**Projeto Cyber Segurança – Relatório de Captura de Pacotes**  
**Teste 11 – Simulação de Ataque com hping3 (TCP SYN Flood e Reconhecimento)**  
**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:** hping3.pcap  
**Local:** CapturasWireshark/Ataques/

**Objetivo do Teste**  
Simular um ataque de reconhecimento e exaustão de recursos utilizando a ferramenta hping3. O teste visa observar o comportamento da vítima frente a múltiplos pacotes TCP com flag SYN, enviados em sequência e com variação de portas, simulando um ataque de TCP SYN Flood e coleta de informações sobre serviços ativos.

**Comando Executado (exemplo)**

sudo hping3 -S -p 80 --flood 192.168.10.10

**Análise da Captura**

* Pacotes TCP com flag SYN enviados em alta frequência para a porta 80 da vítima
* Portas de origem variando entre 1291 e 1310, e posteriormente reutilizadas (ex: 44430 a 44434)
* Janela TCP reduzida (Win=512), típica de ataques de exaustão
* Respostas da vítima com pacotes RST, ACK, indicando que a porta 80 está fechada ou que o serviço está rejeitando conexões
* Presença de pacotes ICMP “Destination unreachable” para tentativas de comunicação externa (8.8.8.8 e 1.1.1.1)
* Tráfego DNS paralelo para ntp.ubuntu.com
* Ruído de rede: STP visível em múltiplos momentos

**Detalhes Técnicos**

* Tipo de ataque: TCP SYN Flood
* Flag utilizada: SYN
* Porta alvo: 80/tcp
* Portas de origem: variáveis e reutilizadas
* Janela TCP: 512 bytes
* Resposta da vítima: RST, ACK (porta fechada)
* ICMP: mensagens de erro de roteamento
* DNS: consultas simultâneas durante o ataque
* STP: tráfego de controle de switches visível

**Resultado do Teste – hping3 TCP Flood**

* Ataque executado com sucesso
* Saturação da porta 80 simulada
* Respostas da vítima indicam rejeição de conexões
* Comunicação externa comprometida
* Ambiente sem firewall permitiu execução irrestrita do ataque
* Rede vulnerável a ataques de negação de serviço (DoS)

**Conclusão**  
O teste com hping3 demonstrou que o ambiente sem ASAv é suscetível a ataques de negação de serviço e varredura de portas. A resposta da vítima com pacotes RST, ACK confirma que o serviço está ativo, mas não aceitando conexões. Em redes protegidas, esse tipo de ataque seria mitigado por firewalls com inspeção de estado, rate limiting ou sistemas de detecção de intrusão (IDS).