Informação Geral:

Unidade Orgânica	Escola Superior de Tecnologia e Gestão	**Ano Letivo**	2017/2018
Curso	Mestrado em Engenharia Informática - Computação Móvel (D) [M238]	**Grau**	Mestrado
Ano Curricular	1	**Período**	S2
UC/Módulo	Segurança Ofensiva em Sistemas Ubíquos a)	**ECTS**	6
Área Científica	Engenharia Informática	**Carácter**	Opcional

Horas Totais	161.6	**T**	0	**TP**	22.5	**PL**	30	**TC**	0	**S**	0	**E**	0	**OT**	0

T - Ensino Teórico; TP - Teórico Prático; PL - Prático e Laboratorial; TC - Trabalho de Campo; S - Seminário; E - Estágio; OT - Orientação Tutorial

Docente responsável:

Carlos Manuel da Silva Rabadão

Docentes que lecionam a unidade curricular:

Carlos Manuel Gonçalves Antunes (52,50 horas semanais de contacto: TP: 22,50; PL: 30,00;)

Pré-requisitos:

Não tem

Idioma:

Português e Inglês

Enquadramento:

A Segurança Ofensiva, também conhecida como Etical Hacking, recorre à utilização de ferramentas habitualmente utilizadas por hackers na execução de ciberataques, para testar as vulnerabilidades dos sistemas que se deseja proteger. Nesta unidade curricular pretende-se utilizar a segurança ofensiva para avaliação e mitigação de vulnerabilidades em sistemas ubíquos, redes e aplicações, com vista a dar uma visão global do processo de exploração e mitigação de falhas, tendo sempre em linha de conta as restrições, diretivas éticas e legalidade das atividades que envolvem um teste de penetração.

Numa primeira fase, caracterizam-se as principais ameaças e ataques em redes de comunicação sem fios, e os principais protocolos e tecnologias de segurança utilizados nestas redes. Numa fase posterior, pretende-se recriar cenários de ataque a estas redes e às aplicações móveis que as utilizem, explorando diversas ferramentas existentes para esta finalidade, nomeadamente as ferramentas da distribuição Linux Kali.

Objetivos de aprendizagem:

O1.Conhecimento das restrições éticas e legais associadas ao ethical hacking

O2.Domínio das etapas de desenvolvimento de testes de penetração e apresentação de resultados

O3.Identificação de aplicações/tráfego malicioso na rede

O4.Implementação de aplicações úteis na exploração de falhas

O5.Identificar ameaças e selecionar as medidas para impedir acesso físico a equipamentos e a mitigar ataques de engenharia social

O6.Aplicar as medidas corretivas adequadas à mitigação de falhas de segurança

O7.Identificar e resolver problemas nas aplicações e serviços web

O8.Determinar falhas de segurança em redes móveis, e para implementar soluções de segurança das comunicações

O9. Reforçar as competetências de planeamento/implementação de sistemas de IDS/IPS

O10. Reforçar as capacidades de planeamento/implementação de serviços de autenticação e controlo de acesso

O11. Identificar vulnerabilidades de dispositivos móveis e aplicação de medidas preventivas

O12. Avaliar o risco da utilização de aplicações móveis

Programa:

Conteúdos Programáticos:

C1. Introdução aos conceitos do Ethical hacking
C2. Tipos de ameaças e ataques a redes cabladas e sem fio
C3. Protocolos e algoritmos de segurança em redes 802.11 (Wireless LAN), 802.15 (wireless PAN); 802.16 (wireless WAN)
C4. Fragilidades protocolares dos sistemas de comunicações móveis
C5. Tecnologia de confidencialidade, privacidade e disponibilidade em redes sem fio
C6. Metodologias para testes de penetração
C7. Caracterização e implementação de ataques contra redes e sistemas móveis
C8. Planeamento de soluções de comunicação segura em redes e sistemas móveis
C9. Identificação e deteção de vulnerabilidades nos sistemas móveis
C10. Implementação de mecanismos e sistemas de segurança em redes sem fio e dispositivos móveis

Fundamentação da coerência dos conteúdos programáticos com os objetivos/competências da unidade curricular:

C1. Introdução aos conceitos do Ethical hacking (O1, O2))
C2. Tipos de ameaças e ataques a redes cabladas e sem fio (O3, O5)
C3. Protocolos e algoritmos de segurança em redes 802.11 (Wireless LAN), 802.15 (wireless PAN) e 802.16 (wireless WAN) (O5, O6)
C4. Fragilidades protocolares dos sistemas de comunicações móveis (O4)
C5. Tecnologia de confidencialidade, privacidade e disponibilidade em redes sem fio (O11)
C6. Metodologias para testes de penetração (O7, O8)
C7. Caracterização e implementação de ataques contra redes e sistemas móveis (O11)
C8. Planeamento de soluções de comunicação segura em redes e sistemas móveis (O10, 012)
C9. Identificação e deteção de vulnerabilidades nos sistemas móveis (O11)
C10. Implementação de mecanismos e sistemas de segurança em redes sem fio e dispositivos móveis (O9)

Metodologia de Ensino / Aprendizagem:

Presencial:

EP.1.Teórico-prático: i) Apresentação pelo professor dos conteúdos programáticos referentes aos capítulos 1 a 10 e a sua assimilação por parte dos estudantes
EP.2. i) Consolidação dos conhecimentos teórico-práticos, através da especificação e execução de procedimentos de ethical hacking associados a exemplos de serviços e sistemas ubiquos; ii) Realização de projeto laboratorial, que corresponde à consolidação dos conhecimentos adquiridos nas fases anteriores

Autónoma:

A1. Leituras complementares
A2. E-aprendizagem
A3. Trabalhos Laboratoriais

Recursos Específicos:

- Plataforma de gestão e distribuição de conteúdos
- Elementos de apoio disponibilizados pelos docentes
- Laboratório específico
- Máquinas virtuais

Avaliação:

Descrição:

AP=Avaliação Periódica

AP.1.Um prova escrita(classificação mínima: 8,0/20,0) (T1)

AP.2.Um teste prático (classificação mínima: 8,0/20,0) (T2)

AP.3.Um projeto (classificação mínima: 9,5/20,0) (P)

AP.4.Classificação final: CF=0,20T1+0,40T2+0,40P

PAF=Avaliação Final

AF.1.Uma prova escrita (classificação mínima: 8,0/20,0) (T)

AF.2.Um teste prático (classificação mínima: 9,5/20,0) (P)

AF.3.Classificação final: 0,20T+0,80P

- Quando tiverem sido obtidos os mínimos exigidos, as notas obtidas numa época de avaliação podem ser guardadas para as épocas subsequentes caso o estudante assim o pretenda.

- O estudante que se inscreva para melhoria de nota tem que realizar todos os elementos de avaliação da época em causa.

Número de elementos de avaliação final:	2
Número de elementos de avaliação contínua/periódica:	3

Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:

A metodologia de ensino teórico-prático baseia-se na transmissão de conhecimentos sobre a segurança ao nível da segurança ofensiva para avaliação e mitigação de vulnerabilidades em sistemas ubíquos, redes e aplicações, com vista a dar uma visão global do processo de exploração e mitigação de falhas, tendo sempre em linha de conta as restrições, diretivas éticas e legalidade das atividades que envolvem um teste de penetração. Permite desenvolver nos estudantes as competências (O1, O2, O3).

A metodologia utilizada na componente laboratorial incide, numa primeira fase, na consolidação dos conhecimentos transmitidos na componete teórico-prática atraves da realização de trabalhos laboratoriais (O1, O2, O3) e, numa fase posterior, na realização de um projeto prático, e que contempla as seguintes fases: a) estudo do cenário proposto, b) identificação de falhas e vulnerabilidades do cenário, c) seleção de mecanismos de exploração de vulnerabilidades adequados, d) realização de testes de penetração, e) mitigação de falhas detetadas e e) escrita de relatório e e) apresentação e defesa do projeto realizado, permitem desenvolver nos estudantes os objetivos (O4, O5, O6, O7, O8, O9, O10, O11, O12).

Bibliografia:

Recomendada:

Hacking Exposed 7; Stuart McClure, Joel Scambray; ISBN: 978-0071780285, McGraw-Hill Education; 7 ed., 2012
Gray Hat Hacking The Ethical Hacker's Handbook; Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn, Stephen Sims; ISBN: 978-0071832380; McGraw-Hill Education; 4 ed., 2015
Documentação disponibilizada pelo docente

Complementar:

The Hacker Playbook 2: Practical Guide To Penetration Testing, Paperback; Peter Kim; ISBN: 978-1512214567; CreateSpace Independent Publishing Platform, 2015.