INFOSECTRAIN

NETWORK PENETRATION TESTING

ONLINE TRAINING COURSE

www.infosectrain.com | sales@infosectrain.com

INFOSECTRAIN

Course Description

Network Penetration Testing Training has been designed to teach the aspirants about penetration testing/ethical hacking from a networking perspective. Our trainers have included all the fundamental information related to network-based ethical hacking which would help you to evolve into a professional penetration tester. Our Network Penetration Testing Course will help you to understand the various exploitation techniques a hacker might use on a network. This will further help you in identifying and exploiting the vulnerabilities in the network. Along with this, we also include training on the additional techniques and networking tools similar to Wireshark or TCPDump. The entire course aims to help you in learning all the skillset which will allow you to use the latest Penetration tools and to secure the client's network. We also offer online Network Penetration Testing Training.

INFOSECTRAIN

Target Audience

- Penetration testers
- Security analysts
- Cybersecurity consultants
- All those interested in learning the concepts of ethical hacking and penetration testing.

Pre-Requisite

- Understanding of the Windows Operating System
- Ability to handle the Linux Operating System or other Unix-based OS
- Knowledge of the TCP/IP protocols
- Experience of using network reconnaissance and associated tools (nmap, nessus, netcat)

INFOSECTRAIN

Why Infosec Train?

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- 4 hrs/day in Weekend/ Weekday

Course Content

Introduction

- TCP/IP Packet Analysis
- Overview of Network Security
- Port and Protocols & Analysis
- Linux Server Installation
- Windows Client / Linux Installation
- Basic commands (Windows / Linux)
- Kali Linux Installation

Wireshark

- Introduction
- ICMP Packet Analysis
- ARP Packet Analysis
- 3 way handshake Analysis
- Tracert Command Analysis
- Packet Forensics
- Nmap Packet Forensics

NMAP Basics

- Network Sweeping
- OS Discovery
- SYN Scan
- UDP Scan
- XMAS Scan
- FIN Scan
- NULL Scan

Nmap Firewall Scan

- Fragment Scan
- Data Length Scan
- TTL Scan
- Source Port Scan
- Decoy Scan
- Spoof IP Scan
- Spoof MAC Scan
- Data String Scan
- Hex String Scan
- IP Options Scan

Metasploit

- 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

Dictionary & Passwords Attacks

- Hydra
- Medussa
- Crunch
- CeWL
- WCE
- Mimikatz
- cUPP
- Online attacks

FTP Penetration Testing (Port 21)

- Introduction & Lab setup
- Banner Grabbing/Banner Hiding
- Port forwarding /Time Scheduling
- Brute forcing/Secure
- Pivoting/Tunneling [windows]

SSH Penetration Testing (Port 22)

- Introduction & Lab setup
- Banner Grabbing/Banner Hiding
- Port forwarding /Time Scheduling
- Brute forcing/Secure
- Pivoting/Tunneling
- Multiple way to secure ssh

Telnet Penetration Testing (Port 23)

- Introduction & Lab setup
- Banner Grabbing/Banner Hiding
- Port forwarding /Time Scheduling
- Brute forcing/Secure
- Pivoting/Tunneling

SMTP Penetration Testing (Port 25)

- Introduction & Lab setup
- Banner Grabbing/Banner Hiding
- Port forwarding /Time Scheduling
- Brute forcing/Secure
- Penetration testing with SWAKS

DNS & DHCP Penetration Testing (Port 53, 67, 68)

- Introduction & Lab setup
- DNS Enumeration
- DHCP Packet Analysis with Wireshark
- DHCP Starvation attack
- Rogue DHCP Server
- Tools (Gobbler, responder, Yersinia)

NetBIOS & SMB Penetration Testing (Port 135-445)

- Introduction & Lab setup
- SMB Enumeration
- SMB Null Sessions
- Enum4Linux
- NetBIOS Spoofing
- Banner Grabbing/Banner Hiding
- Brute forcing/Secure
- Pivoting/Tunneling
- Penetration Testing with (PS exec, eternal blue)
- Multiple way to connect smb

INFOSECTRAIN

SNMP Penetration Testing (Port 161, 162)

- Introduction & Lab setup
- Banner Grabbing/Banner Hiding
- Port forwarding /Time Scheduling
- Brute forcing/Secure
- Penetration Testing with Metasploit and Nmap

MSSQL Penetration Testing (Port 1433)

- MSSQL Brute force Attack
- Enumerate MSSQL configuration setting
- Identifying SQL Server logins
- Identify Database owner
- Identify a User With masquerade privilege
- Execute SQL Statement
- Retrieve MSSQL Password Hashes of Users
- Decode Password Hashes of Users
- Extracting MYSQL Schema Information

MySQL Penetration Testing (Port 3306)

- Introduction and Lab setup
- MYSQL Brute Force Attack
- mysql banner user/file/ Enumeration
- Stealing MYSQL information
- Check File Privileges
- Enumerate MYSQL writeable directories
- Extract MYSQL Username with Hash Password
- Crack Hash Password with John the Ripper
- Secure MYSQL through port forwarding
- Prevent Mysql against brute force attack

Remote Desktop Penetration Testing (Port 3389)

- Introduction & Lab setup
- Banner Grabbing/Banner Hiding
- Port forwarding /Time Scheduling
- Brute forcing/Secure
- Pivoting/Tunneling
- DOS Attack

VNC Penetration Testing (Port 5900, 5901)

- Introduction & Lab setup
- Banner Grabbing/Banner Hiding
- Port forwarding /Time Scheduling
- Brute forcing/Secure
- Penetration Testing with Metasploit and Nmap
- Pivoting/Tunneling

Sniffing & Spoofing

- Introduction
- ARP Poisoning
- MAC Address Snooping
- DNS Spoofing
- DNS Poisoning
- Capture NTLM Hashes
- Xerosploit

Socks Proxy Penetration Testing

- Socks proxy lab setup
- SSH
- FTP
- HTTP

IDS, Firewall, Honeypots

- Setup Snort Lab in Ubuntu
- Understanding Snort Rules
- Introduction to IPtables
- Introduction to Windows Firewall
- ICMP Detect
- TCP Packet Detect
- Detect Nmap Scan
- Detect Dos Attack
- Antivirus Evasion with veil

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

Social Engineering Attack

- Introduction to Social Engineering Attack
- Payload and Listener Attack
- Java Applet Attack
- HTA Attack
- MSFPC
- DOS Attack
- PowerShell Attack Vector
- VNC Attack

Covering Tracks & Maintaining access

- Persistence
- s4u_persistence
- VSS_Persistence
- Registry Persistence
- Netcat
- Clear Event Logs

Network Vulnerability Assessment Tool

- Nessus
- GFI Languard
- Nexpose
- Openvas
- MBSA

www.infosectrain.com | sales@infosectrain.com