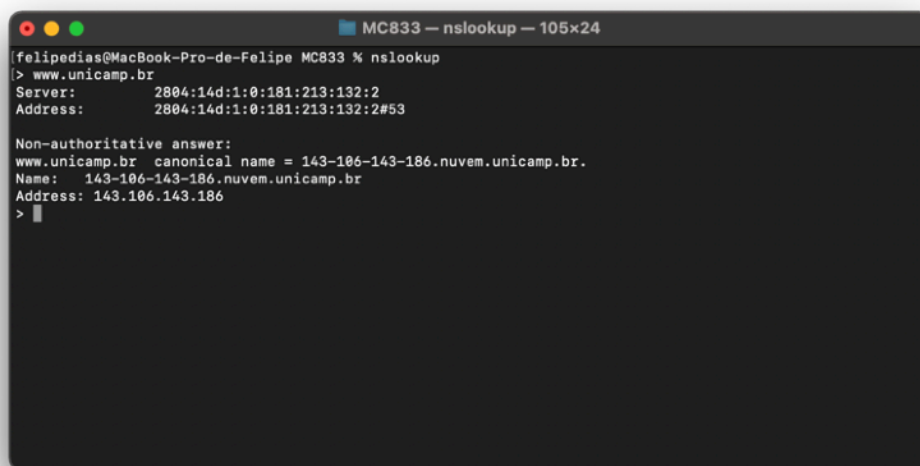


MC833 - Exercício 2

Felipe Santana Dias - 215775

FERRAMENTAS

1. Considere para esta questão o comando *ifconfig*.
 - a. Qual opção deve ser usada para exibir informações sobre todas as interfaces de rede?
`ifconfig -a`
 - b. O que deve ser feito para exibir somente informações de uma interface específica?
`ifconfig eth0`
2. Através da execução do comando *nslookup* seguido dos parâmetros adequados, responda à seguinte questão:
 - a. Quais são os endereços IP do host www.unicamp.br?

A terminal window titled "MC833 — nslookup — 105x24" showing the output of the 'nslookup' command for 'www.unicamp.br'. The output displays the server address as 2804:14d:1:0:181:213:132:2 and the canonical name as 143-106-143-186.nuvem.unicamp.br, with the IP address 143.106.143.186.

```
felipedias@MacBook-Pro-de-Felipe MC833 % nslookup  
> www.unicamp.br  
Server:      2804:14d:1:0:181:213:132:2  
Address:     2804:14d:1:0:181:213:132:2#53  
  
Non-authoritative answer:  
www.unicamp.br canonical name = 143-106-143-186.nuvem.unicamp.br.  
Name:   143-106-143-186.nuvem.unicamp.br  
Address: 143.106.143.186  
>
```

- b. Há alguma vantagem em haver mais de um endereço IP?
Sim, ter mais de um endereço IP pode compensar caso algum host esteja inoperante e garante uma maior segurança para disponibilidade e acesso.

3. Através da execução do comando *traceroute* seguido dos parâmetros adequados, responda à seguinte questão:

- a. Quantos roteadores estão entre a sua estação e o host www.amazon.com? Pelos nomes dos roteadores, quantos deles estão localizados no Brasil?

Há 18 roteadores entre minha estação e o host www.amazon.com, sendo pelo menos 10 deles localizados no Brasil.

```
traceroute -I www.amazon.com — 129x24
-traceroute to d3ag4hukkh62yn.cloudfront.net (13.33.129.30), 64 hops max, 72 byte packets
 1 192.168.0.1 (192.168.0.1) 2.381 ms 2.077 ms 2.291 ms
 2 10.21.0.1 (10.21.0.1) 8.240 ms 9.068 ms 10.472 ms
 3 bd075865.virtua.com.br (189.7.88.101) 9.768 ms 12.461 ms 13.949 ms
 4 200.227.107.1 (200.227.107.1) 9.620 ms 10.810 ms 10.002 ms
 5 200.230.235.143 (200.230.235.143) 23.613 ms 25.261 ms 24.037 ms
 6 ebt-b12-tcore01.cas.embratel.net.br (200.244.214.1) 26.700 ms 29.195 ms 31.477 ms
 7 ebt-b1191-tcore01.spo.embratel.net.br (200.230.252.130) 29.913 ms 28.941 ms 22.872 ms
 8 ebt-b2111-tcore01.rjo.embratel.net.br (200.230.251.1) 27.119 ms 29.147 ms 22.302 ms
 9 ebt-h0-12-0-agg03.rjo.embratel.net.br (200.244.18.0) 20.904 ms 22.500 ms 21.044 ms
10 peer-b57-agg03.rjo.embratel.net.br (200.255.177.26) 22.284 ms 21.169 ms 21.153 ms
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 server-13-33-129-30.gig51.r.cloudfront.net (13.33.129.30) 29.232 ms 21.777 ms 21.183 ms

[Processo concluído]
```

4. Através da execução do comando *telnet*, seguido dos parâmetros adequados, responda às seguintes questões:

- a. É possível conectar-se com este comando em um servidor HTTP? Se sim, como deve se executar o comando para conectar-se no host www.amazon.com na porta padrão do HTTP?

Sim, telnet www.amazon.com 80

- b. Caso não haja um servidor escutando na porta passada pelo comando telnet, o que ocorre? Justifique.

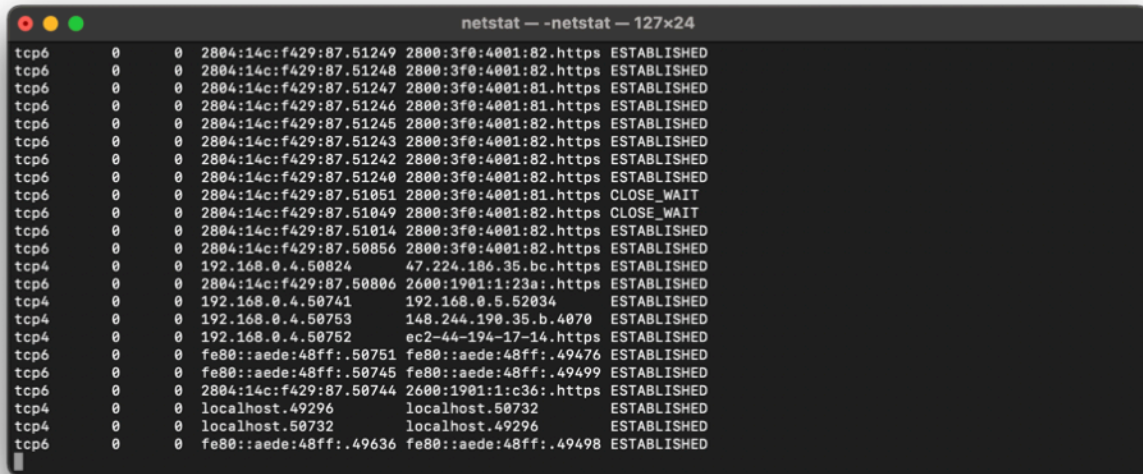
Caso não haja um servidor escutando na porta passada a conexão falha e é emitido uma mensagem de erro.

- c. A qual a camada da rede o telnet pertence?

Camada de transportes.

5. Acesse o site da DAC (<https://www.dac.unicamp.br/>) e, em paralelo em um terminal, verifique a saída do comando *netstat*. Quais são as informações fornecidas a respeito da conexão ao site da DAC?

O comando *netstat* fornece informações sobre o protocolo utilizado, as portas de envio e recebimento, os endereços e o estado das conexões.



```
netstat -- netstat -- 127x24
tcp6      0      0 2804:14c:f429:87.51249 2800:3f0:4001:82.https ESTABLISHED
tcp6      0      0 2804:14c:f429:87.51248 2800:3f0:4001:82.https ESTABLISHED
tcp6      0      0 2804:14c:f429:87.51247 2800:3f0:4001:81.https ESTABLISHED
tcp6      0      0 2804:14c:f429:87.51246 2800:3f0:4001:81.https ESTABLISHED
tcp6      0      0 2804:14c:f429:87.51245 2800:3f0:4001:82.https ESTABLISHED
tcp6      0      0 2804:14c:f429:87.51243 2800:3f0:4001:82.https ESTABLISHED
tcp6      0      0 2804:14c:f429:87.51242 2800:3f0:4001:82.https ESTABLISHED
tcp6      0      0 2804:14c:f429:87.51240 2800:3f0:4001:82.https ESTABLISHED
tcp6      0      0 2804:14c:f429:87.51051 2800:3f0:4001:81.https CLOSE_WAIT
tcp6      0      0 2804:14c:f429:87.51049 2800:3f0:4001:82.https CLOSE_WAIT
tcp6      0      0 2804:14c:f429:87.51014 2800:3f0:4001:82.https ESTABLISHED
tcp6      0      0 2804:14c:f429:87.50856 2800:3f0:4001:82.https ESTABLISHED
tcp4      0      0 192.168.0.4.50824      47.224.186.35.bc.https ESTABLISHED
tcp6      0      0 2804:14c:f429:87.50806 2600:1901:1:23a:.https ESTABLISHED
tcp4      0      0 192.168.0.4.50741      192.168.0.5.52034      ESTABLISHED
tcp4      0      0 192.168.0.4.50753      148.244.190.35.b.4070  ESTABLISHED
tcp4      0      0 192.168.0.4.50752      ec2-44-194-17-14.https ESTABLISHED
tcp6      0      0 fe80::aede:48ff:50751  fe80::aede:48ff:49476  ESTABLISHED
tcp6      0      0 fe80::aede:48ff:50745  fe80::aede:48ff:49499  ESTABLISHED
tcp6      0      0 2804:14c:f429:87.50744 2600:1901:1:c36:.https ESTABLISHED
tcp4      0      0 localhost.49296        localhost.50732        ESTABLISHED
tcp4      0      0 localhost.50732        localhost.49296        ESTABLISHED
tcp6      0      0 fe80::aede:48ff:49636  fe80::aede:48ff:49498  ESTABLISHED
```

SNIFFERS

6. Considere a ferramenta *TCPDUMP*, e responda às seguintes questões (precisa de acesso root):

- a. Utilizando o *TCPDUMP* corretamente com os filtros é possível somente capturar o tráfego HTTPS? Se sim, execute o comando junto com os filtros e anexe uma figura que comprove sua resposta no relatório. Se sua resposta foi não, então justifique-a.

Não, como todo tráfego em HTTPS é encriptado o *TCPDUMP* não consegue filtrá-lo.

- b. Utilizando o comando *TCPDUMP* seguido dos parâmetros corretos imprima somente os pacotes superiores a 64 bits. Indique qual foi a sequência de comandos utilizada.

```
tcpdump greater 64
```

- c. Utilizando o *TCPDUMP* seguido de filtros, imprima somente os resultados que tiverem a flag 'ACK'. Insira o comando seguido dos filtros e uma figura no seu relatório para comprovar o sucesso.

```
tcpdump 'tcp[tcpflags] == tcp-ack'
```

7. Considere a ferramenta Wireshark para responder às questões a seguir: (pergunta teórica)

- a. Comparado às demais ferramentas apresentadas na aula de MC833 descreva quais são principais diferenças e vantagens de usar o Wireshark? Escolha pelo menos uma ferramenta/sniffer e elabore uma tabela comparativa para responder a questão.

Com o Wireshark é possível ver e capturar os dados que passam pela rede além de permitir resolver problemas e identificar tráfegos que são incomuns. Podemos comparar essa ferramenta com o TCPDUMP que possui função semelhante e também é open-source mas possui diferenças, descritas na tabela a seguir:

Wireshark	TCPDUMP
Possui interface gráfica	Baseado em CLI
Realiza análise complexas dos pacotes	Realiza apenas análises simples
Possui filtros complexos	Possui filtros simples
Pode decodificar pacotes caso possua a chave de encriptação	Menos eficiente na decodificação quando comparado com o Wireshark

- b. Com o conhecimento adquirido sobre ferramentas e sniffers responda: Em uma rede com vários processos acontecendo ao mesmo tempo é possível gerenciar de forma isolada um único processo específico na rede utilizando ferramentas/sniffers apresentados nesta disciplina? Se sim, quais ferramentas e/ou sniffers você usaria? Justifique sua resposta. (OBS: Não é necessário apresentar comandos ou prints)

Sim, para gerenciar um único processo específico de forma isolada é possível identificar os protocolos e as portas utilizadas por esse processo através do netstat e com essas informações utilizar o Wireshark para filtrar os pacotes dessas portas.