

CIBERSEGURANÇA OFENSIVA



Aprendizagem
ao Longo da Vida

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

Se não conheces o teu inimigo e apenas te conheces a ti mesmo,
por cada vitória sofrerás uma derrota.

Se não conheces o teu inimigo nem te conheces a ti mesmo serás derrotado
em todas as batalhas."

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

ÍNDICE

1. [A Universidade Aberta](#)
2. [Enquadramento do Curso](#)
3. [Objetivos do Curso](#)
4. [Competências a adquirir](#)
5. [Programa e conteúdos do Curso](#)
6. [Públicos-alvo do Curso](#)
7. [Pré-requisitos dos formandos](#)
8. [Duração e estrutura do Curso](#)
9. [Calendarização do Curso](#)
10. [Atividades dos formandos](#)
11. [Metodologia e sistema de tutoria](#)
12. [Recursos de aprendizagem](#)
13. [Sistema de avaliação e classificação](#)
14. [Diretor, coordenadores e formadores](#)
15. [Acompanhamento do Curso](#)

ANEXOS

[Mapa conceptual](#)

[E-atividades](#)

[Exemplo de e-atividade](#)

[Avaliação de mensagens](#)

[A Plataforma AbERTA](#)

[Modelo do Certificado de Formação](#)

1. A UNIVERSIDADE ABERTA

Universidade Pública de Ensino a Distância

A Universidade Aberta (UAb), universidade pública de ensino a distância estatutariamente tem como missão, no contexto universitário português e de acordo com a lei que o enquadra, a criação, transmissão e difusão da cultura, dos saberes, das artes, da ciência e da tecnologia, ao serviço da sociedade, através da articulação do estudo, do ensino, da aprendizagem, da investigação e da prestação de serviços.

A Universidade é uma pessoa coletiva de direito público (NPC 502 110 660) e goza de autonomia estatutária, pedagógica, científica, cultural, administrativa, financeira, patrimonial e disciplinar, podendo, na prossecução dos seus fins, por si só ou em cooperação com outras entidades, universitárias ou outras, tanto públicas como privadas, criar ou incorporar no seu âmbito pessoas coletivas de direito privado.

A Universidade tem a sua sede em Lisboa e dispõe de delegações nas cidades do Porto e de Coimbra, podendo criar outras delegações ou entidades de apoio, no território nacional ou fora dele, necessárias à realização dos seus objetivos.

Nos termos da lei, são atribuições da Universidade:

- a) Realizar ciclos de estudos visando a atribuição de graus académicos, bem como de outros cursos pós -secundários, de cursos de formação pós-graduada e de outros, nos termos da lei, destinados a populações que procurem o ensino a distância;
- b) Promover a aprendizagem ao longo da vida, nomeadamente através de ações de formação, qualificação e reconversão profissional, em domínios estratégicos para o desenvolvimento e a atualização de conhecimentos;
- c) Garantir que, a todo o tempo, será considerada a especificidade dos estudantes de ensino a distância, através do apoio e enquadramento pedagógico, bem como da salvaguarda dos respetivos direitos;
- d) Realizar investigação e apoiar a participação dos seus docentes e investigadores em instituições científicas;
- e) Conceber, produzir e difundir recursos educacionais mediatizados e em rede, suscetíveis de utilização através das tecnologias de informação e comunicação, destinados ao ensino formal e não formal a qualquer nível, à defesa e promoção

da língua e da cultura portuguesas, no País e no estrangeiro, com especial relevo para os países e comunidades de língua portuguesa;

- f) Contribuir para a difusão e a promoção da sociedade do conhecimento, incentivando, pela sua metodologia própria, a inclusão digital, a apropriação e a autoconstrução de saberes e a transferência e a valorização económica do conhecimento científico e tecnológico;
- g) Promover a cooperação e o intercâmbio cultural, científico e técnico com instituições congéneres, nacionais e estrangeiras;
- h) Contribuir, no seu âmbito de atividade, para a cooperação internacional e para a aproximação entre os povos, com especial destaque para os países de língua oficial portuguesa e os países europeus.

Estas atribuições abrangem o território nacional, podendo ser extensivas a estruturas delegadas, para esse fim criadas no estrangeiro.

Fundada em 1988, a UAb é a única instituição de ensino superior público vocacionada para o ensino a distância. Desde o início, a UAb tem estado orientada para a educação de grandes massas populacionais geograficamente dispersas, tendo-se já proporcionado formação de nível superior a mais de 10 mil estudantes, em 33 países dos cinco continentes, licenciando-se mais de 9 mil estudantes, concedendo-se mais de um milhar de graus de mestre e cerca de uma centena de graus de doutor.

Pioneira no ensino superior a distância em Portugal, a UAb tem promovido ações relacionadas com a formação superior e a formação contínua, contribuindo igualmente para a divulgação e a expansão da língua e da cultura portuguesas, com especial relevo nos países e comunidades lusófonos. Ao longo dos 20 anos de existência da UAb, os seus docentes e investigadores têm desenvolvido atividades de investigação científica através da utilização das tecnologias da informação e da comunicação, concebendo e produzindo materiais pedagógicos nas áreas da tecnologia do ensino e da formação a distância, e da comunicação educacional multimédia.

Com mais de 400 títulos editados, de 3500 horas de produções audiovisuais e de 6000 horas de emissões televisivas, produzidas nos seus estúdios, a UAb tem procurado sobretudo incentivar a apropriação e a autoconstrução de saberes, concebendo e lecionando cursos, formando técnicos e docentes, de acordo com uma filosofia de prestação de serviço público.

Estudantes-alvo

A UAb assume como missão fundamental formar estudantes que, por várias razões, não puderam, no seu tempo próprio, encetar ou prosseguir estudos universitários. Por outro lado, a UAb procura corresponder às expectativas de quantos, tendo eventualmente obtido formação superior, desejam reconvertê-la ou atualizá-la; o que significa que, por vocação, tenta ir ao encontro das expectativas de um público adulto, com experiência de vida e normalmente já empenhado no exercício de uma profissão.

Assim, é condição necessária para ingressar na UAb ter mais de 21 anos de idade e realizar provas de acesso a esta universidade, que não integra o concurso nacional de acesso ao ensino superior. As licenciaturas da UAb não têm *numerus clausus*. A UAb também efetua provas especialmente destinadas a Avaliar a Capacidade para a Frequência do Ensino Superior (ACFES) dos maiores de 23 anos.

Pioneira no *E-Learning* em Portugal

Enquanto universidade pioneira no Ensino Superior a Distância em Portugal, e tendo em conta a sua responsabilidade como principal centro nacional de competência nesta área, a UAb desenvolveu um inestimável *know-how*, que lhe permitiu constituir a maior bolsa de oferta de cursos *online* do País.

No ano letivo 2008-2009, a UAb tornou-se na primeira e única universidade (pública) em Portugal a lecionar todas as licenciaturas e mestrados pela Internet, em regime de *e-learning*, através de um Modelo pedagógico virtual inédito no País e desenvolvido por esta instituição.

A UAb é também considerada um dos *mega-providers* de *e-learning* europeus, desempenhando um papel preponderante na lecionação de cursos de 1.º Ciclo (licenciaturas) e de 2.º Ciclo (mestrados), em domínios das Humanidades, das Ciências e Tecnologia, da Educação e Ensino a Distância, das Ciências Sociais e da Gestão. Todos os cursos de licenciatura e mestrado da UAb estão adequados ao Processo de Bolonha.

Modelo pedagógico virtual

O modelo pedagógico da UAb assenta no regime de *e-learning* e na utilização intensiva das novas ferramentas de comunicação *online*. Promovendo a interação entre estudantes e docentes, este modelo está fortemente centrado no estudante enquanto indivíduo ativo e construtor do seu conhecimento. Permite ainda uma maior *flexibilidade na aprendizagem*, onde a comunicação e a interação se processam de acordo com a

disponibilidade do estudante, partilhando recursos, conhecimentos e atividades com os seus pares. A avaliação dos conhecimentos e competências, baseada na avaliação contínua, assume soluções diversificadas. Nos cursos de graduação, o estudante possui um cartão de aprendizagem onde investe ao longo do seu percurso, realizando *e-fólios*, creditando *e-valores* e efetuando provas presenciais. Nos cursos de pós-graduação, a avaliação desenvolve-se de formas muito variadas, recorrendo, por exemplo, a *portfólios*, blogs, projetos, ensaios, resolução de problemas, participação em discussões, relatórios e testes.

Inclusão digital

A frequência da UAb é fator de inclusão social pela vertente da alfabetização digital: o ensino *online* exige competências específicas por parte do estudante, pelo que todos os programas de formação certificados pela UAb incluem um módulo prévio, de frequência gratuita. Deste modo, os novos estudantes podem adquirir as competências necessárias à frequência do curso ou do programa de formação em que se inscrevem.

A atual expansão da *Internet* e da *Word Wide Web (WWW)* e o desenvolvimento ainda mais recente dos programas informáticos de gestão do ensino/aprendizagem, vieram modificar o panorama do ensino a distância, permitindo a criação de espaços virtuais de ensino com designações diversas, *centro de ensino virtual*, *escola virtual*, etc., onde a palavra virtual apenas significa que esses espaços não têm implantação e realidade físicas palpáveis.

É pois no espaço virtual de formação/aprendizagem da UAb (em <https://elearning.uab.pt/>) que se vai desenvolver a ação de formação de aprendizagem ao longo da vida do domínio da cibersegurança designada **Curso de Cibersegurança Ofensiva**.

A Universidade Aberta, instituição de direito público, tutelada pelo Ministério da Ciência, Tecnologia e Ensino Superior, encontra-se abrangida pelo Art.º 2.º da Portaria n.º 782/97 de 29 de agosto e, por força dos seus Estatutos, não carece de acreditação ou certificação como entidade formadora por parte Direção de Serviços de Qualidade e Acreditação da **Direção-Geral do Emprego e das Relações de Trabalho (DGERT)** ou de qualquer outra entidade de acreditação ou certificação setorial.

2. ENQUADRAMENTO DO CURSO

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. Estes 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.

Este curso 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.

O curso 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.

É neste enquadramento que a Universidade Aberta (UAb) organizou e pretende oferecer ao mercado de formação este curso. O presente curso desenvolve-se em regime de formação teórica e prática a distância online (também dito e-learning), com uma componente de avaliação final baseada na elaboração de um projeto prático, a depositar na plataforma informática para análise, correção e classificação pelos professores, até à data-hora estabelecida

3. OBJETIVOS DO CURSO

O objetivo do curso é proporcionar conhecimentos e competências que permitam aos formandos 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. Assim, no final, os participantes saberão:

- Os aspetos legais e a metodologia associada 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;
- Empregar o uso de ferramentas para a quebra de passwords;
- Proceder à exploração de vulnerabilidade de rede e ataques relacionados com redes wireless.

O regime de funcionamento online suportado por uma plataforma informática de gestão da formação/aprendizagem permitirá ainda alcançar outros objetivos e adquirir outras competências, secundárias em relação ao âmbito geral deste curso, mas de extrema importância para a empregabilidade. Deste modo os formandos irão adquirir e treinar competências nos domínios da comunicação e das Tecnologias de Informação e Comunicação (TIC) que lhes permitam no futuro uma mais fácil pesquisa de informações técnicas de que necessitem para o seu trabalho, mais rápido e fácil contacto com os seus pares nacionais e internacionais e ainda competências para a frequência de outras ações de formação à distância na modalidade de e-learning

4. COMPETÊNCIAS A ADQUIRIR

No final do curso espera-se que os participantes tenham adquirido as seguintes competências:

- 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.

Este curso permitirá ainda aos formandos adquirir diferentes competências ditas para a empregabilidade, designadamente competências:

- Para aprender continuamente e em regime de autoaprendizagem;
- De orientação para resultados;
- De intercomunicação online e de networking;
- De trabalho em equipa;

- Na utilização de tecnologias informáticas;
- Na autogestão do tempo e das atividades.

5. PROGRAMA E CONTEÚDOS DO CURSO

Este está estruturado em 8 módulos, com a duração de uma semana cada, que se desenvolvem sequencialmente. Estes módulos são precedidos de um módulo de ambientação ao contexto online do curso e de integração dos participantes, designado módulo 0 ou pré-curso e incluído gratuitamente.

A componente escolar do curso tem a duração de 104 horas (volume de trabalho dos formandos) a que corresponde um crédito de 4 ECTS¹ da UAb e realiza-se em regime de formação a distância online (e-learning) ao longo das 9 semanas.

Na Internet o curso é suportado pela plataforma informática Moodle em utilização na UAb e adaptada ao seu Modelo Pedagógico Virtual.

MÓDULO 0: AMBIENTAÇÃO AO CONTEXTO *ONLINE* DO CURSO

[Duração: 13 horas práticas | 1 semana]

Objetivos do módulo

Este módulo tem por objetivos a socialização dos participantes e a criação de “um grupo” de trabalho *online*, a familiarização com a utilização do software de gestão do curso (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.

Durante o Módulo 0 será ainda explicada e treinada a forma como pesquisar “depressa e bem” informação na Web e será pedido aos participantes a procura (na Web) de informação relevante sobre temas que constituam matérias do curso

Competências a adquirir

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

- Interagir e comunicar com os colegas, com os formadores e com o interface de aprendizagem no sentido de conseguir resolver problemas básicos de interação, de comunicação;

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.

- Explorar com eficácia todas as ferramentas e possibilidades da plataforma Moodle, 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.

Conteúdos programáticos

Unidade Didática 1: A plataforma informática de ensino/aprendizagem da UAb

O que é o Moodle;

Formas de organizar espaços/sites no Moodle;

Recursos e atividades da plataforma Moodle

Estrutura do espaço Moodle do CEDS; tópicos do curso; recursos disponíveis e ferramentas a utilizar.

Unidade Didática 2: Treino na exploração das ferramentas e recursos da plataforma

Treino com fóruns, trabalhos, questionários, wikis, referendos, equipas, etc.

Unidade Didática 3: Prática de pesquisa de informação na Web

Como procurar informação usando: palavras-chave, operadores booleanos, sinais, especificação de formatos, aspas e asteriscos;

Motores de busca e meta-motores;

Credibilidade da informação na Web. Critérios de avaliação.

MÓDULO 1: FUNDAMENTOS E METODOLOGIAS

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

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;
- Conhecer as metodologias enquadrantes dos testes de penetração.

Conteúdos programáticos

Unidade didática 1: Conceitos fundamentais de redes e sistemas

Hardware/Software;

Aplicações, Sistemas Operativos, Drivers;

Bits, Bytes, Codificação;

Características e finalidades das redes de computadores;

Componentes de uma rede e topologias;

Modelos de referência (OSI e TCP-IP);

Os principais protocolos.

Unidade didática 2: Máquinas virtuais

Virtualização e emulação;

Instalar e utilizar o Virtual Box;

Preparar o ambiente virtual para o curso.

Unidade didática 3: Ambiente Linux (Kali)

Generalidades;

Utilização do terminal;

Comandos de base;

Utilizadores e superuser.

Unidade didática 4: Enquadramento dos testes de penetração

Aspetos legais (Legislação e normas de referência);

Terminologia e conceitos;

Planeamento e escopo;

Metodologias e frameworks;

Confidencialidade e reporte.

Prática em contexto de formação

Para além da componente teórica, este módulo visa também preparar os formandos numa perspetiva prática. Nesse sentido, os formandos irão fazer alguns exercícios nos seus próprios computadores, como exemplo, irão instalar um sistema operativo numa máquina virtual e preparar o ambiente virtual que será utilizado ao longo do curso. O

módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

Os alunos irão realizar ainda um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 2: RECONHECIMENTO COM FONTES ABERTAS (OSINT)

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

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;
- Perceber como criar uma estratégia de ataque partindo de informações obtidas em fontes abertas;
- Adotar uma postura que reduz o potencial da informação publicada na internet, do próprio ou da organização, a ser utilizada para fins maliciosos.

Conteúdos programáticos

Unidade Didática 1: Recolha de informações sobre o alvo

Reconhecer o adversário com recurso a fontes abertas;

Informações sobre uma organização ou indivíduo (e-mails, números de contacto, anúncios de emprego, tecnologias, funcionários relevantes, etc.);

O processo de OSINT e contributo para a identificação de vulnerabilidades;

Documentar a recolha (e.g., dossier de domínios e de e-mails) e definir a estratégia de ataque.

Unidade Didática 2: Ferramentas e técnicas de OSINT

Maltego;

Shodan;

Rede e DNS (Censys, Netcraft, Whois, Nslookup, TheHarvester, Sublist3r, etc.);

Websites, Redes Sociais, Sites de emprego, Google Dorks, etc.;

Bases de dados acerca de vulnerabilidades.

Unidade Didática 3: Recomendações para limitar a exposição

Postura;

Privacidade;

Canais seguros, mascaramento e ocultação, desativação de serviços, etc.

Prática em contexto de formação

Para além da componente teórica, este módulo prevê a realização de diversos exercícios práticos relacionados com a utilização de ferramentas e a aplicação de técnicas de OSINT. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

Os alunos irão realizar ainda um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 3: RECONHECIMENTO ATIVO, VULNERABILIDADES E ENGENHARIA SOCIAL

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

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;
- Compreender o potencial da Engenharia Social nas diversas fases de um ataque.

Conteúdos programáticos

Unidade Didática 1: Scanning/enumeração e fingerprinting

Objetivos (hosts, redes, páginas web, serviços, etc.);

Ping sweep;

NMAP (múltiplos cenários/configurações, TCP/UDP);

Confirmação manual (Telnet, nc, ncat);

Fingerprinting (banner, pacotes).

Unidade Didática 2: Análise de vulnerabilidades

Scanners de vulnerabilidades (OpenVAS, Nikto, Qualys, Nessus, etc.);

Tipos de scans (com ou sem permissões, completo, oculto, conformidade);

Categorização (de ativos e das vulnerabilidades) e priorização.

Unidade Didática 3: Engenharia social

A arte de manipular o fator humano;

Phishing, Spear-Phishing, SMS Phishing, Vishing, etc.;

Ferramentas - o exemplo do Social Engineer Toolkit (SET).

Prática em contexto de formação

Para além da componente teórica, este módulo terá diversos exercícios práticos em que os formandos utilizam as ferramentas expostas nos conteúdos programáticos. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

Os alunos irão realizar ainda um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 4: EXPLORAÇÃO (METASPLOIT)

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

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

- Compreender e 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.

Conteúdos programáticos

Unidade Didática 1: Netcat - Aprender a utilizar o canivete suíço do TCPIP

Introdução ao Netcat;

Criação uma bind shell e uma reverse shell;

Realização de transferência de ficheiros com o Netcat;

Realização de scan à rede com o Netcat;

Utilização do netcat com SSL.

Unidade Didática 2: Utilização da framework Metasploit em Server-Side

Introdução ao Metasploit;

Aplicação de exploits do catálogo para o comprometimento de um servidor;

Introdução à shell meterpreter e aplicação das suas funcionalidades.

Unidade Didática 3: Utilização da framework Metasploit em Client-Side

Criação de payloads com msfvenom e outras ferramentas semelhantes;

Criação de uma apk malicioso para android;

Explorar o browser de um cliente;
Migração de uma shell comum para meterpreter;
Utilização de módulos adicionais do meterpreter.

Prática em contexto de formação

Para além da componente teórica, este módulo visa preparar os formandos com diversos exercícios práticos nos quais estes terão a oportunidade de pôr em prática tudo aquilo que aprenderam relativamente à exploração de serviços e clientes com a framework Metasploit e a ferramenta Netcat. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

Os alunos irão realizar ainda um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 5: EXPLORAÇÃO WEB

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

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

- Compreender e aplicar os conceitos referentes às vulnerabilidades mais comuns segundo o ranking OWASP Top 10;
- Empregar o uso da 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.

Conteúdos programáticos

Unidade didática 1: Aplicações web - exploração de falhas em websites

Introdução a vulnerabilidades segundo o OWASP Top 10;

Introdução ao Burp Suite. Exploração das suas componentes e funcionalidades;

Utilização da ferramenta sqlmap para ataques a vulnerabilidades de SQL injection;

Realização de exercício práticos com vulnerabilidades de SQL injection, XSS e CSRF;

Unidade didática 2: Webshells, comprometimento de aplicações web

Identificar e aplicar o uso de diferentes webshells;

Contornar funcionalidade de upload de ficheiros para execução de webshell maliciosa;

Comprometimento de aplicação web através da manipulação de logs do sistema.

Unidade didática 3: Análise de vulnerabilidades de aplicações web

Introdução ao openVAS;

Utilização das ferramentas openVAS e nikto para a análise de vulnerabilidades da aplicação Multilidae;

Criação de um relatório de análise de vulnerabilidades.

Prática em contexto de formação

Para além da componente teórica, este módulo visa preparar os formandos com diversos exercícios práticos nos quais estes terão a oportunidade de pôr em prática tudo aquilo que aprenderam relativamente à exploração de vulnerabilidades em aplicações web. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

Os alunos irão realizar ainda um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 6: CRACK DE PASSWORDS

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

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.

Conteúdos programáticos

Unidade didática 1: Quebra de passwords forma online

Introdução à quebra de passwords online e offline;

Utilização da ferramenta Burp para a quebra de passwords online;

Utilização das ferramentas Hydra e Medusa para a quebra de passwords online.

Unidade didática 2: Quebra de passwords forma offline

Criação de uma wordlist com a ferramenta Crunch;

Utilização das ferramentas JohnTheRipper e Hashcat para a quebra de passwords offline.

Unidade didática 3: Serviços web online e rainbow tables

Utilização de aplicações online para a quebra de passwords;

Introdução a rainbow tables com exemplos.

Prática em contexto de formação

Para além da componente teórica, este módulo visa preparar os formandos com diversos exercícios práticos nos quais estes terão a oportunidade de pôr em prática tudo aquilo que aprenderam relativamente à quebra de passwords de forma online e offline. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

Os alunos irão realizar ainda um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 7: MITM SPOOFING, REDIRECIONAMENTO - WIRELESS

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

Objetivos do módulo

- Explicar os conceitos de redirecionamento, 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.

Conteúdos programáticos

Unidade didática 1: Rede Local - Redirecionamento, Spoofing e MITM

Conceitos de Redirecionamento, Spoofing e MITM;
Envenenamento de gateway de rede através de arp spoofing;
Realização de DNS spoofing com captura de credenciais;
Realização de um ataque MITM com as ferramentas Ethercap e Mitmproxy;
Captura de tráfego com as ferramentas Wireshark e Cain e Abel.

Unidade didática 2: Wireless - Introdução a Vulnerabilidades Gerais

Introdução a vulnerabilidades gerais de wireless;
Configuração de modo monitorização (iwconfig);

Contornar proteção de endereço MAC;
Realizar ataque DoS em redes wireless;
Exploração de vulnerabilidades em routers wireless.

Unidade didática 3: Wireless - Captura e cracking de chaves de acesso

Captura e quebra de chaves wireless;
Captura de IVs de chaves WEP;
Descobrir chaves WEP;
Captura de handshakes de chaves WPA;
Descobrir chaves WPA;
Identificação e exploração de routers com a funcionalidade WPS ativa.

Prática em contexto de formação

Para além da componente teórica, este módulo visa preparar os formandos com diversos exercícios práticos nos quais estes terão a oportunidade de pôr em prática tudo aquilo que aprenderam relativamente ao conceito de redirecionamento, spoofing e ataques Man-In-The-Middle. Os formandos estarão também aptos a compreender e executar ataques relacionados com redes wireless. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

Os alunos irão realizar ainda um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 8: EXERCÍCIO FINAL

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

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 o curso.

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.

6. PÚBLICO-ALVO DO CURSO

Potencialmente o curso tem um vasto público-alvo que inclui, designadamente:

- Todos os 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;
- Todos os 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;

Trata-se, portanto, de um público adulto, por norma trabalhador no ativo, e este facto deve ser considerado na forma como se deve fazer aprender, como motivar para essa aprendizagem e como avaliar os conhecimentos e competências adquiridos.

7. PRÉ-REQUISITOS DOS FORMANDOS

Considera-se como fator do seu sucesso neste curso a motivação dos formandos e a sua disponibilidade total para interagirem com os formadores e com os outros formandos na colocação de questões ou dúvidas sobre a matéria, e disponibilidade de tempo para estudarem os conteúdos, elaborarem todas as atividades sugeridas, as avaliações propostas e o trabalho final.

Cumulativamente, os formandos devem possuir:

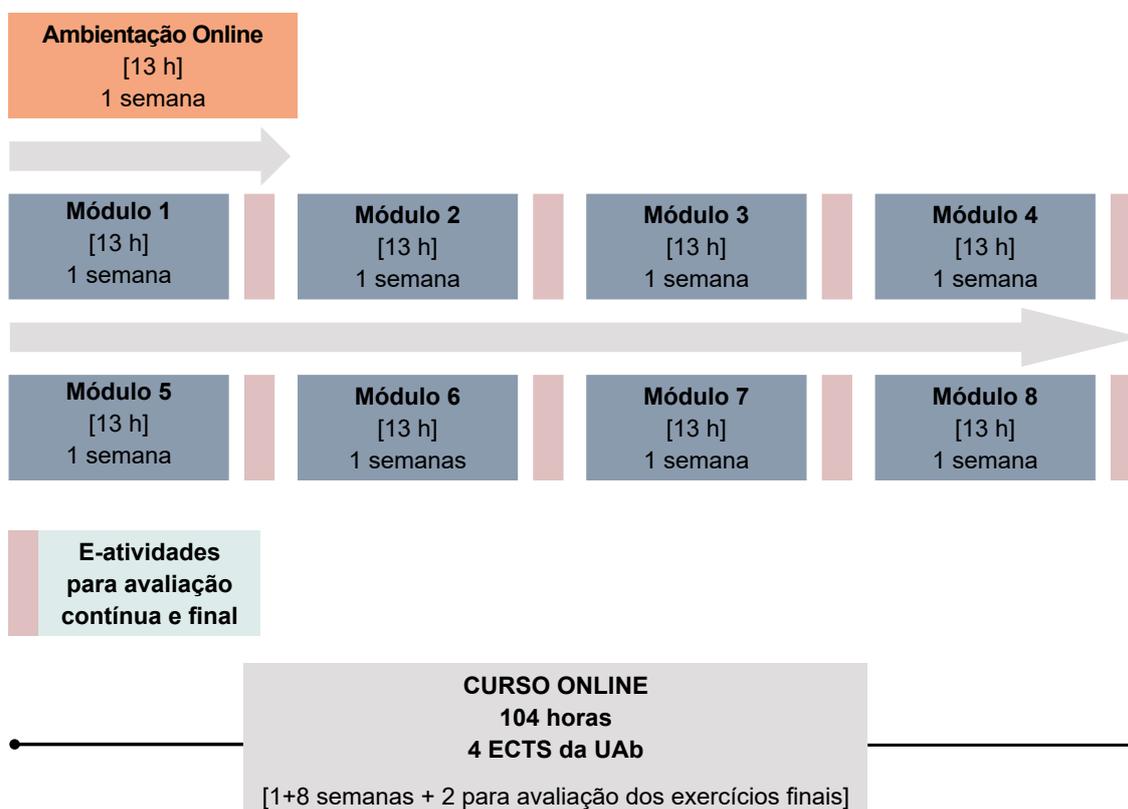
- Habilitações mínimas ao nível do 12.º ano ou equivalente;
- Computador com pelo menos 8GB de memória RAM e 50 GB de espaço em disco disponível;
- Conhecimentos e prática de informática como utilizadores;
- Prática de utilização de browsers de navegação na Web;
- Uma conta de correio eletrónico ativa e prática na sua utilização;
- Disponibilidade de tempo mínima de 13 horas por semana para:
 - Participação nos fóruns de discussão e nos chats;
 - Realização do autoestudo dos conteúdos disponibilizados online;

- Pesquisa de informação com interesse para o âmbito dos diversos módulos;
- Realização de todas as e-atividades propostas (testes, trabalhos, etc.);
- Elaboração do trabalho final de projeto.

Ao formalizarem a sua candidatura a este curso, os interessados assumem implicitamente que cumprem todos os pré-requisitos acima descritos.

8. DURAÇÃO E ESTRUTURA DO CURSO

A duração total do curso é de 104 horas (volume de trabalho dos formandos) sendo o estruturado em 8 módulos de realização sequencial, precedidos de um módulo de Ambientação ao Contexto Online do curso (13 horas), de socialização online e de treino com a plataforma informática que suporta o curso.



9. CALENDARIZAÇÃO DO CURSO

MÓDULOS	DATAS
Módulo 0 Ambientação ao contexto online do curso e ao Moodle	A calendarizar
Módulo 1: Fundamentos e metodologias	Imediatamente a seguir ao módulo anterior
Módulo 2: Reconhecimento com fontes abertas (OSINT)	idem
Módulo 3: Reconhecimento ativo, vulnerabilidades e engenharia social	idem
Módulo 4: Exploração (metasploit)	idem
Módulo 5: Exploração Web	idem
Módulo 6: Crack de passwords	idem
Módulo 7: MITM spoofing, redirecionamento - Wireless	idem
Módulo 8: Exercício Final	idem

10. ATIVIDADES DOS FORMANDOS

MÓDULOS	DESCRIÇÃO
Sessão presencial caso se realize	Abertura do curso Apresentação do plano do curso e dos coordenadores e dos formadores dos diferentes módulos Acesso ao curso na Plataforma AbERTA Moodle da UAb Apresentação da estrutura do curso criado na plataforma e da forma como participar Treino com a Plataforma AbERTA Moodle

<p>Módulo 0 ou Módulo de Ambientação Online Familiarização com a plataforma Moodle e socialização no ambiente <i>online</i></p>	<p>Aceder à PlataformAbERTA Moodle e ao curso Editar o seu perfil e colocar uma fotografia na plataforma Efetuar a apresentação individual no espaço Moodle do curso Consultar o Guia do Curso Consultar o Guia do Formando <i>Online</i> Consultar o tutorial sobre a PlataformAbERTA Moodle Executar as pesquisas de informação pedidas e colocar os resultados no Fórum de Discussão Treinar com as diversas ferramentas da plataforma e de acordo com instruções do formador Participar nos fora de discussão abertos e no chat</p>
<p>Módulos 1 a 7</p>	<p>Ao longo dos diversos módulos os e-formandos são chamados a desenvolver uma série de atividades formativas que se podem sintetizar em:</p> <ul style="list-style-type: none"> • Leitura e estudo das matérias dos Módulos colocadas <i>online</i> e de outros documentos disponibilizados pelos e-formadores • Interação com os formadores e com os outros formandos nos <i>fora</i> de discussão criados. <p>Esta interação (quantidade de mensagens, sua relevância para os temas em discussão e sua oportunidade) é considerada na avaliação contínua</p> <ul style="list-style-type: none"> • Fazer as e-atividades correspondentes ao módulo. <p>Estas e-atividades são objeto de avaliação contínua</p>
<p>Módulo 8 Trabalho Final (e-atividade final)</p>	<p>Recolha das informações necessárias Estruturação e redação do texto Alojamento do trabalho, no local próprio criado no espaço do curso na plataforma Moodle, dentro da data-hora limite imposta. Discussão dos trabalhos em fórum Esta e-atividade é objeto de avaliação final e vale 40% da classificação final no curso.</p>

11. METODOLOGIA E SISTEMA DE TUTORIA

O curso segue um modelo no qual é a instituição formadora que define os objetivos, conteúdos, percursos de aprendizagem e meios e métodos de avaliação. Este modelo pressupõe a existência de canais de comunicação fáceis e disponíveis em permanência, entre a instituição e os formandos e entre estes e os formadores(es), canais esses integrados na plataforma Moodle a utilizar.

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 fóruns de discussão abertos nos diversos tópicos (correspondentes aos módulos da estrutura do curso) na Plataforma AbERTA|Moodle.

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

12. RECURSOS DE APRENDIZAGEM

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 plataforma Moodle 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 plataforma Moodle na situação de e-formando;
- Tutorial “Como Fazer para...”, documento orientador dos procedimentos para aceder ao curso alojado na plataforma Moodle da UAb;
- Guia do Curso;
- Guia do Formando *Online*.

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.

13. SISTEMA DE AVALIAÇÃO E CLASSIFICAÇÃO

A avaliação em formação *online* tem uma importância acrescida em relação à avaliação em regime presencial em virtude da natureza particular do contexto de ensino-aprendizagem. Os instrumentos de avaliação devem, por isso, ser variados por forma a anular ou reduzir a um mínimo aceitável, a possibilidade de fraude intelectual quanto à autoria dos trabalhos. Por isso, todos os aspetos da avaliação devem ser muito claros e explícitos e a avaliação deve ser definida e planeada a par com o percurso formativo que se deseja e estar intimamente relacionada com os objetivos a atingir.

Avaliação nos Módulos

Todos os módulos do curso são sujeitos a avaliação.

A avaliação nos módulos 1 a 7 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 tem um peso de 60% na 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:

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

$AFMx$ representa a Avaliação Final do Módulo x .

Consideram-se com aproveitamento no curso os formandos que obtiverem classificação Final no Curso **igual ou superior 9,5 valores**, numa escala de 0 a 20.

Para efeitos de aproveitamento e de inscrição no Certificado as classificações finais com décimas de 0,5 a 0,9 são arredondadas para o valor inteiro superior e as de 0,1 a 0,4 para o valor inteiro inferior.

A todos os formandos com aproveitamento é entregue um **Certificado de Formação** que será enviado para a morada que consta no formulário de inscrição no curso

A todos os formandos que realizaram integralmente o curso e o terminaram sem aproveitamento, de acordo com o Regulamento do Curso e a seu pedido expresso, será entregue um **Certificado de Frequência**.

14. DIRETOR, COORDENADOR E FORMADORES

O Curso de Especialização em cibersegurança é dirigido pelo Diretor da Unidade de Aprendizagem ao Longo da Vida (UALV) Professor Doutor Fernando Caetano e coordenado por um técnico superior da UALV para os cursos de natureza profissional.

Os formadores do curso têm origens, formações e experiências académicas e profissionais diversas e são os que a seguir se indicam.

FORMADORES	MÓDULOS
UALV	0. Ambientação ao contexto do e-learning, socialização online e treino com ferramentas do Moodle
Luís Dias	1. Fundamentos e metodologias
Luís Dias	2. Reconhecimento com fontes abertas (OSINT)
Luís Dias	3. Reconhecimento ativo, vulnerabilidades e engenharia social
André Calvinho	4. Exploração (metasploit)
André Calvinho	5. Exploração web
André Calvinho	6. <i>Crack de passwords</i>
André Calvinho	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

Sínteses dos *curricula vitae* dos formadores

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. Está habilitado com o Curso de Estado Maior – Conjunto das Forças Armadas, tem o diploma de estudos avançados em Segurança de Informação no Instituto Superior Técnico e Mestrado em Engenharia Eletrotécnica Militar – Especialidade de Transmissões pela Academia Militar. Detém várias certificações da Indústria (SANS GCFE, EC-Council ECSA e ENSA, etc.) e é membro do GIAC advisory board.

Atualmente é docente de “Segurança Informação, Sistemas de Informação e Ciberdefesa” 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.

Membro do Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento (INESC-ID) e do Centro de Investigação da Academia Militar (CINAMIL), desenvolve a sua investigação de doutoramento 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-American Exercise of Cyber Defense (2018).

15. ACOMPANHAMENTO DO CURSO

Para um acompanhamento permanente e coordenação do curso o Coordenador está inscrito como formador no espaço de aprendizagem criado na plataforma Moodle da UAb. Desta forma garante-se que tudo o que se passe *online* será do seu conhecimento imediato e sem necessidades de ser objeto de qualquer relatório, permitindo uma intervenção mais atempada sempre que as situações a justifiquem.

A plataforma Moodle a utilizar como suporte deste curso permite de uma forma automática:

- Controlar e registar as entradas, saídas e percursos dos formandos no espaço onde decorre o curso, indicando as respetivas horas e dias;
- Editar estatísticas da participação diária, de participação por períodos de tempo e de participação total de cada formando;
- Editar resultados da participação de cada participante nos fóruns de discussão;
- Registar a data/hora de entrega de trabalhos;
- Contabilizar as mensagens enviadas para os diversos fóruns por cada participante.

ANEXOS

ANEXO 1: MAPA CONCEPTUAL DO CURSO



ANEXO 2: O QUE SÃO E-ATIVIDADES?

Ao longo deste guia por diversas vezes se fala em *e-atividades*, pelo que se justifica esclarecer o seu significado.

Designam-se *e-atividades* as atividades a realizar pelos estudantes de cursos desenvolvidos em regime de *e-learning*. Este termo provém da analogia com o termo inglês de *e-tivities* enunciado por Gilly Salmon. Segundo Salmon, as *e-atividades* devem incluir o seguinte conjunto de características:

1. Possuir um título “apelativo” e motivador. Salmon defende que os títulos que os formadores *online* dão às *e-atividades* são muito importantes; os títulos devem dar informação, mobilizar os formandos e distinguir entre si as várias atividades.
2. Ter um elemento (faísca) que espolete a atividade e motive o envolvimento dos participantes. Esta “faísca” pode ser um estímulo, um desafio, uma informação.
3. Ter um conjunto de objetivos (e de competências) que os participantes podem esperar adquirir ou desenvolver com a atividade. Os objetivos e competências são desenvolvidos de modo diferente pelo tipo de atividade que foi concebida. O desenho e conceção da *e-atividade* pelo formador deve considerar esse aspeto.
4. Instruções que descrevam como o formando deve participar: por exemplo, explicitar que se espera que o estudante participe com, pelo menos, uma contribuição para a discussão e resposta, pelo menos, a uma contribuição feita por um colega.
5. A lista de leituras bibliográficas ou de outros recursos relevantes para a sua resolução.
6. Instruções sobre o que os participantes devem fazer. De acordo com a autora, é difícil criar instruções claras e concisas, e esta competência desenvolve-se apenas com a prática e com o *feedback* de outros. Normalmente, as instruções criadas são ambíguas e incompletas, podendo gerar grandes dificuldades aos formandos (pois não incluem todas as ações necessárias para a sua realização).

De acordo com o Modelo Pedagógico Virtual da UAb as *e-atividades* podem adquirir variadas formas, designadamente: testes de tipos diversos (escolha múltipla, resposta verdadeira/falsa, de correspondência, etc.), pesquisas orientadas, projetos, sínteses, relatórios, trabalhos, etc. As *e-atividades* podem ser realizadas quer em situação *offline*, quer em situação *online*.

ANEXO 3: EXEMPLO DE E-ATIVIDADE

E-Atividade DO CURSO

Trabalho organizado é meio caminho andado...

Em qualquer atividade os fatores que influenciam positiva ou negativamente as condições de trabalho podem ser materiais, ambientais, psicossociais ou associados à organização do trabalho. Os fatores referentes à organização do próprio trabalho.....

Esta atividade integra o percurso formativo do curso.....e será apresentada aos formandos no final da xª semana, devendo ser devolvida ao professor até às 23h55 da 2ª-feira da yª semana, o que significa que o aluno terá x dias úteis para a sua realização.

Objetivos e competências a adquirir

- Consolidar conhecimentos sobre organização e gestão do trabalho;
- Aplicar os conhecimentos adquiridos na análise de situações concretas de trabalho;
- Identificar os fatores de risco para a trabalhadora da situação de trabalho apresentada;
- Propor medidas preventivas para minimizar/eliminar os fatores de risco identificados.

Participantes

Esta atividade deve ser realizada individualmente por todos os formandos do curso

Durante esta atividade cada formando deve:

- Fazer uma nova leitura dos conteúdos
- Elaborar a sua resposta, que passa a constituir o seu e-fólio;
- Enviar o e-fólio ao formador até à data-limite estabelecida no Calendário.

Estrutura da atividade

Esta atividade é realizada em apenas uma fase e deve dar origem apenas a 1 ficheiro.

Calendário da atividade

Sábado (xx/yy)	Domingo (...../.....)	2ª-Feira (...../.....)	3ª-Feira (...../.....)	4ª-Feira (...../.....)	5ª-Feira (...../.....)	6ª-Feira (...../.....)
	Apresentação da e-Atividade (e-Fólio) no Tópico x no Moodle	Revisão dos conteúdos Análise da situação laboral	Revisão dos conteúdos Análise da situação laboral	Revisão dos conteúdos Análise da situação laboral	Revisão dos conteúdos Redação da atividade	Redação da atividade

Sábado (xx/yy)	Domingo (...../.....)	2ª-Feira (...../.....)				
		Redação da atividade Envio ao formador				

Instruções e sugestões aos formandos

Até ao diavai realizar esta e-atividade na qual deve demonstrar que adquiriu conhecimentos e competências que lhe permitiram analisar a situação proposta e indicar medidas que possibilitem prevenir os fatores de risco que identificou.

Na sua análise os formandos, à medida que leem o caso prático, devem ir anotando aquilo que lhes parece ser um potencial fator de risco e ir esboçando as medidas preventivas que julga mais adequadas. Por exemplo, logo no início do texto da situação laboral diz-se que Filomena trabalha à tarefa. Será este facto um fator de risco ou não? Como poderá ser combatido?

O relatório correspondente à situação de trabalho analisada deve:

- ter no máximo 2 folhas A4, com margens de 2 cm, escritas a Arial 10 ou equivalente e um espaçamento de 1,5 linhas.
- Ser enviado ao professor em formatos doc. ou pdf.

Nos seus relatórios os formandos devem demonstrar que adquiriram as seguintes competências:

- Capacidade para identificar os fatores de risco e os riscos que podem afetar a organização do trabalho e o trabalhador;
- Capacidade para indicar medidas preventivas concretas para anular ou minimizar os riscos detetados e atribuir-lhes prioridades, se for o caso.

Os relatórios devem ainda ser redigidos em linguagem simples e terem uma estrutura que facilite a sua consulta. Devem ser identificados todos os riscos, sejam físicos, químicos, biológicos, psicossociais ou com implicações ergonómicas.

Recursos para a atividade

- Conteúdos sobre
- Guia Orientador da Avaliação de Riscos nos Locais de Trabalho
- Recursos eventualmente obtidos pelo estudante

Ações e tempo do formador

- Tornar visível na Moodle esta e-atividade, no Tópico “E-Atividade” Avaliar e classificar (até x valores) os relatórios individuais dos estudantes (e-fólio) durante a semana seguintes ao final da atividade.

A carga total de trabalho do professor é de 3 horas para a conceção da atividade, acrescida de 20 minutos vezes o n.º de relatórios recebidos para leitura/correção/avaliação e inserção da classificação na plataforma.

Ações e tempo do formando

Espera-se que cada formando:

- releia os conteúdos e
- elabore um pequeno relatório individual de 2 páginas, sobre a avaliação de riscos que efetuou;
- coloque o seu relatório (o seu e-fólio) no curso, na plataforma.

Esta atividade exige a cada estudante uma carga de trabalho estimada de 2 a 3 horas.

Avaliação da atividade

Esta é uma atividade de avaliação sumativa que vale um máximo de x valores. Na avaliação do relatório considera-se:

- a correção na identificação dos fatores de risco (até x valores)
- a correção das medidas de prevenção apresentadas (até x valores)

Situação de trabalho para análise

Filomena é uma jovem trabalhadora de uma microempresa que repara circuitos de microeletrónica, onde a qualidade da iluminação do posto de trabalho é fundamental para o seu bom desempenho.

ANEXO 4: AVALIAÇÃO DAS MENSAGENS

Pelo seu interesse, e como complemento do constante no capítulo sobre a forma como será avaliada a participação nos fóruns de discussão, transcrevemos do Guia do Formando Online documento a que todos os alunos têm acesso no espaço *online* do curso:

Qualidade da participação em fóruns de discussão

Não escreva só por escrever, nem para apenas dizer que concorda com determinada opinião expressa; diga que concorda ou não, mas avance sempre um pouco mais, por exemplo, explicando as razões da concordância ou discordância e, se possível, contribuindo com novos argumentos, novas ideias, novos pontos de vista, novas interrogações, relatos de experiências pessoais ou conhecidas, etc. Em suma, faça a discussão avançar.

Lembre-se de que um dos critérios de avaliação é o da “qualidade das mensagens” de acordo com uma tabela antecipadamente apresentada aos formandos, por exemplo a que é apresentada abaixo (Philips, 2000).

Categorias de Qualidade das Mensagens nos Fóruns de Discussão Online	
CATEGORIA	DESCRIÇÃO
E	Irrelevante; inútil
D	Demonstra acompanhamento das discussões
C	Tentativa de envolvimento na discussão; demonstra pouca compreensão dos assuntos; não faz progredir o debate
B	Bom contributo; demonstra compreensão; faz progredir o debate
A	Excelente contributo; demonstra compreensão profunda; leva o debate para novas áreas

ANEXO 5: A PLATAFORMAbERTA

Este curso desenvolve-se na PlataformAbERTA da UAb que integra o LMS Moodle. Martin Dougiamas lançou em 1999 a primeira versão do LMS Moodle (*modular object-oriented dynamic learning environment*) cuja base pedagógica é a abordagem social-construcionista da educação. Outras premissas do desenvolvimento deste software são o desenho modular, permitindo a evolução rápida das funcionalidades, e ainda uma filosofia open source na distribuição e desenvolvimento. O conceito fundamental consiste numa página, onde professores disponibilizam recursos e desenvolvem atividades com e para os alunos. Uma eventual metáfora para a página Moodle poderia ser a sala de aula ubíqua. A cada utilizador registado está associado um perfil e uma fotografia podendo comunicar com qualquer outro, reforçando a componente social desta plataforma. Atualmente, na versão 9, com milhares de utilizadores e developers, e traduzido para mais de 73 línguas, o Moodle tem-se revelado um importante Learning Management System devido à flexibilidade, valor educativo e facilidade de utilização graças à interface simples e amigável, mesmo para os utilizadores menos experientes.

O Moodle como sistema de gestão de ensino e aprendizagem apresenta funcionalidades com forte componente de participação, comunicação e colaboração entre formandos, formadores e pares. Enquanto *software* educativo, a componente de avaliação (*assessment and inquiry*) não poderia ser esquecida. São oferecidas ferramentas de avaliação específicas de diversas atividades, como a possibilidade de classificar (pelos formadores ou pares), através de escala elaborada para o efeito, discussões de fórum, trabalhos enviados ou realizados online, lições com questões, entradas de glossário, etc.

As principais funcionalidades do LMS Moodle são:

Fórum – é uma ferramenta de discussão por natureza, mas pode ter outro tipo de uso, como por exemplo uma *mailing list*, um blogue, um *wiki* ou mesmo um espaço de reflexão sobre um determinado conteúdo. Os fóruns do Moodle podem ser estruturados de diversas maneiras (discussão geral, uma única discussão, sem respostas, etc.) e podem permitir classificação de cada mensagem, (inclusivamente pelos alunos). As mensagens podem incluir anexos (imagem, pdf, doc, vídeo, áudio, zip).

Trabalho – os trabalhos permitem ao professor classificar e comentar na página Moodle materiais submetidos pelos alunos, ou atividades *offline* como por exemplo apresentações

(texto, *powerpoint*, gráficos/desenhos, etc.). As notas são do conhecimento do próprio aluno e o professor pode exportar os resultados para uma folha em Excel.

Chat – facilita a comunicação síncrona, através de pequenas mensagens, entre formadores e formandos. Pode ser útil como espaço de esclarecimento de dúvidas, mas pode ter outros usos. A sessão de chat pode ser agendada, com repetição.

Referendo – pode ser usado de diversas formas, como recolha de opinião ou inscrição numa determinada atividade, sendo dado aos formandos a escolher de uma lista de opções definida pelo formador.

Diálogo – permite a comunicação privada entre dois participantes da disciplina. O formador pode abrir um diálogo com um formando, o formando pode abrir um diálogo com o formador, e podem existir diálogos entre dois formandos.

Glossário – possibilita aos participantes da disciplina criar dicionários de termos relacionados com a disciplina, bases de dados documentais ou de ficheiros, galerias de imagens ou mesmo links que podem ser facilmente pesquisados. Cada entrada permite comentários e avaliação.

Lição – associa a uma lógica de *delivery* uma componente interativa e de avaliação. Consiste num número de páginas ou diapositivos, que podem ter questões intercaladas com classificação e em que o prosseguimento do aluno está dependente das suas respostas. Um conceito baseado na “aprendizagem programada de Skinner”.

Teste – o formador pode construir uma base de dados de perguntas e respostas. Os testes podem ter diferentes formatos de resposta (verdadeiro ou falso, escolha múltipla, resposta curta ou numérica, correspondência, etc.) e é possível escolher perguntas aleatoriamente, corrigir respostas automaticamente e exportar os dados para Excel.

Questionário – permite construir inquéritos quer a participantes de uma página, quer a participantes do Moodle. É possível manter o anonimato dos inquiridos, e os resultados podem ser exportados para Excel.

Wiki – torna possível a construção de um texto (com elementos multimédia) por vários participantes, onde cada um dá o seu contributo e/ou revê o texto. É possível aceder às várias versões do documento e verificar diferenças entre versões. Quem não conhece a Wikipedia® (<http://pt.wikipedia.org/>)?

(de *O Moodle e as comunidades virtuais de aprendizagem*,
por Paulo Legoinha, João Pais & João Fernandes)

ANEXO 6: MODELO DO CERTIFICADO DE FORMAÇÃO

ABERTA

CERTIFICADO de FORMAÇÃO

Certifica-se que natural de nascido(a) a portador(a) do BI n.º emitido pelos Serviços de Identificação Civil de em / / conduziu o Curso de Formação Profissional de nível (CE)

CURSO DE CIBERSEGURANÇA OFENSIVA

que decorreu de: / / 200 a / / 200 com a duração total de xxx horas (xx ECTS) tendo obtido a classificação final de

Lisboa, de de 200

O REITOR
(Professor Doutor Carlos Reis)



Curso: **CIBERSEGURANÇA OFENSIVA**

Modalidade de Formação: A distância online (*e-learning*)

Área de Formação: XXXXXXXX

Competências Adquiridas: XXXXXXXX

Módulo	Plano Curricular Designação	Duração
0		
1		
2		
7		
8		





UNIVERSIDADE
AbERTA
www.uab.pt