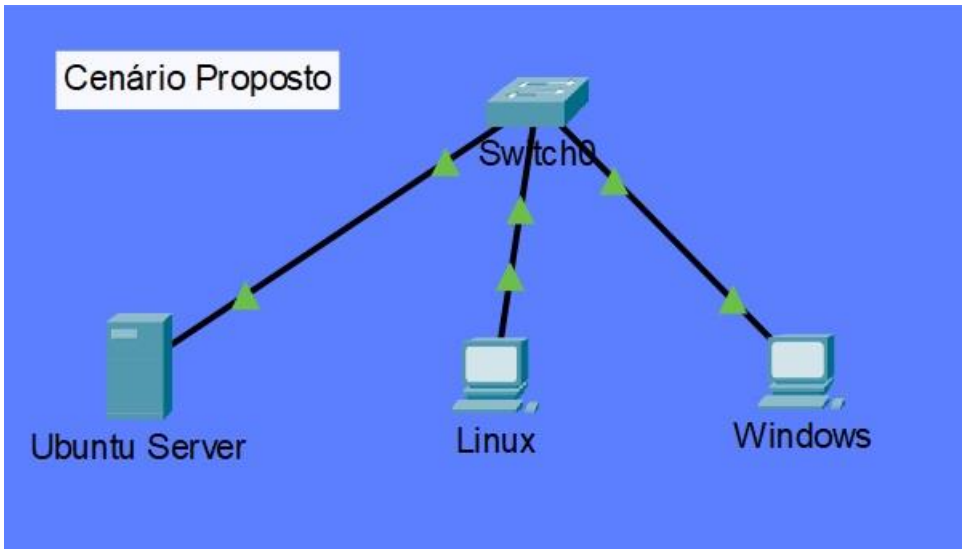
Configuração com Servidores DHCP/DNS/HTTPS/SSH:

Nome: Enzo Arrue

Cenário: Topologia com um servidor DHCP/DNS/HTTPS/SSH e 2 máquinas clientes DHCP/DNS/HTTPS/SSH (Windows e/ou Linux).



Configurações

1.

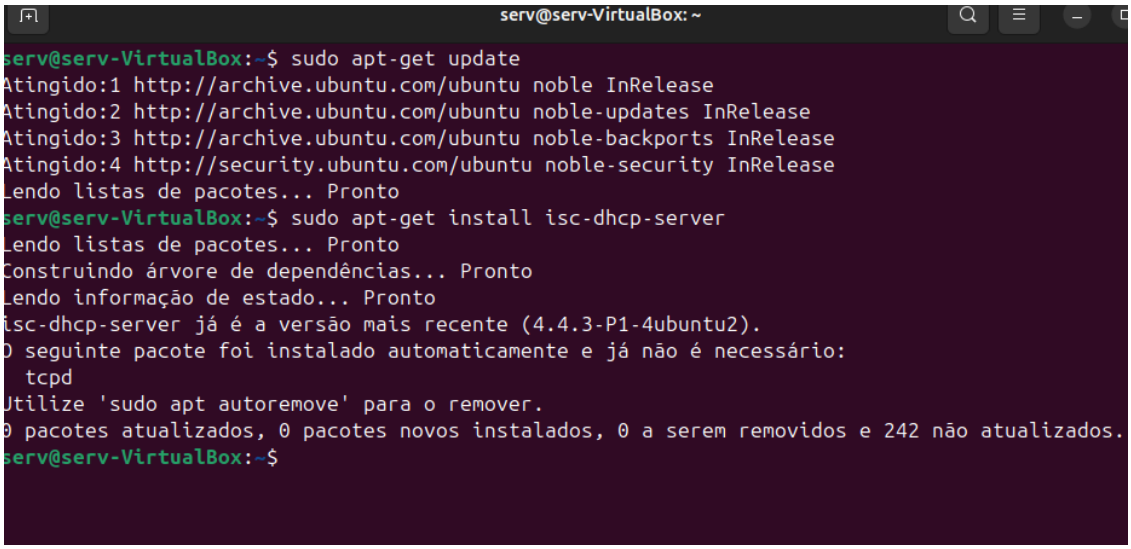
1.1.Criar a configuração para a rede onde estão as máquinas cliente e o servidor DHCP.

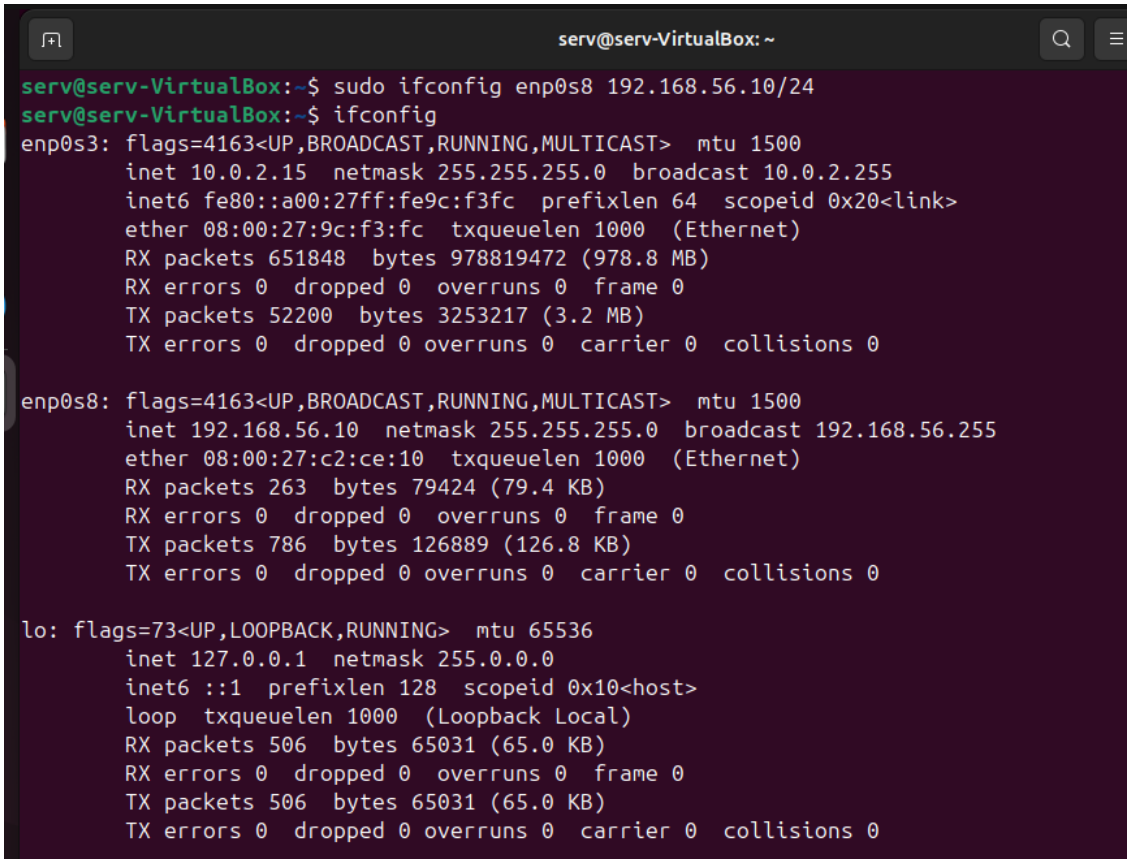
2. Configurar as máquinas (Windows e/ou Linux) e o servidor DHCP com a faixa de endereços IPs conforme o que for escolhido pelo grupo.

2.1. Configurar o arquivo /etc/dhcp/dhcpd.conf no servidor DHCP.

2.2. Testar na(s) máquina(s) Linux e/ou Windows como clientes DHCP para receber IP da faixa de IPs determinada pelo servidor DHCP.

2.3. Capturar o arquivo lease (Windows e/ou Linux) com tail -f /var/lib/dhcp/dhcpd.leases e dhcp-lease-list.


serv@serv-VirtualBox: ~
serv@serv-VirtualBox:~$ sudo apt-get update
Atingido:1 http://archive.ubuntu.com/ubuntu noble InRelease
Atingido:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Atingido:3 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Atingido:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Lendo listas de pacotes... Pronto
serv@serv-VirtualBox:~$ sudo apt-get install isc-dhcp-server
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
isc-dhcp-server já é a versão mais recente (4.4.3-P1-4ubuntu2).
O seguinte pacote foi instalado automaticamente e já não é necessário:
tcpd
Utilize 'sudo apt autoremove' para o remover.
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 242 não atualizados.
serv@serv-VirtualBox:~$


serv@serv-VirtualBox: ~
serv@serv-VirtualBox:~$ sudo ifconfig enp0s8 192.168.56.10/24
serv@serv-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe9c:f3fc prefixlen 64 scopeid 0x20<link>
ether 08:00:27:9c:f3:fc txqueuelen 1000 (Ethernet)
RX packets 651848 bytes 978819472 (978.8 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 52200 bytes 3253217 (3.2 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.10 netmask 255.255.255.0 broadcast 192.168.56.255
ether 08:00:27:c2:ce:10 txqueuelen 1000 (Ethernet)
RX packets 263 bytes 79424 (79.4 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 786 bytes 126889 (126.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Loopback Local)
RX packets 506 bytes 65031 (65.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 506 bytes 65031 (65.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```
  GNU nano 7.2                    /etc/dhcp/dhcpd.conf
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}
subnet 192.168.56.0 netmask 255.255.255.0 {
        range 192.168.56.150 192.168.56.200;
        option routers 192.168.56.1;
        option domain-name-servers 192.168.56.10;
        option domain-name "enzoarrue.com.br";
}



                        [ Escritas 118 linhas ]
^G Ajuda      ^O Gravar     ^W Onde está?^K Recortar   ^T Executar   ^C Local
```

```
serv@serv-VirtualBox: ~
serv@serv-VirtualBox:~$ sudo systemctl restart isc-dhcp-server
serv@serv-VirtualBox:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-05-19 17:22:02 -03; 3s ago
       Docs: man:dhcpd(8)
   Main PID: 36640 (dhcpd)
      Tasks: 1 (limit: 3437)
     Memory: 3.7M (peak: 4.0M)
        CPU: 8ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─36640 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc>

mai 19 17:22:02 serv-VirtualBox dhcpd[36640]: Sending on   LPF/enp0s8/08:00:27:c2:ce:10/192.168.5>
mai 19 17:22:02 serv-VirtualBox dhcpd[36640]:
mai 19 17:22:02 serv-VirtualBox dhcpd[36640]: No subnet declaration for enp0s3 (10.0.2.15).
mai 19 17:22:02 serv-VirtualBox dhcpd[36640]: ** Ignoring requests on enp0s3.  If this is not what
mai 19 17:22:02 serv-VirtualBox dhcpd[36640]:    you want, please write a subnet declaration
mai 19 17:22:02 serv-VirtualBox dhcpd[36640]:    in your dhcpd.conf file for the network segment
mai 19 17:22:02 serv-VirtualBox dhcpd[36640]:    to which interface enp0s3 is attached. **
mai 19 17:22:02 serv-VirtualBox dhcpd[36640]:
mai 19 17:22:02 serv-VirtualBox dhcpd[36640]: Sending on   Socket/fallback/fallback-net
mai 19 17:22:02 serv-VirtualBox dhcpd[36640]: Server starting service.
lines 1-21/21 (END)
```

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet6 fe80::7932:48ea:8b1c:1c28  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:04:42:0f  txqueuelen 1000  (Ethernet)
      RX packets 6  bytes 2480 (2.4 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 40  bytes 5812 (5.6 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet6 fe80::c1c8:bd07:b142:fb23  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:46:35:f8  txqueuelen 1000  (Ethernet)
      RX packets 17  bytes 3276 (3.1 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 59  bytes 10543 (10.2 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
      loop  txqueuelen 1000  (Local Loopback)
      RX packets 8  bytes 480 (480.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 8  bytes 480 (480.0 B)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# dhclient

┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
      inet6 fe80::7932:48ea:8b1c:1c28  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:04:42:0f  txqueuelen 1000  (Ethernet)
      RX packets 8  bytes 3660 (3.5 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 45  bytes 6678 (6.5 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.56.151  netmask 255.255.255.0  broadcast 192.168.56.255
      inet6 fe80::c1c8:bd07:b142:fb23  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:46:35:f8  txqueuelen 1000  (Ethernet)
      RX packets 20  bytes 4022 (3.9 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 62  bytes 11289 (11.0 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

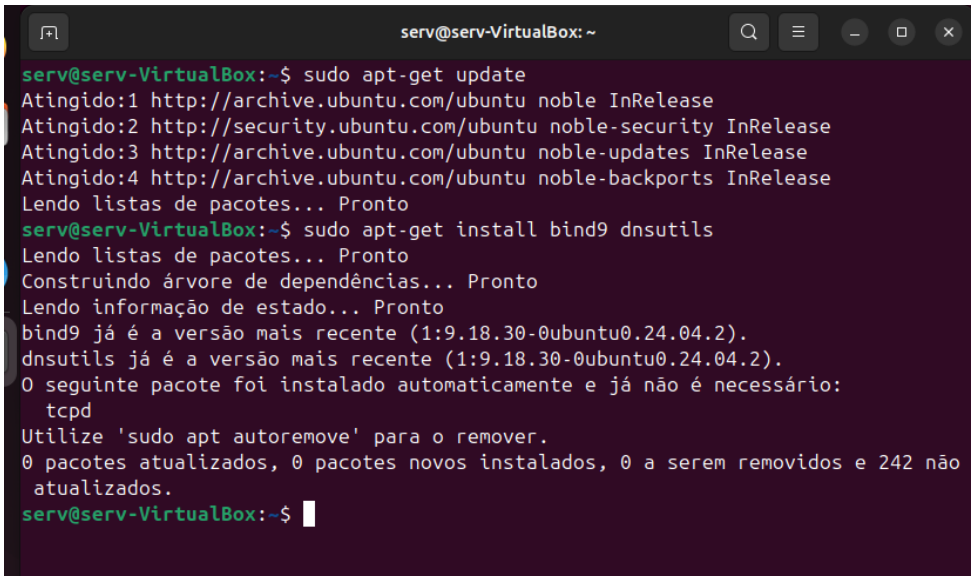
```
serv@serv-VirtualBox:~$ tail -f /var/lib/dhcp/dhcpd.leases
lease 192.168.56.151 {
  starts 1 2025/05/19 20:23:07;
  ends 1 2025/05/19 20:33:07;
  cltt 1 2025/05/19 20:23:07;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:46:35:f8;
  client-hostname "kali";
}
^C
serv@serv-VirtualBox:~$ dhcp-lease-list
To get manufacturer names please download http://standards-oui.ieee.org/oui.txt to /usr/local/etc/
oui.txt
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC               IP              hostname       valid until         manufacturer
==================================================================================================
08:00:27:46:35:f8  192.168.56.150  kali           2025-05-19 20:25:59 -NA-
serv@serv-VirtualBox:~$
```

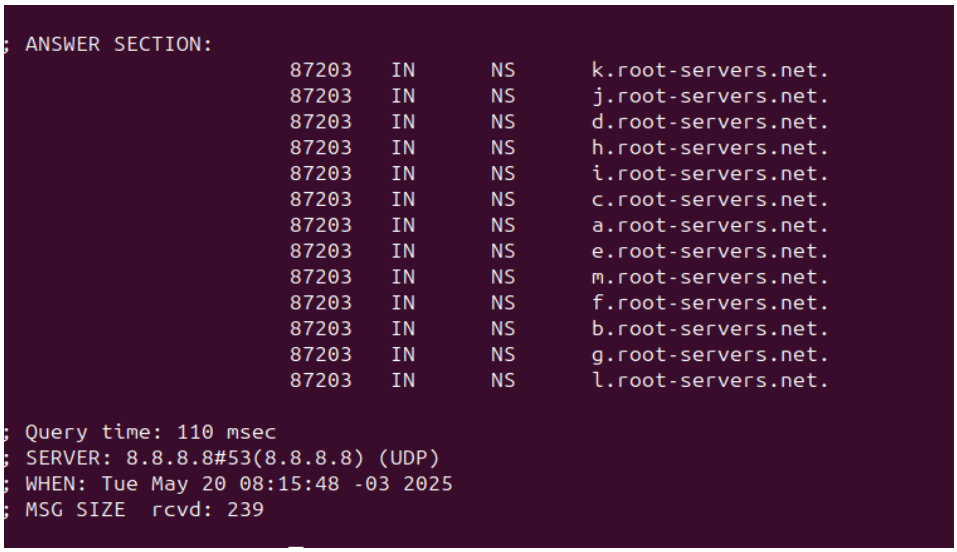
3. Configurar as máquinas (Windows e/ou Linux) e o servidor DNS.

3.1. Configurar o servidor DNS usando um endereço IP do servidor DHCP, criando o domínio do grupo (por exemplo, nomedogrupo.com.br), criando o FQDN, (por exemplo, servidor.nomedogrupo.com.br), assim como os CNAMES (www, phpserver).

3.2. Testar na(s) máquina(s) cliente(s) usando o nslookup e ping.

DNS:





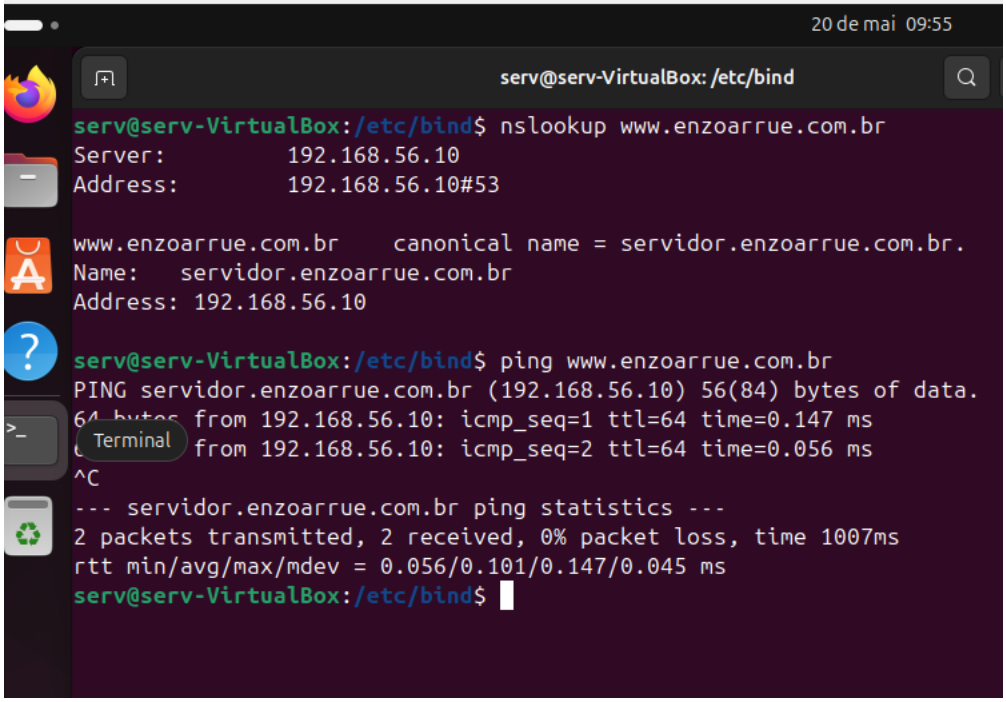
```
serv@serv-VirtualBox:~$ ifconfig
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.10  netmask 255.255.255.0  broadcast 192.168.56.255
        ether 08:00:27:c2:ce:10  txqueuelen 1000  (Ethernet)
        RX packets 168  bytes 55440 (55.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 645  bytes 102744 (102.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Loopback Local)
        RX packets 530  bytes 55674 (55.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 530  bytes 55674 (55.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
serv@serv-VirtualBox:~$ sudo nano /etc/bind/named.conf.local
serv@serv-VirtualBox:~$ sudo nano /etc/bind/db.local
serv@serv-VirtualBox:~$ mkdir /etc/bind/zones
mkdir: não foi possível criar o diretório “/etc/bind/zones”: Permissão negada
serv@serv-VirtualBox:~$ sudo mkdir /etc/bind/zones
serv@serv-VirtualBox:~$ cd /etc/bind
serv@serv-VirtualBox:/etc/bind$ cp db.local zones/db.enzoarrue.com.br
cp: não foi possível criar arquivo comum 'zones/db.enzoarrue.com.br': Permissão negad
a
serv@serv-VirtualBox:/etc/bind$ sudo cp db.local zones/db.enzoarrue.com.br
serv@serv-VirtualBox:/etc/bind$ sudo nano /etc/bind/zones/db.enzoarrue.com.br
```

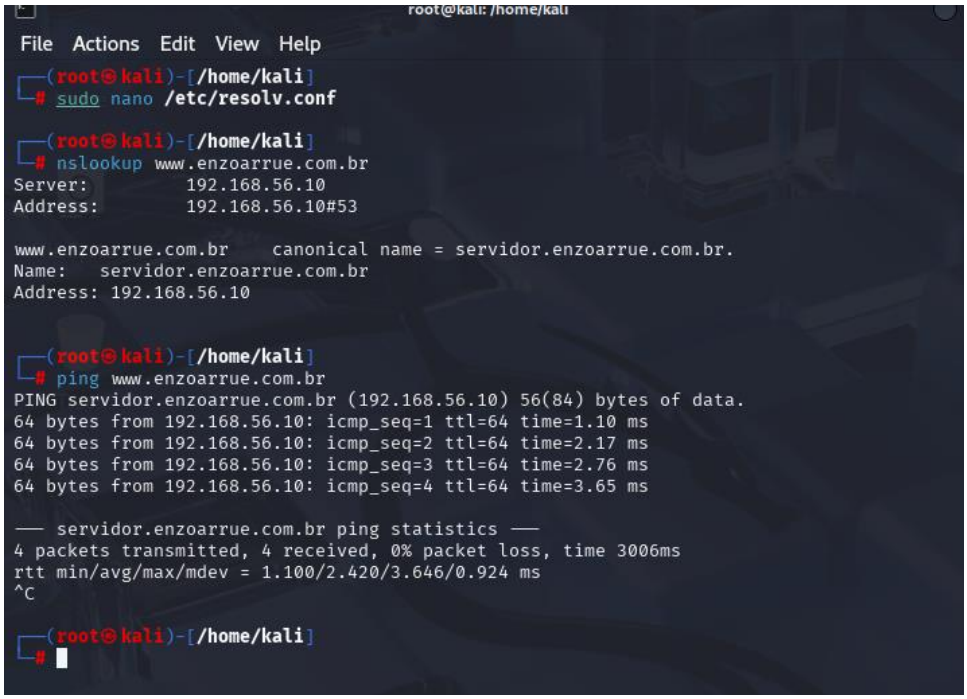
```
 GNU nano 7.2              /etc/bind/zones/db.enzoarrue.com.br

 BIND data file for local loopback interface

TTL    604800
       IN      SOA     servidor.enzoarrue.com.br root.servidor.enzoarrue.com.br. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

       IN      NS      localhost.
       IN      A       192.168.56.10
       IN      AAAA    ::1
ervidor        IN      A       192.168.56.10
ww     IN      CNAME   servidor
```

```
serv@serv-VirtualBox:/etc/bind$ sudo cp /etc/bind/db.127 /etc/bind/zones/db.192
serv@serv-VirtualBox:/etc/bind$ sudo nano /etc/bind/db.127
serv@serv-VirtualBox:/etc/bind$ sudo nano /etc/bind/zones/db.192
serv@serv-VirtualBox:/etc/bind$ named-checkconf
serv@serv-VirtualBox:/etc/bind$ named-checkzone enzoarrue.com.br
^Z
[2]+  Parado                 named-checkzone enzoarrue.com.br
serv@serv-VirtualBox:/etc/bind$ named-checkzone enzoarrue.com.br /etc/bind/zones/db.e
nzoarrue.com.br
zone enzoarrue.com.br/IN: loaded serial 2
OK
serv@serv-VirtualBox:/etc/bind$
```

```
serv@serv-VirtualBox:/etc/bind$ named-checkzone enzoarrue.com.br /etc/bind/zones/db.1
92
zone enzoarrue.com.br/IN: loaded serial 1
OK
serv@serv-VirtualBox:/etc/bind$ systemctl restart bind9
serv@serv-VirtualBox:/etc/bind$
```




```
serv@serv-VirtualBox:/etc/bind$ nslookup www.enzoarrue.com.br
Server:         192.168.56.10
Address:        192.168.56.10#53

www.enzoarrue.com.br    canonical name = servidor.enzoarrue.com.br.
Name:   servidor.enzoarrue.com.br
Address: 192.168.56.10

serv@serv-VirtualBox:/etc/bind$ ping www.enzoarrue.com.br
PING servidor.enzoarrue.com.br (192.168.56.10) 56(84) bytes of data.
64 bytes from 192.168.56.10: icmp_seq=1 ttl=64 time=0.147 ms
64 bytes from 192.168.56.10: icmp_seq=2 ttl=64 time=0.056 ms
^C
--- servidor.enzoarrue.com.br ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.056/0.101/0.147/0.045 ms
serv@serv-VirtualBox:/etc/bind$
```



4. Configurar as máquinas (Windows e/ou Linux) e o servidor HTTPS.

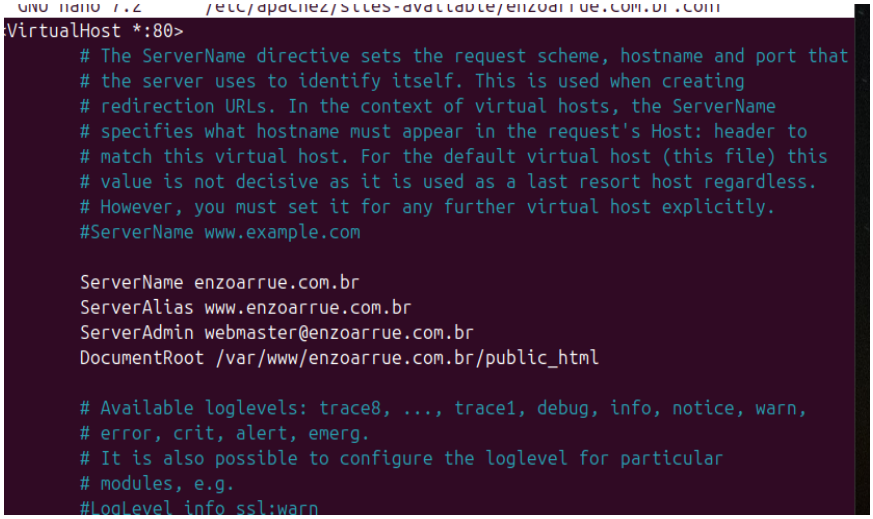
4.1. Configurar o servidor HTTPS com um certificado auto-assinado criado com o OpenSSL, respondendo a http://www.nomedogrupo.com.br e https://www.nomedogrupo.com.br, usando um endereço IP do servidor DHCP, criando o domínio do grupo (por exemplo, nomedogrupo.com.br), criando o FQDN, (por exemplo, servidor.nomedogrupo.com.br), assim como os CNAMES (www, phpserver).

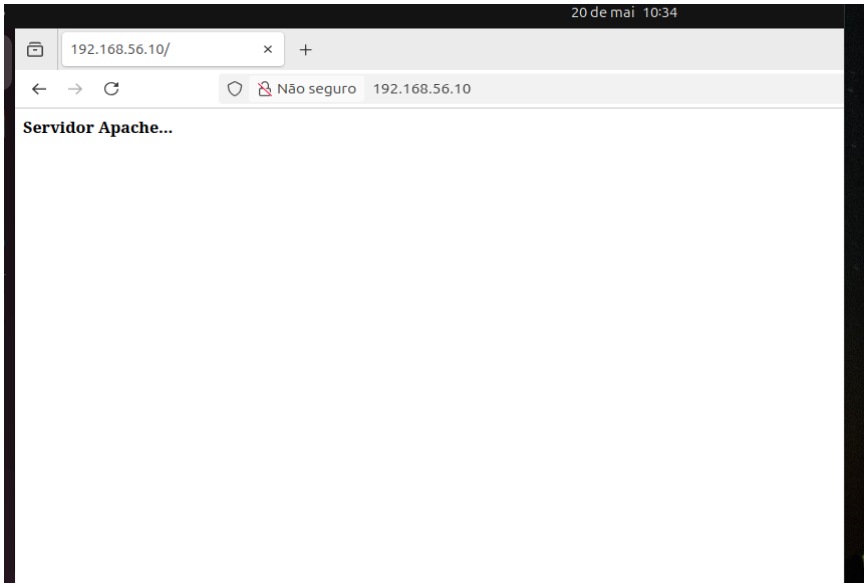
4.2. No servidor iniciar os serviços DHCP, DNS e Apache ou NGINX, monitorar o arquivo access.log (tail -f /var/log/apache2/access.log).

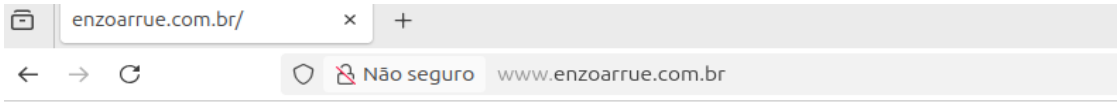
4.3. Testar na(s) máquina(s) cliente(s) HTTPS usando o browser (Firefox, Chrome, entre outros).

4.4. Realizar a captura HTTPS com o Wireshark (Kali)

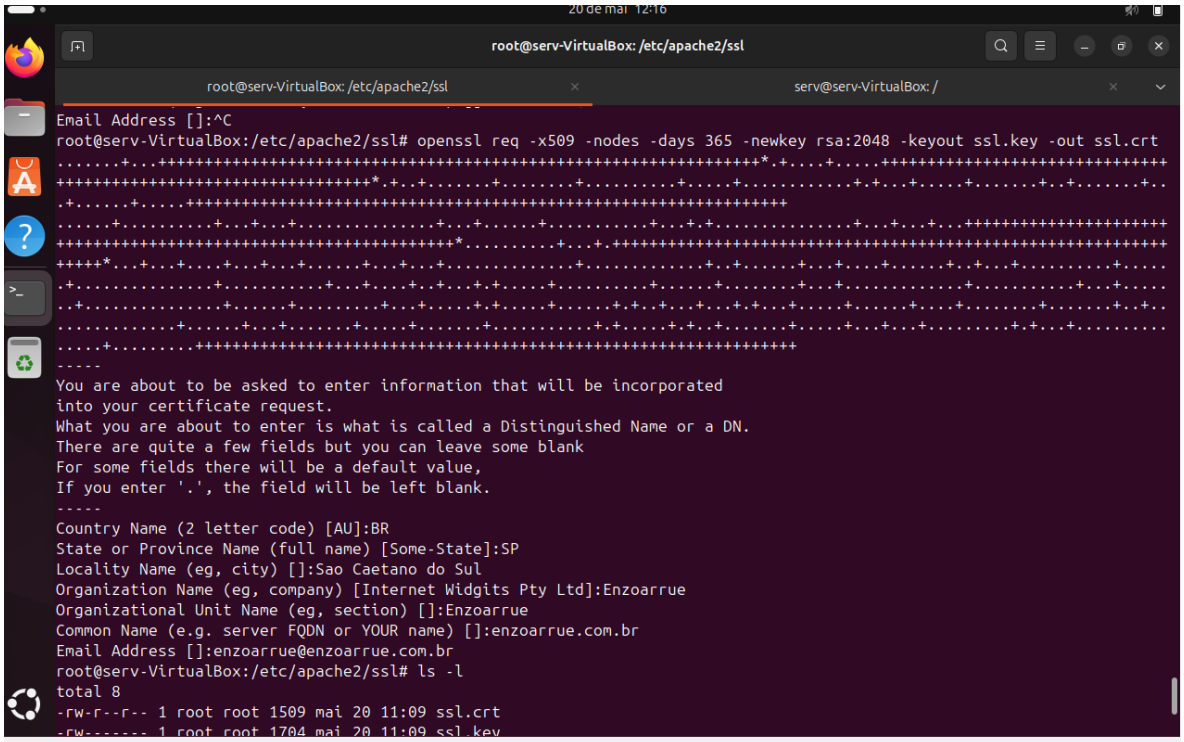
HTTP´/HTTPS:

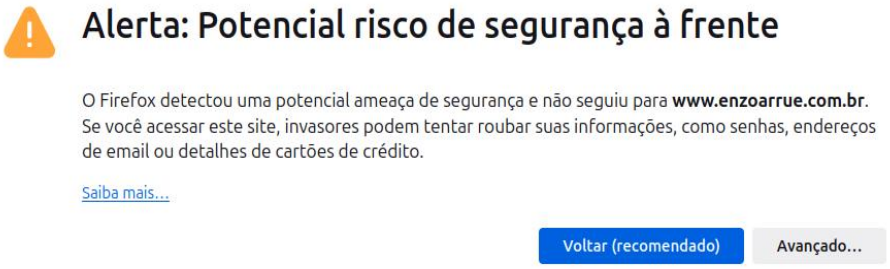

GNU nano 7.2 /etc/apache2/sites-available/enzoarrue.com.br.conf
<VirtualHost *:80>
The ServerName directive sets the request scheme, hostname and port that
the server uses to identify itself. This is used when creating
redirection URLs. In the context of virtual hosts, the ServerName
specifies what hostname must appear in the request's Host: header to
match this virtual host. For the default virtual host (this file) this
value is not decisive as it is used as a last resort host regardless.
However, you must set it for any further virtual host explicitly.
#ServerName www.example.com
ServerName enzoarrue.com.br
ServerAlias www.enzoarrue.com.br
ServerAdmin webmaster@enzoarrue.com.br
DocumentRoot /var/www/enzoarrue.com.br/public_html
Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
error, crit, alert, emerg.
It is also possible to configure the loglevel for particular
modules, e.g.
#LogLevel info ssl:warn

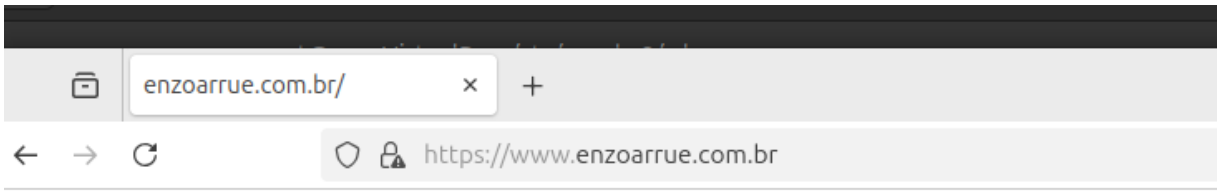




Servidor Apache...







Servidor Apache...

```
root@serv-VirtualBox:/etc/apache2/ssl# tail -f /var/log/apache2/acess.log
tail: não foi possível abrir '/var/log/apache2/acess.log' para leitura: Arquivo ou diretório inexistente
tail: nenhum aquivo restante
root@serv-VirtualBox:/etc/apache2/ssl# tail -f /var/log/apache2/access.log
192.168.56.10 - - [20/May/2025:11:21:47 -0300] "GET / HTTP/1.1" 200 310 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:
138.0) Gecko/20100101 Firefox/138.0"
192.168.56.10 - - [20/May/2025:11:21:47 -0300] "GET /favicon.ico HTTP/1.1" 404 491 "http://192.168.56.10/" "Mozilla/5.0
(X11; Ubuntu; Linux x86_64; rv:138.0) Gecko/20100101 Firefox/138.0"
192.168.56.10 - - [20/May/2025:11:22:00 -0300] "GET / HTTP/1.1" 200 310 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:
138.0) Gecko/20100101 Firefox/138.0"
192.168.56.10 - - [20/May/2025:11:22:00 -0300] "GET /favicon.ico HTTP/1.1" 404 498 "http://www.enzoarrue.com.br/" "Mozil
la/5.0 (X11; Ubuntu; Linux x86_64; rv:138.0) Gecko/20100101 Firefox/138.0"
192.168.56.10 - - [20/May/2025:11:22:35 -0300] "GET / HTTP/1.1" 200 2122 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv
:138.0) Gecko/20100101 Firefox/138.0"
192.168.56.10 - - [20/May/2025:11:22:35 -0300] "GET /favicon.ico HTTP/1.1" 404 517 "https://enzoarrue.com.br/" "Mozilla/
5.0 (X11; Ubuntu; Linux x86_64; rv:138.0) Gecko/20100101 Firefox/138.0"
192.168.56.10 - - [20/May/2025:12:14:46 -0300] "GET / HTTP/1.1" 200 2122 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv
:138.0) Gecko/20100101 Firefox/138.0"
192.168.56.10 - - [20/May/2025:12:14:46 -0300] "GET /favicon.ico HTTP/1.1" 404 521 "https://www.enzoarrue.com.br/" "Mozi
lla/5.0 (X11; Ubuntu; Linux x86_64; rv:138.0) Gecko/20100101 Firefox/138.0"
192.168.56.10 - - [20/May/2025:12:18:15 -0300] "GET / HTTP/1.1" 200 310 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:
138.0) Gecko/20100101 Firefox/138.0"
192.168.56.10 - - [20/May/2025:12:18:15 -0300] "GET /favicon.ico HTTP/1.1" 404 498 "http://www.enzoarrue.com.br/" "Mozil
la/5.0 (X11; Ubuntu; Linux x86_64; rv:138.0) Gecko/20100101 Firefox/138.0"
```

```
oot@serv-VirtualBox:/etc/apache2/ssl# cat server.csr
----BEGIN CERTIFICATE REQUEST-----
IIDCTCCAfECAQAwgZkxCzAJBgNVBAYTAkJSMQswCQYDVQQIDAJTUDEbMBkGA1UE
wwSU2FvIENhZXRhbm8gZG8gU3VsMRIwEAYDVQQKDAlFbnpvYXJydWUxEjAQBgNV
AsMCUVuem9hcnJ1ZTENMAsGA1UEAwwEZW56bzEpMCcGCSqGSIb3DQEJARYaZW56
2FycnVlQGVuem9hcnJ1ZS5jb20uYnIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
gEKAoIBAQDFq5jN4xGS11hkzm0OMgicGZEFW2tXBW2y/3Mg9VpVHR1AeOR4whjZ
rT2eWynqeK7paGrhBiteohimALyCCrkhdPbNz/Vdda0bpG4UJC1XP/7rRdMEIwv
oWmH2c3+I838LJ62+JDDEYo3c9V7x+RBWLDMMpouvFnuRkS3cfdu/CtzBLDJUEe
zyJ9sc2pcxODilNAj++PVWLhhfgg3BW/IVec6hLt0RLowHtKEV8C5Jr7vzqmF01
v3LdfTAaJiDVt9qayIFkVlqaH8HxSsDnSYDI0BPj/mmyMRuBuYk+dr8qyCqoFs1
UyzueagfDIKKFt26RSKQIE0jiHWqntBAgMBAAGgKjATBgkqhkiG9w0BCQIxBgwE
W56bzATBgkqhkiG9w0BCQcxBgwEZW56bzANBgkqhkiG9w0BAQsFAAOCAQEAuMPC
dSP0ap+ebFJdS+Nos64DP2j+Ew3K6wpuhHnW7wY5Shl8p30GI0il7Q1FwUPlOQu
potR3UkfdNWiQW8r9DhR8bJfvyJncPYz7nubU5LgiQshUyJ0nyVbubc1+kczc8w
h1OeChKLpZC7wgi+EdNryRTiFAq1PklaT3uMN/njk5JAf2kymEzmosFKJ6rtkF4
yIPQwJscq0FvTf8tq+8q99k0XmMkcvs3QkqifRgGGFIs4IaysI0daH4AvOMrCgk
LvlhEPrmJ0lRHClywzqcE+xSW9XEy3YwNBTd/AhIh8PHwzKGxgvey2pFd8RDRZF
YoPeU/B3gogg/JSbg==
----END CERTIFICATE REQUEST-----
```

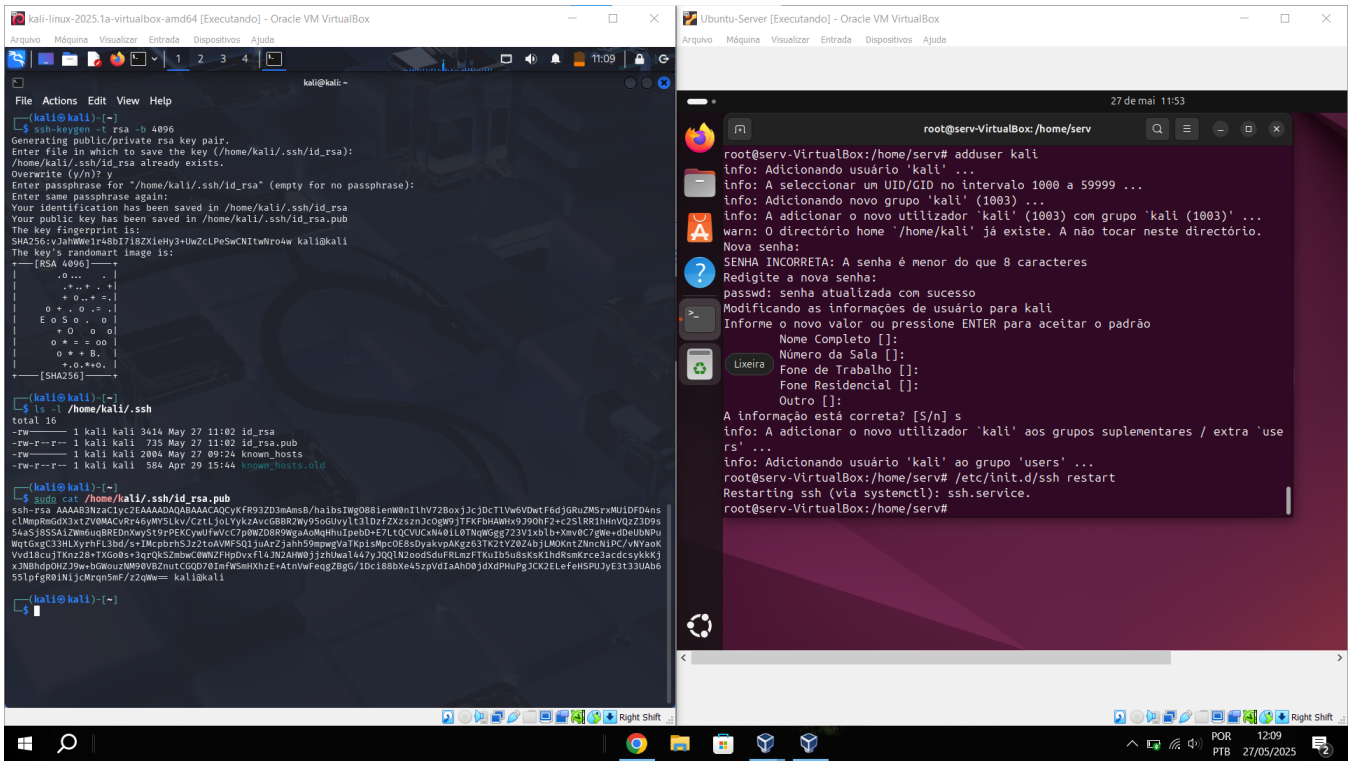
5. Configurar as máquinas (Windows e/ou Linux) e o servidor SSH.

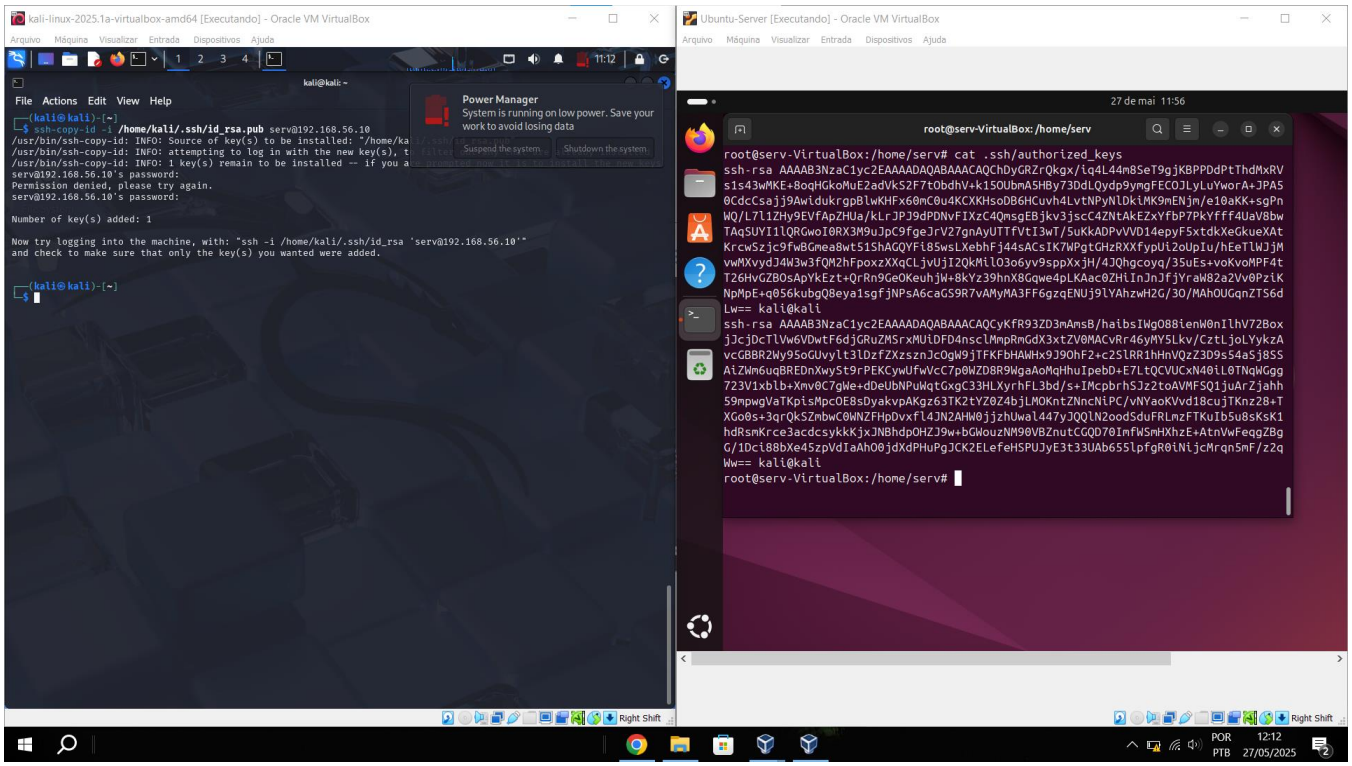
5.1. Configurar o servidor SSH/SFTP considerando as boas práticas de segurança (portas, par de chaves, entre outros).

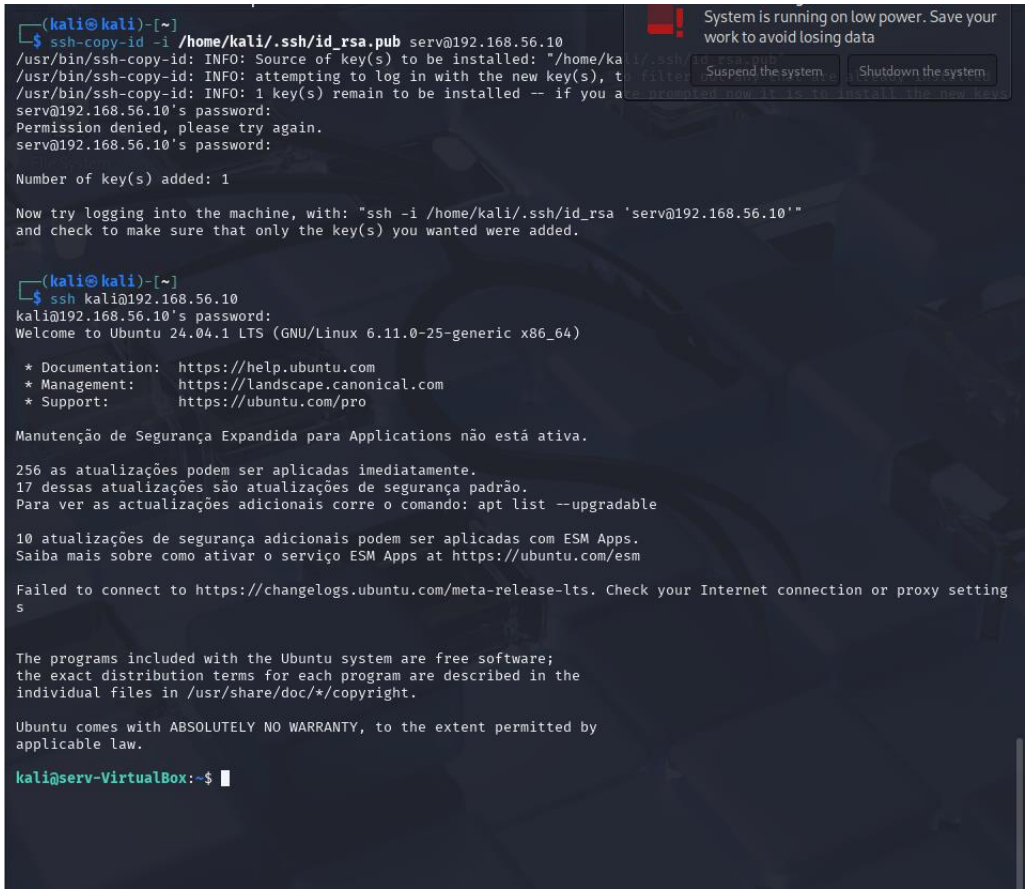
5.2. Testar na(s) máquina(s) cliente(s) usando o cliente ssh e sftp.

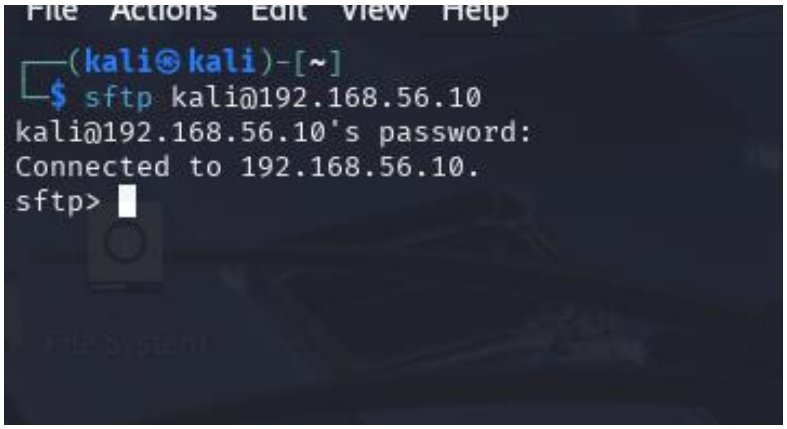
5.3. Realizar a captura SSH com o Wireshark (Kali).

SSH:


kali-linux-2025.1a-virtualbox-amd64 [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
/home/kali/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase for "/home/kali/.ssh/id_rsa" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:vJahWWe1r48bI7i8ZXieHy3+UwZcLPeSwCNItwNro4w kali@kali
The key's randomart image is:
+---[RSA 4096]----+
| .o...   . |
| .+..+ . +|
| + o..+ =.|
| o + . o .= .|
| E o S o . o |
| + O   o o|
| o + = o o |
| o * + B. |
| +.o.*+o. |
+----[SHA256]-----+
(kali㉿kali)-[~]
$ ls -l /home/kali/.ssh
total 16
-rw------- 1 kali kali 3414 May 27 11:02 id_rsa
-rw-r--r-- 1 kali kali 735 May 27 11:02 id_rsa.pub
-rw------- 1 kali kali 2004 May 27 09:24 known_hosts
-rw-r--r-- 1 kali kali 584 Apr 29 15:44 known_hosts.old
(kali㉿kali)-[~]
$ sudo cat /home/kali/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCyKfR93ZD3mAmsB/haibsIWgO88ienW0nIlhV72BoxjJcjDcTlVw6VDwtF6djGRuZMSrxMUiDFD4ns
clMmpRmGdX3xtZV0MACvRr46yMY5Lkv/CztLjoLYykzAvcGBBR2Wy95oGUvylt3lDzFZXzsznJcOgW9jTFKFbHAWHx9J9OhF2+c2SlRR1hHnVQzZ3D9s
54aSj8SSAiZWm6uqBREDnXwySt9rPEKCywUfwVcC7p0WZD8R9WgaAoMqHhuIpebD+E7LtQCVUCxN40iL0TNqWGgg723V1xblb+Xmv0C7gWe+dDeUbNPu
WqtGxgC33HLXyrhFL3bd/s+IMcpbrhSJz2toAVMFSQ1juArZjahh59mpwgVaTKpisMpcOE8sDyakvpAKgz63TK2tYZ0Z4bjLMOKntZNncNiPC/vNYaoK
Vvd18cujTKnz28+TXGo0s+3qrQkSZmbwC0WNZFHpDvxfl4JN2AHW0jjzhUwal447yJQQlN2ood5duFRLmzFTKuIb5u8sKsK1hdRsmKrce3acdcsykkKjx
xJNBhdpOHZJ9w+bGWouzNM90VBZnutCGQD70ImfWSmHXhzE+AtnVwFeqgZBgG/1Dci88bXe45zpVdIaAhO0jdXdPHuPgJCK2ELefeHSPUJyE3t33UAb6
55lpfgR0iNijcMrqn5mF/z2qWw== kali@kali
(kali㉿kali)-[~]
$
Ubuntu-Server [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
27 de mai 11:53
root@serv-VirtualBox: /home/serv
root@serv-VirtualBox:/home/serv# adduser kali
info: Adicionando usuário 'kali' ...
info: A seleccionar um UID/GID no intervalo 1000 a 59999 ...
info: Adicionando novo grupo 'kali' (1003) ...
info: A adicionar o novo utilizador `kali' (1003) com grupo `kali (1003)' ...
warn: O directório home `/home/kali' já existe. A não tocar neste directório.
Nova senha:
SENHA INCORRETA: A senha é menor do que 8 caracteres
Redigite a nova senha:
passwd: senha atualizada com sucesso
Modificando as informações de usuário para kali
Informe o novo valor ou pressione ENTER para aceitar o padrão
Nome Completo []:
Número da Sala []:
Fone de Trabalho []:
Fone Residencial []:
Outro []:
A informação está correta? [S/n] s
info: A adicionar o novo utilizador `kali' aos grupos suplementares / extra `users' ...
info: Adicionando usuário 'kali' ao grupo 'users' ...
root@serv-VirtualBox:/home/serv# /etc/init.d/ssh restart
Restarting ssh (via systemctl): ssh.service.
root@serv-VirtualBox:/home/serv#
Lixeira
Right Shift
POR PTB 12:09 27/05/2025


kali-linux-2025.1a-virtualbox-amd64 [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ssh-copy-id -i /home/kali/.ssh/id_rsa.pub serv@192.168.56.10
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/ka
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), t
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you a
serv@192.168.56.10's password:
Permission denied, please try again.
serv@192.168.56.10's password:
Number of key(s) added: 1
Now try logging into the machine, with: "ssh -i /home/kali/.ssh/id_rsa 'serv@192.168.56.10'"
and check to make sure that only the key(s) you wanted were added.
(kali㉿kali)-[~]
$
Power Manager
System is running on low power. Save your work to avoid losing data
Suspend the system
Shutdown the system
Ubuntu-Server [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
27 de mai 11:56
root@serv-VirtualBox: /home/serv
root@serv-VirtualBox:/home/serv# cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQChDyGRZrQkgx/iq4L44m8SeT9gjKBPPDdPtThdMxRV
s1s43wMKE+8oqHGkoMuE2adVkS2F7tObdhV+k1SOUbmA5HBy73DdLQydp9ymgFECOJLyLuYworA+JPA5
0CdcCsajj9AwidukrgpBlwKHFx60mC0u4KCXKHsoDB6HCuvh4LvtNPyNlDkiMK9mENjm/e10aKK+sgPn
WQ/L7l1ZHy9EVfApZHUa/kLrJPJ9dPDNvFIXzC4QmsgEBjkv3jscC4ZNtAkEZxYfbP7PkYfff4UaV8bw
TAqSUYI1QRGwoI0RX3M9uJpC9fgeJrV27gnAyUTTfVtI3wT/5uKkADPvVVD14epyF5xtdkXeGkueXAt
KrcwSzjc9fwBGmea8wt51ShAGQYFi85wsLXebhFj44sACsIK7WPgtGHzRXXfypUi2oUpIu/hEeTlWJjM
vwMXvydJ4W3w3fQM2hFpoxzXXqCLjvUjI2QkMilO3o6yv9sppXxjH/4JQhgcoyq/35uEs+voKvoMPF4t
T26HvGZBOsApYkEzt+QrRn9GeOKeuhjW+8kYz39hnX8Gqwe4pLKAac0ZHiInJnJfjYraW82a2Vv0PziK
NpMpE+q056kubgQ8eya1sgfjNPsA6caGS9R7vAMyMA3FF6gzqENUj9lYAhzwH2G/3O/MAhOUGqnZTS6d
Lw== kali@kali
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCyKfR93ZD3mAmsB/haibsIWgO88ienW0nIlhV72Box
jJcjDcTlVw6VDwtF6djGRuZMSrxMUiDFD4nsclMmpRmGdX3xtZV0MACvRr46yMY5Lkv/CztLjoLYykzA
vcGBBR2Wy95oGUvylt3lDzfZXzsznJcOgW9jTFKFbHAWHx9J9OhF2+c2SlRR1hHnVQzZ3D9s54aSj8SS
AiZWm6uqBREDnXwySt9rPEKCywUfwVcC7p0WZD8R9WgaAoMqHhuIpebD+E7LtQCVUCxN40iL0TNqWGgg
723V1xblb+Xmv0C7gWe+dDeUbNPuWqtGxgC33HLXyrhFL3bd/s+IMcpbrhSJz2toAVMFSQ1juArZjahh
59mpwgVaTKpisMpcOE8sDyakvpAKgz63TK2tYZ0Z4bjLMOKntZNncNiPC/vNYaoKVvd18cujTKnz28+T
XGo0s+3qrQkSZmbwC0WNZFHpDvxfl4JN2AHW0jjzhUwal447yJQQlN2ood5duFRLmzFTKuIb5u8sKsK1
hdRsmKrce3acdcsykkKjxJNBhdpOHZJ9w+bGWouzNM90VBZnutCGQD70ImfWSmHXhzE+AtnVwFeqgZBg
G/1Dci88bXe45zpVdIaAhO0jdXdPHuPgJCK2ELefeHSPUJyE3t33UAb655lpfgR0iNijcMrqn5mF/z2q
Ww== kali@kali
root@serv-VirtualBox:/home/serv#
Right Shift
POR PTB 12:12 27/05/2025


System is running on low power. Save your work to avoid losing data
Suspend the system
Shutdown the system
(kali㉿kali)-[~]
$ ssh-copy-id -i /home/kali/.ssh/id_rsa.pub serv@192.168.56.10
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/kali/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
serv@192.168.56.10's password:
Permission denied, please try again.
serv@192.168.56.10's password:
Number of key(s) added: 1
Now try logging into the machine, with: "ssh -i /home/kali/.ssh/id_rsa 'serv@192.168.56.10'"
and check to make sure that only the key(s) you wanted were added.
(kali㉿kali)-[~]
$ ssh kali@192.168.56.10
kali@192.168.56.10's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.0-25-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
Manutenção de Segurança Expandida para Applications não está ativa.
256 as atualizações podem ser aplicadas imediatamente.
17 dessas atualizações são atualizações de segurança padrão.
Para ver as actualizações adicionais corre o comando: apt list --upgradable
10 atualizações de segurança adicionais podem ser aplicadas com ESM Apps.
Saiba mais sobre como ativar o serviço ESM Apps at https://ubuntu.com/esm
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
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.
kali@serv-VirtualBox:~$


File Actions Edit View Help
(kali㉿kali)-[~]
$ sftp kali@192.168.56.10
kali@192.168.56.10's password:
Connected to 192.168.56.10.
sftp>