INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

**Professor: Macêdo Firmino**
**Disciplina: Segurança de Computadoores**
**Prática 05: Ferramenta Tcpdump e Hping**

---

Olá turma, hoje iremos conhecer o TCPDump e o Hping. Compreender suas funcionalidades, aprender os principais comandos e aplicar estas ferramentas em testes de rede e análise de segurança. Vamos lá preparados??

## Tcpdump

O tcpdump é um programa analisador de tráfego (*sniffer*) em linha de comando e *software livre*. Ele permite que o usuário exiba pacotes de diversos protocolos TCP/IP. O tcpdump funciona na maioria dos sistemas operacionais do tipo Linux, Solaris , BSDs e MACOS.

Ele fornece uma visão detalhada do tráfego em uma rede, ajudando os administradores a identificar problemas de desempenho, detectar ataques de segurança, solucionar problemas de conectividade e monitorar o uso da rede. Com o tcpdump, os administradores podem filtrar o tráfego com base em vários critérios, como endereços IP de origem e destino, portas de protocolo e tipos de protocolo, permitindo uma análise refinada do tráfego.

Ele pode ser usado também para identificar padrões de tráfego malicioso, detectar tentativas de intrusão e analisar o comportamento de malware. Ao gravar capturas de tráfego durante um incidente de segurança, os analistas podem revisar o tráfego para entender como o ataque foi executado e desenvolver medidas de mitigação adequadas.

Se o tcpdump não estiver instalado, você pode instalá-lo, mas usando o gerenciador de pacotes da sua distribuição. Por exemplo:

```
sudo apt install tcpdump
```

No kali Linux ele já vem instalado por padrão.

### Capturando Pacotes

Para capturar pacotes o tcpdump requer permissões de root, portanto, nos exemplos a seguir, a maioria dos comandos são utilizados com o sudo.

```
sudo tcpdump
```

O tcpdump continua a capturar pacotes até receber um sinal de interrupção. Você pode interromper a captura pressionando [Ctrl+C].

Se quisermos capturar um número limitado de pacotes, podemos utilizar a opção -c, indicando o número de pacotes que desejamos capturar. Por exemplo:

```
sudo tcpdump -i eth0 -c 10
```

Por exemplo, analisando o resultado abaixo:

```
20:48:44.259152 IP 10.0.2.15.57816 >
200.137.1.195.https: Flags [S], seq
1938058989, win 64240, options [...],
length 0
```

O primeiro campo 20:48:44.259152, representa o timestamp do pacote recebido de acordo com o relógio local. A opção -t faz com que o tcpdump não imprima esta marca de tempo.

Em seguida, temos o endereço IP de origem do segmento (10.0.2.15) e sua respectiva porta de origem (57816). Na sequência temos o endereço IP de destino (200.137.1.195), com seu respectivo valor de porta de destino (https). O tcpdump quando possível converte via DNS o endereço IP e o nome da porta. Para evitar esta conversão podemos utilizar a opção -n.

Após a origem e o destino, você pode encontrar os TCP Flags [S.]. Os valores típicos para este campo incluem: A (ACK), R (RST), S (SYN), F (FIN), U (URG) e P (PSH). Quando no flag temos o ponto [.], significa uma mensagem ACK.

Em seguida é o número de sequência dos dados contidos no pacote. Ele representa o número do primeiro byte de dados deste segmento tcp. Neste exemplo, a sequência é seq 1.938.058.989. Ele é utilizado para reordenar os pacotes no receptor.

Depois surge o tamanho da janela (64240), que representa o número de bytes disponíveis no buffer de recebimento, seguido pelas opções do TCP.

Por fim, temos o comprimento do pacote (0), que representa o comprimento, em bytes, dos dados do payload. Como o exemplo mostrado é de estabelecimento de conexão, não foi enviado dados e o comprimento foi de zero.

## Filtrando Pacotes

Um filtro é uma expressão que sucede as opções e que nos permite selecionar os pacotes que desejamos capturar. Na ausência de filtros o tcpdump se capturara todo o tráfego do adaptador de rede selecionado.

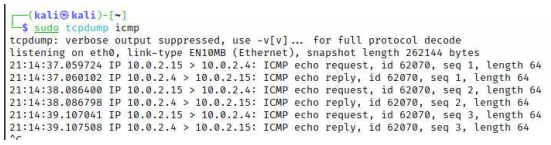
Podemos filtrar pacotes baseados no:

### Protocolo

Podemos especificar um protocolo na linha de comando. Por exemplo, capturando pacotes icmp, tcp, udp, ip, arp, http, ftp, dns, entre outros.

Por exemplo, se desejarmos filtrar somente as mensagens icmp podemos utilziar o filtro:

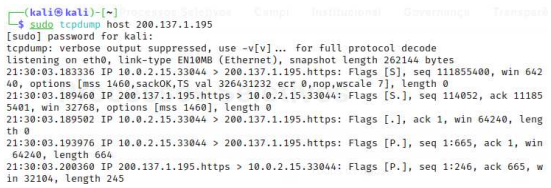
```
sudo tcpdump icmp
```




### Endereço IP (host)

Podemos limitar a captura apenas a pacotes relacionados a um host (IP) específico. Por exemplo, se desejarmos filtrar somente as mensagens IP do host (200.137.1.195) podemos utilziar o filtro:

```
sudo tcpdump host 200.137.1.195
```



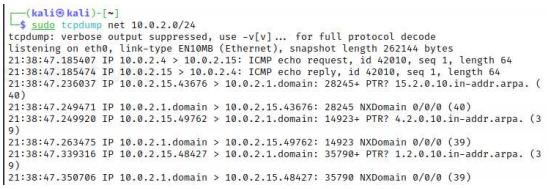

Neste caso, o tcpdump captura tanto pacotes de origem como de destino para este determinado IP. Entretanto, podemos especificar de onde e para onde vão os pacotes que queremos capturar, através das opções: src e dst. Por exemplo, se queremos capturar somente os pacotes que tem destino o endereço 200.137.1.195 e origem 10.0.2.15, basta aplicar um dos filtros abaixo:

```
sudo tcpdump dst 200.137.1.195 and
  src 10.0.2.15
```

### Endereço de Rede

Podemos filtrar a captura apenas para pacotes relacionados a uma determinada rede (net). Por exemplo, se desejarmos filtrar somente as mensagens de hosts pertencentes a rede (10.0.2.0/24) podemos utilizar o filtro:

```
sudo tcpdump net 10.0.2.0/24
```




### Endereço de Portas

Podemos filtrar a captura apenas para pacotes relacionados a uma determinada porta (port). Por exemplo, se desejarmos filtrar somente as mensagens que tem como origem ou destino a porta 443 (https), podemos utilizar o filtro:

```
sudo tcpdump port https
```


Se desejarmos filtrar a captura para os pacotes destinados ou de origem a uma determinada porta podemos utilizar a opção: dst e src, respectivamente. Por exemplo, capturar os pacotes destinados a porta 23, temos:

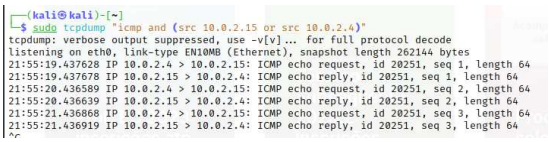
```
tcpdump dst port 23
```

Você também pode combinar filtros usando os operadores lógicos “and” e “or” para criar expressões mais complexas. Por exemplo, para filtrar pacotes de origem do host 192.168.122.98 e na porta do serviço HTTP, usamos o comando:

```
sudo tcpdump src 192.168.122.98 and port 80
```

Podemos ainda, criarmos expressões mais complexas agrupando filtros com parênteses. Nesse caso, coloque toda a expressão de filtro entre aspas para evitar que o shell as confunda com expressões do shell. Por exemplo, para filtrarmos todos os pacotes icmp que se originaram no endereço IP 10.0.2.15 ou 10.0.2.4, temos:

```
sudo tcpdump "icmp and (src 10.0.2.15 or
 src 10.0.2.4)"
```



### Salvando Capturas

Para salvar os pacotes em um arquivo em vez de exibi-los na tela, use a opção -w e o nome do arquivo com a extensão pcap. Por exemplo, o comando abaixo salva a saída da captura para um arquivo chamado file.pcap.

```
sudo tcpdump -w file.pcap
```

O tcpdump cria um arquivo em formato binário. Para ler o conteúdo do arquivo, execute tcpdump com a opção -r. Como você não está mais capturando os pacotes diretamente da interface de rede, sudo não é necessário ler o arquivo. Por exemplo:

```
tcpdump -r file.pcap
```

## Atividades

1. Utilizar o tcpdump para capturar tráfego enquanto um comando ping é executado para o endereço www.ifrn.edu.br (utilize a opções icmp -n). Observe as informações como endereços IP, protocolos e dados enviados.

2. Utilize o tcpdump para capturar os pacotes enquanto roda o Nmap para determinar se a porta 80 (http) está aberta no site do IFRN. Para isso, utilize o comando sudo nmap -sS -p 80 portal.ifrn.edu.br. Observe as mensagens trocadas e informações enviadas.

## Hping

O HPing é uma ferramenta de linha de comando usada para a criação e envio de pacotes personalizados na rede. Diferentemente do ping tradicional, que utiliza apenas pacotes ICMP, o HPing permite enviar pacotes TCP, UDP, ICMP ou IP, oferecendo um controle detalhado sobre cabeçalhos e opções de cada pacote.

O HPing é utilizada em testes de firewall, scans de portas, simulações de ataques DoS (em ambientes controlados) e para compreender o comportamento de dispositivos de rede. Seu uso requer responsabilidade, pois pode ser empregado tanto para defesa quanto para ataques.

Se o hping não estiver instalado, você pode instalá-lo, mas usando o gerenciador de pacotes da sua distribuição. Por exemplo:

```
sudo apt install hping3
```

No kali Linux ele já vem instalado por padrão.

A sintaxe básica dele é:

```
hping3 [opções] [alvo]
```

O Hping poderá ser utilizado para ataque de negação de serviço (DoS) em ambiente controlado e autorizado. **Lembrando que o código penal (Art. 266) estabele-se que interromper ou perturbar serviço telegráfico, radiotelegráfico, informático ou telefônico, impedir ou dificultar-lhe o restabelecimento resulta em pena de detenção, de um a três anos, e multa.**

Portanto utilize o Hping no modo inundação (flood) para as máquinas virtuais aqui no laboratório.

### Criando Pacotes

O Hping usa sockets raw (acesso de baixo nível à pilha TCP/IP) para montar e enviar pacotes manualmente. Isso permite: modificação de cabeçalhos, modificação de tamanho e dados do pacote, modificação de checksum, flags TCP e endereços IP e MAC.

Por exemplo, para enviar de pacotes TCP para uma porta específica:

```
hping3 -S -p 80 <IP>
```

Podemos criar pacotes com endereço de origem randômica:

```
hping3 --rand-source -S -p 80 <IP>
```

Podemos também criar pacotes com IP falso (IP spoofing) e específico.

```
hping3 --spoof 192.168.0.1 <IP>
```

Enviando pacotes UDP para uma porta específica (por exemplo, 53) com o comando:

```
hping3 --udp -p 53 <IP>
```

O Hping pode ser utilizado para ataque DoS Land (lembrando do uso ético apenas em ambientes controlado e autorizados!). Neste ataque são enviadas uma quantidade máxima de pacotes possíveis com IP de origem e destino iguais.

```
hping3 --flood --spoof <IP> <IP>
```

Ataque de DoS do tipo Syn Flooding na qual o atacante envia uma sequência de requisições SYN para um sistema-alvo visando uma sobrecarga direta na camada de transporte. Por exemplo, abrindo conexão na porte de destino (-p) 445 a partir de uma porta de origem (-s) também 445.

```
hping3 --flood -S -p 445 -s 445
  <IP_vitima>
```

Ataque de DoS do tipo Smurf corresponde ao envio de uma série de solicitação de pacotes ICMP Echo para o IP de origem falsificado da vítima usando um endereço de broadcast IP. A maioria dos dispositivos em uma rede, por padrão, responderá a isso enviando uma resposta para o endereço IP de origem. Se o número de máquinas na rede que recebem e respondem a esses pacotes é muito grande, o computador da vítima será inundado com o tráfego. Isso pode retardar o computador da vítima até o ponto em que se torna impossível trabalhar nele.

```
hping3 --icmp --flood --spoof
  <IP_vitima> <IP_Broadcast>
```

Se desejar mais customizações dos pacotes utilize a ferramenta Scapy. Ela é uma biblioteca Python para manipulação, criação, envio e análise de pacotes de rede em baixo nível. Ele permite interagir com protocolos de rede (TCP, UDP, ICMP, ARP, DNS, etc.) de forma programática. Comparado ao Hping, o Scapy oferece mais flexibilidade, pois permite criar pacotes totalmente customizados e automatizar tarefas complexas com scripts Python.

## Atividades

**3.** Em um abiente controlado das máquinas virtuais do LADIR utilize uma máquina alvo com o SSH instalado e uma máquina atacante com o Hping. Na máquina atacante realize uma ataque de flood na porta do SSH na máquina alvo. Veja se consegue fazem com que o SSH pare de responder.

**4.** Utilize o tcpdump para verificar e analisar as mensagens enviadas pelo Hping.