2024

Segurança de Redes e Sistemas Informáticos

Tecnologias de Informação Web e Multimédia

GONÇALO FILIPE DOS SANTOS GARRIDO - A038702

Trabalho Prático

Orientador:

Cláudia Freitas

Índice

Introdução

No âmbito da unidade curricular de Segurança de Redes e Sistemas Informáticos, do segundo semestre do segundo ano da licenciatura em Tecnologias de Informação Web e Multimédia, foi-nos proposta a realização de um trabalho prático, utilizando a ferramenta Cisco Packet Tracer e o respetivo relatório técnico para a empresa XPTO. O principal objetivo deste trabalho é, a partir do enunciado que nos foi entregue, configurar e reestruturar a rede de uma empresa para que esta fique mais segura.

Para contextualizar as mudanças efectuadas na rede, irei também mostrar como se encontrava a rede da empresa antes das alterações. Isto inclui uma análise detalhada da topologia de rede inicial, dos dispositivos utilizados, das configurações de segurança existentes (ou a falta delas) e dos potenciais riscos e vulnerabilidades identificados.

A reestruturação da rede envolverá a implementação de diversas medidas de segurança, tais como a segmentação da rede através de VLANs, a configuração de firewalls e listas de controlo de acesso (ACLs), a utilização de protocolos seguros para a gestão de dispositivos, e a implementação de sistemas de deteção e prevenção de intrusões (IDS/IPS).

Além disso, será dada atenção à configuração de políticas de segurança para acesso remoto, garantindo que todas as conexões externas são devidamente autenticadas e encriptadas. A gestão de utilizadores e a atribuição de permissões de acesso também serão revistas, assegurando que apenas o pessoal autorizado tem acesso aos recursos críticos da rede.

Por fim, o relatório técnico incluirá uma comparação entre o estado inicial e o estado final da rede, destacando as melhorias implementadas e os benefícios obtidos em termos de segurança e desempenho. Esta análise será suportada por diagramas de rede, capturas de configuração e testes de segurança realizados antes e depois das alterações.

Rede Original

No início, a configuração da rede na empresa refletia a organização apresentada nesta tabela.

Sede 192.168.20.0/24	Rede A	100 utilizadores
		5 impressoras de rede
		6 switches
Escritório 1	Rede B 192.168.21.0/24	50 utilizadores
		3 impressoras de rede
		3 switches
	Rede C 192.168.22.0/24	20 utilizadores
		2 impressoras de rede
		3 switches
Escritório 2	Rede D 192.168.23.0/24	20 utilizadores
		2 impressoras de rede
		3 switches
	Rede E 192.168.24.0/24	20 utilizadores
		2 impressoras de rede
		3 switches

Configuração inicial e desenho da rede

Em primeiro lugar, foi essencial começar por definir os IPs das redes e de cada equipamento. As redes A, B, C, D e E mantiveram os mesmos endereços IPs: Rede A - 192.168.20.0/24, Rede B - 192.168.21.0/24, Rede C - 192.168.22.0/24, Rede D - 192.168.23.0/24, Rede E - 192.168.24.0/24. Os routers foram configurados com os endereços de rede 10.0.0.0/30 para garantir uma comunicação eficiente entre as sub-redes.

No que respeita ao desenho inicial da rede, o esquema no Cisco Packet Tracer manteve-se inalterado; contudo, foram adicionadas impressoras em cada uma das redes para atender às necessidades específicas de impressão de cada departamento. Além disso, a configuração das impressoras foi realizada de forma a garantir que estivessem corretamente integradas na rede, com endereços IP estáticos atribuídos a cada uma para evitar conflitos e facilitar a sua gestão.

Esta abordagem inicial de definição de IPs e manutenção do esquema original, com a adição das impressoras, estabeleceu uma base sólida para as subsequentes melhorias de segurança e otimização da rede.

Reestruturação da Rede

Este relatório tem como objetivo apresentar as propostas de alteração na rede da empresa XPTO para aumentar a sua segurança. A solução inclui a substituição do protocolo Telnet pelo protocolo SSH, a criação e implementação de VLANs, a configuração e criptografia de passwords, a utilização do protocolo OSPF e a implementação de ACLs.

Substituir Telnet por SSH

O protocolo Telnet é usado "para fornecer uma instalação de comunicação bidirecional, interativa e orientada a texto que utiliza uma conexão de terminal virtual." (Cisco, 2023). Por outro lado, o protocolo SSH (Secure Shell) "é um protocolo de rede criptográfico para operar serviços de rede com segurança numa rede não segura." (Cisco, 2023).

A empresa XPTO possui o Telnet ativo em todos os equipamentos. Para tornar a gestão remota mais segura, uma das medidas a implementar é substituir o protocolo Telnet pelo protocolo SSH nos equipamentos. Enquanto o Telnet transmite informações em texto simples, o SSH utiliza criptografia em todas as comunicações, tornando assim a gestão remota mais segura.

Para configurar esta mudança, utilizámos o comando “transport input ssh” nos dispositivos. Para verificar se a configuração foi aplicada corretamente, utilizámos o comando “show running-config | section line vty”. Esta configuração garante que todas as sessões de gestão remota sejam realizadas de forma segura, protegendo as credenciais e comandos transmitidos entre os administradores e os equipamentos de rede.

Esta substituição é crucial para a segurança da rede, uma vez que evita que informações sensíveis sejam facilmente interceptadas por atacantes em redes não seguras, melhorando assim a integridade e confidencialidade das comunicações.

```
R1#show running-config | section line vty
line vty 0 4
 exec-timeout 5 30
 password 7 0822455D0A16
 login
 transport input ssh
```

Criar VLANS

Uma VLAN (Virtual Local Area Network) é uma rede local virtual, onde cada VLAN funciona como uma rede independente. Um dos seus benefícios é a maior segurança, pois apenas os dispositivos na mesma VLAN podem comunicar entre si. Na empresa XPTO, uma das soluções seria criar VLANs em cada switch. Isso contribuirá para uma maior segurança e melhor organização da rede. Entre as VLANs criadas em cada switch estão as VLANs para as impressoras e para os utilizadores. O comando para verificar as VLANs criadas é "show vlan brief". Por exemplo, no Switch2, foram criadas as VLANs 10 e 20 para as impressoras e para os utilizadores (hq), respetivamente.

```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   impressoras                      active    Fa0/3
20   hq                               active    Fa0/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

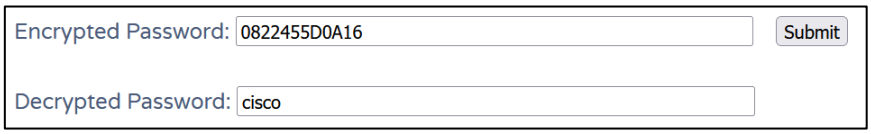
Criar e Criptografar Passwords

Para prevenir acessos não autorizados, é essencial criar passwords e criptografá-las. Foram estabelecidas passwords para proteger o acesso do utilizador ao modo EXEC, ao modo privilegiado e para proteger as linhas vty. É igualmente importante definir o comprimento das passwords e o número de tentativas de erro permitidas ao introduzi-las.

Para criptografar as passwords, é necessário utilizar o comando “service password-encryption” após a sua configuração. Para ver um exemplo da encriptação das passwords nas linhas vty, utilizei o comando “show running-config | section line vty”.

```
R3#show running-config | section line vty
line vty 0 4
 exec-timeout 5 30
 password 7 0822455D0A16
 login
 transport input ssh
```

Com o auxílio de um site que desencripta passwords, é possível verificar que a sequência alfanumérica "0822455D0A16" corresponde à password "cisco" após encriptação.



Nota: No Cisco Packet Tracer, as passwords utilizadas foram "cisco" e "class".

OSPF

O protocolo OSPF (Open Shortest Path First) tem como objetivo permitir que cada nó tenha uma visão da topologia da rede e descubra qual é a melhor rota para um determinado destino (Wikipédia, 2023). Os comandos realizados nos routers servem para tornar a interface passiva, o que significa que ela não envia pacotes OSPF, e também indicam quais interfaces participam no processo de routing.

```
R3#show running-config | section ospf
router ospf 1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/1
 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.0.4 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.255 area 0
 network 192.168.24.0 0.0.0.255 area 0
```

ACLs

As ACLs (Access Control Lists) são utilizadas para controlar o tráfego que pode entrar ou sair de uma interface de rede. Aqui está um exemplo de como configurar ACLs para aumentar a segurança da rede:

```
plaintext
Copiar código
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Este comando cria uma ACL chamada "1" que permite o tráfego da sub-rede 192.168.1.0/24.

```
plaintext
Copiar código
Router(config)# access-list 1 deny any
```

Este comando nega o acesso a qualquer outro tráfego que não seja da sub-rede especificada.

```
plaintext
Copiar código
Router(config)# interface FastEthernet0/0
Router(config-if)# ip access-group 1 in
```

Este comando aplica a ACL ao tráfego que entra na interface FastEthernet0/0 do router.

Esta é uma configuração básica de ACL para bloquear tráfego indesejado na interface especificada. Podem ser criadas ACLs mais complexas para atender a requisitos específicos de segurança da rede.

Referências

(14 de abril de 2023). Obtido em 29 de maio de 2024, de Cisco: https://www.cisco.com/c/pt_br/support/docs/ip/telnet/200718-Configure-Telnet-SSH-Access-to-Device-wi.html

Wikipédia. (27 de agosto de 2023). *Open Shortest Path First*. Obtido em 1 de junho de 2024, de https://pt.wikipedia.org/wiki/Open_Shortest_Path_First