

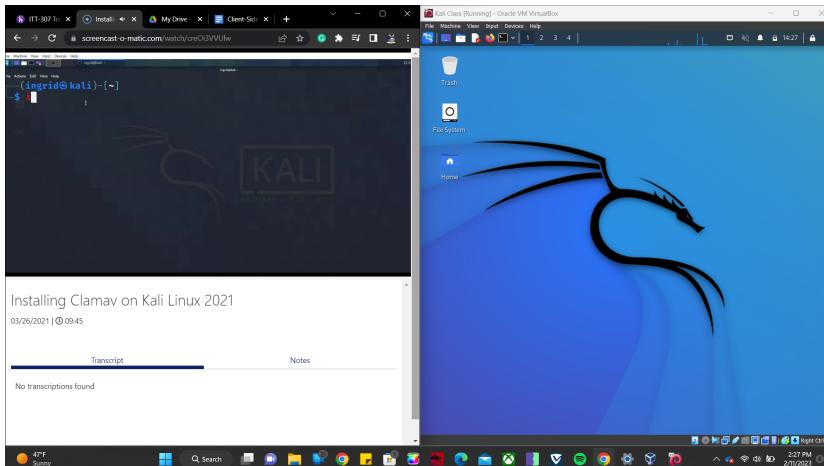
ITT-307 - Client-Side Attacks

Professor: Ingrid Gaviria
Course: ITT-307 Cybersecurity Foundations
Student: Liela Pressley
Date: 2/2/2023
Title: Client-Side Attacks

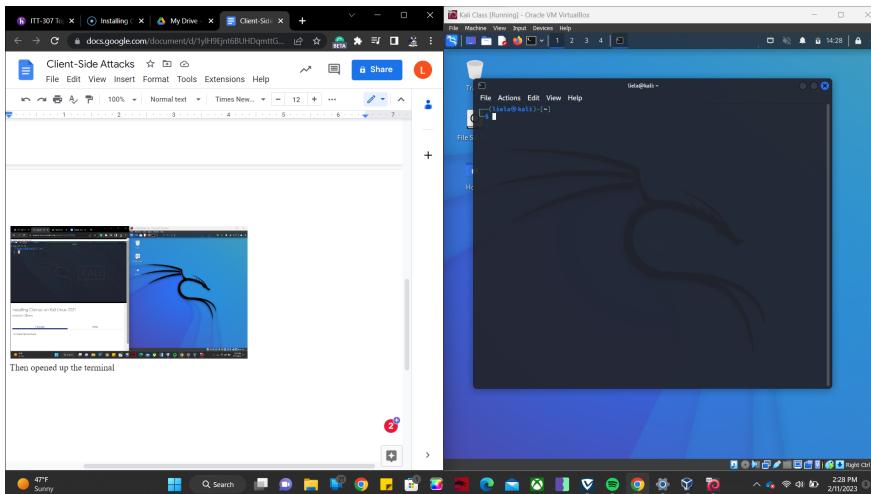
Overview: Antimalware is essential to have on any device, when not installed and enabled, the wrong download, URL, or phishing scam, can lead to your entire device being compromised, accounts being accessed, and much worse. I installed ClamAV to my Kali Linux system in VirtualBox then attempted to download malware but only one was successful in executing in my system, I tried to visit untrustworthy sites and download images and left my machine open to the Internet for over 24 hours. I enabled my antivirus scanner and it was able to detect the main malware file that I downloaded.

Details:

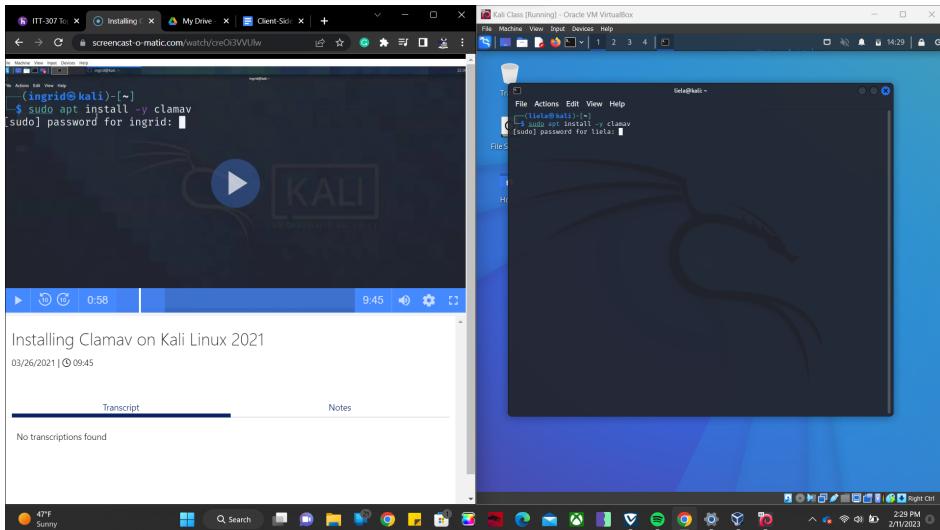
1. First I login into my Virtual Box Kali Linux



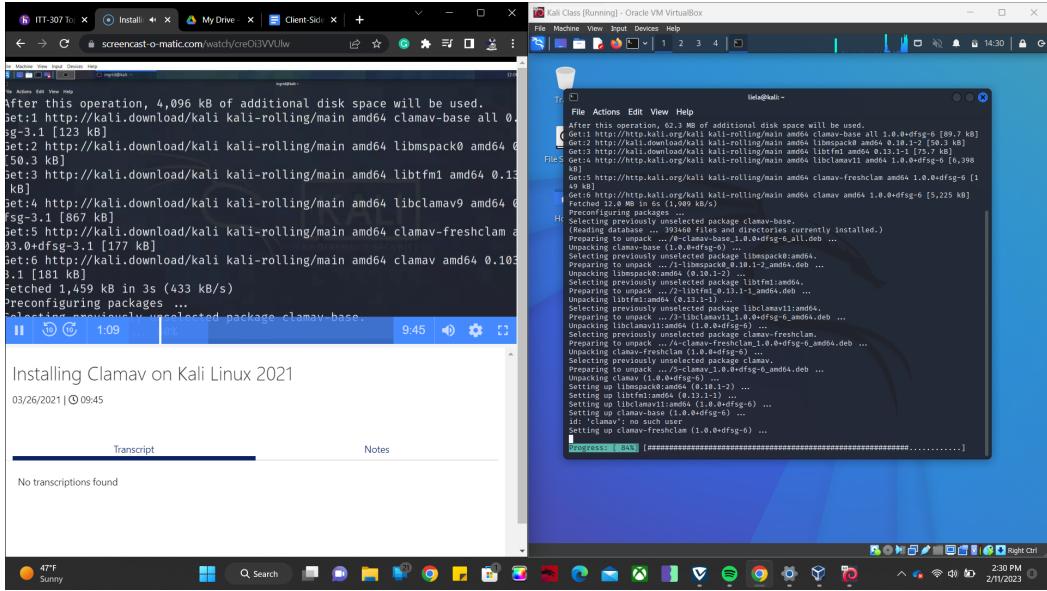
2. Then opened up the terminal



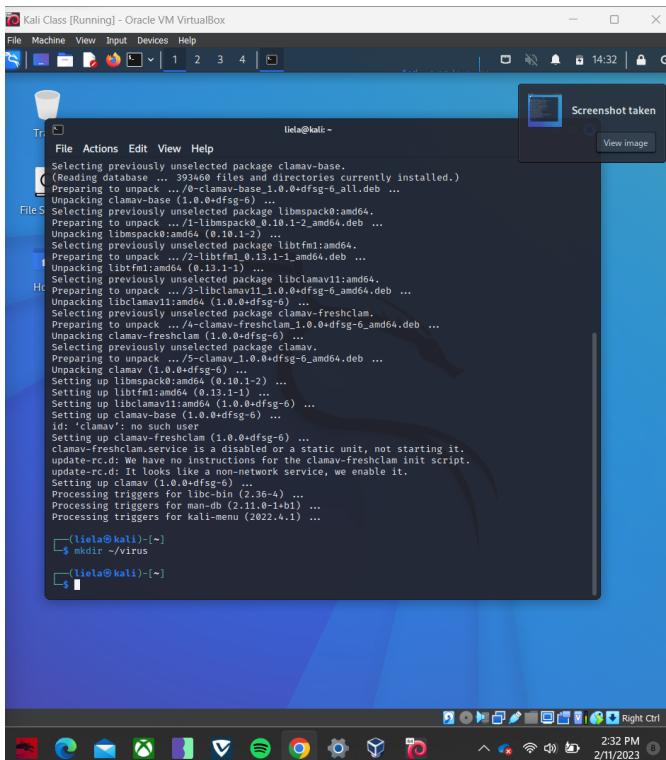
3. I then typed: sudo apt install -y clamav. It prompts for my login credentials.



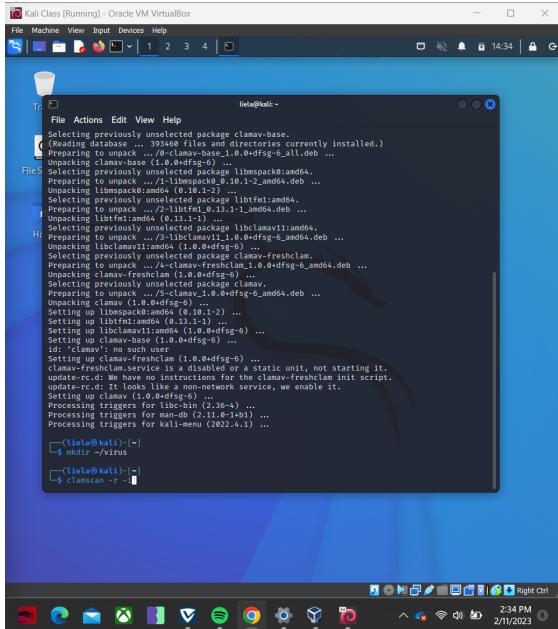
4. It then retrieves and processing and unpacks the packages from clamav



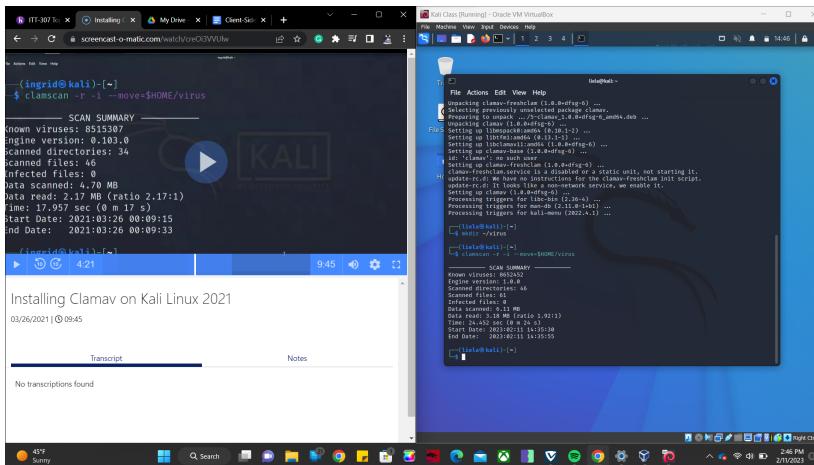
5. Then i made a directory titled Virus; mkdir ~/virus



6. Use clamscan to scan the directory and files only and move the detected files to a specific directory



7. After asking to view it shows the scan summary



8.

```
(liela㉿kali)-[~]
$ sudo apt install -y clamav-freshclam
Command 'sudo' not found, did you mean:
  command 'sup' from deb sup
  command 'sfdf' from deb graphviz
  command 'sudo' from deb sudo
  command 'sudo' from deb sudo-ldap
Try: sudo apt install <deb name>

(liela㉿kali)-[~]
$ sudo apt install -y clamav-freshclam
[sudo] password for liela:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
clamav-freshclam is already the newest version (1.0.0+dfsg-6).
clamav-freshclam set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1217 not upgraded.

(liela㉿kali)-[~]
$ sudo systemctl enabl clamav-freshclam
Unknown command verb enabl.

(liela㉿kali)-[~]
$ sudo systemctl enable clamavfreshclam
Failed to enable unit: Unit file clamavfreshclam.service does not exist.

(liela㉿kali)-[~]
$ sudo systemctl enable clamav-freshclam
Synchronizing state of clamav-freshclam.service with SysV service script with /lib/systemd/sys
temd-sysv-install.
Executing: /lib/systemd/system-sysv-install enable clamav-freshclam
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /lib/sy
stemd/system/clamav-freshclam.service.

(liela㉿kali)-[~]
```

```
(liela㉿kali)-[~]
$ sudo apt install -y clamav-freshclam
[sudo] password for liela:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
clamav-freshclam is already the newest version (1.0.0+dfsg-6).
clamav-freshclam set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1217 not upgraded.

(liela㉿kali)-[~]
$ sudo systemctl enable clamav-freshclam
Unknown command verb enabl.

(liela㉿kali)-[~]
$ sudo systemctl enable clamavfreshclam
Failed to enable unit: Unit file clamavfreshclam.service does not exist.

(liela㉿kali)-[~]
$ sudo systemctl enable clamav-freshclam
Synchronizing state of clamav-freshclam.service with SysV service script with /lib/systemd/sys
temd-sysv-install.
Executing: /lib/systemd/system-sysv-install enable clamav-freshclam
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /lib/sy
stemd/system/clamav-freshclam.service.

(liela㉿kali)-[~]
$ sudo systemctl stop clamav-freshclam
[sudo] password for liela:
Failed to stop clamav-freshclam.service: Unit clamav-freshclam.service not loaded.

(liela㉿kali)-[~]
$ sudo systemctl stop clamav-freshclam
[1]

[1]
```

9. Stop the scan

10. To have my antimalware run checks for 24 hours I entered: grep Checks /etc/clamav/freshclam.conf

Kali Class [Running] - Oracle VM VirtualBox

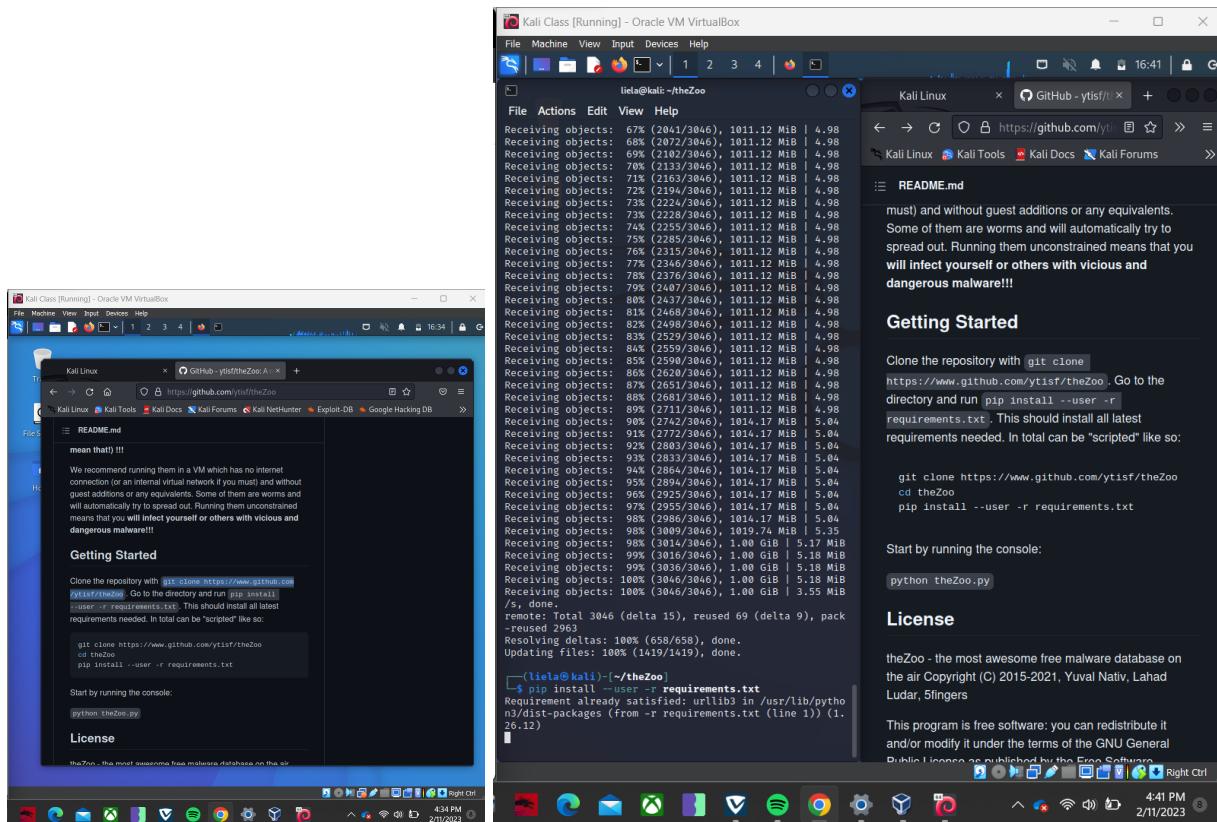
File Machine View Input Devices Help

File Actions Edit View Help

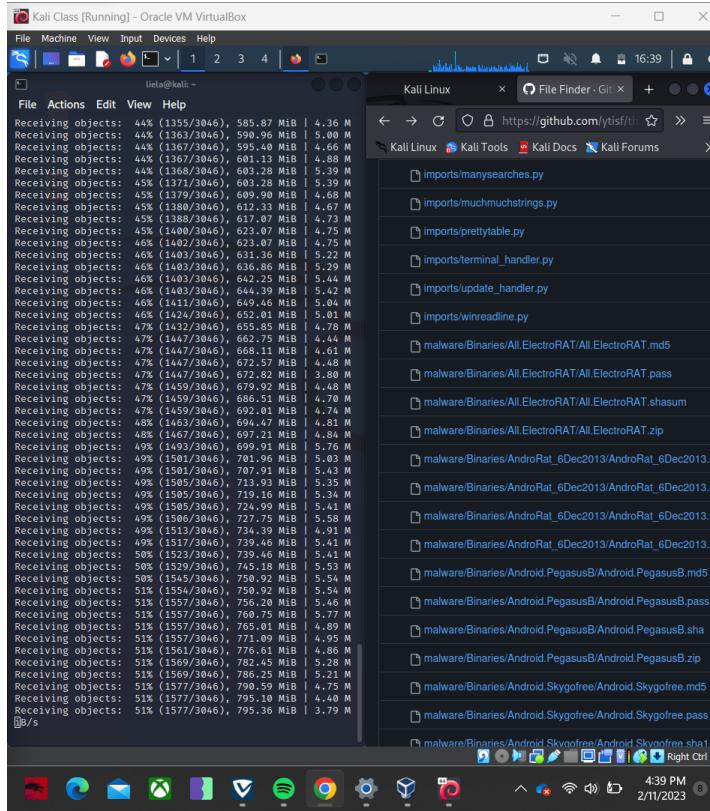
Sat Feb 11 16:03:16 2023 → "remote_cvthead: Download Failed (6) Sat Feb 11 16:03:16 2023 → ^ Message: Couldn't resolve host name
WARNING: Sat Feb 11 16:03:16 2023 → Failed to get daily database version information from ser
ver using user https://database.clamav.net
ERROR: Sat Feb 11 16:03:16 2023 → check_for_new_database_version: Failed to find daily databa
se using server https://database.clamav.net
Sat Feb 11 16:03:16 2023 → Trying again in 5 secs...
Sat Feb 11 16:03:21 2023 → Trying to retrieve CVD header from https://database.clamav.net/dai
ly.cvdb
Sat Feb 11 16:03:21 2023 → "remote_cvthead: Download failed (6) Sat Feb 11 16:03:21 2023 → ^
Message: Couldn't resolve host name
WARNING: Sat Feb 11 16:03:21 2023 → Failed to get daily database version information from ser
ver using user https://database.clamav.net
ERROR: Sat Feb 11 16:03:21 2023 → check_for_new_database_version: Failed to find daily databa
se using server https://database.clamav.net
Sat Feb 11 16:03:21 2023 → Trying again in 5 secs...
Sat Feb 11 16:03:26 2023 → Trying to retrieve CVD header from https://database.clamav.net/dai
ly.cvdb
Sat Feb 11 16:03:26 2023 → "remote_cvthead: download failed (6) Sat Feb 11 16:03:26 2023 → ^
Message: Couldn't resolve host name
WARNING: Sat Feb 11 16:03:26 2023 → Failed to get daily database version information from ser
ver using user https://database.clamav.net
ERROR: Sat Feb 11 16:03:26 2023 → check_for_new_database_version: Failed to find daily databa
se using server https://database.clamav.net
Sat Feb 11 16:03:26 2023 → Giving up after 3 tries...
ERROR: Sat Feb 11 16:03:26 2023 → Update failed for database: daily
ERROR: Sat Feb 11 16:03:26 2023 → Database update process failed: HTTP GET failed
ERROR: Sat Feb 11 16:03:26 2023 → Update failed.

```
(livelab@Kali:~) ~$ sudo systemctl start clamav-freshclam
(livelab@Kali:~) ~$ grep Checks /etc/clamav/freshclam.conf
Checks: 24
(livelab@Kali:~) ~$
```

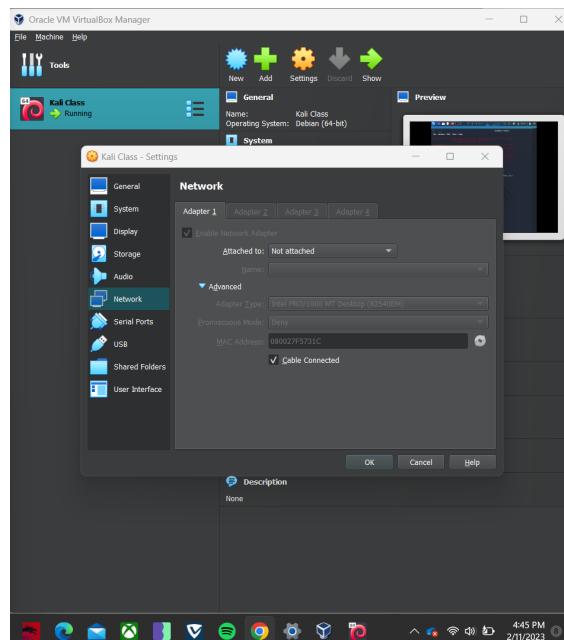
11. Disabled the antimalware for 24 hours and visited a malware repository that I found on Github.



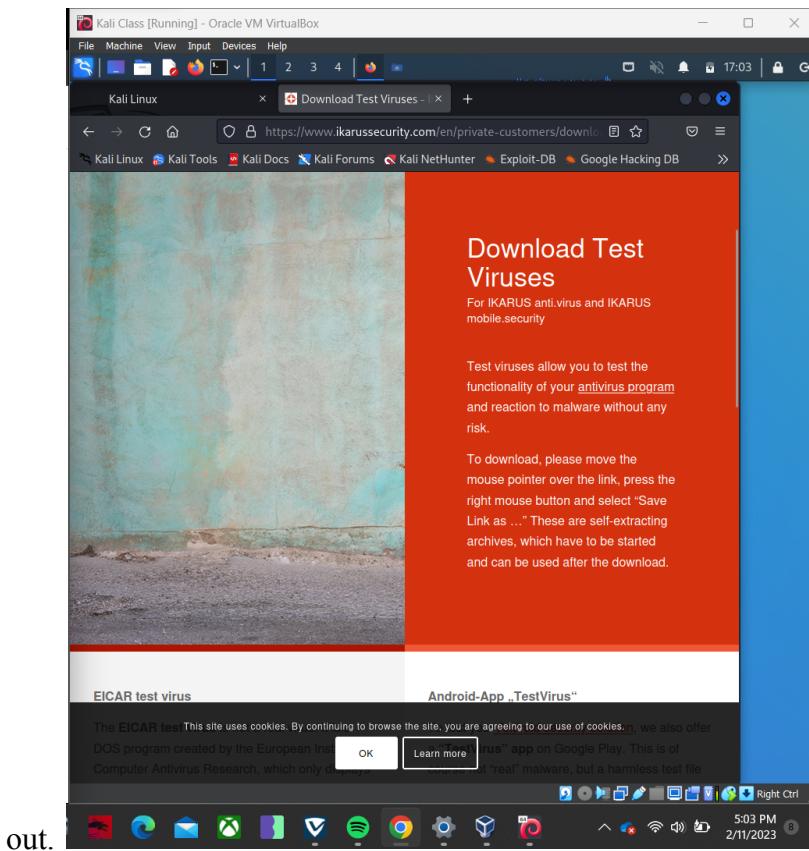
12. Cloned the repository using the instructions they provided. Then installed the requirements.
13. Around this time I started to get a little bit nervous about the amount of files of various malware I downloaded. None of it will run unless I activate it but still.



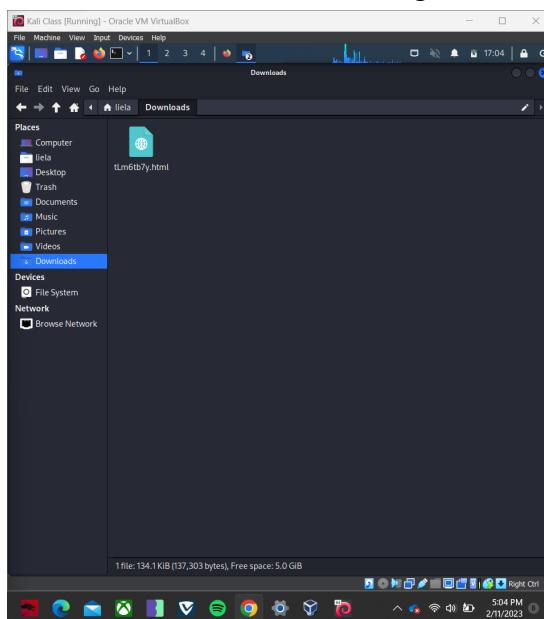
14. Disconnected my VM from any network connection between my OS and the machine as a precaution.



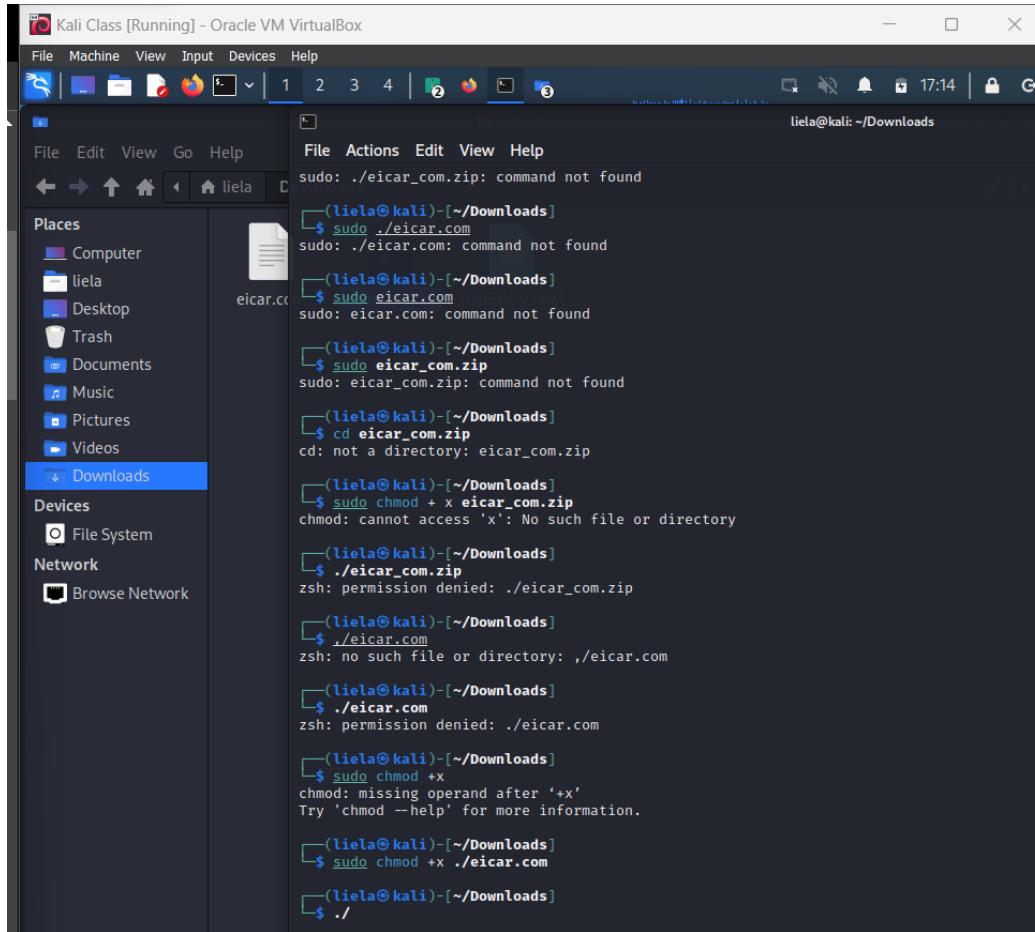
15. I decided to delete the directory and try this site that will download a file that isn't as malicious but does enough that it should trigger malware software. I decided to try this



16. The 2 viruses are meant to trigger antivirus software immediately when downloaded. Since I disabled clamAV, nothing seemed to react to the files being downloaded.



17. After many attempts to get the fake virus to run, I was able to get it to execute. After this I allowed the machine to run for about 22 more hours with clamav disabled.

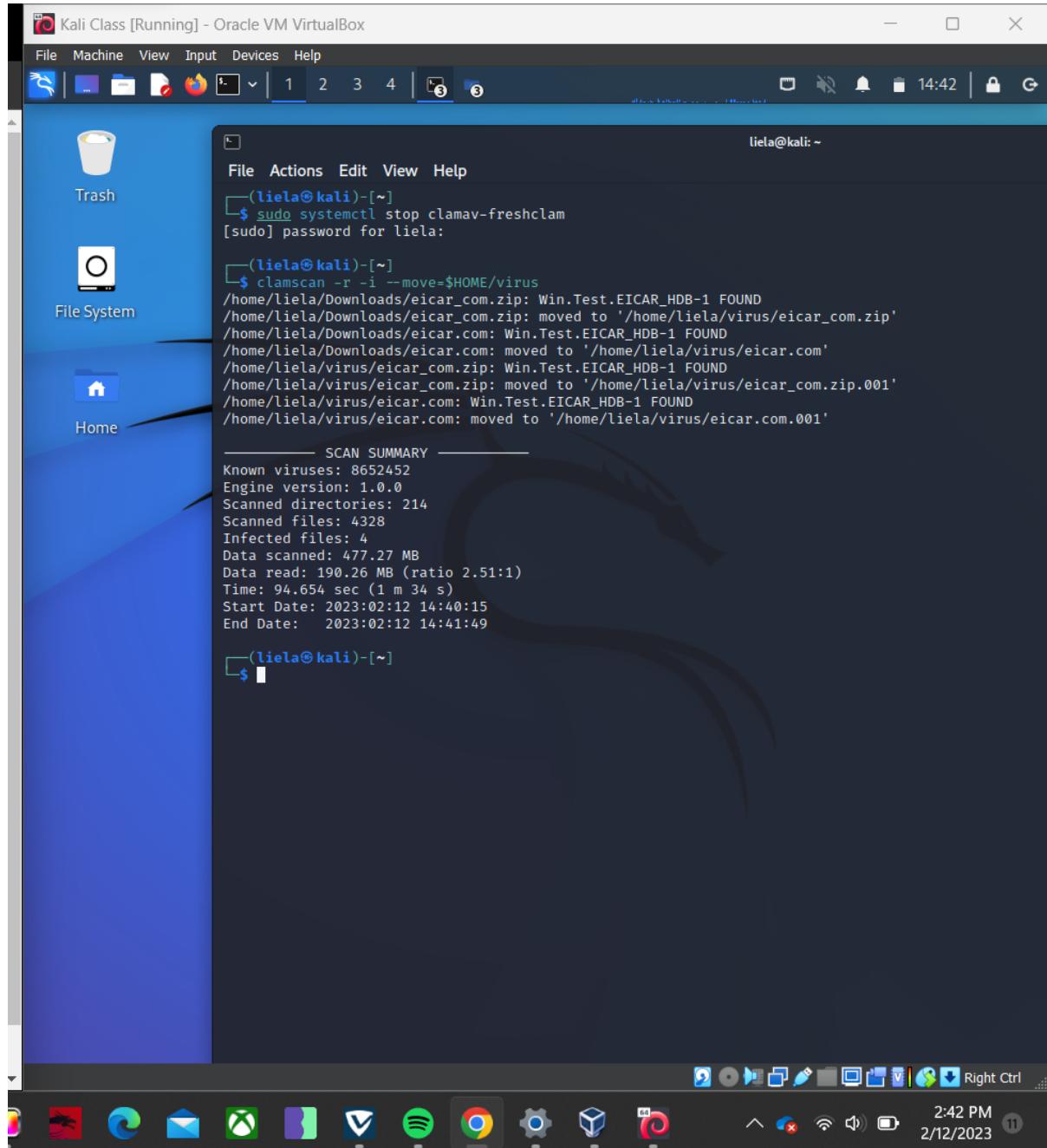


The screenshot shows a terminal window titled "Kali Class [Running] - Oracle VM VirtualBox". The terminal session is running under the user "liela" at the prompt "liela@kali: ~/Downloads". The user has attempted to execute the file "eicar.com" in various ways, including using sudo and chmod +x, but receives errors indicating the command or file does not exist or permission is denied. The terminal also shows a warning about a missing operand for the chmod command.

```
sudo: ./eicar_com.zip: command not found
(liela@kali)-[~/Downloads]
$ sudo ./eicar.com
sudo: ./eicar.com: command not found
(liela@kali)-[~/Downloads]
$ sudo eicar.com
sudo: eicar.com: command not found
(liela@kali)-[~/Downloads]
$ sudo eicar_com.zip
sudo: eicar_com.zip: command not found
(liela@kali)-[~/Downloads]
$ cd eicar_com.zip
cd: not a directory: eicar_com.zip
(liela@kali)-[~/Downloads]
$ sudo chmod +x eicar_com.zip
chmod: cannot access 'x': No such file or directory
(liela@kali)-[~/Downloads]
$ ./eicar_com.zip
zsh: permission denied: ./eicar_com.zip
(liela@kali)-[~/Downloads]
$ ./eicar.com
zsh: no such file or directory: ./eicar.com
(liela@kali)-[~/Downloads]
$ ./eicar.com
zsh: permission denied: ./eicar.com
(liela@kali)-[~/Downloads]
$ sudo chmod +x
chmod: missing operand after '+x'
Try 'chmod --help' for more information.
(liela@kali)-[~/Downloads]
$ sudo chmod +x ./eicar.com
(liela@kali)-[~/Downloads]
$ ./
```

18. The next day I started up the clamav and the scan summary detected the test virus that I downloaded and enabled. It then moved it to the virus folder. You can see the difference

in the amount of files it scanned and the total number of infected files went from 0 to 4.



The screenshot shows a Kali Linux desktop environment within Oracle VM VirtualBox. The desktop has a blue theme with icons for Trash, File System, and Home. A terminal window is open, showing the following command-line session:

```
liela@kali: ~
File Actions Edit View Help
[~]
$ sudo systemctl stop clamav-freshclam
[sudo] password for liela:

[~]
$ clamscan -r -i --move=$HOME/virus
/home/liela/Downloads/eicar_com.zip: Win.Test.EICAR_HDB-1 FOUND
/home/liela/Downloads/eicar_com.zip: moved to '/home/liela/virus/eicar_com.zip'
/home/liela/Downloads/eicar.com: Win.Test.EICAR_HDB-1 FOUND
/home/liela/Downloads/eicar.com: moved to '/home/liela/virus/eicar.com'
/home/liela/virus/eicar_com.zip: Win.Test.EICAR_HDB-1 FOUND
/home/liela/virus/eicar_com.zip: moved to '/home/liela/virus/eicar_com.zip.001'
/home/liela/virus/eicar.com: Win.Test.EICAR_HDB-1 FOUND
/home/liela/virus/eicar.com: moved to '/home/liela/virus/eicar.com.001'

----- SCAN SUMMARY -----
Known viruses: 8652452
Engine version: 1.0.0
Scanned directories: 214
Scanned files: 4328
Infected files: 4
Data scanned: 477.27 MB
Data read: 190.26 MB (ratio 2.51:1)
Time: 94.654 sec (1 m 34 s)
Start Date: 2023:02:12 14:40:15
End Date: 2023:02:12 14:41:49

[~]
$
```

Client-side Malicious Attacks & Network-based Attacks

Malicious attacks also known as malware are when an attacker utilizes software on a computer or system without user consent or knowledge and proceeds to do harmful and unwanted things. There are various types and 100s of millions of malware that release each month, some including ransomware, launch attacks and snooping. Ransomware is when that attacker prevents proper

functionality into the victim's device until a fee is paid, a similar attack is crypto-malware, in which the attack will encrypt files until they are paid. Launch attacks come in different forms such as viruses, worms, and bots. Snooping is when the attacker takes action to collect sensitive or personal information from the victim, for example, keylogging is when the attacker will use a software to record the different words being typed by the user unknowingly. In addition, attackers prey on application vulnerabilities and use scripting, injection or request forgery techniques to do so. Using scripting, attackers can input a script response into a vulnerable website that will actually interact with the code and mess up the site. There are several different attacks that can target a network, a process of the specific endpoint on a network. The different types of network attacks include interception, DNS, scripting, malicious coding, Layer 2 or Data Link, Distributed Denial of Service, scripting, and more. There are various interception methods including a man-in-the-middle attack, this is when the threat actor inserts himself between two parties and is able to collect and view the data being transmitted between both parties.