Pen-200 OSCP

Training and Certification

Cyber Security Educational Courses Professional Sessions

ABOUT US

We offer Cyber Security and Information Security training and Certification in Delhi for Cyber Security and Information Technology aspirants. Since Decade, we have been in the Information Technology and Cybersecurity industry. You can learn more about cybersecurity, Techniques, and Tools to choose a better career path.

DESCRIPTION ⌄

The industry-leading Penetration Testing with Kali Linux (PWK/PEN-200) course just got even better with the addition of five recently retired OSCP exam machines to PWK labs. These five machines represent an entire OSCP exam room! Get more value out of your lab time for the same price, and enjoy extra preparation for the OSCP exam.

Duration - 80 to 100 Hrs

Language - Hindi & English

Mode - Online & Offline

BENEFITS ⌄

1. Basic to Advanced Courses
2. Interview Cracking and Proposal-Making Sessions
3. Transparent Syllabus
4. Career-Oriented Courses and Certifications
5. International Accreditation

CRAW
A C A D E M Y

📍 SAKET ADDRESS

1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station, Saidulajab New Delhi - 110030

📍 LAXMI NAGAR ADDRESS

R31/ 32, 2nd floor Jandu Tower, Vikas marg, Shakarpur, New Delhi -110092

🌐 www.craw.in

📞 +91 951 380 5401

SAMPLE CERTIFICATE

PEN-200 OSCP COURSE MODULE

FOR LINUX MACHINES:

Module	Description
Module 01: Penetration Testing: What You Should Know	• Overview of penetration testing methodologies and ethical hacking. • Legal and ethical considerations in penetration testing. • Understanding different types of penetration tests (black box, white box, grey box). • The role of a penetration tester and the penetration testing process.
Module 02: Getting Comfortable with Kali Linux	• Introduction to Kali Linux as a penetration testing platform. • Navigating the Kali Linux environment and understanding its tools. • Basic Linux commands and file system structure. • Package management and software installation. • Virtualization and network configuration.
Module 03: Command Line Fun	• Advanced Linux command-line usage. • Text processing tools like sed, awk, and grep. • Scripting basics for automation. • Regular expressions for pattern matching.
Module 04: Practical Tools	• Introduction to essential penetration testing tools. • Network scanning tools (Nmap, Masscan). • Vulnerability scanning tools (Nessus, OpenVAS). • Exploitation tools (Metasploit, exploit-db). • Post-exploitation tools (Powercat, Mimikatz).
Module 05: Bash Scripting	• Writing and executing Bash scripts for automation. • Scripting for information gathering, exploitation, and post-exploitation. • Integrating tools and commands into scripts.
Module 06: Passive Information Gathering	• Techniques for collecting information about a target without interacting with it. • Using search engines, social media, and open sources for intelligence. • Analyzing network traffic and DNS records. • WHOIS lookups and domain registration information.
Module 07: Active Information Gathering	• Interacting with a target to gather information. • Port scanning and service identification. • Banner grabbing and version detection. • Directory and file enumeration.

Module	Description
Module 08: Vulnerability Scanning	• Identifying vulnerabilities in systems and applications. • Using vulnerability scanners to automate the process. • Analyzing scan results and prioritizing vulnerabilities.
Module 09: Web Application Attacks	• Understanding web application architecture and vulnerabilities. • Common web application attacks (SQL injection, XSS, CSRF, etc.). • Manual and automated web application testing.
Module 10: Client-Side Attacks	• Exploiting vulnerabilities in web browsers and client-side applications. • Cross-site scripting (XSS) attacks. • Malware delivery through malicious websites.
Module 11: Locating Public Exploits	• Finding exploits for identified vulnerabilities. • Using exploit databases and frameworks. • Understanding exploit code and development.
Module 12: Fixing Exploits	• Modifying and adapting exploits for specific targets. • Bypassing security measures and defenses. • Creating custom exploit code.
Module 13: File Transfers	• Techniques for transferring files between systems. • Secure file transfer protocols (SCP, SFTP). • Data exfiltration methods.
Module 14: Antivirus Evasion	• Techniques to bypass antivirus detection. • Encoding and obfuscation of malicious code. • Fileless execution and persistence.
Module 15: Privilege Escalation	• Gaining higher privileges on a compromised system. • Exploiting system vulnerabilities and misconfigurations. • Lateral movement within a network.
Module 16: Password Attacks	• Cracking passwords using different techniques (brute force, dictionary, rainbow tables). • Password recovery tools and techniques.
Module 17: Port Redirection and Tunneling	• Establishing secure connections through firewalls. • Port forwarding and tunneling protocols (SSH, SOCKS).
Module 18: The Metasploit Framework	• Using Metasploit for exploitation and post-exploitation. • Developing custom payloads and exploits. • Meterpreter and its capabilities.

FOR WINDOWS MACHINES:

Module	Description
Module 01: Penetration Testing: What You Should Know	• Overview of penetration testing methodologies and ethical hacking. • Legal and ethical considerations in penetration testing. • Understanding different types of penetration tests (black box, white box, grey box). • The role of a penetration tester and the penetration testing process.
Module 02: Command Line Fun	• Basic Windows command-line (cmd) usage. • PowerShell basics for automation and scripting.
Module 03: Practical Tools	• Windows-specific penetration testing tools. • Active Directory reconnaissance tools. • Privilege escalation tools.
Module 04: Passive Information Gathering	• Techniques for collecting information about a target without interacting with it. • Using search engines, social media, and open sources for intelligence. • Analyzing network traffic and DNS records. • WHOIS lookups and domain registration information.
Module 05: Active Information Gathering	• Interacting with a target to gather information. • Port scanning and service identification. • Banner grabbing and version detection. • Directory and file enumeration.
Module 06: Vulnerability Scanning	• Identifying vulnerabilities in systems and applications. • Using vulnerability scanners to automate the process. • Analyzing scan results and prioritizing vulnerabilities.
Module 07: Web Application Attacks	• Understanding web application architecture and vulnerabilities. • Common web application attacks (SQL injection, XSS, CSRF, etc.). • Manual and automated web application testing.
Module 08: Client-Side Attacks	• Exploiting vulnerabilities in web browsers and client-side applications. • Cross-site scripting (XSS) attacks. • Malware delivery through malicious websites.
Module 09: Locating Public Exploits	• Finding exploits for identified vulnerabilities. • Using exploit databases and frameworks. • Understanding exploit code and development.
Module 10: Fixing Exploits	• Modifying and adapting exploits for specific targets. • Bypassing security measures and defenses. • Creating custom exploit code.
Module 11: File Transfers	• Techniques for transferring files between systems. • Secure file transfer protocols (SCP, SFTP). • Data exfiltration methods.

Module	Description
Module 12: Antivirus Evasion	- Techniques to bypass antivirus detection. - Encoding and obfuscation of malicious code. - Fileless execution and persistence.
Module 13: Privilege Escalation	- Gaining higher privileges on a compromised system. - Exploiting system vulnerabilities and misconfigurations. - Lateral movement within a network.
Module 14: Password Attacks	- Cracking passwords using different techniques (brute force, dictionary, rainbow tables). - Password recovery tools and techniques.
Module 15: Port Redirection and Tunneling	- Establishing secure connections through firewalls. - Port forwarding and tunneling protocols (SSH, SOCKS).
Module 16: Active Directory Attacks	- Understanding Active Directory structure and vulnerabilities. - Attacking Active Directory for domain dominance. - Privilege escalation within Active Directory.
Module 17: The Metasploit Framework	- Using Metasploit for exploitation and post-exploitation with a focus on Windows exploits and payloads. - Developing custom payloads and exploits. - Meterpreter and its capabilities.
Module 18: PowerShell Empire	- Using PowerShell Empire for post-exploitation and command and control. - Developing custom PowerShell agents and stagers.
Module 19: Assembling the Pieces: Penetration Test Breakdown	- Integrating learned skills into a full penetration test. - Reporting and documentation. - Ethical and legal considerations in reporting findings.
Module 20: Trying Harder: The Labs	- Advanced labs and challenges to enhance skills. - Real-world scenario simulations. - Preparation for the OSCP certification exam.