Truephers Certified Penetration Tester 2.0
Ethical Hacking | Cyber Security | Information Security
60 hours Industrial Training Course

Kali Linux

- Introduction to Kali Linux
- Installing Kali Linux
- File Structure
- Installing and Configuring SSH, FTP, TFTP, Apache, Tomcat, Postgresql, Python, and other important services and daemons in Kali Linux
- Installing and Configuring Kali Pen testing Tools
- Bash Scripting
- Essential Tools – Netcat, Ncat, SOCAT, Wireshark, tcpdump

Active Information Gathering/ Enumeration

- Active Information Gathering
- OS Fingerprinting
- Port Scanning
- Banner Grabbing.
- Different Port Scanning tools and types.
- Port Scanning with Nmap
- Nmap Scripting Engine
- Netcat/ Zenmap
- Domain Name WHOIS lookup
- Reverse hostname lookup
- SMB Enumeration
- SMTP Enumeration
- SNMP Enumeration

Passive Information Gathering/ Enumeration

- Passive Information Gathering
- Google Hacking Database
- Google Dorks
- Online Email Finder
- Online Active ports scanners
- Reverse hostname lookup
- Netcraft
- DNS Zones
- Zone transfer
- Wayback Machine
- Uptime Monitoring
- Online Domain tools

Password Attacks

- Windows/ Linux password hashing
- Windows SAM Database
- Linux passwd/ shadow files
- Windows Password Cracking
- Linux Password Cracking
- Brute-forcing
- Rainbow tables
- Ophcrack
- Cain and Able
- bkhive, samdump2
- Password Hashing and Encryption
- Password profiling with cupp
- Password generator tools
- Hydra
- Hashcat
- John The Ripper
- HTTP – FTP – Telnet – RDP – RAR – ZIP – MD5 – SHA – LM/ NTLM password hashes and cracking with different tools and techniques

Vulnerability Assessment, Scanning

- Vulnerability Scanners
- Configuring and Installing Vulnerability Scanners

- Nessus
- Nexpose
- OpenVAS
- Web Vulnerability Scanners
- Acunetix Vulnerability Scanner
- Nikto
- Dirbuster

Web Application Penetration Testing

- Configuring Vulnerable Web Application for Learning and Testing
- Burp-Suite
- OWASP ZAP
- Nikto
- Dirbuster Dirb
- SQLmap
- Cross Site Scripting XSS
- SQL Injection
- RFI/ LFI
- Insecure Sensitive files (password, backup files)
- Broken Authentication
- OS Command Injections
- Insecure File Uploads
- Insecure Session Management
- And their Mitigations

Client Side Attacks

- Browser based client side attacks
- Java signed applet attacks
- SMB based client side
- PDF, Excels, Word documents based client side attacks
- Responder

Buffer Overflow Exploitation

- Fuzzing
- Debugger
- DEP ASLR

- Crashing
- Registers
- Controlling EIP
- Bad Characters
- Space for Shellcodes
- Finding Return address
- Generating a shell code with msfvenom
- Getting Shell on the box

Metasploit Framework

- Installing or updating
- User Interfaces
- Exploring Auxiliary module
- Exploring Exploit module
- Metasploit Payload module
- Searchsploit Exploit-db
- Staged vs. Non-staged payloads
- Meterpreter

Web Shells | MsfVenom | Malware frameworks

- Web Shells
- Uploading and Executing different types of webshells
- ASP, PHP, Java, Cold-fusion, Perl Web Shells
- Payload Generators
- MSFVenom

Port Redirection and Tunneling

- Port forwarding and redirections
- SSH tunneling
- Local port, Remote Port and Dynamic port forwarding
- HTTP Tunneling benefits
- Proxychains
- Metasploit port forwarding
- Plink
- Other proxy tools

Privilege Escalation

- Linux and Windows Privilege Escalation
- Vertical Privilege Escalation
- Horizontal Privilege Escalation
- Misconfigured File permissions
- Kernel Exploits
- Automated scripts to privilege escalation

System Hardening

- Securing Windows
- Windows Password profiling
- Updating and Patching Windows
- Files Permissions
- User Access Control
- Linux Server Hardening
- Securing sensitive and configuration files
- Updating and Patching system and services
- Configuring Secure CMS

IPS | IDS

- Intrusion Detection Systems
- Firewalls
- Intrusion Prevention System
- WIPS, WIDS
- Snort

Report Generation

- Sample Reports
- Report generation tools
- Maintaining Important links and texts in report generation