

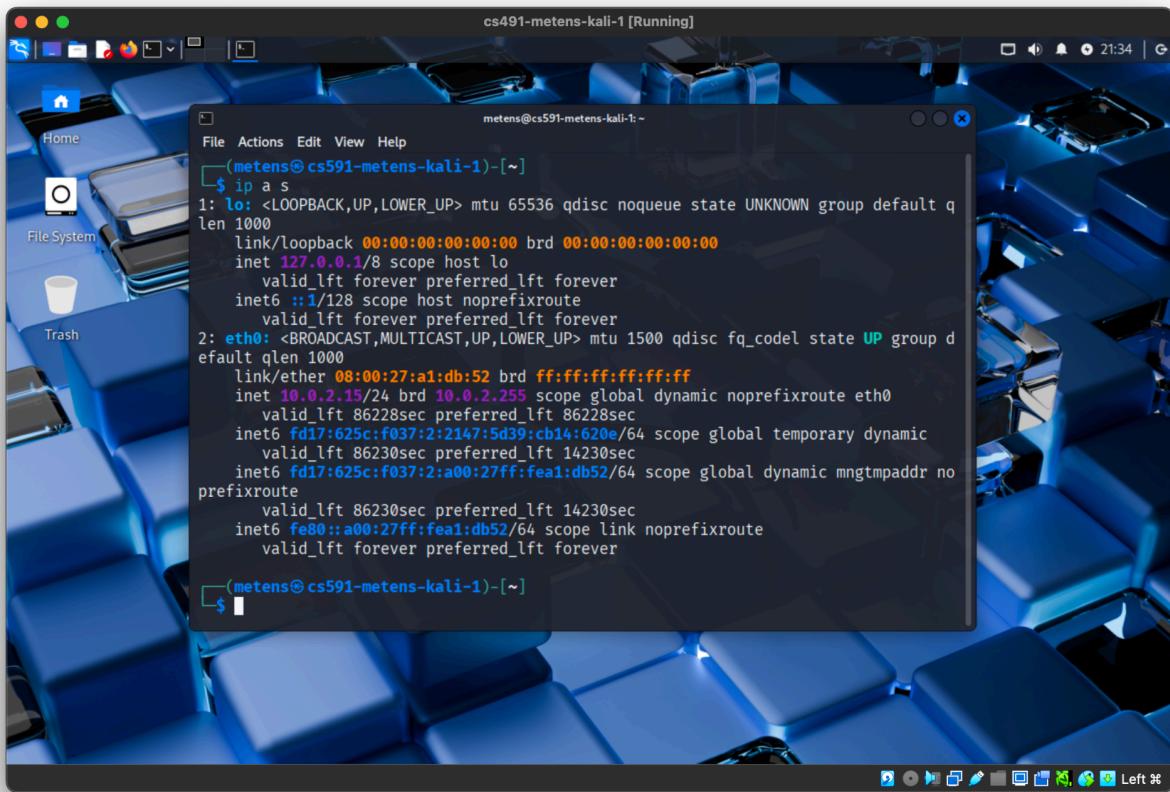
Lab 1

By: Nathan Metens (metens@pdx.edu)

Task 1: Building a Virtual VM running Kali Linux	1
Task 2: Creating the TryHackMe Account	3
Task 3: TryHackMe OpenVPN	4
Task 4: TryHackMe Security Principle	4
Conclusion	5

Task 1: Building a Virtual VM running Kali Linux

Step 32) Using `ip a s`

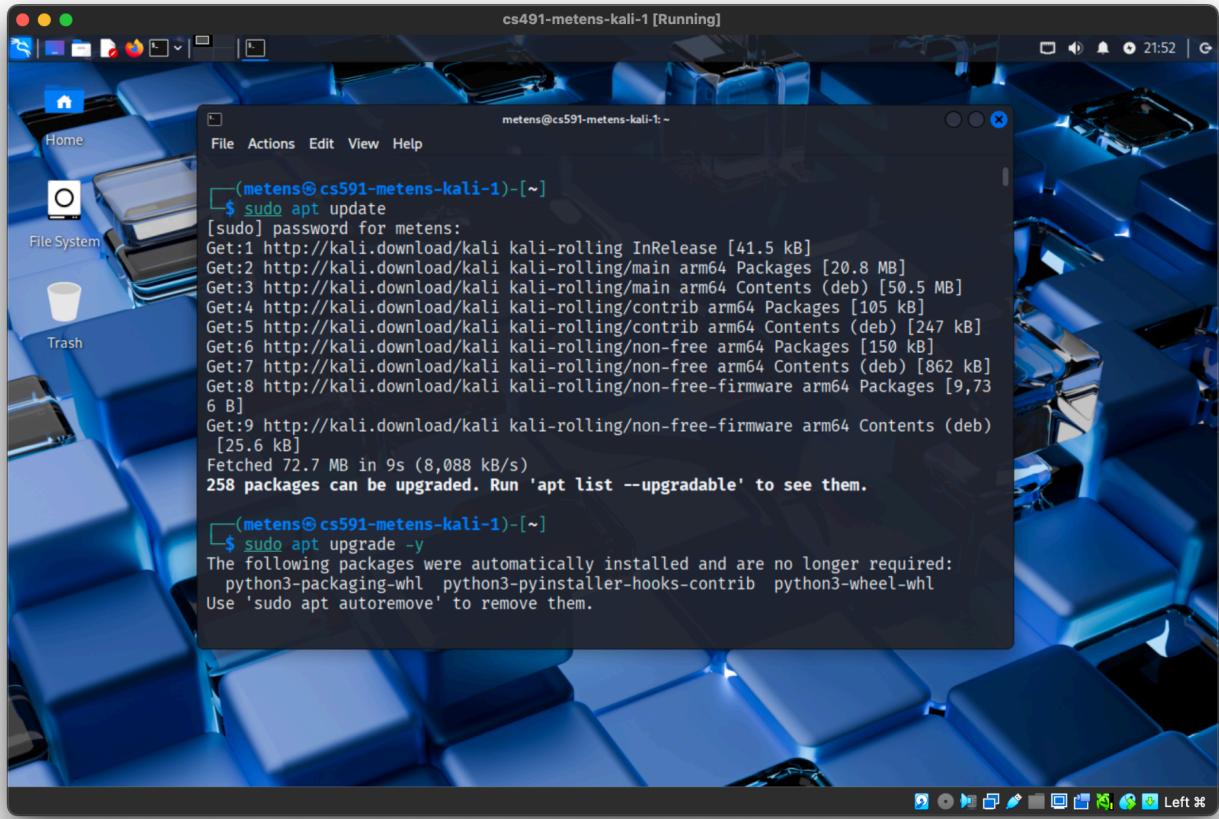


The screenshot shows a Kali Linux desktop environment. A terminal window titled "metens@cs591-metens-kali-1 [Running]" is open, displaying the output of the command "ip a s". The terminal shows two network interfaces: "lo" (loopback) and "eth0" (Ethernet). The "lo" interface has an IP address of 127.0.0.1/8. The "eth0" interface has an IP address of 10.0.2.15/24 and is connected to a bridge named brd. The terminal prompt is metens@cs591-metens-kali-1: ~

```
metens@cs591-metens-kali-1: ~
$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a1:db:52 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 86228sec preferred_lft 86228sec
    inet6 fd17:625c:f037:2:2147:5d39:cb14:620e/64 scope global temporary dynamic
        valid_lft 86230sec preferred_lft 14230sec
    inet6 fd17:625c:f037:2:a00:27ff:fea1:db52/64 scope global dynamic mngtmpaddr no
        valid_lft 86230sec preferred_lft 14230sec
    inet6 fe80::a00:27ff:fea1:db52/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
$
```

After running `ip a s`, I was curious about its meaning, so I looked it up and found that it means "ip address show". I see `lo` and `eth0`. `lo` seems to be the loopback localhost (127.0.0.1), which is useful for testing local websites before deployment. And `eth0` seems to be the Ethernet broadcast, whatever that means. Good to know the basics.

Step 33) Updating and Upgrading

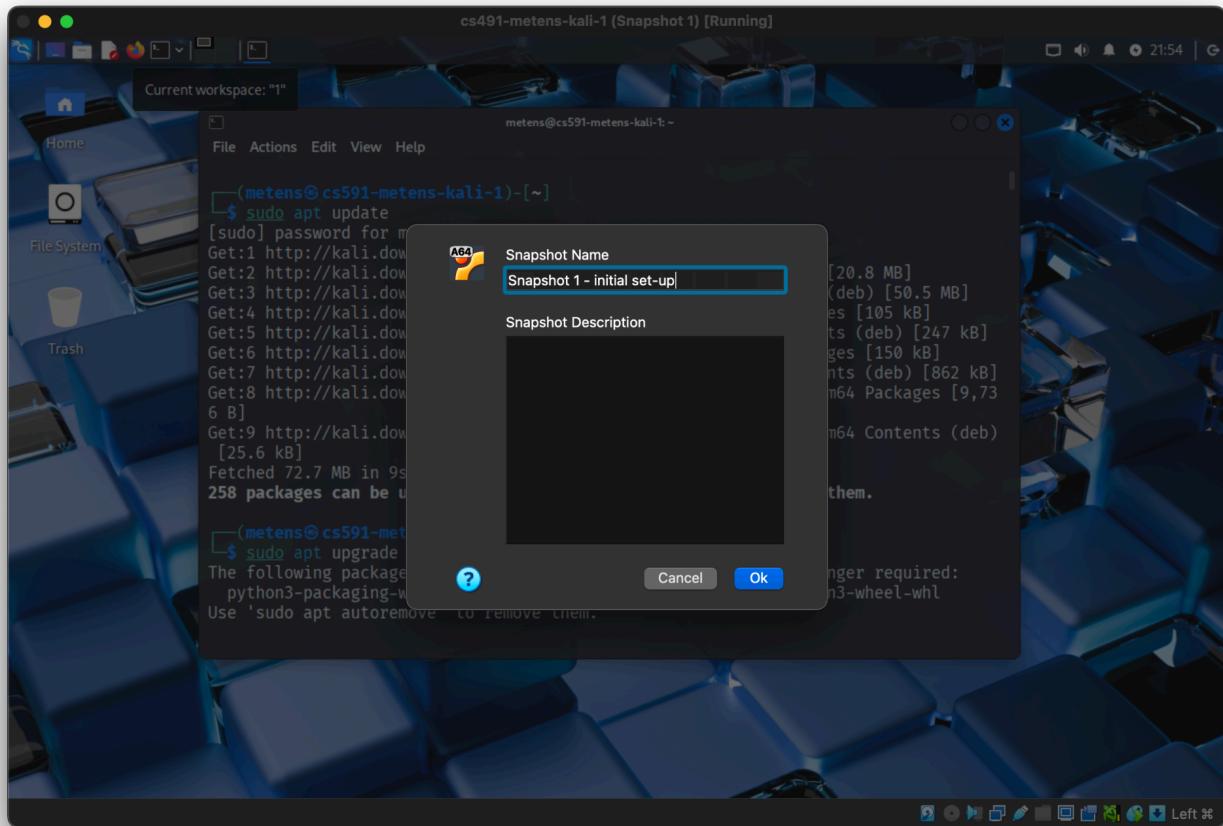


```
(metens@cs591-metens-kali-1:~)
$ sudo apt update
[sudo] password for metens:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main arm64 Packages [20.8 MB]
Get:3 http://kali.download/kali kali-rolling/main arm64 Contents (deb) [50.5 MB]
Get:4 http://kali.download/kali kali-rolling/contrib arm64 Packages [105 kB]
Get:5 http://kali.download/kali kali-rolling/contrib arm64 Contents (deb) [247 kB]
Get:6 http://kali.download/kali kali-rolling/non-free arm64 Packages [150 kB]
Get:7 http://kali.download/kali kali-rolling/non-free arm64 Contents (deb) [862 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware arm64 Packages [9,736 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware arm64 Contents (deb) [25.6 kB]
Fetched 72.7 MB in 9s (8,088 kB/s)
258 packages can be upgraded. Run 'apt list --upgradable' to see them.

(metens@cs591-metens-kali-1:~)
$ sudo apt upgrade -y
The following packages were automatically installed and are no longer required:
  python3-packaging-whl  python3-pyinstaller-hooks-contrib  python3-wheel-whl
Use 'sudo apt autoremove' to remove them.
```

Here I used `sudo`, which means “superuser do”. Running a command as root so that the entire VM updates can be useful. `apt` translates to Advanced Package Tool, which is useful for installing, updating, upgrading, and removing software packages. So, I updated and upgraded all the packages to their newest versions, sweet.

Step 35) snapshot



I followed all the steps perfectly in the notebook guide. Some parts took longer to load than others. I was able to watch a YouTube video while waiting. I went through this setup relatively quickly because I had already set up a Kali Linux VM for my other class (Network Security). I did have to take a second screenshot, however, because the steps didn't mention taking a screenshot of the initial snapshot. All in all, things are working, and I now have a VM for the rest of this term. Wahoo!

Task 2: Creating the TryHackMe Account

The screenshot shows the TryHackMe profile page for user 'metens'. At the top, there's a navigation bar with links for Dashboard, Learn, Compete, and Other. On the right, there's a 'Go Premium' button and a user icon. Below the navigation, the user's profile picture is displayed, followed by their name 'metens [0x1][NEOPHYTE]' and a small globe icon. To the right of the profile picture, there are four stats boxes: Rank (1622717), Badges (0), Streak (0), and Completed rooms (1). Below these stats, there are several tabs: Completed rooms (selected), Certificates, Skills matrix, Badges, Created rooms, Yearly activity, and Tickets. Under the 'Completed rooms' tab, there's a card for 'Offensive Security Intro', which is marked as 'Easy' and 'Free'. It includes a brief description: 'Hack your first website (legally in a safe environment) and experience an ethical hacker's job.' There are also 'Walkthrough' and 'Free' buttons.

I completed an intro room to understand how things worked on this site. It seems very helpful for learning new skills about security.

Task 3: TryHackMe OpenVPN

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'metens@cs591-metens-kali-1:~' and the content shows the user has connected successfully to a TryHackMe machine. The terminal output includes:

```
Connected Successfully!
https://tryhackme.com/room/openvpn
```

Below the terminal, there's a 'Room completed (100%)' message. A list of tasks is shown:

- Task 4: Connecting with Linux
- Task 5: Using TryHackMe without a VPN
- Task 6: Check you're connected

Instructions for Task 6 say: "You can check if you're connected to our network by a green tick next to connected on the Network Information table on the access page. Now verify that you're connected by deploying a machine and accessing its website. Deploy the machine on this task (it will take a few minutes to boot). Go to http://10.10.215.145 - can you see a website?"

A section titled "Answer the questions below" asks: "What is the flag displayed on the deployed machine's website?" The user has entered "flag{connection_verified}" into the input field, and a "Correct Answer" button is visible.

This one was fun because I was doing everything in the Kali VM I had just created.

Task 4: TryHackMe Security Principle

The screenshot shows the TryHackMe 'Learn' section for the 'Security Principles' room. At the top, there's a navigation bar with links for 'Dashboard', 'Learn' (which is active), 'Compete', and 'Other'. On the right, there are buttons for 'Go Premium', a notification bell, and user stats (2 rooms). Below the navigation is a sub-navigation bar with 'Learn > Security Principles'. The main content area features a large 'Security Principles' heading with a lock icon, followed by a brief description: 'Learn about the security triad and common security models and principles.' It indicates the room is 'Easy' and takes '90 min'. Below this are buttons for 'Show Split View', 'Help', 'Save Room', and 'Options'. A progress bar at the bottom shows 'Room progress (33%)'. To the right, a sidebar displays a calendar entry for 'Metens' on June 27, 2025, at 2:53 PM, with a note about 'Freebsd nathan p...'. Below the calendar is a link to 'Previous 7 Days'. At the bottom of the sidebar, there's a list of tasks: Task 1 (Introduction), Task 2 (CIA), Task 3 (DAD), Task 4 (Fundamental Concepts of Security Models), and Task 5 (Defence-in-Depth).

A good overview of CIA and DAD, two major opposites.

Conclusion

This assignment involved creating a Kali Linux VM, creating a TryHackMe account, and performing two TryHackMe room courses. I now have a solid foundation for the remainder of the term, as I performed each task without any major hiccups. I enjoyed the TryHackMe rooms I completed, as they were insightful and gave me a sense that I will be using them for some time to gain new hacking skills.