

TÉCNICAS DE ATAQUE E DEFESA CIBERNÉTICA EM ACTIVE DIRECTORY

Ementa

Apresentar os conceitos e técnicas de ataque e defesa no ambiente cibernético das organizações. Abordar os componentes e a classificação de sistemas e as relações entre segurança cibernética e o ambiente de uma empresa, tratando de bases conceituais e filosóficas da área de sistema de informação (dado, informação, conhecimento) do ponto de vista da segurança da informação. Apresentar as dimensões tecnológicas, organizacional e humana e estudar métodos e técnicas que possibilitam a geração e a gestão da informação em sistemas computacionais como suporte do processo decisório no âmbito da segurança da informação.

Temas

1. Fundamentos de Red Team
2. Fundamentos de Active Directory
3. Acesso inicial
4. Exploração de vulnerabilidades
5. Técnicas de defesa (Blue Team)
6. Documentação técnica

Referências bibliográficas

- ALVES, M. de A. Crimes digitais: análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova. São Paulo: Dialética, 2020.
- JESUS, D. de. Manual de crimes informáticos. São Paulo: Saraiva, 2016.
- VERAS, M. Computação em nuvem: nova arquitetura de TI. Rio de Janeiro: Brasport, 2015.
- WEIMANN, G. Terrorism in cyberspace: the next generation. [S.l.]: Columbia University Press, 2015.