Unidade Curricular	Projeto Integrado II			Área Científica	Ciências Informáticas		
CTeSP em	Cibersegurança			Escola	Escola Superior de Tecnologia e de Gestão de Bragança		
Ano Letivo	2023/2024	Ano Curricular	1	Nível	0-1	Créditos ECTS	9.0
Tipo	Semestral	Semestre	2	Código	4087-712-1015-00-23		

Horas totais de trabalho	243	Horas de Contacto	T	-	TP	-	PL	-	TC	-	S	-	E	-	OT	90	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): Nuno Gonçalves Rodrigues, Rui Pedro Sanches de Castro Lopes, Tiago Miguel Ferreira Guimaraes Pedrosa

Resultados da aprendizagem e competências

No fim da unidade curricular o aluno deve ser capaz de:
1. Instalar e gerir infraestruturas de rede locais e de área alargada, em organizações de pequena dimensão, de forma segura.
2. Instalar e gerir sistemas locais e de rede seguindo procedimentos seguros.
3. Definir políticas de segurança com aplicação no contexto.
4. Instalar e configurar sistemas e redes de acordo com as políticas de segurança definidas e de forma segura.
5. Implementar a segmentação de redes e instalar e configurar serviços de rede de forma segura.
6. Simular os cenários de configuração de rede local e empresarial.
7. Verificar a segurança do cenário implementado identificado as ameaças por forma a mitigá-las.
8. Utilizar ferramentas de recolha e tratamento de informação e evidências.

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

Simular diversos cenários de rede de forma a averiguar a eficácia de soluções seguras. Instalação e configuração de sistemas e redes de forma segura. Instalar e configurar serviços de infraestrutura. Utilizar ferramentas de identificação automática de vulnerabilidades e efetuar a sua análise. Uso de ferramentas para agregação e análise de evidências.

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. Hubbard, D. W. , & Seiersen, R. (2016). How to measure anything in cybersecurity risk. Hoboken: Wiley.
2. Diogenes, Y. , & Ozkaya, E. (2018). Cybersecurity, attack and defense strategies infrastructure security with Red Team and Blue Team tactics.
3. Andriesse, D. (2019). Practical binary analysis: build your own Linux tools for binary instrumentation, analysis, and disassembly. San Francisco: No Starch Press, Inc.
4. Será indicada a biliografia mais indicada para cada projeto proposto

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

Nuno Gonçalves Rodrigues, Rui Pedro Sanches de Castro Lopes, Tiago Miguel Ferreira Guimaraes Pedrosa	José Luís Padrão Exposto	José Carlos Rufino Amaro
20-02-2024	20-02-2024	25-02-2024