APPRISE CYBER
SERVING INFORMATION WITH DIGITAL SECURITY

Apprise Cyber Online Cybersecurity Bootcamp - Batch #8

CYBER SECURITY ENGINEER

16x LiveClass

Batch-08 Classes Start:
2nd May 2026
Limited Seats Available

Early Bird Discount

~~PKR 40,000~~
PKR 30,000

(16x Sessions - 2 Month Program)

Learn cybersecurity skills in just 2 months!
Start from zero with professional guidance.

- Expert Instructors
- 16x Live Class Sessions
- Lifetime Materials
- Recorded Sessions
- Hands-on Practice
- Dedicated Facilitator
- Final Project
- Weekly Projects
- Certificate
- Career Support

APPRISE CYBER
PENETRATION TESTING | INFOSEC SECURITY

WEEK 01 — FOUNDATIONS & NETWORK FUNDAMENTALS

SATURDAY — SESSION 01

Intro to Pentesting & Ethical Hacking

- Pentesting vs Ethical Hacking
- Pentest Phases (Recon → Exploit → Report)
- Legal Scope & Bug Bounty Basics
  - Rules of engagement, responsible disclos.
  - Bug bounty platforms
- Lab Setup (Kali, VM, TryHackMe)
- Certifications Overview (CEH, OSCP, eJPT)

LAB: Setup Kali VM + Complete TryHackMe Intro Room

SUNDAY — SESSION 02

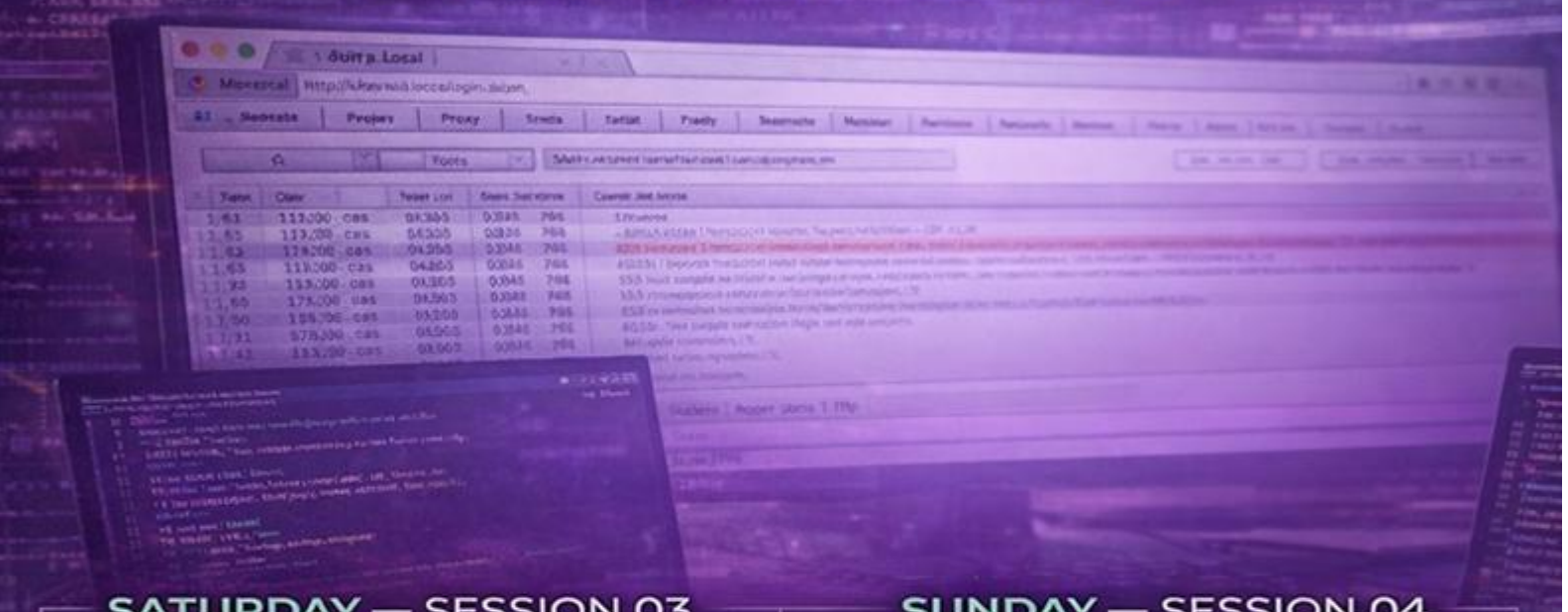
Network Fundamentals & Recon

- TCP/IP Model Basics
- Common Ports (80, 443, 21, 22, 445, etc.)
- TCP vs UDP (Differences & why it matters in pentesting)
- Nmap (Scanning + Detection)
- Passive Recon (WHOIS, Shodan, Google Dorks)

LAB: Scan Metasploitable 2 using Nmap + Report Findings

APPRISE CYBER
PENETRATION TESTING | INFOSEC SECURITY

WEEK 02 — WEB APPLICATION PENETRATION TESTING



SATURDAY — SESSION 03

Web App Fundamentals & OWASP Top 10

- How web apps work: HTTP request/response cycle, cookies, sessions, headers
- OWASP Top 10 overview — the most critical web vulnerabiillities
- Introduction to Burp Suite — proxy setup, intercept, repeater
- SQL Injection — theory, manual testing, error-based vs blind
- Cross-Site Scripting (XSS) — reflected, stored, DOM-based
- Cross-Site Request Forgery (CSRF) basics

LAB: DVWA & BURP SUITE

Set up DVWA (Damn Vulnerable Web App). Use Burp Suite proxy to intercept requests. Exploit low-security SQLi and reflected XSS vulnerabilities manually.

SUNDAY — SESSION 04

Advanced Web Vulnerabilities & Automated Testing

- Authentication flaws — weak passwords, brute force, credential stuffing
- Insecure Direct Object Reference (IDOR) —, accessing unauthortzed data
- File upload vulnerabilities — bypassing extension checks
- Directory traversal & Local File Inclusion (LFI)
- Security misconfigurations — default credentials, exposed admin panels

LAB: JUICE SHOP CTF

Tackle beginner-level OWASP JuiceShop challenges, login bypass, IDOR, XSS, and sensitive data exposure. Document each finding with impact & remedlation notes.

APPRISE CYBER
PENETRATION TESTING | INFOSEC SECURITY

WEEK 03 — MOBILE PENTESTING: ANDROID & iOS

SATURDAY — SESSION 05

Android Penetration Testing

- Android architecture — permissions, components (Activities, Services, Broadcast Receivers)
- OWASP Mobile Top 10 — most common mobile vulnerabilities
- Static analysis: decompiling APKs with JADX, reading
- AndroidManifest.xml
- Identifying hardcoded secrets, insecure data storage, exported components
- Dynamic analysis: ADB commands, traffic interception with Burp Suite on emulator

LAB: INSECURESHOP APK

Decompile InsecureShop APK using JADX. Find hardcoded credentials, exported activities, and insecure SharedPreferences. Intercept traffic using Burp Suite + Android emulator.

SUNDAY — SESSION 06

iOS Penetration Testing

- iOS security model
- Differences between iOS & Android attack surfaces
- Static analysis. inspecting IPA files, Info.plist, ATS settings
- Insecure data storage: NSUserDefaults, Keychain misuse, cleartext storage
- Traffic interception on IOS with Burp Suite + SSL pinning bypass
- Tools: objection, Frida (intro) — testing in simulator vs physical device

LAB: DVIA-v2 (DAMN VULNERABLE iOS APP)

Test DVIA-v2 to identify insecure local storage, broken authentication, and side channel data leakage. Review Info.plist misconfigurations.

APPRISE CYBER
PENETRATION TESTING | INFOSEE. SECURITY

WEEK 04 — EXPLOITATION, POST-EXPLOITATION & REPORTING

SATURDAY — SESSION 07

Exploitation Techniques & Metasploit Framework

- Understanding exploit development basics — buffer overflows, shellcode concepts
- Metasploit Framework architecture: msfconsole, modules, payloads, encoders
- Searching and using exploits: search, use, set, run / exploit
- Staged vs stageless payloads — Meterpreter vs shell
- Exploiting known CVEs on Metasploitable 2 (vsftpd, Samba, UnrealIRCd)
- Generating custom payloads with msfvenom
- Antivirus evasion fundamentals — encoding, obfuscation overview

LAB: METASPLOIT ON METASPLOITABLE 2

Use Metasploit to exploit at least three services on Metasploitable 2 (e.g, vsftpd 2.3.4 backdoor, Samba usermap_script, Java RM). Capture shells and document each step with screenshots in the provided report template.

SUNDAY — SESSION 08

Post-Exploitation, Privilege Escalation & Professional Reporting

- Post-exploitation goals: persistence, lateral movement, data exfiltration concepts
- Linux privilege escalation — SUID binaries, sudo misconfigs, cron jobs, world-writable paths
- Windows privliege escalation — unquoted service paths, weak registry permissions, token impersonation
- Pivoting & port forwarding fundamentals —SSH tunnels, Meterpreter routing
- Covering tracks — log clearing concepts & forensic awareness. lokelncal findings CVSS scoring
- Remediation recommendations a re-test methodology.

LAB: CAPSTONE CTF & FULL PENTEST REPORT

Conduct a mini end-to-end penetration test aginist a provided vulnerable VM (VulnHub). Complete full phases:·Recon ✦ Scarnivs ✦ exploitation ✦ Post-exploitation Deliver a professional pentest report covering exesotive sammary. tamrioal trising reommendaiots.

LEVEL UP YOUR CAREER

GRC INSIGHT BEGINS

GOVERNANCE
Build Strong Foundations

RISK
Identify, Assess & Mitigate

COMPLIANCE
Stay Compliant, Stay Ahead

PERFORMANCE
Improve Processes & Outcomes

CAREER GROWTH
In-Demand Skills, Better Opportunities

LEARN. APPLY. GROW.

APPRISE CYBER
PENETRATION TESTING | INFOSEC. SECURITY

WEEK 01 — GRC FOUNDATIONS & ISMS IMPLEMENTATION BASICS:

SATURDAY — SESSION 01

Module 1: Foundations of GRC & ISO Ecosystem

- Background and history of ISO
- Introduction to ISO/IEC 27001 and ISMS
- Accreditation vs Certification
- Normative vs Informative requirements
- Core components of GRC:
  - Governance
  - Risk Management
  - Compliance
  - Audit & Assurance

LAB: GRC FRAMEWORK MAPPING
Map GRC components to ISO/IEC 27001 clauses. Identify normative vs informative requirements with real examples.

SUNDAY — SESSION 02

Module 2: Implementing the ISMS (ISO 27001)

- Determining the scope of ISMS
- Executing risk assessment
- Development of Statement of Applicability (SoA)
- Planning for internal audits
- Conducting top management review

LAB: RISK ASSESSMENT & SoA
Perform risk assessment for a sample organization. Develop Statement of Applicability (SoA) based on assessed risks.

Outcome: Build strong GRC & ISMS implementation foundations.

APPRISE CYBER
PENETRATION TESTING | INFOSEC. SECURITY

WEEK 02 — IMPLEMENTING ISMS, AUDIT PLANNING & STANDARDS

SATURDAY — SESSION 03

Module 2: Implementing the ISMS (ISO 27001)

- Determining the scope of ISMS
- Executing risk assessment
- Development of Statement of Applicability (SoA)
- Planning for internal audits
- Conducting top management review

LAB: ISMS IMPLEMENTATION WORKSHOP
Hands-on exercise to define ISMS scope, perform risk assessment, and create Statement of Applicability (SoA).

LAB: TOP MANAGEMENT REVIEW PREP
Prepare management review inputs and review ISMS performance metrics.

SUNDAY — SESSION 04

Module 3: Audit Planning & Standards

- Overview of:
  - ISO/IEC 17021
  - ISO/IEC 27006
  - IAF Mandatory Requirements
- Audit team roles and responsibilities
- Developing an annual audit plan

LAB: AUDIT STANDARDS EXPLORER
Review and compare ISO/IEC 17021, ISO/IEC 27006, and IAF Mandatory Requirements.

LAB: ANNUAL AUDIT PLAN BUILDER
Create a risk-based annual audit plan for an ISMS environment.

Outcome: Understand how to implement an ISMS effectively and plan audits in alignment with international standards.

APPRISE CYBER

PENETRATION TESTING | INFOSEC. SECURITY

WEEK 03 – GRC ADVANCED COMPLIANCE & AUDIT JUDGMENT MASTERY

SATURDAY — SESSION 5

Module 5: Regulatory Alignment & Audit Perspective on Compliance

- Auditor's perspective on evaluating regulatory compliance within an ISMS
- Overview of key global and regional regulatory frameworks from an audit standpoint
- Techniques for mapping ISO/IEC 27001 controls to legal, regulatory, and contractual obligations
- Assessing completeness and accuracy of compliance obligations within ISMS scope
- Evaluating evidence of compliance during audits:
  - Policies, procedures, and legal registers
  - Records demonstrating adherence
- Identifying common compliance gaps and audit findings related to regulatory misalignment
- Role of audit in validating ongoing compliance and detecting control weaknesses

LAB: REGULATORY MAPPING & COMPLIANCE EVIDENCE REVIEW
Map ISO/IEC 27001 controls to regulatory requirements. Review compliance evidence and identify gaps.

SUNDAY — SESSION 6

Module 6: Audit Judgment, Real-World Scenarios & Case Analysis

- Auditor's approach to real-world audit situations and complex environments
- Analysis of audit scenarios, including:
  - Major and minor nonconformities
  - Weak control environments and ineffective implementations
- Identification of audit red flags:
  - Inconsistent evidence
  - Over-reliance on documentation without implementation
  - Lack of risk-based decision-making
- Evaluating authenticity and reliability of audit evidence
- Recognizing and addressing attempts to bypass or manipulate audit outcomes
- Applying professional skepticiom and auditor judgment in decision-making

LAB: AUDIT SCENARIO ANALYSIS & JUDGMENT PRACTICE
Analyze real-world audit scenarios. Identify nonconformities, red flags, and apply auditor judgment.

OUTCOME: Build strong GRC & ISMS implementation foundations

APPRISE CYBER
PENETRATION TESTING | INFOSEC. SECURITY

WEEK 04 — ISO 27001 CERTIFICATION LIFECYCLE & EXAM PREPARATION:

SATURDAY — SESSION 07

Module 7: Continuous Improvement, Management Review & Internal Audit

- Management review process
- Internal audit planning & execution
- Nonconformity management
- Corrective & preventive actions (CAPA)
- Performance evaluation & metrics
- Continual improvement strategies

LAB: MANAGEMENT REVIEW & CAPA PRACTICE
Conduct a mock management review meeting and document CAPA actions.

LAB: INTERNAL AUDIT SIMULATION
Perform an internal audit using checklist and identify nonconformities.

SUNDAY — SESSION 08

Module 8: External Audit Preparation & Certification Exam

- Preparing for Stage 1 & Stage 2 audits
- Auditor expectations & evidence preparation
- Handling audit findings
- Mock external audit scenario
- Certification exam strategy & tips
- Certification Exam

FINAL EXAM
Exam Type: Closed Book
Duration: 90 Minutes
Total Questions: 100
Passing Marks: 70% (70/100)
Question Pattern:
- 70% MCQs / BCQs based
- 30% Scenario Based

Outcome: Understand the complete ISO 27001 certification lifecycle and be exam-ready for the comprehensive final exam.

BATCH 8

MARK YOUR CALENDAR

- SATURDAY & SUNDAY ONLY
- 11 am to 2 pm
- 16 SESSIONS ACROSS 8 WEEKS
- 48 HOURS
- LECTURE + HANDS-ON LABS

BATCH 8

APPRISE CYBER
SERVING INFORMATION WITH DIGITAL SECURITY

COURSE BENEFITS

- 48 Hours Intensive Weekend Cyber Security Training
- Beginner to Intermediate Friendly — Step-by-Step Learning
- Hands-on Labs in Every Session (Real Practice)
- Learn Complete Pentesting Workflow (Recon Exploitation Reporting)
- Practical Experience with Tools (Nmap, Burp Suite, Metasploit)
- Web Application Hacking using OWASP Top 10
- Mobile App Pentesting (Android & iOS Basics)
- Real Lab Environments (DVWA, Juice Shop, Metasploitable)
- Capture The Flag (CTF) Challenges for Skill Building
- Exploitation & Privilege Escalation Techniques
- Professional Pentest Report Writing with CVSS
- Career Roadmap Guidance (OSCP, eJPT, Bug Bounty)


HGW
HACK GOVERN WORK
EMPOWERING SECURITY THROUGH GOVERNED PRACTICES
This certificate recognizes your achievement in developing a solid understanding of the fundamental concepts and principles of cybersecurity.
HGW
BATCH 5
has successfully completed the
HACK GOVERN WORK (HGW)
We wish you the best of luck in your future endeavors.
Signature
CEO
Signature
INSTRUCTOR
ASA2301432
Certificate Number

Real-World Hacking Experience in HACK. GOVERN. WORK. Bootcamp

LIVE HACKING PRACTICE & PROFESSIONAL CERTIFICATION

Learn directly from expert cybersecurity mentors in the HACK. GOVERN. WORK. Bootcamp — covering the complete penetration testing workflow from reconnaissance and scanning to exploitation, with comprehensive, hands-on training.

EARLY BIRD DISCOUNT

Till 19th April

Discount
25%

PKR ~~40,000~~
PKR30,000

APPRISE CYBER

www.apprise-cyber.com

Course Duration: 2 Months

WHAT DO OUR ALUMNI SAY ABOUT THE COURSE ?

Apprise Cyber offers a structured and beginner-friendly learning environment. The course covers both fundamentals and practical labs, helping students build strong cybersecurity skills step by step.

Anas Shahnawaz
Cyber Security Student, Batch 6

The course content is well-organized and easy to understand.
Each module is designed with real-world examples, making it easier to learn penetration testing concepts practically.

Muhammad Moiz
Cyber Security Student, Batch 7

Apprise Cyber provides one of the best learning experiences in cybersecurity. The hands-on labs and instructor guidance helped me understand real-world scenarios effectively.

Abdul Ghaffar Bhatti
Cyber Security Student, Batch 6

The **training program** is highly practical and focused on **real skills.**
I especially liked the structured approach and detailed explanations of vulnerabilities and tools.

Solo Pace
Cyber Security Student, Batch 7

This course helped me understand application security concepts clearly. The combination of theory and labs made learning engaging and effective.

Cyber Security Student
Cyber Security Student, Batch 6

Apprise Cyber maintains high-quality training standaras. The instructors explain complex topics in a simple way, making it Ideal for beginners and intermediate learners.

Ali Raza
Cyber Security Student, Batch 7