UNIVERSIDADE ABERTA
www.uab.pt

MICROCREDENCIAL EM CIBERSEGURANÇA OFENSIVA

alv Aprendizagem ao Longo da Vida

PRR Plano de Recuperação e Resiliência
REPUBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

“Conhece o teu inimigo e conhece-te a ti próprio
e em cem batalhas nunca serás derrotado.”

[SunTzu, A Arte da Guerra, 400 a.c.]

ÍNDICE

MICROCREDENCIAIS

Segundo com a Comissão Europeia, “microcredenciais” são qualificações que certificam resultados de aprendizagens resultantes de cursos curtos ou de módulos, tendo em vista a requalificação e atualização profissional de cada um. Estas qualificações podem ser obtidas pelos cidadãos com diversas modalidades de aprendizagem, presencial, a distância online ou mista.

Seja qual for o regime ou forma como são obtidas as qualificações, a Comissão Europeia vê nas microcredenciais uma oportunidade de aprendizagem flexível e inclusiva, no contexto dos sistemas de ensino e formação europeus e uma nova forma de acreditação adequada a diferentes necessidades.

Estas qualificações, por norma de curta duração, serão essencialmente úteis para quem pretende complementar o seu conhecimento e competências ou para quem pretende requalificar-se, procurando novas oportunidades no mercado de trabalho.

Na sua essência as microcredenciais assentam e dão resposta ao conceito e à prática de uma “aprendizagem ao longo da vida”.

ENQUADRAMENTO

Os testes de penetração são cruciais para a segurança de uma organização, uma vez que são estes que ajudam a empresa a aprender como lidar com qualquer tipo de invasão de um ator malicioso. Os testes de penetração servem como uma forma de examinar se as políticas de segurança de uma organização são genuinamente eficazes, e funcionam como uma espécie de simulação de uma situação real para as organizações. Os testes de penetração também podem fornecer soluções que ajudarão as organizações não apenas a prevenir e detetar atacantes, mas também tomar medidas para expulsar o atacante do sistema de uma forma eficiente.

Uma das principais preocupações das empresas atualmente é a avaliação do risco a que os seus negócios estão sujeitos numa situação de ciberataque. Os fatores a ter em consideração vão desde a perda de receitas, devido ao facto dos seus websites estarem inacessíveis, à perda de reputação e processos de indemnização resultantes de quebras de segurança que resultem na perda de dados confidenciais e pessoais dos seus clientes. É desta forma que os testes de penetração também podem oferecer solução a

estes problemas, ao oferecerem uma visão sobre quais canais nas organizações ou que aplicações apresentam maior risco e, portanto, em quais tipos de novas ferramentas de segurança a empresa deve investir ou que protocolos esta deve seguir. Esse processo pode ajudar a descobrir várias das principais deficiências do sistema, nas quais a empresa pode nem sequer ter pensado.

Os relatórios de teste de penetração também podem ajudar os desenvolvedores a cometer menos erros. Quando os desenvolvedores entendem exatamente como um ator mal-intencionado lançou um ataque a uma aplicação web, um sistema operativo ou outro software que ajudaram a desenvolver, estes ficarão mais dedicados a aprender mais sobre segurança e terão menos probabilidade de cometer erros semelhantes no futuro, adotando deste modo uma postura de desenvolvimento de código mais segura.

Esta microcredencial concentra-se nos detalhes técnicos e práticos necessários para o planeamento, realização e reporte de testes de penetração e identificação de vulnerabilidades. Destina-se a pessoas que queiram aprofundar os conhecimentos técnicos em cibersegurança, e especialmente que queiram iniciar-se no papel de *PenTester* para encontrar e testar as vulnerabilidades de uma organização e possuir a habilidade para comunicar as descobertas a públicos não técnicos.

Esta microcredencial inclui os aspetos legais, conceitos e metodologias relativas ao planeamento e execução de testes de penetração, utilização do Kali Linux, o processo de OSINT como contributo à estratégia de ataque, reconhecimento ativo, análise de vulnerabilidades, engenharia social, utilização da *framework* Metasploit, exploração web, exploração de redes e wireless, quebra de passwords e muito mais.

OBJETIVOS

O objetivo do curso é proporcionar conhecimentos e competências que permitam aos participantes realizar testes de penetração de forma metódica aos sistemas e redes de uma organização, para zelar pela autenticidade, integridade, confidencialidade, disponibilidade e não repúdio da informação. No final, os participantes saberão:

- Equacionar os aspetos legais e aplicar metodologias associadas aos testes de penetração;
- Planear, delimitar e reportar os resultados de um teste de penetração;
- Conduzir o processo de reconhecimento passivo e ativo;

- Usar o Kali Linux e a *framework* Metasploit, bem como outras ferramentas para a fase de exploração de vulnerabilidades;
- Proceder à exploração de servidores e aplicações Web;
- Usar ferramentas para a quebra de passwords;
- Exploração vulnerabilidades de rede e ataques relacionados com redes wireless.

COMPETÊNCIAS

Espera-se que os participantes adquiram as seguintes competências que lhes serão conferidas na no documento certificador desta Microcredencial:

- Compreender e conhecer os aspetos legais, a terminologia, conceitos e metodologias relativas ao planeamento, execução e reporte de testes de penetração;
- Aplicar técnicas de reconhecimento com fontes abertas (OSINT) em apoio à estratégia de ataque;
- Proceder ao reconhecimento ativo e passivo e utilizar ferramentas úteis para *scanning*, enumeração e análise de vulnerabilidades;
- Enquadrar a Engenharia Social enquanto técnica de ataque que explora o vetor humano, quer para obtenção de informações quer na fase de exploração;
- Compreender e empregar diferentes técnicas e ferramentas para explorar diversas vulnerabilidades de serviços e utilizadores;
- Experimentar e aplicar a *framework* Metasploit para exploração de vulnerabilidades e manutenção do acesso;
- Compreender e aplicar ataques aos tipos de vulnerabilidades web mais comuns, sendo o ranking OWASP Top 10;
- Empregar o uso da ferramenta Burp Suite para a realização de tarefas relacionadas com a exploração web;
- Distinguir e praticar a quebra de passwords online e offline;
- Compreender e aplicar os conceitos de redirecionamento, *spoofing* e Man-In-The-Middle (MITM);
- Compreender as vulnerabilidades e tipos de ataques wireless.

PROGRAMA E CONTEÚDOS

Esta microcredencial está estruturada em 8 módulos que se desenvolvem sequencialmente, com a duração de uma semana cada, A sua duração total é de 104 horas (volume de trabalho dos formandos) que correspondem 4 ECTS[1] da UAb e realiza-se em regime de formação a distância online, ao longo das 9 semanas.

MÓDULOS	DESCRIÇÃO
0. Ambientação ao contexto online	Módulo que pretende uma socialização dos participantes, a criação de "um grupo" de trabalho online e a familiarização com a utilização do software de gestão do curso.
1. Fundamentos e metodologias	Neste módulo pretende-se explicar os conceitos estruturantes das tecnologias e sistemas de informação e demonstrar a utilização das máquinas virtuais.
2. Reconhecimento com fontes abertas (OSINT)	Apresenta-se o processo de OSINT e mostrar como este é útil na definição de uma estratégia de ataque. Praticar a utilização de ferramentas tipicamente utilizadas em OSINT.
3. Reconhecimento ativo, vulnerabilidades e engenharia social	Conceitos relacionados com scanning e fingerprinting e ferramentas úteis. Descrever o processo de análise de vulnerabilidades e a utilização de ferramentas típicas (scanners de vulnerabilidades). A Engenharia Social como técnica de ataque.
4. Exploração (metasploit)	Descrever e aplicar os uso de ferramentas para a exploração de sistemas e clientes em ambiente Windows e Linux.
5. Exploração web	Identificar e descrever diferentes tipos de vulnerabilidades web conhecidas segundo o ranking OWASP Top 10.
6. Crack de passwords	Distinguir tipos de quebra de passwords quanto à sua forma e usar ferramentas para a quebra de passwords.
7. MITM spoofing, redirecionamento - Wireless	Conceitos de redireccionamento, spoofing e Man-In-The-Middle (MITM). Experimentar diversas ferramentas para a realização de ataques com base nos conceitos anteriormente aprendidos. Demonstrar vulnerabilidades e ataques relacionados com redes wireless.
8. Exercício final	Realização de um teste de penetração a um sistema num ambiente virtualizado e elaboração de um relatório com base nos resultados obtidos na condução do teste.

[1] O ECTS (Sistema Europeu de Transferência de Créditos) foi desenvolvido pela Comissão Europeia. Os créditos ECTS representam o volume de trabalho que o estudante/formando deve produzir. Na UAb 1 ECTS equivale a 26 horas de trabalho do formando.

MÓDULO 0: AMBIENTAÇÃO AO CONTEXTO ONLINE

[Duração: 13 horas | 1 semana]

1. A plataforma de ensino/aprendizagem da UAb, PlataformAbERTA
2. Treino na exploração das ferramentas e recursos da PlataformAbERTA

Objetivos do módulo

Alcançar uma socialização dos participantes, criar de "um grupo" de trabalho online e familiarizar os participantes com a utilização do software de gestão do curso (PlataformAbERTA que integra o *Learning Management System Moodle*, por forma a adquirirem as competências necessárias à exploração eficaz de todas as suas funcionalidades de intercomunicação, em especial as assíncronas, necessárias à frequência do curso.

Competências a adquirir

No final deste módulo, pretende-se que os participantes sejam capazes de:

- Interagir e comunicar com os colegas, com os formadores e com a interface de aprendizagem no sentido de conseguir resolver problemas básicos de interação, de comunicação;
- Explorar com eficácia todas as ferramentas e possibilidades da PlataformAbERTA, com o estatuto de formando;
- Pesquisar, selecionar e organizar informação a partir da Web para a transformar em conhecimento mobilizável;
- Pesquisar, organizar, tratar e produzir informação em função das necessidades, problemas a resolver e das situações.

MÓDULO 1: FUNDAMENTOS E METODOLOGIAS

[Duração: 13 horas teórico-práticas | 1 semana]

1. Conceitos fundamentais de redes e sistemas
2. Máquinas virtuais
3. Ambiente Linux (Kali)
4. Enquadramento dos testes de penetração
5. Prática em contexto de formação

Objetivos do módulo

Explicar os conceitos estruturantes das tecnologias e sistemas de informação. Demonstrar a utilização das máquinas virtuais e usar o Virtual Box em apoio ao ambiente

virtual para o curso. Praticar comandos em ambiente Linux (Kali). Discutir os aspetos legais e apresentar a terminologia, conceitos e metodologias relativas ao planeamento e execução de testes de penetração.

Competências a adquirir

- Perceber os elementos estruturantes das tecnologias e sistemas de informação;
- Instalar e utilizar um sistema operativo numa máquina virtual;
- Utilizar os principais comandos em ambiente Linux e conhecer o Kali Linux;
- Compreender os aspetos legais relativos aos testes de penetração;
- Perceber a terminologia e conceitos relacionados com o *Ethical Hacking*;
- Aplicar as metodologias enquadrantes dos testes de penetração.

MÓDULO 2: RECONHECIMENTO COM FONTES ABERTAS (OSINT)

[Duração: 13 horas teórico-práticas | 1 semana]

1. Recolha de informações sobre o alvo
2. Ferramentas e técnicas de OSINT
3. Recomendações para limitar a exposição
4. Prática de encriptação em contexto de formação

Objetivos do módulo

Apresentar o processo de OSINT e mostrar como este é útil na definição de uma estratégia de ataque.

Praticar a utilização de ferramentas tipicamente utilizadas em OSINT.

Saber realizar algumas técnicas de reconhecimento através de fontes abertas na internet.

Compreender como limitar a exposição individual e/ou da organização.

Competências a adquirir

- Utilizar ferramentas típicas de OSINT (e.g.Maltego, Shodan, TheHarvester, etc.);
- Compreender e aplicar diferentes técnicas de obter informações em fontes abertas;
- Conseguir compilar a informação recolhida em fontes abertas de forma útil e clara para as fases seguintes de um teste de penetração;
- Criar estratégias de ataque partindo de informações obtidas em fontes abertas;
- Adotar uma postura que reduza o potencial da informação publicada na internet, do próprio ou da organização, a ser utilizada para fins maliciosos.

MÓDULO 3: RECONHECIMENTO ATIVO, VULNERABILIDADES E ENGENHARIA SOCIAL

[Duração: 13 horas teórico-práticas | 1 semana]

1. Scanning/enumeração e fingerprinting
2. Análise de vulnerabilidades
3. Engenharia social
4. Prática em contexto de formação

Objetivos do módulo

Apresentar os conceitos relacionados com scanning/enumeração e fingerprinting. Identificar e utilizar um conjunto de ferramentas úteis na fase de scanning e enumeração. Descrever o processo de análise de vulnerabilidades e a utilização de ferramentas típicas (scanners de vulnerabilidades).

Enquadrar a Engenharia Social enquanto técnica de ataque que explora o vetor humano, quer para obtenção de informações na fase de reconhecimento ativo, quer na fase de exploração.

Competências a adquirir

- Utilizar ferramentas e técnicas para descobrir e enumerar os dispositivos e hosts numa rede;
- Compreender em que consiste o fingerprinting para obter informação sobre os serviços e sistemas, quer seja de forma manual ou automatizada através de ferramentas;
- Aplicar um conjunto de ferramentas de análise de vulnerabilidades para melhorar a capacidade de prevenção, sabendo identificar e priorizar os resultados;
- Valorizar o potencial da Engenharia Social nas diversas fases de um ataque.

MÓDULO 4: EXPLORAÇÃO (METASPLOIT)

[Duração: 13 horas teórico-práticas | 1 semana]

1. Netcat - Aprender a utilizar o canivete suíço do TCPIP
2. Utilização da framework Metasploit em Server-Side
3. Prática em contexto de formação

Objetivos do módulo

Descrever e aplicar os uso de ferramentas para a exploração de sistemas (server-side) e clientes (client-side) em ambiente Windows e Linux.

Usar a framework Metasploit e a ferramenta netcat com diferentes tipos de exploits.

Experimentar as diferentes funcionalidades da shell meterpreter.

Competências a adquirir

- Aplicar a ferramenta netcat para estabelecer uma shell, transferir ficheiros e realizar um scan à rede;
- Experimentar e usar a framework Metasploit. Selecionar diferentes tipos de exploits e aplicar a correta configuração para a execução do ataque;
- Escolher uma entre várias sessões ativas e realizar a migração de uma shell para meterpreter;
- Usar diferentes as diversas funcionalidades do meterpreter;
- Criar payloads com o msfvenom e outras ferramentas semelhantes;
- Criar um ficheiro apk malicioso para exploração em ambiente android;
- Aplicar técnicas de exploração a browsers de clientes;
- Usar módulos adicionais da shell meterpreter.

MÓDULO 5: EXPLORAÇÃO WEB

[Duração: 13 horas teórico-práticas | 1 semana]

1. Aplicações web - exploração de falhas em websites
2. Webshells, comprometimento de aplicações web
3. Análise de vulnerabilidades de aplicações web
4. Prática em contexto de formação

Objetivos do módulo

Identificar e descrever diferentes tipos de vulnerabilidades web conhecidas segundo o ranking OWASP Top 10.

Empregar o uso da ferramenta Burp Suite Community Edition e explicar as suas diversas componentes e funcionalidades.

Aplicar a ferramenta sqlmap para ataques de sql injection.

Aplicar o conhecimento adquirido na realização de ataques sql injection, Cross-Site Scripting e Cross Site Request Forgery.

Empregar o uso de técnicas de análise de vulnerabilidades em ambiente web.

Competências a adquirir

- Aplicar os conceitos referentes às vulnerabilidades mais comuns segundo o ranking OWASP Top 10;
- Empregar a ferramenta Burp Suite, assim como fazer uso das suas componentes e funcionalidades;

- Aplicar a ferramenta sqlmap para ataques a vulnerabilidades de SQL injection;
- Usar conhecimentos adquiridos para a exploração de vulnerabilidades de SQL injection, XSS e CSRF;
- Usar técnicas de evasão para o upload de ficheiros maliciosos em ambiente web;
- Usar ferramentas de análise de vulnerabilidade para identificar vulnerabilidades web.

MÓDULO 6: CRACK DE PASSWORDS

[Duração: 13 horas teórico-práticas | 1 semana]

1. Quebra de passwords forma online
2. Quebra de passwords forma offline
3. Serviços web online e rainbow tables
4. Prática em contexto de formação

Objetivos do módulo

Distinguir tipos de quebra de passwords quanto à sua forma.

Empregar o uso de ferramentas para a quebra de passwords.

Compreender o conceito de hashes e de rainbow tables.

Competências a adquirir

- Distinguir quebra de passwords de forma online de quebra de passwords de forma offline;
- Empregar o uso da ferramenta Burp Suite para a quebra de passwords online;
- Empregar ferramentas como a Hydra ou a Medusa para a quebra de passwords online;
- Criar uma lista de palavras com recurso à ferramenta Crunch;
- Usar as ferramentas JohnTheRipper e HashCat para a quebra de passwords offline;
- Compreender o conceito de rainbow tables.

MÓDULO 7: MITM SPOOFING, REDIRECIONAMENTO - WIRELESS

[Duração: 13 horas teórico-práticas | 1 semana]

1. Rede Local - Redirecionamento, Spoofing e MITM
2. Wireless - Introdução a Vulnerabilidades Gerais
3. Wireless - Captura e cracking de chaves de acesso
4. Prática em contexto de formação

Objetivos do módulo

Explicar os conceitos de redireccionamento, spoofing e Man-In-The-Middle (MITM).

Experimentar diversas ferramentas para a realização de ataques com base nos conceitos anteriormente aprendidos.

Explicar e demonstrar vulnerabilidades e ataques relacionados com redes wireless.

Competências a adquirir

- Explicar os conceitos de redirecionamento, spoofing e MITM;
- Aplicar técnicas de envenenamento de dispositivos em redes através de arp spoofing;
- Empregar técnicas de DNS spoofing para a captura de credenciais em rede;
- Empregar ferramentas para a captura de tráfego em rede de protocolos não cifrados;
- Explicar vulnerabilidades e diferentes tipos de ataques wireless;
- Definir o modo de monitorização para redes wireless com recurso a ferramentas para o efeito;
- Aplicar técnicas para contornar proteções relacionadas com endereços MAC;
- Usar ataques de negação de serviço (DoS) em redes wireless;
- Empregar ferramentas para a captura de IVs e chaves em redes WEP;
- Empregar ferramentas para a captura de handshakes em redes WPA;
- Aplicar técnicas para a quebra de chaves WPA;
- Identificar e usar técnicas para a exploração de routers com a funcionalidade WPS ativa.

MÓDULO 8: EXERCÍCIO FINAL

[Duração: 13 horas teórico-práticas | 1 semana]

1. Teste de penetração
2. Relatório

O exercício final consiste na realização de um teste de penetração a um sistema num ambiente virtualizado, e na elaboração de um relatório com base nos resultados obtidos na condução do teste, que deverá ser submetido online, para poder ser visualizado, analisado, avaliado e classificado pelos formadores. Este trabalho tem por objetivo a aplicação dos conhecimentos e competências adquiridas ao longo de todo a microcredencial.

O trabalho final é de realização obrigatória. A sua não realização implica a não aprovação

no curso. O trabalho final escrito é objeto de classificação quantitativa e, para aprovação no curso, a classificação deste trabalho deve ser igual ou superior a 9,5 valores, numa escala de 0 a 20.

Destinatários

São destinatários desta microcredencial:

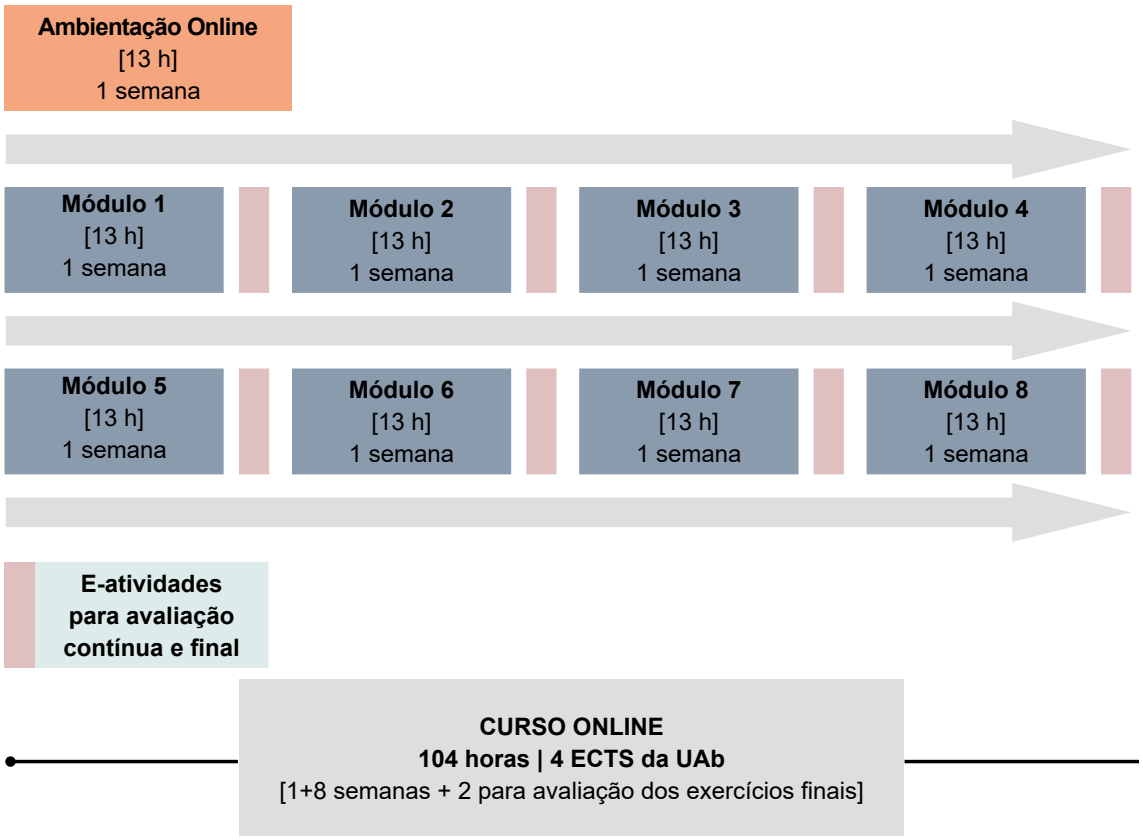
- Profissionais que trabalham na área de IT ou cibersegurança das empresas/ organizações e desejem aprofundar os conhecimentos na área da análise de vulnerabilidades e testes de penetração para melhor protegerem as redes e sistemas;
- Profissionais que pretendam iniciar-se numa carreira de PenTester;
- Indivíduos que desejem iniciar uma especialização em testes de penetração para poderem desempenhar a função de PenTester e integrar equipas de auditoria a organizações/empresas.

Além da necessária motivação e interesse ou necessidade do curso os participantes devem possuir:

- Habilitações mínimas ao nível do 12.º ano ou equivalente;
- Computador com pelo menos 8GB de memória RAM e 50 GB de espaço em disco disponível;
- Conhecimentos e prática de informática como utilizadores;
- Uma conta de correio eletrónico ativa e prática na sua utilização;
- Disponibilidade de tempo mínima de13 horas por semana.

Estrutura

A duração total da microcredencial é de 104 horas (volume de trabalho dos formandos) e está estruturada em 8 módulos de realização sequencial, precedidos de um módulo 0 de Ambientação ao Contexto Online do curso.



METODOLOGIA

A metodologia seguida neste curso é a estabelecida no Modelo Pedagógico Virtual da UAb para ações de aprendizagem ao longo da vida a desenvolver em regime de e-learning, e adota o modelo de ensino/aprendizagem de 5 níveis de que nos fala Gilly Salmon (2000).

A forma de trabalho utilizada neste curso compreende (1) a leitura e reflexão individuais dos conteúdos disponibilizados ou de outros sobre os mesmos temas obtidos pelos formandos, (2) a partilha da reflexão e do estudo com os colegas, assim como também (3) o esclarecimento de dúvidas nos fóruns moderados pelo formador e a (4) realização das e-atividades propostas.

A leitura e a reflexão individuais devem acontecer ao longo de todo o processo de aprendizagem e sem elas o formando fica muito limitado na sua participação nos fóruns previstos, assim como também dificilmente poderá realizar com sucesso as atividades programadas.

A aprendizagem está estruturada por Tópicos que correspondem a módulos do curso.

Em cada Tópico será criado um fórum moderado pelo formador para esclarecimento das dúvidas e ultrapassagem das dificuldades sentidas e apresentadas pelos formandos, proporcionando assim uma possibilidade de interação permanente dos formandos entre si e com o formador. Todos os fóruns decorridos permanecerão abertos ao longo de todo o curso, possibilitando assim a consulta a todo o tempo das mensagens trocadas. No entanto, quaisquer mensagens enviadas depois de terminado o módulo em que o fórum de discussão decorreu não serão consideradas pelos professores para efeitos de classificação da participação nesse fórum.

No módulo 0 e de acordo com o modelo de ensino/aprendizagem de Salmon cumprem se os níveis 1 e 2, respetivamente “acesso e motivação” e a “socialização online”; dependendo do grupo concreto de formandos iniciar-se-á ou não o nível 3 de “processamento de conteúdos” onde a tutoria se consubstancia no apoio na utilização de materiais pedagógicos e nas tarefas, nesta fase apenas em relação ao modo como fazer pesquisa orientada em WWW.

Nos módulos seguintes cumprem-se todos os restantes níveis do modelo de Gilly Salmon, “processamento de conteúdos” centrado na interação com os materiais de aprendizagem e com os restantes participantes do curso (colegas e formadores), “construção do conhecimento” onde é natural que o papel do formador se dilua e “exploração”, nível onde o suporte técnico disponibiliza novas fontes de informação e a tutoria dá apoio e resposta a questões.

Em dados momentos do curso os formadores enviam aos formandos as e-atividades que devem realizar no prazo previsto, e enviar ao formador para avaliação até a data e hora limite indicadas.

Dada a natureza do tipo de trabalho a realizar pelos participantes, o acompanhamento dos mesmos exige grande disponibilidade por parte dos formadores, pelo que cada turma virtual não deve ter um número muito elevado de e-formandos.

Nesta ação de formação os formandos terão, sequencialmente, acesso aos conteúdos dos diversos módulos, para o seu estudo e para a execução das atividades solicitadas, em situações on e offline. O acesso offline possibilita a leitura/estudo dos conteúdos dos módulos por parte dos formandos sem necessidade de ligação à Internet.

A tutoria a prestar pelos formadores será ativa e permanente e far-se-á preferencialmente através dos fora de discussão abertos nos diversos tópicos (correspondentes aos

módulos da estrutura do curso) na PlataformAbERTA.

Podem realizar-se sessões síncronas de discussão online (chats), em datas, horários e locais a comunicar antecipadamente pelos formadores.

RECURSOS DE APRENDIZAGEM

Recursos pedagógicos

Os materiais técnico-pedagógicos a fornecer aos formandos para utilização no curso são textos base sobre os temas a abordar, colocados online no curso criado na PlataformAbERTA, e/ou na Web em servidor a indicar aos participantes para procederem o seu download;

- Apresentações multimédia diversas concebidas pelos formadores para situações de aprendizagem específicas;
- Tutorial sobre a forma de utilizar a PlataformAbERTA na situação de e-formando;
- Guia do curso.

Recursos técnicos

Plataforma informática Moodle (V 2.4), em https://elearning.uab.pt/, apoiada por 4 servidores e utilizando uma ligação com 200 MB de largura de banda.

AVALIAÇÃO E CLASSIFICAÇÃO

Avaliação nos Módulos

Todos os módulos do curso são sujeitos a avaliação que integra:

- Uma componente contínua ao longo do módulo (participação no fórum de discussão e eventual realização de e-atividades intermédias);
- Uma componente final do módulo baseada na realização de uma e-atividade final que pode revestir qualquer forma (trabalho, teste, projeto, etc.).

Os instrumentos de avaliação de um módulo têm o mesmo peso e, por isso, a avaliação final do módulo é dada pela média simples das 2 ou 3 provas realizadas, numa escala de 0 a 20 valores.

A média final da avaliação dos módulos traduz a classificação final.

Na avaliação da participação dos alunos num fórum de discussão têm-se em atenção

os seguintes fatores:

- A qualidade e a quantidade de mensagens com conteúdo significativo para o(s) assunto(s) em discussão;
- A relevância das mensagens para os temas em discussão;
- A clareza e objetividade das mensagens;
- A redação das mensagens (pontuação, erros de ortografia, etc.);
- A oportunidade do envio das mensagens, privilegiando-se a distribuição destas ao longo de todo o período de discussão em fórum.

Todas as mensagens enviadas para os fóruns de módulos já terminados não são consideradas para efeitos de avaliação.

As e-atividades a realizar em cada um dos módulos (tanto as intermédias como a final) podem revestir qualquer tipo – teste tradicional, trabalho offline, trabalho online, síntese, pesquisa, relatório, etc. – ficando a sua escolha ao critério do formador do respetivo módulo.

É obrigatória a realização de todas as e-atividades de avaliação dos módulos que contam para a classificação final do curso. A não realização de uma e-atividade é contabilizada com 0 valores para efeitos de obtenção da média. A não participação num fórum de discussão traduz-se numa classificação de 0 valores nesse fórum.

Todas as e-atividades de avaliação final dos diversos módulos realizam-se numa só data e num período de 24 a 48 horas. **Excepcionalmente**, e apenas por razões de doença ou de inoperacionalidade da plataforma, ambas devidamente comprovadas, se admite a realização das e-atividades para avaliação numa data de **segunda oportunidade**.

Classificação Final no curso

A classificação final no curso (CFC) é obtida pela aplicação da fórmula:

$$\mathrm{CFC} = \left(\frac{\mathrm{AFM1} + \mathrm{AFM2} + \mathrm{AFM3} + \mathrm{AFM4} + \mathrm{AFM5} + \mathrm{AFM6} + \mathrm{AFM7}}{7}\right) \times 0{,}6 + \mathrm{AFM8} \times 0{,}4$$

onde AFMx representa a Avaliação Final do Módulo x.

Consideram-se com aproveitamento e credores da **Microcredencial em Cibersegurança Ofensiva** os formandos que obtiverem uma Classificação Final no Curso **igual ou superior 10 valores**, numa escala de 0 a 20 tendo tido nos módulos 1 a 7 uma classificação igual ou superior a 8 valores.

EQUIPA DOCENTE

FORMADORES	MÓDULOS
UALV	0. Ambientação ao contexto do e-learning, socialização online e treino com ferramentas do Moodle
Luís Dias	1. Fundamentos e metodologias 2. Reconhecimento com fontes abertas (OSINT) 3. Reconhecimento ativo, vulnerabilidades e engenharia social
André Calvinho	4. Exploração (metasploit) 5. Exploração web 6. Crack de passwords 7. MITM spoofing, redirecionamento - Wireless
Luís Dias André Calvinho	8. Exercício Final – Ambiente virtual
Luís Dias André Calvinho	Análise, avaliação e classificação dos exercícios finais

LUÍS FILIPE XAVIER CAVACO DE MENDONÇA DIAS é Major Engenheiro da Arma de Transmissões do Exército Português, especializado em Segurança da Informação e Docente na Academia Militar. É Doutorado em Segurança de Informação pelo Instituto Superior Técnico, Mestre em Engenharia Eletrotécnica Militar (Especialidade de Transmissões) pela Academia Militar, e está ainda habilitado com o Curso de Estado-Maior Conjunto das Forças Armadas. Detém várias certificações da Indústria (SANS GCFE, EC-Council ECSA e ENSA, etc.) e é membro do GIAC advisory board.

Atualmente e desde 2016, é docente de "Segurança Informação, Sistemas de Informação e Ciberdefesa" (entre outras Unidades Curriculares) na Academia Militar.

Desempenhou funções na componente operacional de ciberdefesa do Exército, entre 2010 e 2015. Participou como "jogador" em diversas edições de exercícios de ciberdefesa Nacionais e Internacionais (Ciber Perseu, Cyber Coalition da NATO). Em 2018 e 2019 foi organizador dos Exercícios Nacionais de Ciberdefesa (Ciber Perseu) na área relativa à resposta técnica a incidentes informáticos.

É membro investigador do Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento (INESC-ID) e do Centro de Investigação da Academia Militar (CINAMIL). Desenvolve investigação no âmbito da aprendizagem automática de ameaças no ciberespaço através da análise de dados de segurança, com recurso a algoritmos de aprendizagem não supervisionada. É formador de cursos de Aprendizagem ao Longo da Vida da Universidade Aberta desde 2019.

ANDRÉ VICENTE CALVINHO é Capitão Engenheiro da Arma de Transmissões do Exército Português, especializado na área da Ciberdefesa e Segurança da Informação. Possui 7 anos de experiência na área da cibersegurança. É engenheiro de cibersegurança, investigador na área da segurança e penetration tester. É mestre em Engenharia Eletrotécnica e de Computadores na Academia Militar e Instituto Superior Técnico.

Possui diversas certificações da indústria, tais como: Certified Information Systems Security Professional (CISSP), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH) e GIAC Certified Intrusion Analyst (GCIA). Possui ainda a certificação em GIAC Continuous Monitoring Certification (GMON), é membro do GIAC Advisory Board e detentor de inúmeros cursos na área dos sistemas de informação entre os quais o CCNA-Exploration da Cisco e IBM Security QRadar.

Possui ainda experiência nas áreas de Information Assurance, Vulnerability Assessment, Penetration Testing, Forensics, Configurations Analysis, Security Analysis, Hardening e Incident Response. Desenvolveu vários projetos na área, entre os quais a criação da ferramenta EmailAnalyzer, disponível na plataforma GitHub. Destaque ainda para a sua participação nos seguintes exercícios internacionais: NATO Cyber Coalition (2014, 2015, 2016 e 2019), NATO Locked Shields (2018, 2019 e 2021), CrossedSwords (2020), BRAZIL – CyberSecurity Brazilian Army Course e Ibero-Armerican Exercise of Cyber Defense (2018).


UNIVERSIDADE
ABERTA
www.uab.pt