Faculdade IMPACTA	*Plano de Ensino*

Curso: **Análise e Desenvolvimento de Sistemas, Defesa Cibernética, Engenharia da Computação e Redes de Computadores**	
Nome da Disciplina:**Segurança Cibernética - Cyber Security**	
Carga Horária*:* **80 horas**	Aulas: **Teóricas-50%; Práticas-50%**
Docente: **Prof. Alex Sandro Silva Feitosa**	
Coordenação: **Prof. Dr. Bruno Lima**	

Ementa

- Ser capaz de elevar a postura e maturidade de segurança das organizações, adotando melhores práticas, métodos e ferramentas que aumentam a capacidade de defesa cibernética corporativa.
- Fornecer conscientização sobre as últimas ameaças cibernéticas que podem ajudar a entender, bem como estabelecer os fundamentos para a implementação de um time de respostas a incidentes e um centro de operações de segurança.

Competências

Ao final da disciplina o aluno será capaz de:

- Analisar as tendências e indústrias que mais são alvos de ataques cibernéticos.
- Explorar como os cyber criminosos estão usando as ferramentas para ganhar controle de sistemas.
- Revelar por que cyber criminosos estão mudando suas técnicas para ganhar benefícios ilegais.
- Determinar quais passos você deve fazer para proteger sua empresa contra as ameaças.
- Conhecer as ferramentas utilizadas por pentesters e hackers éticos (ferramentas CLI, Telnet, SSH, Nmap, Wireshark e outras).
- Manipular soluções de segurança em alta demanda.
- Ganhar prática do mundo real em frameworks e metodologias de modelagem de ameaças críticas.
- Entender o que é um Centro de Operações de Segurança (SOC).

Habilidades

- Instalar máquinas virtuais para criar um ambiente seguro para implementar e analisar eventos de ameaças à segurança cibernética.
- Explicar a função do analista de operações de segurança cibernética na empresa.
- Explicar os recursos e as características do sistema operacional Windows necessários para oferecer suporte às análises de segurança cibernética.
- Explicar os recursos e as características do sistema operacional Linux.
- Analisar a operação de protocolos e serviços de rede.
- Explicar a operação da infraestrutura de rede.
- Classificar os vários tipos de ataques à rede.
- Usar ferramentas de monitoramento de rede para identificar ataques contra protocolos e serviços de rede.
- Explicar como evitar o acesso mal-intencionado a redes, hosts e dados de computadores.
- Explicar os impactos da criptografia no monitoramento de segurança de rede.
- Explicar como investigar vulnerabilidades e ataques de endpoints.
- Avaliar os alertas de segurança de rede.
- Analisar dados de invasão de rede para identificar hosts e vulnerabilidades comprometidos.
- Aplicar modelos de resposta a incidentes para gerenciar incidentes de segurança de rede.

Disciplinas Relacionadas

FACULDADE IMPACTA TECNOLOGIA.
Rua Cubatão, 726 – Vila Mariana. São Paulo – SP – CEP 04013-002. Fone (0xx11) 5593-5344.
Site: www.impacta.edu.br

- **Pré – Requisitos:** Arquiteturas e Tecnologias em Segurança de Informação.
- **Requisito Paralelo:** Administração de Redes com Sistemas Operacionais Livres.
- **Requisito Posterior:** Segurança de redes e infraestrutura; Técnicas de Ataque e Defesa Cibernética.

Conteúdo Programático

- Unidade 01 – O Perigo do Mundo Digital
  - Um pouco sobre segurança cibernética
    - Carreira nas operações da segurança cibernética
  - Arquitetura do Sistema Operacional Windows e Linux
    - Como os Protocolos viabilizam as operações das redes
  - Funcionamento dos protocolos Ethernet e IP
    - Verificação de Conectividade
- Unidade 02 – Como os dispositivos e serviços de rede são usados para melhorar a segurança da rede
  - Analisar a PDU do protocolo ARP
    - Entendendo como a camada de transporte trabalha
    - Conhecendo alguns serviços de rede
  - Comunicação sem fio
  - Segurança da infraestrutura de rede
- Unidade 03 – Como as redes são atacadas
  - Evolução das Ameaças
    - Tipos de malwares
  - Monitorando o tráfego de rede
    - Como as vulnerabilidades do TCP/IP possibilitam os ataques às redes
  - Noções básicas sobre defesa
    - Controles de Acesso
    - Usar várias fontes de inteligência para localizar as ameaças à segurança atuais
    - Criptografia
- Unidade 04 – Tipos de proteção e respostas a incidentes
  - Proteção de endpoints
    - Como as vulnerabilidades de endpoints são avaliadas e gerenciadas
    - Common Vulnerability Scoring System (CVSS)
    - Comportamento dos protocolos de rede comuns no contexto do monitoramento de segurança.
  - Tipos de dados de segurança
    - Processo para avaliação de alertas
    - Interpretar dados para determinar a origem de um alerta
    - Investigação dos dados de rede
    - Papel dos processos de computação forense digital.
  - Frameworks
    - Etapas na Cyber Kill Chain
    - Diamond Model
    - tratamento de incidentes do NIST 800-61r2

Metodologia de ensino

- Aulas gravadas nas quais se apresenta e discute os tópicos da disciplina, bem como trabalhos em grupo com apresentação escrita e defesa oral, apresentação de vídeos.
- Atividades contínuas (AC) diárias para acompanhamento do processo ensino aprendizagem.

FACULDADE IMPACTA TECNOLOGIA.
Rua Cubatão, 726 – Vila Mariana. São Paulo – SP – CEP 04013-002. Fone (0xx11) 5593-5344.
Site: www.impacta.edu.br

Bibliografia Básica (até 3 livros, padrão ABNT)

- Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate** v1, 2020 https://www.netacad.com.
- SÊMOLA, Marcos**. Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.
- NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.
- THOMAS, Tom. **Segurança de redes: primeiros passos**. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

Bibliografia Complementar (demais obras utilizadas)

- BEAL, A. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.
- STALLINGS, W. **Network security: applications and standards**. 3.nd. New Jersey: Prentice Hall, 2006.
- **ASSOCIAÇÃO Brasileira de Normas Técnicas. NBR ISO/IEC 27001 E 27002** Tecnologia da informação.
- WADLOW, Thomas A. **Segurança de redes: projeto e gerenciamento de redes seguras**. Rio de Janeiro: Campus, 2000.

FACULDADE IMPACTA TECNOLOGIA.
Rua Cubatão, 726 – Vila Mariana. São Paulo – SP – CEP 04013-002. Fone (0xx11) 5593-5344.
Site: www.impacta.edu.br

Plano de aulas	
Parte	**Conteúdo**
1	Um pouco sobre segurança cibernética
2	Arquitetura do Sistema Operacional Windows e Linux
3	Como os Protocolos viabilizam as operações das redes
4	Analisar a PDU do protocolo ARP
5	Comunicação sem fio
6	Segurança da infraestrutura de rede
7	Evolução das ameaças
8	Monitorando o tráfego de rede
9	Noções básicas sobre defesa
10	Proteção de endpoints
11	Tipos de dados de segurança
12	Frameworks

FACULDADE IMPACTA TECNOLOGIA.
Rua Cubatão, 726 – Vila Mariana. São Paulo – SP – CEP 04013-002. Fone (0xx11) 5593-5344.
Site: www.impacta.edu.br