**Projeto Cyber Segurança – Relatório de Captura de Pacotes**  
**Teste 10 – Descoberta de Hosts via ARP Scan (arp-scan)**  
**Ambiente:** Rede sem ASAv (vulnerável)  
**Data:** 24/10/2025  
**Atacante (PC1):** 192.168.20.10  
**Vítima (PC2):** 192.168.20.1 (gateway)  
**Ferramenta de captura:** Wireshark (modo terminal via tshark)  
**Arquivo gerado:** arp\_scan.pcap  
**Local:** CapturasWireshark/Descoberta/

**Objetivo do Teste**  
Executar uma varredura ARP na sub-rede local para identificar hosts ativos, seus respectivos endereços IP e MAC. O protocolo ARP é utilizado para mapear endereços IP para endereços físicos (MAC) em redes locais, sendo uma técnica eficaz para descoberta de dispositivos em ambientes sem proteção.

**Comando Executado**

sudo arp-scan --interface eth0 --localnet

**Análise da Captura**

* Pacotes ARP enviados pelo atacante para múltiplos IPs da sub-rede 192.168.20.0/24, incluindo:
  + IPs de 192.168.20.0 até 192.168.20.255
* Respostas ARP recebidas de dispositivos ativos, como o gateway (192.168.20.1)
* ARP Announcement para o próprio IP do atacante (192.168.20.10)
* MAC do atacante: 52:54:00:72:94:85
* MAC do gateway: aa:bb:cc:00:09:00
* Presença de tráfego de controle de rede: STP e CDP
* Tentativas de comunicação TCP e DNS com servidores externos (8.8.8.8 e 1.1.1.1) resultando em mensagens ICMP “Destination unreachable”
* Retransmissões TCP indicam ausência de resposta dos servidores externos

**Detalhes Técnicos**

* IPs consultados via ARP: de 192.168.20.0 até 192.168.20.255
* Hosts ativos identificados: pelo menos o gateway (192.168.20.1)
* ARP funcionando corretamente na sub-rede
* ARP Announcement visível para 192.168.20.10
* ICMP “Destination unreachable” recebido do gateway para tentativas de comunicação externa
* Tráfego STP e CDP sugere presença de switches gerenciáveis

**Resultado do Teste – ARP Scan**

* Hosts ativos identificados com sucesso
* MACs mapeados corretamente
* ARP operacional na sub-rede
* Comunicação externa bloqueada ou não roteada
* Ambiente sem firewall permite varredura ARP sem restrições
* Ruído de rede: STP, CDP, ARP visíveis

**Conclusão**  
O teste confirma que a técnica de ARP Scan é eficaz para descoberta de dispositivos em redes locais sem proteção. A resposta do gateway e o anúncio ARP do atacante demonstram que o protocolo está operacional e que a rede permite mapeamento completo de IPs e MACs. Em ambientes protegidos, esse tipo de varredura seria limitado por switches com proteção ARP, segmentação de broadcast ou firewalls com inspeção de camada 2.

Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.