Bộ môn An toàn Thông tin – Khoa MMT&TT
Trường Đại học Công nghệ Thông tin (UIT)

EXERCISE REPORT

Assignment : Using tools to

analyze malware

GENERAL INFORMATION:

Num	Full name	Student ID	Email
1	Le Phan Huu Nghia	20520650	20520650@gm.uit.edu.vn
2	Ngo Vo Viet Khoa	17520642	17520642@gm.uit.edu.vn
3	Nguyen Dinh Kha	20520562	20520562@gm.uit.edu.vn

IMPLEMENTATION CONTENT:

Num	Work	Personal responsibility	Self-assessment Result
1	**Question 1**	Nguyen Dinh Kha + Le Phan Huu Nghia	100%
2	**Question 2:**	Ngo Vo Viet Khoa	0%

Question 1: The team uses tools to create malware for research purposes

The team utilises tools to initiate malware, with the chosen type being Ransomware from the Malware Repository: theZoo: A live malware repository.

- First, we need to install the Malware Repository theZoo: A live malware repository onto our computer:

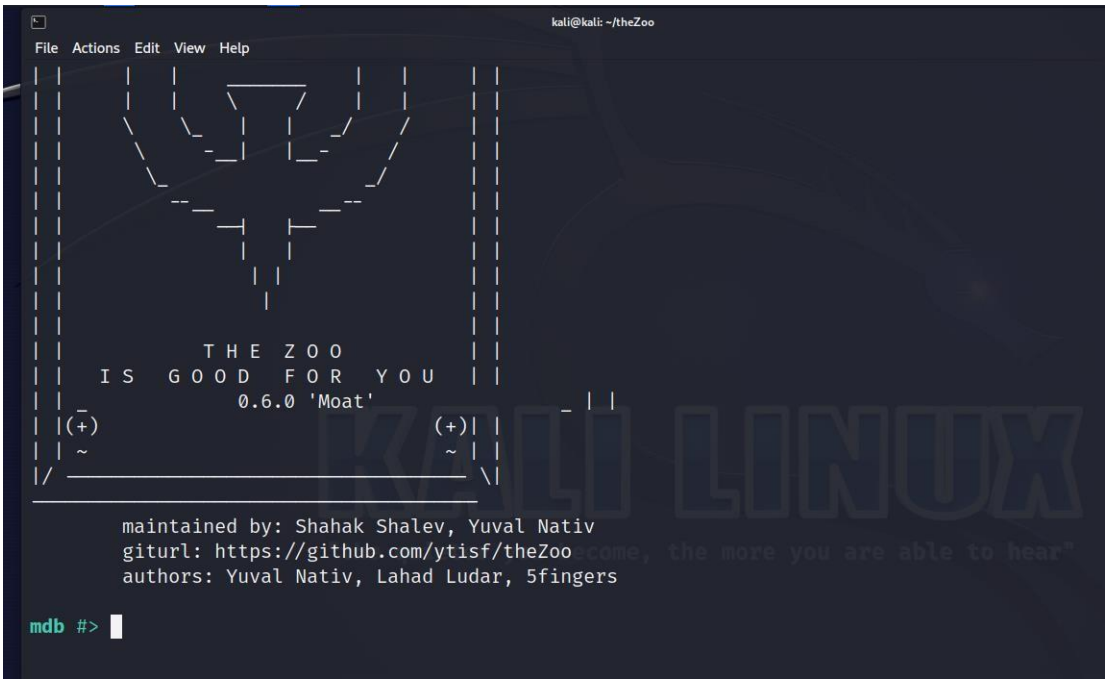
```
┌──(kali㉿kali)-[~/Downloads/NT534.N21.ATCL/theZoo]
└─$ pip install --user -r requirements.txt
Requirement already satisfied: urllib3 in /usr/lib/python3/dist-packages (from -r requirements.tx
t (line 1)) (1.26.12)
Collecting pyminizip
  Downloading pyminizip-0.2.6.tar.gz (261 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 261.2/261.2 kB 2.0 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Building wheels for collected packages: pyminizip
  Building wheel for pyminizip (setup.py) ... done
  Created wheel for pyminizip: filename=pyminizip-0.2.6-cp311-cp311-linux_x86_64.whl size=203205
sha256=0cc0ee9662168ff91d51ccb959e9a8056e8ff3bbee5ea0ce9a175eef0d478f1e
  Stored in directory: /home/kali/.cache/pip/wheels/50/c4/3c/6fb797c8b35d61411c595e7b2074dc657e43
95a7ff525bbace
Successfully built pyminizip
Installing collected packages: pyminizip
Successfully installed pyminizip-0.2.6
```

=> TheZoo installation.

- We then use the ls command in the theZoo directory to see the files within theZoo.

```
┌──(kali㉿kali)-[~/Downloads/NT534.N21.ATCL/theZoo]
└─$ ls
CODE-OF-CONDUCT.md  CONTRIBUTING.md  LICENSE.md  prep_file.py  requirements.txt
conf                imports          malware     README.md     theZoo.py
```

- The interface of theZoo after successful installation:



- After entering theZoo, we navigate to ransomware and select WannaCry for download:

```
mdb #> search ransomware
+-----+------------+----------+--------------+--------------+-----------------------------------------+
| #   | Type       | Language | Architecture | Platform     | Name                                    |
+-----+------------+----------+--------------+--------------+-----------------------------------------+
| 25  | ransomware | bin      | x86          | win32        | CryptoLocker                            |
| 26  | ransomware | bin      | x86          | win32        | CryptoLocker                            |
| 33  | ransomware | bin      | x86          | win32        | CryptoLocker                            |
| 42  | ransomware | bin      | x86          | win32        | Trojan.Ransom                           |
| 62  | ransomware | bin      | x86          | win32        | Zerolocker                              |
| 65  | ransomware | bin      | x86          | win32        | Reveton                                 |
| 81  | ransomware | bin      | x86          | win32        | Matsnu                                  |
| 119 | ransomware | bin      | x86          | win32        | Cryptowall                              |
| 136 | ransomware | bin      | x86          | win32        | TeslaCrypt                              |
| 149 | ransomware | bin      | x86          | win32        | Radamant                                |
| 150 | ransomware | bin      | x86          | win32        | Vipasana                                |
| 151 | ransomware | bin      | x86          | win32        | Locky                                   |
| 156 | ransomware | bin      | x86          | win32        | Petya                                   |
| 157 | ransomware | bin      | x86          | win32        | Jigsaw                                  |
| 159 | ransomware | bin      | x86          | win32        | Satana                                  |
| 160 | ransomware | bin      | x86          | linux        | Rex                                     |
| 163 | ransomware | java     | arm          | android      | andr0id_l0cker                          |
| 165 | ransomware | bin      | x86          | win32        | Petrwrap                                |
| 177 | ransomware | bin      | x86          | win32        | Wannacry+                               |
| 183 | ransomware | bin      | x86          | win32        | WannaPeace                              |
| 188 | ransomware | bin      | x86          | win32        | Unnamed Ransomware                      |
| 290 | ransomware | NA       | x86          | win32        | WannaCry                                |
| 303 | ransomware | NA       | x86          | win32        | KeyPass                                 |
| 325 | ransomware | bin      | x86,x64      | win32, win64 | Thanos, PowGoop, LogicalDuckBill        |
| 339 | ransomware | bin      | x86          | win32        | RedBoot                                 |
| 351 | ransomware | bin      | x86          | win32        | Hells Ransomware (UEFI)                 |
| 352 | ransomware | bin      | x86,x64      | win32, win64 | Petya                                   |
| 354 | ransomware | cpp      | x86,x64      | win32, win64 | Conti Locker                            |
| 355 | ransomware | bin      |              |              | XData Ransomware                        |
| 356 | ransomware | bin      |              | win32,linux  | Hive Ransomware                         |
+-----+------------+----------+--------------+--------------+-----------------------------------------+
[+] Total records found: 30
```

- We can see WannaCry is in section 290, so we proceed to download:

```
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#>
```

=> Use the get command to download WannaCry.

- We check the information of the WannaCry ransomware that we have downloaded:

```
mdb WannaCry#> info
+-------------+------------+------+--------+------+------+-------+-------+------+
| %           | Name       | Ver. | Author | Lang | Date | Arch. | Plat. | Tags |
+-------------+------------+------+--------+------+------+-------+-------+------+
| ransomware | WannaCry | NA   | NA     | NA   | NA   | x86   | win32 | None |
+-------------+------------+------+--------+------+------+-------+-------+------+
[+] Total records found: 1
```

```
┌──(cuckoo)─(kali㉿kali)-[~/theZoo]
└─$ unzip Ransomware.WannaCry.zip
Archive:  Ransomware.WannaCry.zip
[Ransomware.WannaCry.zip] ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe password:
  inflating: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

┌──(cuckoo)─(kali㉿kali)-[~/theZoo]
└─$ ls
CODE-OF-CONDUCT.md                                                  Ransomware.WannaCry.md5
conf                                                                Ransomware.WannaCry.pass
CONTRIBUTING.md                                                     Ransomware.WannaCry.sha256
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe Ransomware.WannaCry.zip
imports                                                             README.md
LICENSE.md                                                          requirements.txt
malware                                                             theZoo.py
prep_file.py
```

⇨ After extracting the file, we find the .exe file to run WannaCry.

- We proceed to create a virtual environment to safely observe the behavior of WannaCry:

```
┌──(kali㉿kali)-[~]
└─$ virtualenv cuckoo
created virtual environment CPython3.11.2.final.0-64 in 508ms
  creator CPython3Posix(dest=/home/kali/cuckoo, clear=False, no_vcs_ignore=False, global=False)
  seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=copy, app_data_dir=/home/kali/.local/share/virtualenv)
    added seed packages: pip==23.0.1, setuptools==66.1.1, wheel==0.38.4
  activators BashActivator,CShellActivator,FishActivator,NushellActivator,PowerShellActivator,PythonActivator

┌──(kali㉿kali)-[~]
└─$
```

- Activate the cuckoo environment:

Brief about Cuckoo Sandbox:
Cuckoo Sandbox is an open-source, automated malware analysis system that allows researchers and security professionals to test and analyze suspicious files and URLs in a safe, isolated environment. Its main features include:

1) **Malware analysis:** Cuckoo Sandbox allows users to automatically analyze malware and provide detailed reports on the behavior and capabilities of the malware.
2) **Scalability:** The system is highly scalable and can be deployed across multiple machines to handle large volumes of malware samples.
3) **Network traffic analysis:** Cuckoo Sandbox also captures and analyzes network traffic generated by the malware, allowing users to identify and understand how the malware communicates with command and control (C2) servers.
4) **API support:** Cuckoo Sandbox offers an API for integration with other security tools and platforms, making the malware analysis process more automated and straightforward.
5) **Customizability:** The system is highly customizable, allowing users to modify and extend its capabilities to suit their specific needs.
6) **User-friendly web interface:** Cuckoo Sandbox comes with a web-based user interface that allows users to manage and monitor the analysis process, view reports, and interact with the system.
7) **Community support:** Cuckoo Sandbox is an actively maintained open-source project supported by a large community of developers and users, providing continuous support and updates for the system.

Question 2: Use malware analysis tools to analyze the behavior of malware when it is activated.

END