COURSE OVERVIEW

01. Network Basics

- TCP/IP Packet Analysis
- Overview of Network Security
- Port and Protocols Analysis
- Windows Lab Setup
- Linux Lab Setup
- Linux major services & commands
- Windows major services & commands

02. Penetration Testing Framework Kali Linux

- Virtual Box
- VMware
- AWS | Google Cloud

03. Analyzing Network Traffic

- Importance of Packet Analysis
- How to Capture Network Traffic
- Promiscuous Mode
- Introduction to Wireshark
- Filtering & Decoding Traffic
- Physical Data-Link Layer
- Network Internet Layer
- Transport Host-Host Layer
- Application Layer

04. Packet Analysis with Tshark

- Introduction to Tshark
- Capture traffic
- Promiscuous mode
- Packet count
- Read and Write in a file
- Output formats
- Display filter
- Endpoints Analysis

iGNITE Technologies

05. Detecting Live Systems & Analyzing Results

- Detecting Live Systems with ICMP
- Detecting Live Systems with TCP
- ICMP Packet Analysis
- Traceroute

06. Nmap Advance Port Scan

- Fragment Scan
- Data Length Scan
- TTL Scan
- Source Port Scan
- Decoy Scan
- TCP and UDP Port Scan
- Nmap Scan with Wireshark
- Nmap Output Scan
- OS Fingerprinting
- Spoof IP Scan
- Spoof MAC Scan
- Data String Scan
- Hex String Scan
- IP Options Scan

07. Metasploit Framework Hands-on

- Metasploit Basic
- Msfvenom
- Auxiliary scanner
- Windows Reverse TCP
- Windows HTTPS Tunnel
- Hidden Bind TCP
- Macro Payloads
- Shell on the Fly (Transport)
- Bypass User Access Control
- Pass the Hash
- Post Exploitation

08. Dictionary & Passwords Attacks

- Hydra
- Medusa
- Crunch
- CeWL
- cUPP
- Online Attacks

09. FTP Penetration Testing

- Introduction & Lab Setup
- Banner Grabbing
- Banner Hiding
- FTP Exploitation
- Brute Force & Password Cracking
- Prevent against brute force
- Remote Port Forwarding
- Pivoting

iGNITE Technologies

10. SSH Penetration Testing

- Introduction & Lab Setup
- Banner Grabbing
- Banner Hiding
- Port Redirection
- Brute Force & Password Cracking
- Prevent SSH Against Brute Force
- SSH User Key Enumeration
- Stealing SSH RSA_KEY
- SSH Persistence
- Remote Port Forwarding
- SSH Tunneling

11. Telnet Penetration Testing

- Introduction & Lab Setup
- Banner Grabbing/Banner Hiding
- Port Redirection
- Brute Force & Password Cracking
- Remote Port Forwarding
- Pivoting

12. SMTP Penetration Testing

- Introduction & Lab setup
- Banner Grabbing | Banner Hiding

Port Redirection

- User Enumeration

13. DNS & DHCP Penetration Testing

- Introduction & Lab Setup
- DNS Enumeration
- DHCP Packet Analysis with Wireshark

DHCP Starvation Attack

- Rogue DHCP Server

14. NetBIOS & SMB Penetration Testing

- Introduction & Lab Setup
- SMB Enumeration
- SMB Null Sessions
- Enum4Linux
- Brute Force & Password Cracking
- SMB DOS
- Eternal Blue & Eternal romance
- Remote Login with SMB

iGNITE Technologies

15. MySQL Penetration Testing

- Introduction and Lab setup
- Brute Force & Password Cracking
- MySQL Enumeration
- Extract MySQL-Schema Information
- Execute MySQL query Remotely
- Extracting Password Hashes
- Enumerate writeable directories
- Enumerating System Files

16. Remote Desktop Penetration Testing

- Introduction & Lab setup
- RDP Enumeration
- RDP MITM over SSL
- Brute Force & Password Cracking
- RDP Session Hijacking
- Remote Port Forwarding
- DOS Attack

17. VNC Penetration Testing

- Introduction & Lab setup
- Banner Grabbing
- Banner Hiding
- Port Redirection
- Brute Force & Password Cracking
- Remote Port Forwarding
- Tunneling Through SSH

18. Credential Dumping

- Wireless Creds
- Auto login Password Dump
- Application Creds
- Fake Services

19. Socks Proxy Penetration Testing

- Socks proxy Lab Setup
- Secure Shell (SSH)
- File Transfer Protocol (FTP)
- HTTP

iGNITE Technologies

20. Sniffing & Spoofing

- Introduction
- ARP Poisoning
- MAC Address Snooping
- DNS Spoofing
- ICMP Redirect
- NTLM Hash Capture

21. DOS Attack Penetration Testing

- Introduction to DOS Attack
- Botnet
- D-DOS Attack
- SYN Flood Attack
- UDP Flood
- Smurf Attack
- Packet Crafting
- Others DOS Attack Tools

22. Covering Tracks & Maintaining Access

- Persistence_Service
- Persistence_Exe
- Registry_Persistence
- Persistence through Netcat
- Clear Event Logs

23. Honeypots

- What are Honeypots
- Working of Honeypots
- Types of Honeypots
- Installation and working of Honeypots

24. Firewall

- Introduction to Firewall
- Types of Firewall
- Windows Firewall
- Linux Firewall
- Untangle Firewall Implementation

25. Intrusion Detection System

- What is Intrusion Detection System
- Working of IDS
- Types of IDS
- Type of IDS Alert
- IDS Implementation using Snort
- Capture ICMP Alert
- TCP Packet Alert
- Capture Malicious Attacks

26. Network Vulnerability Assessment Tool

- Nessus
- Vulnerability Scanning using Nmap
- Nexpose

iGNITE Technologies

CONTACT US

Phone No.

+91 9599 387 41 | +91 1145 1031 30

WhatsApp

https://wa.me/message/HIOPPNENLOX6F1

EMAIL ADDRESS

info@ignitetechnologies.in

WEBSITE

www.ignitetechnologies.in

BLOG

www.hackingarticles.in

LINKEDIN

https://www.linkedin.com/company/hackingarticles/

TWITTER

https://twitter.com/hackinarticles

GITHUB

https://github.com/ignitetechnologies

iGNITE Technologies