LABORATÓRIO DE TESTES DE INTRUSÃO

Pós-Graduação em Cibersegurança e Informática Forense

Código: 124004

Área Cientifica Predominante: Arquitetura de Computadores, Sistemas Distribuidos e Cibersegurança

Docente: Nuno Alberto Ferreira Lopes

Idioma de Instrução: Português

Regime: S2

Carga Letiva: 20h Carga Trabalho: 60h

ECTS: 3,0

Objetivos

Como principais objetivos da unidade curricular estão a passagem do conhecimento prático sobre sistemas, técnicas e teorias de testes de segurança e intrusão de sistemas e redes de comunicações tecnológicas.

Resultados da Aprendizagem

No final da unidade, os alunos deverao perceber os desafios e conseguir efetuar ataques, invasoes e exploracoes de vulnerabilidades em sistemas de informacao como meio de antecipacao desses mesmos ataques.

Deverao ainda conseguir criar programas que permitam extracao de informacao.

Conteúdos Programáticos

1 - Fundamentos de Pentest.

2 - Metodologia de PenTest;

3 - Ultrapassar Firewall e IDS com NMAP;

Bibliografia Recomendada

Georgia Weidman - Penetration Testing: A Hands-On Introduction to Hacking - Paperback NEW Weidman (ISBN: 978-159-327-564-8)

George Sammons - Kali Linux 2: Penetration testing for beginners (ISBN: 978-198-130-367-0)

Métodos de Ensino e de Aprendizagem

Os conteudos estao organizados de forma integrada, visando permitir a analise de perspectivas pertinentes para a intervencao educativa.

Parte-se de aspetos gerais de Pentesting (1.) para o estudo das metodologias de Pentesting (2.) e uma analise profundada das formas e meios de ultrapassar a seguranca ativa de rede (3.)

No conjunto, pretende promover-se a aquisicao de conhecimentos cientificos e praticos para o desenvolvimento de competencias profissionais.

Métodos de Avaliação

Entrega, apresentacao e defesa de trabalho pratico final (100%).