APOSTILA – Análise de Rede

Curso: Educação Profissional Técnica – PROSUB
Componente Curricular: Servidores
Turma: SubTec04
Unidade: 1ª Unidade
Professor: Marcos Brandão

📘 **Apostila: Wireshark no Linux via Terminal (CLI)**

🧠 **1. O que é o Wireshark?**

O **Wireshark** é uma ferramenta de **análise de tráfego de rede (sniffer)** que permite capturar e examinar pacotes que trafegam pela rede.

📌 **Para que serve:**

- Monitorar tráfego de rede
- Detectar problemas de conexão
- Analisar protocolos (HTTP, TCP, DNS, etc.)
- Identificar ataques ou comportamentos suspeitos
- Estudar redes (muito usado em cursos técnicos e faculdade)

⚙️ **2. Instalação via Terminal (Linux)**

🔄 **Atualizando o sistema**

sudo apt update && sudo apt upgrade -y

📦 **Instalando o Wireshark**

sudo apt install wireshark -y

Durante a instalação, aparecerá a pergunta:

👉 **"Permitir que usuários não-root capturem pacotes?"**

Escolha:

Yes

🔐 **3. Configurando permissões (IMPORTANTE)**

Por segurança, apenas root pode capturar pacotes. Para permitir seu usuário:

Adicione o usuário ao grupo wireshark:

sudo usermod -aG wireshark $USER

Atualize as permissões:

newgrp wireshark

Verifique:

groups

🖥️ 4. Uso via Terminal (modo CLI)

Embora o Wireshark seja gráfico, sua versão em terminal se chama:

👉 **TShark**

🚀 5. Comandos básicos do TShark

▶ Listar interfaces de rede:

tshark -D

▶ Capturar pacotes de uma interface:

tshark -i eth0

(Substitua eth0 pela sua interface, como wlan0)

▶ Capturar e salvar em arquivo:

tshark -i eth0 -w captura.pcap

▶ Ler arquivo capturado:

tshark -r captura.pcap

🔍 6. Filtros de captura

Filtros ajudam a capturar apenas o que interessa.

📌 Exemplos:

Capturar apenas HTTP:

tshark -i eth0 -f "port 80"

Capturar apenas DNS:

tshark -i eth0 -f "port 53"

Capturar IP específico:

tshark -i eth0 -f "host 192.168.0.1"

🔎 7. Filtros de exibição (mais avançado)

Após capturar, você pode filtrar:

tshark -r captura.pcap -Y "http"

Outros exemplos:

tshark -r captura.pcap -Y "ip.addr == 192.168.0.1"
tshark -r captura.pcap -Y "tcp.port == 443"

📊 8. Exibindo campos específicos

Mostrar apenas IP origem e destino:

tshark -r captura.pcap -T fields -e ip.src -e ip.dst

Mostrar protocolo e tamanho:

tshark -r captura.pcap -T fields -e _ws.col.Protocol -e frame.len

---

⏱️ 9. Captura com limite

Capturar apenas 10 pacotes:

tshark -i eth0 -c 10

Capturar por tempo:

timeout 10 tshark -i eth0

🧪 10. Testes práticos

Teste 1: Ver tráfego ao acessar um site

1. Inicie captura:

tshark -i wlan0

2. Abra um site no navegador
3. Observe pacotes HTTP/HTTPS

Teste 2: Ping e captura

ping google.com

Em outro terminal:

tshark -i wlan0 -Y "icmp"

🛠️ 11. Dicas importantes

- Use sudo se necessário:

sudo tshark -i eth0

- Descubra sua interface:

ip a

- Interfaces comuns:
    - eth0 → cabo
    - wlan0 → Wi-Fi

⚠️ 12. Boas práticas e ética

- Nunca capture tráfego sem autorização
- Evite redes públicas para testes sensíveis
- Respeite a **LGPD**

📚 13. Conclusão

O **Wireshark/TShark** é uma ferramenta essencial para:

- Administradores de rede
- Técnicos em informática
- Estudantes de TI

Dominar o uso via terminal:
✓ Aumenta produtividade
✓ Permite automação
✓ Funciona em servidores sem interface gráfica

🎯 14. Exercícios propostos

1. Liste suas interfaces de rede
2. Capture 20 pacotes
3. Filtre apenas DNS
4. Salve e leia um arquivo .pcap
5. Mostre apenas IP origem/destino