ROADMAP – SEGURANÇA DA INFORMAÇÃO PT.1

JOAS ANTONIO

JOAS ANTONIO

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

JOAS ANTONIO

SEGURANÇA OFENSIVA

Conceitos de Ethical Hacking e contramedidas	Ameaça x Vulnerabilidade	Conhecimentos em Gestão de Vulnerabilidades	Conhecimentos em Administração de Sistemas (Linhas de Comandos, Hardening e Configurações de rede)	Hacking Tools
Conhecimentos em Ferramentas de Analise de Vulnerabilidade (SAST, DAST, IAST e etc)	C2M2, NIST, HIPAA, PCI-DSS, LGPD/GDPR	Conceitos de desenvolvimento seguro	Conhecimentos em Inteligência Cibernética e Resposta a Incidentes	Arquitetura e Soluções de Segurança da Informação
Tipos de Ameaças e Vetores de Ataques em diversos tipos de ambiente (Web, Infra, IoT, ISC, Wireless, Clouding, Mobile e etc.)	Gerenciamento, Analise e Tratamento de Riscos	Conhecimentos em Metodologias e Frameworks de PenTest (PTES, OSSTM, NIST, OWASP)	Conhecimentos em elaboração de relatórios técnicos e executivos	Conceitos de Segurança em Nuvem
Conhecimentos em Técnicas Avançadas de Enumeração, Scanning e Reconhecimento	Conhecimento em exploração e técnicas de evasão e bypassing de controles de segurança	Conhecimentos em Pós exploração, escalação de privilégios, persistência	Conhecimento de Matrix C2 e Operações Red Team	Conhecimentos em TTPs e Adversary Emulation
Conhecimentos em Forense Computacional e Eliminação de Rastros	Conhecimentos em Programação Baixo Nivel	Conhecimentos em Linguagens de alto nível e desenvolvimento de scripts para automatização	Conhecimentos em Buffer Overflow, Desenvolvimento de Exploits, Engenharia Reversa e Analise de Malware	Habilidades em CTFs e Desafios de Segurança Ofensiva

MATERIAL DE ESTUDO – FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

JOAS ANTONIO

Livros

- Gestão da Segurança da Informação - Uma Visão Executiva;
- Avaliação e Segurança de Redes;
- Fundamentos de Segurança da Informação com base na ISO 27001;
- Segurança da Informação Descomplicada;
- Resposta a Incidentes de Segurança da Informação;
- Criptografia e Segurança de Redes;
- Governança de Dados;
- Guia de Plano de Continuidade de Negócios;
- Gestão de Riscos com Controles Internos;
- The Official ISC2 Guide CISSP;
- Comptia Security+ Guide Exam;
- Alice and Bob Learn Application Security;
- Cyber Security: The Beguinner's Guide;
- Cyber Security Attack and Defense;
- Tratado da computação forense;
- Desvendando a Computação Forense;
- Forense em Redes de Computadores;
- Pericia Forense Digital: Guia prático;
- Livros de PenTest/Red Team (https://bit.ly/3ncK0Jt);

Certificação

- CSCU (ECCOUNCIL);
- CND (ECCOUNCIL);
- CSA (ECCOUNCIL);
- CEH (ECCOUNCIL);
- CTIA (ECCOUNCIL);
- ISO 27001 (EXIN);
- Cyber Security and IT Foudations (EXIN)
- Security+ (CompTIA);
- Network+ (CompTIA);
- SSCP (ISC2)
- CISSP (ISC2);
- Linux+ (CompTIA);
- CSSLP (ISC2);
- CySA+ (CompTIA);
- CRISC (ISACA);
- CISM (ISACA);
- CDPSE (ISACA);
- PDPF (Exin);
- OSCP (OffSec);
- eCPPT (eLearnsecurity);
- eWPTX (eLearnsecurity);
- OSEP (OffSec);
- GPEN (SANS);
- GSEC (SANS);
- GCIH (SANS);
- GNFA (SANS);

Treinamentos

- ACADITI
- CYBRARY
- NETACAD
- PLURALSIGHT
- UDEMY
- CODERED
- SEC4US
- GOHACKING
- EV.ORG.BR
- PENTESTACADEMY
- EDUONIX
- EDX
- COURSERA
- BRASILMAISTI
- MICROSOFT ACADEMY
- FUTURELEARN
- ELEARNSECURITY
- OFFENSIVE SECURITY
- SANS
- ECCOUNCIL

Conclusão

- Esse é um roadmap simples, para quem busca um cronograma de estudo, seja na área de PenTest, ou como um profissional de segurança de redes, um profissional de defesa cibernética ou até mesmo um generalista;
- Espero que seja útil para sua jornada, esse material ele complementa todos os outros que eu desenvolvi ao qual tem materiais complementares e outras dicas e pdfs para auxiliar nos seus estudos e que você pode conferir nesse link (https://bit.ly/3n8Ghgc);
- **Meu LinkedIn:** https://www.linkedin.com/in/joas-antonio-dos-santos/