About the Course

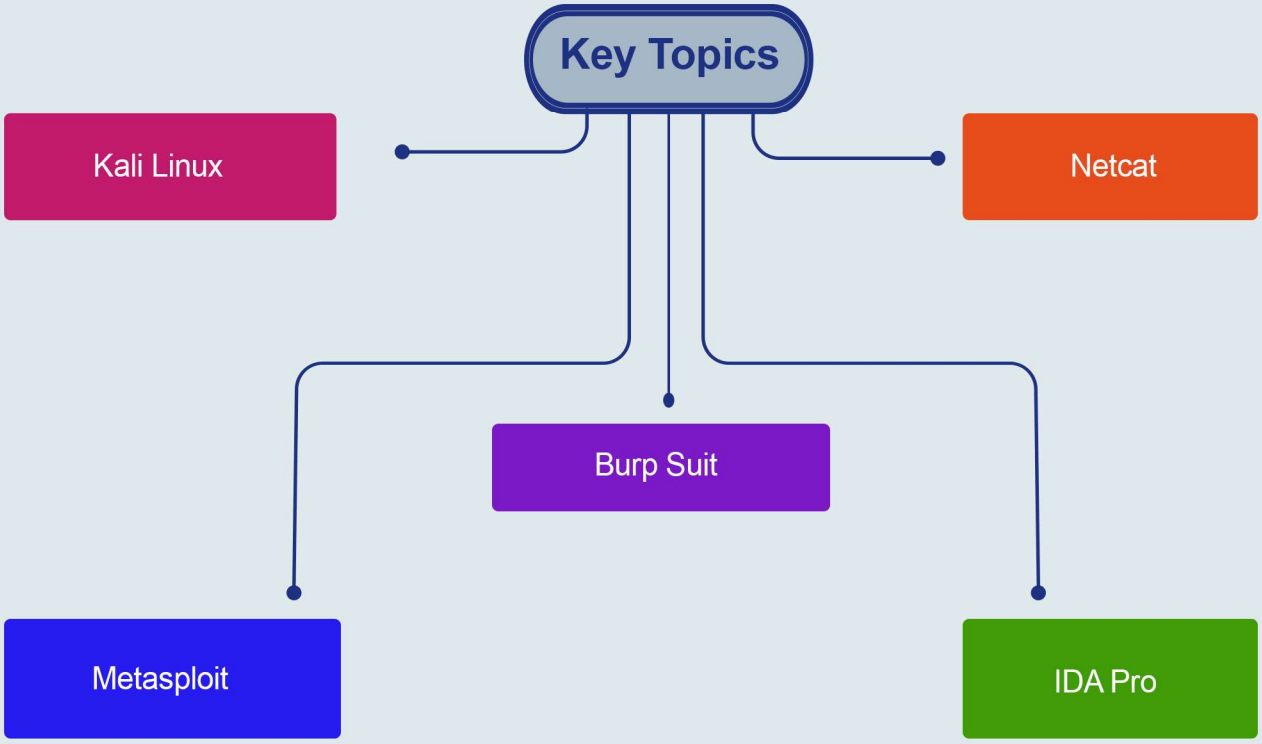
Ethical hacking helps organizations in better protecting their information and systems. It is also one of the best methods to augment the skills of security professionals of an organization. Making ethical hacking a part of the security efforts of an organization can prove to be exceptionally helpful. For ethical hacking and penetration testing you need tools.

Hacking Tools are computer programs and scripts that help you find and exploit weaknesses in computer systems, web applications, servers and networks. In this course some useful and common hacking tools are explained.

Learning Objectives

1. Working with Kali Linux
2. Working with Metasploit
3. Working with Burp Suit
4. Working with IDA Pro
5. Working with Netcat
6. Working with Wireshark

Key Topics



Pre Requisites

It is necessary to take the following course:

- Ethical Hacking & Penetration Testing Concepts

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Ethical Hacking & Penetration Testing Tools eBook

Who Should Attend

Anybody who is in charge of security assessment and penetration testing and also:

- CISOs
- PenTesters
- Threat & Vulnerability Analysts
- Security Specialists

Syllabus

Kali Linux

- Introducing Kali Linux
- Getting Familiar with Hardware Requirements and Recommendations
- Installing Kali Linux in VirtualBox
- Installing Kali Linux on Raspberry Pi
- Introducing Kali Linux Interface and Tools
- Updating Kali Linux
- Networking Fundamentals
- Creating a Pen-Testing Lab Environment

Metasploit for Enterprise Pen Testing

- Overview of Metasploit's Architecture and Components
- Msfconsole Interface
- Exploitation using Metasploit
- Metasploit Meterpreter
- Metasploit Sniffing on Exploited Systems
- Metasploit's Integration into a Professional Testing Methodology
- Meterpreter Scripts
- Using Metasploit as a Recon Tool
- Port and Vulnerability Scanning with Metasploit
- Metasploit Integration with Other Tools
- Client-Side Exploitation
- Making the Most of Windows Payloads
- Launching Unix Payload Attacks
- AUX Modules
- SNMP Modules
- SMB Modules
- WEBDAV Modules
- Database Services

Syllabus

- o Exploits
- o Payloads
- o Meterpreter
- o Meterpreter in Action
- o Additional Payloads
- o Binary Payloads
- o Multihandler
- o Porting Exploits
- o Post Exploitation

Burp Suite

- o Introduction to Burp GUI, tools, audit workflow, inline help
- o Exploitation using Burp Suite
- o Advanced Proxy module
- o Advanced Intruder module
- o Privileges escalation
- o Macros and sessions module
- o Transparent management of anti-CSRF tokens and short sessions
- o Extensions module

IDA Pro

- o IDA overview
- o Common executable file features
- o Debugger
- o IDC
- o Memory organization
- o IDS files
- o Working with IDA
- o Creating the database: various information sources
- o Various views of the database
- o Navigation, Modifying the listing

Syllabus

Netcat

- Connecting to a Server
- Fetching HTTP header
- Chatting
- Creating a Backdoor
- Verbose Mode
- Save Output to Disk
- Port Scanning
- TCP Delay Scan
- UDP Scan
- Reverse TCP Shell Exploitation
- Randomize Port
- File Transfer
- Reverse Netcat Shell Exploitation
- Banner grabbing

WireShark

- TCP Connect Scan
- Network Sweeping
- SYN Scan
- UDP Scan
- FIN Scan
- Null Scan
- OS Discovery
- NSE Scripts

Nmap

- Nmap Firewall Scan

Hands-on Training

- Lab 1 – Kali Platform
- Lab 2 – Metasploit Platform
- Lab 3 – Privilege Escalating with Burp Suit
- Lab 4 – Debugging with IDA Pro
- Lab 5 – Port Scanning with Netcat
- Lab 6 – Network Traffic Scan with Wireshark