100 Days of Blue Team Cybersecurity Challenge: Roadmap for Upskilling

Introduction

This roadmap is designed to help you build practical skills in blue team operations, focusing on defensive cybersecurity such as monitoring threats, responding to incidents, analyzing forensics, and hardening systems against attacks. It is structured for beginners with some basic IT knowledge, assuming 2-4 hours of daily commitment. Each phase builds on the previous one, incorporating theory, hands-on labs, and reviews. Resources include free platforms like TryHackMe (THM), Hack The Box (HTB), CyberDefenders, YouTube channels (e.g., NetworkChuck, John Hammond), and official docs (e.g., NIST, MITRE ATT&CK). Use tools like VirtualBox for VMs, Wireshark for packet analysis, and free trials of SIEMs (e.g., Splunk or ELK Stack). Track progress in a journal, and join communities like Reddit's r/blueteam or Discord groups for support.

1 Phase 1: Foundations (Days 1-25)

Build core IT and security knowledge to understand defensive postures. Focus on operating systems, networking, and basic threats.

1.1 Days 1-5: IT Basics and Operating Systems

- **Day 1:** Introduction to blue team roles (SOC analyst, incident responder). Read NIST SP 800-61 (Incident Handling Guide).
- **Day 2:** Windows basics (commands, registry, services). Practice in a VM.
- **Day 3:** Linux basics (commands, file systems, permissions). Use Ubuntu VM.
- **Day 4:** Virtualization setup (install VirtualBox, create Windows/Linux VMs).
- **Day 5:** Review and quiz yourself on OS differences. Resource: Professor Messer's free videos on CompTIA A+.

1.2 Days 6-10: Networking Fundamentals

- **Day 6:** OSI/TCP-IP models, IP addressing, subnets.

- **Day 7:** Common protocols (HTTP, DNS, SMTP). Use Wireshark to capture traffic.
- **Day 8:** Network devices (routers, switches, firewalls). Simulate with Packet Tracer (free from Cisco).
- **Day 9:** Basic network security (ports, firewalls). Configure Windows Firewall.
- **Day 10:** Review with THM's "Networking Fundamentals" room.

1.3 Days 11-15: Cybersecurity Basics

- **Day 11:** CIA triad, threats, vulnerabilities, risks.
- **Day 12:** Common attack types (phishing, malware, DDoS). Study MITRE ATT&CK framework intro.
- **Day 13:** Access controls (RBAC, least privilege). Practice on Linux.
- **Day 14:** Encryption basics (symmetric/asymmetric, HTTPS).
- **Day 15:** Compliance intro (GDPR, HIPAA). Resource: Cybrary's free cybersecurity fundamentals course.

1.4 Days 16-20: Blue Team Intro and Log Analysis

- **Day 16:** Blue vs. Red vs. Purple teams. Read about SOC operations.
- **Day 17:** Logging basics (syslog, event logs). Enable logging on your VMs.
- **Day 18:** Parse logs manually (use grep on Linux, Event Viewer on Windows).
- **Day 19:** Intro to threat intelligence (sources like VirusTotal).
- **Day 20:** Weekly review: Set up a simple home lab network.

1.5 Days 21-25: Hands-On Practice and Review

- **Days 21-24:** Complete THM's "Blue Team Fundamentals" path (labs on monitoring and basics).
- **Day 25:** Phase review: Write a summary of key concepts; self-assess gaps.

2 Phase 2: Defensive Tools and Monitoring (Days 26-50)

Learn to use tools for detection and monitoring, core to blue team ops like SIEM and IDS.

2.1 Days 26-30: Intrusion Detection and Prevention

- **Day 26:** IDS/IPS basics (Snort, Suricata). Install Snort on Linux VM.
- **Day 27:** Signature vs. anomaly detection. Write simple rules.

- **Day 28:** Network monitoring with Zeek (formerly Bro).
- **Day 29:** Firewall configs (pfSense or iptables). Simulate attacks (e.g., port scans).
- **Day 30:** Review with HTB's intro labs on network defense.

2.2 Days 31-35: SIEM and Log Management

- **Day 31:** SIEM intro (Splunk, ELK Stack). Install ELK on VM.
- **Day 32:** Ingest logs into SIEM (forward Windows/Linux logs).
- **Day 33:** Querying and dashboards (Kibana or Splunk searches).
- **Day 34:** Alerting setup for suspicious activity.
- **Day 35:** Resource: Free Splunk tutorials; practice on sample datasets.

2.3 Days 36-40: Endpoint Security

- **Day 36:** EDR basics (CrowdStrike, Microsoft Defender). Use free alternatives like OSSEC.
- **Day 37:** Antivirus and anti-malware (install ClamAV).
- **Day 38:** Endpoint hardening (group policies, AppLocker).
- **Day 39:** Vulnerability scanning (OpenVAS or Nessus Community).
- **Day 40:** Simulate malware detection in your lab.

2.4 Days 41-45: Cloud Security Basics

- **Day 41:** Cloud intro (AWS, Azure security). Sign up for free tiers.
- **Day 42:** IAM and access management.
- **Day 43:** Monitoring cloud logs (CloudTrail, Azure Monitor).
- **Day 44:** Common cloud threats and defenses.
- **Day 45:** THM's "Cloud Security" room (focus on defense).

2.5 Days 46-50: Integration and Review

- **Days 46-49:** Build a mini-SOC: Integrate tools (e.g., ELK + Snort) and monitor simulated traffic.
- **Day 50:** Phase review: Run a vulnerability scan on your lab; document findings.

3 Phase 3: Incident Response and Forensics (Days 51-75)

Develop skills for responding to breaches, a key blue team function.

3.1 Days 51-55: Incident Response Fundamentals

- **Day 51:** IR lifecycle (NIST model: Preparation, Detection, Analysis, Containment, Eradication, Recovery).
- **Day 52:** Triage and prioritization.
- **Day 53:** Documentation and reporting.
- **Day 54:** Playbooks creation (e.g., for ransomware).
- **Day 55:** Resource: SANS IR cheat sheets.

3.2 Days 56-60: Digital Forensics Basics

- **Day 56:** Forensics intro (chain of custody, tools like Autopsy).
- **Day 57:** Disk imaging (dd, FTK Imager).
- **Day 58:** File system analysis (NTFS, ext4).
- **Day 59:** Memory forensics (Volatility framework).
- **Day 60:** Practice on CyberDefenders' free forensics labs.

3.3 Days 61-65: Malware Analysis Intro

- **Day 61:** Static analysis (strings, PEiD).
- **Day 62:** Dynamic analysis (ProcMon, Sysinternals).
- **Day 63:** Sandboxing (Cuckoo or online sandboxes).
- **Day 64:** YARA rules for detection.
- **Day 65:** Analyze sample malware from MalwareBazaar (safely in VM).

3.4 Days 66-70: Network Forensics

- **Day 66:** Packet analysis deep dive (Wireshark filters).
- **Day 67:** Detecting C2 traffic.
- **Day 68:** Log correlation for incidents.
- **Day 69:** HTB DFIR labs (incident investigation).
- **Day 70:** Simulate an incident (e.g., inject fake malware logs).

3.5 Days 71-75: Advanced IR and Review

- **Days 71-74:** Full IR simulation using THM or HTB ranges (triage, forensics, report).
- **Day 75:** Phase review: Create a personal IR plan; test it on a mock breach.

4 Phase 4: Advanced Topics, Threat Hunting, and Projects (Days 76-100)

Apply skills in proactive defense and real-world scenarios.

4.1 Days 76-80: Threat Hunting Basics

- **Day 76:** Hunting methodologies (hypothesis-driven, data-driven).
- **Day 77:** Using MITRE ATT&CK for hunts.
- **Day 78:** Anomaly detection in logs.
- **Day 79:** Tools like Jupyter for hunts.
- **Day 80:** HTB threat hunting labs.

4.2 Days 81-85: SOAR and Automation

- **Day 81:** SOAR intro (Phantom, Swimlane free).
- **Day 82:** Playbook automation (Python scripts for alerts).
- **Day 83:** Integration with SIEM.
- **Day 84:** UEBA basics (user behavior analytics).
- **Day 85:** Automate a simple response workflow.

4.3 Days 86-90: Vulnerability Management and Compliance

- **Day 86:** Vuln assessment processes.
- **Day 87:** Patch management.
- **Day 88:** Risk assessment frameworks.
- **Day 89:** Compliance audits (simulate PCI-DSS).
- **Day 90:** Resource: OWASP for web defense.

4.4 Days 91-95: Purple Team and Collaboration

- **Day 91:** Intro to purple teaming (collaborate with red team concepts).
- **Days 92-94:** Run hybrid exercises (e.g., attack/defend in lab).
- **Day 95:** Review team metrics (MTTD, MTTR).

4.5 Days 96-100: Capstone Projects and Final Review

- **Days 96-99:** Build a project (e.g., home SOC with ELK, IR report on a simulated breach, or contribute to open-source blue team tools).
- **Day 100:** Overall review: Assess progress, certify (e.g., aim for CompTIA Security+), plan next steps.

Conclusion

By the end, you will have a solid blue team portfolio. Adjust based on your pace, and remember consistency is key. If you encounter roadblocks, leverage free communities or revisit resources. Good luck!