Packet Tracer - Registro de atividade de rede

Tabela de Endereçamento

Dispositivo	Endereço IP privado	Endereço IP público
FTP_server	192.168.30.253	209.165.200.227
SYSLOG_SERVER	192.168.11.254	209.165.200.229
Router2	N/A	209.165.200.226

Objetivos

Parte 1: Criar tráfego FTP.

Parte 2: Investigar o tráfego de FTP

Parte 3: Ver mensagens do Syslog

Background

Nesta atividade, você usará o Packet Tracer para analisar e registrar o tráfego de rede. Você visualizará uma vulnerabilidade de segurança em um aplicativo de rede e exibirá o tráfego ICMP registrado com syslog.

Instruções

Parte 1: Crie tráfego de FTP.

Etapa 1: Ative o dispositivo de analise.

a. Clique no dispositivo **sniffer Sniffer1**.

b. Vá para a guia **Físico** e ative a alimentação do sniffer.

c. Vá para a guia **GUI** e ative o serviço sniffer.

d. Os pacotes FTP e syslog que entram no sniffer do Roteador 2 estão sendo monitorados.

Etapa 2: Conecte-se remotamente ao servidor FTP.

a. Clique em **PC-B** e vá para a área de trabalho.

b. Clique em **Prompt de comandot**. No prompt de comando, abra uma sessão FTP com **FTP_SERVER** usando seu endereço IP público. A ajuda com a linha de comando está disponível digitando **?** no prompt.

c. Digite o nome de usuário **cisco** e a senha **cisco** para autenticar com o **FTP_Server.**

Etapa 3: Faça o upload de um arquivo para o servidor FTP.

a. No prompt **ftp>**, digite o comando **dir** para visualizar os arquivos atuais armazenados no servidor FTP remoto.

b. Faça upload do arquivo **clientinfo.txt** para o servidor FTP digitando o comando **put clientinfo.txt.**

c. No prompt **ftp>**, digite o comando **dir** e verifique se o arquivo **clientinfo.txt** está agora no servidor FTP.

d. Digite **quit** no prompt FTP para fechar a sessão.

Parte 2: Investigar o tráfego de FTP

a. Clique no dispositivo **Sniffer1** e, em seguida, clique na guia **GUI** .

b. Clique em alguns dos primeiros pacotes FTP na sessão. Certifique-se de rolar para baixo para exibir as informações do protocolo da camada de aplicativo nos detalhes do pacote de cada um. (Isso pressupõe que esta seja a sua primeira sessão de FTP. Se você tiver aberto outras sessões, limpe a janela e repita o processo de login e transferência de arquivos.)

Qual é a vulnerabilidade de segurança apresentada pelo FTP?

O que deve ser feito para mitigar essa vulnerabilidade?

Parte 3: Ver mensagens no syslog

Etapa 1: Conecte-se remotamente ao Roteador 2.

a. Da linha de comando **PC-B** , telnet para **Roteador 2**.

b. Use o nome de usuário **ADMIN** e senha **CISCO** para autenticação.

c. Digite os seguintes comandos no prompt do roteador:

```
Router2# debug ip icmp
```

d. Digite **logout** no prompt para fechar a sessão Telnet.

Etapa 2: Gerar e exibir as mensagens do syslog.

a. Clique no dispositivo **SYSLOG_SERVER** e vá para a guia **Serviços**.

b. Clique no serviço **SYSLOG**. Verifique se o serviço está ativado. As mensagens do Syslog aparecerão aqui.

c. Vá para o host PC-B e abra a guia **Área de trabalho**.

d. Abra o **prompt de comando** e **ping** Router2.

e. Vá para o host PC-A e abra a guia **Área de Trabalho**.

f. Vá para o Prompt de Comando e **ping** Router2.

g. No servidor syslog investigue as mensagens registradas.

h. Deve haver quatro mensagens de PC-A e quatro PC-B.

Você pode dizer quais respostas de eco são para PC-A e PC-B a partir dos endereços de destino? Explique.

i. **Ping** Router2 a partir do PC-C.
Qual será o endereço de destino para as respostas?