iGNITE Technologies

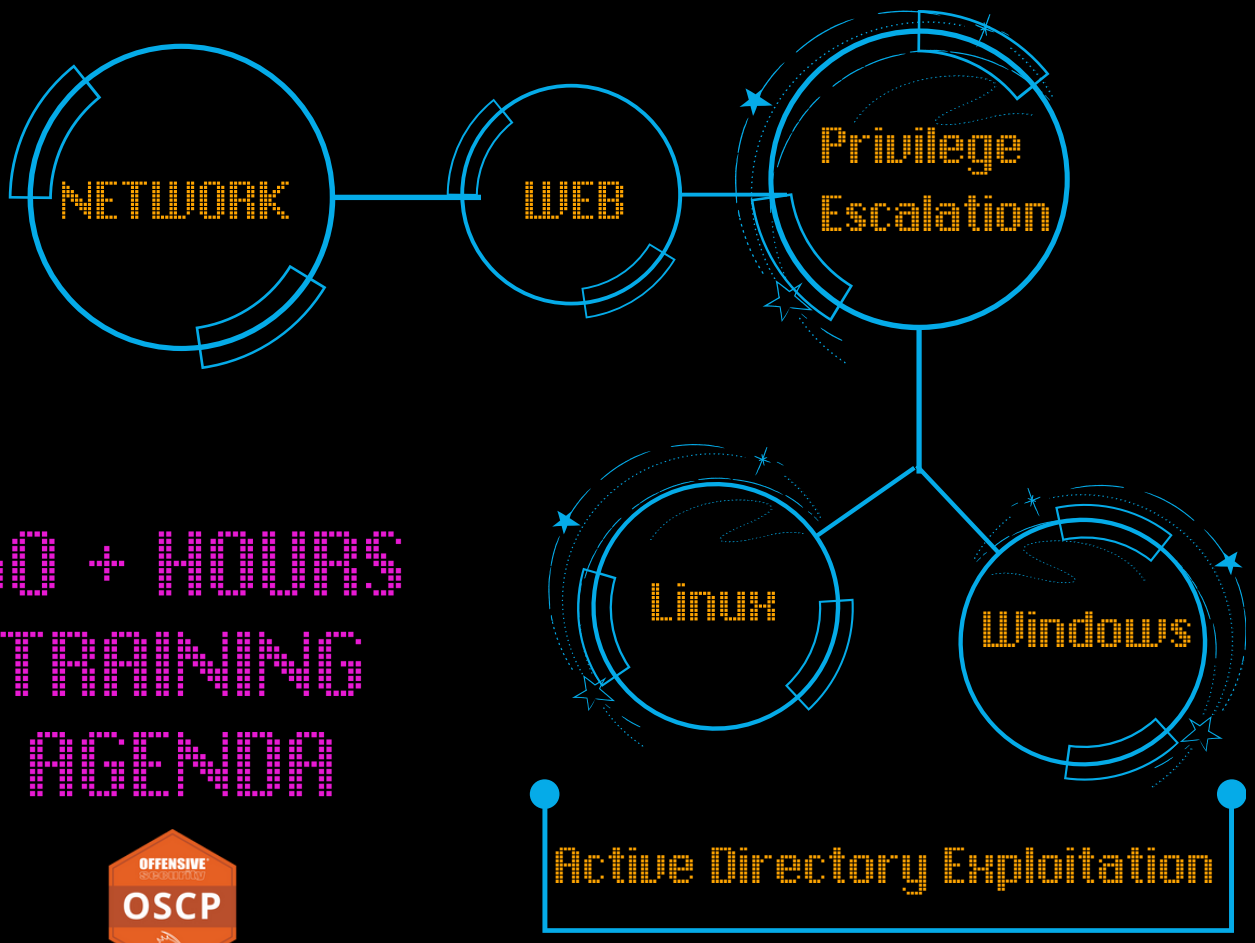
Get Ready for OSCP + with advanced pentesting skills

CTF +

Capture the Flag.....

www.ignitetechnologies.in

iGNITE Technologies



60 + HOURS TRAINING AGENDA

OFFENSIVE SECURITY OSCP

Who needs CTF Learning?

If the candidate wants to achieve accreditation such as **CREST, OSCP, Advanced Network Pentesting** and etc then needs to solve CTFs that which is based on real-time scenarios. This course will focus on core concepts that will the candidate the tricks and techniques to solve the challenge.

CTF for OSCP Practice

SECTION -A : 6 WEEKS JOURNEY

Course Introduction

Objective: This module will define the OSCP Guidelines and the holistic approach to be followed for OSCP preparation.

- About the OSCP exam pattern
- Points breakouts of the Exam machines
- Exam Preparation methodologies
- Introduction to Note keeping tools
- Introduction to Note and Chee sheet keeping methodologies
- Information about the Exam and Lab Guidelines

Network Enumeration

Objective: This module will focus on the enumeration of TCP and UDP services to identify the loopholes and sensitive information to proceed for the Initial foothold.

- FTP
- SMB Pentesting
- NFS Pentesting
- LDAP
- SNMP
- MSSQL/Postgre

Tools: Nmap & Scripts, Metasploit, Enum4linux, Ldapsearch, Smbclient, Snmpwalk and Responder, Impacket-psexec and etc.

Hunting Public Exploit

Objective: This module will focus on how to hunt for the exploit for vulnerable software packets in online and offline modes.

- Offline Exploit Resources
- Online Exploit Resources

Tools: Exploit-DB, Packetstrome, Github, Searchsploit, Nmap-NSE Script

Web Application Attacks

Objective: This module will focus on web application exploitation by injecting payloads and establishing initial footholds.

- Web Application Assessment Tools
- Web Application Enumeration
- Web Shells and One-liner payloads
- Directory Traversal
- File Inclusion Vulnerabilities
- File Upload Vulnerabilities
- Command Injection
- SQL Injection-Manual

Tools: Impacket-Mssqlclient, Webshells (multiple type and technique), Feroxbuster, jwt.io, Burpsuite.

Password Attack

Objective: This module will focus on the password attack technique and tools for remote login services.

- Attacking Network Services Logins (Hydra, Crackmapexec)
- Password Cracking Fundamentals (Crackstation, John, Hashcat)
- Access the Services (SSH, SMB, RDP, FTP)

Tools: Hydra, Crackmapexec, Crackstation, John, Hashcat

Port forwarding & Tunneling

Objective: The module is very important with respect to OSCP and majorly part of insane labs where the pentester need to perform lateral movement and try to connect the machine to the different network through port forwarding and pivoting.

- Port forwarding from Linux to Windows.
- Port forwarding from Windows to Linux
- Port forwarding Linux to Linux
- Tunneling: Local, Remote and dynamic

Tools: Proxychain, Chisel, SSH Tunneling, Ligolo-ng

Windows Exploitation & Privilege Escalation

Objective: This module will focus on the basic utilities and, dangerous permission, exploitation and privilege escalation.

- Windows Powershell
- Windows file transfer
- Windows basic commands
- Windows Reverse shell & one-linear payloads
- Post Enumeration
- DLL hijacking
- Absuing SAM & Registry Hive
- Unquoted Path
- Always Install Elevated
- Scheduled Tasks
- SEImpersonate
- UAC bypass & Runcmdas
- Kernel exploit

Tools: Powershell scripts, Msfvenom, Revshell, Winpeas, Impact-Smbshare, mimkatz, Metasploit.

Linux Privilege Escalation

Objective: This module will focus on the basic utilities and, dangerous permission, exploitation and privilege escalation.

- Fundamentals of Linux
- Understanding Files and Users Privileges on Linux
- Manual Enumeration
- Abusing Cron Jobs
- Abusing Password Authentication
- SSH RSA Key Authentication
- Linux Privilege Escalation
- Automated Post Enumeration
- Abusing SUID Permissions
- Abusing Sudo Rights
- Abusing Group Premissions
- Python Liberary Hijacking
- Exploiting Kernel Vulnerabilities

Tools: Netcat, Revshell, SSH-keygen, Gftobin, OpenSSL, Linpeas,

SECTION -B : 2 WEEKS JOURNEY

Active Directory

Objective: The module is very important with respect to OSCP, in this section the trainer will focus on Active Directory Enumeration, Exploitation, Post Exploitation, Credential Dumping, and Lateral Movement.

- Active Directory Introduction, Labsetup and Enumeration
- Active Directory - Manual Enumeration
- Manual Enumeration - Expanding our Repertoire
- Active Directory - Automated Enumeration
- Attacking Active Directory Authentication
- Enumeration
- Multiple Kerberos Attack
- Abusing DACL
- Abusing Group Permission
- Credential Dumping
- DC Sync Attack
- SAM vs NTDS.dit
- Domain Cache Credential
- Pass the Hash-RDP
- Privilege Escalation
- Lateral Movement in Domain Network

Tools: Mimikatz, Evilwinrm, Crackmapexec, Impacket, Remmina, Rubeus, Powerview, Ad Recon, Bloodhound and etc.

SECTION -C : 4 WEEKS JOURNEY

Capture The Flags
Objective: The aim of the training is to explain how to solve vulnerable boxes by compromising vulnerabilities related to the Web, Networks, Cryptography, and Privilege Escalation of Windows and Linux OS and get the privilege of the administrator/root user account.

- Easy CTF Linux / Windows/AD.
- Medium CTF Linux / Windows, /AD.
- Insan CTF Linux / Windows/AD.

Platform: Hack The Box , Vulnhub, Try Hack Me, Offesc PG labs

Note to Readers:

The CTF training program is structured for approximately 12 weeks. The exact duration may vary depending on session schedules, such as 2-hour or 4-hour batches, and the total weekly training hours. This flexible approach ensures an optimal learning experience tailored to the batch timings. For more details, feel free to contact us.

Contact US

PHONE

+91-9599387841 | +91 9599387841

WHATSAPP

https://wa.me/message/HIOPPNENLOX6F1

EMAIL ADDRESS

info@ignitetechnologies.in

WEBSITE

www.ignitetechnologies.in

BLOG

www.hackingarticles.in

LINKEDIN

https://www.linkedin.com/company/hackingarticles/

TWITTER

https://twitter.com/hackinarticles

GITHUB

https://github.com/Ignitetechnologies

iGNITE Technologies