**List of Labs:**

**Phase # 1: Vulnerability Assessment**

**Topic 01: Introduction to Ethical Hacking**

Lab: VirtualBox Installation

Lab: Parrot Security VirtualBox Installation

Lab: Windows 10 VirtualBox Installation

Lab: Integrate ShellGPT in the Parrot Security Machine

**Topic 02: Footprinting & Reconnaissance**

Lab: Gather Information using Advanced Google Hacking Techniques

Lab: Find the Company’s Domains, Subdomains, and Hosts using Netcraft and DNSdumpster

Lab: Gather Personal Information from Various Social Networking Sites using Sherlock

Lab: Perform Whois Lookup using DomainTools

Lab: Gather DNS Information using nslookup Command Line Utility and Online Tool

Lab: Perform Network Tracerouting in Windows and Linux Machines

Lab: Gather Information about a Target by Tracing Emails using eMailTrackerPro

Lab: Footprinting a Target using Recon-ng

Lab: Footprinting a Target using ShellGPT

**Topic 03: Scanning Networks**

Lab: Perform Host Discovery using Nmap

Lab: Explore Various Network Scanning Techniques using Nmap

Lab: Perform OS Discovery using Nmap Script Engine (NSE)

Lab: Scan beyond IDSFirewall using Various Evasion Techniques

Lab: Scan a Target Network using Metasploit

Lab: Scan a Target using ShellGPT

**Topic 04: Enumeration**

Lab: Perform NetBIOS Enumeration using Windows Command-Line Utilities

Lab: Perform SNMP Enumeration using SnmpWalk

Lab: Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

Lab: Perform NFS Enumeration using RPCScan and SuperEnum

Lab: Perform DNS Enumeration using Zone Transfer

Lab: Perform SMTP Enumeration using Nmap

Lab: Enumerate Information using Global Network Inventory

Lab: Perform Enumeration using ShellGPT

**Topic 05: Vulnerability Analysis**

Lab: Perform Vulnerability Research in Common Weakness Enumeration (CWE)

Lab: Perform Vulnerability Analysis using OpenVAS

Lab: Perform Vulnerability Analysis using ShellGPT

**Phase # 2: Gaining Access**

**Topic 06: System Hacking**

Lab: Perform an Active Online Attack to Crack the System’s Password using Responder

Lab: Gain Access to a Remote System using Reverse Shell Generator

Lab: Perform Buffer Overflow Attack to Gain Access to a Remote System

Lab: Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys

Lab: User System Monitoring and Surveillance using Spyrix

Lab: Maintain Persistence by Modifying Registry Run Keys

Lab: Clear Windows Machine Logs using Various Utilities

Lab: Clear Linux Machine Logs using the BASH Shell

Lab: Perform Initial Scans to Obtain Domain Controller IP and Domain Name

Lab: Perform AS-REP Roasting Attack

Lab: Spray Cracked Password into Network using CrackMapExec

Lab: Perform Post-Enumeration using PowerView

Lab: Perform an Attack on MSSQL service

Lab: Perform Privilege Escalation

Lab: Perform Kerberoasting Attack

Lab: Perform System Hacking using ShellGPT

**Topic 07: Malware Threats**

Lab: Gain Control over a Victim Machine using the njRAT RAT Trojan

Lab: Create a Virus using the JPS Virus Maker Tool and Infect the Target System

Lab: Perform Malware Scanning using Hybrid Analysis

Lab: Analyze ELF Executable File using Detect It Easy (DIE)

Lab: Perform Malware Disassembly using IDA and OllyDbg

Lab: Perform Port Monitoring using TCPView and CurrPorts

Lab: Perform Process Monitoring using Process Monitor

**Topic 08: Sniffing**

Lab: Perform MAC Flooding using macof

Lab: Perform a DHCP Starvation Attack using Yersinia

Lab: Perform Password Sniffing using Wireshark

Lab: Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network

**Topic 09: Social Engineering**

Lab: Sniff Credentials using the Social-Engineer Toolkit (SET)

Lab: Detect Phishing using Netcraft

Lab: Craft Phishing Emails with ChatGPT

**Topic 10: Denial-of-Service (DoS)**

Lab: Perform a DDoS Attack using ISB and UltraDDOS-v2

Lab: Perform a DDoS Attack using Botnet

Lab: Detect and Protect Against DDoS Attacks using Anti DDoS Guardian

**Phase # 3: Perimeter and Web App Exploitation**

**Topic 11: Session Hijacking**

Lab: Hijack a Session using Caido

Lab: Intercept HTTP Traffic using Hetty

Lab: Detect Session Hijacking using Wireshark

**Topic 12: Evading IDS, Firewalls & Honeypots**

Lab: Detect Intrusions using Snort

Lab: Deploy Cowrie Honeypot to Detect Malicious Network Traffic

**Topic 13: Hacking Web Servers**

Lab: Footprint a Web Server using Netcat and Telnet

Lab: Enumerate Web Server Information using Nmap Scripting Engine (NSE)

Lab: Crack FTP Credentials Using a Dictionary Attack

Lab: Gain Access to Target Web Server by Exploiting Log4j Vulnerability

Lab: Perform Web Server Footprinting and Attacks using ShellGPT

**Topic 14: Hacking Web Applications**

Lab: Perform web application Reconnaissance using Nmap and Telnet

Lab: Perform Web Spidering using OWASP ZAP

Lab: Perform Web Application Vulnerability Scanning using SmartScanner

Lab: Perform a Brute-force Attack using Burp Suite

Lab: Perform Remote Code Execution (RCE) Attack

Lab: Detect Web Application Vulnerabilities using Wapiti Web Application Security Scanner

Lab: Perform Web Application Hacking using ShellGPT

**Topic 15: SQL Injection**

Lab: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

Lab: Detect SQL Injection Vulnerabilities using OWASP ZAP

Lab: Perform SQL Injection using ShellGPT

**Phase # 4: Mobile, IoT, and OT Exploitation**

**Topic 16: Hacking Wireless Networks**

Lab: Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark

Lab: Crack a WPA2 Network using Aircrack-ng

**Topic 17: Hacking Mobile Platforms**

Lab: Exploit the Android Platform through ADB using PhoneSploit

Lab: Hack an Android Device by Creating an APK File using AndroRAT

Lab: Secure Android Devices from Malicious Apps using AVG

**Topic 18: IoT & OT Hacking**

Lab: Gather Information using Online Footprinting Tools

Lab: Capture and Analyze IoT Traffic using Wireshark

Lab: Perform Replay Attack on CAN Protocol

**Topic 19: Cloud Computing**

Lab: Azure Reconnaissance with AADInternals

Lab: Exploit Open S3 Buckets using AWS CLI

Lab: Escalate IAM User Privileges by Exploiting Misconfigured User Policy

Lab: Vulnerability Assessment on Docker Images using Trivy

**Topic 20: Cryptography**

Lab: Perform Multi-layer Hashing using CyberChef

Lab: Perform File and Text Message Encryption using CryptoForge

Lab: Create and use Self-Signed Certificate

Lab: Perform Disk Encryption using VeraCrypt

Lab: Perform Cryptographic Techniques using ShellGPT