24-Wochen Lernplan — Cyber Security (ausführlich)

Erstellt: 2025-10-12 23:42 (Europe/Berlin, empfohlenes Startdatum flexibel)

Woche 0: Vorbereitung

Lernziele: Homelab einrichten: VirtualBox/VMware, Kali Linux, Ubuntu VM, Windows 10/11 VM. Accounts: TryHackMe, HackTheBox, CTFtime, GitHub. Notizsystem (Obsidian/Notion/Markdown).
Tools & Ressourcen: VirtualBox/VMware, Kali Linux ISO, Ubuntu ISO, Windows ISO, TryHackMe, HackTheBox, GitHub, Obsidian/Notion
Praktische Übungen: Setze die VMs auf, erstelle Accounts, lege ein Notiz-Repo an, teste Snapshots.
Geschätzte Stunden/Woche: 6-10

Woche 1: TCP/IP & Grundlagen

Lernziele: OSI vs TCP/IP, IP-Adressierung, Subnetting, ARP, DHCP, DNS, Ports (0–65535). Verstehen, wie Pakete im Netzwerk fließen.
Tools & Ressourcen: ping, traceroute, ip, netstat, ss, Packet-diagramme, Subnetting-Rechner
Praktische Übungen: Subnetting-Drills, einfache Scans im Homelab, TryHackMe Räume zu Netzwerken.
Geschätzte Stunden/Woche: 8-12

Woche 2: Linux tief

Lernziele: Filesystem, Prozesse, permissions, systemd, package managers, Benutzerverwaltung, Shell-Grundlagen.
Tools & Ressourcen: bash, grep, sed, awk, ssh, systemctl, apt/yum/pacman
Praktische Übungen: Skripte schreiben (Backup, Log-Parsing), Grundeinstellungen in der VM härten, TryHackMe Linux-Kurse.
Geschätzte Stunden/Woche: 8-12

Woche 3: Windows Internals

Lernziele: Registry, Event Logs, Services, SMB, RDP, Windows Berechtigungen, NTFS, PowerShell Basics.
Tools & Ressourcen: PowerShell, Sysinternals (ProcMon, Autoruns, Process Explorer), Event Viewer
Praktische Übungen: Analysiere Eventlogs, erstelle einfache PowerShell-Skripte, probiere Sysinternals-Tools.
Geschätzte Stunden/Woche: 8-12

Woche 4: Web-Technologien

Lernziele: HTTP/HTTPS, Cookies, Sessions, Headers, CORS, REST APIs; Funktionsweise von Webservern und Web-Apps.
Tools & Ressourcen: Browser DevTools, curl, einfache Webserver (nginx/apache), OWASP Top 10
Praktische Übungen: Installiere DVWA oder Juice Shop und untersuche Request/Response. Experimentiere mit curl.
Geschätzte Stunden/Woche: 8-12

Woche 5: Programmierung & Scripting

Lernziele: Python-Grundlagen (Scripting, Netzwerklibs), Bash- und PowerShell-Scripting. Konzeptuelles C-Verständnis.
Tools & Ressourcen: Python3, pip, requests, pwntools (Grundlagen), bash, PowerShell
Praktische Übungen: Schreibe Portscanner in Python, Log-Parser, Automatisierungs-Skripte.
Geschätzte Stunden/Woche: 8-15

Woche 6: Kryptographie & Authentifikation

Lernziele: Hashes, symmetrische/ asymmetrische Verschlüsselung, TLS, Zertifikate, OAuth, MFA-Konzepte.
Tools & Ressourcen: openssl, Hash-Identifier, Online-CVE-Datenbanken (nur Referenz)
Praktische Übungen: TLS für lokale Webapp einrichten, Hashes identifizieren, einfache Krypto-CTF-Aufgaben.
Geschätzte Stunden/Woche: 6-10

Woche 7: Recon & Scanning

Lernziele: Footprinting, DNS-Enumeration, Port-Scanning, Service-Enumeration, passive vs aktive Recon.
Tools & Ressourcen: nmap, masscan, amass, dig, whois
Praktische Übungen: Scanne Ziel-VMs, baue eigene Enumeration-Skripte, dokumentiere Ergebnisse.
Geschätzte Stunden/Woche: 8-12

Woche 8: Schwachstellenanalyse

Lernziele: CVE Konzept, Exploit DB, Priorisierung von Schwachstellen, CVSS-Grundlagen.
Tools & Ressourcen: searchsploit, OpenVAS/Nessus (Trial), CVE Details
Praktische Übungen: Finde CVEs in Test-VMs, dokumentiere Impact & mögliche Remediation.
Geschätzte Stunden/Woche: 8-12

Woche 9: Web-App Hacking (Grundlagen)

Lernziele: XSS, SQLi, CSRF, Auth-Probleme, Input-Validation Failures; OWASP Top 10 vertiefen.
Tools & Ressourcen: Burp Suite Community, OWASP ZAP, Browser DevTools
Praktische Übungen: Teste Juice Shop / DVWA: finde und exploit SQLi, XSS, CSRF; schreibe Report.
Geschätzte Stunden/Woche: 10-15

Woche 10: Passwort-Angriffe & Authentifizierung

Lernziele: Passwort-Hashes, Salting, Brute-force vs Hash-Cracking, Rate-limiting, MFA Angriffe verstehen.
Tools & Ressourcen: John the Ripper, Hashcat, Hydra, rockyou/wordlists
Praktische Übungen: Cracke Beispiel-Hashes, analysiere Passwortpolicy-Schwächen.
Geschätzte Stunden/Woche: 8-12

Woche 11: Post-Exploitation Basics

Lernziele: Lateral Movement, Persistence-Mechanismen, Privilege Escalation Techniken (Linux & Windows).
Tools & Ressourcen: Metasploit (Meterpreter), linpeas/winpeas, mimikatz (nur in Labor), sysadmin-Tools
Praktische Übungen: Privilege Escalation auf vulns VMs üben, Persistence-Skripte analysieren.
Geschätzte Stunden/Woche: 10-15

Woche 12: Praktische CTF-Woche I

Lernziele: Anwenden: Web, Crypto, Forensik, Pwn. Fokus auf Struktur: Recon → Exploit → PostEx → Report.
Tools & Ressourcen: TryHackMe, HackTheBox, OverTheWire, CTFtime
Praktische Übungen: Löse 3-5 Einsteiger-CTFs, dokumentiere Writeups ausführlich.
Geschätzte Stunden/Woche: 12-18

Woche 13: Logging & SIEM Grundlagen

Lernziele: Log-Quellen, Parsing, Alert-Design, Threat Hunting Basics, Log-Retention.
Tools & Ressourcen: ELK Stack (ELK/Elastic), Splunk (Trial), Filebeat/Winlogbeat
Praktische Übungen: Ingest: Windows/Linux Logs, erstelle einfache Alerts und Dashboards.
Geschätzte Stunden/Woche: 8-12

Woche 14: Netzwerksicherheit

Lernziele: IDS/IPS Konzepte, Netzwerk-Segmentierung, Firewalls, VPN-Grundlagen.
Tools & Ressourcen: Snort/Suricata, Wireshark, iptables/nftables
Praktische Übungen: Erstelle IDS-Regeln, analysiere Traffic mit Wireshark, simuliere Angriffe und beobachte Alerts.
Geschätzte Stunden/Woche: 8-14

Woche 15: Incident Response & Forensik

Lernziele: IR-Phasen (Identification, Containment, Eradication, Recovery), Memory/Filesystem Forensics.
Tools & Ressourcen: Volatility, Autopsy, FTK Imager (theorie), outils de forensique
Praktische Übungen: Analysiere kompromittierte VM: Memory dump untersuchen, Plattenforensik durchführen.
Geschätzte Stunden/Woche: 10-15

Woche 16: Secure DevOps / AppSec Basics

Lernziele: Sichere SDLC, SAST/DAST, Dependency-Management, Secrets-Management, Container Security Grundlagen.
Tools & Ressourcen: Bandit, Snyk (theorie), Trivy, Docker Best Practices
Praktische Übungen: Integriere SAST (Bandit) in ein kleines Projekt, scan Docker images mit Trivy.
Geschätzte Stunden/Woche: 8-12

Woche 17: Hardening

Lernziele: System-Hardening für Linux/Windows, CIS Benchmarks, Least Privilege, Patch-Management Prozesse.
Tools & Ressourcen: CIS Benchmarks, Audit-Tools, Baseline-Konfigurationen
Praktische Übungen: Harde eine VM anhand eines Benchmark-Checks, dokumentiere Änderungen und Tests.
Geschätzte Stunden/Woche: 8-12

Woche 18: Purple Team: Angriff vs Detection

Lernziele: Koordination zwischen Red & Blue: TTPs testen, Detection-Tuning, Playbook-Erstellung.
Tools & Ressourcen: Eigene Tools aus vorherigen Wochen + SIEM/ELK
Praktische Übungen: Führe gezielte Angriffe durch, verbessere Detection Rules, messe Detection-Rate.
Geschätzte Stunden/Woche: 10-15

Woche 19: Exploitentwicklung Basics

Lernziele: Buffer Overflows, Stack/Heap Grundlagen, ASLR/DEP Konzepte, Return-Oriented Programming (ROP) Basics.
Tools & Ressourcen: gdb, pwntools, gcc, objdump, radare2 (Grundlagen)
Praktische Übungen: Solve einfache pwn-challenges, entwickle kleine Proof-of-Concepts in kontrollierter Umgebung.
Geschätzte Stunden/Woche: 12-18

Woche 20: Erweiterte Web- & API-Security

Lernziele: SSRF, IDOR, Auth-Bypass, API-Rate-Limiting, GraphQL Security Besonderheiten.
Tools & Ressourcen: Burp Extensions, Postman, OWASP Juice Shop advanced modules
Praktische Übungen: Führe fortgeschrittene Angriffe gegen API-Endpunkte durch, präsentiere Findings im Report.
Geschätzte Stunden/Woche: 10-15

Woche 21: Red Teaming Konzepte

Lernziele: OpSec, C2-Konzepte (theorie), Taktiken, Techniken und Verfahren (TTP) Mapping zu MITRE ATT&CK.;
Tools & Ressourcen: MITRE ATT&CK; Framework, Theoretical C2 concepts
Praktische Übungen: Erstelle eine red-team-Übung (nur im Homelab), dokumentiere Kill Chain und Lessons Learned.
Geschätzte Stunden/Woche: 8-12

Woche 22: Cloud Security (Grundlagen)

Lernziele: IAM, Objekt-Storage (S3), Netzwerk-Security in Cloud, Shared Responsibility Model, Cloud Logging.
Tools & Ressourcen: AWS/Azure/GCP Free Tier, AWS CLI, IAM Policies, CloudTrail/CloudWatch
Praktische Übungen: Setze eine kostenbewusste Cloud-Umgebung auf, sichere S3-Buckets, erstelle minimale IAM-Policies.
Geschätzte Stunden/Woche: 8-14

Woche 23: Zertifikatsvorbereitung / Vertiefung

Lernziele: Wahl: OSCP-Prep (offensive) oder CISSP-Basics (management); Wiederholung kritischer Themen und Prüfungsstrategien.
Tools & Ressourcen: PWK-Materialien (theorie), CISSP CBK (Überblick), Prüfungs-Sammlungen
Praktische Übungen: Arbeite gezielt an Schwächen, löse mittlere CTFs, übe Lab-Exploitation unter Zeitdruck.
Geschätzte Stunden/Woche: 12-20

Woche 24: Abschlussprojekt & Portfolio

Lernziele: Komplettes Engagement dokumentieren: Recon, Exploit, PostEx, Detection & Remediation; Writeups und Code auf GitHub.
Tools & Ressourcen: GitHub, Markdown-Writeups, Präsentationsfolien, ggf. Blog-Post
Praktische Übungen: Führe das Abschlussprojekt aus, erstelle 4-6 ausführliche Writeups, baue Portfolio/Readme.
Geschätzte Stunden/Woche: 15-25