

Cadastre - se

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

estilo de mapa mental. Ele é mais amplo e facilita enxergar conexões e a estrutura dos estudos. Utilizando uma ferramenta específica para essa

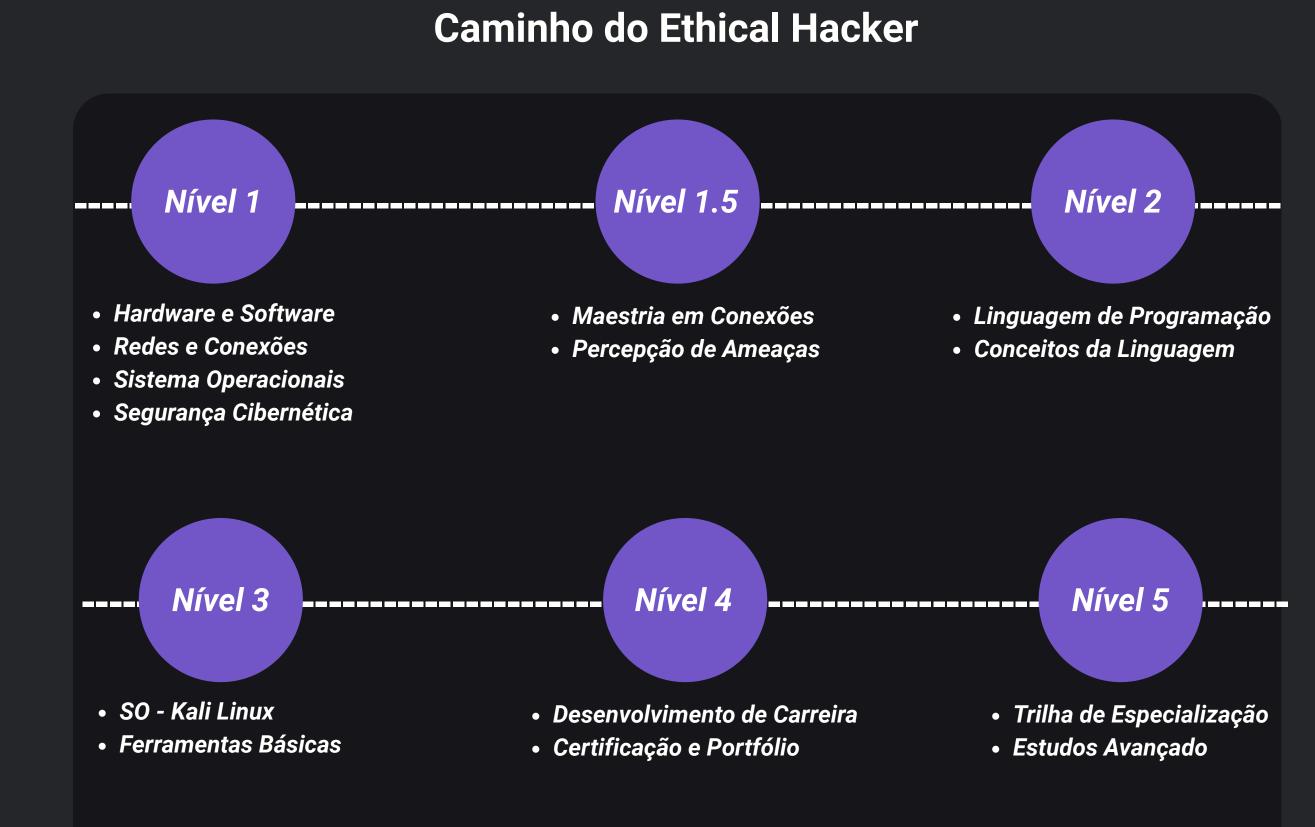
Aqui você pode visualizar o roadmap em

funcionalidade. Ver Mapa Mental

Os cards são a estrutura usada para montar o

em estilo cascata: cada etapa depende da conclusão da anterior, promovendo uma progressão sequencial no aprendizado. Ver Cardes

roadmap neste site. A metodologia aplicada é



Infraestrutura e Sistemas Fundamentos da Segurança Cibernética

Nível 1 - Fundamentos Essenciais

2. Redes e Conexões

Como os dados se movem pela rede;

1. Hardwares e Software

- Protocolos e portas;
- Firewalls;
- DNS;
- Endereço IP;
- 3. Sistema Operacional
- Distro Linux (Kali Linux);
- Windows;
- MacBook;

Ameaças; Vulnerabilidades;

Ataques;

1. Segurança Cibernética

- 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

Percepção de Ameaças Maestria em conexões

3. Modelo TCP/IP 4. Diferença entre IP Público x Privado

5. Sub-redes e máscara de sub-rede

1. LAN, WAN, WLAN e PAN

2. Modelo OSI

Exploits

2. Ataques - Phishing, DDos, Malware e

3. Pentest 4. Engenharia Social

1. Hacker - White/Black/GreyHat

5.0 papel do Ethical *Hacker**

Estruturas de decisão e lógicas 1. JavaScript booleana; 2. Python

Nível 2 - Fundamentos Técnicos em Programação

Deve Entender

Escolha uma Linguagem

- Front-end e Back-end;
- API (requisições, JSON, REST); • Tipos de dados (booleano, string,

chown)

3. C

inteiro, lista, dicionário);

Condicionais (if/else);

• Como a comunicação na internet acontece (HTTP request/response);

autorização (login/senha, tokens);

Dica: Fazer exercícios de pratica/projetos

• Conceito de autenticação e

Laços de repetição (for/while);

Conceitos básicos de criptografia;

para aprender a solucionar erros;

Ferramentas Básicas

nmap - scanner de redes e portas;

• Wireshark - análise de pacotes;

• traceroute / ping - checagem de 3. Comandos Básicos (cd. ls, mkdir, cp, mv, rm, etc) conectividade/rastreamento de rotas;

Nível 3 - Sistema Operacional e Testes em Ferramentas

5. Gerenciamento de processos e serviços

4. Permissões de arquivos (chmod,

Kali Linux - Deve Entender

1. Conceito de Terminal e Shell (Bash)

2. Estrutura de diretórios no Kali Linux

Desenvolvimento de Carreira

2. Estágios na área de TI ou

• HelpDesk, Suporte de TI, etc;

Segurança da Informação;

3. Considerar iniciar uma graduação

Cibersegurança

6. Instalação de programas via terminal (apt, dpkg)

netstat - visualizar conexões de rede; • ufw - configuração de firewall básico;

• **Proxychains** - roteamento de tráfego;

• VPN básica - conceito e prática de uso; Dica: Montar mini-lab de testes (Vm + targets);

• ssh - acesso remoto;

- Certificação e Portfólio 1. Começar a tirar certificações de
- segurança; CompTIA Network+ - conceitos de redes;

• Linux Essentials - conceitos básicos

relacionada 2. Montar um portfólio com projeto, • ex. Ciência da Computação, Redes, laboratorios de pratica e relatorios de

Escolher uma Trilha

1.*Red Team* (Testes de invasão)

Pentest e Exploração de

- Vulnerabilidade; • Engenharia Social; • Engenharia Reversa;
- 2. **Blue Team** (Defesa e Monitoramento) • Threat Intelligence (Inteligência de

Malware Analysis;

• Teste de Aplicação;

- 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 Póliticas de Segurança;

Linkedin

1. Participar de comunidade de cibersegurança e eventos entrada • CompTIA Security+ - conceitos de Discords, fóruns, LinkedIn, CTFs; • Roadsec, H2HC e entre outros;

de Linux;

teste (éticos);

Nível 4 - Networking e Desenvolvimento Profissional

Nível 5 - Especialização e Evolução Contínua

- Plano de Estudos Avançado 1. Criar um roteiro próprio de estudo,
- 2. Buscar mentorias, comunidades técnicas ou grupos de estudos

focado na especialização escolhida

4. Realizar projetos, testes práticos e desenvolver um portifólio mais técnico

atualizações constantes do setor

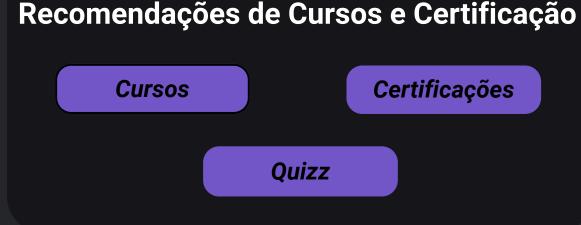
3. Acompanhar tendências e

6. Praticar em laboratórios mais avançados 7. Desenvolver projetos mais robustos e

5. Continuar tirando certificações

intermediarias e avançadas

fazer relatórios de teste profissionais



Cadastre -se

Home | Roadmap | Certificação | Entretenimento | Caminho do Hacker

+ © 2025 LPAroadmap. Desenvolvido por Lucas Pereira Amorim Santos.

GitHub