Atividade TDS:

-Endereços IP e MAC: Funções / Funcionamento, Configuração / Segurança nas Redes de Computadores:

-Definição e Função:

Os endereços IP e MAC são de extrema importância para a comunicação em redes de computadores, onde cada um possui um papel distinto.

-Endereço IP (Internet Protocol):

É um identificador numérico único atribuído a cada dispositivo conectado a uma rede que utiliza o protocolo IP. Podendo ser de dois tipos: IPv4 (por exemplo, 192.168.0.1) ou IPv6 por exemplo, (2001:0db8:85a3:0000:0000:8a2e:0370:7334). O endereço IP é responsável por identificar um dispositivo logicamente dentro de uma rede e permite que dados sejam roteados corretamente entre diferentes redes.

- Endereço MAC (Media Access Control):

É um identificador físico único gravado na placa de rede (NIC) de um dispositivo. Ele é representado por seis grupos de dois dígitos hexadecimais (por exemplo, 00:1A:2B:3C:4D:5E). O endereço MAC opera na camada de enlace de dados do modelo OSI e garante que os dispositivos possam se comunicar em uma rede local (LAN).

-Propósito:

O propósito de um endereço IP é permitir que os dispositivos se comuniquem através de redes externas (por exemplo, a internet), enquanto o endereço MAC permite a comunicação dentro de uma rede local. Ambos desempenham papéis essenciais e complementares na rede.

-Funcionamento:

Os endereços IP e MAC trabalham em conjunto para garantir a comunicação eficaz entre dispositivos. O endereço MAC é usado para a comunicação de dispositivos em uma rede local, como quando um computador se conecta a um roteador. O endereço IP, por sua vez, permite que dados sejam transmitidos de um dispositivo para outro através de diferentes redes.

Exemplo de comunicação:

1. Quando um computador deseja acessar um site, ele precisa descobrir o endereço MAC do roteador. Isso é feito através de um protocolo chamado ARP (Address Resolution Protocol), que mapeia endereços IP para endereços MAC.
2. Após essa resolução, o dispositivo envia o pacote de dados com o endereço IP de destino e o endereço MAC do roteador. O roteador, então, roteia o pacote para a internet.

-Configuração e Ferramentas:

Os endereços IP podem ser configurados manualmente ou atribuídos automaticamente via DHCP (Dynamic Host Configuration Protocol). Já os endereços MAC são fixos para cada dispositivo e geralmente não podem ser alterados (embora existam técnicas para falsificar endereços MAC, como veremos mais adiante).

-Ferramentas comuns para configurar e identificar esses endereços:

-ipconfig (Windows):

-No Prompt de Comando, digite “ipconfig /all”.

-Ele exibe informações detalhadas da rede, como o endereço IP (IPv4 e IPv6) e o endereço MAC (chamado de "Endereço Físico") das interfaces de rede.

-ifconfig (Linux/macOS):

- No terminal, digite “ifconfig”.

- O comando lista as interfaces de rede ativas e seus endereços IP e MAC. É útil para diagnosticar problemas de rede e verificar configurações.

-Wireshark:

- Abra o Wireshark e selecione uma interface de rede para começar a capturar pacotes.

- Após capturar dados, filtre por "ARP" para ver os endereços MAC ou "IP" para observar pacotes com endereços IP.

- Wireshark permite analisar o tráfego de rede, ajudando a identificar comunicação entre dispositivos e possíveis problemas de rede.

-Implicações Práticas e de Segurança:

Na prática, a existência de endereços IP e MAC distintos é útil para o gerenciamento de rede, diagnóstico de problemas e otimização de desempenho. Por exemplo, os administradores podem usar endereços MAC para controlar quais dispositivos podem se conectar a uma rede, através de técnicas de filtragem MAC, uma medida básica de segurança.

Porém, existem “ameaças de segurança” associadas a esses endereços:

-Spoofing de MAC: Um invasor pode falsificar o endereço MAC de um dispositivo para obter acesso não autorizado a uma rede.
-Spoofing de IP: Ocorre quando um invasor falsifica o endereço IP de um pacote para se passar por outro dispositivo. Isso pode ser usado para realizar ataques de negação de serviço (DoS) ou man-in-the-middle.

Essas ameaças podem ser mitigadas com algumas práticas de segurança:

-Filtragem de MAC: Restringir o acesso à rede apenas a dispositivos com endereços MAC permitidos.
-Autenticação forte e criptografia: Usar protocolos como WPA3 em redes sem fio para evitar o acesso não autorizado.
-Monitoramento de rede: Ferramentas como o Wireshark permitem que administradores identifiquem atividades suspeitas na rede, como tráfego anômalo que pode indicar um ataque de spoofing.