**Projeto Cyber Segurança – Relatório de Captura de Pacotes**  
**Teste 09 – Nmap Version Detection (nmap -sV)**  
**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\_sV.pcap  
**Local:** CapturasWireshark/Fingerprinting/

**Objetivo do Teste**  
Identificar os serviços ativos e suas respectivas versões na máquina vítima utilizando o Nmap com a opção -sV. Essa técnica permite obter banners e respostas específicas dos serviços, facilitando a identificação de vulnerabilidades conhecidas.

**Comando Executado**

sudo nmap -sV 192.168.10.10

**Análise da Captura**

* Handshake TCP completo com a porta 22/tcp (SSH):  
  SYN → SYN-ACK → ACK
* Banner SSH recebido:  
  SSH-2.0-OpenSSH\_9.6p1 Ubuntu-3ubuntu13.11
* Conexão encerrada corretamente com troca de FIN-ACK → ACK → FIN-ACK → ACK
* Outras portas escaneadas responderam com RST-ACK, indicando que estão fechadas
* Consultas DNS paralelas para ntp.ubuntu.com e in-addr.arpa
* Respostas ICMP “Destination unreachable” do gateway (192.168.20.1) para servidores externos
* Ruído de rede: STP, CDP, ARP visíveis

**Detalhes Técnicos**

* Serviço identificado: SSH
* Versão: OpenSSH\_9.6p1
* Sistema operacional inferido: Ubuntu (com base no banner)
* Porta ativa: 22/tcp
* Portas fechadas: 80, 443, 445, 3389, 5900, 3306, entre outras
* Banner completo: SSH-2.0-OpenSSH\_9.6p1 Ubuntu-3ubuntu13.11
* TCP Window Size e opções como MSS, SACK e Timestamps foram analisadas durante o handshake

**Resultado do Teste – Nmap Version Detection**

* Serviço ativo identificado: SSH
* Versão detectada com sucesso: OpenSSH\_9.6p1
* Sistema operacional inferido: Ubuntu
* Demais serviços: Não detectados (portas fechadas)
* Firewall: Ausente ou permissivo
* Comunicação entre VLANs: Permitida
* Ruído de rede: STP, CDP, ARP, DNS visíveis

**Conclusão**  
O teste confirma que o nmap -sV é eficaz para identificar serviços ativos e suas versões em ambientes desprotegidos. A detecção do banner SSH permite inferir o sistema operacional e a versão do serviço, o que pode ser explorado em ataques direcionados. Em redes protegidas, esse tipo de coleta seria bloqueado por firewalls com inspeção de estado ou proxies de aplicação