GUIA DE CARREIRA

CIBERSEGURANÇA

Criado por Joas Antonio

Segurança da Informação - Base

Informática Avançada

Fundamentos Computacionais Conhecimentos profundos em Gerenciamento de Redes e configuralções

Redes de Computadores Algoritmos, POO, Linguagem de Programação Alto e Baixo Nível e etc

> Lógica da Programação

Conhecimentos em Administração de Ambientes Linux e Windows

> Conhecimentos em Sistemas Operacionais

Pilares da Segurança, Conceitos de Segurança, Ameaças Cibernéticas, ISSO 27001, LGPD e Gestão de Segurança em Geral

Conhecimentos em Segurança da Informação

Esse são alguns dos pilares que a área da segurança da informação exige que você conheça, o melhor método de se aprofundar nesse campo base, é procurando cursos e estudando e lendo artigos sobre Tecnologia. Lembre-se que nós protegemos o negócio e para isso precisamos entender de todas as tecnologias e serviços possíveis.

Segurança da Informação - Base 2

Containers

Conhecimentos em soluções de containers e afins Cloud Computer e IOT

Conhecimentos em nuvem e gerenciamento de infraestrutura cloud.

Conhecimento de soluções de cibersegurança

Conhecer de ferramentas que auxiliam na proteção e no gerenciamento da informação e a segurança do mesmo Conhecimentos em Gestão de Riscos e Vulnerabilidades

> Entender os riscos existentes e como gerenciar vulnerabilidades

BLUE TEAM OU RED TEAM?

Defesa ou Ataque, escolha um e se aprofunde

Essa é a base 2 que você precisa conhecer também, e por fim definir por qual caminho você vai seguir, seja ele Blue Team ou Red Team, pois dentro de cada um tem um determinado Segmento. Pense, qual área eu me daria bem? Atacar ou defender? E o que eu preciso para me qualificar nessas duas áreas, o que o mercado pede? Vou responder isso na próxima página

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

Segurança da Informação - Blue Team

Gestão de Riscos, Analise de Riscos

Conhecer de riscos e analisos é essencial

CSIRT E FORENSE COMPUTACIONAL

Responder e tratar incidentes, além de investiga-los é um papel fundamental

Analise de Malware e Engenharia Reversa

Apesar de acharem que é o papel só do Red Team, mas analisar Malware é um papel fundamental na defesa. Conhecimentos em soluções de cibersegurança, Arquitetura de Segurança

Conhecer de soluções que auxiliam na segurança da informação é fundamental

Threat
Intelligence,
Gerenciamento
de Logs e etc

O trabalho de inteligência é fundamental, jutamente com gerenciamento de logs e outras ferramentas

Em resumo, um profissional de segurança Blue Team precisa conhecer tanto da base, mas além disso gerenciar soluções como Firewall, SIEM, DLP, AV, EDR e por ai vai. Um fator predominante é você visualizar as vagas de Blue Team e ver o que o mercado pede. Além disso, conhecer de frameworks e padrões, como a Familia ISO27K, C2M2, NIST, CIS Controls, HIPAA, Sarbanes-Oxley, LGPD e muitas outras por ai. Um profissional de Blue Team tem que estar atento e conhecer dos TTPs (Tática, técnicas e procedimentos dos atacantes), para criar bons indicadores, pensar no Cyber Kill Chain atrelado a Blue Team. Lembre-se, certificações ajudam na sua carreira.

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

Segurança da Informação - RED TEAM

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

Conhecimentos em Metodologias de PenTest e do seu processo

Saber como um PenTest funciona é fundamental Conhecimentos teste de invasão em aplicações Mobile, Desktop e Web

Conhecimentos nessas áreas são fundamentais para realizar PenTest nesses escopos Analise de Malware, Engenharia Reversa, Binary Exploitation e Buffer Overflow

Partindo do principio mais avançado, fazer novas descobertas e ir mais a fundo, sempre é bom para um Red Team Conhecimento de Soluções de Analise e Gestão de Vuln, Metodologias e Frameworks

Conhecer de soluções de analise de vuln é essencial para levantar as brechas do ambiente, além de metodologias e framework que são essenciais Técnicas de Invasão Avançada, Segurança de App e Mitre Att&ck

técnicas de invasão,
conhecer de segurança de
aplicação e entender a
estrutura Mitre é

Em resumo, um profissional de Red Team ele não só faz PenTest, mas ele avalia os riscos, levanta vulnerabilidades e trabalha junto com o Blue Team, com certeza conhecimentos em invasão é essencial, por recomendação, se aprofunde bastante em conhecer metodologias e frameworks, como Mitre, Cyber Kill Chain, OSSTMM, NIST, PTES, OWASP e por ai vai. Além disso ajudar no desenvolvimento de aplicações seguras, identificar brechas de segurança, trabalhar com sinergia com as outras áreas afim de encontrar potênciais riscos. Saber elaborar documentações e relatórios de PEnTest é essencial. Conhecimentos em programação. Conhecimentos em sistemas operacionais principalmente se você é um invasor. Além de Técnicas avançadas de PenTest, estar sempre atualizado todos os dias. E lembre-se, certificações ajudam na sua carreira.

Material complementar: Mapas Mentais

- https://www.mindmeister.com/pt/1746180947/web-attacks-bug-bounty-and-appsec-by-joas-antonio
- https://www.mindmeister.com/pt/1760781948/information-security-certifications-by-joas-antonio
- https://www.mindmeister.com/pt/1781013629/the-best-labs-and-ctf-red-team-and-pentest
- https://www.mindmeister.com/pt/1760781948/information-security-certifications-by-joas-antonio
- https://www.mindmeister.com/pt/1746187693/cyber-security-career-knowledge-by-joas-antonio



Material complementar: Road Maps

Esse é um roadmap que fiz mais aprofundado sobre Fundamentos de segurança JUAS AN IUNIU

FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

ISO 27001/27002	Ameaça x Vulnerabilidade	Conceito de Riscos em segurança da informação (ISO 27005)	Conceitos de Segurança de Redes	C.I.D
Dados x Informação	Gestão e Tipos de Informação	Politicas de Segurança da Informação	Gestão de Ativos de Segurança da Informação	Controle e Criptografia
Tipos de Ameaças e Vetores de Ataques	Conceito de Arquitetura em Segurança da Informação	C2M2, NIST, HIPAA, PCI-DSS, LGPD/GDPR	Conceitos de desenvolvimento seguro	Conceitos de Segurança em Nuvem
Conceitos de Segurança Física	Gestão de Vulnerabilidades	Gestão de Mudanças	Gerenciamento de Patches e Hardening	Tratamento e Resposta a Incidentes
Conhecimentos em Forense Computacional	Conhecimentos em Teste de Invasão	Conhecimentos em Inteligência Cibernética	Disaster Recovery e conhecimentos em operações de segurança	Soluções de Cibersegurança e Gerenciamento de Redes

SEGURANÇA OFENSIVA

Material complementar: Road Maps

Esse é um roadmap que fiz mais aprofundado sobre Segurança Ofensiva Conceitos de Ethical Hacking e contramedidas

Conhecimentos em Ferramentas de Analis de Vulnerabilidade (SAST, DAST, IAST e etc

Tipos de Ameaças e Vetores de Ataques em diversos tipos de ambiente (Web, Infra, IoT, ISC, Wireless, Clouding, Mobile e etc.)

Conhecimentos em Técnicas Avançadas de Enumeração, Scanning e Reconhecimento

Conhecimentos em Forense Computacional e Eliminação de Rastros Ameaça x Vulnerabilidade

C2M2, NIST, HIPAA, PCI-DSS, LGPD/GDPR

Gerenciamento, Analise e Tratamento de Riscos

Conhecimento em exploração e técnicas de evasão e bypassing de controles de segurança

Conhecimentos em Programação Baixo Nivel Conhecimentos em Gestão de Vulnerabilida<u>des</u>

Conceitos de desenvolvimento seguro

Conhecimentos em Metodologias e Frameworks de PenTest (PTES, OSSTM, NIST, OWASP)

Conhecimentos em Pós exploração, escalação de privilégios, persistência

Conhecimentos em Linguagens de alto nível e desenvolvimento de scripts para automatização Conhecimentos em Administração de Sistemas (Linhas de Comandos, Hardening e Configurações de rede)

Conhecimentos em Inteligência Cibernética e Resposta a Incidentes

Conhecimentos em elaboração de relatórios técnicos e executivos

Conhecimento de Matrix C2 e Operações Red Team

Conhecimentos em Buffer Overflow, Desenvolvimento de Exploits, Engenharia Reversa e Analise de Malware Hacking Tools

Arquitetura e Soluções de Segurança da Informação

Conceitos de Segurança em Nuvem

Conhecimentos em TTPs e Adversary Emulation

Habilidades em CTFs e Desafios de Segurança Ofensiva

Material complementar

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

https://drive.google.com/file/d/1rcfM00j6V7skggk47DViklaDPPMvYFqt/view?usp=sharing (Red Team)

https://drive.google.com/file/d/1flBEwk7EWucgak4RMMSjbMn69tyT8XKD/view?usp=sharing (Hack The Box e Vulnhub Dicas)

https://drive.google.com/file/d/1kcL4kjQ9iUVo HaZehzp1uYSQYBgIUIS/view?usp=sharing (Blue Team e o Mercado de Trabalho)

https://drive.google.com/file/d/1lOp4IQVSzFt5F6d5W4nn--NK-JvdZkPn/view?usp=sharing (Carreira na área de SOC)

https://drive.google.com/file/d/1lObhWau7E5aN0X c-OWLoL5bo1RJx MI/view?usp=sharing (Bug Bounty Career)

Material complementar

Criado por Joas Antonio – Linkedin: https://www.linkedin.com/in/joas-antonio-dos-santos

https://drive.google.com/file/d/13QAcBYjfYZRPLnclDDVMJeROXK0d4pLm/view?usp=sharing (Carreira de PenTester do Jr ao Especialista)

https://drive.google.com/file/d/1kNjwtaxodCZ8s5WQDuLPYnyIdh1169hl/view?usp=sharing (Carreira em Cyber Security do Jr ao Especialista)

https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizy Wt87YunkU (Todos meus outros ebooks)

https://drive.google.com/file/d/18GcrfBtk0CTiAzkiy0LgKXOy5OvgXjcy/view?usp=sharing (Guia de Conhecimento na área de TI recomendo!)

Material complementar – Iniciando Carreira em PenTest



Material complementar – Iniciando Carreira em PenTest



GUIA DO TI

O Guia do TI é um documento muito legal, recomendo bastante, segue o Download

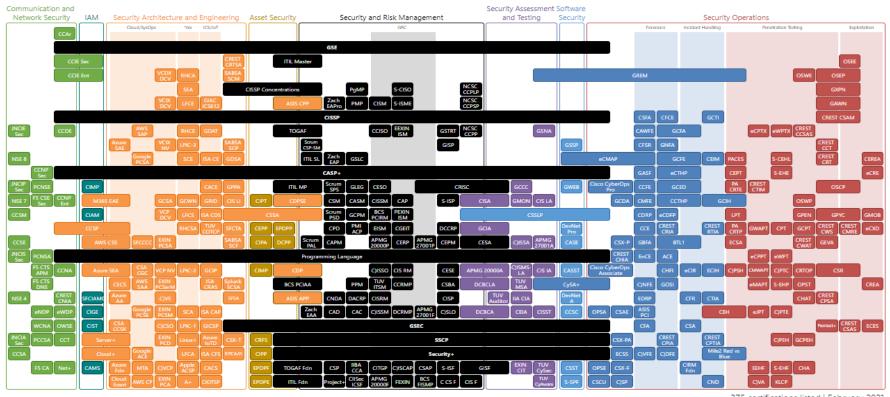
https://drive.google.com/file/d/18GcrfBtk0CTiAzki y0LgKXOy5OvgXjcy/view?usp=sharing

Criador da Obra: Jaime Linhares



SECURITY CERTIFIED ROADMAP

Roadmap com mais de 375 certificações de Sec https://github.com/sinecurelife/SecCertRoadmapHTML https://pauljerimy.com/security-certification-roadmap/



375 certifications listed | February 2021

LABORATÓRIOS

```
https://blueteamlabs.online/
https://www.hackthebox.eu/
https://www.vulnhub.com/
https://www.offensive-security.com/labs/
https://tryhackme.com/
http://vulnmachines.com/
https://pentesterlab.com/
+ Laboratórios aqui >>
https://github.com/michelbernardods/labs-pentest
```