INSTITUTO POLITÉCNICO DE BRAGANÇA

Unidade Curricular	Wargamming			Área Científica	Ciências Informáticas		
CTeSP em	Cibersegurança			Escola	Escola Superior de Tecnologia e de Gestão de Bragança		
Ano Letivo	2022/2023	Ano Curricular	2	Nível	0-2	Créditos ECTS	3.0
Tipo	Semestral	Semestre	1	Código	4087-712-2009-00-22		

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

Resultados da aprendizagem e competências

No fim da unidade curricular o aluno deve ser capaz de:
1. Desenvolver os procedimentos de segurança de informação de acordo com o tipo de ameaças e incidentes
2. Caracterizar os diversos tipos de operações em redes e sistemas no contexto da cibersegurança e ciberdefesa
3. Instalar e parametrizar ferramentas e soluções para garantir a cibersegurança e ciberdefesa em ambiente simulado virtual
4. Compreender a filosofia e métodos dos atacantes
5. Utilizar técnicas e ferramentas de testes de intrusão.
6. Testar diversas situações de ataque e abordagens de defesa e analisar a capacidade de resposta individual, da equipa e da organização.
7. 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)

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

Bibliografia recomendada

1. C. Buchanan (2014). Kali Linux CTF Blueprints. Packt Publishing.
2. B. Clark (2014). The Red Team Field Manual (RTFM). CreateSpace Independent Publishing Platform.
3. P. Kim (2015). The hacker playbook 2: Practical guide to penetration testing. Secure Planet LLC.
4. 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	Paulo Alexandre Vara Alves
30-09-2022	30-09-2022	05-11-2022