सत्यमेव जयते

CYBER SECURITY SERVICES
CYBER INTELLIGENCE AGENCY
CYBER SECURITY EDUCATION

सूक्ष्म , लघु एवं मध्यम उद्यम
MICRO, SMALL & MEDIUM ENTERPRISES

www.cianet.in

Cyber Intelligence Agency , Hero Honda Chowk , Opp. Trends Showroom ,
Narnaul , Mahendergarh , Haryana , India – 123001

08529145541 ☎08200748270 info@cianet.in cia.info.help@gmail.com

GSTIN : 06GORPM2877A1ZM UDHYAM-HR-12-0028344

Certified Cyber Warrior Program

CCWP is comprehensive course specially designed for beginners to take them to hardcore level , below is the complete list of modules……….

- Introduction to Cyber Security & Hacking
- Networking Concepts
- Cyber Crimes & Awareness (How to be Secure)
- Information Gathering
- Penetration Testing & Metasploit Framework
- Web Testing using Burp Suite & Bug Bounty
- Android Hacking
- Windows Testing
- Wireless Network Testing
- Miscellaneous Attacks & Tools
- Important Hacking Tools (Hardware)
- Digital & Cyber Forensics
- Cryptography Basics
- Deep and Dark Web
- Hacker's Case Studies, Methodologies & Mentality
- Aptitude & Logic Building
- Miscellaneous (M.) — Integrated across the course

1/31/2026

X

Mohit Yogi
CEO - Cyber Intelligence Agency
Signed by: d41e73b9-54cb-4cf0-b89a-4ff0155312d2

Syllabus

🔐 Module 1: Introduction to Cyber Security & Hacking

3 weeks (30 hrs)

1.1 Definition and Importance of Cyber Security
1.2 Overview of Ethical Hacking
1.3 Hacking Fundamentals & Types of Hackers
1.4 Types of Attacks on a System
1.5 Basic Terminologies in Cyber Security
1.6 Difference B/W Ethical Hacking & Cyber Security
1.7 Security Triad
1.8 Basics of Malware
1.9 Introduction to Security Controls
1.10 Introduction to Linux & Features of Linux
1.11 Setting Up Hacking Labs
1.12 Introduction to Kali Linux and Terminology
1.13 Important Kali Linux Commands
1.14 Introduction to Famous Kali Linux Tools
1.15 Social Media Accounts Hacking
1.16 Social Engineering Toolkit
1.17 Email Verification Bypass
1.18 SMS Verification Bypass
1.19 SMS, Call & Email Bombing
1.20 Email Address Spoofing
1.21 Man-in-the-Middle Attack
1.22 DNS Spoofing
1.23 Advanced Phishing Techniques
1.24 Red Team vs Blue Team vs Purple Team Concepts
1.25 Evolution of Hacking: From Script Kiddies to APTs
1.26 Understanding Hacker Psychology & Motivation
1.27 Underground Hacker Culture & Communities
1.28 Miscellaneous Topics
1.29 Doubt Session

🌐 Module 2: Networking Concepts

4 weeks (45 hrs)

2.1 Data Communication Basics
2.2 Basics of Computer Networks
2.3 Working of Network & Types of Network
2.4 LAN, MAN, WAN & PAN Differences
2.5 Client-Server Model vs Peer-to-Peer Networks
2.6 Unicast, Broadcast, Multicast & Anycast Communication
2.7 Types of Cables & Connectors
2.8 Network Devices (Hub, Switch, Router, Bridge, Modem, Access Point)
2.9 Network Topologies and Devices
2.10 IP Address (IPv4 vs IPv6)
2.11 Public, Private & Reserved IP Addresses
2.12 Subnetting & CIDR Notation Basics
2.13 IPv6 Basics
2.14 TCP/IP Protocol Suite
2.15 Concept of OSI Model-1
2.16 OSI Model-2
2.17 Network Protocols and Port Numbers
2.18 Ports & Services Mapping
2.19 DHCP (Dynamic Host Configuration Protocol)
2.20 ARP & RARP (Address Resolution Protocol)
2.21 ICMP Protocol (Ping, Traceroute)
2.22 Domain name & DNS
2.23 DNS Record Types
2.24 Network Address Translation (NAT)
2.25 NAT Types (Static, Dynamic, PAT)
2.26 Virtual Private Networks (VPNs)
2.27 VPN Basics (Site-to-Site vs Remote Access)
2.28 VPN & Proxy setup
2.29 Proxy Servers vs Gateways vs Load Balancers

2.30 Wireless Networking Basics
2.31 Understanding Firewalls and IDS/IPS
2.32 Working Of Firewalls, IDS & IPS
2.33 Network Security Best Practices
2.34 Network Monitoring Tools
2.35 Packet Analysis with Wireshark
2.36 Network Mapping (NMAP) Introduction
2.37 Network Scanning using NMAP 1
2.38 NMAP -2 & Zenmap
2.39 Advance Scanning (Bypassing Firewalls)
2.40 Miscellaneous Topics
2.41 Doubt Session

🛡️ Module 3: Cyber Crimes & Awareness (How to be Secure)

2 weeks (20 hrs)

3.1 Introduction to Cybercrime
3.2 History & Evolution of Cybercrime
3.3 Categories of Cybercrime
3.4 Types of Cyber Crimes
3.5 Mindset of Criminal
3.6 Motivation Behind Cyber Crimes
3.7 Cybercrime Ecosystem
3.8 Digital Footprints & Why They Matter
3.9 How to be Secure
3.10 How to Report Cyber Criminals
3.11 Difference Between Cyber Crime, Security, and Law
3.12 How to Avoid Phishing & Vishing
3.13 Basics of Strong Passwords & Password Managers
3.14 Two-Factor Authentication (2FA) Basics
3.15 Cyber Laws
3.16 Secure Browsing Practices
3.17 Secure Use of Social Media
3.18 Protecting Personal Information Online
3.19 Understanding and Preventing Identity Theft
3.20 Awareness and Training Programs
3.21 Cyber Bullying and Harassment Prevention
3.22 Common Scams & Frauds
3.23 Child Online Safety & Awareness
3.24 Miscellaneous Topics
3.25 Doubt Session

🔎 Module 4: Information Gathering

3 weeks (30 hrs)

4.1 Introduction to Footprinting & Reconnaissance
4.2 Importance of Information Gathering in Hacking
4.3 Legal & Ethical Considerations in Reconnaissance
4.4 Difference Between Passive & Active Reconnaissance
4.5 Types of Information Gathering
4.6 Passive Information Gathering Techniques
4.7 Active Information Gathering Techniques
4.8 Types of Information Gathering Using OSINT
4.9 OSINT Frameworks & Methodology
4.10 Doxing
4.11 Information Gathering using GHDB (Google Hacking Database)
4.12 Nslookup & Whois Lookup
4.13 Mobile Number Footprinting
4.14 Website Footprinting
4.15 SMS, Call & Email Bombing
4.16 Email Footprinting
4.17 Image Footprinting
4.18 Information Gathering Using NMAP
4.19 Various Information Gathering Tools
4.20 Information Gathering Using Maltego
4.21 Information Gathering Methodology
4.22 Using Tools like Whois, Nslookup, and Dig
4.23 Social Engineering and Open Source Intelligence
4.24 Network Scanning and Enumeration
4.25 Identifying and Mapping Targets
4.26 Shodan & Censys Basics
4.27 Metadata Extraction from Files
4.28 Introduction to Footprinting Automation
4.29 Miscellaneous Topics
4.30 Doubt Session

💻 Module 5: Penetration Testing & Metasploit Framework

4 weeks (45 hrs)

5.1 Introduction to Penetration Testing
5.2 Importance of Penetration Testing in Cybersecurity
5.3 Legal & Ethical Aspects of Pentesting
5.4 Types of Penetration Testing
5.5 Pentesting Methodologies
5.6 Vulnerability Assessment
5.7 VAPT
5.8 VAPT Methodology
5.9 Phases of Penetration Testing
5.10 Scoping & Defining Targets in Pentesting
5.11 Setting Up a Penetration Testing Lab (Local + Cloud)
5.12 Introduction to Metasploit Framework
5.13 Exploiting Vulnerabilities with Metasploit
5.14 Post-Exploitation Techniques
5.15 Writing Custom Exploits
5.16 Reporting and Documenting Penetration Tests
5.17 Windows Hacking using Payloads & Exploits
5.18 Enumeration
5.19 SMTP Enumeration
5.20 FTP Enumeration
5.21 Remote Desktop Protocols (RDP) & Telnet Service
5.22 Working on Different Auxiliaries & Exploits
5.23 Advanced Exploiting Techniques
5.24 Hacking on WAN (Port Forwarding)
5.25 Maintaining Access & Covering Tracks
5.26 Penetration Testing Projects
5.27 Doubt Session

🌍 Module 6: Web Testing using Burp Suite & Bug Bounty

5 weeks (10 hrs/week = 50 hrs)

6.1 Introduction to Web Application Security
6.2 How the Web Works
6.3 URLs, Query Parameters & HTTP Methods
6.4 Cookies, Sessions, and Authentication Mechanisms
6.5 Common Web Technologies
6.6 Same-Origin Policy (SOP) & CORS Basics
6.7 Introduction to Website Hacking
6.8 WordPress Websites Hacking
6.9 Setting Up Burp Suite
6.10 Introduction to Burp Suite (Community Version)
6.11 Burp Suite - 1 (Proxy, Repeater, Intruder Basics)
6.12 Burp Suite - 2 (Decoder, Comparer, Sequencer)
6.13 OTP Bypass using Burp Suite
6.14 Payment Gateways Bypass using Burp Suite
6.15 Common Web Vulnerabilities (OWASP Top 10)
6.16 Performing Web Application Scans
6.17 Exploiting Web Vulnerabilities
6.18 Burp Suite - 3 (Burp Suite Pro Advanced Features)
6.19 Important Extensions in Burp Suite
6.20 Introduction to Bug Bounty Programs
6.21 Bug Bounty using Burp Suite
6.22 Reporting Vulnerabilities
6.23 Legal & Ethical Aspects of Bug Hunting
6.24 Website Hacking Project - 1
6.25 Website Hacking Project - 2
6.26 Miscellaneous Topics
6.27 Doubt Session

📱 Module 7: Android Hacking

3 weeks (35 hrs)

7.1 Overview of Android OS and Security Architecture
7.2 Android File System & Directory Structure
7.3 Android App Structure
7.4 Android Permissions & Security Model
7.5 Rooting & Jailbreaking Basics
7.6 OWASP Mobile Top 10 Overview
7.7 Setting Up an Android Hacking Environment
7.8 Introduction to Android Payloads & Trojans
7.9 Android Device Hacking using Metasploit
7.10 Android Application Penetration Testing
7.11 Exploiting Android Vulnerabilities
7.12 Reverse Engineering Android Apps (APKTool, JADX)
7.13 Malware Analysis on Android
7.14 Introduction to RAT (Remote Access Trojans)
7.15 Payload Crypting & Making Fully Undetectable
7.16 Payload Binding
7.17 Binding of Payload Manually
7.18 Control Android Device over the Internet Remotely
7.19 Take Control of Device Cameras Wirelessly
7.20 Introduction to Android Debug Bridge (ADB)
7.21 Android Device Testing using ADB
7.22 Screen Lock Bypass or Password Cracking
7.23 Introduction to Termux
7.24 Testing using Termux
7.25 MITM using Android Device
7.26 Location Tracing
7.27 Secure App Development Basics
7.28 Miscellaneous Topics
7.29 Doubt Session

💻 Module 8: Windows Testing

3 weeks (35 hrs)

8.1 Introduction to Windows OS Architecture
8.2 Windows File System & Registry Basics
8.3 Windows User Accounts, Groups & Privileges
8.4 Windows Authentication Mechanisms
8.5 Windows Security Features
8.6 Setting Up a Windows Hacking Lab
8.7 Windows Exploitation Basics
8.8 Payload Creation for Windows Systems
8.9 Gaining Access via Exploits
8.10 Post-Exploitation in Windows
8.11 Windows RAT (Remote Access Trojans)
8.12 Maintaining Access in Windows Systems
8.13 Windows Password Cracking
8.14 Windows Enumeration (Users, Shares, Services)
8.15 SMB Exploitation & EternalBlue Attack
8.16 Mimikatz Basics (Credential Dumping)
8.17 Keylogging in Windows
8.18 Windows Remote Desktop Exploitation
8.19 Powershell for Windows Hacking
8.20 Fileless Malware in Windows
8.21 Windows Event Logs & Clearing Tracks
8.22 Windows Persistence Techniques
8.23 Basics of Active Directory & Domain Controller
8.24 Introduction to Lateral Movement in Windows Networks
8.25 Real-World Windows Exploits & Case Studies
8.26 Windows Hardening Basics
8.27 Miscellaneous Topics
8.28 Doubt Session

CIA

📶 Module 9: Wireless Network Testing

2 weeks (25 hrs)

9.1 Basics of Wireless Networks
9.2 Wi-Fi Standards & Protocols
9.3 Introduction & Working of Wi-Fi
9.4 Wireless Encryption Fundamentals
9.5 Wireless Network Security Protocols
9.6 Wi-Fi Authentication & Key Management
9.7 Wireless Hardware & Radios
9.8 Setting Up a Wireless Testing Lab
9.9 Wi-Fi Hacking Using Raspberry Pi
9.10 Wireless Network Scanning and Enumeration
9.11 Attacking WEP/WPA/WPA2 Networks
9.12 Rogue Access Points and Evil Twin Attacks
9.13 Hacking Using Fake Wi-Fi Point
9.14 Wireless Sniffing and Traffic Analysis
9.15 Jamming & Denial of Service
9.16 Wireless Attack Tools & Scripts
9.17 Bluetooth & BLE Security Basics
9.18 Wireless Hardening & Mitigations
9.19 Wireless Forensics & Incident Response
9.20 Miscellaneous Topics & Doubt Session

⚔️ Module 10: Miscellaneous Attacks & Tools

2 weeks (25 hrs)

10.1 Introduction to Miscellaneous Attacks
10.2 DNS and DNSSEC Attacks
10.3 DoS / DDoS Attacks
10.4 Email Attacks (Spoofing, Phishing, Spamming)
10.5 Physical Security Attacks (USB Drops, Lock Picking)
10.6 IoT Security and Attacks
10.7 Cloud Security and Attacks
10.8 Social Engineering Attacks
10.9 Advanced Persistent Threats (APT)
10.10 Password Sniffing
10.11 Brute Force Attack
10.12 Dictionary Attack
10.13 SQL Injection Attack
10.14 Windows Password Cracking
10.15 Browser Exploitation Framework (BeEF)
10.16 Nessus Tool Installation & Working
10.17 Shell Scripting Basics
10.18 Session Hijacking
10.19 Reverse Engineering
10.20 Advanced MITM Attack
10.21 Flooding Attack
10.22 Wireshark - 1
10.23 Wireshark - 2
10.24 Introduction to Keyloggers
10.25 Introduction to Malware & Virus
10.26 Working with Ransomwares
10.27 Use of Proxychains
10.28 Call Spoofing
10.29 SIM Cloning
10.30 Introduction to Flag Capturing (CTF)
10.31 Various CTF Techniques
10.32 Introduction to Exploit Development Basics
10.33 Basics of Malware Types

10.34 Understanding Botnets
10.35 Basics of Rootkits and How They Work
10.36 File Upload Vulnerabilities & Exploitation
10.37 Basics of Exploit Kits
10.38 Introduction to Security Testing Tools
10.39 Basics of Threat Intelligence
10.40 Miscellaneous
10.41 Doubt Session

🛠️ Module 11: Important Hacking Tools (Hardware)

2 weeks (10 hrs/week = 20 hrs)

11.1 Introduction to Hardware Hacking
11.2 Safety, Legal & Ethical Concerns in Hardware Hack
11.3 Basics of Electronics for Hackers
11.4 Understanding Microcontrollers
11.5 Basics of SDR (Software Defined Radio)
11.6 Overview of Hardware Hacking Tools
11.7 Introduction To USB Rubber Ducky
11.8 Hacking Using USB Rubber Ducky
11.9 Cool Tips & Tricks Using Rubber Ducky
11.10 Introduction to Raspberry Pi
11.11 Use of Raspberry Pi for Hacking
11.12 WiFi hacking using Raspberry Pi Pico
11.13 DoS/DDOS Attack using Hardware Tools
11.14 SDR for Hacking (Advanced Use)
11.15 Hardware Keyloggers and Their Use
11.16 SIM Card Cloner
11.17 Introduction to Network Jammers
11.18 Working Model of Network Jammers
11.19 Basics of ATM/POS Skimmers
11.20 Introduction to Car Hacking (OBD-II, CAN Bus)
11.21 Basics of Wireless Signal Jamming
11.22 Building DIY Low-Cost Hacking Gadgets
11.23 Miscellaneous
11.24 Doubt Session

🕵️‍♀️ Module 12: Digital & Cyber Forensics

4 weeks (40 hrs)

12.1 Introduction to Digital Forensics

12.2 History & Evolution of Digital Forensics

12.3 Importance & Scope of Digital Forensics in Cybersec.

12.4 Types of Digital Evidence (Volatile vs Non-Volatile)

12.5 Chain of Custody & Legal Admissibility of Evidence

12.6 Basics of Incident Response & Relation to Forensics

12.7 Computer Forensics Fundamentals

12.8 Computer Forensics Investigation Process

12.9 Forensic Investigation Methodology

12.10 Collecting and Preserving Digital Evidence

12.11 Analyzing Digital Evidence

12.12 Understanding Hard Disk & File System

12.13 Data Acquisition & Duplication

12.14 Defeating Anti-Forensic Techniques

12.15 Using Forensic Tools (FTK, EnCase)

12.16 Windows Forensics

12.17 Linux & Mac Forensics

12.18 Network Forensics

12.19 Mobile Device Forensics

12.20 Investigating Web Attacks

12.21 Dark Web Forensics

12.22 Investigating Email Crimes

12.23 Malware Forensics

12.24 Autopsy Tool Installation

12.25 Introduction To Autopsy

12.26 Reporting Forensic Findings

12.27 Deleted Data Recovery using Autopsy

12.28 Recovering Data from Virtual Disk

12.29 Miscellaneous Topics

12.30 Doubt Session

🔐 Module 13: Cryptography Basics

2 weeks (20 hrs)

13.1 Introduction to Cryptography
13.2 History & Evolution of Cryptography
13.3 Importance of Cryptography in Cybersecurity
13.4 Difference Between Encoding, Hashing & Cryptography
13.5 Types of Cryptography (Symmetric, Asymmetric, Hybrid)
13.6 Symmetric vs. Asymmetric Encryption
13.7 Common Cryptographic Algorithms (AES, DES, RSA, ECC, Blowfish)
13.8 Stream vs Block Ciphers Basics
13.9 Implementing Encryption in Systems
13.10 Cryptographic Attacks (Known-Plaintext, Chosen-Plaintext, Birthday Attack)
13.11 Introduction to Hashing Algorithms (MD5, SHA family, BLAKE2)
13.12 Cryptography Tools (GPG, OpenSSL, Hashcat)
13.13 Encoding Tools (Base64, URL encoding, Hex)
13.14 Hash Functions and Digital Signatures
13.15 Public Key Infrastructure (PKI)
13.16 Certificates, SSL/TLS Basics & HTTPS
13.17 Key Management Fundamentals
13.18 Doubt Session

Module 14: Deep and Dark Web

1 week (15 hrs)

14.1 Understanding the Dark Web
14.2 Difference B/W Surface Web, Deep Web & Dark Web
14.3 Understanding Onion Services & Hidden Networks
14.4 Dark Web Safety & Best Practices
14.5 Introduction to Tor Browser
14.6 Tor Network and Anonymity
14.7 Accessing Dark Web Safely
14.8 Threat Analysis on Dark Web
14.9 Dark Web Marketplaces
14.10 Dark Web Forums & Communities
14.11 Legal and Ethical Considerations
14.12 Cryptocurrency Basics for Dark Web Transactions (Bitcoin, Monero intro)
14.13 Introduction to Carding
14.14 How Carding is Done?
14.15 Basics of Digital Footprinting & OPSEC on Dark Web
14.16 Miscellaneous
14.17 Doubt Session

🧠 Module 15: Hacker's Case Studies, Methodologies & Mentality

1 week (15 hrs)

15.1 Introduction to Hacker Mindset
15.2 Types of Hackers
15.3 Hacker Ethics & Rules of Engagement
15.4 Hacker Tools & Learning Path Overview
15.5 Famous Hacking Cases and Their Impact
15.6 Methodologies Used by Hackers
15.7 Hacker Recon & Footprinting Mindset
15.8 Psychological Aspects of Hackers
15.9 Studying Hacker Profiles
15.10 Lessons Learned from Real-World Attacks
15.11 How to Build Own Methodology
15.12 Importance of Anonymity in Hacking
15.13 How to Increase Your Hacking Knowledge
15.14 Continuous Learning & Staying Updated
15.15 Understanding Red Team vs Blue Team vs Purple Team Mentality

🧩 Module 16: Aptitude & Logic Building

1 week (15 hrs)

16.1 Introduction to Aptitude & Logical Thinking
16.2 Basics of Problem-Solving (Step-by-Step Approach)
16.3 Types of Logical Reasoning
16.4 Pattern Recognition & Sequence Solving
16.5 Critical Thinking in Cyber Security
16.6 Cyber Security Challenges and Competitions
16.7 Verbal Reasoning & Comprehension
16.8 Quantitative Aptitude Basics
16.9 Capture the Flag (CTF) Competitions
16.10 Developing Problem-Solving Skills
16.11 Project - 1 (Beginner Level CTF/Challenge)
16.12 Project - 2 (Intermediate CTF/Logic Challenge)
16.13 Miscellaneous Topics

🔧 Miscellaneous (M.) – Integrated across the course

(≈10 hrs total)

M.1 Introduction to Miscellaneous Hacking Concepts
M.2 Understanding System Vulnerabilities & Weak Points
M.3 Basics of CCTV Systems & How They Work
M.4 Introduction to PDF Exploits & Malicious Documents
M.5 Basics of Remote Access Trojans (RATs) & How They Operate
M.6 Introduction to Website Admin Panels & Login Mechanisms
M.7 Basics of SQL Mapping & Injection Concepts
M.8 Introduction to Ransomware & Decrypting Files (Safe Lab Practice)
M.9 Understanding Port Forwarding & Free Services
M.10 Introduction to Viruses & How They Spread
M.11 Scripting Basics for Automation & Attacks (Python, Bash)
M.12 Server Basics & Common Exploitation Techniques
M.13 Understanding System Exploitation Fundamentals
M.14 Active Directory Basics (Users, Groups, Permissions)
M.15 Pivoting Attack Fundamentals