Plano de Estudos — Trilha Red Team (Ofensiva)

Este documento contém um plano de estudos semanal/mensal para seguir a trilha ofensiva (Red Team) de forma ética e segura. Todas as atividades práticas devem ser realizadas apenas em ambientes autorizados (laboratórios, CTFs, VMs locais). Se você for menor de idade, peça sempre autorização e supervisão de um adulto ou mentor.

Visão geral (3 meses)

- Mês 1 — Fundamentos sólidos (Linux, redes, Python básico, conceitos de segurança). - Mês 2 — Ferramentas e técnicas ofensivas em lab (reconhecimento, web, exploração em VMs autorizadas). - Mês 3 — Emulação e aplicação prática (CTFs, exercícios Purple Team, relatório de simulação).

Níveis de intensidade

- Leve: ~3–4 horas/semana — ideal para quem tem pouco tempo. - Moderado: ~8–10 horas/semana — ritmo equilibrado. - Intensivo: ~15+ horas/semana — evolução mais rápida.

Mês 1 — Fundamentos (meta: ficar confortável com Linux, redes e Python)

Semanas 1–4: Linux básico, redes (modelo OSI/TCP-IP), Python básico e conceitos de segurança (CIA, criptografia). Plano Leve (3–4 h/semana): - 2 sessões/semana (1h): Linux básico. - 1 sessão (1h): redes - modelo OSI, TCP/UDP. - 1 sessão (30–60min): Python básico. Checkpoint: listar processos, manipular arquivos e escrever um script Python simples. Plano Moderado (8–10 h/semana): - 3 sessões semanais hands-on: Linux. - 2 sessões: redes (subnetting, ping, traceroute). - 2 sessões: Python (scripts para processamento de texto). Checkpoint: criar VM local e automatizar tarefa básica com Python. Plano Intensivo (15+ h/semana): - Linux 6–8h: permissões, serviços, logs. - Redes 3–4h: tcpdump, handshakes TCP. - Python 3–4h: scripts para automatização e parsing. Checkpoint: ambiente com 2 VMs e script para coleta de logs.

Mês 2 — Ferramentas & Técnicas (meta: executar labs em plataformas autorizadas)

Semanas 5–8: Reconhecimento/OSINT, Nmap, HTTP/HTTPS, Burp Suite (conceitos) e prática em máquinas intencionais. Plano Leve (3–4 h/semana): - 1h: teoria OSINT/footprinting. - 1h: Nmap (uso em lab). - 1h: OWASP Top 10 - XSS e SQLi (teoria). - 30–60min: TryHackMe - módulo básico. Checkpoint: resolver 1 máquina/tutorial básico. Plano Moderado (8–10 h/semana): - Nmap e reconhecimento: 3h hands-on. - Burp Suite/Proxy: 2h. - Web vulnerabilities: 3h (DVWA/TryHackMe). Checkpoint: completar 2 boxes em TryHackMe. Plano Intensivo (15+ h/semana): - Reconhecimento 3–4h. - Burp Suite & Web Exploitation 6–8h. - Post-exploit & Escalada 3–4h. Checkpoint: explorar vulnerabilidade em máquina de treino e documentar.

Mês 3 — Emulação, CTFs e relatório (meta: participar de CTFs e executar exercício Purple Team)

Semanas 9–12: CTFs práticos, movimentação lateral, MITRE ATT&CK; e elaboração de relatório técnico. Plano Leve (3–4 h/semana): - 1h: desafio CTF introdutório. - 1h: estudar MITRE ATT&CK.; - 1h: escrever relatório curto. Checkpoint: mini-relatório com 3 achados e recomendações. Plano Moderado (8–10 h/semana): - 4–6h: resolver 2–3 desafios CTF. - 2h: exercício Purple Team (lab). - 1–2h: elaborar relatório técnico. Checkpoint: completar CTF simples e relatório com evidências. Plano Intensivo (15+ h/semana): - 8–10h: CTFs e máquinas VulnHub. - 3–4h: Purple Team completo. - 3–4h: mapear técnicas com MITRE e produzir relatório profissional. Checkpoint: exercício de 1–2 dias em lab com relatório detalhado.

Checkpoints & Avaliação

- Mês 1: uso de Linux, script Python simples, entendimento TCP/UDP. - Mês 2: uso de Nmap, diagnóstico de tráfego simples, exploração em VM de treino. - Mês 3: resolver CTF iniciante e produzir relatório com recomendações. Mantenha um diário de estudo e registre comandos e insights.

Recursos sugeridos (rápido)

- Plataformas: TryHackMe, Hack The Box, VulnHub, OverTheWire. - Leituras: OWASP Top 10, MITRE ATT&CK.; - Ferramentas para lab: VirtualBox, distribuições Linux, DVWA, Metasploitable (usar apenas em lab isolado).

Rotina diária sugerida

- 20–30 min revisão teórica. - 30–60 min prática (lab/tryhackme). - 20–30 min escrita: anotar aprendizados. Para menores: dividir em blocos menores com pausas.

Notas de segurança e ética (obrigatório)

- Nunca aplicar técnicas contra sistemas reais sem permissão. - Peça autorização por escrito para qualquer teste. - Documente objetivos, escopo e resultados. - Priorize detectar e mitigar, não apenas explorar.

Gerado por assistente — versão em PDF do plano de estudos.