

Segurança Apresentação

Agenda:

1. Enquadramento
2. Programa
3. Corpo docente
4. Avaliação

*Esta apresentação não dispensa a
leitura da *Ficha da Unidade*
Curricular disponível no Moodle.*

1

Enquadramento curricular

Ramo de Redes e Administração de Sistemas

3º Semestre

Introdução
Redes
Comunicação

4º Semestre

Serviços
Rede
1

Cablagem
Estruturada

Encaminhamento
Dados

Segurança

5º Semestre

Serviços
Rede
2

Tecnologias
Ligação

Disponibilidade
Desempenho

Gestão
Redes

As
competências
adquiridas em
IRC são
fundamentais

2

Programa

Objetivos

- *Compreender os princípios fundamentais bem como as tecnologias, ferramentas, e configurações disponíveis que envolvem a segurança de redes de comunicação.*

Programa (previsto)

1. Vulnerabilidades de segurança em sistema de informação e comunicação;
2. Tecnologias e mecanismos de encriptação;
3. Protocolos de comunicação seguros;
4. Tecnologias e mecanismos de autenticação;
5. Dispositivos de controlo de acesso (Firewalls, IDS, IPS)

Programa (detalhe)

Teórica (28h)	T	Prática (28h)	P
Segurança em redes	8	Reprodução de ataques	2
Criptografia	18	Protecção de equipamentos activos	4
Protocolo SSH	0	Autenticação centralizada	2
Protocolo SSL/TLS	2	Listas de controlo de acesso	8
Protocolo IPSec	0	Programação de firewalls	4
Segurança em redes WiFi	0	Sistemas de detecção de Intrusão	2
Norma IEEE 802.1x	0	Sistemas de prevenção de Intrusão	2
Segurança em redes VoIP	0	Segurança em LANs	2
Projeto de redes seguras	0	[Revisões]	2
Ataques e serviços de segurança	4		

Avaliação

Avaliação contínua

- Testes teórico 1 e 2; trabalho prático 1 e 2
 - Valoração individual: 25% (5 valores)
 - Mínimos : 35% (1,75 valores)
- Frequência
 - Mínimo: 18 horas Teórica e 18 horas Laboratorial

Avaliação por exame

- Exame escrito, com componente teórica e prática
 - Valoração: 50% (10 valores)
 - Trabalho prático 1 e 2: 25% (5 valores cada um)
 - Mínimos: 35% (3,5 e 1,75 valores, respetivamente)

Avaliação (datas importantes)

- **Teste 1** (5 valores): **30/03/2020**
- **Teste 2** (5 valores): **25/05/2020**
- **Trabalho Prático 1** (5 valores):
 - Diurno: **23/04/2020**
 - Pós-Laboral: **20/04/2020**
- **Trabalho Prático 2** (5 Valores):
 - Diurno: **4/06/2020**
 - Pós-Laboral: **1/06/2020**
- Os conteúdos abordados farão parte do programa em avaliação nos exames da disciplina.

Corpo docente

Teórica / Práticas (2h + 2h semana T+PL)

Pedro Vapi

vapi@isec.pt

Horário de atendimento

- Por solicitação / mail / moodle

Segurança & CCNA Security

Objetivo final










- Integrar formalmente o currículo "CCNA Security"
 - (80% da disciplina)
- Neste momento: vamos cobrir os principais conteúdos mas não será possível a inscrição formal dos alunos no currículo.



Nota: O exame de certificação CCNA Security (Cisco 640-553 IINS) apenas pode ser realizado por indivíduos com a certificação CCNA.



Segurança & CCNA Security

Course Outline		Segurança	Serviços de Rede I
Chapter	Goals		
1. Modern Network Security Threats	Explain network threats, mitigation techniques, and the basics of securing a network		
2. Securing Network Devices	Secure administrative access on Cisco routers		
3. Authentication, Authorization and Accounting	Secure administrative access with AAA		
4. Implementing Firewall Technologies	Implement firewall technologies to secure the network perimeter		
5. Implementing Intrusion Prevention	Configure IPS to mitigate attacks on the network		
6. Securing the Local Area Network	Describe LAN security considerations and implement endpoint and Layer 2 security features		
7. Cryptography	Describe methods for implementing data confidentiality and integrity		
8. Implementing Virtual Private Networks	Implement secure virtual private networks		
9. Putting It All Together	Given the security needs of an enterprise, create and implement a comprehensive security policy		

Segurança & Legislação

Legislação portuguesa

- < 1991 : Disposições avulsas no Código Penal
- 1991 : Lei da Criminalidade Informática (109/91, 17/Ago)
- 1995 : Criada a Brigada de Investigação de Criminalidade Informática - BICI
- 2009 : Lei 109/2009 de 15 de Setembro
- Outra legislação aplicável:



Lei n.º 109/2009

de 15 de Setembro

Aprova a **Lei do Cibercrime**, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

• <http://www.inst-informatica.pt/legislacao-e-directivas>

• <http://www.assoft.pt/default.asp?flag=1&idmenu=1&idsubmenu=7>

Segurança & Legislação

- Lei do Cibercrime (Lei 109/2009)
 - Moldura penal até 10 anos
 - Todos os crimes informáticos são crimes graves
 - Polícias recebem poderes acrescidos p/ combate
 - Comportamentos que instiguem ou auxiliem ataques informáticos são agora crime.



Atenção: Todo o software/hardware usado bem como experimentações realizadas no âmbito da disciplina estão obrigatoriamente limitados, de forma exclusiva, ao contexto de redes físicas ou virtuais isoladas e criadas para o efeito. !!!!! SEJA RESPONSÁVEL !!!!!

Referências

- Moodle: <https://moodle.isec.pt/moodle/course/view.php?id=8029>
- Fernando Boavida, Mário Bernardes, "Introdução à criptografia", FCA, 2019, ISBN 978-972-722-902-4
- Yusuf Bhajji, "Network security technologies and solutions", Cisco Press, 2008, ISBN 978-1-58705-246-0, 1A-6-183 (ISEC)
- Roberta Bragg, Mark Rhodes-Ousley, Keith Strassberg, "Network security : the complete reference", McGraw-Hill/Osborne, 2004, ISBN 0-07-222697-8, 1A-6-180 (ISEC)
- André Zúquete, "Segurança em Redes Informáticas", 2ª edição, FCA, 2008, ISBN 978-972-722-565-1 1A-6-138 (ISEC);
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", ISBN: 0-8493-8523-7, CRC-Press, 1997, (disponível on-line) <http://www.cacr.math.uwaterloo.ca/hac/>
- Denise Helfrich, Lou Ronnau, Jason Frazier, Paul Forbes, "Cisco network admission control", Vol I/II, Cisco Press, 2007, ISBN 1-58705-241-5, 1A-6-172 (ISEC)
- Bob Vachon, Rick Graziani, "Accessing the WAN : CCNA exploration companion guide", Cisco Press, 2008, ISBN 978-1-58713-205-6, 1A-6-181 (ISEC), 1A-6-181CD (ISEC);
- John Rullan, "Accessing the WAN : CCNA exploration labs and study guide", Cisco Press, 2008, ISBN 978-1-58713-201-8, 1A-6-174 (ISEC), 1A-6-174CD (ISEC);
- Amâncio Santos, José Marinho, José Rosado, Luís Santos, "CCNA 4: Acesso às redes WAN", 2008, 1A-6-193 (ISEC)