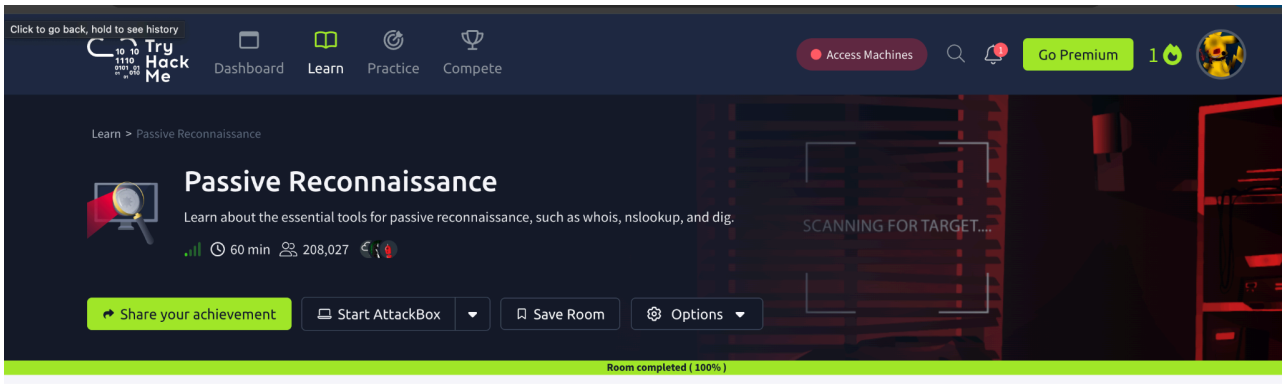
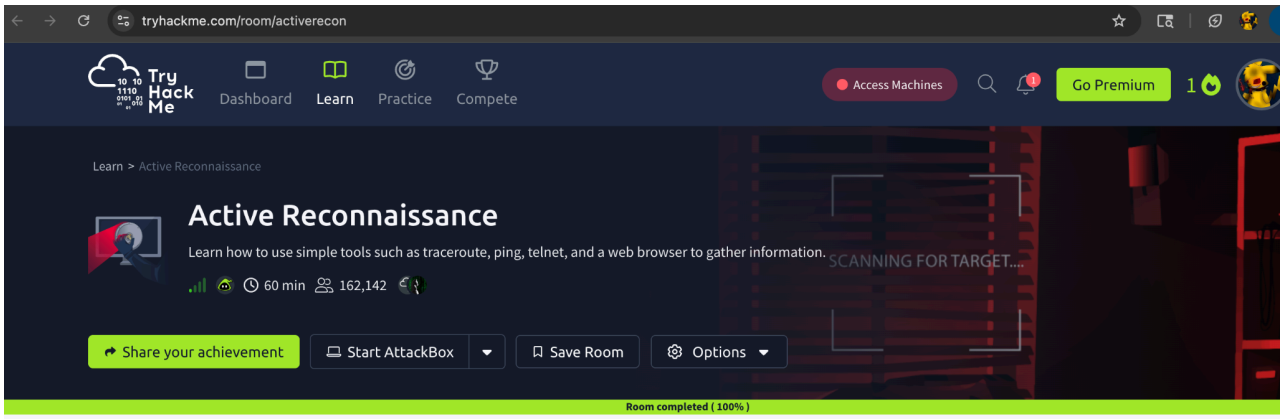
Scott Van Sise
CPS 593
Assignment 3

TryHackMe lab screenshots:

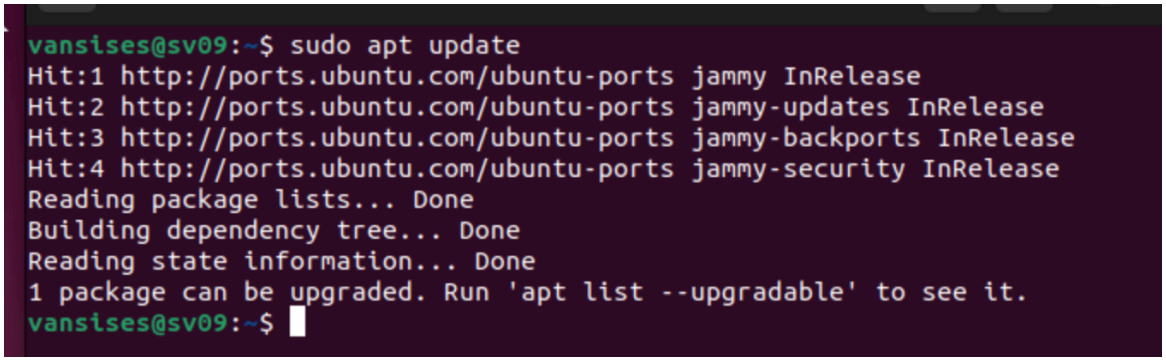
Passive Reconnaissance lab:



Active Reconnaissance lab:



In-Class Lab portion:



The first step I took was updating my VM before installing Lynis.

```
vansises@sv09:~$ sudo apt install lynis -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  menu
Suggested packages:
  apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu
  | kde-runtime | ktsuss
The following NEW packages will be installed:
  lynis menu
0 upgraded, 2 newly installed, 0 to remove and 1 not upgraded.
Need to get 565 kB of archives.
After this operation, 3,103 kB of additional disk space will be used.
Get:1 http://ports.ubuntu.com/ubuntu-ports jammy/universe arm64 lynis all 3.0.7-
```

The second step I took was downloading Lynis onto my VM in order to do audits and check on the status of my VM.

```
vansises@sv09:~$ lynis show version
3.0.7
vansises@sv09:~$
```

Once Lynis finished installing, I checked the version to be sure everything installed correctly.

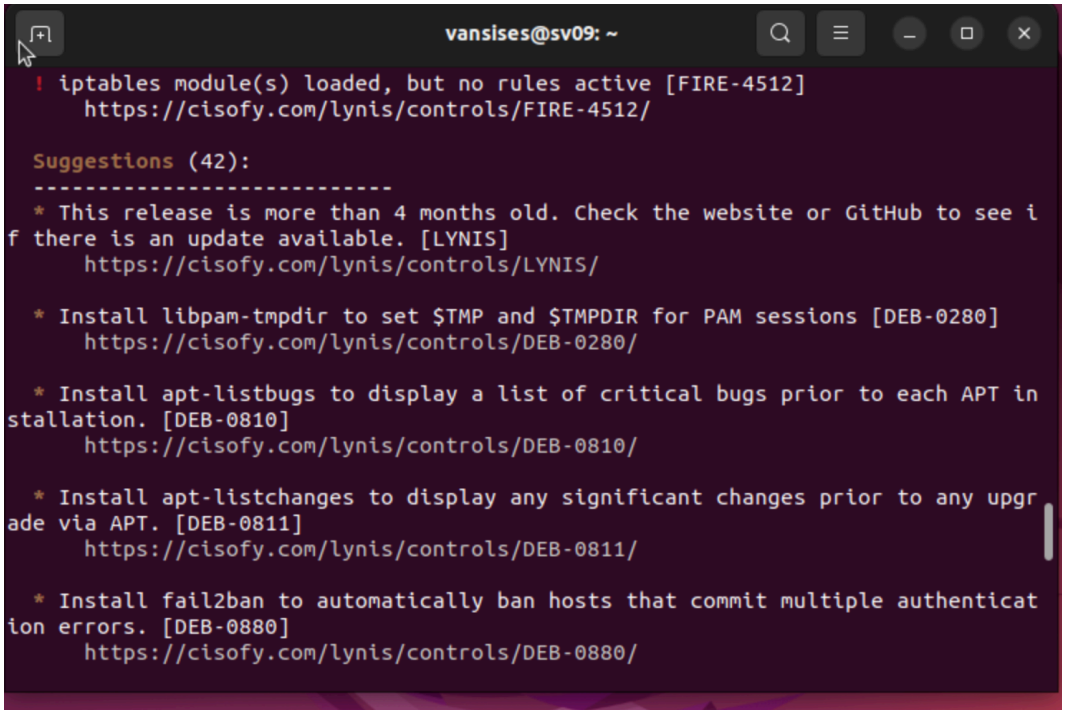
```
vansises@sv09:~$ sudo lynis audit system

[ Lynis 3.0.7 ]

################################################################################
```

When I finally confirmed that Lynis was good to go, I did a system audit on my VM.

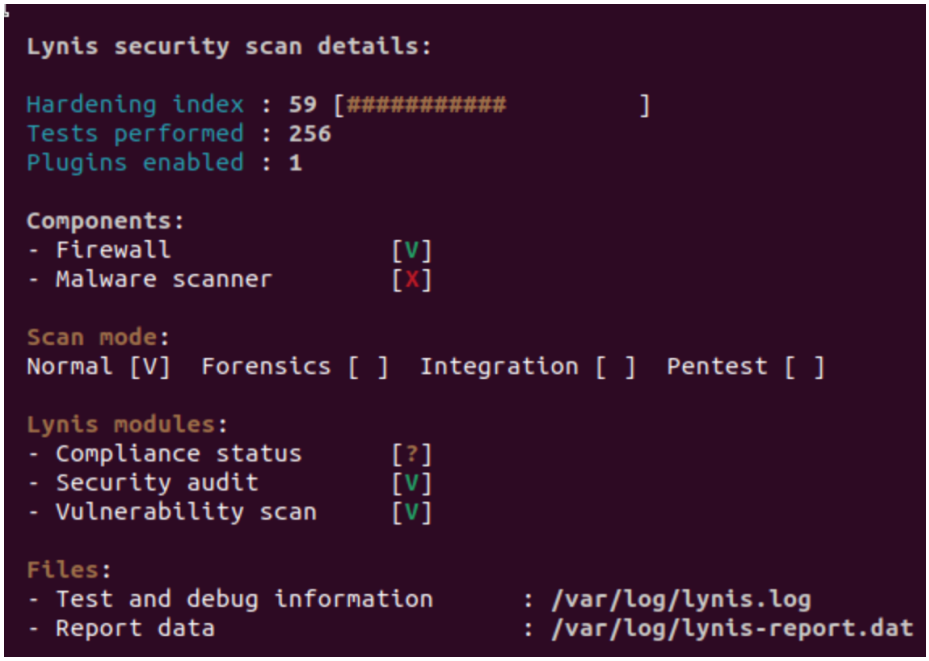
Results of the system audit:

```
[+] Printers and Spools
------------------------------------
  - Checking cups daemon                                    [ RUNNING ]
  - Checking CUPS configuration file                        [ OK ]
    - File permissions                                      [ WARNING ]
  - Checking CUPS addresses/sockets                         [ FOUND ]
  - Checking lp daemon                                      [ NOT RUNNING ]

[+] Software: e-mail and messaging
------------------------------------

[+] Software: firewalls
------------------------------------
  - Checking iptables kernel module                         [ FOUND ]
    - Checking iptables policies of chains                  [ FOUND ]
    - Checking for empty ruleset                            [ WARNING ]
    - Checking for unused rules                             [ OK ]
  - Checking host based firewall                            [ ACTIVE ]
```

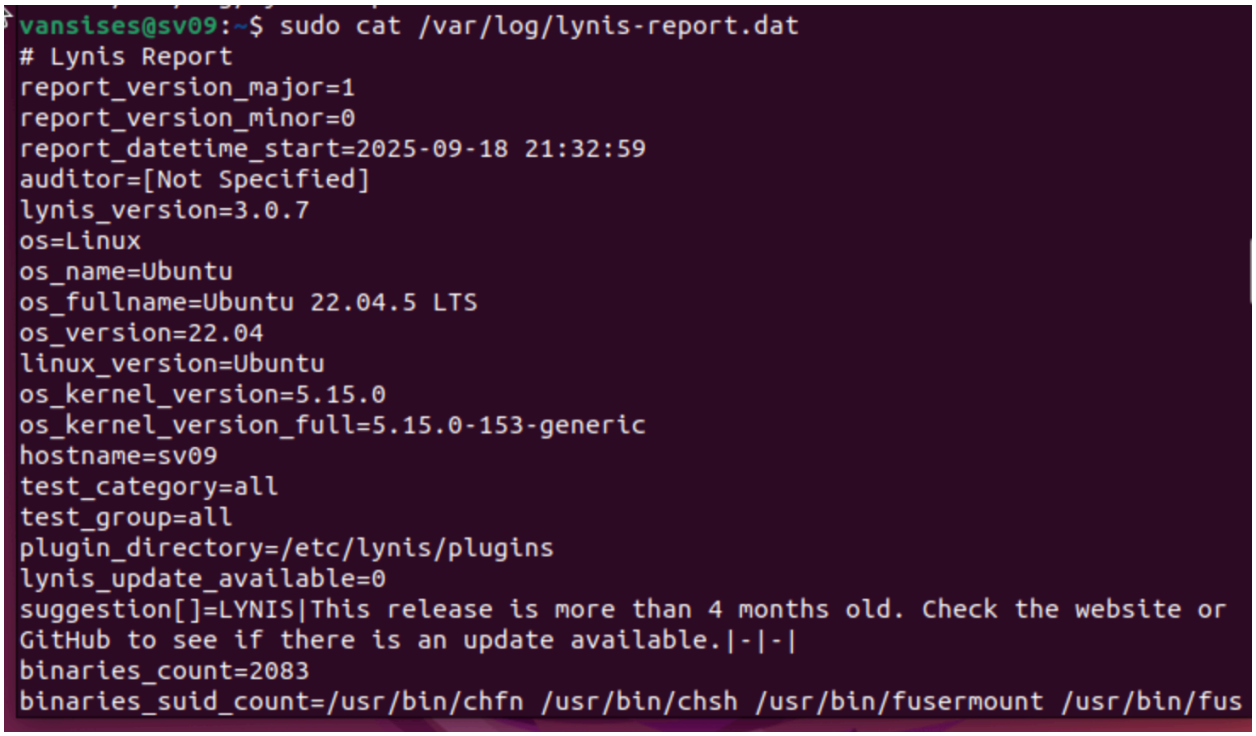
The first thing I did when the audit had completed was check for any warnings. I was able to find 2 warnings, one related to the file permissions for printers and spools with the other warning coming from my firewalls having an empty ruleset.



After I finished checking for warnings, I went to the suggestions section which is shown above. There were a total of 42 suggestions from things such as installing apt-listbugs as well as installing fail2ban onto my VM.



Towards the bottom of my audit I was also able to find the hardening index. My VM came out with a result of 59 for the hardening index. This number is meant to represent how secure you are against vulnerabilities by helping minimize the amount of places you can be attacked from as well as helping strengthen your systems settings.



Lastly, printed out the Lynis report data to see the results of the audit I had just completed.

Through this lab I was able to learn a lot about my VM as well as how prone it is to attacks. I did this through the use of Lynis' audit feature to check for vulnerabilities in my system. My system came out with a result of 59 for the hardening index score. This is a quite low score meaning my VM has a lot of vulnerabilities that need to be fixed. This audit also gave me warnings such as one related to the file permissions for printers and spools with the other warning coming from my firewalls having an empty ruleset. On top of the 2 warnings it also gave me 42 suggestions from things such as installing apt-listbugs as well as installing fail2ban onto my VM. If I took some of these steps I could strengthen the security against attackers on my VM. Overall, I learnt that the process of auditing is very important because it helps secure your system while also informing you on the parts that are not as secure and how to fix them.