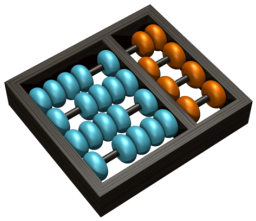


MC833 Relatório 2

Ferramentas e Sniffers

Aluno: Fábio Camargo Ricci

RA: 170781

Instituto de Computação

Universidade Estadual de Campinas

Campinas, 2 de Setembro de 2021.

Sumário

1 Questões

1. Considere para esta questão o comando ifconfig.

   (a) Qual opção deve ser usada para exibir informações sobre todas as interfaces de rede?

   (b) O que deve ser feito para exibir somente informações de uma interface específica?

2. Através da execução do comando nslookup seguido dos parâmetros adequados, responda à seguinte questões:

   (a) Quais são os endereços IP do host www.unicamp.br?

   (b) Há alguma vantagem em haver mais de um endereço IP?

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?

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?

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

   (c) A qual a camada da rede o telnet pertence?

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?

6. Considere a ferramenta TCPDUMP, e responda às seguintes questões:

   (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.

   (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.

   (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.

7. Considere a ferramenta Wireshark para responder às questões a seguir:

   (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.

   (b) Com o conhecimento adquirido sobre ferramentas e sniffers responda:

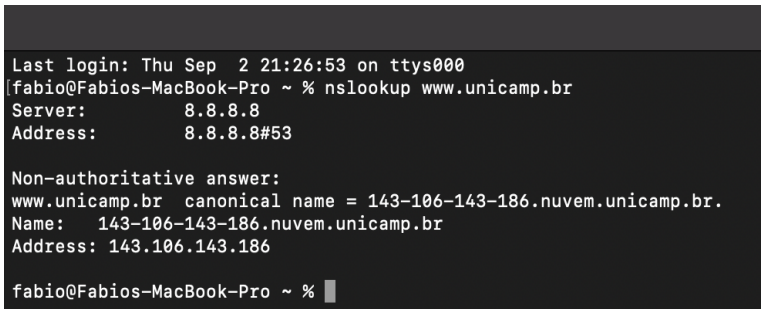
i. Em uma rede com vários processos acontecendo ao mesmo tempo é possível gerenciar de forma isolada um único processo específico na rede utilizando ferramentas/sniffers apresentados nesta disciplina? Se sim, quais ferramentas e/ou sniffers você usaria? Justifique sua resposta. (OBS: Não é necessário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

2 Respostas

1. (a) Deve ser utilizada a opção -a (ex: ifconfig -a), mostrando todas as interfaces de rede, sendo utilizadas ou não

   (b) Deve ser utilizado o nome da interface (ex: ifconfig eth0), mostrando apenas as informações da interface eth0

2. (a) O endereço IP do host www.unicamp.br é 143.106.143.187. Foi executado o comando nslookup www.unicamp.br



   (b) Sim, com mais de um endereço IP, a escalabilidade de um serviço ou servidor se torna mais fácil, possivelmente aumentando o alcance geográfico e a distribuição de carga do mesmo.

3. (a) A flag -I indica para o comando traceroute utilizar o protocolo ICMP, a fim de tentar passar por possíveis firewalls (muitos

deles deixam conexões ICMP passarem) que barrem a conexão TCP que o traceroute faça com os roteadores.

```
fabio@Fabios-MacBook-Pro workspace % traceroute -I www.amazon.com
traceroute to d3ag4hukkh62yn.cloudfront.net (13.227.107.129), 64 hops max, 72 byte packets
 1  192.168.1.1 (192.168.1.1)  1.839 ms  1.379 ms  2.820 ms
 2  * * *
 3  152-255-152-240.user.vivozap.com.br (152.255.152.240)  4.989 ms  13.816 ms  5.518 ms
 4  152-255-180-224.user.vivozap.com.br (152.255.180.224)  7.014 ms  4.537 ms  7.002 ms
 5  * * *
 6  * * *
 7  52.93.146.145 (52.93.146.145)  10.669 ms  7.110 ms  8.775 ms
 8  150.222.70.49 (150.222.70.49)  31.256 ms  8.534 ms  7.731 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  server-13-227-107-129.gru50.r.cloudfront.net (13.227.107.129)  8.122 ms  7.868 ms  9.423 ms
fabio@Fabios-MacBook-Pro workspace %
```

Existem 5 roteadores entre a minha estação e o host www.amazon.com. Pelo nome dos roteadores apresentados, 3 deles estão localizados no Brasil, o primeiro (residencial) e os 2 seguintes da Vivo.

4. (a) Sim, é possível, basta executar:
telnet www.amazon.com 80

```
fabio@Fabios-MacBook-Pro ~ % telnet www.amazon.com 80

Trying 104.89.245.220...
Connected to e15316.a.akamaiedge.net.
Escape character is '^]'.
```

(b) Caso não haja um servidor escutando na porta passada, o comando telnet falhará e encerrará a conexão. Foi passada a porta 5434 arbitrariamente esperando-se que não havia servidor escutando nessa porta

```
fabio@Fabios-MacBook-Pro ~ % telnet www.amazon.com 5434

Trying 52.84.79.159...
telnet: connect to address 52.84.79.159: Operation timed out
telnet: Unable to connect to remote host
fabio@Fabios-MacBook-Pro ~ %
```

(c) O telnet é um protocolo que pertence à camada de aplicação

5. Executando-se o comando nslookup www.dac.unicamp.br, descobrimos o endereço IP do site da DAC (143.106.227.165). Com essa informação, podemos executar o comando.
   netstat -an | grep 143.106.227.165
   -a para apenas conexões ativas.
   -n para evitar que o netstat tente determinar o nome dos hosts para endereços IPs externos, diminuindo consideravelmente o tempo de execução.

```
fabio@Fabios-MacBook-Pro ~ % nslookup www.dac.unicamp.br

Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.dac.unicamp.br      canonical name = 143-106-227-165.nuvem.unicamp.br.
Name:   143-106-227-165.nuvem.unicamp.br
Address: 143.106.227.165

fabio@Fabios-MacBook-Pro ~ % netstat -an | grep  143.106.227.165

tcp4       0      0  192.168.1.65.60496     143.106.227.165.443    ESTABLISHED
fabio@Fabios-MacBook-Pro ~ %
```

   Conseguimos informações como, os protocolos (Proto) sendo utilizados (tcp4 - TCP IPv6), quantos dados estão na fila para serem recebidos (Recv-Q) e (Send-Q) enviados (0 e 0), o endereços e portas locais e externos da conexão com o servidor (192.168.1.65:60496 e 143.106.227.165:443 respectivamente) e o status da conexão (ESTABLISHED).

6. (a) Sim é possível, uma vez que nunca haverá tráfego HTTPS em outra porta (protocolo). Assim, basta executar:
   sudo tcpdump -i any 'tcp port 443' -w ./http-only.pcap
   -i: qualquer interface de rede
   'tcp port 443': todas as conexões TCP na porta 443 (padrão HTTPS)

```
fabio@Fabios-MacBook-Pro ~ % sudo tcpdump -i any 'tcp port 443' -w ./http-only.pcap

tcpdump: data link type PKTAP
tcpdump: listening on any, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
^C155 packets captured
223 packets received by filter
0 packets dropped by kernel
fabio@Fabios-MacBook-Pro ~ %
```

(b) sudo tcpdump -i any 'len > 64' -w ./greater64.pcap

-i: qualquer interface de rede

'len > 64': todos os pacotes com tamanho maior que 64 bytes

```
fabio@Fabios-MacBook-Pro workspace % sudo tcpdump -i any 'len > 64' -w ./greater64.pcap

tcpdump: data link type PKTAP
tcpdump: listening on any, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
^C47 packets captured
64 packets received by filter
0 packets dropped by kernel
fabio@Fabios-MacBook-Pro workspace %
```

(c) sudo tcpdump -i any 'tcp[tcpflags] == tcp-ack' -w ./ack.pcap

-i: qualquer interface de rede

'tcp[tcpflags] == tcp-ack': Filtra todos os pacotes TCP que possuem a flag ACK

```
fabio@Fabios-MacBook-Pro workspace % sudo tcpdump -i any 'tcp[tcpflags] == tcp-ack' -w ./ack.pcap

tcpdump: data link type PKTAP
tcpdump: listening on any, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
^C23 packets captured
245 packets received by filter
0 packets dropped by kernel
fabio@Fabios-MacBook-Pro workspace %
```

7. (a)

	Wireshark	**tcpdump**
Interface	Interface gráfica (GUI)	CLI (linha de comando)
Análise de pacotes	Possibilidade de análise de payload de pacotes, mesmo sendo criptografados (chaves são necessárias) ou se protocolos de transporte de arquivo (STMP, HTTP, etc)	Apenas análise simples como tipos de tráfego (ex: DNS queries)
Interfaces de redes	Possui interfaces de redes avançadas	Apenas possui interfaces de redes convencionais
Filtros	Fornece filtros complexos	Fornece apenas filtros simples

A principal vantagem de se utilizar o Wireshark é a interface gráfica e possibilidade de filtros avançados/análise de pacotes que ele fornece, sendo possível ter uma visão mais detalhada de todas as informações disponíveis na rede.

(b) i. Sim. Utilizando o tcpdump ou wireshark, por exemplo, é possível verificar todos os processos na rede, o process ID de cada um, e as portas sendo utilizadas pelos mesmos, também havendo a possibilidade da aplicação de filtros e análise de pacotes (no caso do wireshark).