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

**Teste 05 – Nmap OS Detection (nmap -O)**  
**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\_O.pcap  
**Local:** CapturasWireshark/Fingerprinting/

**Objetivo do Teste**  
Identificar o sistema operacional da vítima por meio de técnicas de fingerprinting TCP/IP e ICMP. O Nmap utiliza padrões de resposta, TTL, tamanho de janela e comportamento de pacotes para inferir o tipo e versão do sistema operacional.

**Comando Executado**  
sudo nmap -O 192.168.10.10

Análise da Captura  
A captura mostra:

* Pacotes TCP com flag SYN enviados para diversas portas da vítima (ex: 22, 80, 443, 445, 3389, 1723, etc.)
* Respostas TCP da vítima:
  + SYN-ACK indicando porta 22 (SSH) aberta
  + RST-ACK indicando demais portas fechadas
* Pacotes ICMP Echo Request e Timestamp Request enviados como parte do fingerprinting
* Respostas ICMP Echo Reply e Timestamp Reply recebidas da vítima
* Pacotes com combinações incomuns de flags TCP (ex: FIN, PSH, URG) usados para testar comportamento do stack TCP
* Retransmissões e ACKs duplicados indicam tentativa de análise de tolerância e resposta do sistema
* DNS queries para ntp.ubuntu.com e in-addr.arpa como tráfego paralelo
* ARP, STP e CDP presentes como ruído de rede

**Detalhes Técnicos**

* Fingerprinting TCP: análise de resposta a pacotes SYN, FIN, PSH, URG e ACK em múltiplas portas
* Fingerprinting ICMP: uso de Echo e Timestamp para medir TTL e comportamento
* Porta 22 respondeu com SYN-ACK, indicando serviço ativo
* Outras portas responderam com RST-ACK, indicando ausência de serviço
* ICMP replies foram recebidos com TTL=63, janela padrão e sem fragmentação
* TCP Window Size, MSS e opções como SACK e Timestamps foram analisadas

**Resultado do Teste – Nmap OS Detection**

• Fingerprinting TCP/IP: Realizado com sucesso

• Respostas ICMP da vítima: Recebidas (Echo e Timestamp)

• Porta aberta identificada: 22 (SSH)

• Portas fechadas: 80, 443, 445, 3389, 1723, 135, 5900, entre outras

• Bloqueio por firewall: Não existente

• Comunicação entre VLANs: Permitida

• Sistema operacional identificado: Linux 4.15 – 5.8

• CPE: cpe:/o:linux:linux\_kernel:4 e cpe:/o:linux:linux\_kernel:5

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

**Conclusão**  
O teste confirma que o ambiente sem ASAv permite coleta de informações detalhadas sobre o sistema da vítima. As respostas ICMP e TCP fornecem dados suficientes para que o Nmap identifique o sistema operacional com alto grau de precisão. Em redes protegidas, esse tipo de fingerprinting seria bloqueado ou ofuscado por firewalls com inspeção de estado ou proxies de segurança.

Tela de computador com jogo

O conteúdo gerado por IA pode estar incorreto.