Atividade extra

1. Envenenamento ARP: Pesquise sobre o ataque de envenenamento ARP e explique como ele funciona.
   R: Primeiro é necessário pontuar que há dois tipos de ataque ARP: o envenenamento ARP (ARP Poisoning) e a falsificação ARP (ARP Spoofing). Ambos operam de maneira semelhante, mudando apenas o resultado final do ataque.
   O ataque funciona geralmente com o broadcast de um Gratuitous ARP em uma rede que anuncia a alteração do IP de um determinado MAC para um novo IP, este sendo um IP inexistente (buraco negro) ou um dispositivo malicioso (alteração do IP do gateway para uma máquina maliciosa, por exemplo).
   O envenenamento resulta em DOS (Negação de serviço), pois a máquina de destino nunca é alcançada. Já o ARP Spoofing resulta em ataques do tipo MiTM (Man in The Middle), que é gravíssimo em trocas de informações não criptografadas, pois permite que o dispositivo intermediário acesse todas as informações da troca e, em caso de trocas criptografadas, é possível realizar o sequestro de sessão, que permite que o dispositivo malicioso possa se passar pelo dispositivo atacado em diversas aplicações (redes sociais, por ex).
2. Tempo de Vida do Cache ARP: Qual é a quantidade padrão de tempo que uma entrada permanece
   no cache ARP antes de ser removida? Como você determinou esse valor?
   R: No linux, há duas configurações para o tempo de vida do cache do ARP. É possível visualizar através dos seguintes arquivos: /proc/sys/net/ipv4/neigh/{INTERFACE_UTILIZADA}/gc_stale_time e /proc/sys/net/ipv4/neigh/{INTERFACE_UTILIZADA}/base_reachable_time_ms
   O primeiro arquivo é informado em segundos e é o intervalo do garbage collector do linux. Já o segundo arquivo é em milissegundos e define realmente o tempo de vida de cada registro na tabela ARP. Cada nova adesão à tabela ARP operará em um intervalo entre base_reachable_time_ms / 2 e 3*base_reachable_time_ms / 2. Por ex: valor informado = 30000 (30s), o novo registro ARP terá uma vida útil entre 15s e 45s.
   Fonte: https://serverfault.com/questions/684380/default-arp-cache-timeout