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

**Teste 03 – Nmap UDP Scan (nmap -sU)  
Ambiente:** Rede sem ASAv (vulnerável) **Data:** [24/09/2025] **Atacante (PC1**): 192.168.20.10  
**Vítima (PC2**): 192.168.10.10  
**Ferramenta de captura**: Wireshark (modo terminal via tshark)  
**Arquivo gerado:** nmap\_sU.pcap  
**Local:** CapturasWireshark/Reconhecimento/

**Objetivo do Teste**

Avaliar a resposta da vítima a uma varredura UDP, identificando se há portas abertas, fechadas ou filtradas, e se a rede permite esse tipo de sondagem sem inspeção**.**

**Comando Executado**

sudo nmap -sU -Pn 192.168.10.10

**Análise da Captura**

**A captura mostra:**

* **Pacotes UDP** enviados para dezenas de portas da vítima, com tamanhos variados (Len=0, Len=40, Len=72)
* **Respostas ICMP tipo 3, código 3 →** "Destination Unreachable – Port Unreachable", indicando que as portas estão fechadas
* **Respostas ICMP tipo 3, código 1 →** "Host Unreachable", indicando falha de roteamento ou ausência de resposta

**Presença de DNS, MDNS e Portmap** como tráfego paralelo (ruído de rede) **Ausência de firewall:** os pacotes UDP chegam diretamente à vítima e as respostas ICMP retornam sem bloqueio

**Detalhes Técnicos**

* UDP enviado para portas como: 68, 22, 1043, 27015, 49220, 32780, 3052, 19500, 16680, 25709, entre outras
* ICMP retornado com tamanhos entre 70 e 142 bytes
* DNS queries para ntp.ubuntu.com e in-addr.arpa aparecem como tráfego de fundo
* MDNS e Portmap indicam serviços locais ativos, mas não relacionados ao teste

**Resultado do Teste – Nmap UDP Scan**

* **Envio de pacotes UDP:** Realizado com sucesso
* **Respostas ICMP da vítima:** Recebidas (Port Unreachable e Host Unreachable)
* **Bloqueio por firewall:** Não existente
* **Comunicação entre VLANs:** Permitida
* **Portas UDP abertas**: Não identificadas neste teste
* **Ruído de rede:** DNS, MDNS, DHCP e RPC presentes

**Conclusão**

O teste confirma que o ambiente sem ASAv permite varredura UDP sem qualquer inspeção ou bloqueio. As respostas ICMP indicam que as portas estão fechadas, mas o simples fato de o atacante receber essas respostas já representa uma falha de segurança. Em redes protegidas, esse tipo de sondagem seria filtrado ou ignorado.

Tela de computador

O conteúdo gerado por IA pode estar incorreto.