INSTITUTO POLITÉCNICO DE BRAGANÇA

Unidade Curricular	Cibersegurança Ativa			Área Científica	Ciências Informáticas		
CTeSP em	Cibersegurança			Escola	Escola Superior de Tecnologia e Gestão de Bragança		
Ano Letivo	2022/2023	Ano Curricular	2	Nível	0-2	Créditos ECTS	3.0
Tipo	Semestral	Semestre	1	Código	4087-712-2002-00-22		

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, Miguel de Lacerda Pereira

Resultados da aprendizagem e competências

No fim da unidade curricular o aluno deve ser capaz de:
1. Descrever a resposta a incidentes na informática forense
2. Identificar evidências de incidentes
3. Utilizar ferramentas de análise e recolha de logs e salvaguarda
4. Utilizar sistemas de deteção e prevenção de intrusão e soluções de honeypots
5. Analise forense de redes e sistemas
6. Dotar sistemas e redes de capacidade de deteção, contenção e reação a ataques
7. Efetuar auditoria de segurança básica

Pré-requisitos

Antes da unidade curricular o aluno deve ser capaz de:
Ter bases sobre Redes de Computadores, Tecnologias de Comunicação e Segurança Informática.

Conteúdo da unidade curricular

Verificar os mecanismos de segurança na rede e sistemas, sugerindo pontos de melhoria e implementação de novos controlos para detetar, conter e reagir a possíveis ataques. Utilizar ferramentas de analise forense de redes e sistemas, bem como identificar evidências de incidentes.

Conteúdo da unidade curricular (versão detalhada)

1. Tratamento de ameaças
2. Resposta a incidentes
3. Verificação de robustez de sistemas de autenticação
4. Defesa em profundidade
5. Análise forense de redes e sistemas
6. Introdução à auditoria de segurança

Bibliografia recomendada

1. C. Sanders and J. Smith (2013). Applied Network Security Monitoring: Collection, Detection, and Analysis. Syngress, 1 edition.
2. C. Altheide and H. Carvey (2011). Digital Forensics with Open Source Tools. Syngress, 1 edition.
3. Oriyano (2016). CEH v9: Certified Ethical Hacker Version 9 Study Guide. Sybex, 3 edition.
4. J. T. Luttgens, M. Pepe, and K. Mandia (2014). Incident Response and Computer Forensics, Third Edition. McGraw-Hill Education, 3 edition.
5. EC-Council 2016. Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage (CHFI), 2nd Edition (Computer Hacking Forensic Investigator). Course Technology.

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

- Avaliação Normal - (Ordinário, Trabalhador) (Final, Recurso, Especial)
  - Trabalhos Práticos - 50% (Instalação de soluções de honeypot e de logs para identificar ameaças de cibersegurança.)
  - Trabalhos Práticos - 50% (Desenvolver relatório de análise forense de um artefacto associado a uma ameaça de cibersegurança.)

Língua em que é ministrada

Português, com apoio em inglês para alunos estrangeiros

Validação Eletrónica

Tiago Miguel Ferreira Guimaraes Pedrosa	José Luís Padrão Exposto	Paulo Alexandre Vara Alves
30-09-2022	30-09-2022	05-11-2022