

Core Linux

Objetivo da atividade realizada é criar uma máquina virtual (Virtual Machine Box), para assim criar um site fakebook.

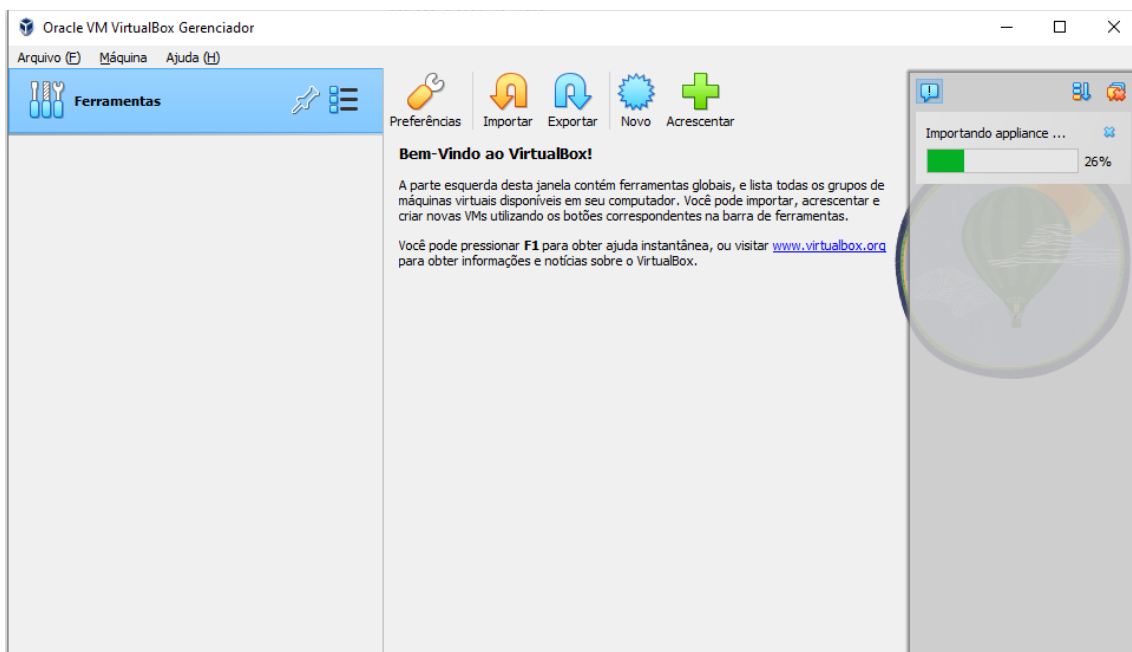
Conceitos trabalhados: Serviço, servidores e protocolos.

Serviço: No caso dessa atividade, o serviço funciona como uma forma de autenticar e validar o site.

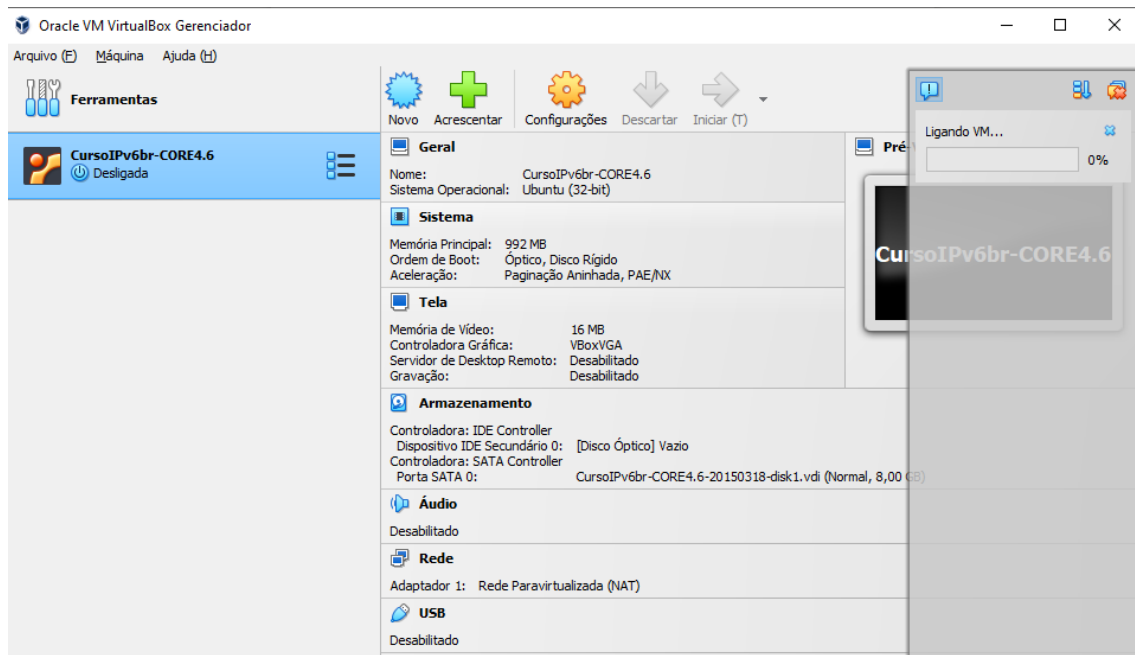
Servidores: O servidor funciona como um todo, desde hosts e switch até o funcionamento de uma rede. No caso do fakebook, o putty funciona como servidor e que deve ficar ativo a todo momento.

Protocolo: O protocolo de rede é o endereço, como: IP,TCP,UDP,HTTP. No caso da atividade do fakebook, utilizei o protocolo de rede http.

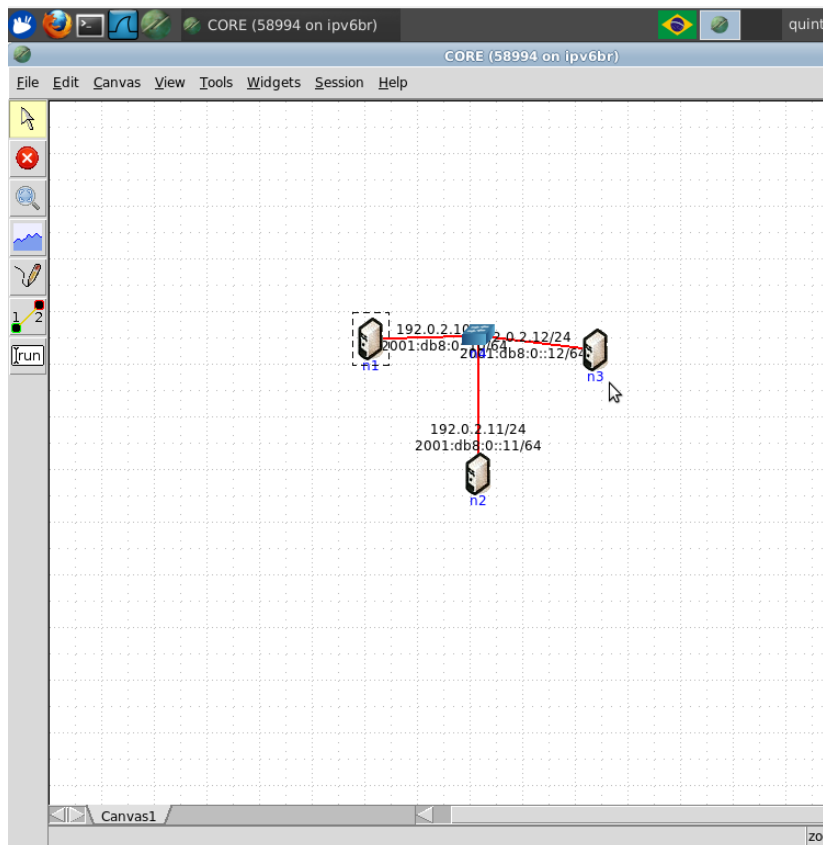
Primeiro passo é importar a máquina virtual:



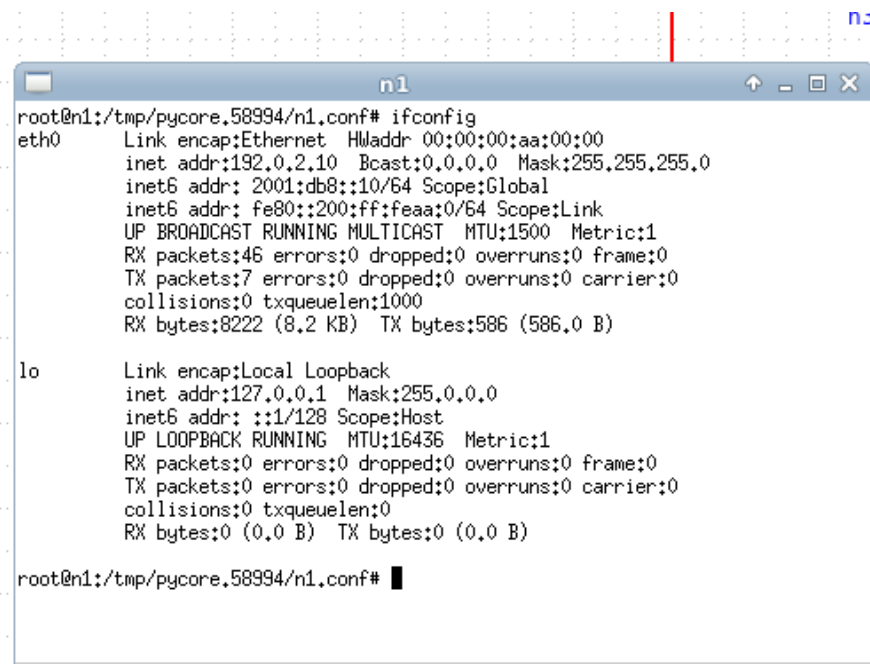
Depois ligar a máquina:



Abri o core Linux que se encontrava na área de trabalho, e depois montei uma esquemática:



Depois iniciei o servidor e utilizei o terminal da máquina (n1):



```
root@n1:/tmp/pycore.58994/n1.conf# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:00:00:aa:00:00
          inet addr:192.0.2.10  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: 2001:db8::10/64 Scope:Global
          inet6 addr: fe80::200:ff:feaa:0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8222 (8.2 KB)  TX bytes:586 (586.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@n1:/tmp/pycore.58994/n1.conf#
```

Utilizei um comando de máscara de rede:

```
root@n1:/tmp/pycore.58994/n1.conf# ifconfig eht0 10.0.0.1 netmask 255.255.255.0
SIOCSIFADDR: No such device
eht0: ERROR while getting interface flags: No such device
SIOCSIFNETMASK: No such device
root@n1:/tmp/pycore.58994/n1.conf# ifconfig eth0 10.0.0.1 netmask 255.255.255.0
root@n1:/tmp/pycore.58994/n1.conf#
```

Perceba que não deu nenhum retorno, isso acontece quando o comando é utilizado de forma correta.

Depois disso abri o terminal da máquina *n2* e configurei o ip:

```
n2
root@n2:/tmp/pycore.58994/n2.conf# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:00:00:aa:00:01
          inet addr:192.0.2.11  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: 2001:db8::11/64 Scope:Global
          inet6 addr: fe80::200:ff:feaa:1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8112 (8.1 KB)  TX bytes:586 (586.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@n2:/tmp/pycore.58994/n2.conf# ifconfig eth0 10.0.0.2 netmask 255.255.255.0
root@n2:/tmp/pycore.58994/n2.conf#
```

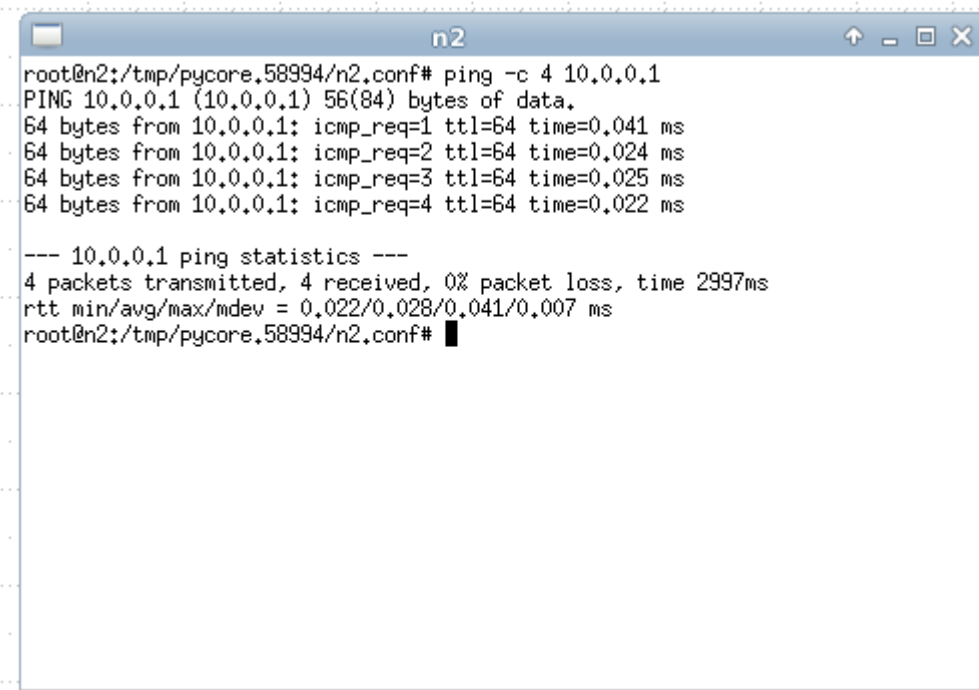
Repeti o processo na máquina n3:

```
n3
root@n3:/tmp/pycore.58994/n3.conf# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:00:00:aa:00:02
          inet addr:192.0.2.12  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::200:ff:feaa:2/64 Scope:Link
          inet6 addr: 2001:db8::12/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8002 (8.0 KB)  TX bytes:586 (586.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@n3:/tmp/pycore.58994/n3.conf# ifconfig eth0 10.0.0.3 255.255.255.0
SIOCSIFADDR: Invalid argument
root@n3:/tmp/pycore.58994/n3.conf# ifconfig eth0 10.0.0.3 netmask 255.255.255.0
root@n3:/tmp/pycore.58994/n3.conf#
```

Após configurar o ip das três máquinas, testei o comando para o teste de ping:



```
root@n2:/tmp/pycore.58994/n2.conf# ping -c 4 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data:
64 bytes from 10.0.0.1: icmp_req=1 ttl=64 time=0.041 ms
64 bytes from 10.0.0.1: icmp_req=2 ttl=64 time=0.024 ms
64 bytes from 10.0.0.1: icmp_req=3 ttl=64 time=0.025 ms
64 bytes from 10.0.0.1: icmp_req=4 ttl=64 time=0.022 ms

--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.022/0.028/0.041/0.007 ms
root@n2:/tmp/pycore.58994/n2.conf#
```

Utilizei o comando `man ping` para acessar o manual de informações no Linux, pelo terminal:

```

PING(8)                                     System Manager's Manual: iputils                                     PING(8)
NAME
    ping, ping6 - send ICMP ECHO_REQUEST to network hosts

SYNOPSIS
    ping [-LRUbfmrvWaAB] [-c count] [-m mark] [-i interval] [-l preload]
    [-p pattern] [-s packetsize] [-t ttl] [-w deadline] [-F flowlabel] [-I
    interface] [-H hint] [-N nioption] [-Q tos] [-S sndbuf] [-T timestamp
    option] [-W timeout] [hop ...] destination

DESCRIPTION
    ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit
    an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams
    ('pings') have an IP and ICMP header, followed by a struct timeval
    and then an arbitrary number of 'pad' bytes used to fill out the
    packet.

    ping6 can also send Node Information Queries (RFC4620).

OPTIONS
    -a      Audible ping.

Manual page ping(8) line 1 (press h for help or q to quit)

```

Teste comandos como ls, mkdir, cd, touch(para criar arquivo txt) e nano para editar um arquivo txt diretamente do terminal.

```

n2
TEXT0 ESCRITO A AAA

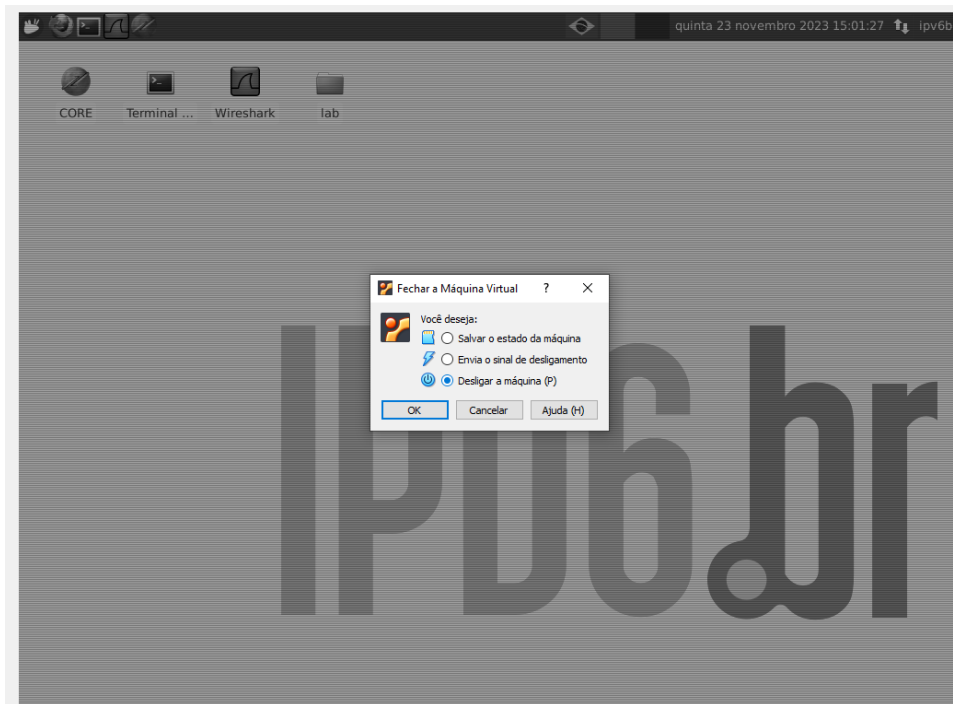
[ Wrote 1 line ]

root@n2:/tmp/pycore.58994/n2.conf/aluno-pasta# cat aluno-texto
TEXT0 ESCRITO A AAA
root@n2:/tmp/pycore.58994/n2.conf/aluno-pasta#

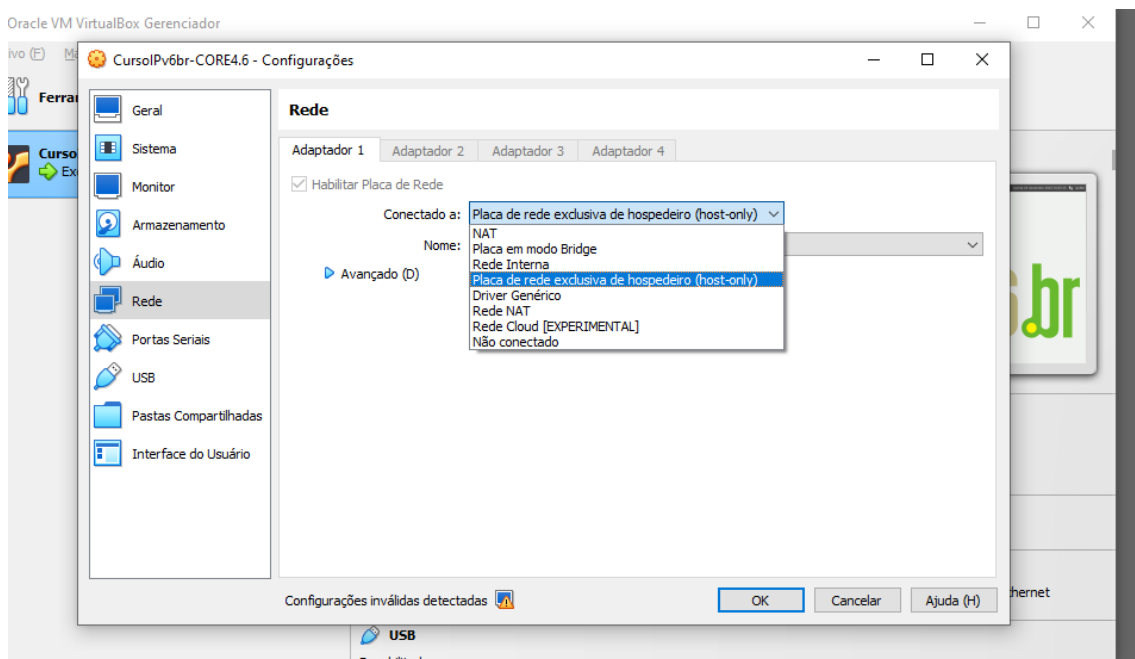
```

Parte final: Criando um “fakebook”

Passo 1 : desligando a máquina do processo anterior:



Passo 2: Alterar configurações de rede da virtual box para “placa de rede exclusiva de hospedeiro:



Passo 3: Após abrir a máquina, inserir o comando ifconfig para pegar o ip:



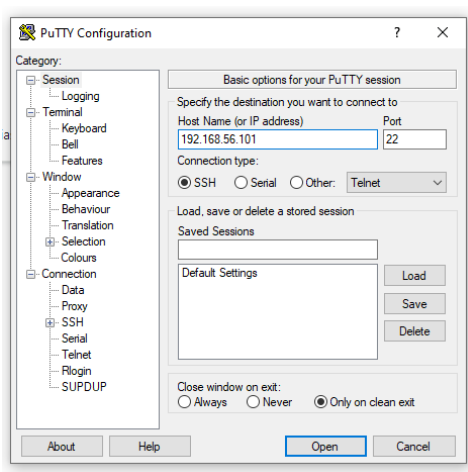
```
Terminal - ipv6br@ipv6b...
Terminal - ipv6br@ipv6br: ~
File Edit View Terminal Go Help
ipv6br@ipv6br:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c4:de:f0
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec4:def0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4724 (4.7 KB)  TX bytes:11457 (11.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:536 errors:0 dropped:0 overruns:0 frame:0
          TX packets:536 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:37560 (37.5 KB)  TX bytes:37560 (37.5 KB)

ipv6br@ipv6br:~$
```

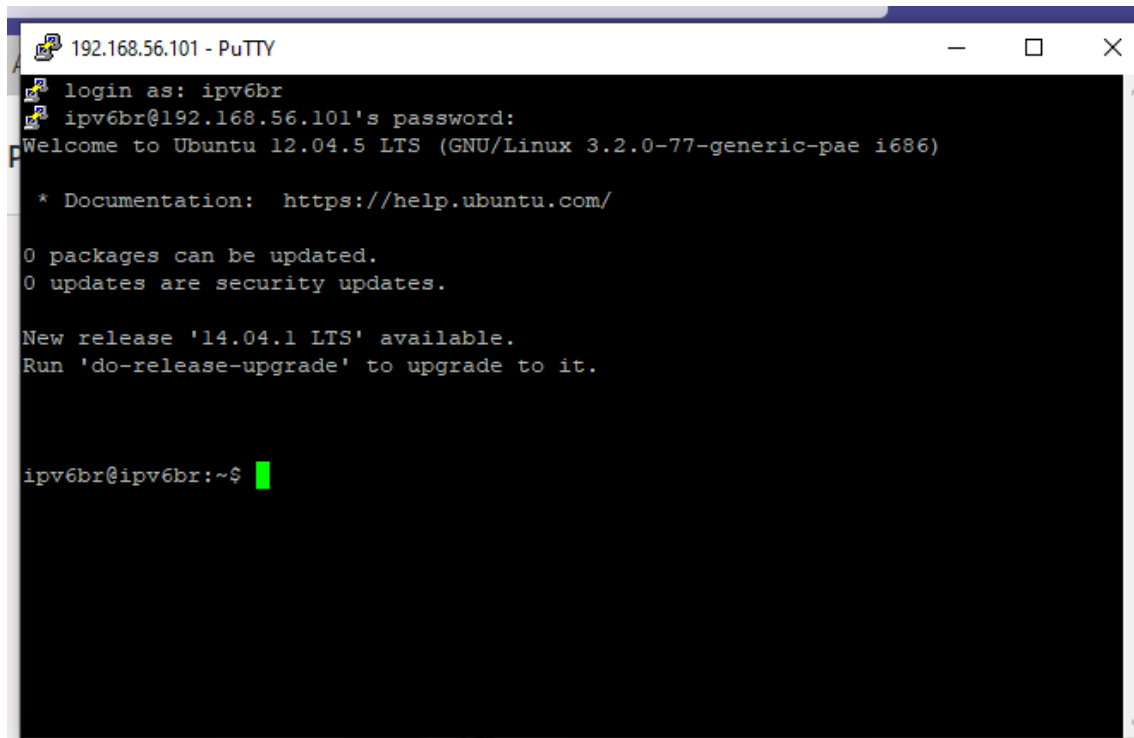
O ip fica ao lado de “inet addr” (192.158.56.101)

Passo 4: Instalar um software chamado “Putty”:



Executar o programa.. E inserir o ip que observamos no terminal da virtual box.

Passo 5: Inserir o login e senha no put (ipv6br).



```
192.168.56.101 - PuTTY
login as: ipv6br
ipv6br@192.168.56.101's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.2.0-77-generic-pae i686)

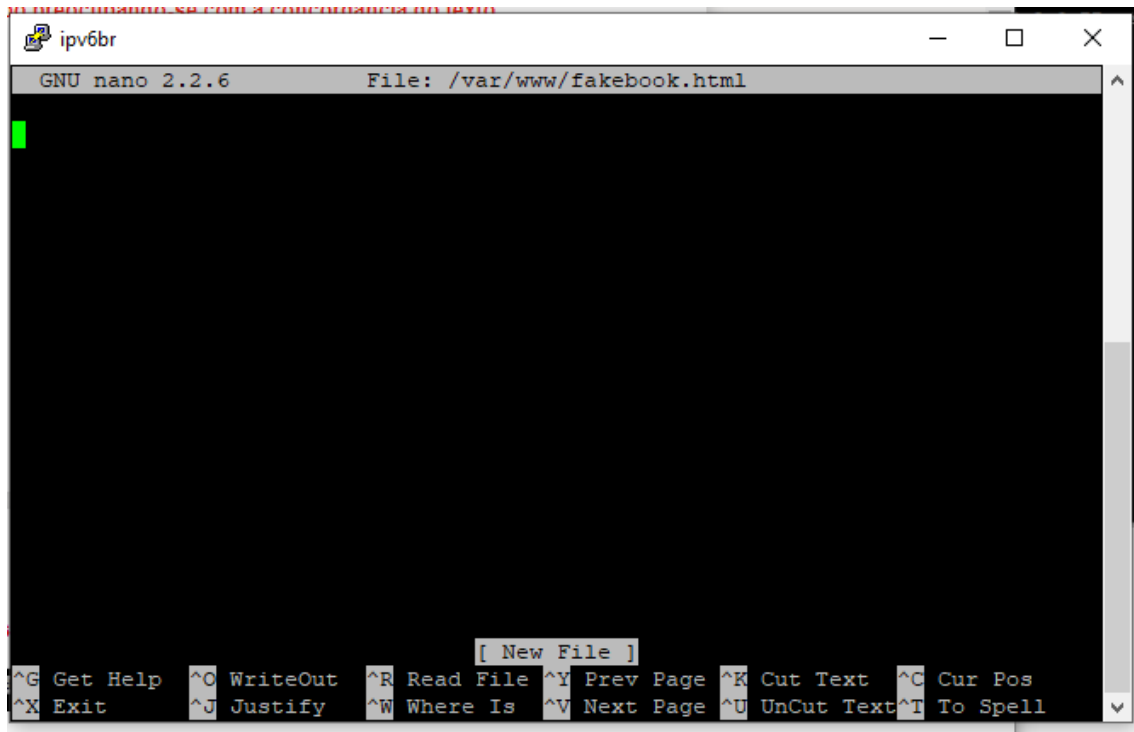
 * Documentation:  https://help.ubuntu.com/

0 packages can be updated.
0 updates are security updates.

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

ipv6br@ipv6br:~$
```

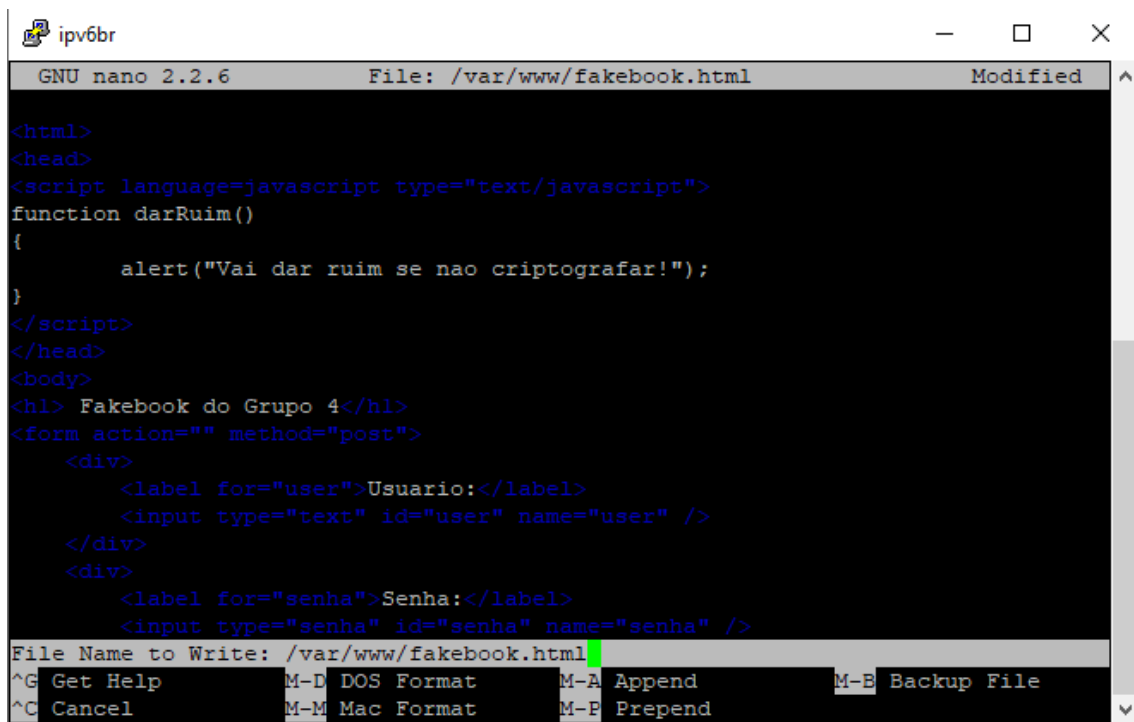
Passo 6: Utilizei o comando sudo su, seguido de: "nano /var/www/fakebook.html"



```
GNU nano 2.2.6 File: /var/www/fakebook.html

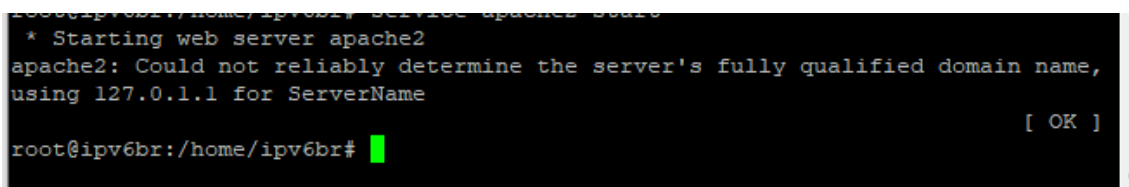
[ New File ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

Passo 7: Copiei o código em html do fakebook, depois alterei o nome para o do grupo:



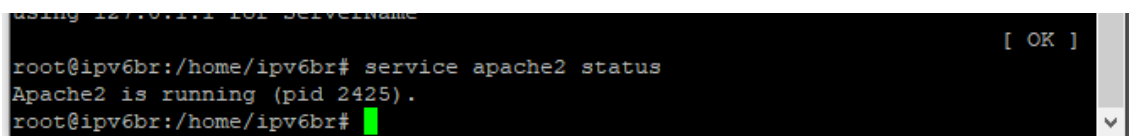
```
GNU nano 2.2.6 File: /var/www/fakebook.html Modified
<html>
<head>
<script language=javascript type="text/javascript">
function darRuim()
{
    alert("Vai dar ruim se nao criptografar!");
}
</script>
</head>
<body>
<h1> Fakebook do Grupo 4</h1>
<form action="" method="post">
    <div>
        <label for="user">Usuario:</label>
        <input type="text" id="user" name="user" />
    </div>
    <div>
        <label for="senha">Senha:</label>
        <input type="senha" id="senha" name="senha" />
    </div>
</form>
</body>
</html>
```

Passo 8: Utilizei o comando service apache2 start, para iniciar os serviços web:



```
root@ipv6br:/home/ipv6br# service apache2 start
* Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
root@ipv6br:/home/ipv6br#
```

Passo 9: Utilizei o comando service apache2 status para verificar se está funcionando corretamente:



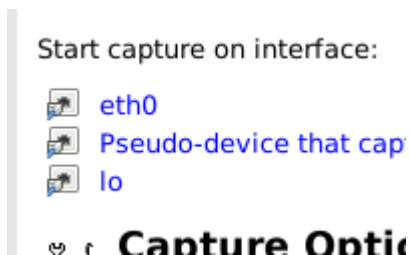
```
root@ipv6br:/home/ipv6br# service apache2 status
Apache2 is running (pid 2425).
root@ipv6br:/home/ipv6br#
```

Passo 10: Acessei o site:

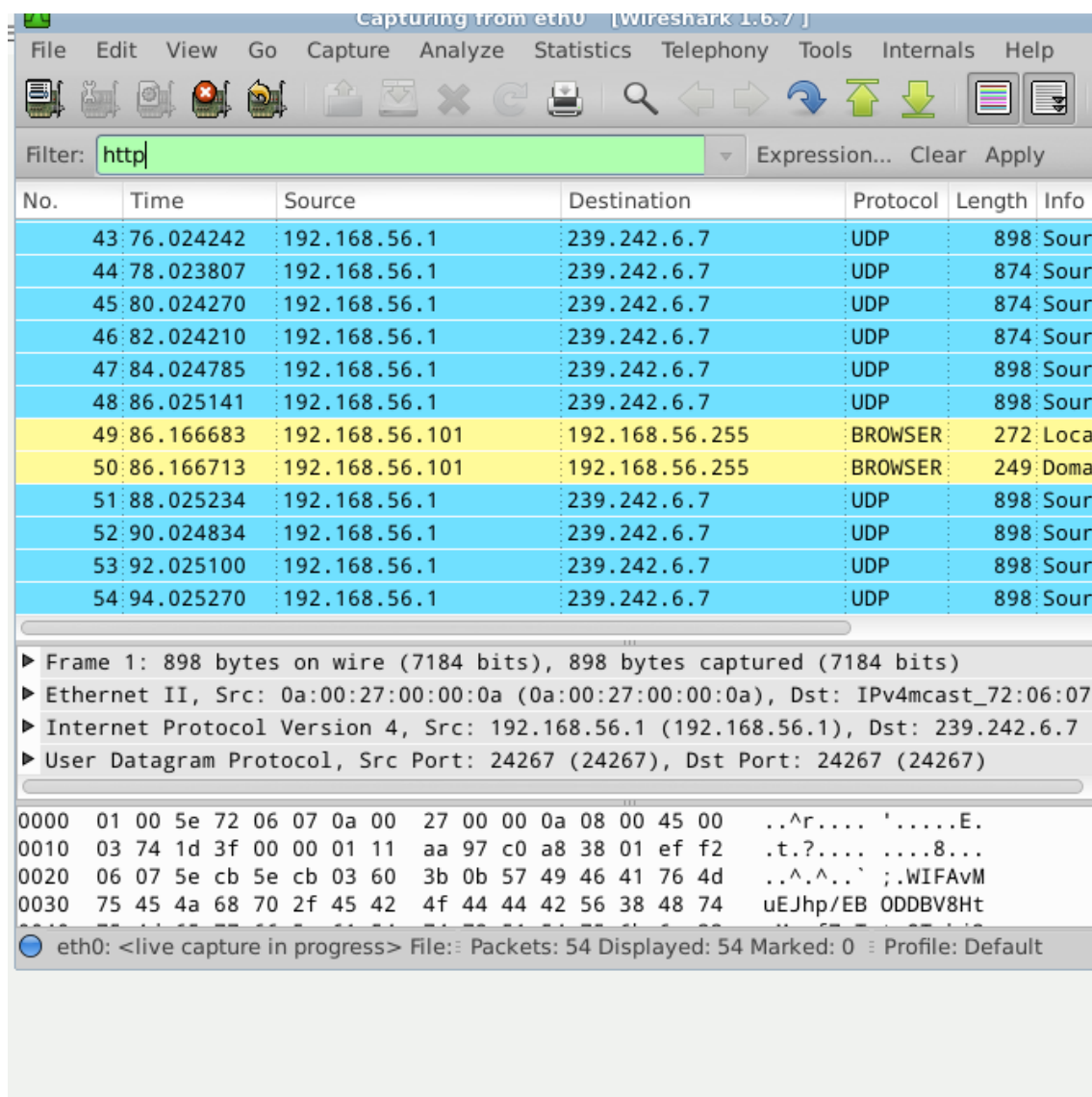


Utilizei o ip para acessar.

Passo 11: Abrir o Wireshark na VirtualBox, e aperta no eth0:



Passo 12: Após abrir a aba eth0 do “Wireshark”, Filtrei o termo http:



Passo 13:Voltei no site eu utilizei o mesmo login registrado na programação html de antes;

Fakebook do Grupo 4

Usuário:
 Senha:

192.168.56.101 diz
 Vai dar ruim se nao criptografar!

Passo 14: Voltei no wireshark para o virtualbox, arrastei a barra vertical e procurei pelo termo “HTTP/1.1 200 OK” na sessão de informações:

Iter:	http	▼	Expression...	Clear	Apply
Destination	Protocol	Length	Info		
192.168.56.101	TCP	66	55685 > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W		
192.168.56.1	TCP	66	http > 55685 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0		
192.168.56.101	TCP	66	55686 > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W		
192.168.56.1	TCP	66	http > 55686 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0		
192.168.56.101	TCP	54	55685 > http [ACK] Seq=1 Ack=1 Win=2102272 Len=0		
192.168.56.101	TCP	54	55686 > http [ACK] Seq=1 Ack=1 Win=2102272 Len=0		
192.168.56.101	HTTP	714	POST /fakebook.html HTTP/1.1 (application/x-www-fo		
192.168.56.1	TCP	54	http > 55685 [ACK] Seq=1 Ack=661 Win=15920 Len=0		
192.168.56.1	HTTP	702	HTTP/1.1 200 OK (text/html)		
192.168.56.101	TCP	54	55685 > http [ACK] Seq=661 Ack=649 Win=2101504 Len=		
192.168.56.1	TCP	66	http > 55686 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0		
192.168.56.101	TCP	66	[TCP Dup ACK 132#1] 55686 > http [ACK] Seq=1 Ack=1		

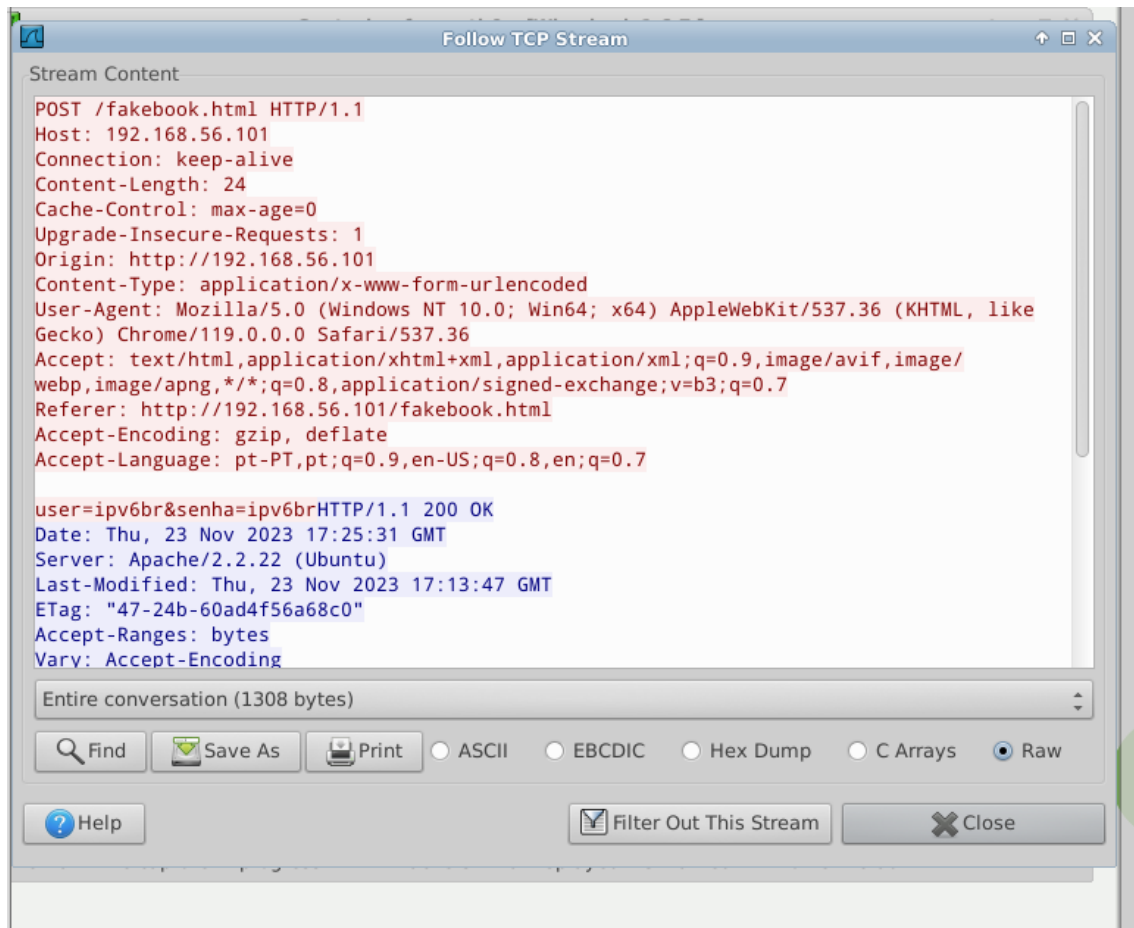
Frame 135: 702 bytes on wire (5616 bits), 702 bytes captured (5616 bits)

Ethernet II, Src: CadmusCo_c4:de:f0 (08:00:27:c4:de:f0), Dst: 0a:00:27:00:00:0a (0a:00:27:00:00:0a)

Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 192.168.56.1 (192.168.56.1)

Transmission Control Protocol, Src Port: http (80), Dst Port: 55685 (55685), Seq: 1, Ack:

Passo 15: Selecione a informação, apertei o botão direito e selecionei a opção “Follow TCP Stream”:



Aqui vemos diversas codificações sobre o site e também mostra que a segurança é falha, onde mostra o login que utilizei na máquina com o Google.