

Unidade Curricular	Segurança em Redes Informáticas	Área Científica	Ciências Informáticas
CTeSP em	Cibersegurança	Escola	Escola Superior de Tecnologia e Gestão de Bragança
Ano Letivo	2022/2023	Ano Curricular	2
Nível	0-2	Créditos ECTS	3.0
Tipo	Semestral	Semestre	1
Código	4087-712-2008-00-22		
Horas totais de trabalho	81	Horas de Contacto	T - , TP 7 , PL 23 , 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. Configurar regras de autorização na CLI usando níveis de privilégios e políticas baseadas em funções
4. Implementar a administração segura e a monitorização de dispositivos de rede
5. Configure a framework AAA para proteger uma rede
6. Mitigar ameaças em redes usando ACLs e firewalls do tipo ZPF

### 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. Mitigação de Ameaças. Proteção dos dispositivos de rede. Autenticação, Autorização e Contabilização (AAA). Implementação de tecnologias de firewall e de Sistemas de Prevenção de Intrusão.

### Conteúdo da unidade curricular (versão detalhada)

1. Proteção das Redes
  - Situação atual
  - Visão geral das topologias de rede
2. Ameaças à Rede
  - Quem está a atacar a nossa rede?
  - Ferramentas dos agentes de ameaças
  - Malware
  - Tipos de ataques de rede
3. Mitigação de Ameaças
  - Políticas de segurança de rede
  - Ferramentas, plataformas e serviços de segurança
  - Mitigação de ataques típicos à rede
  - Framework de proteção da Cisco Network Foundation
4. Proteção do Acesso aos Dispositivos
  - Proteção do router de fronteira
  - Configuração do acesso administrativo seguro
  - Configuração de segurança reforçada para logins virtuais
  - Configuração do SSH
5. Atribuição de Funções Administrativas
  - Configuração de níveis de privilégios
  - Configuração da CLI com base em funções
6. Monitorização e Gestão de Dispositivos
  - Imagem segura no Cisco IOS e ficheiros de configuração
  - Proteção do router com o Autosecure
  - Autenticação dos protocolos de encaminhamento
  - Administração e Reporting Seguros
  - Segurança de Rede com Syslog
  - Configuração do NTP
  - Configuração do SNMP
7. Autenticação, Autorização e Contabilização (AAA)
  - Características AAA
  - Configuração da autenticação AAA local
  - Características e protocolos AAA baseados em servidor
  - Configuração da autenticação baseada em servidor
  - Configuração da autorização e contabilização baseadas em servidor
8. Listas de Controlo de Acesso
  - Introdução às ACL
  - Máscaras curinga
  - Configuração e modificação de ACLs
  - Implementação de ACLs
  - Mitigação de ataques com ACLs
  - ACLs IPv6
9. Tecnologias de Firewall
  - Proteção das Redes com firewalls
  - Firewalls no projeto de rede
10. Firewalls baseadas em políticas de zonas (ZPF)
  - Introdução às ZPF
  - Operação das ZPF
  - Configuração de uma ZPF
11. Tecnologias IPS
  - Características dos IDS e IPS
  - Implementações IPS
  - IPS nos Cisco ISR
  - Analisador de porta em Switches Cisco

**Bibliografia recomendada**

1. Cisco Networking Academy, Network Security 1. 0, Cisco Systems, 2021
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
12-10-2022	12-10-2022	13-10-2022	24-10-2022