

Unidade Curricular	Projeto Integrado III		Área Científica	Ciências Informáticas	
CTeSP em	Cibersegurança		Escola	Escola Superior de Tecnologia e Gestão de Bragança	
Ano Letivo	2020/2021	Ano Curricular	2	Nível	0-2
Tipo	Semestral	Semestre	1	Créditos ECTS	9.0
			Código	4087-712-2006-00-20	
Horas totais de trabalho	243	Horas de Contacto	T -	TP -	PL -
			TC -	S -	E -
			OT 90	O 153	

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

Nome(s) do(s) docente(s) Tiago Miguel Ferreira Guimaraes Pedrosa, Nuno Gonçalves Rodrigues, Rui Pedro Sanches de Castro Lopes, Tomas Oliveira Perestrelo de Lima

Resultados da aprendizagem e competências

No fim da unidade curricular o aluno deve ser capaz de:

1. Implementar um projeto integrado de segurança da infra-estrutura IT, configurando soluções para defesa em profundidade.
2. Simulação de redes de sensores e de outros dispositivos IoT.
3. Instalar e configurar sistemas de deteção e prevenção de intrusão combinados com honeypots.
4. Compreender e implementar soluções centralizadas de registos de sistemas e redes para facilitar a análise de evidências, e de informação e eventos de segurança.
5. Utilizar diversas ferramentas e abordagens para determinar possíveis ameaças de segurança a sistemas, serviços, redes e aplicações.
6. Identificar possíveis formas de mitigar as ameaças encontradas em cenários reais e simulados.
7. Testar técnicas de metodologias de análise forense recorrendo a ferramentas de simulação.
8. Utilizar cenários virtuais para testar abordagens de proteção e ataques, analisando a capacidade de resposta individual, da equipa e da organização no que concerne a cibersegurança e ciberdefesa.

Pré-requisitos

Antes da unidade curricular o aluno deve ser capaz de:

Conhecimentos básicos de sistemas operativos e de redes de computadores

Conteúdo da unidade curricular

Projeto integrado de segurança da infra-estrutura IT. Implementar defesa em profundidade, recorrendo quando necessário ao robustecimento da rede e sistemas. Simulação de redes de sensores e de outros dispositivos IoT. Analisar as possíveis ameaças nos cenários propostos, ou existentes, sejam eles reais ou simulados, propondo e implementando soluções de mitigação. Simular operações de cibersegurança e ciberdefesa.

Conteúdo da unidade curricular (versão detalhada)

1. Componente específico de cada projeto, com integração multidisciplinar das competências adquiridas.
2. Módulos auxiliares que se considerem pertinentes ao desenvolvimento do projeto.

Bibliografia recomendada

1. Cisco Networking Academy (2019). CCNA Security 2. 01, Cisco Systems.
2. B. Clark (2014). The Red Team Field Manual (RTFM). CreateSpace Independent Publishing Platform.
3. D. Murdoch (2014). Blue Team Handbook: Incident Response Edition: a Condensed Field Guide for the Cyber Security Incident Responder. CreateSpace Independent Publishing.
4. J. M. Stewart, M. Chapple, and D. Gibson (2015). CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide. Sybex, 7 edition, 9.
5. Oriyano (2016). CEH v9: Certified Ethical Hacker Version 9 Study Guide. Sybex, 3 edition, 5.

Métodos de ensino e de aprendizagem

Será usada uma metodologia pedagógica baseada em projetos (PBL) com a definição inicial de um problema base. Este será definido conjuntamente com os alunos, professores de outras unidades curriculares e com a comunidade. O professor intervém em todas as fases de forma a manter a motivação, ajudar a enquadrar os temas de investigação e desenvolver o conhecimento nos alunos.

Alternativas de avaliação

- Projeto - (Ordinário, Trabalhador) (Final, Recurso, Especial)

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
30-10-2020	11-11-2020	14-11-2020