Complete Cybersecurity & Ethical Hacking — Comprehensive Guide

Author: Generated by ChatGPT  
Date: Aug 14, 2025  
  
This document is a detailed, practical, and career-focused guide covering foundations, specializations, labs, projects, certifications, study plans, career advice, templates and ethics in cybersecurity and ethical hacking.

# Table of Contents

* 1. Introduction & How to Use This Guide
* 2. Foundations (Core Knowledge for All Paths)
* 3. Role-specific Tracks and Roadmaps
* 3.1 Blue Team (Defensive)
* 3.2 Red Team (Offensive)
* 3.3 Purple Team
* 3.4 Governance, Risk & Compliance (GRC)
* 3.5 Specialized Roles (Cloud, AppSec, OT, Cryptography)
* 4. Skills, Tools & Labs (By Role)
* 5. Hands-on Projects & Lab Exercises (Practical)
* 6. Certifications Map (Entry → Advanced)
* 7. Study Plans & Timelines (3/6/12 months)
* 8. Resume, Interview Prep & Job Search
* 9. Ethics, Laws & Responsible Disclosure
* 10. Templates & Playbooks (Incident report, SOC handover)
* 11. Glossary & Cheat Sheets
* 12. Resources (Books, Courses, Platforms, Communities)
* 13. Career Ladder, Salaries & Market Advice
* 14. Appendix: Quick Reference Commands & Commands by Tool

# 1. Introduction & How to Use This Guide

Purpose: This guide is designed to be a one-stop, exhaustive roadmap for learners and practitioners who want a structured path into cybersecurity and ethical hacking—from complete beginner to advanced specialist. It includes theoretical topics, practical labs, projects, certifications, career advice and templates you can reuse.

How to use this guide:

* Start at 'Foundations' if you are new — build strong networking, OS, and security fundamentals.
* Pick a specialization (Blue/Red/Purple/GRC/Specialized) after the foundation stage.
* Follow the 'Skills & Tools' and complete the 'Hands-on Projects' for practical experience.
* Use the Study Plans to structure your learning timeline.
* Use Templates & Playbooks when working in real SOCs or during mock incidents.

# 2. Foundations (Core Knowledge for All Paths)

## 2.1 Networking

* OSI vs TCP/IP model: Layers and functions.
* IPv4/IPv6 addressing, subnetting, CIDR notation.
* Routing basics: routers, switches, routing tables, default gateway.
* Common protocols: TCP, UDP, ICMP, ARP, DNS, HTTP/HTTPS, SMTP, FTP, SSH.
* Network services and ports: well-known ports and services.
* Network devices and appliances: firewalls, load balancers, IDS/IPS, proxies.

## 2.2 Operating Systems

* Windows internals: registry, event logs, services, Active Directory basics.
* Linux fundamentals: file permissions, systemd, logs (/var/log), shells, package managers.
* Command-line proficiency (bash, PowerShell).
* Process and memory concepts, basic troubleshooting.

## 2.3 Security Fundamentals

* CIA Triad: Confidentiality, Integrity, Availability.
* Authentication vs Authorization vs Accounting (AAA).
* Common attack types: phishing, malware, XSS, SQLi, RCE, MITM, brute force.
* Risk vs vulnerability vs threat concepts.
* Cryptography basics: symmetric/asymmetric, hashing, TLS/SSL, PKI.

## 2.4 Core Tools & Concepts

* Packet capture and analysis: Wireshark, tcpdump.
* Port & service scanning: Nmap.
* Vulnerability scanning: Nessus, OpenVAS.
* Web testing: Burp Suite (Proxy, Intruder, Scanner).
* SIEM basics: Splunk, ELK/Elastic Stack, QRadar.
* Version control (git), virtualization (VirtualBox, VMware), containers (Docker).

# 3. Role-specific Tracks and Roadmaps

Below are detailed learning paths and progressive skills for major cybersecurity roles. Each sub-section contains recommended skills, tools, practical exercises and suggested certifications.

## 3.1 Blue Team (Defensive Security)

Goal: Detect, monitor, and respond to security incidents and improve defensive posture.

### Core skills

* Log analysis and SIEM use (Splunk, Elastic, QRadar).
* Network monitoring and traffic analysis.
* Endpoint detection & response (EDR) tools (CrowdStrike, Carbon Black).
* Incident response methodology and playbook creation.
* Digital forensics (disk and memory forensics).
* Threat intelligence and MITRE ATT&CK mapping.

### Typical roles & progression

* SOC Analyst Tier 1 → Tier 2 → Tier 3
* Incident Responder
* Threat Hunter
* Forensic Analyst
* Security Engineer (defensive tooling & detection engineering)

### Hands-on exercises

* Set up a SIEM with sample logs and write correlation rules.
* Analyze a suspicious pcap with Wireshark and produce findings.
* Perform a host memory capture and analyze with Volatility.
* Run EDR alerts in a controlled lab and create detection signatures.

### Certifications (recommended)

* CompTIA Security+,
* Splunk Core Certified User/Power User,
* GIAC GCIH (Incident Handler),
* GIAC GCIA/GCFA (Intrusion Analyst/Forensics),
* Microsoft SC-200 (Security Operations).

## 3.2 Red Team (Offensive Security)

Goal: Simulate realistic attacker behavior to find and exploit vulnerabilities to improve defenses.

### Core skills

* Penetration testing methodologies (PTES, OWASP testing guide).
* Exploitation frameworks (Metasploit, Cobalt Strike).
* Web application hacking: SQLi, XSS, CSRF, RCE.
* Network exploitation and pivoting techniques.
* Post-exploitation persistence and evasion.
* Scripting and automation: Python, Bash, PowerShell.

### Typical roles & progression

* Junior Penetration Tester → Senior Pentester
* Red Team Operator
* Exploit Developer
* Adversary Simulation Engineer

### Hands-on exercises

* Complete a full web app pentest on a deliberately vulnerable VM (DVWA, Juice Shop).
* Practice buffer overflow basics in a controlled lab.
* Set up and use Metasploit for exploitation and post-exploitation activities.
* Perform internal network pivoting in a multi-host lab.

### Certifications (recommended)

* eJPT (entry),
* OSCP (Practical penetration testing),
* CRTO/CRTP (Red Team operator),
* OSCE/OSED (advanced exploit development).

## 3.3 Purple Team

Goal: Facilitate collaboration between offensive and defensive teams to validate detections and improve defenses.

* Understand attack techniques and map them to existing detections.
* Design iterative red/blue exercises.
* Use frameworks: MITRE ATT&CK, Caldera, Atomic Red Team.
* Build detection engineering pipelines and improvement loops.

Certifications and exercises:

* Practical exercises using Atomic Red Team to validate SIEM rules.
* Workshops combining pentesting tasks with detection tuning.

## 3.4 Governance, Risk & Compliance (GRC)

Goal: Ensure that organizational security meets regulatory and business requirements.

* Frameworks: ISO 27001, NIST CSF, COBIT.
* Risk management methodologies and assessments.
* Policy creation, audits, compliance (PCI-DSS, GDPR, HIPAA).
* Security awareness and training programs.

### Certifications (recommended)

* CISM, CRISC, CISSP (broad),
* ISO 27001 Lead Implementer/Auditor.

## 3.5 Specialized Roles (Cloud, AppSec, OT, Cryptography)

Each of these areas requires domain knowledge plus security skills.

* Cloud Security Engineer: AWS/Azure/GCP security, IAM, cloud networking, CASB, cloud-native monitoring.
* Application Security Engineer: secure SDLC, SAST/DAST, code review, threat modeling.
* OT/ICS Security Specialist: SCADA protocols, ICS safety considerations, air-gapped network strategies.
* Cryptographer: maths, protocols, crypto implementations, side-channel considerations.

# 4. Skills, Tools & Labs (By Role)

## Common Tools (full list)

* Network: Wireshark, tcpdump, Nmap, Zeek (Bro)
* Pentest: Metasploit, Burp Suite, sqlmap, Hydra, Nikto
* Forensics: Autopsy, Sleuth Kit, Volatility, FTK Imager
* SIEM & Logging: Splunk, Elastic Stack, QRadar, Graylog
* EDR: CrowdStrike, Microsoft Defender for Endpoint, Carbon Black
* Malware Analysis: Ghidra, IDA, x64dbg, Cuckoo Sandbox
* Cloud: AWS CLI, Azure CLI, cloud security posture tools (ScoutSuite)
* DevSecOps: Jenkins, GitHub Actions, SAST tools (SonarQube)

## Setting up labs

* Local VMs: Use VirtualBox/VMware to create isolated networks.
* Use intentionally vulnerable VMs: Metasploitable, OWASP Juice Shop, DVWA.
* Online labs: TryHackMe, HackTheBox, RangeForce, Offensive Labs.
* Blue team labs: Security Onion, Elastic SIEM with Beats, Splunk sandbox.
* Version control and documentation: Use git to track lab work.

# 5. Hands-on Projects & Lab Exercises (Practical)

## Beginner projects

* Build a home lab: 2 VMs (Windows Server + Linux), a small web app, and a vulnerable app to test.
* Packet capture exercise: Capture DNS and HTTP traffic and explain it.
* Simple web pentest: Find an XSS or SQLi in a DVWA instance and report it.

## Intermediate projects

* Full internal network compromise lab: exploit a workstation, escalate privileges, and pivot.
* Set up a SIEM ingestion pipeline (Filebeat → Elasticsearch → Kibana) and create dashboards.
* Create an incident response runbook and run a tabletop with friends/peers.

## Advanced projects

* Develop custom detection rules (Sigma) and test them with simulated attacks.
* Reverse engineer a sample malware in a sandbox and document its behavior.
* Design and execute a purple-team engagement: red team sim + detection validation.

# 6. Certifications Map (Entry → Advanced)

Entry-level:

* CompTIA Network+ (network basics)
* CompTIA Security+ (security fundamentals)
* eJPT (basic pentesting)

Mid-level:

* OSCP (practical pentesting)
* Splunk Core Certified Power User
* GCIH (GIAC Incident Handler)

Advanced / Specialized:

* OSCE, OSED, CRTO, CRTP (offensive advanced)
* GCFA, GCIA, GREM (forensics, intrusion analysis, malware)
* CISSP, CISM, CRISC (management & governance)

# 7. Study Plans & Timelines (3/6/12 months)

## 3-Month Plan (fast track basics)

* Month 1: Networking + Linux + Windows basics. Start Security+ material.
* Month 2: Basic pentesting tools (Nmap, Burp), simple labs (TryHackMe beginner paths).
* Month 3: Complete Security+ or eJPT, build a small portfolio of lab reports.

## 6-Month Plan (entry-level SOC or pentest)

* Months 1–2: Foundations (networking, OS, scripting with Python).
* Months 3–4: Role training (choose Blue or Red), practical labs (SIEM or DVWA).
* Months 5–6: Certification (Security+/eJPT) and 3 projects uploaded to portfolio.

## 12-Month Plan (specialize + job readiness)

* Months 1–4: Deep foundations + scripting + Git.
* Months 5–8: Specialization coursework + hands-on projects + mentorship.
* Months 9–12: Advanced certifications (OSCP, GCIH), build resume, apply for jobs.

# 8. Resume, Interview Prep & Job Search

## Resume tips

* Focus on measurable outcomes (eg. 'Reduced incident response time by X' — if true).
* List projects and labs with short descriptions and links to write-ups.
* Include tools and technologies used (SIEM, EDR, Burp, etc.).
* Keep it one page for junior roles; 1–2 pages for mid-level.

## Interview prep

* Know the fundamentals: TCP/IP, common protocols, basic Linux/Windows commands.
* Be ready to explain past lab projects step-by-step.
* Prepare for scenario questions (eg. 'How would you respond to X alert?').
* Practice whiteboard explanations and command-line demos.

## Job search strategies

* Contribute write-ups to GitHub/GitLab or a personal blog.
* Network at local security meetups and conferences.
* Apply for internships and entry-level SOC roles to get experience.

# 9. Ethics, Laws & Responsible Disclosure

Ethics are central to cybersecurity. Always follow legal and ethical boundaries:

* Never test systems without explicit permission (written authorization).
* Understand local laws: unauthorized access can be a criminal offense.
* Responsible disclosure: report vulnerabilities to the owner following a clear timeline; use bug bounty programs when available.
* Follow company policies and code of conduct.

# 10. Templates & Playbooks

## Incident Report Template

Use this template for documenting incidents:

* Incident ID:
* Date/Time detected:
* Detected by (tool/person):
* Description:
* Indicators of Compromise (IOCs):
* Scope/Impact:
* Actions taken:
* Root cause:
* Remediation steps:
* Lessons learned & recommendations:

## SOC Handover / Shift Notes

* Current open incidents and status.
* Alerts escalated during shift (with timestamps).
* Pending investigations and next steps.
* Known maintenance windows or false-positive sources.

# 11. Glossary & Cheat Sheets

A short glossary of commonly used terms:

* IOC — Indicator of Compromise
* TTP — Tactics, Techniques, and Procedures
* EDR — Endpoint Detection and Response
* SIEM — Security Information and Event Management
* XSS — Cross-Site Scripting
* SQLi — SQL Injection

## Quick cheat sheet: Useful commands

* Linux: ps aux | grep <process>, netstat -tulpn, ss -tulpn, tail -f /var/log/syslog
* Windows (PowerShell): Get-Process, Get-Service, Get-EventLog -LogName System
* Nmap: nmap -sC -sV -oA output <target>
* Tcpdump: tcpdump -i eth0 -w capture.pcap host 1.2.3.4

# 12. Resources (Books, Courses, Platforms, Communities)

Books: (classic recommendations)

* 'The Web Application Hacker's Handbook' — for appsec
* 'Practical Malware Analysis' — for malware reverse engineering
* 'Hacking: The Art of Exploitation' — for exploitation fundamentals
* 'Incident Response & Computer Forensics' — for forensics practitioners

Online learning platforms and labs:

* TryHackMe, HackTheBox, Offensive Security labs, RangeForce, SANS training
* YouTube channels and community blogs for up-to-date tutorials

Communities:

* Local OWASP chapters, security meetups, Discord/Slack groups, Twitter/X and Mastodon security researchers

# 13. Career Ladder, Salaries & Market Advice

Career progression typically moves from junior hands-on roles into senior and then management/specialist positions. Examples:

* SOC Analyst (junior) → Senior SOC Analyst / Incident Responder → Detection Engineer → Head of SOC
* Penetration Tester → Senior Pentester → Red Team Lead / Offensive Security Architect
* GRC Analyst → Risk Manager → Chief Information Security Officer (CISO)

Salary note: Salaries vary by country, experience, and company. Focus on building demonstrable skills and projects to negotiate offers.

# 14. Appendix: Quick Reference Commands & Tool Examples

Sample commands and quick examples:

* Wireshark: Use display filters such as http.request.method == "POST" or ip.addr == 1.2.3.4
* Sqlmap: sqlmap -u "http://target/vuln.php?id=1" --dbs
* Metasploit: use exploit/multi/handler ; set payload windows/meterpreter/reverse\_tcp ; exploit
* Splunk: search index=main sourcetype=wineventlog | stats count by EventCode