# ITT-307 - Client-Side Attacks

**Professor:** Ingrid Gaviria

**Course:** ITT-307 Cybersecurity Foundations

**Student:** Liela Pressley

**Date:** 2/2/2023

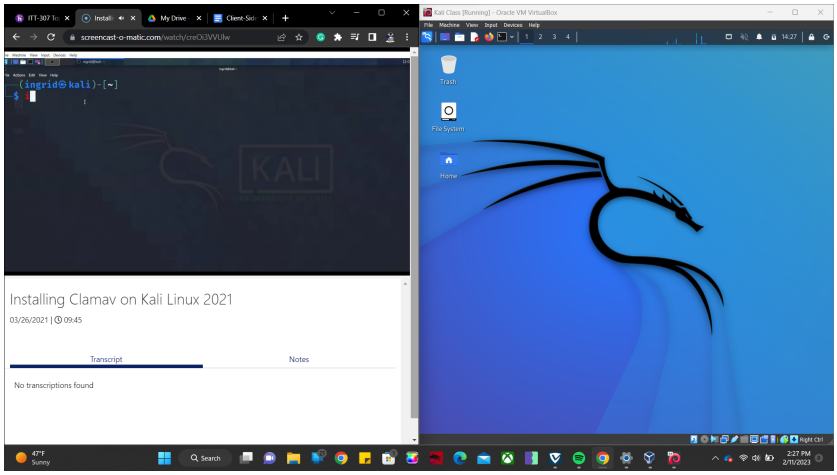
**Title:** Client-Side Attacks

---

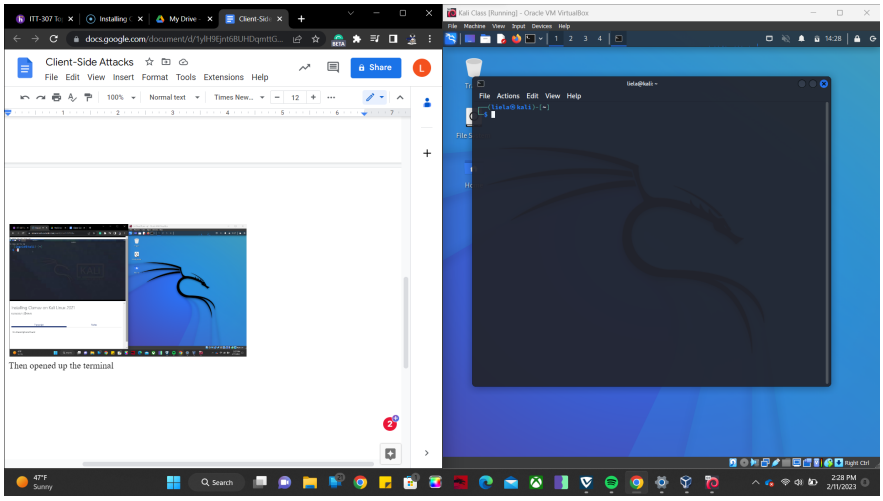
Overview: Antimalware is essential to have on any device, when not installed and enabled, the wrong download, URL, or phishing scam, can lead to your entire device being compromised, accounts being accessed, and much worse. I installed ClamAV to my Kali Linux system in VirtualBox then attempted to download 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:

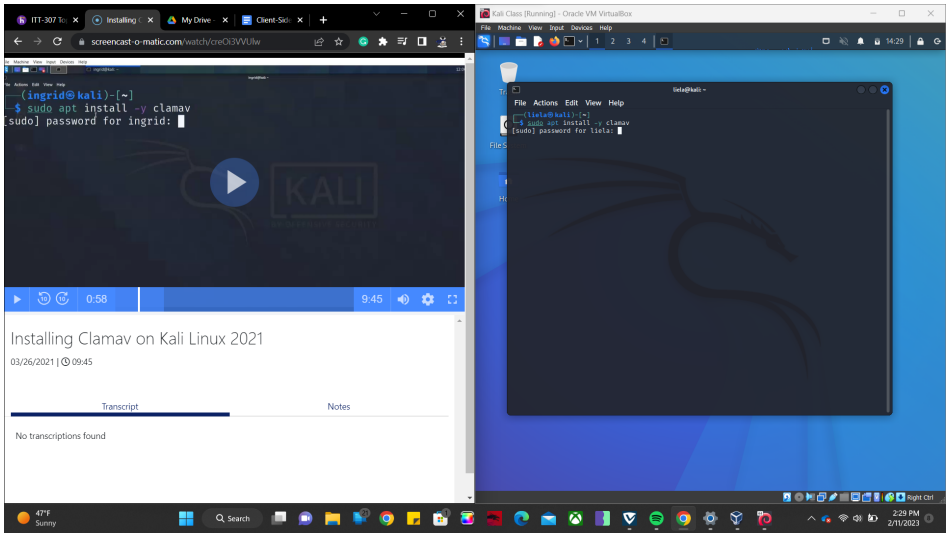
1. First I login into my Virtual Box Kali Linux



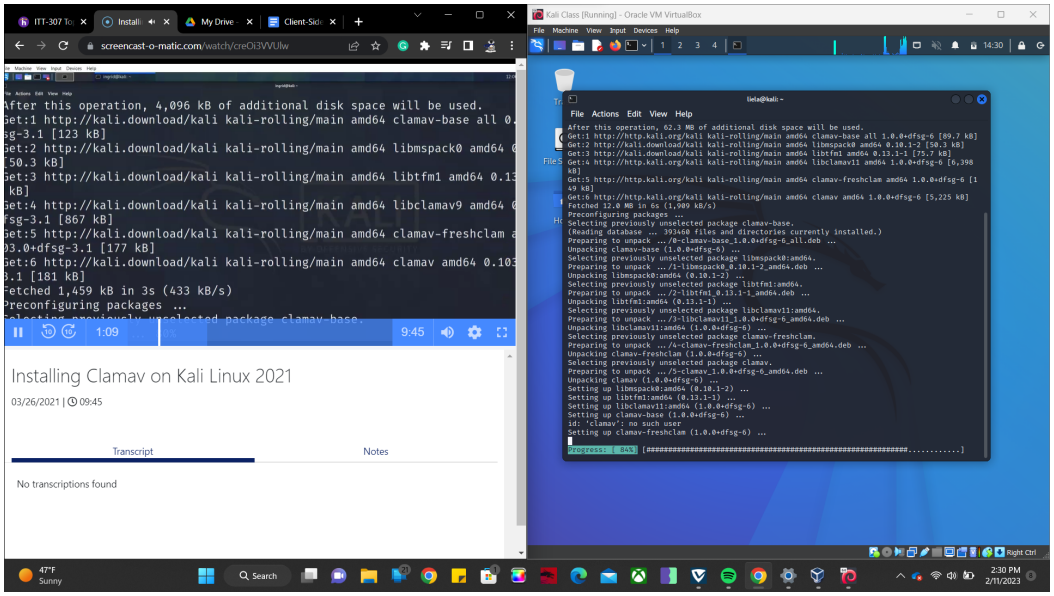

2. Then opened up the terminal



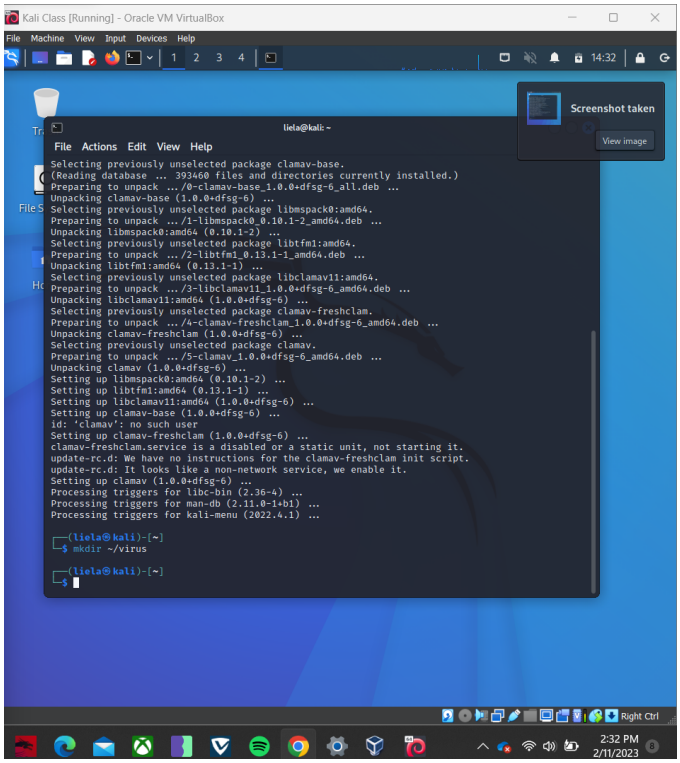

3. I then typed: sudo apt install -y clamav. It prompts for my login credentials.



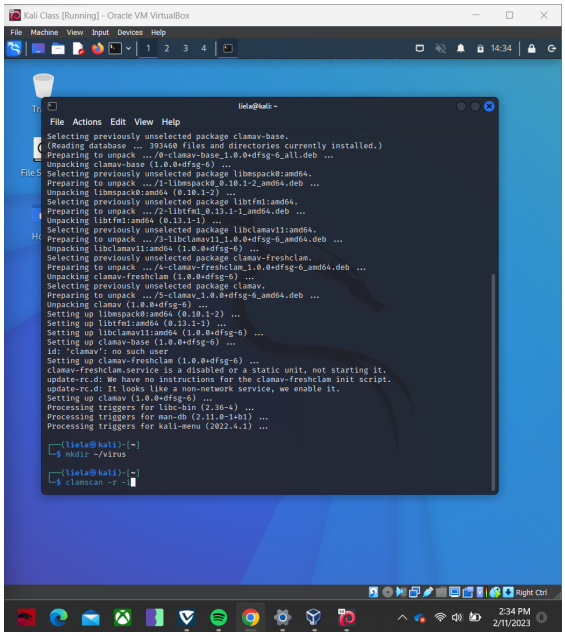

4. It then retrieves and processing and unpacks the packages from clamav



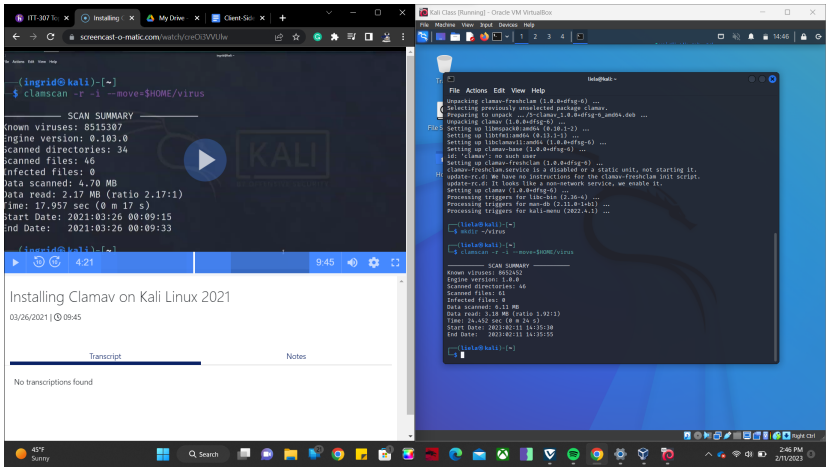

5. Then i made a directory titled Virus; mkdir ~/virus

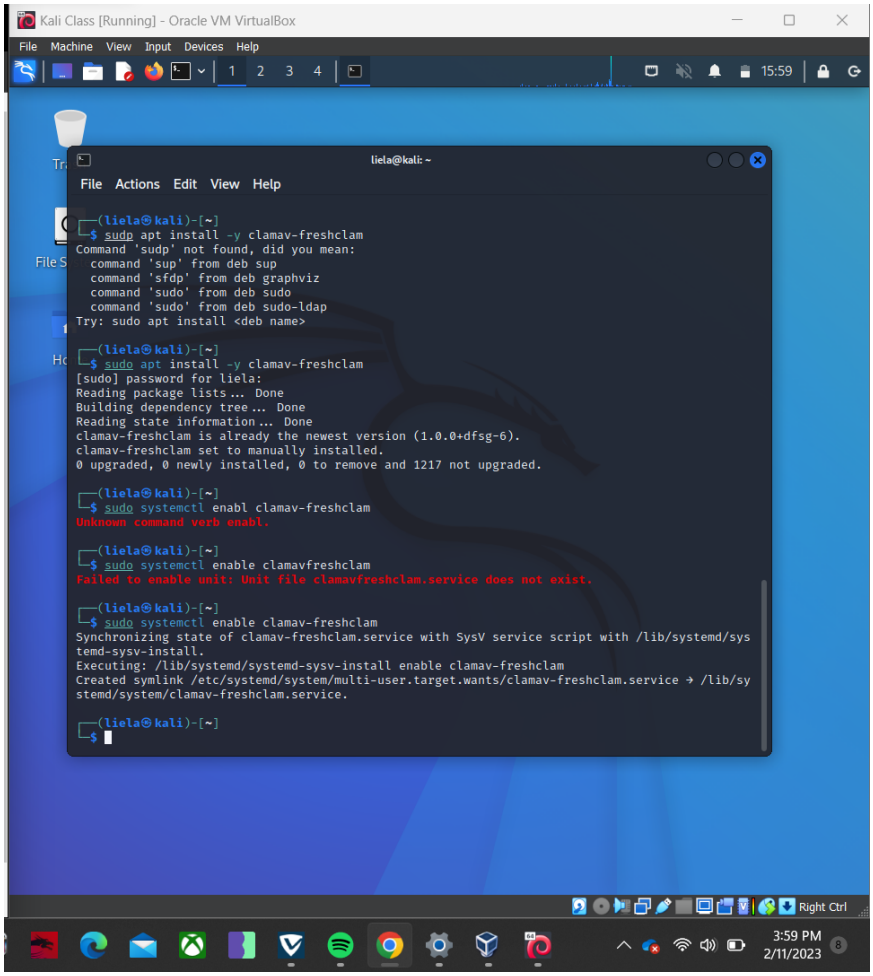


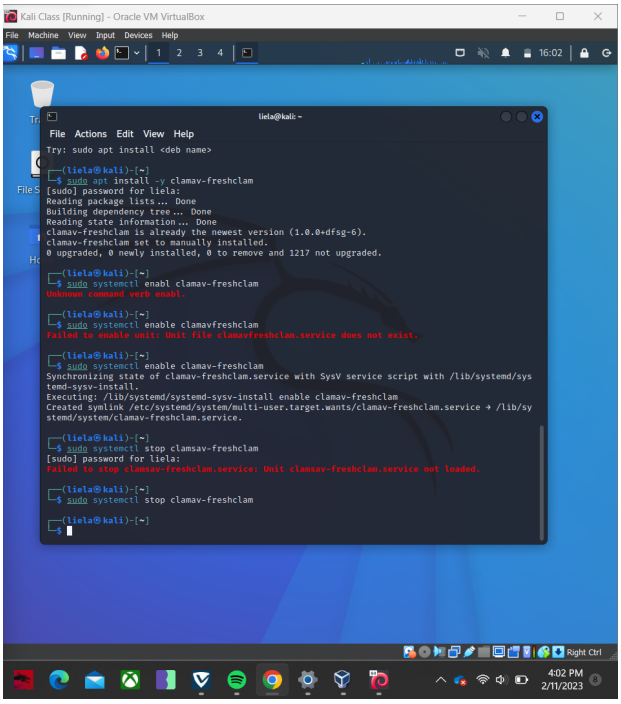

6. Use clamscan to scan the directory and files only and move the detected files to a specific directory



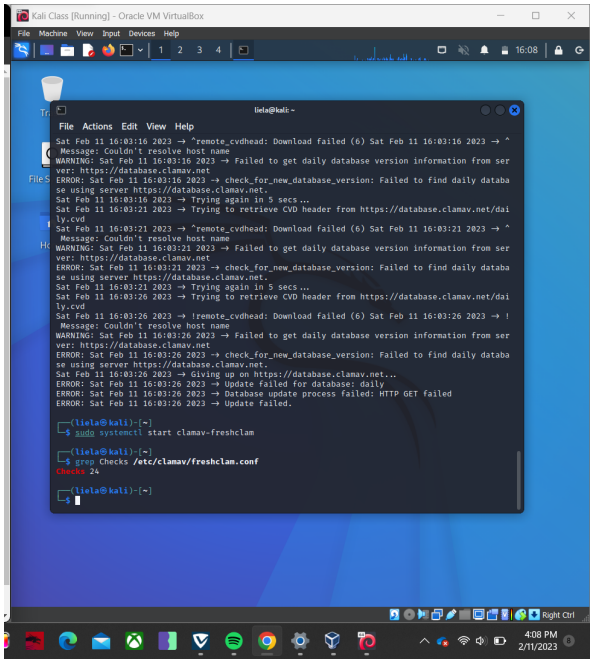

7. After asking to view it shows the scan summary



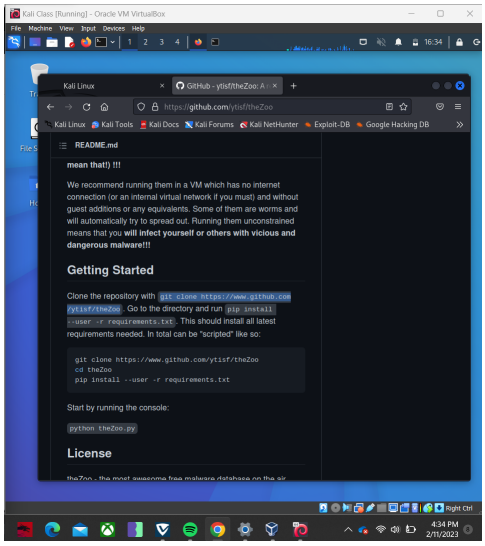
8. 

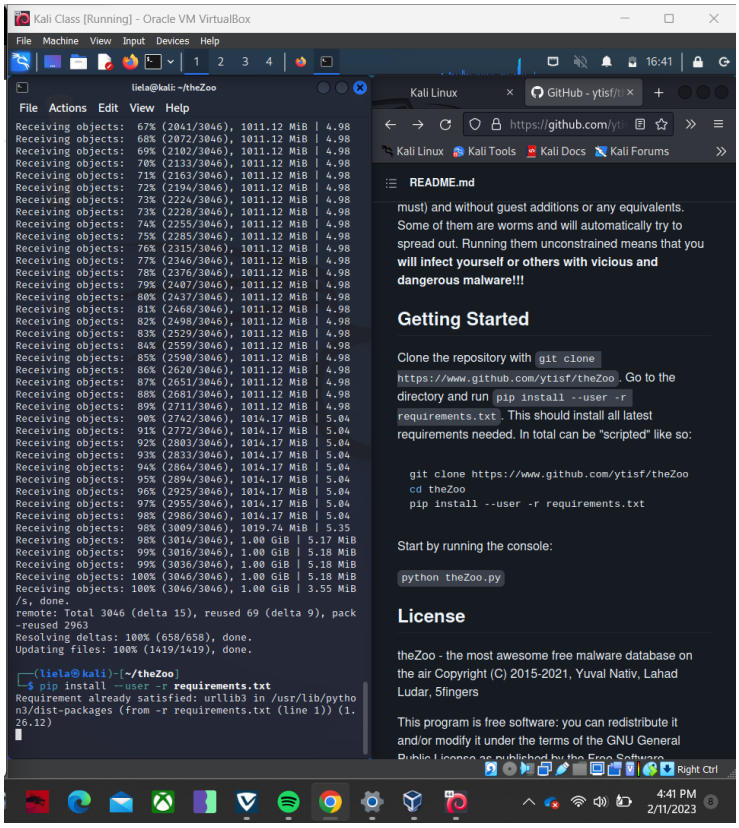

9. Stop the scan 

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

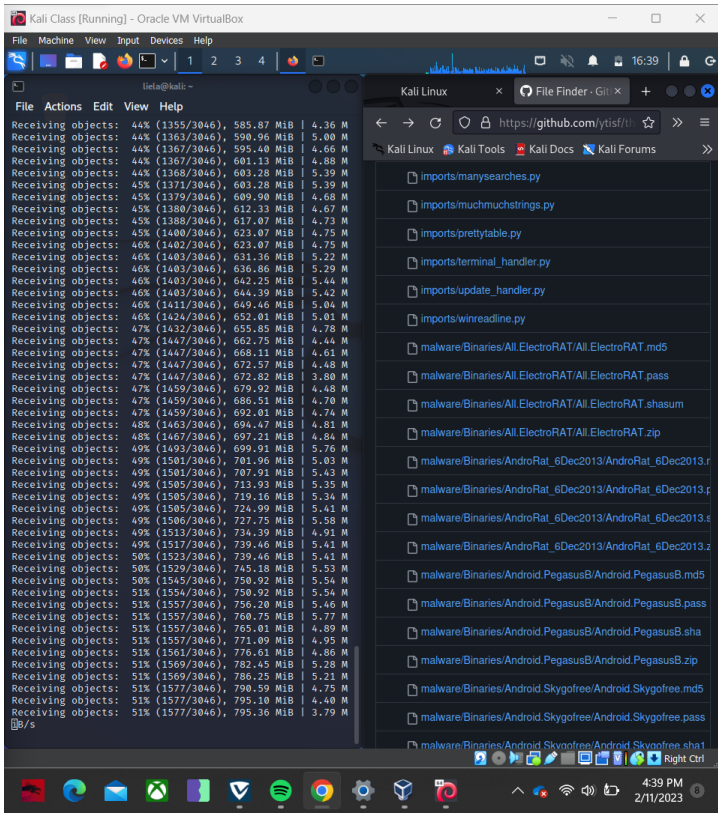



11. Disabled the antimalware for 24 hours and visited a malware repository that I found on Github.

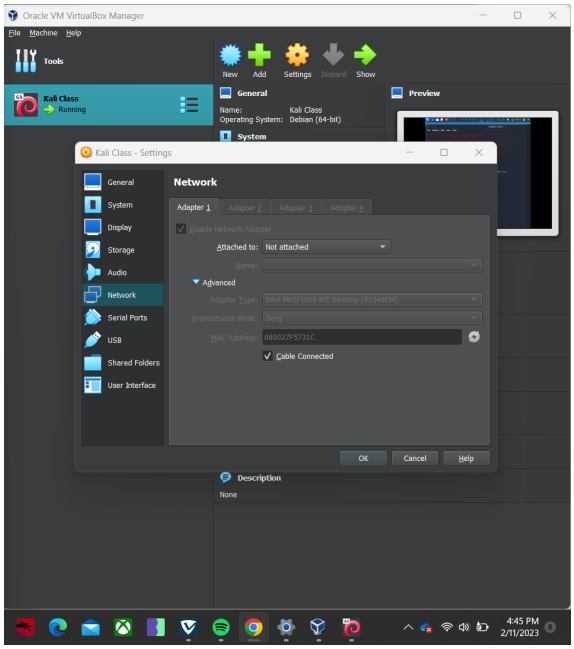


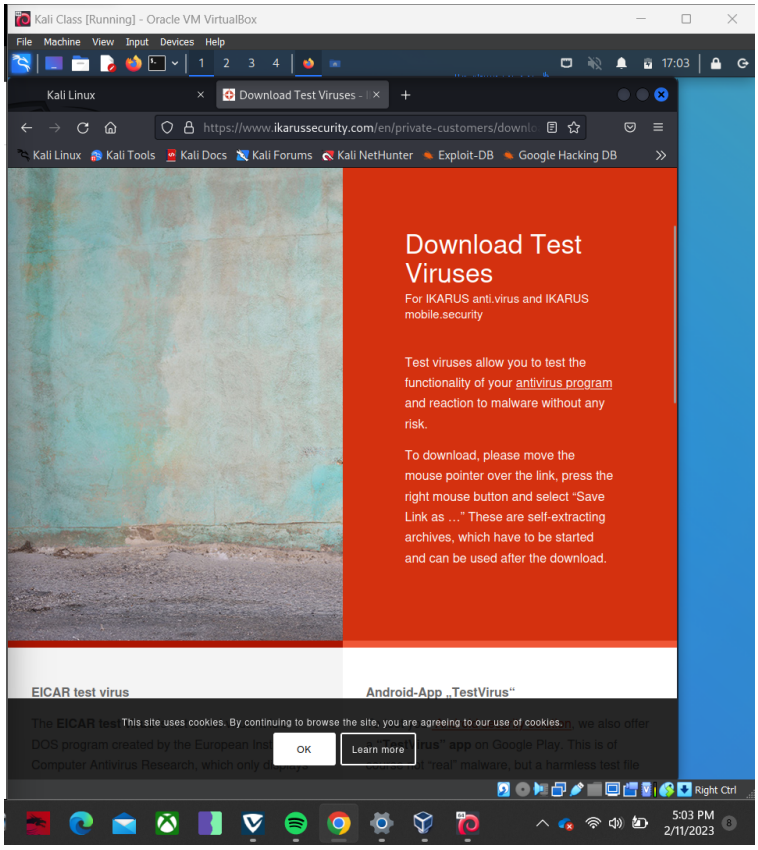



12. Cloned the repository using the instructions they provided. Then installed the requirements.
13. Around this time I started to get a little bit nervous about the amount of files of various malware I downloaded. None of it will run unless I activate it but still.

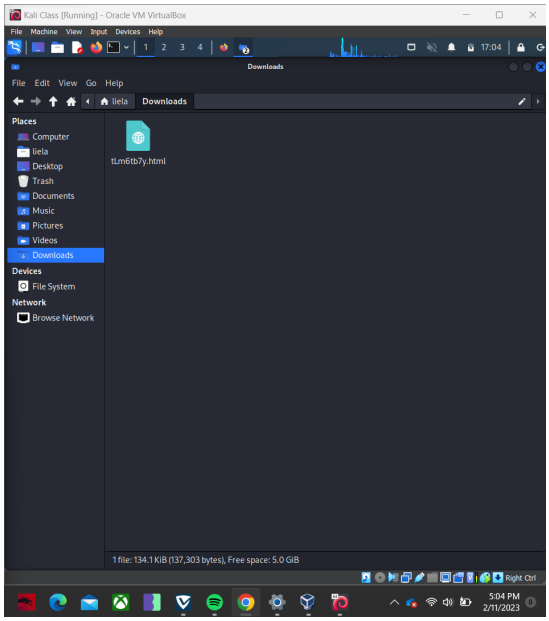



14. Disconnected my VM from any network  connection between my OS and the machine as a precaution.

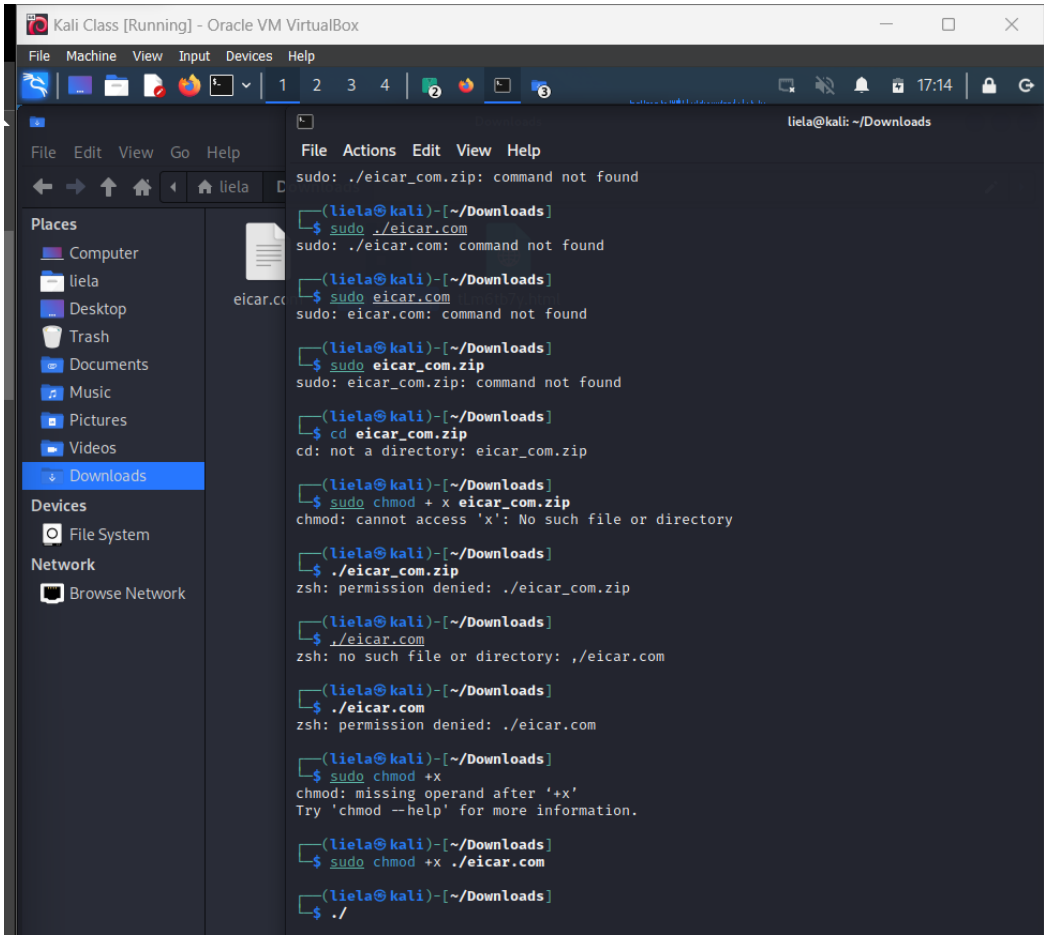


15. I decided to delete the directory and try this site that will download a file that isn't as malicious but does enough that it should trigger malware software. I decided to try this out. 


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.

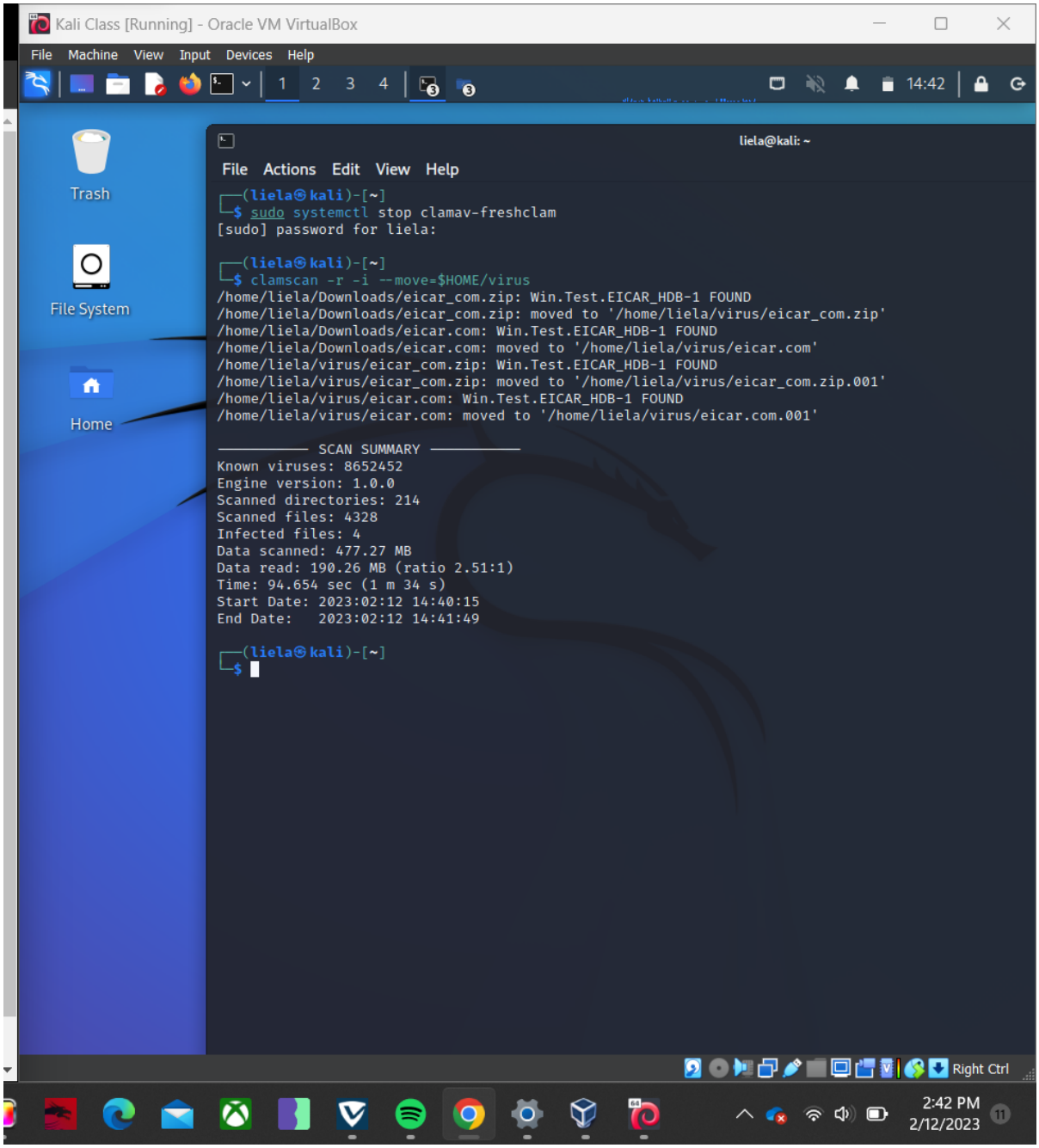


17. After many attempts to get the fake virus to run, I was able to get it to execute. After this I allowed the machine to run for about 22 more hours with clamav disabled.




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.




**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.