iGNITE
Technologies

TRAINING PROGRAM

CAPTURE THE FLAG

Advanced Hacking Course

ENROLL NOW

www.ignitetechnologies.in

ABOUT COURSE

CTF is the latest edition of our training which provides the most advance modules that connect to the real infrastructures in the organizations and also assist students/professionals to prepare for global certification 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 practical knowledge of the different kind of attacks and issues in the real world.

WHO NEEDS CTF LEARNING?

If the candidate wants to achieve accreditation such CREST, OSCP, and etc then need to solve CTFs that which is based on real time scenario.

This course will focus on core concept that will the candidate the tricks and techniques to solve the challenge.

IGNITE TRAINING OBJECTIVE

- Aid the candidate to have required skill for achieve the global certification.
- Provide the accurate techniques to enhance the pentest for Network, Web, Active Directory and Privilege Escalation.
- Help to solve CTF through various platform such as Offsec-labs, HTB, THM, Vulnhub and etc.

PREREQUISITES

Course Duration: 50 Hours (Tentative)

ABOUT COURSE
IGNITE

Well-Known Entity for Offensive Security
{Training and Services}

About us

With an outreach to over a million students and over thousand colleges, Ignite Technologies stood out to be a trusted brand in cyber security training and services

WHO CAN ?

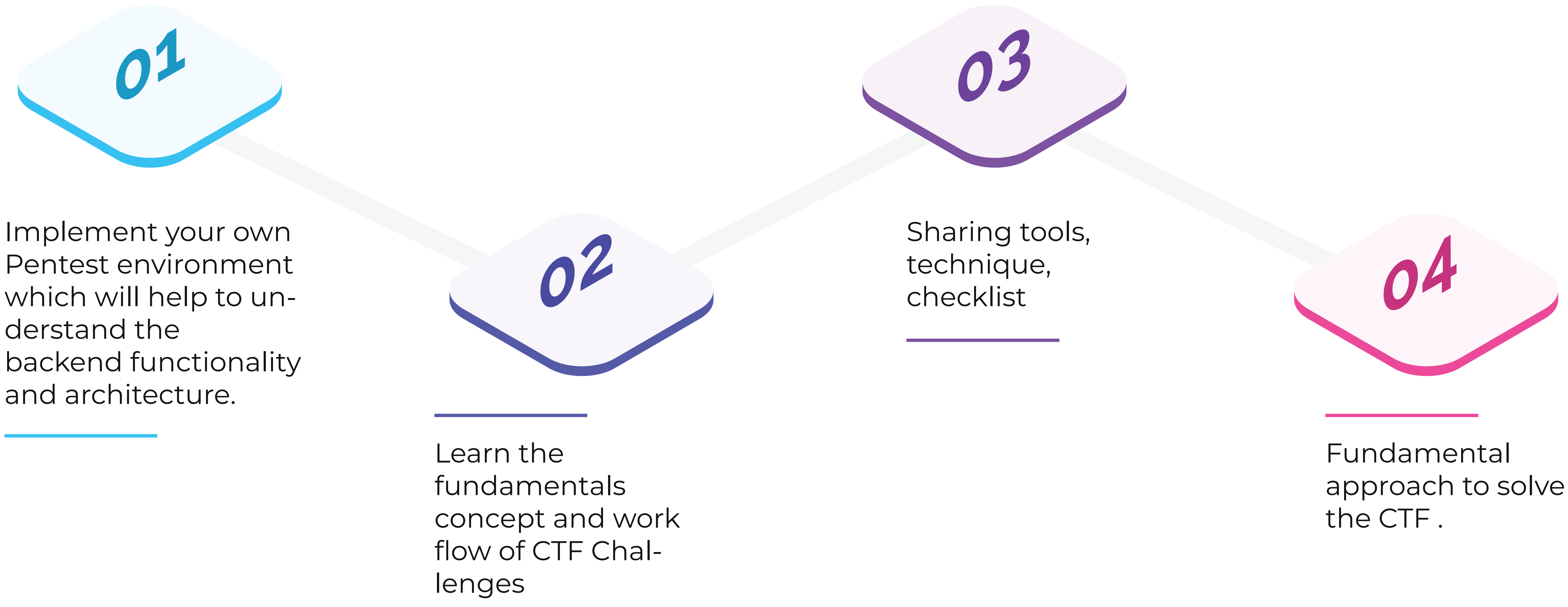
- College Students
- IS/IT specialist, analyst, or manager
- IS/IT auditor or consultant
- IT operations manager
- Network security officers and
- Practitioners
- Site administrators
- Technical support engineer
- Senior systems engineer
- Systems analyst or administrator
- IT security specialist, analyst, manager,
- Architect, or administrator
- IT security officer, auditor, or engineer
- Network specialist, analyst, manager,
- Architect, consultant, or administrator

WHY US ?

- Level up each candidate by providing the fundamental knowledge required to begin the Sessions.
- Hands-on Experience for all Practical Sessions.
- Get Course PDF and famous website links for content and Tools
- Customized and flexible training schedule.
- Get recorded videos after the session for each participant.
- Get post-training assistance and backup sessions.
- Common Platform for Group discussion along with the trainer.
- Work-in Professional Trainer to provide realtime exposure.
- Get a training certificate of participation.

iGNITE
Technologies

HOW WE FUNCTION



01 Implement your own Pentest environment which will help to understand the backend functionality and architecture.

02 Learn the fundamentals concept and work flow of CTF Challenges

03 Sharing tools, technique, checklist

04 Fundamental approach to solve the CTF .

COURSE INTRODUCTION

Objective: This module will define the OSCP Guidelines & holistic approach to follow 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

iGNITE Technologies

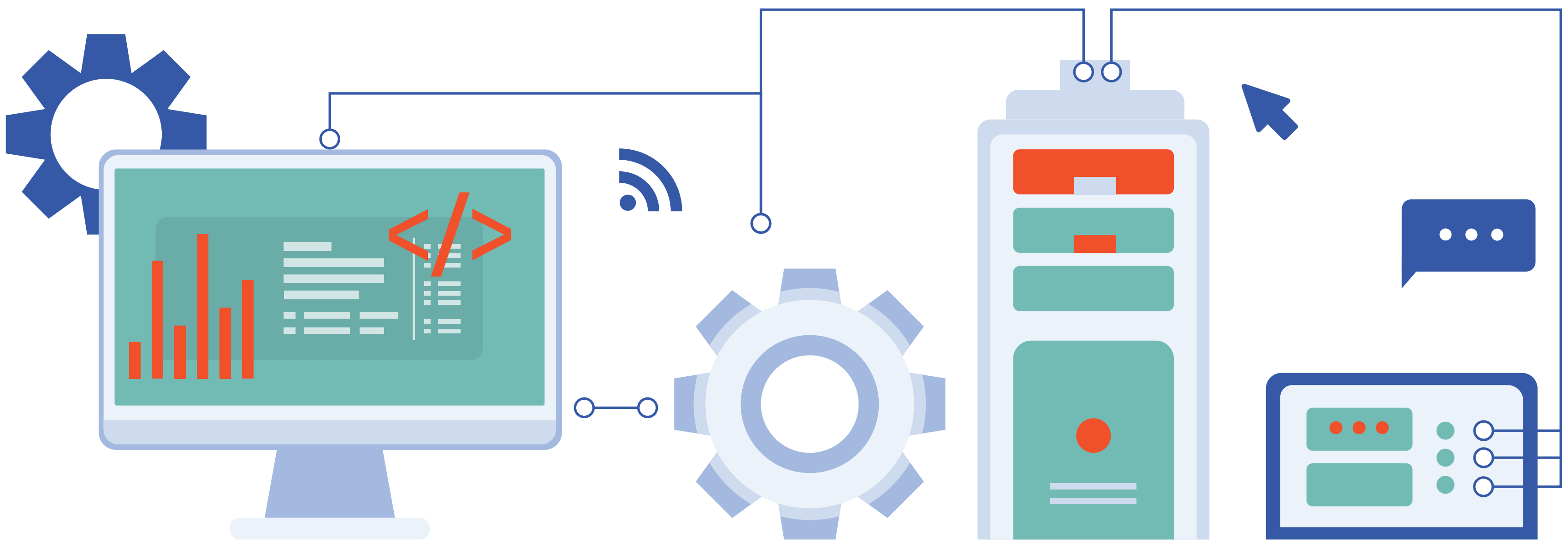
NETWORK ENUMERATION

Objective: This module will focus the enumeration of TCP & UDP service to identify the loopholes and sensitive information to proceed for 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 the web application exploitation by injecting payloads and establishing initial footholds.

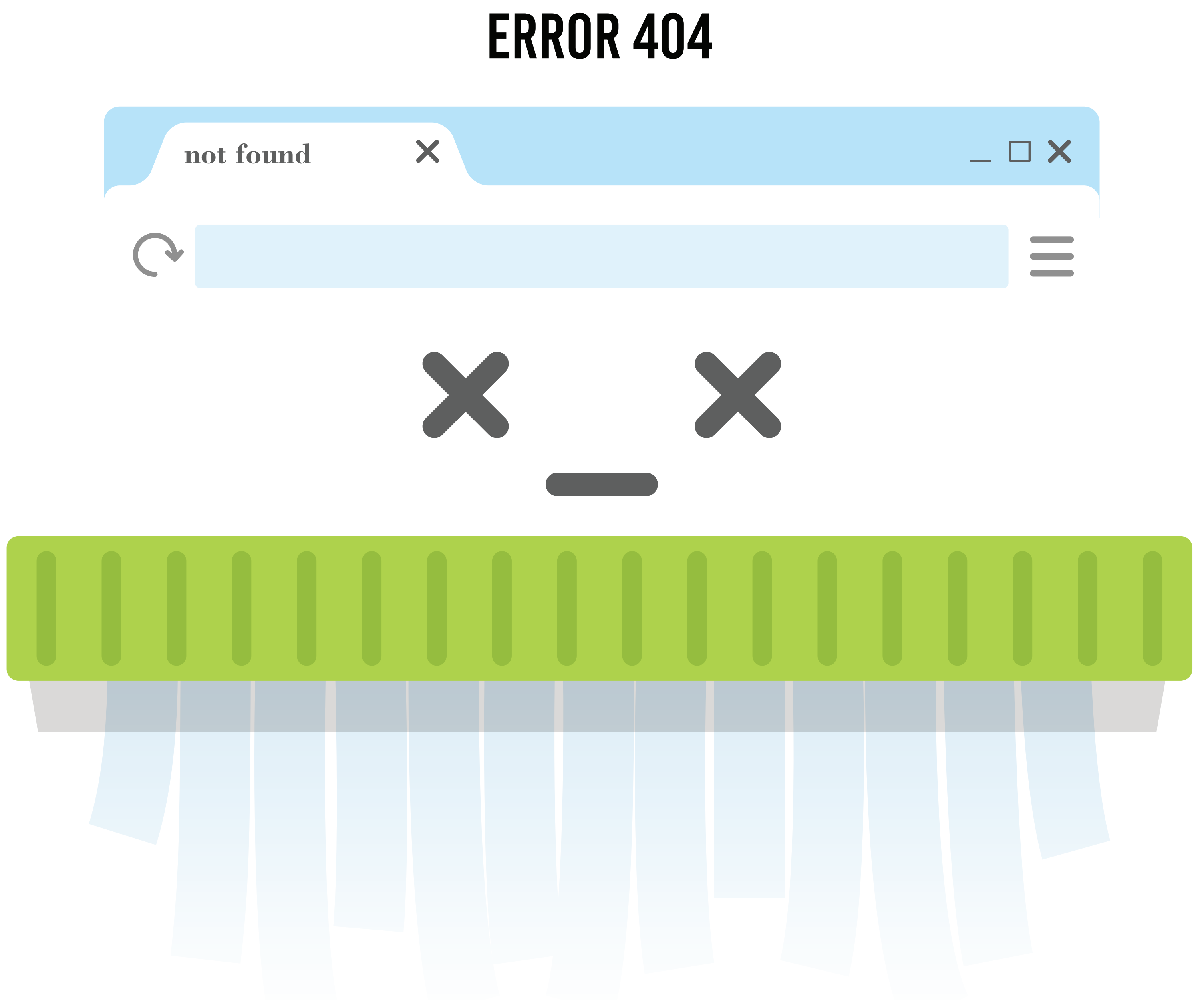
- Web Application Assessment Tools
- Web Application Enumeration
- Web Shells and One-liner payloads
- Directory Traversal
- File Inclusion Vulnerabilities
- File Upload Vulnerabilities
- Command Injection
- SQL Injection-Manual

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, Certutil.



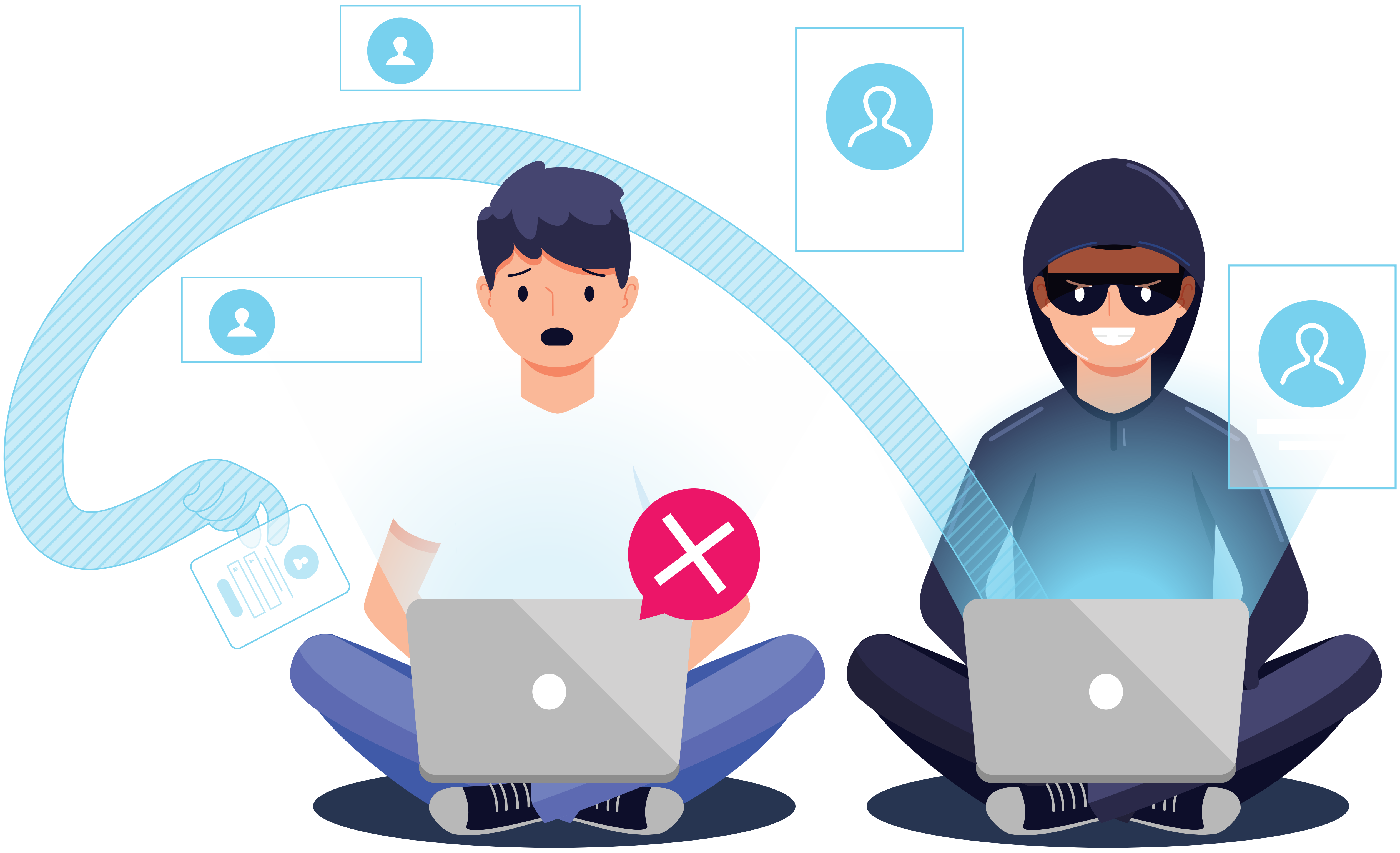
iGNITE Technologies

PASSWORD ATTACKS

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



iGNITE Technologies

HUNTING PUBLIC EXPLOITS

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

- 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, wget.

iGNITE Technologies

PORT FORWARDING & TUNNELING

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

ACTIVE DIRECTORY INTRODUCTION & ENUMERATION

Objective: : This module will focus on Active Directory Enumeration and exploitation and Privilege Escalation.

- Active Directory
- Enumeration
- Lateral Movement
- Kerberos Attack
- Pass the Hash-RDP
- Privilege Escalation

Tools: Crackmapexec, Evil-Winrm, Impacket-Library, Mimikatz, lagazne, Kerbrute.

CONTACT US

Phone No.

☎ +91 9599 387 41 | +91 1145 1031 30

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