

Unidade Curricular	Wargaming	Área Científica	Ciências Informáticas
CTeSP em	Cibersegurança	Escola	Escola Superior de Tecnologia e de Gestão de Bragança
Ano Letivo	2023/2024	Ano Curricular	2
Nível	0-2	Créditos ECTS	3.0
Tipo	Semestral	Semestre	1
Código	4087-712-2009-00-23		
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

Resultados da aprendizagem e competências

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

- Desenvolver os procedimentos de segurança de informação de acordo com o tipo de ameaças e incidentes
- Caracterizar os diversos tipos de operações em redes e sistemas no contexto da cibersegurança e ciberdefesa
- Instalar e parametrizar ferramentas e soluções para garantir a cibersegurança e ciberdefesa em ambiente simulado virtual
- Compreender a filosofia e métodos dos atacantes
- Utilizar técnicas e ferramentas de testes de intrusão.
- Testar diversas situações de ataque e abordagens de defesa e analisar a capacidade de resposta individual, da equipa e da organização.
- Experiência em exercícios de simulação ("Capture The Flag" e "Red and Blue")

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

Simular em ambiente virtual cenários para testar diversas abordagens de proteção e ataques que possam surgir e analisar a capacidade de resposta individual, da equipa e da organização.

Conteúdo da unidade curricular (versão detalhada)

- Aspetos diferenciadores da cibersegurança e ciberdefesa
- Operações de segurança em redes de computadores
- A cadeia de ataque
- Pensar como o atacantes (Penetration testing)
- Desenvolvimento de cenários de cibersegurança e ciberdefesa.
- Exercícios de simulação

Bibliografia recomendada

- C. Buchanan (2014). Kali Linux CTF Blueprints. Packt Publishing.
- B. Clark (2014). The Red Team Field Manual (RTFM). CreateSpace Independent Publishing Platform.
- P. Kim (2015). The hacker playbook 2: Practical guide to penetration testing. Secure Planet LLC.
- D. Murdoch (2014). Blue Team Handbook: Incident Response Edition: a Condensed Field Guide for the Cyber Security Incident Responder. CreateSpace Independent Publishing.

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)
 - Exame Final Escrito - 35%
 - Trabalhos Práticos - 65% (Desafios de ataque e defesa de sistemas num cenário controlado.)

Língua em que é ministrada

Português, com apoio em inglês para alunos estrangeiros

Validação Eletrónica

Tiago Miguel Ferreira Guimaraes Pedrosa	José Luís Padrão Exposto	José Carlos Rufino Amaro
03-10-2023	03-10-2023	07-10-2023