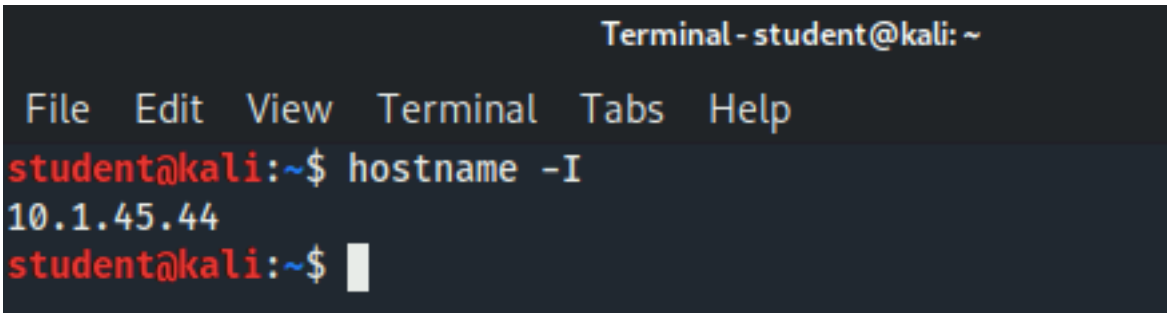
Roozah Khan

12/5/20

Lab #5

1.)



2.)

```
student@kali:~$ -git clone https://github.com/ytisf/theZoo.git
bash: -git: command not found
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 | 55.92 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:~$
```

3.)

File Edit View Terminal Tabs Help

300	DarkTequila	trojan
301	Triton	apt
302	MyLobot	botnet
303	KeyPass	ransomware
304	Carbanak	apt
305	APT34	apt
306	Pegasus	apt
307	BigBang	apt
308	MuddyWater	apt
309	GreenBug	apt
310	Cozy Bear Collection	apt
311	DarkHydrus	apt
312	AppleJeus	apt
313	ZeroCleare, Dustman	apt
314	KerrDown	apt
315	POWERSTATS	apt
316	StrongPity	apt
317	NukeSped, AllStar	apt
318	AsyncRAT	rat
319	NjRAT	rat
320	RevengeRAT	rat
321	CobianRAT	rat
322	SpyNote	rat
323	Mirai	apt
324	PlugX,CobalStrike,PoisionIvy	apt
325	Thanos, PowGoop, LogicalDuckBill	randomware
326	Transparent Tribe	apt
327	LuckyCat, TA413	apt
328	FASTCash	apt
329	PoisionFrog	apt
330	Zeus	botnet
331	Cerebrus	botnet
332	Assorted ASM Oldschool Trojans	trojan
333	Mirai Family	trojan

[+] Total records found: 332

mdb #>

4.)

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

5.)

```
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$
```

6.) The executable asked if I want to let the program make changes to my computer and when I clicked “no” the ransomware program popped up on the desktop and when I would click cancel the ransomware kept popping up.