

ETHICAL HACKING & BUG BOUNTY

Complete Course Roadmap & Syllabus • 2026 Edition

Course Objective

This comprehensive curriculum is designed to take you from foundational security concepts to advanced penetration testing and bug bounty hunting. Every module is highly practical, lab-based, and focused on modern real-world techniques used in professional engagements globally.

PHASE 1 Security Foundations & Core Workflows

Module 1: Introduction to Cybersecurity

- Deep dive into Offensive and Defensive Security
- Setting up VMware Workstation or VirtualBox
- Installing and configuring Kali Linux
- Essential tools overview and installation basics
- Getting comfortable with the terminal

Module 2: Master Linux from Basic to Advanced

- Understanding the Linux file system
- Mastering the Kali Linux command line
- Networking commands and file transfers
- Shell environment and customization
- Users, groups, and permissions
- Process management, services, and systemd
- Package management and repositories

Module 3: Penetration Testing and Types

- White Box Testing
- Black Box Testing
- Grey Box Testing

Module 4: Phases in Pentesting

- Pre-Engagement
- Scanning and Enumeration
- Exploitation
- Privilege Escalation
- Maintaining Access (if required)
- Reporting
- Information Gathering (Reconnaissance)
- Vulnerability Assessment
- Post-Exploitation
- Lateral Movement
- Cleanup
- Remediation and Retesting

Module 5: Burp Suite Professional Mastery

- Installing Burp Suite Professional on Windows and Linux
- Setting up the proxy between browser and Burp
- Installing the Burp CA certificate
- **Core Tabs Walkthrough:**
 - Dashboard: Tasks, Event log, Issue activity
 - Target: Site map, Scope, Issue definitions
 - Proxy: Intercept, HTTP history, WebSockets, Match & Replace
 - Intruder: Positions, Payloads, Resource pool
 - Repeater, Sequencer, Decoder, Comparer, Logger, Organizer
 - Extensions: Installed, BApp Store, APIs
 - Scanner (Pro-only detection) & Burp AI (Pro)
- **Practical Skills:** Intercepting/modifying requests, Fuzzing & brute force, Out-of-band detection

PHASE 2 Reconnaissance & Target Mapping

Module 6: Reconnaissance Fundamentals

- What is reconnaissance and why it matters
- Active vs passive reconnaissance
- The mindset: thinking like a target mapper
- Understanding domains, subdomains, hosts, and resolution
- Target mapping: building a complete picture
- Scope and out-of-scope rules
- Rate limiting and staying under the radar

Module 7: **Passive Recon with OSINT Platforms**

- Shodan: exposed services search
- FOFA: asset discovery and fingerprinting
- Google dorking for exposed files
- GitHub and source code leakage hunting
- Combining OSINT output into profiles
- Censys: internet-wide scanning
- HackerTarget: DNS, WHOIS, host lookups
- Certificate transparency logs
- Wayback Machine and historical data

Module 8: **Active Recon with Nmap**

- What Nmap is and why we use it
- TCP vs UDP overview
- TCP SYN Scan (Stealth Scan)
- Version & OS Detection
- TCP & UDP Full Port Scans (65535 ports)
- **Practical Machine:** Challenge NetSec
- Ports: what they are & why they matter
- Basic Nmap Scan
- TCP Connect & UDP Scans
- Full Port Range & Aggressive Scans
- Common Protocols and Services

Module 9: **Recon Automation using Bash Scripting**

- Why automate reconnaissance & building project structures
- Subdomain enumeration (Subfinder, Assetfinder, Findomain)
- Identifying live subdomains with httpx
- URL and endpoint discovery with Waymore and Katana
- Extracting interesting files (backups, configs, logs) & filtering
- Hunting with Nuclei (templates, severity, rate limits)
- Building a full end-to-end recon script with checkpoint/resume

Module 10: **Manual Hunting – Info Disclosure**

- What counts as information disclosure
- Disclosure in error messages & debug pages
- Source code disclosure via backup files
- Directory brute forcing with Feroxbuster, FFUF, Dirbuster

Module 11: **File Path Traversal Vulnerabilities**

- Basic exploitation: reading arbitrary files
- Absolute path & non-recursive sequence bypass techniques
- Automating path traversal discovery

Module 12: Automated Information Disclosure Techniques

- Automating information disclosure detection
- Building an automated reconnaissance workflow
- Chaining recon tools into a single pipeline
- Reducing false positives and reporting findings

PHASE 3 Web Application Pentesting & Exploitation

Module 13: OS Command Injection

- Introduction & basic command injection exploitation
- Blind command injection using time delays & output redirection
- Bypassing basic input filters

Module 14: Server-Side Request Forgery (SSRF)

- SSRF against a local server & internal backend systems
- SSRF blacklist filter bypass
- Using Burp Collaborator for detection

Module 15: File Upload Vulnerabilities & RCE

- Web shell upload and remote code execution
- Content-Type restriction & Path traversal upload bypass
- Polyglot web shell upload & Obfuscated file extension bypass

Module 16: Access Control Vulnerabilities

- Unprotected admin panels
- Privilege escalation via requests
- Insecure Direct Object References (IDOR)
- Admin access via predictable URLs
- Role modification exploits
- Password disclosure via user ID

Module 17: Business Logic Vulnerabilities

- Client-side trust exploitation
- Security control inconsistencies
- Dual-use endpoint vulnerabilities
- High-level logic vulnerabilities
- Weak business rule enforcement
- Workflow validation failures

Module 18: Cross-Site Scripting (XSS)

- Introduction to Reflected, Stored, and DOM-Based XSS
- Advanced DOM XSS exploitation techniques

Module 19 & 20: SQL Injection (Fundamentals to Advanced)

- SQL programming basics & Authentication bypass
- UNION-based SQL injection & Column enumeration
- Extracting data from tables & Multi-value data extraction
- Database enumeration & Blind SQL injection (time-based)
- SQLMap automation: complete guide

Module 21: XML Injection & XXE Attacks

- XML injection overview
- XXE file disclosure & XXE SSRF exploitation
- Blind XXE with out-of-band interaction

Module 22: SSTI to RCE

- Identifying template engines
- Exploiting Server-Side Template Injection to achieve RCE
- Hands-on practical labs

Module 23: API Testing

- Exploiting API endpoints using documentation
- Exploiting server-side parameter pollution in a query string
- Finding and exploiting an unused API endpoint

Module 24: JWT Attacks

- JWT authentication bypass via unverified signature
- JWT authentication bypass via flawed signature verification

PHASE 4 Network Security & Frameworks

Module 25: Vulnerabilities 101

- How vulnerabilities are rated and Common Vulnerability Scoring System (CVSS)
- Databases for vulnerability research
- **Practical machine:** Capstone

Module 26: **Nessus — Vulnerability Scanner**

- Installing, configuring, and setting up scans and policies
- Running Nessus against real targets
- Reading scan results and prioritizing findings

Module 27: **Master Metasploit**

- Understanding modules: exploits, payloads, auxiliaries, post
- Setting up target details (RHOSTS, RPORT) and payloads (LHOST, LPORT)
- Choosing the right exploit for a service
- Working with sessions, backgrounds, and Meterpreter fundamentals
- **Practical Machine using Metasploit:** Blue (Windows)

PHASE 5 Privilege Escalation & Lateral Movement

Module 28: **Linux Privilege Escalation**

- Linux Enumeration Methodology
- Weak File Permissions & Cron Jobs
- Sudo Exploitation: LD_PRELOAD
- SUID Exploitation (CVEs & Injection)
- NFS & Kernel Exploitation Basics
- Sensitive Credentials Hunting
- Sudo Shell Escape Sequences
- Sudo Exploitation: LD_LIBRARY_PATH
- Linux Capabilities Abuse

Boot-to-Root Practical Machines (Linux):

- Mr. Robot CTF
- TryHackMe Walkthroughs
- DailyBugle & Kenobi
- Game Zone & Skynet

Module 29: **Windows Privilege Architecture**

- User Account Control (UAC) & Shells File Transfer
- Windows Services & Weak Service Executable Exploitation
- Unquoted Service Path Exploitation & DLL Hijacking

- SAM (Security Account Manager) Dumping & Sensitive Credentials Hunting
- Registry Autorun Exploitation & AlwaysInstallElevated
- Impersonation Attacks (JuicyPotato, PrintSpoofer, RoguePotato)
- Universal Methodology: SeTakeOwnership Exploit
- Scheduled Task Resource Abuse & UAC Bypass Techniques
- Windows 10 Kernel Exploitation

Boot-to-Root Practical Machines (Windows):

- Steel Mountain
- HackPark (TryHackMe)
- Alfred Walkthrough
- Relevant (TryHackMe)

Module 30: [Pivoting & SSH Tunneling](#)

- SSH Local, Remote/Reverse, and Dynamic Port Forwarding (SOCKS Proxy)
- Pivoting Concepts and Real-World Scenarios

PHASE 6 Real-World Application & Automation

Module 31: [Capstone — Real-World Hunting](#)

- Picking the right bug bounty program & Reading rules of engagement
- Running the full recon-to-exploit workflow
- Writing a clean, professional bug report and avoiding rejections
- Building your own methodology over time

Module 32: [Bash Scripting for Pentesting](#)

- Variables, Loops, and Conditionals
- Networking Basics (curl, nc, ping)
- Building Directory & Subdomain Tools
- Error Handling and Debugging Scripts
- File Handling (grep, awk, sed, cut)
- Building a Port Scanner in Bash
- Parsing Output and Generating Reports

Final Milestone Achieved

By completing this roadmap, you will have mastered Linux, executed professional reconnaissance, exploited complex web vulnerabilities, utilized industry-standard tools, escalated privileges across systems, and built custom automation tools — fully preparing you for professional bug bounty programs and enterprise engagements.