OSCP Exam Preparation Course

Getting Comfortable with Kali Linux

- Booting Up Kali Linux
- The Kali Menu

Finding Your Way Around Kali

- The Linux Filesystem
- Basic Linux Commands
- Finding Files in Kali Linux

Managing Kali Linux Services

- SSH Service
- HTTP Service
- Exercises

Searching, Installing, and Removing Tools

- apt update
- apt upgrade
- apt-cache search and apt show
- apt install
- apt remove –purge
- dpkg

Command Line Fun

- The Bash Environment
- Environment Variables
- Tab Completion
- Bash History Tricks
- Piping and Redirection
- Redirecting to a New File
- Redirecting to an Existing File
- Redirecting from a File
- Redirecting STDERR
- Piping

Text Searching and Manipulation

- grep
- sed
- cut
- awk

Editing Files from the Command Line

- nano

- vi
- Comparing Files
- comm
- diff
- vimdiff

Managing Processes

- Backgrounding Processes (bg)
- Jobs Control: jobs and fg
- Process Control: ps and kill
- File and Command Monitoring
- tail
- watch
- Downloading Files
- wget
- curl
- axel

Customizing the Bash Environment

- Bash History Customization
- Alias
- Persistent Bash Customization
- Netcat
- Connecting to a TCP/UDP Port
- Listening on a TCP/UDP Port
- Transferring Files with Netcat
- Remote Administration with Netcat
- Socat
- Netcat vs Socat
- Socat File Transfers
- Socat Reverse Shells
- Socat Encrypted Bind Shells
- PowerShell and Powercat
- PowerShell File Transfers
- PowerShell Reverse Shells
- PowerShell Bind Shells
- Powercat
- Powercat File Transfers
- Powercat Reverse Shells
- Powercat Bind Shells
- Powercat Stand-Alone Payloads

Packet Capturing

- Wireshark Basics

- Launching Wireshark
- Capture Filters
- Display Filters
- Following TCP Streams
- Tcpdump
- Filtering Traffic
- Advanced Header Filtering

Bash Scripting

- Intro to Bash Scripting
- Variables
- Arguments
- Reading User Input
- If, Else, Elif Statements
- Boolean Logical Operations
- Loops
- For Loops
- While Loops
- Functions
- Practical Examples
- Practical Bash Usage – Example
- Practical Bash Usage – Example
- Practical Bash Usage – Example

Passive Information Gathering

- Taking Notes
- Website Recon
- Whois Enumeration
- Google Hacking
- Netcraft
- Recon-ng
- Open-Source Code
- Shodan
- Security Headers Scanner
- SSL Server Test
- Pastebin
- User Information Gathering
- Email Harvesting
- Password Dumps
- Social Media Tools
- Site-Specific Tools
- Stack Overflow
- Information Gathering Frameworks
- OSINT Framework

- Maltego

Active Information Gathering

- DNS Enumeration
- Interacting with a DNS Server
- Automating Lookups
- Forward Lookup Brute Force
- Reverse Lookup Brute Force
- DNS Zone Transfers
- Relevant Tools in Kali Linux
- Port Scanning
- TCP / UDP Scanning
- Port Scanning with Nmap
- Masscan
- SMB Enumeration
- Scanning for the NetBIOS Service
- Nmap SMB NSE Scripts
- NFS Enumeration
- Scanning for NFS Shares
- Nmap NFS NSE Scripts
- SMTP Enumeration
- SNMP Enumeration
- The SNMP MIB Tree
- Scanning for SNMP
- Windows SNMP Enumeration Example

Vulnerability Scanning

- Vulnerability Scanning Overview and Considerations
- How Vulnerability Scanners Work
- Manual vs Automated Scanning
- Internet Scanning vs Internal Scanning
- Authenticated vs Unauthenticated Scanning
- Vulnerability Scanning with Nessus
- Installing Nessus
- Defining Targets
- Unauthenticated Scanning with Nessus
- Authenticated Scanning with Nessus
- Scanning with Individual Nessus Plugins
- Vulnerability Scanning with Nmap

Web Application Attacks

- Web Application Assessment Methodology
- Web Application Enumeration
- Inspecting URLs

- Inspecting Page Content
- Viewing Response Headers
- Inspecting Sitemaps
- Locating Administration Consoles
- Web Application Assessment Tools
- DIRB
- Burp Suite
- Nikto
- Exploiting Web-based Vulnerabilities
- Exploiting Admin Consoles
- Cross-Site Scripting (XSS)
- Directory Traversal Vulnerabilities
- File Inclusion Vulnerabilities
- SQL Injection
- Extra Miles
- Exercises

Introduction to Buffer Overflows

- Introduction to the x Architecture
- Program Memory
- CPU Registers
- Buffer Overflow Walkthrough
- Sample Vulnerable Code
- Introducing the Immunity Debugger
- Navigating Code
- Overflowing the Buffer
- Exercises
- Windows Buffer Overflows
- Discovering the Vulnerability
- Fuzzing the HTTP Protocol
- Win Buffer Overflow Exploitation
- A Word About DEP, ASLR, and CFG
- Replicating the Crash
- Controlling EIP
- Locating Space for Our Shellcode
- Checking for Bad Characters
- Redirecting the Execution Flow
- Finding a Return Address
- Generating Shellcode with Metasploit
- Getting a Shell

Client-Side Attacks

- Know Your Target
- Passive Client Information Gathering

- Active Client Information Gathering
- Leveraging HTML Applications
- Exploring HTML Applications
- HTA Attack in Action
- Exploiting Microsoft Office
- Installing Microsoft Office
- Microsoft Word Macro
- Object Linking and Embedding
- Evading Protected View
- Wrapping Up
- Locating Public Exploits
- A Word of Caution
- Searching for Exploits
- Online Exploit Resources
- Offline Exploit Resources
- Putting It All Together
- Fixing Exploits
- Fixing Memory Corruption Exploits
- Overview and Considerations
- Importing and Examining the Exploit
- Cross-Compiling Exploit Code
- Changing the Socket Information
- Changing the Return Address
- Changing the Payload
- Changing the Overflow Buffer
- Fixing Web Exploits
- Considerations and Overview
- Selecting the Vulnerability
- Changing Connectivity Information

Antivirus Evasion

- What is Antivirus Software
- Methods of Detecting Malicious Code
- Signature-Based Detection
- Heuristic and Behavioral-Based Detection
- Bypassing Antivirus Detection
- On-Disk Evasion
- In-Memory Evasion
- AV Evasion: Practical Example

Privilege Escalation

- Information Gathering
- Manual Enumeration
- Automated Enumeration

- Windows Privilege Escalation Examples
- Understanding Windows Privileges and Integrity Levels
- Leveraging Unquoted Service Paths
- Linux Privilege Escalation Examples
- Understanding Linux Privileges
- Insecure File Permissions: Cron Case Study
- Insecure File Permissions: /etc/passwd Case Study
- Kernel Vulnerabilities: CVE- - Case Study

Wordlists

- Standard Wordlists
- Brute Force Wordlists
- Common Network Service Attack Methods
- HTTP .htaccess Attack with Medusa
- Remote Desktop Protocol Attack with Crowbar
- SSH Attack with THC-Hydra
- HTTP POST Attack with THC-Hydra
- Leveraging Password Hashes
- Retrieving Password Hashes
- Passing the Hash in Windows
- Password Cracking

Port Redirection and Tunneling

- Port Forwarding
- SSH Tunneling
- SSH Local Port Forwarding
- SSH Remote Port Forwarding
- SSH Dynamic Port Forwarding
- NETSH
- HTTP Tunnelling

Active Directory Attacks

- Active Directory Theory
- Active Directory Enumeration
- Traditional Approach
- A Modern Approach
- Resolving Nested Groups
- Currently Logged on Users
- Enumeration Through Service Principal Names
- Active Directory Authentication
- NTLM Authentication
- Kerberos Authentication
- Cached Credential Storage and Retrieval
- Service Account Attacks

- Low and Slow Password Guessing
- Active Directory Lateral Movement
- Pass the Hash
- Overpass the Hash
- Pass the Ticket
- Active Directory Persistence
- Golden Tickets
- Domain Controller Synchronization

The Metasploit Framework

- Metasploit User Interfaces and Setup
- Getting Familiar with MSF Syntax
- Metasploit Database Access
- Auxiliary Modules
- Exploit Modules
- SyncBreeze Enterprise
- Metasploit Payloads
- Staged vs Non-Staged Payloads
- Meterpreter Payloads
- Experimenting with Meterpreter
- Executable Payloads
- Metasploit Exploit Multi Handler
- Client-Side Attacks
- Advanced Features and Transports
- Building Our Own MSF Module
- Post-Exploitation with Metasploit
- Core Post-Exploitation Features
- Migrating Processes
- Post-Exploitation Modules
- Pivoting with the Metasploit Framework

PowerShell Empire

- Installation, Setup, and Usage
- PowerShell Empire Syntax
- Listeners and Stagers
- The Empire Agent
- PowerShell Modules
- Situational Awareness
- Credentials and Privilege Escalation
- Lateral Movement
- Switching Between Empire and Metasploit

Assembling the Pieces: Penetration Test Breakdown

- Public Network Enumeration

- Targeting the Web Application
- Web Application Enumeration
- SQL Injection Exploitation
- Cracking the Password
- Enumerating the Admin Interface
- Obtaining a Shell
- Post-Exploitation Enumeration
- Creating a Stable Pivot Point
- Targeting the Database
- Enumeration
- Attempting to Exploit the Database
- Deeper Enumeration of the Web Application Server
- More Thorough Post Exploitation
- Privilege Escalation
- Searching for DB Credentials
- Targeting the Database Again
- Exploitation
- Post-Exploitation Enumeration
- Creating a Stable Reverse Tunnel