting Engine (NSE) |
| 5 | Footprint the Web Infrastructure   1. Perform Web Application Reconnaissance 2. Perform Web Application Reconnaissance using What Web 3. Perform Web Spidering using OWASP ZAP 4. Detect Load Balancers using various tools. 5. Identify web server directories. 6. Perform Web Application Vulnerability Scanning using Vega 7. Identify Clickjacking Vulnerability using iframe |
| 6 | Perform Web Application Attacks   1. Perform a Brute Force attack using Burp Suite 2. Perform Parameter Tampering using Burp Suite 3. Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications 4. Perform Cross-site Request Forgery (CSRF) attack 5. Enumerate and Hack a Web Application using WPScan and Metasploit 6. Exploit a Remote Command Execution Vulnerability to compromise a target web server 7. Exploit a file upload vulnerability at different security levels. 8. Gain Backdoor access via a web shell using Weevely |
| 7 | Detect Web Application Vulnerabilities using Various Web Application Security Tools   1. Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner |
| 8 | Perform Footprinting Through Web Services   1. Find the company’s domains and sub domains using Netcraft 2. Gather an Email list using the Harvester 3. Determine target OS through Passive Footprinting |
| 9 | Perform Footprinting through Social Networking Sites   1. Gather Employee’s information from LinkedIn using the Harvester 2. Gather Personal Information from various social networking sites using Sherlock 3. Gather Information using Followerwonk |
| 10 | Perform Website Footprinting   1. Gather information about a target website using Ping Command Line Utility 2. Gather information about a target website using Website Informer 3. Extracts a company data using Web Data Extractor 4. Gather a wordlist from the target website using CeWL |
| 11 | Perform Whois Footprinting   1. Perform Whois Lookup using Domain tools |
| 12 | Perform DNS Footprinting   1. Gather DNS Information using nslookup Command Line Utility and Online tool 2. Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon |
| 13 | Perform Network Footprinting   1. Locate the Network Range 2. Perform Network Tracerouting in Windows and Linux machines |
| 14 | Perform Footprinting using Various Footprinting Tools   1. Footprinting a Target using Recon-ng 2. Footprinting a Target using Maltego 3. Footprinting a Target using OSRFramework 4. Footprinting a Target using BillCipher |