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

**Teste 04 – Nmap TCP SYN Scan (**nmap -sS)

**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:** nmap\_sS.pcap

**Local:** CapturasWireshark/reconhecimento/

**Objetivo do Teste**

Realizar uma varredura TCP do tipo SYN stealth para identificar portas abertas na vítima, sem completar a conexão TCP. Esse tipo de scan é comumente usado por atacantes para mapear serviços ativos sem gerar logs evidentes.

**Comando Executado**

sudo nmap -sS -Pn 192.168.10.10

**Análise da Captura**

A captura mostra:

• **Pacotes TCP com flag SYN** enviados do atacante para diversas portas da vítima

• **Respostas da vítima** variam entre:

• **SYN-ACK →** indica porta aberta

• **RST-ACK →** indica porta fechada

• O atacante responde com **RST** para evitar completar a conexão (técnica stealth)

• **Presença de ICMP tipo 3, código 1 →** "Host Unreachable", indicando falhas de roteamento ou ausência de resposta em alguns momentos

• **DNS e DHCP** aparecem como tráfego paralelo (ruído de rede)

**Detalhes Técnicos**

• Portas sondadas: 22, 135, 1723, 143, 5900, 139, 3306, 256, 80, 8080, 1025, 995, 199, 23

• Porta **22 (SSH)** respondeu com **SYN-ACK →** considerada aberta

• Demais portas responderam com **RST-ACK →** consideradas fechadas

• O atacante enviou **RST** após receber **SYN-ACK**, encerrando a tentativa de conexão

**Resultado do Teste – Nmap TCP SYN Scan**

• **Envio de pacotes SYN**: Realizado com sucesso

• **Porta aberta identificada**: 22 (SSH)

• **Portas fechadas**: 135, 1723, 143, 5900, 139, 3306, 256, 80, 8080, 1025, 995, 199, 23

• **Bloqueio por firewall**: Não existente

• **Comunicação entre VLANs:** Permitida

• **Ruído de rede**: DNS, DHCP, STP e CDP presentes

**Conclusão**

O teste confirma que o ambiente sem ASAv permite varredura TCP stealth sem qualquer inspeção ou bloqueio. A resposta SYN-ACK da porta 22 indica que o serviço SSH está ativo e acessível. Em redes protegidas, esse tipo de sondagem seria detectado e bloqueado por firewalls com inspeção de estado. Tela de computador

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.