

# Cyber Security

## 1 Year Diploma

### v2.0 with A.I.

The 1-Year Diploma in Cyber Security v2.0 provides foundational knowledge and hands-on skills in protecting networks, systems, and data from cyber threats, with an updated curriculum focused on the latest security trends and technologies.

#### Cyber Security Advanced Course

- **Duration:** 9 Months
- **Eligibility:** Only for candidates who qualify via **Entrance Test**
- **Structure:**
  - 3 hours of theory
  - 2 hours of practical
  - Includes: Training Materials, Pre-recorded Videos, Live Work Exposure, and Internship

## Networking Fundamentals

- Introduction to Cybersecurity
- Networking Models & Types
- OSI and TCP/IP Model Overview
- Understanding IP Addressing & Subnetting
- Packet Structure and Protocols (IP, TCP, UDP, ICMP)
- Network Devices: Routers, Switches, and Firewalls
- Network Topologies and Architectures
- NAT, DNS, and DHCP Fundamentals
- Port Forwarding and IP Routing Explained
- Network Security Fundamentals (Firewalls, IDS/IPS, Proxies, VPNs)
- Network Address Translation (NAT) and Security Implications
- Introduction to Wireshark and Packet Capture Analysis
- Introduction to Network Scanning (Nmap, Zenmap)
- Setting Up a Simple Network Attack Simulation Lab
- Detecting Common Network Attacks (DDoS, Spoofing, MITM)
- Preventing Network Attacks (DDoS Mitigation, Firewalls, IDS/IPS)
- Real-World Network Security Best Practices (Securing Routers, Firewalls)

Network Fundamentals refer to the core principles, technologies, and protocols that enable devices to communicate and share resources within a connected system. It encompasses the design, implementation, and management of networks, focusing on how data is transmitted, routed, and secured across wired or wireless connections.

## 2. Linux for Cybersecurity

- Setting Up Virtual Labs (VirtualBox, VMware, ISO Installation)
- Introduction to Linux (Shell, CLI vs GUI, Distributions)
- Basic Linux Commands (pwd, cd, ls, cp, mv, rm)
- File and Directory Management (mkdir, touch, nano, cat, less)
- User & Group Management (adduser, usermod, groups)
- File Permissions & Ownership (chmod, chown, umask)
- Linux File System Hierarchy & Navigation
- Process Management (ps, top, kill, nice, jobs)
- Package Management (apt, yum, dpkg, snap)
- Networking Basics (IP, DNS, Gateway, netplan)
- Network Commands (ping, netstat, traceroute, ss, ifconfig/ip)
- Essential Security Tools (nmap, netcat, tcpdump, whois)
- Bash Scripting Fundamentals (Variables, Loops, Conditions)
- Automation with Bash (Practical Scripts & Crontab Jobs)
- System Logs & Monitoring (journalctl, syslog, logrotate)
- Hardening Linux Systems (UFW, Fail2ban, SELinux, AppArmor)

Linux is an open-source operating system widely used in cybersecurity due to its flexibility, stability, and robust security features. It serves as the foundation for many security tools, penetration testing frameworks, and secure server environments.



### 3. Ethical Hacking

- Introduction to Packet Sniffing (Wireshark, tcpdump)
- Analyzing Live Network Traffic
- ARP Spoofing and MITM Attacks
- DNS Spoofing and Poisoning Techniques
- Information Gathering (Active & Passive)
- Understanding Port Scanning (SYN, ACK, FIN Scans)
- Using Nmap for Advanced Network Reconnaissance
- Packet Crafting and Injection (Scapy, Hping3..)
- Network Tunneling and Evasion Techniques
- Wireless Security Protocols (WEP, WPA, WPA2)
- Wireless Network Cracking
- Evil Twin Attacks and Rogue Access Point Setup
- Network Defense Mechanisms (Segmentation, VLANs, NAC)
- Setting Up IDS/IPS Systems (Snort, Suricata)
- Detecting and Responding to Network Attacks
- Final Lab: Full Network Penetration Testing Simulation



Ethical Hacking refers to the authorized and legal practice of bypassing system security to identify potential vulnerabilities and threats in a network or computer system. Unlike malicious hacking, ethical hacking is performed with the explicit permission of the organization or individual owning the system, with the goal of improving security rather than exploiting it.

### 4. Web Application Hacking

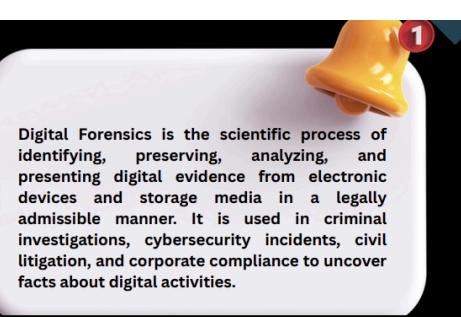
- Introduction to HTTP/HTTPS (Request Methods, Headers)
- Understanding the Web Application Attack Surface
- Introduction to OWASP Top 10 Vulnerabilities
- Lab Setup: Installing and Configuring Burp Suite
- Exploring Burp Suite Basics (Proxy, Repeater)
- Understanding and Exploiting Cross-Site Scripting (XSS)
- Preventing and Mitigating Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF) Attacks and Prevention Techniques
- Identifying and Exploiting Input Validation Vulnerabilities
- Introduction to SQL Injection Attacks (Manual Exploitation)
- SQL Injection Attacks (Automated Exploitation)
- Using SQLmap for Automated Database Exploitation
- Techniques for Preventing SQL Injections (Prepared Statements, ORM)
- Understanding and Exploiting File Upload Vulnerabilities
- Preventing Arbitrary File Execution via File Uploads
- Directory Traversal Attacks and Exploitation Techniques
- Mitigating Directory Traversal Attacks
- Session Management Vulnerabilities (Session Hijacking, Fixation)
- Preventing Session Hijacking and Session Fixation
- Authentication and Authorization Flaws (Insecure Password Storage)
- Exploiting Broken Access Control and Mitigation Techniques
- Exploiting Insecure Direct Object References (IDOR)
- Using Burp Suite for Automated Vulnerability Scanning
- Final Case Study: Performing a Full Web Application Penetration Test



Web Application Hacking refers to the process of identifying, exploiting, and mitigating security vulnerabilities in web applications (websites, APIs, or web services) to assess their security posture. Unlike malicious hacking, ethical hackers perform these tests with permission to improve defenses, while cybercriminals exploit flaws for data theft, fraud, or service disruption.

## 5. Digital Forensics

- Introduction to Digital Forensics & Chain of Custody
- Understanding Incident Response Lifecycle
- Memory Acquisition Techniques
- Memory Analysis using Volatility Framework
- Disk Imaging and Evidence Preservation
- File System Forensics (NTFS, FAT32, EXT)
- Using Tools: FTK Imager & Autopsy for Disk Analysis
- Windows Registry Forensics
- Log Analysis and Event Correlation
- Network Forensics (Analyzing PCAP files)
- Investigating Email Headers and Artifacts
- Malware Analysis
- Mobile Forensics
- Reporting & Documentation
- Final Lab: Full Digital Forensics Investigation Simulation



## 6. Final Project and Exam

### 1. Hands-on Project: Full Penetration Testing

- Perform a full penetration test on a virtual environment
- Identify vulnerabilities, exploit them, and conduct post-exploitation tasks
- Report writing and documentation of findings

### 2. Post-Exploitation Tasks

- Analysis of compromised systems
- Gathering evidence and conducting forensics on the compromised system

### 3. Final Exam Preparation

- Review all theoretical and practical aspects of the course
- Hands-on practice sessions to solidify knowledge before the final exam

### 4. Final Exam

- A comprehensive exam covering both theory and practical skills learned throughout the course