

Unidade Curricular	Projeto Integrado III		Área Científica	Ciências Informáticas	
CTeSP em	Cibersegurança		Escola	Escola Superior de Tecnologia e Gestão de Bragança	
Ano Letivo	2019/2020	Ano Curricular	2	Nível	0-2
Tipo	Semestral	Semestre	1	Créditos ECTS	6.0
Horas totais de trabalho	162	Horas de Contacto	T - TP - PL - TC - S - E - OT - O -	Código	4087-639-2105-00-19

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) 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 média dimensão, de forma segura.
2. Implementar a segmentação de redes.
3. Instalar e configurar serviços de rede de forma segura.
4. Simular os cenários de configuração de rede local e de área alargada.
5. Verificar a segurança do cenário implementado identificado as ameaças por forma a mitigá-las.
6. 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

Simulação de diversos cenários de rede de forma a averiguar a eficácia de soluções seguras. Simulação de redes de sensores e de outros dispositivos IoT. Instalação e configuração serviços de infraestrutura. Utilização ferramentas de identificação automática de vulnerabilidades.

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. Sanders, C. & Smith, J. (2014). Applied network security monitoring : collection, detection, and analysis. Elsevier

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	Paulo Alexandre Vara Alves
29-10-2019	11-11-2019	13-11-2019