Making a Career in Ethical Hacking

Skills, roadmap and what it actually takes to get started.

AUTHOR	Babashaheer
VERSION	1.0
DATE	April 2026
SERIES	Cybersecurity Career Series — Document 01 of 06
AUDIENCE	Students and beginners considering a career in cybersecurity

Contents

Baba Shaheer Gutappa
Digitally signed by Baba Shaheer Gutappa
Date: 2026.04.14 13:01:44 +01'00'

1. What Is Ethical Hacking — and Is It a Real Job?

Yes — ethical hacking is a real, well-paid and in-demand profession. The title sounds unusual, but the idea is simple. Companies and governments hire people to try to break into their own systems — before the bad guys do. If you can find the weakness first and report it, it can be fixed. If nobody finds it, a real attacker will eventually.

The formal job titles vary: Penetration Tester, Security Analyst, Red Team Engineer, Vulnerability Researcher, Security Consultant. What they all share is the same core activity — thinking like an attacker to help defenders.

> **Ethical hacking is not just 'hacking but legal'.**
> It is a structured, professional discipline with defined methodology, legal agreements, detailed reporting and real business accountability.

Is the demand real?

The global cybersecurity skills gap is well documented. As of 2023, there were approximately 3.5 million unfilled cybersecurity positions worldwide (ISC2, 2023). The UK Government's Cyber Security Skills in the UK Labour Market report (DSIT, 2024) found that around half of UK businesses have a basic cybersecurity skills gap. Penetration testers and security analysts are consistently in the top five most requested cybersecurity roles.

Salaries reflect the demand. In the UK, a junior penetration tester earns between £30,000–£45,000. At mid-level, £50,000–£75,000 is common. Senior testers and consultants frequently earn over £80,000, and independent contractors can charge £500–£1,000 per day (CW Jobs Salary Survey, 2024).

Level	Typical UK Salary	Typical Experience
Junior / Graduate	£30,000 – £45,000	0–2 years, entry cert (CEH, CompTIA)
Mid-level	£50,000 – £75,000	2–5 years, OSCP or CREST CRT
Senior / Lead	£75,000 – £95,000+	5+ years, CREST CCT, specialist areas
Independent Contractor	£400 – £1,000/day	3+ years, strong portfolio

Table 1: Typical UK salary ranges for ethical hacking roles (CW Jobs, 2024)

2. The Cybersecurity Tree — Where Ethical Hacking Sits

Cybersecurity is a broad field. Think of it as a tree with a single trunk — the discipline of keeping systems and data safe — and many branches growing from it. Ethical hacking is one of those branches. It is important to understand this early on, because it helps you decide which branch suits you best and plan your learning accordingly.

This document series covers each major branch separately. For now, here is a map of the landscape so you know where ethical hacking sits relative to everything else:

Branch	What It Involves	Who Suits It
Ethical Hacking / Penetration Testing	Simulating attacks to find vulnerabilities before real attackers do. Active, offensive mindset.	People who enjoy problem-solving, thinking outside the box and technical challenge.
Digital Forensics	Investigating incidents after they happen. Recovering deleted files, tracing attackers, preserving evidence for court.	Detail-oriented people who enjoy investigation and methodical analysis.
Malware Analysis	Reverse-engineering malicious software to understand how it works and how to stop it.	People with strong programming skills and patience for deep technical analysis.
Network Security	Designing, monitoring and defending network infrastructure. Firewalls, IDS/IPS, SIEM.	People who enjoy networking fundamentals and operational security.
Application Security (AppSec)	Securing software during development. Code reviews, threat modelling, SAST/DAST tooling.	Developers who want to specialise in security and understand secure coding.
Cloud Security	Securing cloud infrastructure (AWS, Azure, GCP). Misconfiguration audits, IAM, serverless.	People already working with cloud platforms who want to add a security specialism.
Security Operations (SOC / Blue Team)	24/7 monitoring of systems for active threats. Alert triage, incident response, threat hunting.	People who enjoy working under pressure, real-time analysis and clear processes.
GRC (Governance, Risk & Compliance)	Policies, frameworks, audits, risk assessments. ISO 27001, GDPR, NIST, Cyber Essentials.	People with strong written communication who prefer strategy and policy over technical hands-on work.

Table 2: Major branches of cybersecurity. Each will be covered in a separate document in this series.

This document focuses entirely on Ethical Hacking and Penetration Testing.
Each other branch has its own dedicated document in this series.
Start with ethical hacking if the offensive, hands-on side of security appeals to you.

3. What an Ethical Hacker Actually Does Day to Day

People often imagine ethical hackers sitting in dark rooms running scripts continuously until something breaks. The reality is considerably more structured — and involves a lot more writing than most people expect.

Activity	Time Split (approx.)	Details
Reconnaissance and planning	15–20%	Understanding the target, reviewing scope documentation, planning the test approach. This is done before touching any system.
Active testing	30–40%	Running scans, exploiting vulnerabilities, chaining weaknesses together. The hands-on technical work people picture.
Documentation and notes	20–25%	Recording every step, every finding, every tool command and every screenshot as you go. This is essential — you cannot write a report from memory.
Report writing	20–25%	Translating technical findings into clear written reports for two audiences — management (executive summary) and the technical team (detailed findings with remediation steps).
Research and tool updates	5–10%	Keeping up with new CVEs, new tools, new techniques and changes to the threat landscape. This never stops.

Table 3: Typical time split during a penetration testing engagement

One thing new entrants consistently underestimate is how much writing is involved. A penetration test with no report is worthless — the client paid to understand their risks, not to watch someone run Metasploit. The ability to explain a complex technical finding in plain English is one of the most valued skills in the industry.

A penetration tester who cannot write clearly will not progress far.
Practise writing technical explanations for non-technical audiences.
Every lab you do — write it up as if you were reporting it to a client.

4. The Core Skills You Need to Build

Ethical hacking draws on a wide range of technical disciplines. You do not need to be an expert in all of them before you start — nobody is. But you do need a solid foundation in each area, and you need to keep building on it throughout your career. Below are the core skill areas, what each involves and why it matters.

4.1 Networking Fundamentals

This is the single most important foundational skill. Almost every attack and every defence involves a network in some way. If you do not understand how data moves, you cannot understand how to intercept, manipulate or exploit it.

- The TCP/IP model — how packets are structured and how they travel from source to destination
- IP addressing, subnetting and CIDR notation — understanding network ranges like 192.168.1.0/24
- Common protocols: HTTP/S, DNS, DHCP, FTP, SSH, SMTP, SMB, RDP — what each does and which ports it uses
- How DNS works — name resolution, zone transfers, DNS enumeration
- Firewalls, NAT, VPNs and proxies — how traffic is filtered and redirected
- Packet capture and analysis using Wireshark — being able to read raw network traffic
- The OSI model — how each layer relates to security vulnerabilities

Resources: CompTIA Network+ covers all of this. Professor Messer's free N+ course is a solid starting point. Supplement with Cisco Packet Tracer for hands-on practice (Messer, 2024).

4.2 Operating Systems — Linux and Windows

Most penetration testing is done from a Linux environment (Kali Linux is the standard). But most targets run Windows. You need to be comfortable in both.

Linux Skills	Windows Skills
Command line navigation — moving files, reading logs, running scripts	Active Directory structure — domains, forests, users, groups, GPOs
File permissions — reading and modifying chmod/chown	The Windows registry — where configuration and credentials are stored
Bash scripting — automating repetitive tasks	PowerShell — essential for post-exploitation and automation
Service management — starting, stopping, configuring services	Windows Event Logs — understanding what gets recorded and where
Networking tools — netstat, ss, ip, curl, wget	SMB — how file sharing works and how it is commonly exploited
Package management — apt, pip, installing tools from source	Credential storage — SAM database, NTLM hashes, credential caching

Table 4: Linux and Windows skills for ethical hackers

4.3 Programming and Scripting

You do not need to be a software developer. But you do need to be able to read code, write basic scripts and understand what a piece of code is doing when you encounter it during a test. The most useful languages for ethical hacking are:

Language	Why It Matters for Ethical Hacking	Priority
Python	The go-to scripting language for the industry. Used for writing custom exploits, automation scripts, network tools, parsers and almost everything else. Most public PoC exploit code is Python.	Essential
Bash	The default shell on Linux. You will write Bash scripts to automate scanning, post-exploitation tasks and report generation. Even basic Bash skills save enormous amounts of time.	Essential
PowerShell	Microsoft's scripting language. Critical for Windows post-exploitation — running commands on compromised systems without triggering antivirus, extracting credentials, lateral movement.	Very important
JavaScript	Understanding JS is needed for web application testing — identifying XSS, understanding how client-side logic works and writing proof-of-concept payloads.	Important
SQL	SQL injection is still one of the most common web vulnerabilities. You need to understand how SQL works to write injection payloads and extract data.	Important
C / C++	Useful for understanding buffer overflows and low-level memory exploitation. Not essential to start with, but valuable for more advanced roles.	Intermediate+

Table 5: Programming languages relevant to ethical hacking

4.4 Web Application Security

Web applications are one of the most common attack surfaces in any organisation. Understanding how websites work — at both the HTTP protocol level and the application code level — is fundamental. The OWASP Top 10 is the standard reference for web application vulnerabilities (OWASP Foundation, 2021). Every ethical hacker should know all ten inside out:

- Broken Access Control — accessing data or functionality you should not have permission to reach
- Cryptographic Failures — sensitive data transmitted or stored without proper encryption
- Injection — SQL, command and LDAP injection attacks that manipulate backend systems
- Insecure Design — fundamental flaws in how an application is architected
- Security Misconfiguration — default credentials, unnecessary features left enabled, verbose error messages
- Vulnerable and Outdated Components — third-party libraries and frameworks with known CVEs
- Authentication Failures — weak passwords, missing multi-factor authentication, session management flaws
- Software and Data Integrity Failures — untrusted update mechanisms, insecure deserialisation

- Security Logging and Monitoring Failures — insufficient logging to detect or investigate attacks
- Server-Side Request Forgery (SSRF) — forcing a server to make requests on behalf of an attacker

> **Practical resource: PortSwigger Web Security Academy (portswigger.net/web-security)**
> is free, structured and the best web hacking learning resource available.
> Work through all labs — it is what professionals actually use to learn.

5. The Learning Roadmap — Where to Start

The biggest mistake people make when getting into ethical hacking is jumping straight into hacking tools without building the foundations first. Tools change. Techniques evolve. But if you understand the underlying technology, you will always be able to adapt. Follow this roadmap in order — it is tempting to skip stages, but the earlier stages make the later ones considerably easier.

1. **Build your networking foundation**
   Study TCP/IP, DNS, HTTP, subnetting and how packets flow. Complete CompTIA Network+ or equivalent. Use Cisco Packet Tracer or GNS3 to practice. This should take 4–8 weeks of focused study.

2. **Get comfortable with Linux**
   Set up Kali Linux in VirtualBox or VMware. Learn the command line — file navigation, permissions, processes, networking tools. Complete OverTheWire Bandit challenges (free, beginner Linux wargame). Aim for 4–6 weeks.

3. **Understand Windows internals**
   Set up a Windows Server VM. Learn Active Directory basics, PowerShell, the registry and Windows Event Logs. TryHackMe's Windows Fundamentals path is excellent for this. Allow 3–4 weeks.

4. **Learn basic scripting**
   Start with Python. Work through a beginner Python course, then write simple networking scripts — port scanners, banner grabbers, basic automation. Automate Something You Do Manually is good practice. 2–4 weeks.

5. **Work through structured hacking labs**
   TryHackMe beginner path, then Hack The Box Starting Point. These guided environments let you practice real attack techniques safely and legally. Start here for practical skills. Ongoing — never stop.

6. **Study the CEH or CompTIA Security+ curriculum**
   These certifications structure your theoretical knowledge across all hacking domains. Even if you sit the exam later, studying the curriculum fills in gaps. 6–8 weeks of structured study.

7. **Get your first certification**
   CompTIA Security+ for broad foundation, or CEH for hacking-specific knowledge. Then aim for OSCP when you have 6–12 months of practical lab time. OSCP is the gold standard for junior–mid roles.

8. **Build a portfolio and start applying**
   Document your TryHackMe and HTB progress. Write up walkthroughs. Create a GitHub with your scripts. Contribute to bug bounty programmes via HackerOne or Bugcrowd. This is your CV evidence.

Realistic timelines:

Starting from zero, entry-level ready: 12–18 months of consistent self-study.

Bootcamp / structured programme: 6–9 months with daily commitment.

Degree route: 3 years, but you can work part of the roadmap above in parallel.

6. Certifications That Actually Matter

Certifications in cybersecurity are worth having — but only the right ones. Some certifications are respected industry-wide and genuinely demonstrate capability. Others are expensive, widely recognised by name but less meaningful in practice. Below is an honest breakdown of the certifications that will actually help you get hired.

Certification	Level	Focus	Why It Matters
CompTIA Security+	Beginner	Broad security foundations — threats, cryptography, networking, compliance	Widely accepted as a baseline. Required by many government and defence roles. Good first cert.
CompTIA PenTest+	Beginner–Mid	Penetration testing methodology, planning, scoping and reporting	Good theoretical grounding in pentest process. Less hands-on than OSCP but a credible start.
CEH (Certified Ethical Hacker)	Beginner–Mid	Ethical hacking concepts, tools and methodology across all domains	Strong employer recognition, especially in consulting and corporate roles. Good curriculum even if you study without sitting the exam.
eJPT (eLearnSecurity Junior PenTester)	Beginner	Practical network and web penetration testing	Highly practical, affordable, and increasingly respected. Excellent first hands-on cert.
OSCP (Offensive Security Certified Professional)	Intermediate	Real-world exploitation — 24-hour hands-on exam on live machines	The most respected practical pentest certification. Required or strongly preferred by most serious pentest firms. Work towards this after 6–12 months of lab experience.
CREST CRT / CCT	Intermediate–Senior	UK industry standard for commercial penetration testing	Essential for working with UK government, financial services and large corporates. CREST-accredited firms need CREST-certified testers.
GPEN (GIAC Penetration Tester)	Intermediate	Comprehensive pentest techniques — network, exploitation, post-exploitation	Respected globally, especially in the US. Expensive but thorough.

Table 6: Certifications for ethical hackers, ordered roughly by progression

A sensible certification path

- **Start here:** CompTIA Security+ or eJPT — whichever suits your learning style (theory vs practical)
- **Then:** CEH — to structure your hacking knowledge across all domains
- **Goal:** OSCP — once you have a year of hands-on lab practice behind you. This is the certification that opens doors to most pentest firms
- **UK-specific goal:** CREST CRT — if you want to work on UK commercial engagements
- **Keep studying regardless:** TryHackMe and Hack The Box paths matter as much as paper certifications

Expensive certifications are not always the most valued.
OSCP is significantly cheaper than many enterprise certs and far more respected by hiring managers at penetration testing firms.

7. Tools Every Ethical Hacker Should Know

Kali Linux comes with hundreds of tools pre-installed. You do not need to know all of them. What matters is understanding a core set deeply — knowing what they do, why you would use them, what the output means, and how to interpret the results. Tools you have used once in a tutorial are not tools you know.

Tool	Category	What It Does	Priority
Nmap	Reconnaissance	Network scanner. Discovers hosts, open ports, running services and OS versions. Fundamental — used on almost every engagement.	Essential
Burp Suite	Web Testing	HTTP proxy that intercepts and modifies web traffic. Includes scanner, repeater, intruder and decoder modules. Industry standard for web application testing.	Essential
Metasploit	Exploitation	Framework containing hundreds of exploits, payloads and auxiliary modules. Automates exploitation of known vulnerabilities. Critical to understand, not just run.	Essential
Wireshark	Network Analysis	Packet capture and analysis tool. Read raw network traffic, analyse protocols, identify credentials sent in clear text.	Essential
John the Ripper / Hashcat	Password Cracking	Offline password hash cracking using wordlists and rule-based attacks. John for general use, Hashcat for GPU-accelerated cracking.	Essential
Gobuster / ffuf	Web Enumeration	Directory and file brute-forcing on web servers. Discovers hidden paths, admin panels and unlinked content.	Important
Nikto	Web Scanning	Web server vulnerability scanner. Checks for outdated software, misconfigurations and common vulnerabilities quickly.	Important
SQLmap	SQL Injection	Automated SQL injection detection and exploitation. Useful for verifying SQLi vulnerabilities and extracting database content.	Important
Netcat	Networking	The 'Swiss army knife' of networking. Used for port scanning, banner grabbing, file transfer and setting up reverse shells.	Important
Bloodhound	Active Directory	Maps Active Directory relationships visually. Identifies attack paths to Domain Admin through misconfigured permissions and group memberships.	Intermediate+
Mimikatz	Credential Harvesting	Extracts credentials, hashes and Kerberos tickets from Windows memory. The most important post-exploitation credential tool for Windows environments.	Intermediate+
Nessus / OpenVAS	Vulnerability Scanning	Automated vulnerability scanners. Nessus is commercial (free for home use), OpenVAS is open source. Used in the vulnerability analysis phase.	Important

Table 7: Core tools for ethical hackers. 'Essential' tools should be understood deeply before starting any professional engagement.

> **The best way to learn tools is to use them in labs, not to read about them.**
> TryHackMe and Hack The Box provide safe, legal environments to practice all of these tools on purpose-built vulnerable machines. That is where real skill develops.

8. Breaking In — Getting Your First Role

Breaking into the cybersecurity industry is genuinely achievable without a traditional computer science degree — but it requires deliberate effort, visible evidence of skill, and patience. The good news is that hiring managers in cybersecurity are generally more interested in what you can do than where you went to university.

Build something visible

The most important thing you can do before applying for roles is create evidence of what you can do. A strong portfolio consistently outperforms a generic CV in this industry:

- **TryHackMe profile:** Complete the Beginner and Jr Penetration Tester paths. Your public profile shows your rank, completed rooms and skills — link it in your CV
- **Hack The Box profile:** Progress through Starting Point and Easy-difficulty machines. Write-ups are shared publicly once machines retire — publishing yours shows you can explain technical work clearly
- **GitHub:** Put your scripts, custom tools and notes here. Even small Python tools that solve a specific problem show initiative
- **Blog or write-ups:** Writing about what you have learned — even explaining basic concepts simply — demonstrates communication skills that employers value
- **Bug bounty:** Finding and responsibly disclosing a real vulnerability — however small — on a bug bounty programme carries significant weight on a CV
- **CTF competitions:** Capture the Flag competitions (picoCTF, HackTheBox CTF, SANS Holiday Hack) are team-based challenges where you demonstrate practical skills publicly

Where to look for roles

Junior penetration tester roles, security analyst positions and graduate schemes are the typical entry points. CREST-accredited firms, MSSP (Managed Security Service Providers) and the public sector all hire regularly at junior level.

Where to Look	Notes
CyberSecurityJobs.com	UK-focused job board dedicated to cybersecurity roles
LinkedIn	Most firms post here; recruiters actively source candidates from here
Indeed / CW Jobs	Good for volume; filter by 'junior', 'graduate', 'entry level'
CREST website	Lists accredited companies — apply directly to firms you want to work for
Government GCHQ / NCSC schemes	NCSC Graduate Programme and apprenticeship schemes — competitive but excellent
CTF team networking	Many first roles come from meeting people at competitions or on Discord servers
Bug bounty platforms	HackerOne and Bugcrowd list responsible disclosure programmes; some lead to job offers

Table 8: Where to find junior ethical hacking and security roles

What to expect in interviews

Technical interviews for junior pentest roles typically cover a mix of conceptual questions and practical tasks. Common topics include:

- Explain the TCP three-way handshake — why does it exist and what does a tester look for in it?
- What is the difference between a vulnerability assessment and a penetration test?
- Walk me through how you would approach a black box web application test from scratch
- What is SQL injection and how would you test for it manually?
- You run Nmap on a target and see port 445 open. What does that tell you and what do you do next?
- What is a reverse shell? How does it differ from a bind shell?
- How would you escalate privileges on a Linux system after gaining low-privilege access?
- Tell me about a box you have completed on TryHackMe or HTB. Walk me through your methodology.

> **The most important thing you can say in an interview:**
> "I have been practising on TryHackMe / Hack The Box. Here is my profile."
> Practical evidence beats academic knowledge every time in this industry.

9. References

1. CW Jobs (2024) *Technology Salary Survey 2024.* Available at: https://www.cwjobs.co.uk/salary-checker [Accessed: 10 April 2026].
2. DSIT (2024) *Cyber Security Skills in the UK Labour Market 2024.* Department for Science, Innovation and Technology. Available at: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024 [Accessed: 10 April 2026].
3. EC-Council (2023) *Certified Ethical Hacker (CEH) v13.* Available at: https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/ [Accessed: 11 April 2026].
4. Hack The Box (2024) *HTB Academy — Penetration Tester Path.* Available at: https://academy.hackthebox.com [Accessed: 11 April 2026].
5. ISC2 (2023) *Cybersecurity Workforce Study 2023.* Available at: https://www.isc2.org/Research/Workforce-Study [Accessed: 11 April 2026].
6. Messer, J. (2024) *Professor Messer's CompTIA Network+ Course.* Available at: https://www.professormesser.com/network-plus/n10-009/n10-009-video/n10-009-training-course/ [Accessed: 12 April 2026].
7. Offensive Security (2024) *PWK Course and OSCP Certification.* Available at: https://www.offensive-security.com/pwk-oscp/ [Accessed: 12 April 2026].
8. OWASP Foundation (2021) *OWASP Top Ten 2021.* Available at: https://owasp.org/Top10/ [Accessed: 12 April 2026].
9. PortSwigger (2024) *Web Security Academy — Free Online Web Security Training.* Available at: https://portswigger.net/web-security [Accessed: 13 April 2026].
10. TryHackMe (2024) *Learning Paths — Jr Penetration Tester.* Available at: https://tryhackme.com/paths [Accessed: 13 April 2026].
11. CREST (2024) *Certified Penetration Testing Certifications.* Available at: https://www.crest-approved.org/examination/crest-registered-tester/ [Accessed: 14 April 2026].

Document prepared by **Babashaheer**. Version 1.0 — April 2026. Cybersecurity Career Series — Document 01 of 06. This document is for educational purposes.