TOR:The Onion Router
CS471: Assignment 7

Abstract

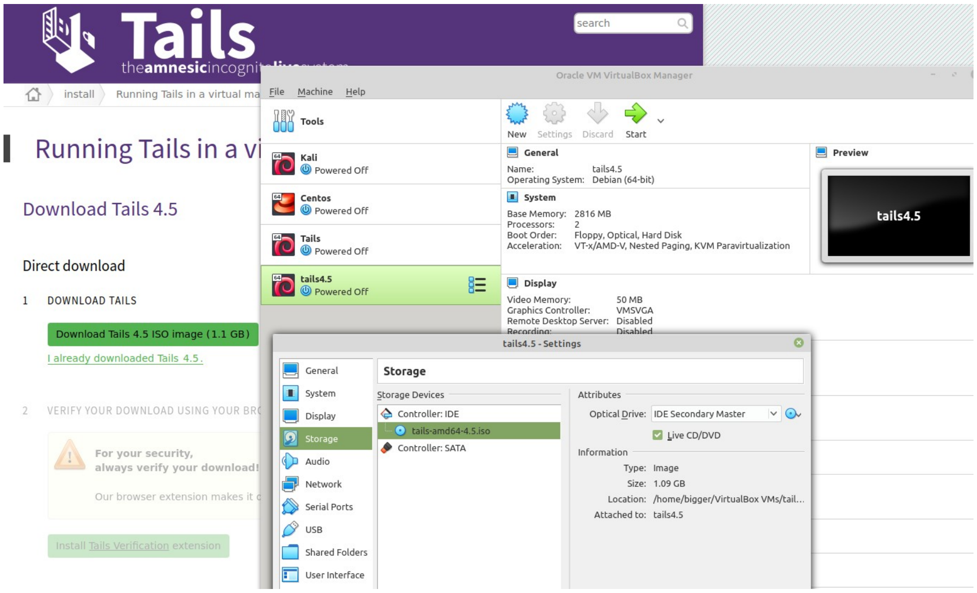
Use, analyze, and understand TOR and Tails.

Activity

Use the Tails operating system in Virtual Box to investigate Tor, the onion router. Download the iso file for the Tails OS here:

https://tails.boum.org/install/vm-download/index.en.html

Add this to Virtual box with no hard drive. Add the Tails iso as a new optical drive in Virtual box. Select the option for ‘Live CD/DVD’.



General
Name: tails4.5
Operating System: Debian (64-bit)

System
Base Memory: 2816 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display
Video Memory: 50 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

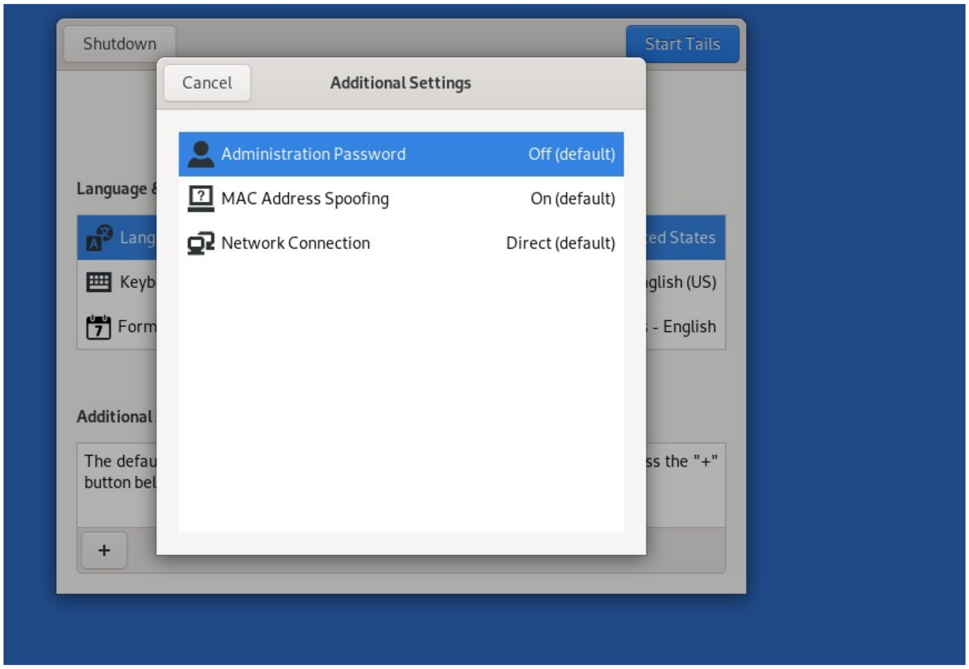
Storage

Storage Devices
Controller: IDE
tails-amd64-4.5.iso
Controller: SATA

Attributes
Optical Drive: IDE Secondary Master
☑ Live CD/DVD

Information
Type: Image
Size: 1.09 GB
Location: /home/bigger/VirtualBox VMs/tail...
Attached to: tails4.5

When starting Tails, be sure to set a sudo password. This is required for sudo.



Administration Password Off (default)

MAC Address Spoofing On (default)

Network Connection Direct (default)

After starting Tails, use tcpdump to capture all packets, as you have done in previous assignments. Be sure to save the output file in a Wireshark compatible format.

```
tcpdump -i any -s 65535 -w /home/amnesia/Desktop/packets.pcap
```

Now start the Tor browser and check if Tor is working by going here:

https://check.torproject.org/

Try using the DuckDuckGo search engine from inside the Tor network using an onion address. Try this from the Tor browser and the 'unsafe browser'. Try other sites, also.

https://3g2upl4pq6kufc4m.onion

Create a new file and encrypt the contents using symmetric encryption. Name this file secrets.txt. Share this file using OnionShare.

Last, stop the packet capture, save the capture file, fix the permissions, and save your screenshots. Transfer these files to your Kali VM. Email it, Dropbox it, save it to a thumbdrive, upload it to blackboard, or some other approach. This capture file will be needed for packet analysis and the screenshots are needed for your submission.

The capture file will be owned by root and may create permission problems. The following may help.

```
sudo chown amnesia:amnesia /home/amnesia/Desktop/packets.pcap
sudo chmod 777 /home/amnesia/Desktop/packets.pcap
```

Transfer the capture files to your Kali VM, open the capture in Wireshark. Begin your traffic analysis.

Compile your research and screenshots into a Word document. Present your findings, annotate your figures, and explain your methods and results.

Include a final summary that describes the Tor Onion Router in your own words. Describe the technology. What are the risks?

Conclusion

In addition to your conclusion, add the following:

- How can a does TOR improve security? Be specific!

- What tools does Tail offer to improve security?

- How is using TOR with Tails different than simply using TOR alone?

Deliverables

A document detailing the activity, including your process, methods, and results. This includes annotated screenshots. Clearly detail your work in a reproducible way following the provided sample format. Do not provide any image or text from another source without citation.

Submit all files created for this assignment. Attach these files to your submission. Do not zip, tar, or archive. The packet capture files should only include the requested files; these should be fairly small files.

Additionally, submit a single text file with all of the commands used for this assignment. One command per line. This should be complete and organized in order of use.

Submit your original work including screenshots, packet capture file, and your analysis to Canvas before the posted deadline.