Mindluster Platform

About the course OSCP Training 2024

Course Presenter : Motasem Hamdan

OSCP Training 2024 course is a comprehensive program offered by Offensive Security. Explore hands-on offensive security techniques, including network penetration testing and exploit development. Learn to identify vulnerabilities, exploit systems, and gain practical experience in real-world scenarios. Develop skills in information gathering, vulnerability assessment, and post-exploitation. Join this course to enhance your understanding of offensive security and prepare for the OSCP certification, a highly recognized credential in the cybersecurity industry. Please note that for pricing and specific course details, it is recommended to refer to the official Offensive Security website. Motasem Hamdan

Computer Science Category's Courses

Course Lesson(160)

Lesson 1 : **From Local File Inclusion to Remote Shell OSCP Preparation**

Lesson 2 : **HTTP Headers Manipulation Linux Privilege Escalation Vulnhub CTF**

Lesson 3 : **Linux Penetration Testing and Privilege Escalation Sunrise Vulnhub Walkthrough**

Lesson 4 : **OWASP Directory Traversal Sunrise Vulnhub Walkthrough**

Lesson 5 : **Linux Penetration Testing and Privilege Escalation DC9 Vulnhub Walkthrough**

Lesson 6 : **Automated Fuzzing and Testing For Buffer Overflow P5**

Lesson 7 : **Firewall and IDS Evasion with NMAP Practical Scenario**

Lesson 8 : **SNMP Enumeration Information Gathering 6**

Lesson 9 : **Mastering Shodan Search Engine Filters OSINT 5**

Lesson 10 : **Linux Penetration Testing HA Naruto Vulnhub Walkthrough**

Lesson 11 : **Pentesting HTTP Headers Authentication with Burp Suite HA Joker Vulnhub**

Lesson 12 : **Wordpress Penetration Testing prime 1 Vulnhub CTF Walkthrough**

Lesson 13 : **OWASP Local File Inclusion Vulnerability Prime 1 Vulnhub CTF Walkthrough**

Lesson 14 : **Linux Privilege Escalation and Penetration Testing Red Team Training AI Web Vulnhub**

Lesson 15 : **SQL Injection With SQL map Database Penetration Testing AI Web Vulnhub**

Lesson 16 : **MYSQL Database Manipulation with sqlmap Red Team Training Aiweb1 vulnhub**

Lesson 17 :
Linux Privilege Escalation and Penetration Testing Training GrimTheRipper CTF Vulnhub

Lesson 18 :
Linux Privilege Escalation and Pentesting Red Team Training Nezuko Vulnhub Walkthrough

Lesson 19 : **Practical Web Application Pentesting Red Team Training Nezuko CTF vulnhub**

Lesson 20 : **Blue Team Cyber Security Training Nmap Scanning**

Lesson 21 : **MyHouse7 Vulnhub Walkthrough Part 2 Network Pivoting**

Lesson 22 :
My House7 Vulnhub Walkthrough Part 1 Penetration Testing and Cybersecurity Training

Lesson 23 : **Raven 2 Vulnhub Walkthrough Penetration Testing and Cybersecurity Training**

Lesson 24 : **Machine Matrix Vulnhub Walkthrough Limited Shell**

Lesson 25 : **Lampaio Vulnhub CTF Walkthrough OSCP Training**

Lesson 26 : **WinterMute Vulnhub CTF Walkthrogh OSCP machine**

Lesson 27 : **Bulldog2 CTF vulnhub walkthrough OSCP Intermediate level**

Lesson 28 : **GoldenEye Vulnhub CTF walkthrough OSCP Machine**

Lesson 29 :
Basic Pentesting 2 Vulnhub Walkthrough CTF Penetration Testing and Cybersecurity Training

Lesson 30 : **Toppo Vulnhub CTF walkthrough OSCP Training**

Lesson 31 : **Orcus Vulnhub CTF Walkthrough OSCP Training**

Lesson 32 : **Super Mario Vulnhub Walkthrough Part 2 OSCP Training**

Lesson 33 : **Super Mario Vulnhub Walkthrough Network Pivoting part1**

Lesson 34 : **Pinky Palace V2 Vulnhub walkthrough RCE and Buffer Over Flow P7**

Lesson 35 :
Pinky s Palace V1 Vulnhub CTF Walkthrough Penetration Testing and Cybersecurity Training

Lesson 36 : **Penetration Testing For Beginners Blackmarket Vulnhub CTF Walkthrough**

Lesson 37 : **Port Knocking Cyberry Vulnhub CTF Walkthrough P1**

Lesson 38 : **Binary Exploitation with GDB Debugger Cyberry Vulnhub CTF Walkthrough P2**

Lesson 39 : **Linux Privilege Escalation EP1 Zico2 Vulnhub CTF Walkthrough P2**

Lesson 40 : **PhpMyAdmin Command Injection EP1 Zico2 VulnHub CTF Walkthrough**

Lesson 41 : **From Web Into SSH Shell Covfefe VulnHub CTF WalkThrough**

Lesson 42 : **Practical Command Injection with Burp Suite EP2 OWASP Hackademic Challenge 008**

Lesson 43 : **Ultimate Guide to Manual SQL Injection Testing and Training**

Lesson 44 : **Windows and Linux Privilege Escalation OSCP Prep**

Lesson 45 : **Active Directory Penetration testing with Powershell and Mimikatz Part 3**

Lesson 46 : **Active Directory Privilege Escalation on Windows Server Pentesting Part 4**

Lesson 47 : **Privilege Escalation and Persistence on Windows Server AD Part 5**

Lesson 48 : **Metasploit Framework Series Metasploit with Nmap Scanning Part 1**

Lesson 49 :
Metasploit Framework Tutorial Series Taking a look at Testing Antivirus Strength Part 2

Lesson 50 : **Windows Privilege Escalation and Keyboard Sniffing with Metasploit and Powershell**

Lesson 51 : **Database Penetration testing and Privilege Escalation OSCP 2020**

Lesson 52 : **Cybesecurity and Penetration testing Home Lab OSCP 2020**

Lesson 53 : **Essential Linux Course For Penetration testing OSCP 2020**

Lesson 54 : **Information Gathering For Penetration Testing OSCP 2020**

Lesson 55 : **Vulnerability scanning with Nmap and Metasploit OSCP Prep**

Lesson 56 :
Solving Penetration Testing and CTF Challenge for OSCP Photographer Vulnhub Walkthrough

Lesson 57 : **Linux Essentials Course For Penetration Testing Part 2**

Lesson 58 : **Scanning Networks with Python and Nmap Python Penetration Testing**

Lesson 59 : **PhpMyAdmin and MySQL Database Penetration testing OSCP 2020**

Lesson 60 : **Wordperss Penetration Testing So simple 1 Vulnhub**

Lesson 61 : **Windows Penetration Testing Part 1 tryhackme Eternal Blue**

Lesson 62 : **Active Directory Penetration Testing on Windows Server Part 2**

Lesson 63 : **Active Directory Penetration Testing on Windows Server Part 1**

Lesson 64 : **Explaining Microsoft Word Remote Code Execution**

Lesson 65 : **Explaining HTML Based Exploitation with Powershell Windows Penetration Testing**

Lesson 66 : **Penetration Testing Series Part 6 Cyberseclabs Potato Walkthrough**

Lesson 67 : **Penetration testing series Part8 Cyberseclabs Boats Walkthrough**

Lesson 68 : **Penetration testing series Part10 Cyberseclabs CMS walkthrough**

Lesson 69 : **Windows Operating System Pentration Testing EP1 Cyberseclabs Cold**

Lesson 70 : **Windows Registry Privilege Escalation Cyberseclabs Glass Walkthrough**

Lesson 71 : **Windows Services Privilege Escalation Cyberseclabs Cold Walkthrough**

Lesson 72 : **Python Training Cyberseclabs Fuel Walkthrough**

Lesson 73 : **Windows Privilege Escalation in XML Files Cyberseclabs Unattend**

Lesson 74 : **Basic and Easy to learn Linux Penetration Testing Cyberseclabs PIE**

Lesson 75 : **FTP Penetration Testing Cyberseclabs Imposter**

Lesson 76 :
Learnning Windows Privilege Escalation Through DLL Hijacking Cyberseclabs Walkthrough

Lesson 77 : **Windows Privilege Escalation Through Windows Services Cyberseclabs SAM**

Lesson 78 : **Linux Privilege Escalation Through Security Misconfigurations Cyberseclabs Unroot**

Lesson 79 : **Linux Penetration Testing and Cybersecurity Training Cyberseclabs Outdated**

Lesson 80 : **Windows Weak Login Credentials Cyberseclabs Weak**

Lesson 81 : **Windows Penetration Testing Training Metasploitable 3**

Lesson 82 : **File Upload Vulnerability P2 Cyberseclabs Engine**

Lesson 83 :
Learning Metasploitable 3 Part 2 Windows Penetration Testing and Cybersecurity Training

Lesson 84 : **How to Decrypt Password Databases Offline Cyberseclabs Stack**

Lesson 85 : **Unquoted services in Windows Server Cyberseclabs Deployable**

Lesson 86 : **Windows Penetration Testing and Cybersecurity Training Metaslpoitable 3**

Lesson 87 : **Demonstrating Linux Systemctl Services Exploitation Cyberseclabs Simple**

Lesson 88 :
Linux Privilege Escalation Through Misconfigured File Permissions Cyberseclabs Leakage

Lesson 89 : **Using Python and SSH To Gain Root Access Cyberseclabs Shares**

Lesson 90 : **Demonstrating Web Application Vulnerabilities Cyberseclabs Shock**

Lesson 91 : **How to Perform Windows Active Directory Penetration Testing Cybeseclabs Secret**

Lesson 92 : **The Zero Logon Active Directory Vulnerability Cyberseclabs Zero**

Lesson 93 : **Using Python Interpreters and Hex Editors To Gain Root Access Cyberseclabs Debug**

Lesson 94 : **Advanced Active Directory Penetration Testing Cyberseclabs Sync**

Lesson 95 :
Experiment on Bypassing Windows Anti Malware Scanner with Powershell Cyberseclabs Toast

Lesson 96 : **CTF Walkthrough Using Azure DevOps To Gain Administrative Access to Windows**

Lesson 97 : **Pentesting Microsoft SQL Server In Windows Active Directory Cyberseclabs Mount**

Lesson 98 : **Pentesting Windows XP Manually CTF Walkthrough**

Lesson 99 :
Extract FireFox Browser Credentials in Windows Active Directory Cyberseclabs Dictionary

Lesson 100 : **Pentesting Service Accounts in Windows Active Directory Cyberseclabs Roast**

Lesson 101 : **DNS Admins in Windows Active Directory Cyberseclabs Brute**

Lesson 102 : **Pentesting WordPress And Accessing Filtered Ports Cyberseclabs Office**

Lesson 103 : **IP Telephony and CRM Sales Software CTF Walkthrough**

Lesson 104 : **Pentesting Windows Server 2012 R2 CTF Walkthrough**

Lesson 105 : **Pentesting Windows Server 2008 DataCenter CTF Walkthrough**

Lesson 106 : **Windows Active Directory Drivers CTF Walkthrough**

Lesson 107 : **Microsoft IIS Web Server Vulnerabilities CTF Walkthrough OSCP Prep**

Lesson 108 : **OSCP Realistic Linux Machine Nully Cybersecurity Vulnhub**

Lesson 109 : **Windows Services with Weak Permissions TryHackMe Steel Mountain Mr Robot**

Lesson 110 : **FTP and Linux Environment Variables TryHackMe Kenobi**

Lesson 111 : **Linux lxd Group For Privilege Escalation OSCP HackTheBack Tabby**

Lesson 112 : **File Upload Vulnerability Adobe Cold Fusion 8 P3 CTF Walkthrough**

Lesson 113 : **Bypassing File Upload Filters P4 CTF Walkthrough**

Lesson 114 : **Laravel PHP Framework CTF Walkthrough**

Lesson 115 : **Using Python Modules For Root Access TryHackMe Jack**

Lesson 116 : **Demonstrating PHP Filters Bypass For Local File Inclusion TryHackMe DogCat**

Lesson 117 : **Windows 10 Enterprise Buffer OverFlow CTF Walkthrough**

Lesson 118 : **Buffer Overflow in IIS Server 6 CTF Walkthrough**

Lesson 119 : **Easy OSCP Linux Machine CTF Walkthrough**

Lesson 120 : **Simple OSCP Windows Box CTF Walkthrough**

Lesson 121 : **Active Directory Penetration Testing Lab TryHackMe Attacktive Directory**

Lesson 122 : **Demonstrationg Buffer Overflow and ASLR Protection P4 CTF Walkthrough**

Lesson 123 : **TryHackMe OSCP Pathway Alfred Walkthrough**

Lesson 124 : **Pentesting Windows Scheduled Tasks TryHackMe OSCP Pathway HackPark**

Lesson 125 : **Demonstrating SQL Injection and SSH tunnels TryHackMe OSCP Pathway GameZone**

Lesson 126 : **Pentesting Linux Screen GNU Tool CTF Walkthrough**

Lesson 127 : **Pentesting Wild Cards in Linux File Archiving TryHackMe OSCP Path The Terminal**

Lesson 128 : **Analyzing Cyber Security Incidents TryHackMe Overpass 2**

Lesson 129 : **Demonstrating Black Box Penetration Testing TryHackMe Relevant**

Lesson 130 : **Pentesting Jenkins Server and SSH Tunnels TryHackMe OSCP Internal**

Lesson 131 : **Basics of Powershell For Penetration Testers TryHackMe Hacking with Powershell P1**

Lesson 132 :
Explaining Buffer Overflow with Immunity Debugger P1 TryHackMe Buffer Overflow P1

Lesson 133 :
Basics of PowerShell P2 Port Scanning and Pattern Matching TryHackme Hacking with Powershell

Lesson 134 : **Practicing Buffer OverFlow P8 TryHackMe Solving All Tasks**

Lesson 135 : **Demonstrating Windows App Locker Bypass TryHackMe OSCP Pathway Corp**

Lesson 136 : **WordPress Penetration Testing and Nmap Interactive TryHackMe OSCP Mr Robot**

Lesson 137 : **Pentesting Windows Server 2016 Three Methods TryHackMe OSCP Retro**

Lesson 138 : **Demonstrating Windows Post Exploitation OSCP Blaster TryHackMe**

Lesson 139 : **Demonstrating PHPliteAdmin and Chkrootkit takeover OSCP CTF Walkthrough**

Lesson 140 : **Linux CVE 2017 6074 OSCP CTF Walkthrough**

Lesson 141 : **Docker Containers Exploitation Explained CTF Walkthrough**

Lesson 142 : **Windows Pass The Hash Technique and Persistence CTF Walkthrough**

Lesson 143 : **Exploiting Node js and Buffer OverFlow using RET2GOT P13 CTF Walkthrough**

Lesson 144 : **Windows Active Directory PAC Vulnerability CTF Walkthrough**

Lesson 145 : **Demonstrating BufferOver Flow using Pwndbg P12 TryHackMe The Cod Caper**

Lesson 146 : **Steganography and SUDO exploitation Agent Sudo TryHackMe**

Lesson 147 : **XML External Entity Injection and Wordpress Login Poisoning CTF Walkthrough**

Lesson 148 : **Remote Buffer OverFlow P22 and Windows Privilege Escalation CTF Walkthrough**

Lesson 149 : **Pentesting OpenClinic Healthcare Management System TryHackMe Flatline**

Lesson 150 : **Pentesting Traffic Management System TryHackMe Plotted TMS**

Lesson 151 : **Penetration Testing for Healthcare OpenEMR system HIPAA TryHackMe Plotted EMR**

Lesson 152 : **Network Pivoting on Windows Active Directory CTF Walkthrough**

Lesson 153 : **Docker Containers Exploitation Explained CTF Walkthrough**

Lesson 154 : **HeartBleed Vulnerability and Tmux Exploitation CTF Walkthrough**

Lesson 155 :
The Complete Linux Privilege Escalation Capstone TryHackMe Junior Penetration Tester

Lesson 156 : **Cookie Security Via HTTPONLY and secure Flag OWASP Top 10**

Lesson 157 : **NFS Protocol Explained TryHackMe Network Services 2**

Lesson 158 : **Weaponization Explained Cyber Kill Chain TryHackMe Weaponization**

Lesson 159 : **Password Attacks Explained Part Two TryHackMe**

Lesson 160 : **Local File Inclusion Log Poisoning Explained CTF Walkthrough**

Related courses

Linear Algebra for Computer Scientists

Insertion Sort

Bubble Sort

GCSE Computer Science

Random Access Memory

Binary Trees