

Programação Distribuída com redes usando Linux e Python



Nome: Ian costa dos Santos

Turma: 24E2_4

1. Teste a conexão do Servidor Web com endereço google.com utilizando o protocolo telnet. Copie a saída gerada para o arquivo google_index.html e abra em um navegador. Descreva a diferença entre o conteúdo de google_index.html e a página inicial de google.com.

Estabelecendo conexão com o google:

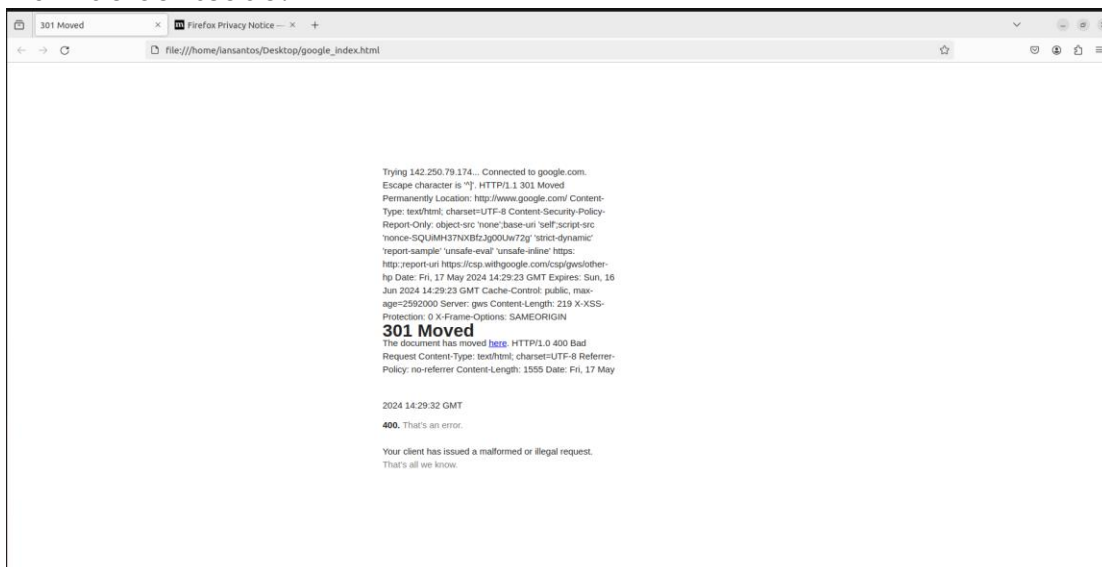
```
lansantos@lansantos:~/Desktop$ telnet google.com 80
Trying 142.250.79.174...
Connected to google.com.
Escape character is '^]'.
GET / HTTP/1.1
Host: google.com

HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=utf-8
Content-Security-Policy: Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-JtSe9pZUNCKyRbL7pVHaqW' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri http://csp.withgoogle.com/csp/gws/other-hp
Date: Fri, 17 May 2024 14:26:20 GMT
Expires: Sun, 16 Jun 2024 14:26:20 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
xdg-open google_index.html
HTTP/1.0 400 Bad Request
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 1555
Date: Fri, 17 May 2024 14:27:59 GMT

<!DOCTYPE html>
<html lang=en>
<meta charset=utf-8>
<meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
<title>Error 400 (Bad Request)!!!</title>
<style>
  [margin:0;padding:0]html{code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0 0/100% 100%;no-repeat;border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;webkit-background-size:100% 100%;display:inline-block;height:54px;width:150px}}
</style>
<a href="//www.google.com/"><span id=logo aria-label=Google></span></a>
<p><b>400.</b></p>
<ins>That's an error.</ins>
<p>Your client has issued a malformed or illegal request. <ins>That's all we know.</ins>
```

Abrindo conteúdo:



Descrição da Diferença entre google_index.html e a Página Inicial de google.com

google_index.html:

O arquivo google_index.html conterá a resposta bruta do servidor web do Google, incluindo cabeçalhos HTTP e o conteúdo HTML básico da página de resposta. Esse conteúdo será muito simplista e pode não incluir todos os recursos e estilos da página web completa.

Página inicial de google.com:

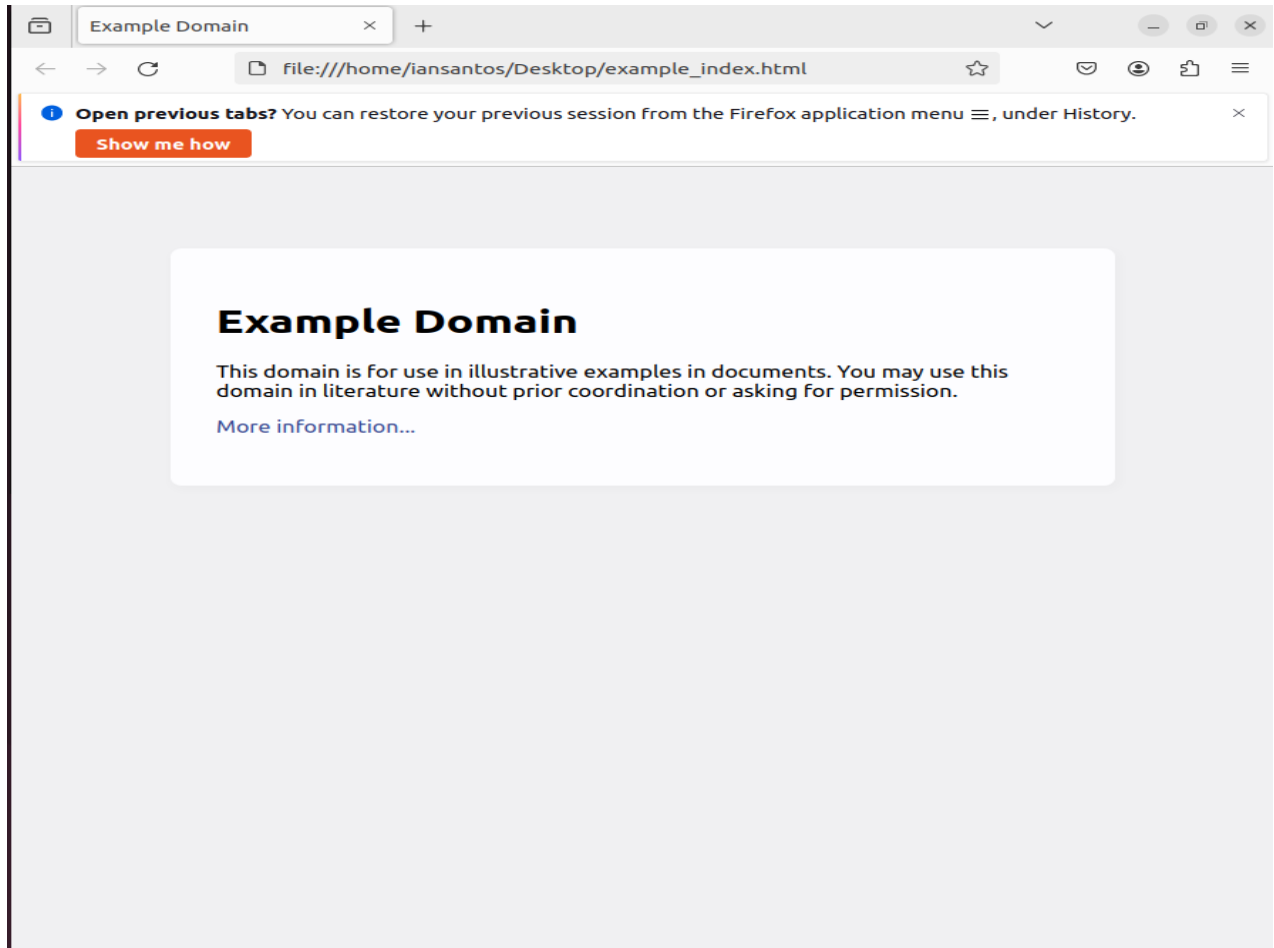
A página inicial de google.com, quando acessada por um navegador, inclui uma variedade de recursos que são carregados dinamicamente, como folhas de estilo CSS, scripts JavaScript, imagens, e outros conteúdos multimídia. O navegador processa esses recursos para exibir uma página completa, interativa e estilizada.

2. Faça o download da página example.com com curl para o arquivo chamado example_index.html e abra o arquivo no navegador.

Comandos:

```
iansantos@iansantos:~/Desktop$ curl http://example.com -o example_index.html
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left     Speed
100 1256 100 1256    0     0  4805      0 --:--:-- --:--:-- --:--:-- 4812
iansantos@iansantos:~/Desktop$ xdg-open example_index.html
```

Resultado:



3. Realize o Gerenciamento Remoto de Hospedeiro para o usuário carol no localhost com o protocolo ssh. Navegue até o diretório home do usuário e mostre o caminho absoluto deste diretório para mostrar que o login foi realizado com sucesso.

Verificando status servidor SSH:

```
carol@iansantos:/home/iansantos/Desktop$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
carol@iansantos:/home/iansantos/Desktop$ sudo systemctl start ssh
carol@iansantos:/home/iansantos/Desktop$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Fri 2024-05-17 11:42:36 -03; 1min 32s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 10115 (sshd)
      Tasks: 1 (limit: 2261)
     Memory: 2.0M
        CPU: 20ms
    CGroup: /system.slice/ssh.service
            └─10115 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

mai 17 11:42:36 iansantos systemd[1]: Starting OpenBSD Secure Shell server...
mai 17 11:42:36 iansantos sshd[10115]: Server listening on 0.0.0.0 port 22.
mai 17 11:42:36 iansantos sshd[10115]: Server listening on :: port 22.
mai 17 11:42:36 iansantos systemd[1]: Started OpenBSD Secure Shell server.
lines 1-16/16 (END)
```

Realizar login e navegando ate o diretorio home:

```
carol@iansamtos:/home/iansantos/Desktop$ ssh carol@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:1Gl26/HRwqXeivLaTLlCbi5K3p37NDHNE+YMPCECQGs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
carol@localhost's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

74 updates can be applied immediately.
26 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

carol@iansamtos:~$ pwd
/home/carol
carol@iansamtos:~$
```

4. Abra uma conexão TCP com algum Servidor Web e mostre a saída detalhada das estatísticas da interface de rede antes e depois da abertura de conexão TCP. Indique alguma estatística que demonstre que a conexão foi aberta.

Passo 1: Verifique as estatísticas da interface de rede antes da conexão

```
carol@iansantos:~$ netstat -i
Kernel Interface table
Iface      MTU      RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0    1500      0      0      0 0          0      0      0      0 BMU
enp0s3     1500    1982      0      0 0        918      0      0      0 BMRU
lo         65536    878      0      0 0        878      0      0      0 LRU
```

Passo 2: Abra uma conexão TCP com um servidor web

```
carol@iansantos:~$ netstat -i
Kernel Interface table
Iface      MTU      RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0    1500      0      0      0 0          0      0      0      0 BMU
enp0s3     1500    1982      0      0 0        918      0      0      0 BMRU
lo         65536    878      0      0 0        878      0      0      0 LRU

carol@iansantos:~$ telnet google.com 80
Trying 142.250.79.174...
Connected to google.com.
Escape character is '^]'.
GET / HTTP/1.1
Host: google.com

HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-RXzwQ8dxl5xhBap12stetA' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: https://csp.withgoogle.com/csp/gws/other-hp
Date: Fri, 17 May 2024 14:50:29 GMT
Expires: Sun, 16 Jun 2024 14:50:29 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
```

Passo 3: Verifique as estatísticas da interface de rede após a conexão

```
carol@iansantos:~$ netstat -i
Kernel Interface table
Iface      MTU      RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0    1500      0      0      0 0          0      0      0      0 0 BMU
enp0s3     1500    2004      0      0 0        940      0      0      0 0 BMRU
lo         65536    1022      0      0 0       1022      0      0      0 0 LRU
carol@iansantos:~$
```

Pacotes Recebidos com Sucesso (RX-OK):

Antes da conexão: enp0s3 tinha 1982 pacotes recebidos.

Depois da conexão: enp0s3 tem 2004 pacotes recebidos.

Diferença: $2004 - 1982 = 22$ pacotes recebidos durante a conexão.

Pacotes Transmitidos com Sucesso (TX-OK):

Antes da conexão: enp0s3 tinha 918 pacotes transmitidos.

Depois da conexão: enp0s3 tem 940 pacotes transmitidos.

Diferença: $940 - 918 = 22$ pacotes transmitidos durante a conexão.

A diferença nas estatísticas de RX-OK e TX-OK demonstra claramente que pacotes foram recebidos e transmitidos durante a abertura da conexão TCP. Essas mudanças indicam que a interface de rede enp0s3 foi utilizada para estabelecer e manter a conexão com o servidor web (google.com), evidenciando a atividade de rede relacionada à conexão TCP.

Portanto, os valores aumentados em RX-OK e TX-OK após a tentativa de conexão com telnet confirmam que a conexão foi aberta e dados foram transmitidos e recebidos.

5. Abra uma conexão ssh para o usuário bob no localhost. Assuma que esta conexão é indevida e realize a Análise e Auditoria de Conexão ssh com lsof.

Conexão SSH para o Usuário Bob no Localhost:

```
carol@iansantos:~$ ssh bob@localhost
bob@localhost's password:
Permission denied, please try again.
bob@localhost's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

74 updates can be applied immediately.
26 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
bob@iansantos:~$ sudo lsof -i -n -P | grep ssh
[sudo] password for bob:
sshd      10115      root    3u  IPv4  45659      0t0  TCP *:22 (LISTEN)
sshd      10115      root    4u  IPv6  45670      0t0  TCP *:22 (LISTEN)
ssh       17593      carol    3u  IPv4  58196      0t0  TCP 127.0.0.1:44630->127.0.0.1:22 (ESTABLISHED)
sshd      17594      root    4u  IPv4  58197      0t0  TCP 127.0.0.1:22->127.0.0.1:44630 (ESTABLISHED)
sshd      17722      carol    4u  IPv4  58197      0t0  TCP 127.0.0.1:22->127.0.0.1:44630 (ESTABLISHED)
ssh       18188      carol    3u  IPv4  68538      0t0  TCP 127.0.0.1:52890->127.0.0.1:22 (ESTABLISHED)
sshd      18189      root    4u  IPv4  68539      0t0  TCP 127.0.0.1:22->127.0.0.1:52890 (ESTABLISHED)
sshd      18301      bob     4u  IPv4  68539      0t0  TCP 127.0.0.1:22->127.0.0.1:52890 (ESTABLISHED)
```

Matando conexão:

```
carol@iansantos
bob@iansantos:~$ sudo kill 18301
Connection to localhost closed by remote host.
Connection to localhost closed.
carol@iansantos:~$
```

6. Escaneie todas as portas do localhost, pare todos os serviços de Login Remoto com conexões abertas e realize novo escaneamento para mostrar que as conexões não estão mais abertas.

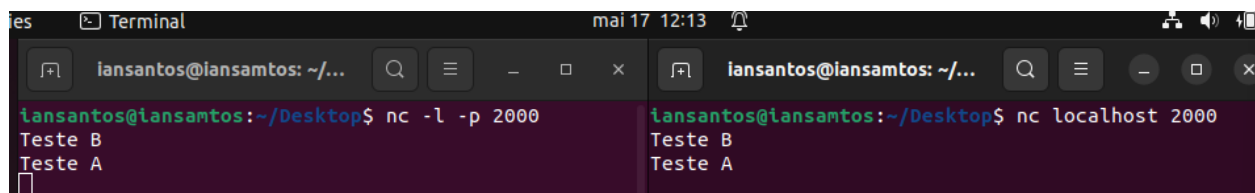
```
iansantos@iansantos:~/Desktop$ sudo nmap -p- localhost
[sudo] password for iansantos:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-17 12:11 -03
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp    open  ipp
3306/tcp   open  mysql
33060/tcp  open  mysqlx
46561/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
iansantos@iansantos:~/Desktop$ sudo systemctl stop ssh
iansantos@iansantos:~/Desktop$ sudo nmap -p- localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-17 12:11 -03
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
631/tcp    open  ipp
3306/tcp   open  mysql
33060/tcp  open  mysqlx
46561/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
iansantos@iansantos:~/Desktop$
```

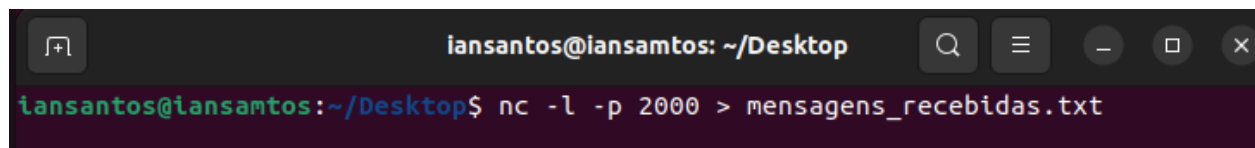
7. Utilize netcat para criar um socket TCP A para escutar na porta 2000 e criar um outro socket TCP B para enviar e receber dados de/para A. Envie a mensagem "Teste B" de B para A e a mensagem "Teste A" de A para B.

Trocando mensagens na porta 2000



The image shows two terminal windows side-by-side. The left window has the prompt `iansantos@iansantos: ~/Desktop$` and contains the command `nc -l -p 2000`. Below the command, it shows the received messages `Teste B` and `Teste A`. The right window has the prompt `iansantos@iansantos: ~/Desktop$` and contains the command `nc localhost 2000`. Below the command, it shows the sent messages `Teste B` and `Teste A`.

Verificando mensagens recebidas de B por A:



The image shows a terminal window with the prompt `iansantos@iansantos: ~/Desktop$`. The command entered is `nc -l -p 2000 > mensagens_recebidas.txt`.

Resultado:



The image shows a Text Editor window titled `*mensagens_recebidas.txt` with the file path `~/Desktop`. The content of the file is `1 teste B`.