Roadmap de Cibersegurança
Guia de aprendizado progressivo

Esse roteiro (roadmap) foi feito pra te ajudar a organizar de forma mais objetiva os teus estudos em cibersegurança. Abaixo, temos os assuntos organizados de acordo com a curva progressiva de aprendizagem da área.

Todavia, ele não abrange os temas mais emergentes, pois ele foi pensado para descrever os assuntos que são pertencentes a base conhecimentos que fundamentam a área de cibersegurança.

Já adianto, você não conseguirá absorver tudo e todos os conteúdos, logo, não entre em desespero ao ver o tanto de coisas a serem estudadas, foque em um aprendizado contínuo diário, onde você se dispõe a aprender algo novo todo dia.

Reforço que a constância te levará mais longe do que a força empregada pra você se tornar mais veloz na área da TI.

No mais, bons estudos e sucesso em sua jornada em cibersegurança! Afinal, você está dando os primeiros passos em uma caminhada que não têm fim, exceto se você desistir dela, migrar para outra área profissional, aposentar-se ou se você bater as botas, for de arrasta, assim por diante…rsrsrs….

Até mais,

Samira Silva
linkedin: samirasilva

Componentes de hardware de computador

Processador, memória RAM, armazenamento, placa-mãe
Placas de rede, fontes de alimentação, periféricos

Solução de problemas independente de SO

Diagnóstico básico de hardware e software
Metodologias de troubleshooting

Tipos de conexão e suas funções

USB, HDMI, Ethernet, conexões sem fio
Cabos e conectores básicos

WiFi

Conceitos básicos de redes sem fio
Configuração e troubleshooting

Entender o básico de suítes populares

iCloud: Armazenamento e sincronização Apple
Google Suite: Gmail, Drive, Docs, Sheets
Microsoft Office Suite: Word, Excel, PowerPoint, Outlook

Sistemas Operacionais

Windows

Instalação e configuração
Diferentes versões e diferenças: Windows 10, 11, Server
Entender permissões: Usuários, grupos, ACLs
Instalação de software e aplicações
Executar CRUD em arquivos: Criar, ler, atualizar, deletar
Navegação usando GUI e CLI: Interface gráfica e linha de comando
Troubleshooting: Resolução de problemas
Comandos comuns: cmd, PowerShell

Linux

Instalação e configuração
Diferentes distribuições: Ubuntu, CentOS, Debian
Entender permissões: chmod, chown, grupos
Instalação de software: apt, yum, rpm
Executar CRUD em Arquivos: comandos básicos
Navegação usando GUI e CLI: Terminal e interface gráfica
Troubleshooting: Logs, processos
Comandos comuns: ls, cd, grep, find, ps, top

macOS

Instalação e configuração
Entender permissões: Sistema de permissões macOS
Instalação de software: App Store, Homebrew
Executar CRUD em Arquivos: Finder e Terminal
Navegação usando GUI e CLI: Terminal e Finder
Troubleshooting: Utilitários do sistema
Comandos comuns: Comandos Unix-like

Conhecimento dos fundamentos de redes de computadores

Entender o Modelo OSI

Camada 7: Aplicação
Camada 6: Apresentação
Camada 5: Sessão
Camada 4: Transporte
Camada 3: Rede
Camada 2: Enlace de dados
Camada 1: Física

Entender o Modelo TCP/IP

Camada 4: Aplicação
Camada 3: Transporte
Camada 2: Internet
Camada 1: Acesso a rede

Obs: O modelo de referência TCP/IP é o modelo mais usado atualmente, sendo ele uma simplificação do Modelo OSI. Nele, as sete camadas do OSI são agrupadas em quatro camadas funcionais presentes no modelo TCP/IP, facilitando assim, o gerenciamento da comunicação entre redes, e principalmente, a comunicação dessas redes com a Internet.

Portas comuns e seus usos

HTTP: 80
HTTPS: 443
SSH: 22
FTP: 21
SMTP: 25
DNS: 53
DHCP: 67/68

Protocolos comuns e seus usos

TCP/IP: Protocolo base da internet
HTTP/HTTPS: Navegação web
SSH: Acesso remoto seguro
FTP/SFTP: Transferência de arquivos

Entender terminologias

VLAN: Virtual LAN
DMZ: Zona desmilitarizada
ARP: Address Resolution Protocol
VM: Máquina Virtual
NAT: Network Address Translation
IP: Internet Protocol
DNS: Domain Name System
DHCP: Dynamic Host Configuration Protocol
Router: Roteador
Switch: Comutador
VPN: Virtual Private Network

SSL e TLS básico

Protocolos de criptografia para comunicação segura
Certificados digitais e PKI

Endereços IP públicos X privados

Públicos: Roteáveis na internet
Privados: Uso interno (192.168.x.x, 10.x.x.x, 172.16-31.x.x)

Terminologia de IP

localhost: 127.0.0.1
loopback: Interface de retorno
subnet mask: Máscara de sub-rede
default gateway: Gateway padrão
CIDR: Classless Inter-Domain Routing

Conceitos a serem entendidos sobre os tipos de rede

MAN: Metropolitan Area Network - Redes metropolitanas
LAN: Local Area Network - Redes locais
WAN: Wide Area Network - Redes de longa distância
WLAN: Wireless LAN - Redes sem fio
PAN: - Redes pessoais

Função de cada serviço

DHCP: Atribuição automática de IP
DNS: Resolução de nomes
NTP: Sincronização de tempo
IPAM: Gerenciamento de endereços IP

Topologias de rede

Ponto a Ponto (Point-to-Point): Conexão direta entre dois dispositivos.

Barramento (Bus): Todos os dispositivos compartilham um único cabo de comunicação.

Anel (Ring): Dispositivos conectados em um loop fechado; os dados passam de um a um até chegar ao destino.

Estrela (Star): Dispositivos conectados a um ponto central (hub ou switch), que distribui os dados.

Árvore (Tree): Estrutura hierárquica com dispositivos ligados a um "nó pai", formando uma rede em ramificações.

Malha (Mesh): Dispositivos interconectados com múltiplos caminhos; oferece alta redundância e confiabilidade.

Híbrida: Combinação de duas ou mais topologias para atender necessidades específicas da rede.

Básico de sub-redes

Divisão de redes em sub-redes menores
Cálculo de sub-redes e hosts

Básico de NAS e SAN

NAS: Network Attached Storage
SAN: Storage Area Network

Entender o básico de virtualização

Hypervisor: Software de virtualização
VM: Máquina Virtual
Guest OS: Sistema operacional convidado
Host OS: Sistema operacional hospedeiro

Tecnologias comuns de virtualização

VMware: ESXi, Workstation
VirtualBox: Virtualização gratuita
Proxmox: Plataforma de virtualização open-source

Protocolos mais comuns

SSH: Secure Shell
FTP: File Transfer Protocol
RDP: Remote Desktop Protocol
SFTP: Secure FTP
HTTP/HTTPS: Navegação web
SSL/TLS: Criptografia de transporte
Kerberos: Autenticação
LDAP: Lightweight Directory Access Protocol
SSO: Single Sign-On

Certificados e autenticação

Certificates: Certificados digitais
Local Auth: Autenticação local
RADIUS: Remote Authentication Dial-In User Service

Ferramentas de troubleshooting

Packet Sniffers (Capturadores de pacote)

Wireshark: Análise de tráfego de rede
tcpdump: Captura de pacotes em linha de comando

Port Scanners (Scanners de porta)

nmap: Network mapper e scanner de portas

Protocol Analyzers (Analizadores de protocolo)

Ferramentas para análise detalhada de protocolos

Comandos Essenciais

ping: Teste de conectividade
tracert/traceroute: Rastreamento de rota
dig: Consulta DNS
nslookup: Resolução de nomes
ipconfig/ifconfig: Configuração de interface

iptables: Firewall Linux
netstat: Estatísticas de rede
arp: Tabela ARP
route: Tabela de roteamento

Habilidades e conhecimentos de segurança da informação

Tríade CID

Confidentiality: Confidencialidade
Integrity: Integridade
Availability: Disponibilidade

Tipos de ataque e diferenças

Engenharia Social

Phishing: E-mails fraudulentos
Vishing: Phishing por telefone
Whaling: Phishing direcionado a executivos
Smishing: Phishing por SMS
Spam vs Spim: E-mail vs mensagem instantânea indesejada
Shoulder Surfing: Observação por cima do ombro
Dumpster Diving: Busca em lixo
Tailgating: Seguir pessoa autorizada
Impersonation: Personificação
Watering Hole Attack: Ataque de poço d'água
Drive by Attack: Ataque por download
Typo Squatting: Domínios similares maliciosos

Ataques de força bruta

Brute Force: Força bruta
Password Spray: Pulverização de senha

Zero Day

Vulnerabilidades não conhecidas publicamente

Tipos de malware

Vírus, worms, trojans, ransomware, spyware

Ataques baseados na Web e OWASP Top 10

Principais vulnerabilidades em aplicações web

Escalação de privilégios / Ataques baseados em usuário

Técnicas para obter privilégios elevados

Conceitos básicos

Handshakes

Processo de estabelecimento de conexão

Threat intel e OSINT

Threat Intelligence: Inteligência de ameaças
OSINT: Open Source Intelligence

Falso negativo / Falso positivo

False negative: Ameaça não detectada
False positive: Falso alarme
True negative: Corretamente identificado como seguro
True positive: Ameaça corretamente identificada

Times de segurança

Blue Team: Defesa
Red Team: Ataque simulado
Purple Team: Colaboração entre blue e red

Cyber Kill Chain

Modelo de fases de um ataque cibernético

Hardening de sistema operacional

MFA e 2FA

Multi-Factor Authentication: Autenticação multifator
Two-Factor Authentication: Autenticação de dois fatores

Autenticação vs autorização

Authentication: Verificação de identidade
Authorization: Permissão de acesso

Entender sobre backups e resiliência

Estratégias de backup e recuperação
Papéis de Compliance e Auditores
Conformidade regulatória e auditorias
Entender a Definição de Risco

Avaliação e gerenciamento de riscos

Conceitos centrais de Zero Trust - Modelo de segurança "nunca confie, sempre verifique"

Basics de IDS e IPS

IDS: Intrusion Detection System
IPS: Intrusion Prevention System
Honeypots: Armadilhas para atacantes

Entender o conceito de isolamento

Segmentação e isolamento de redes

Perímetro vs DMZ vs segmentação

Diferentes abordagens de defesa de rede

Teste de penetração - Regras de engajamento

Metodologia e ética em testes de invasão

Básico de engenharia reversa

Análise de software e malware

Conceitos de gerenciamento de vulnerabilidades

Identificação, avaliação e correção de vulnerabilidades

Conceitos de threat hunting

Busca proativa por ameaças

Conceitos básicos de Forense

Investigação de incidentes de segurança

Conceito de runbooks

Procedimentos padronizados de resposta

Conceito de defesa em profundidade

Múltiplas camadas de segurança

Entender frameworks comuns de exploit

Metasploit, Cobalt Strike, etc.

Ataques comuns baseados em rede

Ataques de negação de serviço
DoS: Denial of Service
DDoS: Distributed Denial of Service

Outros ataques de rede

Evil Twin: Ponto de acesso malicioso
MITM: Man in the Middle
DNS Poisoning: Envenenamento de DNS
ARP Poisoning: Envenenamento de ARP
Spoofing: Falsificação
Deauth Attack: Ataque de desautenticação

VLAN Hopping: Salto entre VLANs
Rogue Access Point: Ponto de acesso não autorizado
War-driving/dialing: Busca por redes vulneráveis

Ataques de aplicação

Buffer Overflow: Estouro de buffer
Memory Leak: Vazamento de memória
SQL Injection: Injeção SQL
XSS: Cross-Site Scripting
CSRF: Cross-Site Request Forgery
Pass the Hash: Reutilização de hash
Replay Attack: Ataque de repetição
Directory Traversal: Travessia de diretório

Proteção de endpoint

Antivirus: Antivírus
Antimalware: Anti-malware
EDR: Endpoint Detection and Response
DLP: Data Loss Prevention

Proteção de rede

Firewall: Firewall tradicional
Next-gen Firewall: Firewall de próxima geração
HIPS: Host-based Intrusion Prevention System
NIDS: Network Intrusion Detection System
NIPS: Network Intrusion Prevention System
Host Based Firewall: Firewall baseado em host

Outras tecnologias a serem vistas

Sandboxing: Ambiente isolado para análise
ACL: Access Control List

Segurança Wireless

WPA vs WPA2 vs WPA3 vs WEP: Protocolos de segurança WiFi
EAP vs PEAP: Protocolos de autenticação
WPS: WiFi Protected Setup

Processo de resposta a incidentes

Preparation: Preparação
Identification: Identificação
Containment: Contenção
Eradication: Erradicação
Recovery: Recuperação
Lessons Learned: Lições aprendidas

Ferramentas para resposta a incidentes e descoberta

nmap: Scanner de rede
tracert: Rastreamento de rota
nslookup: Consulta DNS
dig: Ferramenta DNS
curl: Cliente de URL
ipconfig: Configuração IP
hping: Gerador de pacotes
ping: Teste de conectividade
arp: Protocolo ARP
cat: Visualizar arquivos
dd: Cópia de dados
head/tail: Visualizar início/fim de arquivos
grep: Busca em texto
wireshark: Análise de pacotes
winhex: Editor hexadecimal
memdump: Dump de memória
FTK Imager: Criação de imagens forenses
autopsy: Análise forense

Modelos de ameaças

ATT&CK: Framework MITRE ATT&CK
Kill chain: Cadeia de eliminação
Diamond Model: Modelo diamante

Padrões e frameworks

ISO: International Organization for Standardization
NIST RMF: NIST Risk Management Framework
CIS: Center for Internet Security
CSF: Cybersecurity Framework

Entender SIEM

Security Information and Event Management: Gerenciamento de informações e eventos de segurança

Entender SOAR

Security Orchestration, Automation and Response: Orquestração, automação e resposta de segurança

Distribuições comuns para hacking

ParrotOS: Distribuição para testes de segurança
Kali Linux: Distribuição para testes de penetração

LOLBAS

Living Off The Land Binaries and Scripts: Uso de ferramentas legítimas para fins maliciosos

Logs e monitoramento

Event Logs: Logs de eventos
syslogs: Logs do sistema
netflow: Fluxo de rede
Packet Captures: Capturas de pacotes
Firewall Logs: Logs de firewall

Conceitos de hardening - Técnicas de endurecimento

MAC-based: Controle de acesso baseado em MAC
Port Blocking: Bloqueio de portas
Group Policy: Política de grupo
ACLs: Listas de controle de acesso
Sinkholes: Redirecionamento de tráfego malicioso
NAC-based: Controle de acesso à rede
Patching: Aplicação de patches
Jump Server: Servidor de salto

Endpoint Security

Segurança de pontos finais

Ameaças avançadas

Zero Day: Vulnerabilidades desconhecidas
Known vs Unknown: Ameaças conhecidas vs desconhecidas
APT: Advanced Persistent Threat

Comunicação e relatórios - Entender o público envolvido

Stakeholders: Partes interessadas
HR: Recursos Humanos
Legal: Jurídico
Compliance: Conformidade
Management: Gerência

Ferramentas comuns de análise

VirusTotal: Análise de malware
Joe Sandbox: Sandbox para análise
any.run: Sandbox interativo
urlvoid: Verificação de URL
urlscan: Scanner de URL
WHOIS: Informações de domínio

Entender sobre as ferramentas comuns de hacking

Metasploit, Burp Suite, etc.

Entender serviços de cloud

SaaS: Software as a Service
PaaS: Platform as a Service
IaaS: Infrastructure as a Service

Modelos de cloud

Private: Privado
Public: Público
Hybrid: Híbrido

Ambientes comuns de cloud

AWS: Amazon Web Services
GCP: Google Cloud Platform
Azure: Microsoft Azure

Armazenamento comum em cloud

S3: Amazon S3
Dropbox: Armazenamento Dropbox
Box: Box.com
OneDrive: Microsoft OneDrive
Google Drive: Google Drive
iCloud: Apple iCloud

Conceitos de segurança na cloud

Responsabilidade compartilhada
Configuração segura
Monitoramento e logging

Conceitos avançados

Infrastructure as Code: Infraestrutura como código
Serverless: Computação sem servidor
CDN: Content Delivery Network

Fundamentos em criptografia

Salting: Adição de salt a hashes
Hashing: Função de hash
Key Exchange: Troca de chaves

PKI (Public Key Infrastructure)

Private Key vs Public Key: Chave privada vs pública
Obfuscation: Ofuscação

Protocolos seguros vs inseguros

FTP vs SFTP: File Transfer Protocol vs Secure FTP
SSL vs TLS: Secure Sockets Layer vs Transport Layer Security
IPSEC: Internet Protocol Security
DNSSEC: DNS Security Extensions
LDAPS: LDAP over SSL
SRTP: Secure Real-time Transport Protocol
S/MIME: Secure/Multipurpose Internet Mail Extensions

Tecnologias de comunicação

Infrared: Infravermelho
Bluetooth: Bluetooth
NFC: Near Field Communication

Classificação de ameaças - Entender a classificação de ameaças

Categorização de diferentes tipos de ameaças
Níveis de severidade e impacto

Aprender a encontrar e usar logs

Localização e análise de logs de sistema
Correlação de eventos

Usar ferramentas para propósitos não intencionais

Living off the land
Uso dual de ferramentas legítimas

Padrões e frameworks

ISO 27001, NIST, CIS Controls

Entender sobre os frameworks de segurança

MITRE ATT&CK, NIST Cybersecurity Framework

Certificações iniciais

CompTIA A+: Fundamentos de TI
CompTIA Linux+: Administração Linux
CompTIA Network+: Fundamentos de rede
CompTIA Security+: Fundamentos de segurança

Certificações avançadas

CISSP: Certified Information Systems Security Professional
CISA: Certified Information Systems Auditor
CISM: Certified Information Security Manager
GSEC: GIAC Security Essentials
GPEN: GIAC Penetration Tester
GWAPT: GIAC Web Application Penetration Tester
OSCP: Offensive Security Certified Professional
GIAC: Global Information Assurance Certification
CREST: Council of Registered Ethical Security Testers
CEH: Certified Ethical Hacker
CCNA: Cisco Certified Network Associate

CTFs (Capture the Flag) - Plataformas de prática

HackTheBox: Laboratórios de hacking
TryHackMe: Plataforma de aprendizado
VulnHub: Máquinas virtuais vulneráveis
picoCTF: CTF educacional
SANS Holiday Hack Challenge: Desafio anual

Habilidades de programação (opcional mas recomendado)

Python: Automação e scripting
Bash: Scripts de sistema Unix/Linux
PowerShell: Scripts de sistema Windows
Go: Linguagem moderna para ferramentas
JavaScript: Desenvolvimento web e automação
C++: Desenvolvimento de baixo nível

Continue aprendendo

Mantenha-se atualizado com as últimas ameaças
Participe de comunidades de segurança
Leia blogs e publicações especializadas
Pratique regularmente em laboratórios
Desenvolva projetos pessoais
Contribua para projetos open-source