

Unidade Curricular	Segurança em Redes Informáticas	Área Científica	Ciências Informáticas
CTeSP em	Cibersegurança	Escola	Escola Superior de Tecnologia e Gestão de Bragança
Ano Letivo	2020/2021	Ano Curricular	2
Nível	0-2	Créditos ECTS	3.0
Tipo	Semestral	Semestre	1
Código	4087-712-2008-00-20		
Horas totais de trabalho	81	Horas de Contacto	T - - TP 10 PL 20 TC - S - E - OT 30 O 51

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

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.

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

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
31-10-2020	11-11-2020	16-11-2020	23-11-2020