5 Days

Offensive Security Certified Professional (OSCP)

Offensive Security Certified Professional (OSCP) training is the world's first hands-on offensive information security certification.

An OSCP can demonstrate their ability to:

- Be presented with an unknown network
- Enumerate the targets within their scope
- Exploit the targets within their scope
- Clearly, document their results in a penetration test report

Through a twenty-four (24) hour certification exam, it will challenge the students to prove that they have a clear and practical understanding of the:

- Penetration testing process
- Life-cycle

Note: 30 Days Lab Access with Exam Voucher

Objectives:

You should be able to meet the following objectives after the completion of the course:

- Analyse, correct, modify, cross-compile, and port public exploit code.
- Demonstrate creative problem solving and lateral thinking
- Deploy tunneling techniques to bypass firewalls.
- Identify and exploit XSS, SQL injection, and file inclusion vulnerabilities in web applications.
- Successfully conduct both remote and client-side attacks.
- Write basic scripts & tools to aid in the penetration testing process.
- Using multiple information gathering techniques for identifying and enumerating targets running various operating systems and services.

Course Details

Course Outline

Module 1: Penetration Testing

- About Kali Linux

- About Penetration Testing
- Legal
- The megacorpone.com Domain
- Offensive Security Labs

Module 2: Getting Comfortable with Kali Linux

- Managing Kali Linux Services
- The Bash Environment
- Intro to Bash Scripting

Module 3: The Essential Tools

- Netcam
- Ncat
- Wireshark
- Tcpdump

Module 4: Passive Information Gathering

- Open Web Information Gathering
- Email Harvesting
- Additional Resources
- Recon-ng

Module 5: Active Information Gathering

- DNS Enumeration
- Port Scanning
- SMB Enumeration
- SMTP Enumeration
- SNMP Enumeration

Module 6: Vulnerability Scanning

- Vulnerability Scanning with Nmap
- The OpenVAS Vulnerability Scanner

Module 7: Buffer Overflows

- Fuzzing

Module 8: Win32 Buffer Overflow Exploitation

- Replicating the Crash
- Controlling EIP
- Locating Space for Your Shellcode
- Checking for Bad Characters
- Redirecting the Execution Flow
- Generating Shellcode with Metasploit
- Getting a Shell
- Improving the Exploit

Module 9: Linux Buffer Overflow Exploitation

- Controlling EIP
- Finding Space for Our Shellcode
- Improving Exploit Reliability
- Discovering Bad Characters
- Finding a Return Address
- Getting a Shell

Module 10: Working with Exploits

- Searching for Exploits
- Customizing and Fixing Exploits

Module 11: File Transfers

- A Word About Anti-Virus Software
- File Transfer Methods

Module 12: Privilege Escalation

- Privilege Escalation Exploits
- Configuration Issues

Module 13: Client Side Attacks

- Know Your Target
- MS12-037- Internet Explorer 8 Fixed Col Span ID
- Java Signed Applet Attack

Module 14: Web Application Attacks

- Essential Ice-Weasel Add-ons
- Cross Site Scripting (XSS)
- File Inclusion Vulnerabilities

- MySQL SQL Injection
- Web Application Proxies
- Automated SQL Injection Tools

Module 15: Password Attacks

- Prepare for Brute Force
- Online Password Attacks
- Password Hash Attacks

Module 16: Port Redirection and Tunnelling

- Port Forwarding/Redirection
- SSH Tunnelling
- Proxy chains
- HTTP Tunnelling
- Traffic Encapsulation

Module 17: The Metasploit Framework

- Metasploit User Interfaces
- Setup Metasploit Framework on Kali
- Explore the Metasploit Framework
- Auxiliary Modules
- Exploit Modules
- Metasploit Payloads
- Build Your Own MSF Module
- Post Exploitation with Metasploit

Module 18: Bypassing Antivirus Software

- Encode Payloads with Metasploit
- Cryptic Known Malware with Software Protectors
- Use Custom/Uncommon Tools and Payloads

Module 19: Assembling the Pieces: Penetration Test Breakdown

- Phase 0 – Scenario Description
- Phase 1 – Information Gathering
- Phase 2 – Vulnerability Identification and Prioritization
- Phase 3 – Research and Development
- Phase 4 – Exploitation

- Phase 5 – Post-Exploitation

Who Should Attend

The OSCP Course is ideal for:

- Security officers
- Security Professionals
- Auditors
- Site Administrators

Pre Requisite

- Basic know-how of Networking
- Basic Knowledge of Server and Network Components

464, Udyog Vihar Phase V,Gurgaon (Delhi NCR)-122016,India	+91 8882 233 777	training@mercury.co.in	www.mercurysolutions.co

Date - Apr 25, 2024