Atividade Prática: Análise de Protocolo com Wireshark

Disciplina: Fundamentos de Redes
Professor: Laerte Peotta de Melo, Dr.

O que é o Wireshark?

O Wireshark é um software analisador de protocolos, também conhecido como "packet sniffer". Ele é amplamente utilizado para solucionar problemas de rede, analisar dados, desenvolver softwares e protocolos, e para fins educacionais. A ferramenta captura cada unidade de dados de protocolo (PDU) que trafega na rede, permitindo a decodificação e análise de seu conteúdo.

Nesta atividade, vamos explorar como o Wireshark pode ser usado para capturar e examinar pacotes ICMP (gerados pelo comando `ping`) e os quadros Ethernet associados, para entender melhor os endereços IP e MAC em uma rede local (LAN).

Objetivos de Aprendizagem

Ao final desta atividade, você será capaz de:

- Instalar e configurar o software Wireshark.
- Capturar pacotes de dados em uma rede local.
- Analisar os pacotes ICMP para identificar endereços de origem e destino.
- Diferenciar a comunicação com dispositivos locais (na mesma LAN) e remotos (fora da LAN).
- Compreender o encapsulamento de dados nas camadas de rede e de enlace.

Parte 1: Instalação do Wireshark

Nesta primeira parte, você irá baixar e instalar o Wireshark em seu computador.

> **Observação:** Se o Wireshark já estiver instalado, você pode pular esta parte e ir diretamente para a **Parte 2**.

Etapa 1: Baixar o Wireshark

1. Acesse o site oficial do Wireshark: www.wireshark.org.
2. Na página inicial, clique no botão de **Download**.
3. Escolha a versão correta para o sistema operacional e a arquitetura do seu PC (por exemplo, **Windows Installer 64-bit**). O download iniciará automaticamente. O arquivo geralmente é salvo na pasta **Downloads**.

Etapa 2: Instalar o Wireshark

1. Localize o arquivo de instalação (ex: `Wireshark-win64-x.x.x.exe`) e clique duas vezes para iniciar.
2. Se uma versão antiga for detectada, o instalador perguntará se você deseja desinstalá-la primeiro. É recomendado clicar em **Sim** para remover a versão anterior.
3. Siga as instruções do assistente de instalação:

    - Na tela de boas-vindas, clique em **Next**.
    - Aceite o contrato de licença clicando em **I Agree**.
    - Mantenha os componentes padrão e clique em **Next**.
    - Escolha os atalhos que desejar e clique em **Next**.
    - Mantenha o local de instalação padrão e clique em **Next**.
4. **Instalação do WinPcap:** O Wireshark precisa do WinPcap para capturar pacotes da rede.
    - O instalador irá verificar se o WinPcap já está presente. Se a caixa **Install WinPcap** estiver desmarcada, significa que ele já está instalado.
    - Se necessário, marque a caixa para instalar o WinPcap e prossiga com a sua instalação.
5. O Wireshark começará a instalar os arquivos. Ao final, clique em **Next** e, em seguida, em **Finish** para concluir a instalação.

Parte 2: Capturar e Analisar Dados ICMP na Rede Local

Agora, vamos usar o Wireshark para capturar e analisar pacotes ICMP trocados com um colega na mesma rede.

Etapa 1: Identificar Endereços da sua Interface de Rede

1. Abra o Prompt de Comando (`cmd.exe`).
2. Digite o comando `ipconfig /all` e pressione Enter.
3. Anote o seu **Endereço IPv4** e o seu **Endereço Físico (MAC)**.
4. Troque o seu endereço IP com um colega de turma. **Não compartilhe seu endereço MAC ainda**.

Etapa 2: Iniciar a Captura de Pacotes

1. Abra o Wireshark.
2. Clique em **Interface List** para ver as interfaces de rede disponíveis.
3. Marque a caixa de seleção da interface de rede que você está utilizando (a que está conectada à LAN).
    - **Dica:** Se não tiver certeza, clique em **Details** e verifique na aba **802.3 (Ethernet)** se o endereço MAC corresponde ao que você anotou na etapa anterior.
4. Clique no botão **Start** para começar a captura. Pacotes começarão a aparecer na tela.
5. Para vermos apenas o tráfego que nos interessa, digite `icmp` na caixa de **Filtro** e clique em **Apply**. A tela de captura ficará vazia, o que é normal.
6. Volte ao Prompt de Comando e execute o comando `ping` para o endereço IP do seu colega (ex: `ping 192.168.1.12`).
7. Observe que o tráfego ICMP (solicitações e respostas de ping) agora aparece na janela do Wireshark.
8. Após os pings terminarem, pare a captura clicando no ícone vermelho de **Stop Capture**.

Etapa 3: Examinar os Dados Capturados

A tela do Wireshark se divide em três seções:

- **Seção Superior:** Lista de todos os pacotes capturados.
- **Seção Média:** Detalhes do pacote selecionado, divididos por camadas de protocolo.
- **Seção Inferior:** Dados brutos do pacote em hexadecimal.

1. Na seção superior, selecione o primeiro pacote do tipo **"Echo (ping) request"**. Verifique se o IP de origem (Source) é o seu e o de destino (Destination) é o do seu colega.
2. Com este pacote ainda selecionado, vá para a seção do meio.
3. Clique no sinal `+` ao lado de **Ethernet II** para expandir os detalhes da camada de enlace.
4. Analise os endereços MAC:
    - O endereço MAC de origem (Source) corresponde ao MAC do seu computador?
    - O endereço MAC de destino (Destination) corresponde ao MAC do computador do seu colega?

Parte 3: Capturar e Analisar Dados ICMP Remotos

Nesta parte, vamos comparar o tráfego local com o tráfego destinado a redes externas (remotas).

Etapa 1: Iniciar uma Nova Captura

1. No Wireshark, clique novamente em **Interface List**, selecione a mesma interface e clique em **Start**.
2. O programa perguntará se você deseja salvar a captura anterior. Clique em **Continue without Saving**.
3. Com a captura ativa, volte ao Prompt de Comando e execute o comando `ping` para os seguintes sites:
    - `ping www.yahoo.com`
    - `ping www.cisco.com`
    - `ping www.google.com`
4. Observe que o DNS converte as URLs para endereços IP. Anote os IPs correspondentes.
5. Pare a captura de dados no Wireshark.

Etapa 2: Examinar os Dados da Captura Remota

1. Para cada um dos pings que você realizou, selecione o primeiro pacote de **"Echo (ping) request"**.
2. Na seção do meio, expanda a camada **Ethernet II**.
3. Preencha a tabela abaixo com os endereços IP e MAC de **destino** de cada um dos três pings:

Local	Endereço IP de Destino	Endereço MAC de Destino
Yahoo	(preencher)	(preencher)
Cisco	(preencher)	(preencher)
Google	(preencher)	(preencher)

Questões dissertativas

Responda às seguintes perguntas com base em sua análise:

1. Na Parte 2, como o seu computador descobriu o endereço MAC do computador do seu colega? (Dica: pesquise sobre o protocolo ARP).

2. Na Parte 3, os endereços MAC de destino que você anotou pertencem aos servidores da Cisco, Google e Yahoo? Se não, a qual dispositivo eles pertencem? Qual é a importância dessa informação?

3. Comparando os resultados da Parte 2 e da Parte 3, explique por que o Wireshark exibe o endereço MAC real do host de destino para pings locais, mas não para pings remotos.