Airoman
ZID SE HI, JEET HAI

Diploma in Cyber Security 6 Months

NETWORKING BASICS

- Network Theory
- Network Communications
- Methods Network Media and
- Hardware Bounded Network
- Media Unbounded Network
- Media Noise Control
- Network Connectivity
- Devices Network
- Implementations Ethernet
- Networks Wireless Networks
- The OSI Model
- The TCP/IP Model
- TCP/IP Addressing and Data Delivery
- The TCP/IP Protocol Suite
- IP Addressing
- Default IP Addressing Schemes
- Create Custom IP Addressing Schemes
- Implement IPv6 Addresses
- Delivery Techniques
- TCP/IP Services
- Assign IP Addresses
- Domain Naming Services
- TCP/IP Commands
- Common TCP/IP Protocols
- TCP/IP Interoperability Services
- LAN Infrastructure
- Switching
- Enable Static Routing
- Implement Dynamic Routing
- Plan a SOHO Network

LINUX

- Getting started with Linux
- Access the command line
- Manage files from the command line
- Get help in Linux Create, view
- edit text files Manage local users
- & groups Control access to files
- Monitor & manage Linux processes

- Configure & secure SSH
- Analyze & store logs
- Manage networking
- Archive & transfer files
- Install & update software
- Access Linux file systems
- Analyse servers & get support
- Comprehensive review
- Improving command line productivity using shell
- Scripts Schedule future tasks
- Tune system performance
- Manage security
- Maintain basic storage
- Manage storage stack
- Access network-a ached
- storage Control the boot process
- Manage network security
- Install Linux Run
- Containers Comprehensive
- Review

BASIC PYTHON

Introduction to Python

- **Why Python**
- **Application areas of**
- **python implementations**
    - Python
    - Python
    - Iron
    - Python
    - Puppy

Python versions
Installing python
Python interpreter architecture

- Python byte code compiler
- Python virtual machine
  (pvm)

Writing and Execu ng First Python Program

- **Using interactive mode Using script**
- **Mode**
    - General text editor and command window
    - idle editor and idle shell
- **Understanding print () func on**
- **How to compile python program explicitly**

Python Language Fundamentals

- **Character set**
- **Keywords**
- **Comments**
- **Variables**

- **Literals**
- **Operators**
- **Reading input from console**
- **Parsing string to int, float**

Python Conditional Statements If

- **statement**
- **If else statement**
- **If elif statement**
- **If elif else statement**

Looping Statements

- **While loop**
- **for loop**
- **Nested loops**

String Handling

- **String func on s, methods**
- **String indexing, slicing and iteration**

Python Functions

- **Defining a func on**
- **calling a func on**
- **Types of func on s**
- **Func on n**

Object Oriented Programming

- **OOP Principles**
- **Defining a Class & Object Crea ng**
- **n Inheritance**

ETHICAL HACKING V-12

Introduction to Ethical Hacking

- **Information Security Overview**
- **Information Security Threats and Attack Vectors**
- **Top Information Security Attack Vectors**
- **Motives, Goals, and Objectives of Information Security Attacks**
- **Information Security Threats**
- **Information Warfare**
- **Hacking Concepts**
- **Hacking vs. Ethical Hacking**
- **Effects of Hacking on Business**
- **Who Is a Hacker?**
- **Hacker Classes**
- **Hacktivism**
- **Hacking Phases**
- **Types of Attacks**
- **Types of Attacks on a System**
- **Operating System Attacks**
- **Misconfiguration Attacks**
- **Application-Level Attacks**
- **Skills of an Ethical Hacker**
- **Defence in Depth**
- **Incident Management Process**
- **Information Security Policies**

- **Classification of Security Policies**
- **Structure and Contents of Security Policies**

Footprinting and Reconnaissance

- **Footprinting Concepts**
- **Foot printing Terminology**
- **What is Footprinting?**
- **Why Footprinting?**
- **Objectives of Footprinting**
- **Footprinting Threats**
- **Footprinting through Search Engines**
- **Finding Company's External and Internal URLs**
- **Mirroring Entire Website**
- **Website Mirroring Tools**
- **Extract Website Information from**
- **Google Hacking Tool: Google**
- **Hacking Database (GHDB)**
- **Google Hacking Tools**
- **WHOIS Footprinting**
- **WHOIS Lookup**
- **DNS Footprinting**
- **Extracting DNS Information**
- **Footprinting through Social Engineering**

Scanning Networks

- **Check for Live Systems**
- **Ping Sweep**
- **Check for Open Ports**
- **Scanning Tool: Nmap**
- **Hping2 / Hping3**
- **Scanning Techniques**
- **Scanning Tool: NetscanTools Pro**
- **Scanning Tools**
- **Port Scanning Countermeasures**
- **Proxy Servers**

Enumeration

- **What is Enumeration?**
- **Techniques for Enumeration**
- **Services and Ports to Enumerate**
- **Enumerating User Accounts**

System Hacking

- **Information at Hand Before System Hacking Stage**
- **System Hacking: Goals**
- **Cracking Passwords**
- **Password Cracking**
- **Password Complexity**
- **Password Cracking Techniques**
- **Types of Password Attacks**
- **Distributed Network Attack**
- **Default Passwords**
- **Manual Password Cracking (Guessing)**
- **Stealing Passwords Using Key loggers**
- **Spyware**
- **How to Defend Against Keyloggers**

- Anti-Spywares
- What Is Steganography?

Trojans and Backdoors

- Trojan Concepts
- What is a Trojan?
- Trojan Infection
- Types of Trojans
- Command Shell Trojans
- Command Shell Trojan: Netcat
- GUI Trojan: MoSucker
- GUI Trojan: Jumper and Biodox
- Document Trojans
- E-mail Trojans
- E-mail Trojans: RemoteByMail
- Trojan Detection
- How to Detect Trojans
- Scanning for Suspicious Ports
- Trojan Horse Construction Kit
- Anti-Trojan Software

Viruses and Worms

- Virus and Worms Concepts
- Introduction to Viruses
- Virus and Worm Statistics
- Types of Viruses
- File and Multipartite Viruses
- Stealth/Tunnelling Viruses
- Encryption Viruses
- Malware Analysis
- Online Malware Testing: Virus Total
- Online Malware Analysis Services
- Anti-virus Tools

Sniffers

- Sniffing Concepts
- Wiretapping
- Lawful Interception
- Packet Sniffing
- Sniffing Threats
- SPAN Port
- MAC Attacks
- MAC Flooding
- MAC Address/CAM Table
- How CAM Works
- DHCP Attacks
- How DHCP Works
- DHCP Request/Reply Messages
- IPv4 DHCP Packet Format
- ARP Poisoning
- What Is Address Resolution Protocol (ARP)?
- ARP Spoofing Techniques
- ARP Spoofing Attack
- Spoofing Attack
- Spoofing Attack Threats

- DNS Poisoning
- DNS Poisoning Techniques

Social Engineering

- Social Engineering Concepts
- What is Social Engineering?
- Behaviours Vulnerable to Attacks
- Social Engineering Techniques
- Types of Social Engineering
- Human-based Social Engineering
- Technical Support Example
- Authority Support Example
- Social Networking Sites
- Social Engineering Through
- Impersonation on Social
- Networking Sites
- How to Detect Phishing Emails
- Anti-Phishing Toolbar: Net craft
- Anti-Phishing Toolbar: Phish Tank
- Identity Theft Countermeasures

Denial of Service

- DoS/DDoS Concepts
- What is a Denial of Service Attack?
- What Are Distributed Denial of Service Attacks?
- Symptoms of a DoS Attack
- DoS Attack Techniques
- Bandwidth Attacks
- Service Request Floods
- SYN Attack
- SYN Flooding
- ICMP Flood Attack
- Peer-to-Peer Attacks
- Permanent Denial-of-Service Attack
- Application Level Flood Attacks
- Botnet
- Botnet Propagation Technique
- DDoS Attack
- DDoS Attack Tool:LOIC
- DoS Attack Tools

Session Hijacking

- Session Hijacking Concepts
- What is Session Hijacking?
- Dangers Posed by Hijacking
- Why is Session Hijacking Successful?
- Key Session Hijacking Techniques
- Brute Forcing Attack
- Network-level Session Hijacking
- The 3-Way Handshake
- Sequence Numbers
- Session Hijacking Tools
- Session Hijacking Tool: Zaproxy
- Session Hijacking Tool: Burp Suite
- Session Hijacking Tool: Hijack

- Session Hijacking Tools

Hacking Web Servers

- Web Server Concepts
- Web Server Market Shares
- Open Source Web Server Architecture
- Attack Methodology
- Web Server Attack Methodology
- Web Server Attack Methodology: Information Gathering
- Web Server Attack Methodology: Web Server Footprinting
- Counter-measures
- Countermeasures: Patches and Updates
- Countermeasures: Protocols
- Countermeasures: Accounts
- Countermeasures: Files and Directories
- How to Defend Against Web Server Attacks
- How to Defend against HTTP
- Response Splitting and Web Cache
- Poisoning
- Web Server Penetration Testing

Hacking Web Applications

- Web App Concepts
- Web Application Security Statistics
- Introduction to Web Applications
- SQL Injection Attacks
- Command Injection Attacks
- Web App Hacking Methodology
- Footprint Web Infrastructure
- Footprint Web Infrastructure:ServerDiscovery
- Hacking Web Servers
- Web Server Hacking Tool:WebInspect
- Web Services Probing Attacks
- Web Service Attacks: SOAP Injection
- Web Service Attacks: XML Injection
- Web Services Parsing Attacks
- Web Service Attack Tool: soapUI

SQL Injection

- SQLInjection Concepts
- SQL Injection
- Scenario
- SQL Injection Threats
- What is SQL Injection?
- SQL Injection Attacks
- SQL Injection Detection
- Types of SQL Injection
- Simple SQL Injection Attack
- Union SQL Injection Example
- SQL Injection Error Based
- Blind SQL Injection
- What is Blind SQL Injection?
- SQL Injection Methodology
- Advanced SQL Injection
- Information Gathering

- Extracting Information through ErrorMessages
- Interacting with the File System
- SQL Injection Tools
- SQL Injection Tools: BSQLHacker
- SQL Injection Tools: Marathon Tool
- SQL Injection Tools: SQL Power Injector
- SQL Injection Tools: Havij
- SQL Injection Tools

Hacking Wireless Networks

- Wireless Concepts
- Wireless Networks
- Wi-Fi Networks at Home and Public Places
- Types of Wireless Networks
- Wireless Encryption
- Wireless Threats
- Wireless Threats: Access Control Attacks
- Wireless Threats: Integrity Attacks
- Footprint the Wireless Network
- Attackers Scanning for Wi-Fi Networks
- Bluetooth Hacking
- Bluetooth Threats

Evading IDS, Firewalls, and Honeypots

- IDS, Firewall and Honeypot Concepts
- How does IDS Work?
- Ways to Detect an Intrusion
- Denial-of-Service Attack (DoS)
- ASCII Shellcode
- Other Types of Evasion
- Evading Firewalls
- IP Address Spoofing
- Source Routing
- Website Surfing Sites
- Detecting Honeypots
- Detecting Honeypots

Buffer Overflow

- Buffer Overflow Concepts
- Buffer Overflow
- Shell code
- No Operations (NOPs)
- Buffer Overflow Methodology
- Overflow using Format String
- Smashing the Stack
- Once the Stack is smashed...
- Buffer Overflow Security Tools
- BoF Security Tool: Buffer Shield
- BoF Security Tools

Cryptography

- Cryptography Concepts
- Cryptography
- Types of Cryptography
- Government Access to Keys (GAK)
- Encryption Algorithms

- **Ciphers**
- **Advanced Encryption Standard (AES)**
- **Public Key Infrastructure(PKI)**
- **Public Key Infrastructure (PKI)Certification Authorities**
- **Email Encryption**
- **Digital Signature**
- **SSL (Secure Sockets Layer)**
- **Transport Layer Security (TLS)**
- **Disk Encryption Tools**
- **Cryptanalysis Tool: CrypTool**
- **Cryptanalysis Tools**
- **Online MD5 Decryption Tool**

Penetration Testing

- **Pen Testing Concepts**
- **Security Assessments**
- **Security Audit**
- **Vulnerability Assessment**
- **Limitations of Vulnerability Assessment**
- **Introduction to Penetration Testing**
- **Penetration Testing**
- **Why Penetration Testing?**
- **Testing Locations**
- **Types of Pen Testing**
- **Types of Penetration Testing**
- **External Penetration Testing**
- **Internal Security Assessment**
- **Black-box Penetration Testing**
- **Grey-box Penetration Testing**
- **White-box Penetration Testing**