Essa atividade será prolongada para a semana inteira, para ficar mais confortável a realização da mesma. Dúvidas, estou no meet ou pelo e-mail após o horário da aula.

- Pelo Ubuntu, faça o download de atualizações, pelo cmd(prompt de comando): sudo apt update
- Agora instale as atualizações baixadas com: sudo apt upgrade
- Instale o Wireshark, pelo comando: sudo apt-get install wireshark
- Execute como administrador: sudo wireshark
- Ou instale pelo windows: https://www.wireshark.org/download.html
- Após a instalação, execute também como administrador.

EXERCÍCIOS

Para pesquisar o ip de um endereço web, abra o cmd:

- Digite o comando ping seguido do endereço url(preferível começar pelo www.endereço, removendo o https);
- Aparecerá o ip do endereço, conforme segue a imagem:

```
orlando131@orlando131-Aspire-E1-572:~ Q = - - ×

orlando131@orlando131-Aspire-E1-572:~$ ping www.google.com

PING www.google.com(2800:3f0:4001:833::2004 (2800:3f0:4001:833::2004)) 56 data b

ytes

64 bytes from 2800:3f0:4001:833::2004 (2800:3f0:4001:833::2004): icmp_seq=1 ttl=

115 time=25.4 ms

64 bytes from 2800:3f0:4001:833::2004 (2800:3f0:4001:833::2004): icmp_seq=2 ttl=

115 time=23.2 ms

64 bytes from 2800:3f0:4001:833::2004 (2800:3f0:4001:833::2004): icmp_seq=3 ttl=

115 time=72.3 ms

64 bytes from 2800:3f0:4001:833::2004 (2800:3f0:4001:833::2004): icmp_seq=4 ttl=

115 time=24.2 ms

64 bytes from 2800:3f0:4001:833::2004 (2800:3f0:4001:833::2004): icmp_seq=5 ttl=

115 time=25.2 ms

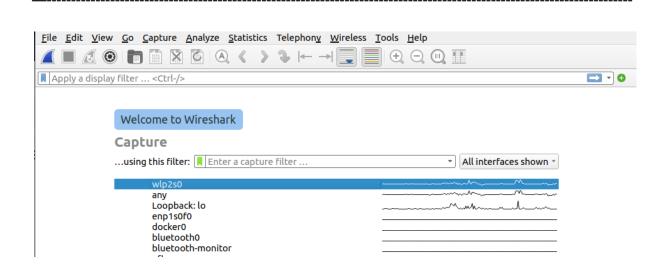
64 bytes from 2800:3f0:4001:833::2004 (2800:3f0:4001:833::2004): icmp_seq=5 ttl=

115 time=25.2 ms

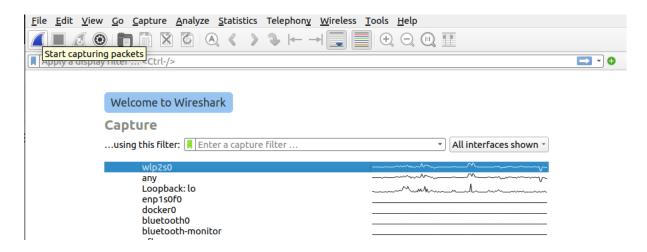
64 bytes from 2800:3f0:4001:833::2004 (2800:3f0:4001:833::2004): icmp_seq=6 ttl=

115 time=22.3 ms
```

- Copie o endereço IP para prosseguir no wireshark;(No caso 2800:3f0:4001:833::2004), cole em um bloco de notas.
- Caso a resposta dos pacotes não pare no cmd, aperte ctrl+shift+z



Perceba que temos 3 interfaces de rede ativas, ilustrando as frequências do tráfego na rede. Escolha uma interface e inicialize o serviço de capturas de pacotes na rede, pelo botão similar a uma barbatana(abaixo do file).



Ao iniciar na interface selecionada, teremos pacotes sendo capturados, de acordo com as navegações realizadas nas máquinas:

```
<u>F</u>ile <u>E</u>dit <u>V</u>iew <u>G</u>o <u>C</u>apture <u>A</u>nalyze <u>S</u>tatistics Telephon<u>y</u> <u>W</u>ireless <u>T</u>ools <u>H</u>elp
Apply a display filter ... <Ctrl-/>
                                                                                                       - · O
                     Source
                                                               Destination
                                                                                                        Protoco
       Time
  4593 8.966402329
                     192.168.0.14
                                                               74.125.250.147
                                                                                                        UDP
  4594 8.966443457
                                                                                                        UDP
                     192.168.0.14
                                                               74.125.250.147
  4595 8.966507958
4596 8.966551647
                                                               74.125.250.147
                                                                                                        UDP
                     192.168.0.14
                                                                                                        UDP
                     192.168.0.14
                                                               74.125.250.147
  4597 8.968344966
4598 8.968420664
                                                                                                        UDP
                     192.168.0.14
                                                               74.125.250.147
                                                                                                        UDP
                     192.168.0.14
                                                               74.125.250.147
                                                                                                        UDP
  4599 8.968493742
                     192.168.0.14
                                                               74.125.250.147
  4600 8.968536465 192.168.0.14
                                                               74.125.250.147
                                                                                                        UDP
Frame 1: 1248 bytes on wire (9984 bits), 1248 bytes captured (9984 bits) on interface wlp2s0, id 0
Fethernet II, Src: LiteonTe_d2:c5:c2 (5c:93:a2:d2:c5:c2), Dst: Technico_97:80:c9 (5c:76:95:97:80:c9)
▶ Internet Protocol Version 4, Src: 192.168.0.14, Dst: 74.125.250.147
User Datagram Protocol, Src Port: 42220, Dst Port: 19305
Data (1206 bytes)
```

OBSERVAÇÃO: Os comandos sempre têm de serem feitos minúsculos, pois a sintaxe do software só aceita dessa forma. Quando a janela de filtros fica verde, quer dizer que está tudo ok.

Então, para começarmos os exercícios, na barra de filtros(apply a display filter) do wireshark digite os comandos seguidos do ip que está no bloco de notas(cada comando por vez):

ip.addr == ip à sua escolha

ip.src == ip à sua escolha

ip.dst == ip à sua escolha

Caso o ip selecionado não dê, escolha outro ip dando um ping de um outro website no cmd.

 Tire print do resultado dos 3 comandos, e diga o que você pôde observar de diferença entre os objetivos dos 3 comandos.

 Com o sinal de exclamação, você consegue negar a aparição do ip filtrado, como neste exemplo de comando: !(ip.addr == ip à sua escolha). Com base no exercício anterior, negue a filtragem de 1 ip diferente para cada comando. (Tire print)

• Faça dois protocolos a sua escolha não aparecerem na filtragem, com o comando: not nome protocolo à sua escolha. (TIRE PRINT)

O protocolo está na coluna protocol, então selecione os protocolos que estão sendo capturados, e inclua seus nomes no comando.

Curiosidade(Não precisa fazer): ip.addr = ip à escolha && tcp.port == 80 && http.request.method(Para acessar login)

Site de tentativa de logins para teste: http://testphp.vulnweb.com/login.php

https://wiki.archlinux.org/title/Wireshark (Portugu%C3%AAs) => biblioteca Wireshark