iGNITE Technologies

CTF

2023

ITS TIME FOR OSCP

Training and Services

CTF

ABOUT COURSE

CTF is the latest edition of our training which provides the most advanced modules that connect to the real infrastructures in the organizations and also assist students/professionals to prepare for **global certifications** such as OSCP. This curriculum has been designed in such a manner that it accommodates both freshers and specialists and provides them with the necessary training w.r.t their skills.

Capture the Flag is an information security competition that is an amalgamation of various challenges that applies concepts like **Reverse engineering, Web Applications, Binary, Network, Cryptography, Forensics**, etc. Each challenge holds a certain number of points based on its difficulty level. The idea behind these CTFs is to provide an individual with practical knowledge of the different kinds of attacks and issues in the real world.

AGENDA

Active Directory Exploitation

Who needs CTF Learning?

If the candidate wants to achieve accreditation such as CREST, OSCP, 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.

ROADMAP

Stage 1 (1)
Basic of Network & Web

Stage 2 (2)
Basic of Linux & Windows

Stage 3 (3)
Ethical Hacking Tools & Tactics

Stage 4 (4)
Web Application Exploitation

Stage 5 (5)
Network Pentesting

Stage 9 (6)
Linux Privilege Escalation

Stage 10 (7)
Windows Privilege Escalation

Stage 11 (8)
Active Directory Exploitation

Stage 12 (9)
Technical Report Writing

Stage 13 (10)
Solve CTFs-Easy

Stage 14 (11)
Solve CTFs-Medium

Stage 15 (12)
Solve CTFs-High

Stage 16 (13)
Bonus Labs

iGNITE Technologies

CONTENTS

SECTION -A

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

Tools: Nmap & Scripts, Metasploit, Enum4linux, Ldapsearch, Smbclient, Snmpwalk

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: Whatweb, Nikto, Burp Suite, Dirb, Gobuster, ffuf, netcat, Revshell

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
- MS Office Macros Exploit
- Windows Reverse shell & one-linear payloads
- Post Enumeration
- Unquoted Path
- Always Install Elevated
- Scheduled Tasks
- Kernel exploit

Tools: Powershell scripts, Msfvenom, Revshell, Winpeas, Macropack, Impacket-Smbshare,

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

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, Packetstromsecurity, Github, Searchsploit, Nmap-NSE Script

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 Setuid Binaries
- Abusing Sudo
- Exploiting Kernel Vulnerabilities

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

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

CONTENTS

SECTION -B

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 and Enumeration

- Active Directory - Manual Enumeration
- Manual Enumeration - Expanding our Repertoire
- Active Directory - Automated Enumeration

Attacking Active Directory Authentication

- Enumeration
- Kerberos
- Pass the Hash-RDP
- Privilege Escalation

Lateral Movement in Active Directory

- Crackmapexec
- EvilWinrm
- Impacket-Library

Tools: Mimikatz, Evil-winrm, Crackmapexec, Impacket, Remmina, Rubeus, Powerview, Ad Recon, Bloodhound and etc.

iGNITE Technologies

CONTENTS

SECTION -C

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.
- Medium CTF Linux / Windows.
- Hard CTF Linux / Windows.

Platform**:** Hack The Box , Vulnhub, Try Hack Me

iGNITE Technologies

CONTACT US

PHONE

+91-9599387841 | +91-7805803296

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