INSTITUTO POLITÉCNICO DE BRAGANÇA

Unidade Curricular	Análise de Vulnerabilidades	Área Científica	Ciências Informáticas
CTeSP em	Cibersegurança	Escola	Escola Superior de Tecnologia e de Gestão de Bragança
Ano Letivo	2022/2023	Ano Curricular	1
Nível	0-1	Créditos ECTS	3.0
Tipo	Semestral	Semestre	2
Código	4087-712-1005-00-22		

Horas totais de trabalho	81	Horas de Contacto	T -	TP 7	PL 23	TC -	S -	E -	OT -	O -

T - Ensino Teórico; TP - Teórico Prático; PL - Prático e Laboratorial; TC - Trabalho de Campo; S - Seminário; E - Estágio; OT - Orientação Tutórica; O - Outra

Nome(s) do(s) docente(s): Tiago Miguel Ferreira Guimaraes Pedrosa, Rui Alexandre Coelho Alves

Resultados da aprendizagem e competências

No fim da unidade curricular o aluno deve ser capaz de:
1. Identificar as boas práticas de segurança na configuração e gestão de sistemas e rede.
2. Identificar vulnerabilidades em equipamentos de redes e sistemas.
3. Interpretar fontes de informação pública sobre vulnerabilidades e ameaças conhecidas.
4. Compreender e analisar as vulnerabilidades mais comuns presentes em soluções web.
5. Aplicar técnicas, baseadas em agentes e sondas, para deteção de vulnerabilidades de segurança em sistemas e rede.
6. Utilizar ferramentas de busca, análise e exploração de vulnerabilidades em redes e sistemas e interpretar os resultados obtidos.

Pré-requisitos

Não aplicável

Conteúdo da unidade curricular

Boas práticas de segurança na configuração e gestão de sistemas e redes. Fontes de informação públicas sobre vulnerabilidades e ameaças conhecidas. Vulnerabilidades mais comuns em soluções web. Aplicação de técnicas, baseadas em agentes e sondas, a para deteção de vulnerabilidades de segurança em sistemas e redes. Ferramentas de procura, análise e exploração de vulnerabilidades em redes e sistemas e interpretação dos resultados obtidos.

Conteúdo da unidade curricular (versão detalhada)

1. Fontes de informação sobre vulnerabilidades, ameaças e erros de configuração mais comuns.
2. Compreender as vulnerabilidades associadas a aplicações web.
3. Boas práticas de configuração de sistemas, redes e serviços.
4. Soluções de monitorização continua para deteção de vulnerabilidades de segurança em sistemas e rede.
5. Ferramentas de busca, análise e exploração de vulnerabilidades.

Bibliografia recomendada

1. G. Najera-Gutierrez. Kali Linux Web Penetration Testing Cookbook. Packt Publishing - ebooks Account, 2 2016.
2. R. W. Beggs. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing - ebooks Account, 5 2014.
3. V. Ramachandran and C. Buchanan. Kali Linux: Wireless Penetration Testing Beginner's Guide. Packt Publishing - ebooks Account, 2 edition, 3 2015.
4. B. Lhotsky. Instant OSSEC Host-based Intrusion Detection System. Packt Publishing, 7 2013.

Métodos de ensino e de aprendizagem

Exposição teórica dos conceitos acompanhada de demonstrações. Resolução de exercícios práticos. Período não presencial: Estudo individual e em grupo da matéria abordada.

Alternativas de avaliação

- Avaliaçã - (Ordinário, Trabalhador) (Final, Recurso, Especial)
  - Trabalhos Práticos - 20%
  - Exame Final Escrito - 40%
  - Projetos - 40%

Língua em que é ministrada

Português

Validação Eletrónica

Tiago Miguel Ferreira Guimaraes Pedrosa	José Luís Padrão Exposto	José Carlos Rufino Amaro
06-03-2023	17-03-2023	17-03-2023

Este documento só tem validade académica depois de autenticado, em todas as suas folhas, com o selo a óleo da Instituição.