Exercicio Wireshark

1. Ethernet (ETH)

- **O que faz?**
    - Fornece comunicação em redes locais (LAN) transmitindo quadros (frames) entre dispositivos conectados.
    - Usa **endereços MAC** para identificar dispositivos na rede.
    - Opera na **camada 2** (Enlace) do modelo **OSI**.
- **Exemplo de uso:** Conexão entre computadores em um escritório usando cabos ou Wi-Fi.

---

2. Address Resolution Protocol (ARP)

- **O que faz?**
    - Traduz endereços IP (lógicos) para endereços MAC (físicos).
    - Permite que dispositivos na mesma rede local se comuniquem diretamente.
- **Exemplo de uso:** Quando um computador precisa saber o endereço MAC do roteador para enviar dados.

---

3. Reverse ARP (RARP)

- **O que faz?**
    - Descobre o endereço IP de um dispositivo com base no seu endereço MAC.
    - Foi substituído por protocolos mais modernos, como DHCP.
- **Exemplo de uso:** Dispositivos sem IP configurado automaticamente, como impressoras de rede antigas.

---

4. Internet Protocol (IP - IPv4 e IPv6)

- **O que faz?**

    - Roteia pacotes entre redes diferentes.
    - Define endereços IP para identificar dispositivos de forma única.
    - IPv6 resolve limitações do IPv4, como escassez de endereços.
- **Exemplo de uso:** Comunicação entre dispositivos conectados à Internet.

---

5. Internet Control Message Protocol (ICMP)

- **O que faz?**
    - Diagnostica problemas de rede e comunica erros.
    - Suporta comandos como **ping** para testar conectividade.
- **Exemplo de uso:** Identificar se um servidor está acessível ou detectar pacotes perdidos na rede.

---

6. Internet Group Management Protocol (IGMP)

- **O que faz?**
    - Gerencia grupos multicast (transmissão para vários dispositivos).
    - É usado para vídeos ao vivo, IPTV e conferências online.
- **Exemplo de uso:** Streaming de vídeo para vários dispositivos na mesma rede.

---

7. Transmission Control Protocol (TCP)

- **O que faz?**
    - Garante a entrega confiável e ordenada de pacotes.
    - Controla fluxos de dados, retransmitindo pacotes perdidos e corrigindo erros.
- **Exemplo de uso:** Transferência de arquivos (FTP) ou navegação segura na web (HTTPS).

---

8. User Datagram Protocol (UDP)

- **O que faz?**

    - Envia pacotes sem garantir entrega ou ordem (rápido, mas menos confiável).
    - Usado para comunicações em tempo real.
- **Exemplo de uso:** Vídeo chamadas, jogos online e streaming de mídia.

---

9. Dynamic Host Configuration Protocol (DHCP)

- **O que faz?**
    - Atribui automaticamente endereços IP e configurações de rede (DNS, gateway).
- **Exemplo de uso:** Conectar um smartphone ao Wi-Fi e receber automaticamente um endereço IP.

---

10. Domain Name System (DNS)

- **O que faz?**
    - Traduz nomes de domínio (ex: google.com) para endereços IP (ex: 172.217.10.46).
- **Exemplo de uso:** Acessar sites na Internet sem precisar memorizar endereços IP.

---

11. Hypertext Transfer Protocol (HTTP e HTTPS)

- **O que faz?**
    - **HTTP:** Transferência de páginas web e conteúdo.
    - **HTTPS:** Versão segura (criptografada com SSL/TLS).
- **Exemplo de uso:** Navegação em sites e envio de formulários online.

---

12. File Transfer Protocol (FTP)

- **O que faz?**
    - Transfere arquivos entre computadores e servidores.
    - Suporta envio e download de arquivos em redes locais ou remotas.
- **Exemplo de uso:** Enviar arquivos para um servidor web.

---

13. Simple Mail Transfer Protocol (SMTP)

- **O que faz?**
    - Envia e-mails entre servidores.
    - Usa comandos para especificar remetente, destinatário e conteúdo.
- **Exemplo de uso:** Enviar e-mails pelo Outlook ou Gmail.

---

14. Post Office Protocol (POP3) e Internet Message Access Protocol (IMAP)

- **O que faz?**
    - **POP3:** Baixa e-mails do servidor para o dispositivo local e os remove do servidor.
    - **IMAP:** Sincroniza e-mails entre dispositivos e mantém cópias no servidor.
- **Exemplo de uso:** Receber e-mails em aplicativos como Thunderbird e Outlook.

---

15. Simple Network Management Protocol (SNMP)

- **O que faz?**
    - Monitora e controla dispositivos de rede, como switches e roteadores.
    - Coleta informações sobre tráfego, desempenho e falhas.
- **Exemplo de uso:** Administrar redes corporativas e verificar status de equipamentos.

---

16. Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

- **O que faz?**
    - Criptografa dados transmitidos na rede para garantir privacidade e integridade.
    - TLS é a versão mais segura e moderna do SSL.

- **Exemplo de uso:** Proteção de transações bancárias e autenticação em sites seguros.

---

17. Secure Shell (SSH)

- **O que faz?**
  - Permite acesso remoto seguro a servidores e dispositivos de rede.
  - Criptografa dados para proteger contra espionagem.
- **Exemplo de uso:** Gerenciar remotamente um servidor Linux.

---

18. Trivial File Transfer Protocol (TFTP)

- **O que faz?**
  - Transferência simples de arquivos sem autenticação ou segurança.
  - Usado em redes locais para configurações rápidas.
- **Exemplo de uso:** Enviar configurações para switches ou roteadores.

WELL KNOWN PORTS

1. Comunicação e Transferência de Arquivos

Porta	Protocolo	TCP/UDP	Criptografia	Função
20	FTP (Data)	TCP	Não	Transferência de dados de arquivos.
21	FTP (Control)	TCP	Não	Controle e comandos FTP (login, navegação).
22	SSH / SFTP / SCP	TCP	Sim	Conexão segura e transferência criptografada de arquivos.
69	TFTP	UDP	Não	Transferência simplificada de arquivos sem autenticação.
989	FTPS (Data)	TCP	Sim	Transferência segura de dados via FTP com SSL/TLS.
990	FTPS (Control)	TCP	Sim	Controle seguro de FTP com SSL/TLS.

2. Protocolo de E-mail

Porta	Protocolo	TCP/UDP	Criptografia	Função
25	SMTP	TCP	Não	Envio de e-mails (não seguro).
110	POP3	TCP	Não	Recebimento de e-mails (download do servidor).
143	IMAP	TCP	Não	Gerenciamento de e-mails no servidor.
465	SMTPS	TCP	Sim	Envio seguro de e-mails com SSL/TLS.
587	SMTP Secure	TCP	Sim	Envio seguro de e-mails com STARTTLS.
993	IMAPS	TCP	Sim	Gerenciamento seguro de e-mails via IMAP com SSL/TLS.
995	POP3S	TCP	Sim	Recebimento seguro de e-mails via POP3 com SSL/TLS.

3. Navegação Web

Porta	Protocolo	TCP/UDP	Criptografia	Função
80	HTTP	TCP	Não	Navegação web (não segura).
443	HTTPS	TCP	Sim	Navegação web segura com SSL/TLS.
8080	HTTP Proxy / Alternate	TCP	Não	Alternativa para HTTP, geralmente para proxies.

4. Transferência Segura e VPN

Porta	Protocolo	TCP/UDP	Criptografia	Função
500	ISAKMP (IPsec)	UDP	Sim	Protocolo de estabelecimento de segurança para VPNs.
1701	L2TP (VPN)	UDP	Sim	Protocolo de túnel para VPNs (usado com IPsec).
4500	IPsec NAT-T	UDP	Sim	Túnel VPN para NAT traversal (com IPsec).
1194	OpenVPN	TCP/UDP	Sim	VPN baseada em SSL/TLS para conexões seguras.

5. Administração Remota e Monitoramento

Porta	Protocolo	TCP/UDP	Criptografia	Função
23	Telnet	TCP	Não	Acesso remoto não seguro (substituído por SSH).
3389	RDP (Remote Desktop)	TCP/UDP	Sim	Controle remoto seguro de computadores Windows.
161	SNMP	UDP	Não	Monitoramento de dispositivos de rede.
162	SNMP Trap	UDP	Não	Alertas e notificações de dispositivos de rede.

6. DNS e Serviços de Rede

Porta	Protocolo	TCP/UDP	Criptografia	Função
53	DNS	TCP/UDP	Não	Resolução de nomes de domínio para endereços IP.
853	DNS sobre TLS (DoT)	TCP	Sim	Resolução DNS segura com criptografia TLS.
67	DHCP Server	UDP	Não	Atribuição de IPs dinâmicos pelo servidor DHCP.
68	DHCP Client	UDP	Não	Solicitação de IPs dinâmicos pelo cliente DHCP.

7. Streaming e Multimídia

Porta	Protocolo	TCP/UDP	Criptografia	Função
123	NTP	UDP	Não	Sincronização de horário na rede.
554	RTSP	TCP/UDP	Não	Controle de streams de áudio e vídeo.
5004	RTP	UDP	Não	Transporte de mídia em tempo real.
5005	RTCP	UDP	Não	Controle e monitoramento do RTP.

8. Compartilhamento de Arquivos

Porta	Protocolo	TCP/UDP	Criptografia	Função
137	NetBIOS Name Service	UDP	Não	Resolução de nomes em redes Windows.
138	NetBIOS Datagram Service	UDP	Não	Transmissão de mensagens em redes Windows.
139	NetBIOS Session Service	TCP	Não	Transferência de arquivos em redes Windows.
445	SMB/CIFS	TCP	Não	Compartilhamento de arquivos e impressoras.
2049	NFS	TCP/UDP	Não	Compartilhamento de arquivos em redes Unix/Linux.