

O Caminho do Ethical Hacker

Esse Roadmap foi criado para te guiar na jornada de aprendizado em Cibersegurança. Ele está dividido em Níveis, como em um jogo — cada fase representa uma etapa fundamentos, formação técnica, prática e teste em laboratório, especialização, networking e certificações. Do básico ao avançado, você vai encontrar o que estudar, por onde começar, e quais ferramentas explorar. Siga no seu ritmo, e seja um autodidata.

[Caminho do Hacker](#)

Aqui você pode visualizar o roadmap em estilo de mapa mental. Ele é mais amplo e facilita enxergar conexões e a estrutura dos estudos. Utilizando uma ferramenta específica para essa funcionalidade.

[Ver Mapa Mental](#)

Os cards são a estrutura usada para montar o roadmap neste site. A metodologia aplicada é em estilo cascata: cada etapa depende da conclusão da anterior, promovendo uma progressão sequencial no aprendizado.

[Ver Cardes](#)

Caminho do Ethical Hacker

Nível 1

- *Hardware e Software*
- *Redes e Conexões*
- *Sistema Operacionais*
- *Segurança Cibernética*

Nível 1.5

- *Maestria em Conexões*
- *Percepção de Ameaças*

Nível 2

- *Linguagem de Programação*
- *Conceitos da Linguagem*

Nível 3

- *SO - Kali Linux*
- *Ferramentas Básicas*

Nível 4

- *Desenvolvimento de Carreira*
- *Certificação e Portfólio*

Nível 5

- *Trilha de Especialização*
- *Estudos Avançado*

Nível 1 - Fundamentos Essenciais

Infraestrutura e Sistemas

1. *Hardware e Software*
2. *Redes e Conexões*
 - Como os dados se movem pela rede;
 - Protocolos e portas;
 - Firewalls;
 - DNS;
 - Endereço IP;
3. *Sistema Operacional*
 - Distro Linux (Kali Linux);
 - Windows;
 - MacBook;

Fundamentos da Segurança Cibernética

1. *Segurança Cibernética*
 - Ameaças;
 - Vulnerabilidades;
 - Ataques;
2. *Tríade da CIA*
 - Confidencialidade;
 - Disponibilidade;
 - Integridade;
- Disponibilidade;

"A maior vulnerabilidade em qualquer sistema está entre o teclado e a cadeira." - Kevin Mitnick

Nível 1.5 - Maestria em Redes e Segurança

Maestria em conexões

1. LAN, WAN, WLAN e PAN
2. Modelo OSI
3. Modelo TCP/IP
4. Diferença entre IP Público x Privado
5. Sub-redes e máscara de sub-rede

Percepção de Ameaças

1. Hacker - White/Black/GreyHat
2. Ataques - Phishing, DDos, Malware e Exploits
3. Pentest
4. Engenharia Social
5. O papel do Ethical Hacker*

Nível 2 - Fundamentos Técnicos em Programação

Escolha uma Linguagem

1. JavaScript
2. Python
3. C

Deve Entender

- Front-end e Back-end;
- API (requisições, JSON, REST);
- Tipos de dados (booleano, string, inteiro, lista, dicionário);
- Condicionais (if/else);

- Laços de repetição (for/while);
- Estruturas de decisão e lógicas booleana;
- Conceito de autenticação e autorização (login/senha, tokens);
- Como a comunicação na internet acontece (HTTP request/response);
- Conceitos básicos de criptografia;

Dica: Fazer exercícios de pratica/projetos para aprender a solucionar erros;

Nível 3 - Sistema Operacional e Testes em Ferramentas

Kali Linux - Deve Entender

1. Conceito de Terminal e Shell (Bash)
2. Estrutura de diretórios no Kali Linux
3. Comandos Básicos (cd, ls, mkdir, cp, mv, rm, etc)
4. Permissões de arquivos (chmod, chown)
5. Gerenciamento de processos e serviços
6. Instalação de programas via terminal (apt, dpkg)

Ferramentas Básicas

- **nmap** - scanner de redes e portas;
- **Wireshark** - análise de pacotes;
- **traceroute / ping** - checagem de conectividade/rastreamento de rotas;
- **netstat** - visualizar conexões de rede;
- **ufw** - configuração de firewall básico;
- **ssh** - acesso remoto;
- **Proxychains** - roteamento de tráfego;
- **VPN básica** - conceito e prática de uso;

Dica: Montar mini-lab de testes (Vm + targets);

Nível 4 - Networking e Desenvolvimento Profissional

Desenvolvimento de Carreira

1. Participar de comunidade de cibersegurança e eventos
 - Discords, fóruns, LinkedIn, CTFs;
 - Roadsec, H2HC e entre outros;
2. Estágios na área de TI ou Cibersegurança
 - HelpDesk, Suporte de TI, etc;
3. Considerar iniciar uma graduação relacionada
 - ex. Ciência da Computação, Redes, Segurança da Informação;

Certificação e Portfólio

1. Começar a tirar certificações de entrada
 - CompTIA Security+ - conceitos de segurança;
 - CompTIA Network+ - conceitos de redes;
 - Linux Essentials - conceitos básicos de Linux;
2. Montar um portfólio com projeto, laboratórios de pratica e relatorios de teste (éticos);

Nível 5 - Especialização e Evolução Contínua

Escolher uma Trilha

1. **Red Team** (Testes de invasão)
 - Pentest e Exploração de Vulnerabilidade;
 - Engenharia Social;
 - Engenharia Reversa;
 - Malware Analysis;
 - Teste de Aplicação;
2. **Blue Team** (Defesa e Monitoramento)
 - Threat Intelligence (Inteligência de Ameaças);
 - Segurança de Aplicações;
 - Monitoramento com SIEM;
 - Resposta a Incidentes;
 - Forense Digital;
 - Segurança em Nuvem;
3. **Governança e Liderança**
 - GRC (Governança, Risco e Conformidades);
 - LGP e Leis de Privacidade;
 - Gestão de Segurança da Informação;
 - Normas como ISO 27001, NIST, COBIT;
 - Auditoria e Políticas de Segurança;

Plano de Estudos Avançado

1. Criar um roteiro próprio de estudo, focado na especialização escolhida
2. Buscar mentorias, comunidades técnicas ou grupos de estudos
3. Acompanhar tendências e atualizações constantes do setor
4. Realizar projetos, testes práticos e desenvolver um portfólio mais técnico
5. Continuar tirando certificações intermediarias e avançadas
6. Praticar em laboratórios mais avançados
7. Desenvolver projetos mais robustos e fazer relatórios de teste profissionais

Recomendações de Cursos e Certificação

[Cursos](#)

[Certificações](#)

[Quizz](#)