Cyberpaths

- Ransomware Lab -

Lab Goals

1. Understand the detrimental effects of ransomware.

2. Reverse engineer simple ransomware software.

Quick introduction to Ransomware

Ransomware is malicious software that blocks access to a computer or information until a specific amount of money has been paid. It belongs to the general category of malware, i.e., malicious, intrusive software.

Prerequisites

1. You will need basic command line knowledge to complete this lab. Codecademy has a great tutorial on this topic.

2. Basic cryptography: Khan academy has a great class on cryptography and these ciphers that can be found here.

3. Hashing: Here is an interesting video from khan academy on hash functions.

Part 1: Setting up the topology

1. Reserve a single Xen VM with default settings

2. Log onto the node and download the provided [text files] and python script [scan_directories.py]

3. To download all the files use the following commands:

```
wget https://github.com/mundruid/CyberPaths/raw/master/Ransomware.zip
```

and

```
wget https://raw.githubusercontent.com/mundruid/CyberPaths/master/pythonScripts/scan_directories.py
```

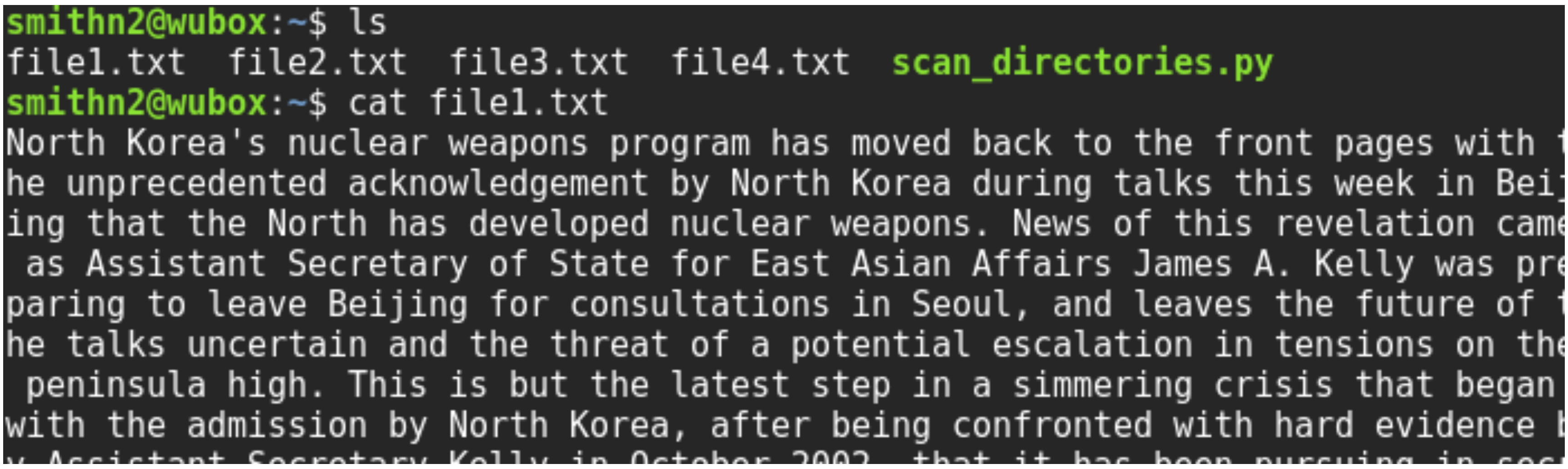
4. To unzip your files use the following command:

```
unzip Ransomware.zip
```

Part 2: The Mission

1. Log onto the machine assigned by your instructor. If you have reserved your own virtual machine, you may login to this machine.

2. Find all the files by using the proper directory listing commands and view those files.

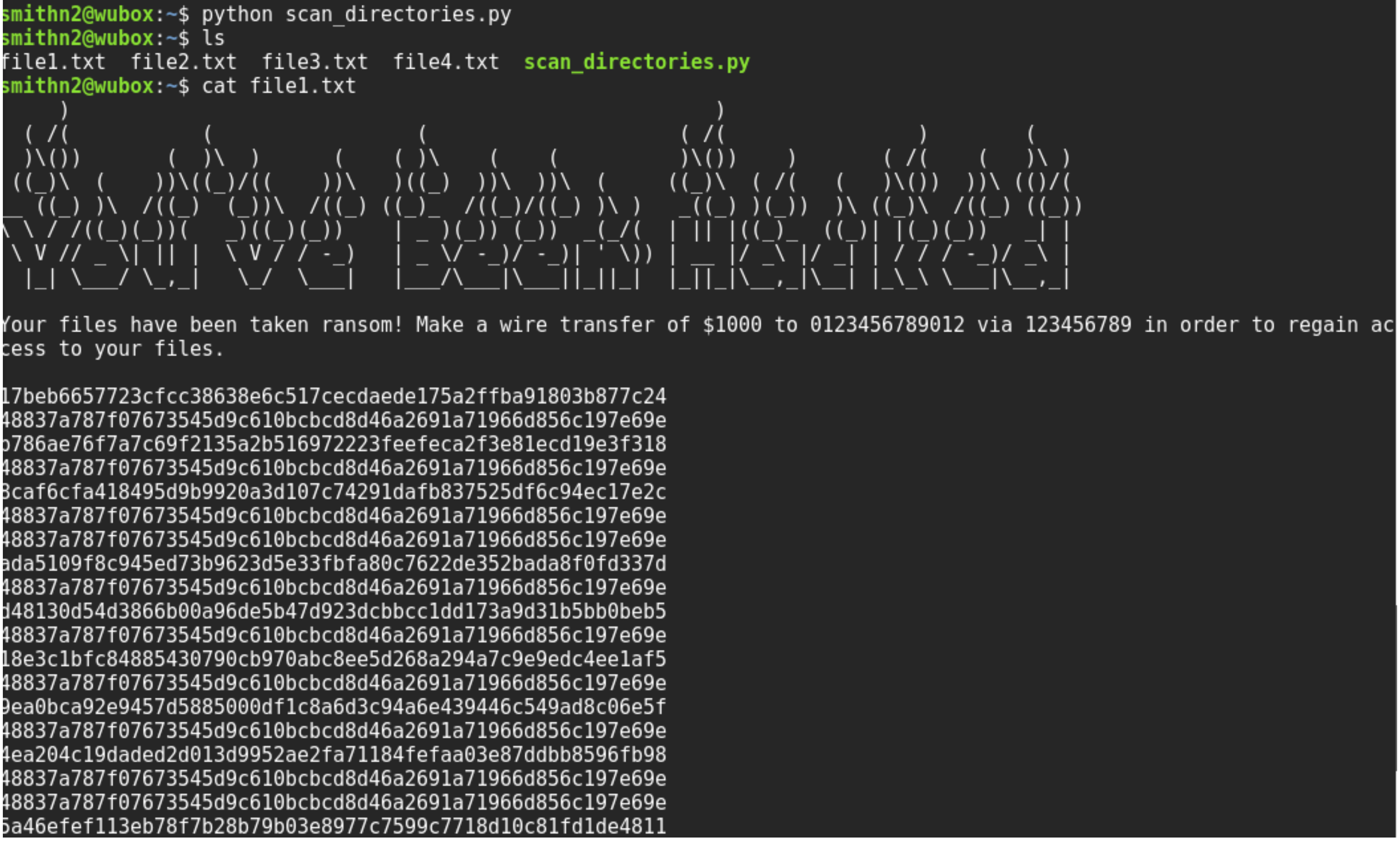


```
smithn2@wubox:~$ ls
file1.txt  file2.txt  file3.txt  file4.txt  scan_directories.py
smithn2@wubox:~$ cat file1.txt
North Korea's nuclear weapons program has moved back to the front pages with t
he unprecedented acknowledgement by North Korea during talks this week in Bei
ing that the North has developed nuclear weapons. News of this revelation came
 as Assistant Secretary of State for East Asian Affairs James A. Kelly was pre
paring to leave Beijing for consultations in Seoul, and leaves the future of t
he talks uncertain and the threat of a potential escalation in tensions on the
 peninsula high. This is but the latest step in a simmering crisis that began
with the admission by North Korea, after being confronted with hard evidence b
y Assistant Secretary Kelly in October 2002, that it has been pursuing in sec
```

3. Run the file scan_directories.py to scan your machine for viruses by using the following command:

```
python scan_directories.py
```

4. Open the text files again, after the scan_directories.py has been executed.



```
smithn2@wubox:~$ python scan_directories.py
smithn2@wubox:~$ ls
file1.txt  file2.txt  file3.txt  file4.txt  scan_directories.py
smithn2@wubox:~$ cat file1.txt
     )                                                       )
  ( /(            (                 (                     ( /(                )        (
  )\())       (   )\  )      (    ( )\    (    (          )\())    )       ( /(    (    )\ )
 ((_)\  (    ))\((_)/((    ))\   )((_)  ))\  ))\  (     ((_)\  ( /(   (   )\())  ))\ (()/(
__ ((_) )\  /((_)  (_))\  /((_) ((_)_  /((_)/((_) )\ )   _((_) )(_))  )\ ((_)\  /((_) ((_))
\ \ / /((_)(_))(   _)((_)(_))    | _ )(_)) (_))  _(_/(  | || |((_)_  ((_)| |(_)(_))   _| |
 \ V // _ \| || |  \ V / / -_)   | _ \/ -_)/ -_)| ' \)) | __ |/ _` |/ _| | / / / -_)/ _` |
  |_| \___/ \_,_|   \_/  \___|   |___/\___|\___||_||_|  |_||_|\__,_|\__| |_\_\ \___|\__,_|

Your files have been taken ransom! Make a wire transfer of $1000 to 0123456789012 via 123456789 in order to regain ac
cess to your files.

17beb6657723cfcc38638e6c517cecdaede175a2ffba91803b877c24
48837a787f07673545d9c610bcbcd8d46a2691a71966d856c197e69e
b786ae76f7a7c69f2135a2b516972223feefeca2f3e81ecd19e3f318
48837a787f07673545d9c610bcbcd8d46a2691a71966d856c197e69e
3caf6cfa418495d9b9920a3d107c74291dafb837525df6c94ec17e2c
48837a787f07673545d9c610bcbcd8d46a2691a71966d856c197e69e
48837a787f07673545d9c610bcbcd8d46a2691a71966d856c197e69e
ada5109f8c945ed73b9623d5e33fbfa80c7622de352bada8f0fd337d
48837a787f07673545d9c610bcbcd8d46a2691a71966d856c197e69e
d48130d54d3866b00a96de5b47d923dcbbcc1dd173a9d31b5bb0beb5
48837a787f07673545d9c610bcbcd8d46a2691a71966d856c197e69e
18e3c1bfc84885430790cb970abc8ee5d268a294a7c9e9edc4ee1af5
48837a787f07673545d9c610bcbcd8d46a2691a71966d856c197e69e
9ea0bca92e9457d5885000df1c8a6d3c94a6e439446c549ad8c06e5f
48837a787f07673545d9c610bcbcd8d46a2691a71966d856c197e69e
4ea204c19daded2d013d9952ae2fa71184fefaa03e87ddbb8596fb98
48837a787f07673545d9c610bcbcd8d46a2691a71966d856c197e69e
48837a787f07673545d9c610bcbcd8d46a2691a71966d856c197e69e
5a46efef113eb78f7b28b79b03e8977c7599c7718d10c81fd1de4811
```

5. What do you think happened? Can you convert the files back to their original form?

6. Open the file scan_directories.py with your favorite text editor. My favorite is vim, but a simpler editor would be nano:

```
nano scan_directories.py
```

. What do you think this code is doing?

7. Should you run a file that someone sent you on an email, even if this looks like a file sent by your manager/instructor/ someone you know? **Why?**