FORMAÇÃO AVANÇADA
EM CIBERSEGURANÇA

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

CACADEMY

PRR
Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia
NextGenerationEU

Nível E

Hacking e Testes de Penetração - Edição 22-06-2026 | ECTS

Universidade de Coimbra

70 horas / Online / 100€

Sinopse

Esta formação destina-se a todas as pessoas, portadoras de sólidos conhecimentos de redes, serviços, sistemas operativos e soluções de virtualização, que pretendam adquirir competências na execução de testes de penetração a redes e sistemas, com objetivo de integrar equipas de "Red Team".

Short bio do Formador

Bruno Sousa, é Professor Auxiliar no Departamento de Engenharia Informática da Universidade de Coimbra, Portugal, desde dezembro de 2018, onde obteve o doutoramento em Engenharia Informática na disciplina de Multihoming para redes baseadas em IP, em dezembro de 2014. É investigador sénior do Centro de Informática e Sistemas da UC (CISUC), onde iniciou a sua actividade em 2006. É autor de vários capítulos de livros, diversas publicações em revistas e conferências internacionais. Participou no TPC de diversas conferências. Participou em vários projetos de investigação europeus e nacionais, como IST FP6 Integrated Projects, EuQoS e WEIRD, ICT FP7, MobiTRUst, SALUS, Mobile Cloud Networking, LiveCity e FI-WARE, e H2020 EMPATIA. Os seus interesses de investigação incluem mecanismos de resiliência em redes e aplicações/serviços, e deteção e prevenção de intrusões em redes 5G e para Internet das Coisas (IoT).

Conteúdos Programáticos

Módulo 1 – Conceitos de Cibersegurança

- Definição de Cibersegurança Ativa e Defensiva
- Importância e Metodologia de um Teste de Penetração
- Anonimização
- Ferramentas e frameworks
- Ambiente laboratorial do curso

Módulo 2 – Pedido de Autorização

- Tópicos essenciais e facultativos a estar presentes num pedido de autorização
- A importância dos regulamentos e certificações
- Diferenças entre tipos e formatos de testes a realizar

Módulo 3 – Organização e elaboração de relatórios (Reporting)

- Organização e armazenamento da informação
- Estrutura de elaboração de um relatório de conformidade
- Estrutura de elaboração de relatório de footprinting
- Estrutura de elaboração de relatório de testes de penetração

Módulo 4 – Recolha pública de Informações (footprinting)

- Tipo de informação relevante a ser recolhida

- Definição e conceitos de footprinting
- Metodologia para a realização do footprinting
- Etapas na recolha e análise de informação
- Elaboração do relatório de footprinting

Módulo 5 – Acesso à rede (Network access)

- Conceitos gerais de redes, serviços e sistemas
- Conceitos gerais de protocolos e sistemas de acesso à rede
- Conceitos e metodologia de acesso à rede (network access)

Módulo 6 – Recolha e análise de informação (Sniffing)

- Conceitos gerais de protocolos de comunicação
- Conceitos e metodologia de recolha de dados (sniffing)
- Técnicas e métodos de análise de dados

Módulo 7 – Análise de sistemas e protocolos (scanning e enumeration)

- Conceitos e metodologia para determinar sistemas ativos e execução de mapeamentos de rede (scanning)
- Conceitos e metodologia para determinar portas de comunicação ativas (scanning)
- Conceitos e metodologia para determinar serviços, sistemas, protocolos e configurações (enumeration)
- Execução de análises às configurações implementadas (enumeration)

Módulo 8 – Análise de Vulnerabilidades

- Conceitos e tipo de vulnerabilidades
- Metodologias de análise de vulnerabilidades
- Técnicas e métodos de análise de vulnerabilidades

Módulo 9 – Ganhar Acesso

- Metodologias de exploração de vulnerabilidades
- Conceitos e metodologias de interceção de tráfego
- Conceitos e metodologias de cracking
- Conceitos e metodologias de testes de autenticação
- Conceitos e metodologia de utilização de exploits baseados em CVE

Módulo 10 – Análise de plataformas Web

- Conceitos e tipo de plataformas web
- Metodologias na análise de plataformas web
- Técnicas e métodos na análise de plataformas

Módulo 11 – Escalar Privilégios

- Conceitos e tipo de técnicas utilizadas para escalar privilégios
- Metodologias de escalonamento de privilégios
- Técnicas e métodos de escalar privilégios e soluções de mitigação

Módulo 12 – Engenharia Social

- Conceitos e tipo de técnicas de engenharia social
- Conceitos e tipos de malware e a sua utilização
- Metodologias de engenharia social
- Técnicas e métodos de execução de engenharia social e soluções de mitigação

Avaliação e Certificado

Para efetuar a avaliação é necessário estar presente em pelo menos 70% das sessões. Para obter o Certificado de Conclusão, requer igualmente a assiduidade mínima de 70% das sessões e obter pelo menos 9,5 valores na avaliação.

Pré-requisitos para quem vai frequentar a formação:

Sólidos conhecimentos de redes, serviços, sistemas operativos e soluções de virtualização; Familiarização em trabalho com linhas de comandos, desenvolvimento de scripts e sistemas virtuais são também uma mais-valia.
Observações: Não aplicável.

Calendário

Local	Dia	Horário	Formato
	22/6/2026	17:00-22:00	Online
	23/6/2026	17:00-22:00	Online
	24/6/2026	17:00-22:00	Online
	25/6/2026	17:00-22:00	Online
	26/6/2026	17:00-22:00	Online
	29/6/2026	17:00-22:00	Online
	30/6/2026	17:00-22:00	Online
	1/7/2026	17:00-22:00	Online
	2/7/2026	17:00-22:00	Online
	3/7/2026	17:00-22:00	Online
	6/7/2026	17:00-22:00	Online
	7/7/2026	17:00-22:00	Online
	8/7/2026	17:00-22:00	Online
	9/7/2026	17:00-22:00	Online