**Projeto Cyber Segurança – Relatório de Captura de Pacotes**

**Teste 01 – Ping ICMP (Echo Request/Reply)**

**Ambiente**: Rede sem ASAv (vulnerável)

**Data**: [24/10/2025]

**Atacante (PC1):** 192.168.20.10

**Vítima (PC2):** 192.168.10.10

**Ferramenta de captura:** Wireshark (modo terminal via tshark)

**Arquivo gerado:** ping\_icmp.pcap

**Local:** CapturasWiresahck/Reconhecimento/

**Objetivo do Teste**

Verificar a conectividade básica entre as VLANs 20 e 10, demonstrando que o atacante pode alcançar diretamente a vítima via protocolo ICMP, sem qualquer bloqueio ou inspeção.

**Comando Executado**

ping -c 4 192.168.10.10

**Análise da Captura**

A captura realizada com o Wireshark mostra claramente os seguintes elementos:

• **Pacotes ICMP tipo 8 (Echo Request)** enviados do PC1 para o PC2

• **Pacotes ICMP tipo 0 (Echo Reply)** retornando da vítima para o atacante

• **Tempo de resposta (latência)** visível entre requisição e resposta

• **Ausência de bloqueio ou filtragem** → confirma que não há firewall ativo entre as VLANs

**Evidência Visual**

A captura inclui:

• Timestamps dos pacotes

• IP de origem e destino

• Protocolo ICMP identificado corretamente

• Informações como "Echo (ping) request" e "Echo reply"

**Resultado**

|  |  |
| --- | --- |
| **Item** | **Resultado** |
| Conectividade ICMP | Sucesso |
| Resposta da vítima | Recebida |
| Bloqueio por firewall | Não existente |
| Comunicação entre VLANs | Permitida |

**📌 Conclusão**

O teste de ping ICMP confirma que o ambiente sem ASAv permite comunicação direta entre dispositivos de VLANs distintas. Essa ausência de controle representa uma vulnerabilidade crítica, pois permite que qualquer dispositivo realize reconhecimento de rede e ataques subsequentes.

Uma imagem contendo Aplicativo

O conteúdo gerado por IA pode estar incorreto.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |