Diploma In Cyber Security

SevenMentor PVT.LTD

www.sevenmentor.com

1.0 Introduction It Security

Information Security
Security and Its Needs
It Security Life Cycle

2.0 Desktop Security

Operating System Basics
Windows Installation
Windows Policies
What Is Vmware
Basic of Computer Networking
OSI and TCP/IP Model
Tcp Vs Udp
Tcp Frame Header
Udp Frame Header
Tcp Communication Flags
Networking Devices (Hub,Router,Switch,Etc.)
Windows and Linux Dual Boot

3.0 Networking Security

Mac address, IP-address Classes
What is Router
Static and Dynamic Routing
Sending the Messages
Routing the Traffic
Transmitting the Packets
Configuration of Router
Protocols on Router
Nat (Network Address Translation)
Pat (Port Address Translation)
What Is Dsl and Adsl Router
ACL
Troubleshooting
Securing the Routers

SevenMentor PVT.LTD

4.0 Linux Security

Introduction
Benefits of Linux
Kali Linux and Red Hat
Linux Directory and File System Structure
File Permission on Linux
Linux Commands (Find,grep,etc)
How to Set Up a Firewall Under Linux?
Iptables and Configuration
Windows Vs. Linux Design

5.0 Introduction to Hacking

Introduction to Ethical Hacking
Windows and Linux Intro
Kali Linux (Usages)
Deep/Dark Web

6.0 Reconnaissance

Information Intelligence.
Organize Your Information
Google/bing Hacking.
Whois Lookup.
Os Info Hunting.
Uptime Info Hunting.

7.0 Scanning

Web Server Info Hunting.
Traceroute Target Ip Address.
Tcp Port Scanning.
Syn Port Scanning.
Tcp Ack Firewall Scanning.
Finding Live Hosts
Udp Sweeping and Probing

8.0 Enumeration

Enumerating Username Groups and Passwords.
Hunting and Profiling People.
Gathering Email Accounts Sub Domains/host.
Database Enumeration.
Dns Enumeration.

9.0 Hacking Web Server

Attacking Apache Web Server.
Attacking IIS Web Server.

10.0 System Hacking

Linux Hacking and Securing
Windows Hacking and Securing

11.0 Wireless Hacking

Attacking Wep Protected 802.11 Networks.
Attacking Wpa/wpa2 Protected 802.11 Networks.
Rogue Access Point
Man in Middle Attack (Mitm)
Evil Twin Attack
Bluetooth Hacking

12.0 Dos and Ddos

Dos and DDos
Dos and Ddos Tools and Commands
DDos Attack on Bank-Website
Dos Attack on Server (Self)

13.0 Cryptography

What Is Cryptography
What Is Cipher?
Ciphers Types
Types of Cryptography
Hashing
Hashing File and Passwords
Pkc

14.0 Steganography

What Is Steganography
LSB Algorithm
Steganography in Images
Steganography in Audio
Whitespace Steganography

15.0 PassWords Attacks

Cryptography Attacks
Password Attacks
Types of Password Attacks
Password Cracking of Windows, Linux, Ssh.
Website Password Cracking

16.0 Social Engineering

Phishing
Advanced Social Engineering Attacks
Spear Phishing Attacks.
Sms Spoofing
Email Spoofing
Hacking Email Accounts
Countermeasures

17.0 Sniffing and Spoofing

What Is a Cam Table
Sniffing Network Passwords
Sniffing Http Passwords
Sniffing Ftp and Telnet Passwords.
Active Sniffing
Passive Sniffing
Sniffing Cookies
Man in the Middle Attack.

18.0 Systems Hacking and Exploit-development

Windows and Linux Hacking
Advanced Antivirus Detection Evasion and Bypassing.
Advanced Firewall Outbound/inbound Rules Evasion and Bypassing.
Advanced Windows User Access Control (Uac) Evasion and Bypassing.
Assembly Language
Exploit Writing
Windows Buffer Overflow Exploit
Linux Buffer Overflow Exploit

19.0 Firewall,IDS,IPS and Honeypot

What Is Ids
Ids Types
What Is Ips
Firewall
Firewall Types
Hardware and Software Firewall
Securing Network With (Smoothsec Express) Next-Gen Firewall.
Honeypot and Honeynet
Honeypot Low and High Interaction
Tracing Black-Hat Hacker
Evading Ids, Firewall,honeypot

20.0 VPN and Proxy-server

What Is Proxy
Proxy Types
Socks and Reverse-proxy
Vpn
Vpn Types
Open Vpn
Ipsec Vpn
Vpn Types
Vpn Security Issues

SevenMentor
PVT.LTD

21.0 Malwares

Writing Trojan for Windows.
What Is a Botnet and Attacks.
Mobile Malware
Mobile Anti-malware
Virus and Worms
Ransomware for Linux and Windows
Anti-malware
Malware Analysis
Sheep-dip System
Malwares Countermeasures

22.0 Cloud Computing

What Is Cloud.
What Is Types and Use.
Cloud for Hackers

23.0 Android Introduction

Introduction to the Course
Course Instructions
What Is Android.

24.0 Interacting With Android Devices

Rooting
Termux for Android
Vnc-remote Access
Busybox Tools.

25.0 Android Hacking and Exploitation.

Exploiting Android Devices Using Metasploit
Hacking Windows,android Using Android Phone.
Bypassing Android Locks
Data Hacking of Android

SevenMentor PVT.LTD

26.0 Android Pentesting

Removing-ads From Android
Cracking Application for Free Use.
Hiding Identity From Police.
Hacking Calls Logs and Sms Messages From Android Devices.

27.0 Introduction to WAPT

What Is Web Penetration Testing
What Is Web?
Understanding the Depth of Web

28.0 Owasp Top 10 Injection

What Is Owasp Top 10 Injection
What Is Proxy?
What Is Interception Proxies
Burp Suite Introduction

29.0 Information Gathering WAPT

Finding Whois and Dns
Dns Harvesting Extracting
A Open Source Information Gathering
The Http Protocols
Http Methods
Http Status Codes
Http Request and Response
What Is HTTPS
Http Methods and Verb Tampering
Http Method Testing With Nmap and Metasploit

30.0 Web App Basic Test

Web App Cryptography Attacks
Data Encoding
Encoding Schemes, URL Encoding, Unicode Encoding
Bypassing Weak Cipher
Testing Https
Nmap Scan
Gathering Server Info

31.0 Burp Suite in-depth

Burp Target
Burp Proxy
Burp Intruder
Burp Repeater
Burp Scripting
Spidering Web Application
Analysing Spidering
Burp Fuzzing

32.0 Broken Authentication and Session Management

Information Leakage
Directory Browsing
What Is Authentication
Http Response Splitting
Http Basic Authentication
Bypass Authentication Prompt
Attacking Http Basic Authentication With Nmap and Metasploit
Http Digest Authentication
Http Set-cookie With Httpcookie
Username Harvest

33.0 Injection Attacks

Html Injection Basics
Html Injection in Tag Parameters
Session Tracking
Session Fixation
Authentication Bypass

34.0 Command Injection

Command Injection
Web to Shell on the Server
Web Shell: Php Meterpreter
Web Shell: Netcat Reverse Connects
Web Shell: Using Python, Php Etc.

35.0 LFI and RFI

Remote Basics
RFI to Meterpreter
LFI Basics
LFI With Directory Prepends
Remote Code Execution With LFI and File Upload Vulnerability

36.0 Upload Attacks

File Upload Vulnerability Basics
Beating Content-type Check in File Upload
Bypassing Blacklists in File Upload
Bypassing Whitelists Using Double Extensions in File Uploads
Null Byte Injection in File Uploads
Exploiting File Uploads to Get Meterpreter

37.0 Unvalidated Redirects and Forwards

Unvalidated Redirects
Exploitation Open Redirects
Securing Open Redirects

38.0 Sql Injection

Sql Injection
Sqli Discovering
Error Based Sqli
Blind Based Sqli
Data Extraction
Sql Tools
Sqlmap
Sqlmap + Zap

39.0 Client-side Attacks

What Is Javascript
Dom-based XSS
Explotating Dom-XSS
Javascript Injection
Cross-site Scripting
Reflective XSS
Stored XSS
XSS Tools
XSS Fuzzing
XSS Exploitation
Beef Tool Stealing Cookies
Ajax
Ajax XSS

40.0 Csrf Attacks

Cross-site Request Forgery
Exploitation CSRF
Login Attack

41.0 Web App Tools

What Is Automation Testing
What Is Manual Testing
Wpscan
W3af
Wordpress Testing

42.0 Firewall Testing

Web Application Firewall
Wap Options
Mod_security
Waf Detection

43.0 Methodology and Reporting

Web Application Penetration Testing Methods
Reporting and Presenting

44.0 Other Attacks

SSI Attacks
Server-side Template Injection
IDOR Injection
LDAP Injection
Xml External Entity

45.0 Platform

Cross-site Request Forgery
Exploitation CSRF
Login Attack

46.0 Penetration testing with Bash script

Chapter 1: Getting to Know Bash

Navigating and searching the filesystem
Using I/O redirection
Using pipes
Getting to know grep

Chapter 2: Customizing your shell

Formatting the terminal Output
The Prompt String
Aliases
Customizing the command history
Customizing tab completion

Chapter 3: Network Reconnaissance

Interrogation the Whois servers
Interrogating the DNS servers
Enumerating target on the local network

Chapter 4: Exploitation and Reverse Engineering

Using the Metasploit command-line interface
Preparing payloads with Metsploit
Creating and deploying a payload
Diassembling binaries
Debugging binaries for dynamic analysis

Chapter 5: Network Exploitation and Monitoring

MAC and ARP abuse
Man in the middle attacks
Interrogating servers
Brute forcing authentication
Traffic filtering with TCPDump
Assessing SSL Implementation security
Automated web application security assessment

47.0 Penetration testing with Python

Chapter 1: Python with Penetration Testing and Networking

Introducing the scope of pentesting
Approaches to pentesting
Introducing Python scripting
Understanding the tests and tools you'll need
Learning the common testing platforms with Python
Network sockets
Server socket methods
Client Socket methods
General socket methods
Moving on the practical

Chapter 2: Scanning Pentesting

How to check live system in a network and concept of a live system
What are the services running on the target machine?

Chapter 3: Sniffing and Penetration Testing

Introducing a network sniffer
Implementing a network sniffer using python
Learning about packing crafing
Introducing ARP spoofing and implementing it using Python
Tesing and Security system using custom packet crafting and injection

Chapter 4: Wireless Pentesting

Wireless SSID finding and wireless traffic analysis by python
Wireless attacks

Chapter 5: Foot Printing of a Web Server and a Web Application

The concept of foot printing of a web server
Information gathering of a website from smartwhois by the parser BeautifulSoup
Banner Grabbing of a website
Hardening of a web server

Chapter 6: Client-Side and DDoS Attacks

Introducing client-side validation
Tampering with the client-side parameter with Python
Effects of parameter tempering on business
Introducing DoS and DDoS

Chaptr 7: Pentesting of SQLI and XSS

Introducing the SQL injection attack
Types of SQL injections
Understanding the SQL injection by a Python Script
Learning about Cross-site scripting

48.0 Computer Forensics in Today's World

Intro to Computer Forensics
Need for Computer Forensics
What Is Cyber Crime
Forensics Investigation Process
Cyber Crime Reports
Deft, Caine OS.

49.0 Computer Forensics Investigation Process

Forensic Workstation Building Sift
Chain of Custody
Data Imaging(FTK Imager)
Data Integrity(Sha256sum)
Data Carving(Physical Level)
Data Analysis(FTK Toolkit)
Expert Witness

50.0 Hacking Laws

PCI-DSS, DMCA, FISMA Act
It Act 2000

51.0 Understanding Hard Disks and File Systems

Disk Drive Overview
The Sleuth Kit(Tsk) and Autopsy

52.0 Data Acquisition and Duplication

Volatile Information From Linux and Windows
Acquiring Data on Windows
Acquiring Data on Linux
Ftk Imager and Ddclfd(Bit-stream Copy)
Netcat for Forensic

53.0 Defeating Anti-forensics Techniques

Cryptography, PKI, PKC, VPN
Steganography and Steganalysis
Password Cracking System and Application
Cracking Bios Password
Alternate Data Stream
Encrypted File System

54.0 Operating System Forensics

Network and Process Information
Cache , Cookie and History Analysis
Registry Analysis
Linux Configuration Analysis
Windows Event Viewer

55.0 Network Forensics

Network Forensic
Intrusion Detection System(IDS)
Firewall, IPS and Reverse-proxy.
Honeypot and Tracing.
Traffic Capturing and Analysis

56.0 Investigating Web Attacks

Web Application Architecture
Web Attacks
Apache Web Server Logs Investigation
Web Attack Detection
Tracing Ip Address

57.0 Database Forensics

Logon Event in Windows and Linux
Syslog Identification
Log Capturing and Analysis

58.0 Malware Forensic

Unstructured Memory Analysis
Bulk Extractor
Cridex Malware Identification
Network Activity to a Process

59.0 Investigating Email Crimes

Email System Architecture
Email Crimes
Email Header Analysis.
Tracing Emails

60.0 Forensics Report Writing

Forensics Report
Report Writing and Documentation.
Sample Report Writing
Writing Reports Using FTL
Writing Reports Using Autopsy

61.0 Case Studies

Mumbai Case
Pune Case