

Unidade Curricular	Laboratórios de 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
Tipo	Semestral	Semestre	1	Créditos ECTS	3.0
Horas totais de trabalho		81	Horas de Contacto		T - - TP 7 PL 23 TC - S - E - OT - O -
<small>T - Ensino Teórico; TP - Teórico Prático; PL - Prático e Laboratorial; TC - Trabalho de Campo; S - Seminário; E - Estágio; OT - Orientação Tutoria; O - Outra</small>					

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. Explicar como os sistemas de prevenção de intrusões baseados em rede são usados para ajudar a proteger uma rede.
2. Explicar vulnerabilidades de endpoint e métodos de proteção.
3. Implementar medidas de segurança para mitigar ataques da camada 2.
4. Explicar como os tipos de criptografia, hashes e assinaturas digitais funcionam em conjunto para fornecer confidencialidade, integridade e autenticação.
5. Explicar como a infraestrutura de chave pública é usada para garantir a confidencialidade dos dados e fornecer autenticação.
6. Configurar uma VPN IPsec site a site.
7. Explicar como a ASA opera como uma avançada stateful firewall e implementar uma configuração de firewall ASA.
8. Testar a segurança da rede.

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

Implementação e operação de IPS. Segurança de Endpoint. Segurança na camada 2. Serviços criptográficos. Integridade e autenticidade. Criptografia de chave pública. Implementação de VPNs. Introdução à firewall ASA. Configuração da firewall ASA. Testes de segurança da rede.

Conteúdo da unidade curricular (versão detalhada)

1. Operação e implementação de um IPS
 - Assinaturas IPS
 - IPS Cisco Snort
 - Configuração do IPS Snort
2. Segurança de Endpoint
 - Visão geral da segurança de endpoint
 - Autenticação 802.1X
3. Segurança na Camada 2
 - Ameaças de segurança na camada 2
 - Ataques à tabela MAC
 - Mitigação de ataques à tabela MAC
 - Mitigação de ataques à infraestrutura de VLANs
 - Mitigação de ataques ao DHCP
 - Mitigação de ataques ao ARP
 - Mitigação de ataques de falsificação de endereços
 - Protocolo Spanning Tree (STP)
 - Mitigação de ataques ao STP
4. Serviços criptográficos
 - Comunicações Seguras
 - Criptografia
 - Criptanálise
 - Criptologia
5. Integridade e autenticidade
 - Gestão de Chaves
 - Confidencialidade
6. Criptografia de chave pública
 - Criptografia de chave pública com assinaturas digitais
 - Autoridades e o sistema de confiança PKI
 - Aplicações e impactos da criptografia
7. VPNs
 - Visão geral das VPNs
 - Topologias de VPN
 - Visão geral do IPsec
 - Protocolos IPsec
 - O protocolo Internet Key Exchange
8. Implementação de VPNs IPsec Site a Site na CLI
 - Configurar uma VPN IPsec Site a Site
 - Política ISAKMP
 - Política IPsec
 - Mapas criptográficos
 - VPN IPsec
9. Introdução à firewall ASA
 - Soluções ASA
 - A ASA 5506-X com serviços FirePOWER
10. Configuração da Firewall ASA
 - Configuração Básica da Firewall ASA
 - Definição de configurações e serviços de administração
 - Grupos de Objetos
 - ACLs na ASA
 - Serviços NAT numa ASA
 - Framework AAA
 - Políticas de serviço numa ASA
 - Resumo da configuração da firewall ASA
11. Teste de segurança da rede
 - Técnicas de teste de segurança da rede

Conteúdo da unidade curricular (versão detalhada)

- Ferramentas de teste de segurança da rede

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