ByteLearned

Certified Cyber Security Professional Program

Practical • Job-Oriented • Video-Based LMS Training

■■■■■ 4.9 Rating | 12,400+ Students Enrolled | Updated May 2026

■ 30 Video Lessons	■■ 60+ Hours Total Content	■ 50+ Hands-on Labs	■ 20+ Section Quizzes	■ 10+ Certifications	■■ Lifetime Access

■ WHAT YOU WILL LEARN

■ Perform Ethical Hacking & Penetration Testing	■ Detect & Respond to incidents like a SOC Analyst
■ Secure Web Applications — OWASP Top 10	■ Master 50+ tools: Metasploit, Burp Suite, Splunk
■ Configure Firewalls, IDS/IPS & SIEM systems	■ Perform Cloud Security assessment on AWS & Azure
■ Analyse Malware — Static & Dynamic techniques	■ Crack CEH, Security+, eJPT certifications
■ Implement ISO 27001, GDPR, PCI-DSS compliance	■ Get hired — resume, interviews & portfolio

■ THIS COURSE INCLUDES

■ 30 in-depth video lessons (HD, 1–3 hrs each)	■ 30+ downloadable PDF cheat sheets & resources
■ 50+ hands-on lab exercises inside each video	■ 20+ quizzes after each section
■■ Access on Mobile, Tablet & Desktop	■■ Full lifetime access — watch anytime
■ ByteLearned Certificate of Completion	■■■ Live doubt-clearing sessions
■ Tool kits, scripts & lab files	■ Private student community access

■ COURSE CONTENT — 30 Video Lessons • 60+ Hours • 20 Sections

■ PHASE 1 — FOUNDATION

Video 1	Section 1: Introduction to Cyber Security	2 hrs 30 min

- What is Cyber Security — CIA Triad (Confidentiality, Integrity, Availability)
- Types of Cyber Threats: Malware, Phishing, Ransomware, Social Engineering
- Cyber Security Career Paths and Job Roles in 2026
- Overview of NIST, ISO 27001 and CIS Controls Frameworks
- Dark Web vs Deep Web vs Surface Web Explained
- Setting Up Your Learning Environment (VirtualBox + Kali Linux)
- **Quiz — Cyber Security Basics — 15 Questions**
- *Download: Cyber Security Career Roadmap 2026.pdf*

Video 2	Section 2: Networking Fundamentals — Part 1	2 hrs 45 min

- OSI Model — All 7 Layers Explained with Real-World Examples
- TCP/IP Protocol Suite — Deep Dive
- IP Addressing, Subnetting & CIDR Notation (with practice problems)
- DNS, DHCP, HTTP/HTTPS, FTP, SSH, SMTP — Security Implications
- Firewalls, Routers, Switches, IDS/IPS — Roles in Security
- VLANs, NAT and VPN Concepts
- *Download: Networking Protocols Cheat Sheet.pdf*

Video 3	Section 2: Networking Fundamentals — Part 2 (Labs)	2 hrs 30 min

- Lab: Installing & Configuring Wireshark for Packet Capture
- Lab: Capturing & Analysing HTTP, DNS, ARP Traffic
- Lab: Nmap — All Scan Types Explained with Practicals
- Lab: Network Topology Setup in GNS3 / Packet Tracer
- Reading and Interpreting Network Diagrams
- **Quiz — Networking for Security — 20 Questions**
- *Download: Nmap Cheat Sheet.pdf*
- *Download: Wireshark Filter Guide.pdf*

■ Video 4 — Section 3: Linux for Cyber Security — ■ 3 hrs

- ■ Linux File System, Directory Structure & Navigation
- ■ Users, Groups, File Permissions — chmod, chown, sudo
- ■ Essential Linux Commands Every Security Pro Must Know
- ■ Bash Scripting for Security Automation — Variables, Loops, Functions
- ■ Log Analysis & System Monitoring: journalctl, syslog, auth.log
- ■ Lab: Setting Up Kali Linux / Parrot OS in VirtualBox
- ■ Lab: SSH Hardening — Disable root login, key-based auth, UFW firewall
- ■ Lab: Writing a Port Scanner Script in Bash from Scratch
- ■ **Quiz — Linux Security — 15 Questions**
- ■ *Download: Linux Commands Cheat Sheet.pdf*
- ■ *Download: Bash Scripting Starter Kit.pdf*

■ Video 5 — Section 4: Windows Security & Active Directory — ■ 2 hrs 30 min

- ■ Windows Security Architecture — LSA, SAM, Security Subsystem
- ■ Active Directory Structure — Domains, OUs, Users, Groups, Trusts
- ■ Group Policy Objects (GPOs) — Setup & Security Hardening Use Cases
- ■ Windows Event Logs — Key Event IDs every analyst must know
- ■ Common Windows Attack Vectors and Defences
- ■ PowerShell for Security — Enumeration, Auditing & Automation
- ■ Lab: Active Directory Setup in Windows Server 2022
- ■ Lab: Analysing Windows Event Logs for Suspicious Activity
- ■ **Quiz — Windows & Active Directory — 15 Questions**
- ■ *Download: Windows Event IDs Cheat Sheet.pdf*
- ■ *Download: PowerShell Security Commands.pdf*

■ PHASE 2 — OFFENSIVE SECURITY / ETHICAL HACKING

■ Video 6	Section 5: Ethical Hacking Methodology & Lab Setup	■ 2 hrs

- ■ What is Ethical Hacking — Legal Aspects, Bug Bounty, Scope
- ■ Penetration Testing Phases: Recon → Scan → Exploit → Report
- ■ Lab: Full Hacking Lab Setup — Kali + Metasploitable + DVWA
- ■ How to Write a Professional Penetration Testing Report
- ■ **Quiz — Ethical Hacking Basics — 10 Questions**
- ■ *Download: Pentest Report Template.pdf*

■ Video 7	Section 6: Reconnaissance & OSINT	■ 2 hrs 30 min

- ■ Passive Recon — OSINT Methodology & Frameworks
- ■ Google Dorking — Advanced Search Operators for Recon
- ■ Shodan — Finding Exposed Devices & Services
- ■ DNS Enumeration, WHOIS Lookup & Subdomain Discovery
- ■ Lab: theHarvester — Email & Domain Recon in Practice
- ■ Lab: Maltego — Visualising the Attack Surface
- ■ Lab: Recon-ng & SpiderFoot — Automated OSINT Workflow
- ■ Active Recon with Nmap — Advanced Scan Techniques
- ■ **Quiz — Recon & OSINT — 15 Questions**
- ■ *Download: OSINT Toolkit & Resources List.pdf*

■ Video 8	Section 7: Vulnerability Assessment — Scanning & Analysis	■ 2 hrs 30 min

- ■ Vulnerability Scanning with Nessus — Full Walkthrough
- ■ OpenVAS — Installation, Configuration & Scanning
- ■ CVE Database & CVSS Scoring — Understanding Severity Ratings
- ■ Analysing Scan Reports & Prioritising Vulnerabilities
- ■ Lab: Scanning Metasploitable with Nessus & OpenVAS
- ■ Exploit-DB — Finding Public Exploits for Vulnerabilities
- ■ *Download: Vulnerability Management Process.pdf*

Video 9 — Section 7: Exploitation & Post-Exploitation with Metasploit — 3 hrs

- Metasploit Framework Architecture — Modules, Payloads, Encoders
- Lab: Exploiting Metasploitable — Multiple Attack Vectors
- Manual Exploitation Techniques — Without Metasploit
- Buffer Overflow Basics — Stack-Based Overflow Explained
- Privilege Escalation — Linux (SUID, Cron, Sudo) Techniques
- Privilege Escalation — Windows (Token Impersonation, AlwaysInstallElevated)
- Post-Exploitation — Persistence, Pivoting & Data Exfiltration
- Lab: Full Pentest on Metasploitable + CTF Challenge
- **Quiz — Exploitation Techniques — 20 Questions**
- *Download: Metasploit Cheat Sheet.pdf*
- *Download: PrivEsc Checklist Linux+Windows.pdf*

Video 10 — Section 8: Web Application Security — OWASP Top 10 (Part 1) — 3 hrs

- OWASP Top 10 — 2023 Edition Overview & Real-World Examples
- SQL Injection — Detection, Exploitation & Prevention (Manual + SQLMap)
- Cross-Site Scripting (XSS) — Stored, Reflected & DOM-Based
- Broken Authentication & Session Management Attacks
- IDOR (Insecure Direct Object Reference) — Finding & Exploiting
- Lab: SQL Injection & XSS on DVWA — Full Practical
- *Download: OWASP Top 10 Quick Reference.pdf*

Video 11 — Section 8: Web Application Security — Burp Suite & API Testing (Part 2) — 3 hrs

- CSRF, SSRF, XXE & Insecure Deserialization Explained
- Security Misconfigurations & Sensitive Data Exposure
- Burp Suite Complete Guide — Intercept, Repeater, Intruder, Scanner
- Lab: Full Web Application Pentest Workflow with Burp Suite
- API Security Testing — REST & GraphQL Vulnerabilities
- Lab: API Pentesting Practical on Vulnerable API
- Bug Bounty Hunting — Methodology & Top Platforms (HackerOne, Bugcrowd)
- **Quiz — Web App Security — 20 Questions**
- *Download: Burp Suite Shortcuts.pdf*
- *Download: Bug Bounty Hunting Checklist.pdf*

■ PHASE 3 — DEFENSIVE SECURITY

■ Video 12	Section 9: Network Security & Firewall Management	■ 2 hrs 30 min

- ■ Firewall Types — Stateful, Stateless, Next-Gen Firewalls (NGFW)
- ■ Lab: pfSense Firewall — Complete Setup, Rules & Configuration
- ■ IDS/IPS — Snort Rule Writing & Alert Configuration
- ■ Lab: Suricata IDS Setup, Traffic Analysis & Alert Tuning
- ■ Network Segmentation, DMZ Architecture & Zero Trust Concepts
- ■ VPN Setup — OpenVPN & WireGuard Practical Configuration
- ■ **Quiz — Network Security — 15 Questions**
- ■ *Download: pfSense Config Guide.pdf*
- ■ *Download: Snort Rules Cheat Sheet.pdf*

■ Video 13	Section 10: SIEM & Security Monitoring with Splunk	■ 3 hrs

- ■ What is SIEM? — Architecture, Use Cases & How It Fits in a SOC
- ■ Lab: Splunk Installation, Configuration & Log Ingestion
- ■ Splunk Search Processing Language (SPL) — Complete Guide
- ■ Building Dashboards, Alerts & Correlation Rules in Splunk
- ■ Writing SIEM Use Cases for Real-World Threats
- ■ Threat Hunting Methodology Using Splunk
- ■ Lab: ELK Stack (Elasticsearch, Logstash, Kibana) Setup & Use
- ■ Microsoft Sentinel Overview — Cloud-Native SIEM
- ■ **Quiz — SIEM & Monitoring — 15 Questions**
- ■ *Download: Splunk SPL Cheat Sheet.pdf*
- ■ *Download: ELK Stack Setup Guide.pdf*

■ Video 14 — Section 11: Incident Response & Digital Forensics — ■ 3 hrs

- ■ Incident Response Lifecycle — NIST SP 800-61 Framework
- ■ Malware Analysis — Static Analysis (Strings, PE Headers, YARA Rules)
- ■ Malware Analysis — Dynamic Analysis (Cuckoo Sandbox, ANY.RUN)
- ■ Disk Forensics — Evidence Acquisition with FTK Imager
- ■ Lab: Autopsy — Full Disk Investigation & Artefact Recovery
- ■ Memory Forensics with Volatility — Process, Network & Registry Analysis
- ■ Network Forensics — Packet-Level Investigation with Wireshark
- ■ Writing Professional Incident Response Reports
- ■ **Quiz — IR & Digital Forensics — 15 Questions**
- ■ *Download: IR Playbook Template.pdf*
- ■ *Download: Volatility Commands Cheat Sheet.pdf*

■ Video 15 — Section 12: Endpoint Security & Threat Intelligence — ■ 2 hrs

- ■ EDR Solutions — CrowdStrike Falcon & SentinelOne Overview
- ■ MITRE ATT&CK; Framework — Complete Practical Guide
- ■ IOC (Indicators of Compromise) — Collection, Analysis & Sharing
- ■ Threat Intelligence Platforms — VirusTotal & AlienVault OTX
- ■ Email Security — Phishing Header Analysis in Depth
- ■ SPF, DKIM & DMARC — Setup, Verification & Troubleshooting
- ■ **Quiz — Threat Intelligence — 10 Questions**
- ■ *Download: MITRE ATT&CK; Quick Reference.pdf*
- ■ *Download: Phishing Analysis Checklist.pdf*

■ PHASE 4 — CLOUD, GRC & ADVANCED TOPICS

■ Video 16 — Section 13: Cloud Security — AWS & Azure — ■ 3 hrs

- ■ Cloud Security Fundamentals & Shared Responsibility Model
- ■ AWS IAM — Users, Roles, Policies & Permission Boundaries Best Practices
- ■ AWS Security Services — GuardDuty, CloudTrail, Security Hub, Macie
- ■ Lab: AWS Security Assessment — Finding Misconfigurations
- ■ Azure Security Center, Microsoft Defender & Sentinel Overview
- ■ Container Security — Docker Hardening & Kubernetes Security
- ■ Lab: Docker Security — Scanning Images & Hardening Containers
- ■ S3 Bucket Security, Serverless Security & Secrets Management
- ■ **Quiz — Cloud Security — 15 Questions**
- ■ *Download: AWS Security Cheat Sheet.pdf*
- ■ *Download: Docker Security Checklist.pdf*

■ Video 17 — Section 14: Governance, Risk & Compliance (GRC) — ■ 2 hrs

- ■ Introduction to GRC — Why Compliance is a Career in Itself
- ■ ISO 27001 — ISMS Implementation Step-by-Step Guide
- ■ GDPR, India PDPB, PCI-DSS & HIPAA — Key Requirements
- ■ Risk Assessment, Risk Register & Risk Treatment Planning
- ■ Writing Security Policies, Procedures & Standards
- ■ Security Audit Process — Planning, Execution & Reporting
- ■ **Quiz — GRC & Compliance — 15 Questions**
- ■ *Download: ISO 27001 Controls Summary.pdf*
- ■ *Download: Risk Assessment Template.pdf*

Video 18	Section 15: Cryptography, PKI & Password Security	2 hrs

- Symmetric Encryption — AES, DES, 3DES with Real Examples
- Asymmetric Encryption — RSA, ECC — How Public/Private Keys Work
- Hashing Algorithms — MD5, SHA-1, SHA-256 — Uses & Weaknesses
- SSL/TLS — How HTTPS Works Internally Step by Step
- PKI & Digital Certificates — CA, CSR, Certificate Chains
- Lab: Hashcat — Password Cracking (Dictionary, Brute Force, Rules)
- Lab: John the Ripper — Cracking Linux & Windows Password Hashes
- **Quiz — Cryptography — 15 Questions**
- *Download: Cryptography Cheat Sheet.pdf*
- *Download: Hashcat Attack Modes Guide.pdf*

Video 19	Section 16: Malware Analysis & Reverse Engineering	2 hrs 30 min

- Types of Malware — Viruses, Worms, Trojans, RATs, Ransomware, Rootkits
- Static Analysis — PE Headers, Strings, Imports & YARA Rule Writing
- Dynamic Analysis — ANY.RUN & Cuckoo Sandbox Walkthrough
- Introduction to Assembly Language for Reverse Engineering
- Lab: Ghidra — Reverse Engineering a Real Malware Sample
- Lab: IDA Free — Binary Analysis Practical
- Python Scripting for Security Automation — Practical Examples
- **Quiz — Malware Analysis — 10 Questions**
- *Download: Malware Analysis Cheat Sheet.pdf*
- *Download: YARA Rules Starter Pack.pdf*

■ PHASE 5 — SPECIALISATION & CAREER PREPARATION

■ Video 20	Section 17: Advanced Penetration Testing	■ 3 hrs

- ■ Advanced Metasploit — Custom Payloads, Encoding & AV Evasion
- ■ Active Directory Attacks — Pass-the-Hash, Pass-the-Ticket
- ■ Kerberoasting — Extraction & Cracking Service Account Hashes
- ■ BloodHound — Mapping AD Attack Paths Visually
- ■ Lab: Full Active Directory Attack Chain from Foothold to DA
- ■ Red Team vs Blue Team — Exercises & Adversary Simulation
- ■ C2 Frameworks — Cobalt Strike & Sliver Overview
- ■ Physical Security & Social Engineering Attack Techniques
- ■ **Quiz — Advanced Pentesting — 10 Questions**
- ■ *Download: AD Attack Cheat Sheet.pdf*
- ■ *Download: BloodHound Query Guide.pdf*

■ Video 21	Section 18: SOC Analyst Training — Tier 1 & Tier 2	■ 2 hrs 30 min

- ■ SOC Structure — Tier 1, Tier 2, Tier 3 Roles & Responsibilities
- ■ Alert Triage & Prioritisation — Real-World Workflow
- ■ Lab: Handling a Real-World Phishing Incident End-to-End
- ■ Lab: Ransomware Incident Simulation — Detection to Containment
- ■ Playbook Creation & SOAR Automation — Splunk SOAR Overview
- ■ Lab: TheHive — Incident & Case Management Platform
- ■ Shift Handover, SOC Metrics & Daily Reporting
- ■ **Quiz — SOC Operations — 15 Questions**
- ■ *Download: SOC Analyst Playbook Template.pdf*
- ■ *Download: Alert Triage Decision Tree.pdf*

■ Video 22 — Section 19: Certification Preparation — Security+, CEH, eJPT — ■ 2 hrs 30 min

- CompTIA Security+ (SY0-701) — Full Syllabus Review & Exam Tips
- CEH v12 — Key Domains, Exam Format & Strategy
- eJPT (eLearnSecurity Junior Pentester) — Complete Exam Walkthrough
- OSCP Path — How to Continue After This Course
- Google Cyber Security Certificate — Overview & Value
- Mock Exam — 60 Mixed Questions (Security+ Style)
- Exam Day Tips — Time Management & Eliminating Wrong Answers
- *Download: Security+ Study Guide.pdf*
- *Download: CEH Domain Summary.pdf*
- *Download: eJPT Tips & Tricks.pdf*

■ Video 23 — Section 20: Career Development & Job Placement — ■ 2 hrs

- Building a Cyber Security Resume That Gets Shortlisted
- Optimising Your LinkedIn Profile for Security Recruiters
- Building Your Portfolio — TryHackMe, HackTheBox & GitHub
- Top 50 Cyber Security Interview Q&A; — Technical + HR Rounds
- Freelancing in Cyber Security — Bug Bounty, Consulting & VAPT
- Salary Benchmarks — Freshers to Senior Roles in India & Globally
- Live Mock Interview Assignment — Submit for Feedback
- *Download: Resume Template.pdf*
- *Download: LinkedIn Optimisation Guide.pdf*
- *Download: Top 50 Interview Q&A.pdf;*

■ BONUS VIDEOS — Extra Skills & Deep Dives

■ Video 24 — Section B1: Wireless Network Security — ■ 1 hr 30 min

- WiFi Security Protocols — WEP, WPA, WPA2, WPA3
- Wireless Attacks — Evil Twin, Deauth, PMKID Attack
- Lab: Aircrack-ng — Cracking WPA2 Handshake in a Lab Setup
- Bluetooth & IoT Security Overview
- **Quiz — Wireless Security — 10 Questions**
- *Download: Wireless Attacks Cheat Sheet.pdf*

■ Video 25 — Section B2: Social Engineering & Phishing Attacks — ■ 1 hr 30 min

- Social Engineering Techniques — Pretexting, Baiting, Tailgating
- Phishing, Spear Phishing & Whaling — Real Examples
- Lab: GoPhish — Setting Up a Phishing Simulation Campaign
- Defending Against Social Engineering — Awareness Training
- *Download: Social Engineering Playbook.pdf*

■ Video 26 — Section B3: Dark Web Monitoring & Threat Hunting — ■ 1 hr 30 min

- How the Dark Web Works — Tor Network Explained
- Dark Web Monitoring Tools — Intelligence Gathering
- Proactive Threat Hunting — Hypothesis-Driven Methodology
- Lab: Threat Hunting using Splunk & ELK Stack
- *Download: Threat Hunting Playbook.pdf*

■ Video 27 — Section B4: DevSecOps — Security in CI/CD Pipelines — ■ 1 hr 30 min

- What is DevSecOps — Shifting Security Left
- SAST & DAST Tools — SonarQube, OWASP ZAP Integration
- Secrets Scanning — Detecting API Keys in Code Repos
- Lab: Adding Security Checks to a GitHub Actions Pipeline
- *Download: DevSecOps Checklist.pdf*

■ Video 28 — Section B5: Zero Day Research & Responsible Disclosure — ■ 1 hr

- What is a Zero Day Vulnerability — Discovery & Lifecycle
- CVE Process — How Vulnerabilities Get Assigned & Published
- Responsible Disclosure — How to Report Bugs Ethically
- Building a Bug Bounty Report that Gets Paid

■ Video 29 — Section B6: Cyber Security for Small Businesses — ■ 1 hr

- ■ Most Common Cyber Attacks Targeting Small Businesses
- ■ Essential Security Measures Every Business Needs
- ■ Setting Up a Basic Security Stack on a Budget
- ■ Employee Security Awareness Training Tips
- ■ *Download: SMB Security Checklist.pdf*

■ Video 30 — Section B7: Final Capstone Project & Graduation — ■ 2 hrs

- ■ Capstone Overview — Full Pentest + Defence Report on Lab Environment
- ■ Step 1: Recon & Vulnerability Assessment on Target Network
- ■ Step 2: Exploitation & Post-Exploitation
- ■ Step 3: Incident Response & Forensics on the Compromised System
- ■ Step 4: Writing Your Professional Final Report
- ■ Certificate of Completion Awarded ■
- ■ *Download: Capstone Project Guide.pdf*
- ■ *Download: Final Report Template.pdf*

■ JOB ROLES & SALARY AFTER COMPLETION

Job Role	Experience	Avg Salary (India)
SOC Analyst Tier 1 / Tier 2	Fresher – 1 yr	■3.5 – 6 LPA
Penetration Tester / Ethical Hacker	1 – 2 yrs	■5 – 10 LPA
Security Engineer	1 – 3 yrs	■6 – 14 LPA
Cloud Security Engineer	2 – 4 yrs	■10 – 22 LPA
Incident Responder / DFIR Analyst	2 – 4 yrs	■8 – 18 LPA
GRC / Compliance Analyst	1 – 3 yrs	■5 – 12 LPA
Security Architect / Manager	5+ yrs	■22 – 45 LPA+

■■ 50+ TOOLS YOU WILL MASTER

Kali Linux	Metasploit	Nmap	Wireshark	Burp Suite	Nessus
OpenVAS	Splunk	ELK Stack	Snort	Suricata	pfSense
BloodHound	Mimikatz	Hashcat	John the Ripper	SQLMap	Nikto
Autopsy	Volatility	Ghidra	IDA Free	ANY.RUN	Shodan
Maltego	theHarvester	Recon-ng	OWASP ZAP	Docker	AWS Security
Azure Sentinel	CrowdStrike	VirusTotal	AlienVault OTX	GoPhish	Aircrack-ng
CyberChef	OpenSSL	TryHackMe	HackTheBox	TheHive	Cuckoo Sandbox
VirtualBox	VMware	PowerShell	Python		