DIPLOMA IN CYBERSECURITY

Duration: 6 months

CHAPTER 1

Basics of Linux operating system

Installation and configuration of Kali Linux OS

Basic Linux commands

File and System Management

Networking Commands

Data Manipulation Commands

Privilege escalation

Summary

CHAPTER 2

Introduction to Cybersecurity

Motives of Information Technology

Goals of IT

Various types of Attacks

Summary

CHAPTER 3

Information Security Overview

Cybersecurity Concepts

Information Security Laws and Standards

Summary

CHAPTER 4

Footprinting

What is Footprinting, Reconnaissance

Whois Footprinting

Website Footprinting

Email Footprinting

Summary

CHAPTER 5

Scanning Concepts

Network Scanning concepts

Discovery scans, Port scans

Scanning tools

Nmap

Network Proxies

Summary

CHAPTER 6

Network Enumeration

What is Network Enumeration

SMB_NetBIOS enumeration

Website enumeration

What is vulnerability scanning

Scanning with OpenVAS

Summary

CHAPTER 7

System Security

System security concepts

Common OS exploits

Metasploit

Meterpreter

Keylogging and Spyware

CHAPTER 8

Viruses and Malware

CHAPTER 9

Sniffing Technology

CHAPTER 10

Social Engineering

CHAPTER 11

Denial Of Services

DoS/DdoS Concepts

DDoS Case Study

Botnets

Summary

CHAPTER 12

Session Hijacking Concepts

Hijack a Telnet connection

Evading IDS, Honeypots and Firewall

Use Social Engineering to Bypass a Windows Firewall

Summary

CHAPTER 13

Web Server Security Concepts

Web Server Atta

Web Server Attack Methodology

Web Application concepts

Attacking Web Apps

Web Application Security

SQL Injection Concepts

Summary

CHAPTER 14

Wireless Security

Wireless Encryption

Wireless Threats, Wireless Attacking Tools

Cracking WEP

Wireless Security Tools

Mobile device overview

Mobile platform attack vectors

Exploiting Android OS

Mobile Security Guidelines and Tools

Summary

CHAPTER 15

IOT (Internet of Things) & OT

IoT Vulnerabilities and Threats

IoT Attacks, IoT Security

OT (Operational Technology) Concepts

OT Attacks

Summary

CHAPTER 16

Cloud Computing

Basics of cloud computing

Container Technology

Cloud Security

Summary

CHAPTER 17

Cryptography

Encryption Algorithms

Cryptography Tools

Email encryption

Disk encryption

Cryptanalysis and Hashing

Cryptography Attack Countermeasure

Cryptanalysis Tools

Summary

CHAPTER 18

Network Penetration Testing

Introduction to Penetration Testing

Types of Penetration Testing

Pentesting Services

Penetration Testing Phases

Pre-Engagement Actions

Exploitation (Automated)

Password Cracking

Red Team Vs Blue Team Operations

Advanced Network Pentesting

Manual Exploitation of System Vulnerabilities

Post-Exploitation

Privilege Escalation (Linux and Windows)

CyberKill Chain, MITRE ATT&CK

Penetration Testing Standards

OWASP, SANS25, PTES and OSSTMM

Summary

FINAL EXAM