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

**Teste 06 – Nmap Port Scan (nmap -p)**

**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:**

**Local:**

**Objetivo do Teste**

Realizar varredura de portas TCP na máquina vítima utilizando o Nmap com especificação direta de portas (). O objetivo é identificar quais serviços estão ativos e expostos, permitindo inferir vulnerabilidades e vetores de ataque.

**Comando Executado**

**Análise da Captura**

A captura mostra:

• **Pacotes TCP SYN** enviados da máquina atacante para múltiplas portas da vítima

• **Respostas TCP RST ou RST-ACK** da vítima indicando portas fechadas

• **Pacotes ICMP Echo Request e Timestamp Request** como parte do fingerprinting complementar

• **Respostas ICMP Echo Reply e Timestamp Reply** recebidas da vítima

• **Retransmissões TCP** indicando ausência de resposta ou perda de pacotes

• **Consultas DNS paralelas** para ntp.ubuntu.com e in-addr.arpa

• **Ruído de rede** como STP, CDP e ARP presentes na camada 2

**Detalhes Técnicos**

• **TCP SYN Scan:** Pacotes enviados para portas 21, 80, 443, 445, 993, 995, 1025, 1723, 256, 554, 111

• **Respostas da vítima:**

• Portas **80 e 443** responderam com , indicando fechadas

• Portas **445, 1723, 21, 993, 995, 1025, 554, 111, 256** também responderam com

• **ICMP replies:**

• Echo Reply com TTL=63

• Timestamp Reply com valores consistentes

**• TCP Retransmissions:** Indicando ausência de resposta ou tentativa de reconexão

• **DNS Queries:** Indicando resolução reversa e paralela durante o scan

• **ARP Broadcasts**: Solicitação de MAC para gateway ()

• **CDP e STP:** Tráfego de gerenciamento de switches visível

**Resultado do Teste – Nmap Port Scan**

• Portas escaneadas: 21, 80, 443, 445, 993, 995, 1025, 1723, 256, 554, 111

• Portas abertas: Nenhuma identificada

• Respostas ICMP: Recebidas com TTL padrão

• Retransmissões TCP: Presentes

• Firewall: Ausente ou permissivo

• Comunicação entre VLANs: Permitida

• Ruído de rede: STP, CDP, ARP, DNS visíveis

**Conclusão**

O teste confirma que, mesmo sem ASAv, a vítima não possui serviços ativos nas portas escaneadas. O ambiente permite coleta de informações detalhadas, como comportamento de rede, respostas ICMP e estrutura de pacotes TCP. Em redes protegidas, esse tipo de varredura seria bloqueado por firewalls com inspeção de estado ou IDS/IPS. A ausência de resposta nas portas indica que o sistema está minimamente exposto, mas ainda vulnerável a fingerprinting e análise passiva.

Uma imagem contendo Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.