eJPT TRAINING AND NETWORK PENTESING COURSE

Introduction

- What is Hacking & Ethical Hacking
- What is Cyber Security
- Types of Hacker
- What are the Hacking Attacks
- Types of Malware
- CIA triad

Hacking Lab Setup

- Installing Virtual Box / VMware
- Installing Kali Linux
- Installing Windows OS
- Install Web server

Networking Fundamentals

- Intro to Networking
- All About IP Address
- Getting into MAC Address
- Working of TCP & UDP
- TCP / UDP & Three Way Handshake
- Common Port & Protocol
- knowing about Subnet
- TCP/IP vs OSI Model
- Network Topologies

Information Gathering

- Intro to Information Gathering
- Search Engine Information Gathering
- Advance Google Search in Information Gathering
- In-details Google Dorking
- Netcraft & Wappalyzer add-ons
- Mail Footprinting In-detail
- DNS Footprinting
- Whois Lookup
- Website Information Gathering
- Social Network Site Information gathering
- Looking for Databreaches

Scanning Netwoks

- What is Scanning
- Different types of Scanning
- Discovering open ports
- Looking at running services
- Grabbing version of services
- Detecting Host Name

- Bypassing Firewall
- Getting more inside of the network

Network Enumeration

- Knowing what is Enumeration
- Enumerating SMB
- Enumerating FTP
- Enumerating SSH
- Enumerating HTTP
- Enumerating SQL
- Enumerating SMTP

Vulnerability Scanning

- Introduction to Vulnerability Scanning
- Scanning Vulnerability with Nmap
- Scanning Vulnerability with Metasploit Framework
- Scanning with Nessus
- Performing Manually Scanning

Exploitation [Windows & Linux]

Windows

- Exploiting Windows Vulnerability
- Exploiting WinRM
- Exploiting SMB with PSExec
- Exploiting Windows SMB Vulnerability - Eternal Blue
- Exploiting Remote Desktop Protocol
- Exploiting Windows RDP Vulnerability - Bluekeep

Linux

- Exploiting Linux vulnerability
- Exploiting FTP
- Exploiting SSH
- Exploiting Telnet
- Exploiting Samba
- Exploiting Bind Shell

Post-Exploitation [Windows & Linux]

Windows

- WindowsPrivilegeEscalation
- WindowsKernelExploit
- UACbypasswithUACMe
- AccessTokenImpersonation
- WindowsCredentialDumping
- WindowsPasswordHashes
- PasswordinWindowsconfigurationfiles
- Dumpinghasheswithmimikatz
- Pass-The-Hashattack

Linux

- LinuxPrivilegesEscalation
- LinuxKernelExpl
- ExploitingMisconfiguredCronJobs
- ExploitingSUIDBinaries
- LinuxCredentialsDumping
- DumpingLinuxPasswordHashesoit

Metasploit Framework

Introduction To MSF

- BasicofMSF
- BasicofMSFpart2

Information Gathering using MSF

- NMAP
- PortScanning&Enumeration
- ImportingNMAPresultstoMSF

Enumeration

- PortScanningwithAuxiliarymodules
- FTPEnumeration
- SMBEnumeration
- WebServerEnumeration
- MySQLEnumeration
- SSHEnumeration
- SMTPEnumeration

Vulnerability Scanning

- MSF
- VulnerabilityScanningwithMSF
- Nessus
- VulnerabilityScanningwithNessus
- WebApp
- WebAppvulnerabilityscanningwithWMAP

Client Side Attacks

- Payload
- GeneratingBasicPayload
- GeneratingEncodedPayload
- GeneratingAdvancePayload
- GeneratingEncryptedPayload
- InjectingPayloadtoExecutables
- Automation
- AutomatingMetasploitwithResourceScripting

Exploitation

- Windows Exploitation
- Exploiting a Vulnerable HTTP File
- Server Exploiting Windows SMB
- Vulnerability Exploiting Windows RDP
- Vulnerability Exploiting Windows WinRM Protocol

Linux Exploitation

- ExploitingVulnerableFTPServer
- ExploitingSamba
- ExploitingVulnerableSSHServer
- ExploitingVulnerableSMTPServer

Post Exploitation

- PostExploitationFundamentals
- MeterpreterFundamentals
- UpgradingCommandShelltoMeterpreterShell
- WindowsPostExploitation
- WindowsPostExploitationModules
- PrivilegesEscalation-UACBypass
- PrivilegesEscalation-TokenImpersonation
- HashDumpingwithMimikatz Pass-The-
- HashwithPS-Exec
- EstablishingPersistenceonwindows
- EnablingRDP WindowsKeylogging
- ClearingWindowsEventLogs
-
- LinuxPostExploitation
- Linuxpostexploitationmodules
- ExploitingVulnerableSoftware
- DumpingHashesWithHashdump
- EstablishingPersistenceonLinux