Packet Tracer – Configurando a Segurança de Portas do Switch

Topologia

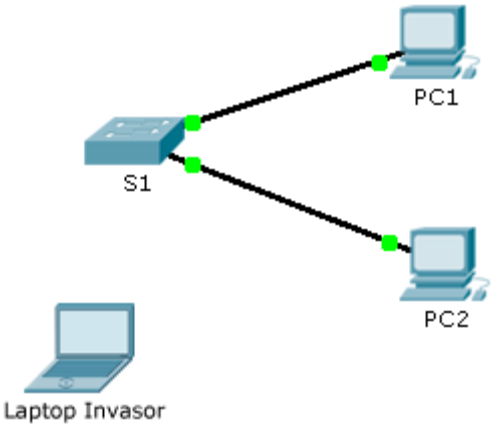

Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Laptop Invasor	Placa de rede	10.10.10.12	255.255.255.0

Objetivo

Parte 1: Configurar a segurança de portas

Parte 2: Verificar a segurança de portas

Histórico

Nesta atividade, você irá configurar e verificar a segurança de portas em um switch. A segurança de portas permite restringir o tráfego de ingresso em uma porta por meio da limitação de endereços MAC autorizados a encaminhar o tráfego para a porta.

Parte 1: Configurar a segurança da porta

a. Acesse a linha de comando para **S1** e ative a segurança de portas nas portas Fast Ethernet 0/1 e 0/2.

```
S1(config)# interface range fa0/1 – 2
S1(config-if-range)# switchport port-security
```

b. Defina o máximo de modo que somente um dispositivo possa acessar as portas Fast Ethernet 0/1 e 0/2.

```
S1(config-if-range)# switchport port-security maximum 1
```

c. Proteja as portas para que o endereço MAC de um dispositivo seja dinamicamente reconhecido e adicionado à configuração em execução.

```
S1(config-if-range)# switchport port-security mac-address sticky
```


d. Defina a violação de modo que as portas Fast Ethernet 0/1 e 0/2 não sejam desabilitadas quando ocorrer uma violação, mas que os pacotes sejam descartados de uma fonte desconhecida.

```
S1(config-if-range)# switchport port-security violation restrict
```

e. Desabilite todas as portas não utilizadas. Dica: use a palavra-chave **range** para aplicar simultaneamente essa configuração em todas as portas.

```
S1(config-if-range)# interface range fa0/3 – 24 , gi1/1 – 2
```

```
S1(config-if-range)#shutdown
```

Parte 2: Verifique a segurança de portas

a. Do **PC1**, faça ping para o **PC2**.

b. Verifique se segurança de portas está ativada e se o endereço MAC de **PC1** e **PC2** foram adicionados à configuração em execução.

c. Conecte o **Laptop Invasor** a qualquer porta de switch não usada e observe que as luzes de link estão vermelhas.

d. Ative a porta e verifique se o **Laptop Invasor** pode fazer ping no **PC1** e **PC2**. Após a verificação, desligue a porta conectada ao **laptop invasor**.

e. Desconecte **PC2** e conecte o **Laptop Invasor** à porta de **PC2**. Verifique se o **Laptop Invasor** não consegue executar ping para **PC1**.

f. Exiba as violações de segurança de portas para a porta na qual o **laptop invasor** está conectado.

```
S1# show port-security interface fa0/2
```

g. Desconecte o **Laptop Invasor** e reconecte **PC2**. Verifique se **PC2** pode executar ping para **PC1**.

h. Por que **PC2** pode executar ping para **PC1**, mas o **Laptop Invasor** não pode? A segurança da porta que foi habilitada na porta permitiu que apenas o dispositivo, cujo MAC foi aprendido primeiro, acessasse a porta enquanto impedia que outros dispositivos acessassem.

