

Como Capturar Pacotes no Linux Usando Ferramentas de Linha de Comando

A captura de pacotes é uma técnica essencial para a análise de redes, solução de problemas e segurança. No ambiente Linux, existem diversas ferramentas poderosas que permitem a captura e análise de pacotes de rede diretamente via linha de comando. Este artigo abordará como utilizar algumas dessas ferramentas, como tcpdump e Wireshark, para capturar pacotes no Linux.

Exemplos:

1. Captura de Pacotes com tcpdump

O tcpdump é uma das ferramentas mais populares e amplamente utilizadas para captura de pacotes no Linux. Ele permite a captura e análise de pacotes em tempo real.

Instalação:

```
sudo apt-get install tcpdump
```

Captura de Pacotes: Para capturar pacotes em uma interface específica (por exemplo, eth0), use o seguinte comando:

```
sudo tcpdump -i eth0
```

Salvar Captura em um Arquivo: Para salvar a captura em um arquivo para análise posterior:

```
sudo tcpdump -i eth0 -w captura.pcap
```

Filtragem de Pacotes: Para capturar apenas pacotes de um determinado protocolo ou porta, você pode usar filtros. Por exemplo, para capturar apenas pacotes HTTP:

```
sudo tcpdump -i eth0 'tcp port 80'
```

2. Captura de Pacotes com Wireshark

O Wireshark é uma ferramenta gráfica poderosa para análise de pacotes, mas também pode ser usada via linha de comando com o utilitário tshark.

Instalação:

```
sudo apt-get install wireshark
```

Captura de Pacotes com tshark: Para capturar pacotes usando tshark:

```
sudo tshark -i eth0
```

Salvar Captura em um Arquivo: Para salvar a captura em um arquivo:

```
sudo tshark -i eth0 -w captura.pcap
```

Filtragem de Pacotes: Para capturar apenas pacotes de um determinado protocolo ou porta:

```
sudo tshark -i eth0 -f 'tcp port 80'
```