

Unidade Curricular	Segurança em Redes Informáticas	Área Científica	Ciências Informáticas
CTeSP em	Cibersegurança	Escola	Escola Superior de Tecnologia e Gestão de Bragança
Ano Letivo	2019/2020	Ano Curricular	2
Nível	0-2	Créditos ECTS	3.0
Tipo	Semestral	Semestre	2
Código	4087-639-2205-00-19		
Horas totais de trabalho	81	Horas de Contacto	T - TP - PL - TC - S - E - OT - O -

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

Nome(s) do(s) docente(s) Nuno Gonçalves Rodrigues

Resultados da aprendizagem e competências

- No fim da unidade curricular o aluno deve ser capaz de:
1. Descrever as ameaças à segurança que enfrentam as modernas infra-estruturas de rede
 2. Implementar medidas básicas de segurança em routers e switches Cisco
 3. Mitigar ameaças em redes usando ACLs e firewalls
 4. Implementar sistemas do tipo IPS e IDS para proteger redes contra ataques
 5. Mitigar ameaças ao e-mail, ataques baseados na web e ataques comuns à camada 2
 6. Proteger as comunicações para garantir integridade, autenticidade e confidencialidade
 7. Descrever a finalidade das VPNs e implementar VPNs de Acesso Remoto e VPNs Site-to-Site
 8. Proteger as redes de computadores usando firewalls Cisco ASA

Pré-requisitos

Antes da unidade curricular o aluno deve ser capaz de:
Demonstrar possuir conhecimentos e práticas fundamentais de Redes de Computadores

Conteúdo da unidade curricular

Ameaças modernas à segurança da rede. Proteção de dispositivos de rede. Autenticação, Autorização e Contabilização (AAA). Implementação de tecnologias de firewall e de Sistemas de Prevenção de Intrusão. Proteção da Rede Local. Sistemas criptográficos e implementação de redes privadas virtuais. Configuração da Cisco Adaptive Security Appliance (ASA). Administração de uma Rede Segura.

Conteúdo da unidade curricular (versão detalhada)

1. Ameaças Modernas à Segurança da Rede
 - Tornando as Redes Seguras
 - Ameaças à Rede
 - Mitigando Ameaças
2. Proteção dos Dispositivos de Rede
 - Proteção dos Dispositivos de Rede
 - Atribuição de Funções Administrativas
 - Monitorização e Gestão dos Dispositivos
 - Uso de Funcionalidades Automatizadas de Segurança
3. Autenticação, Autorização e Contabilização
 - Finalidades do Mecanismo AAA
 - Autenticação AAA Local
 - Servidor AAA
 - Autenticação baseada num Servidor AAA
 - Autorização e Contabilização baseada num Servidor AAA
4. Implementação de Tecnologias de Firewall
 - Listas de Controlo de Acesso
 - Tecnologias de Firewall
 - Firewalls Baseadas em Políticas de Zonas
5. Implementação de Sistemas de Prevenção de Intrusões
 - Tecnologias IPS
 - Assinaturas IPS
 - Implementação de Sistemas IPS
6. Proteção da Rede Local
 - Segurança de EndPoint
 - Considerações de Segurança do Nível 2
7. Sistemas Criptográficos
 - Serviços Criptográficos
 - Integridade e Autenticidade
 - Confidencialidade
 - Criptografia de Chave Pública
8. Implementação de Redes Privadas Virtuais
 - VPNs
 - Componentes e Operação das VPNs IPSec
 - Implementação de VPNs IPSec Site-to-Site usando a CLI
9. Implementação da Appliance de Segurança Cisco ASA
 - Introdução à ASA
 - Configurações da Firewall ASA
10. Funcionalidades Avançadas da ASA
 - Uso do Security Device Manager para gestão da ASA
 - Configuração de VPNs na ASA
11. Gestão de uma Rede Segura
 - Testar a Segurança da Rede
 - Desenvolvimento de uma Política de Segurança Abrangente

Bibliografia recomendada

1. Cisco Networking Academy, CCNA Security 2.01, Cisco Systems, 2019
2. Zúquete, A., Segurança em Redes Informáticas, FCA, 2013
3. Stallings, W., Network Security Essentials, Prentice Hall, 2003
4. Stallings, W., Cryptography and Network Security, Pearson, 2006

Métodos de ensino e de aprendizagem

Exposição e explicação dos conteúdos programáticos, ilustrada com exemplos. Exercitação dos conceitos teóricos, através da realização de trabalhos práticos e laboratoriais.

Alternativas de avaliação

1. Alternativa 1 - Avaliação contínua - (Ordinário, Trabalhador) (Final)
 - Trabalhos Práticos - 60% (Trabalhos práticos e laboratoriais.)
 - Exame Final Escrito - 40% (Avaliação final teórica. Nota mínima: 35%)
2. Alternativa 2 - Avaliação de Recurso - (Ordinário, Trabalhador) (Recurso, Especial)
 - Exame Final Escrito - 40% (Exame final teórico. Nota mínima: 35%)
 - Trabalhos Laboratoriais - 60% (Trabalho prático laboratorial.)

Língua em que é ministrada

Português, com apoio em inglês para alunos estrangeiros

Validação Eletrónica

Nuno Gonçalves Rodrigues	José Luís Padrão Exposto	Tiago Miguel Ferreira Guimaraes Pedrosa	Paulo Alexandre Vara Alves
03-03-2020	04-03-2020	04-03-2020	21-03-2020