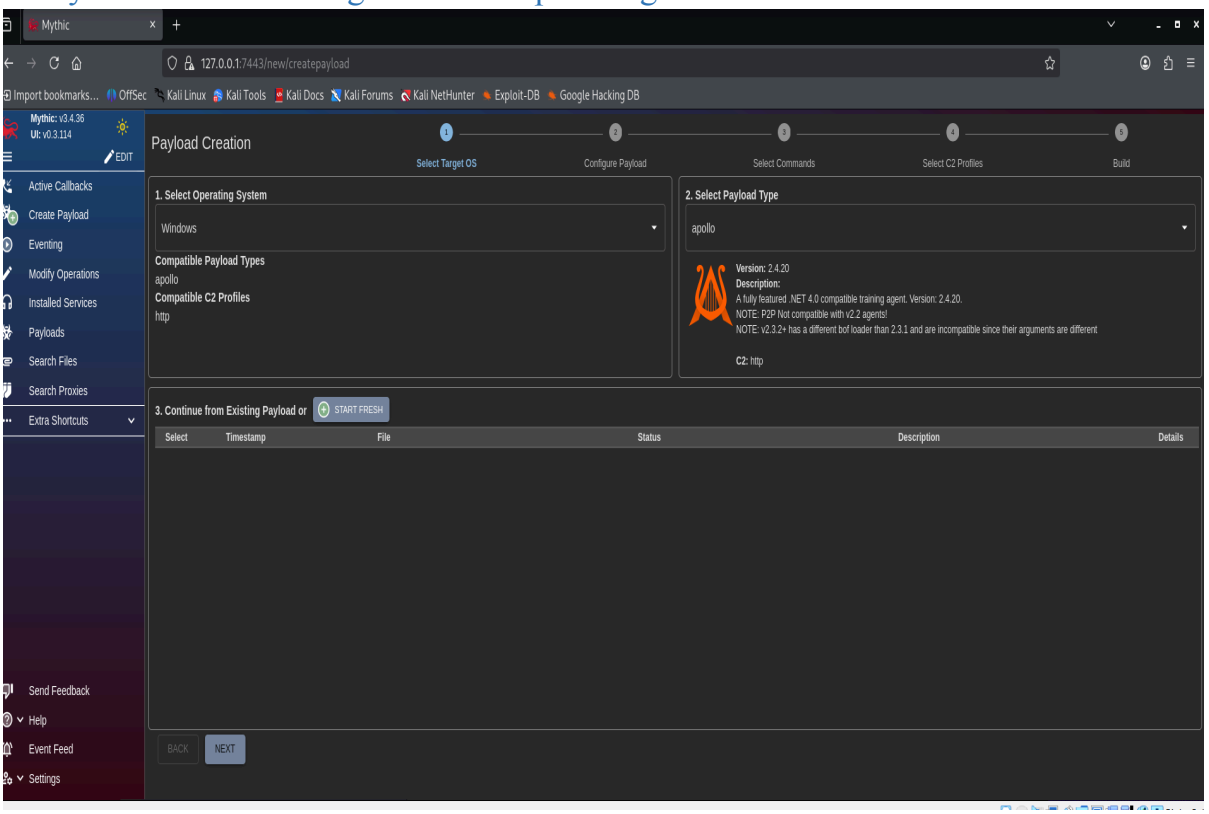
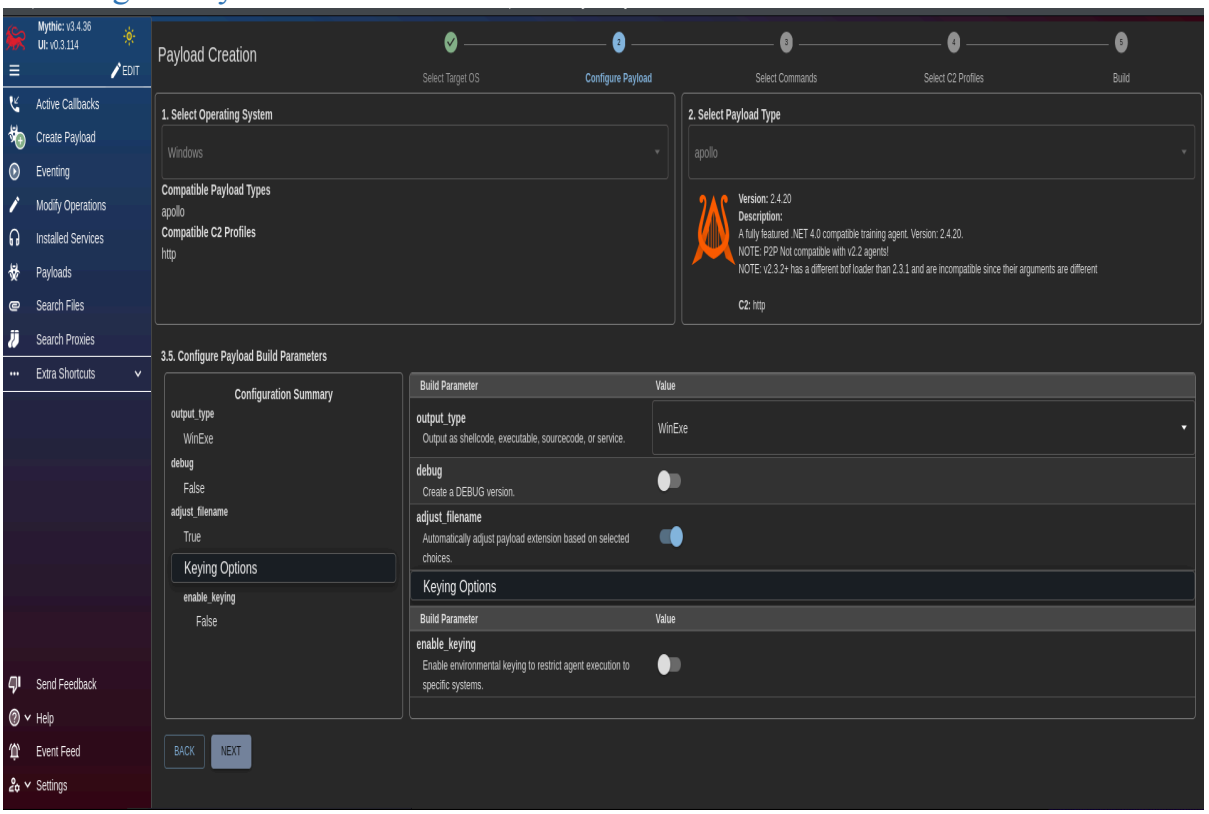
Windows 11 VM Pentest Report
Using Mythic C2 Framework with Apollo Payload

So Basically I had big issue with silver C2 and decided to try Mythic C2 Framework instead much mire modern and a clean easy to use GUI. The next load of images are just me using the default options for creating a payload. Note that IP's have changed as my firewall vm was not allowing my other VM's to connect to the internet so I bypassed it for now as its not the point of this exercise.

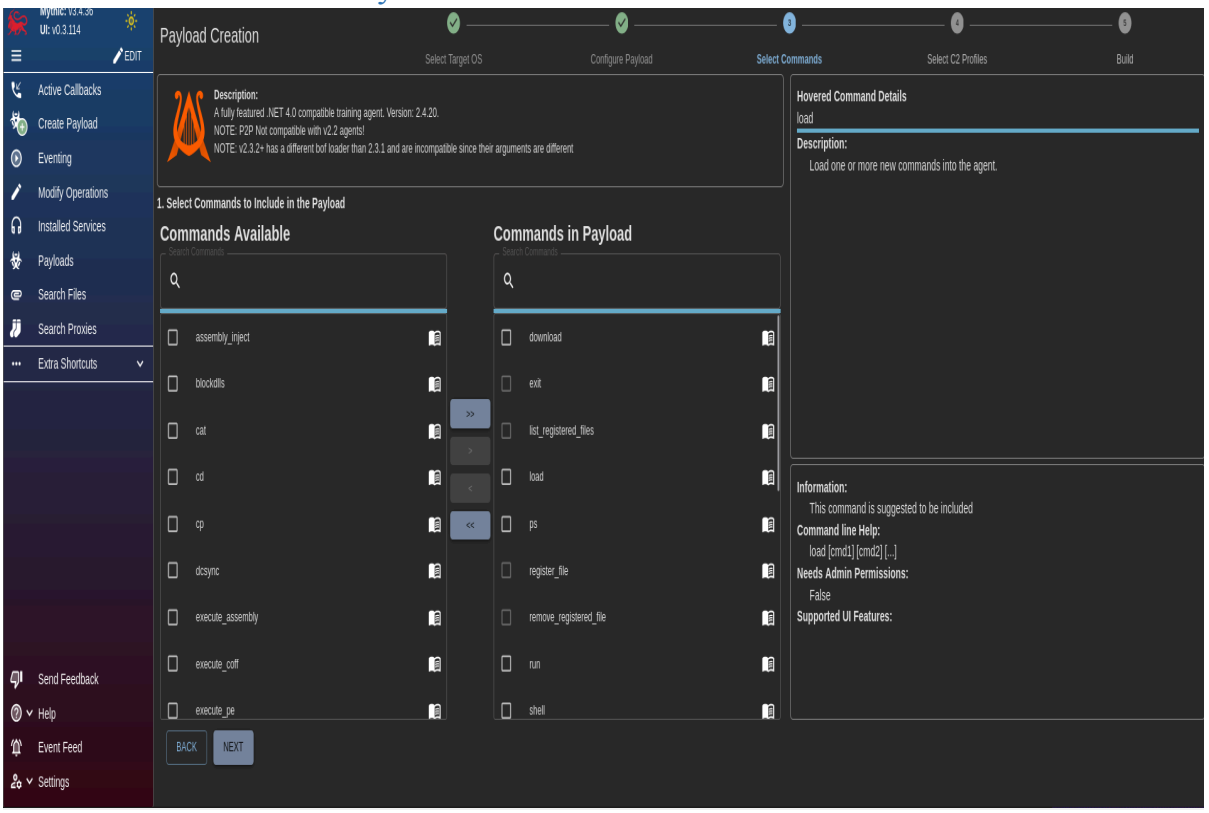
1. Payload Creation - Target OS and Apollo Agent



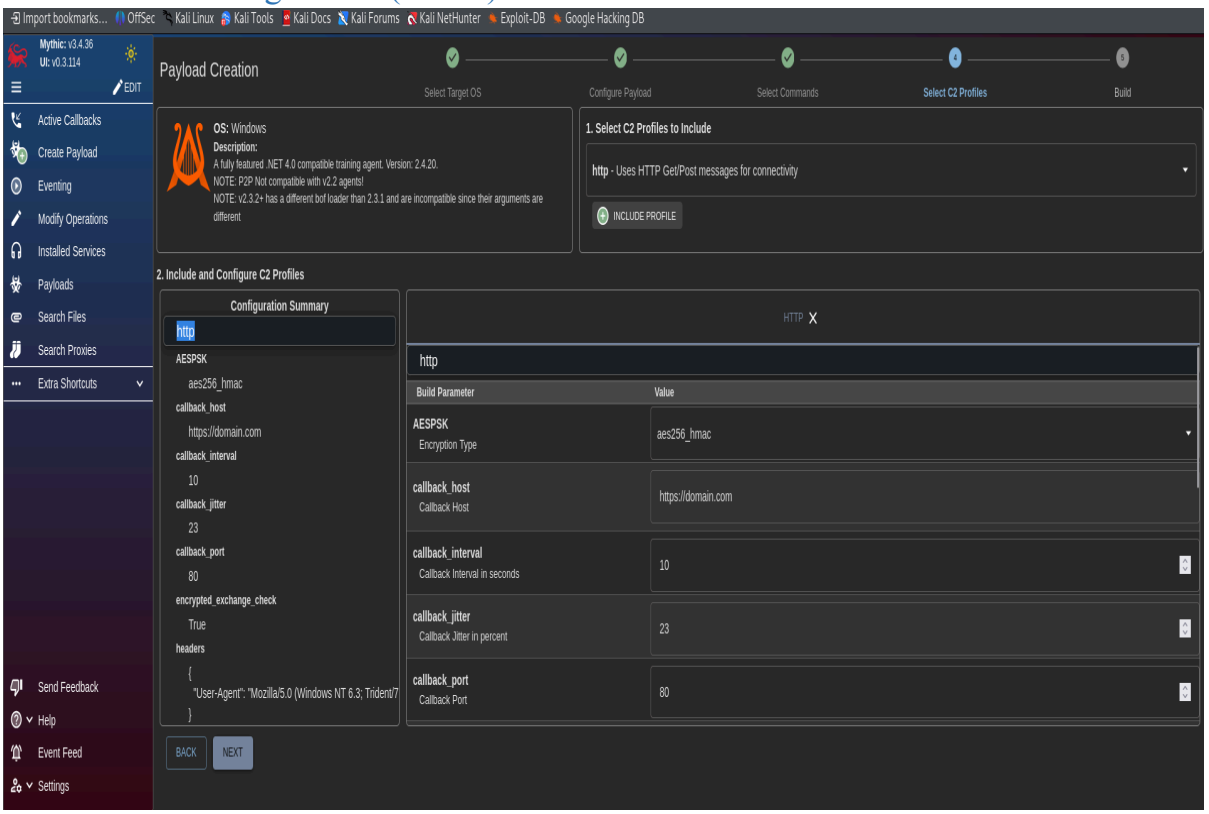
2. Configure Payload Build Parameters



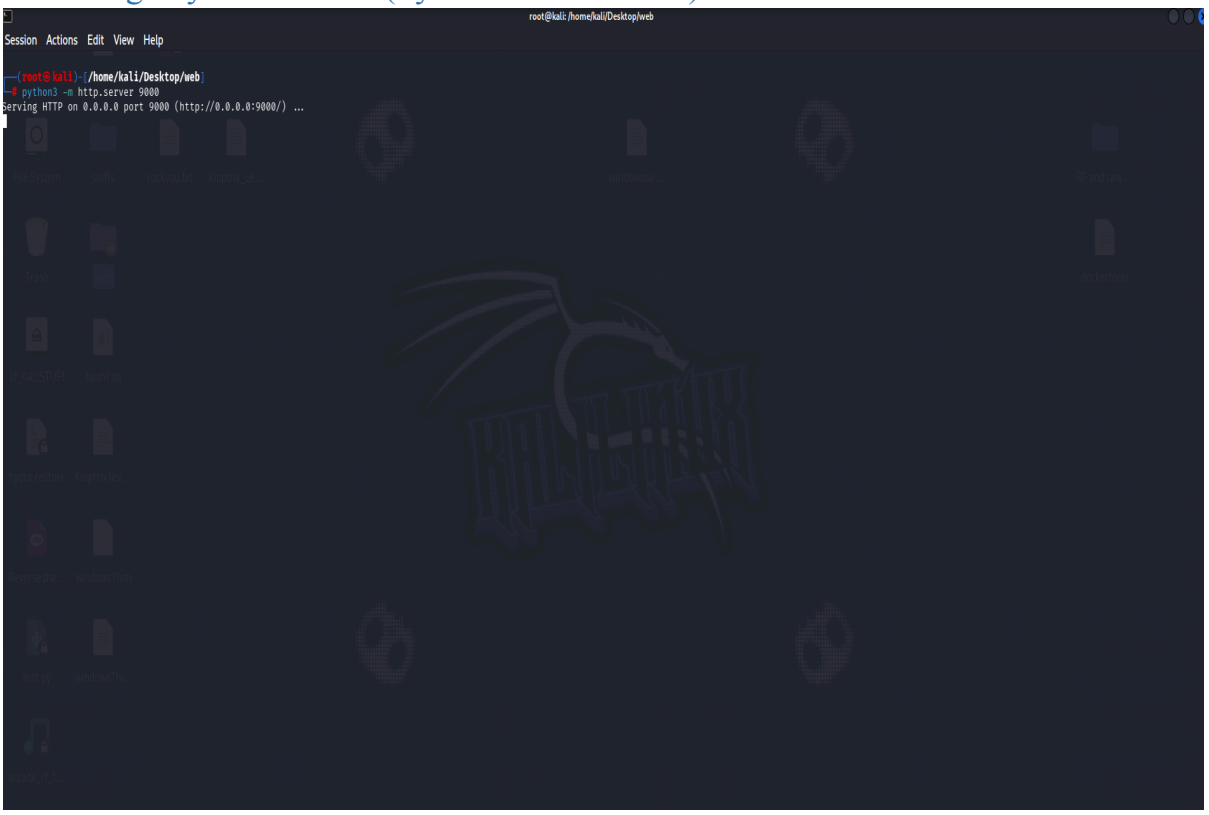
3. Select Commands for Payload



4. C2 Profile Configuration (HTTP)

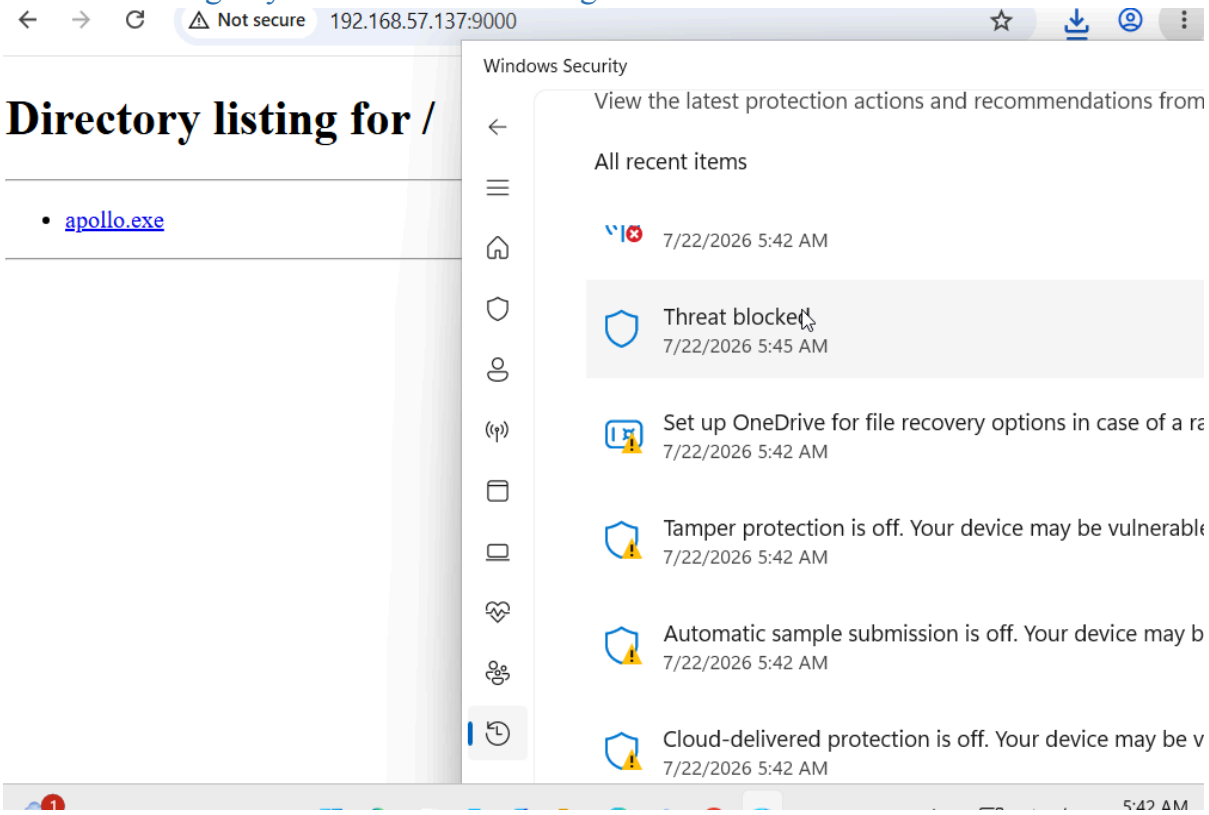


5. Hosting Payload on Kali (Python HTTP Server)



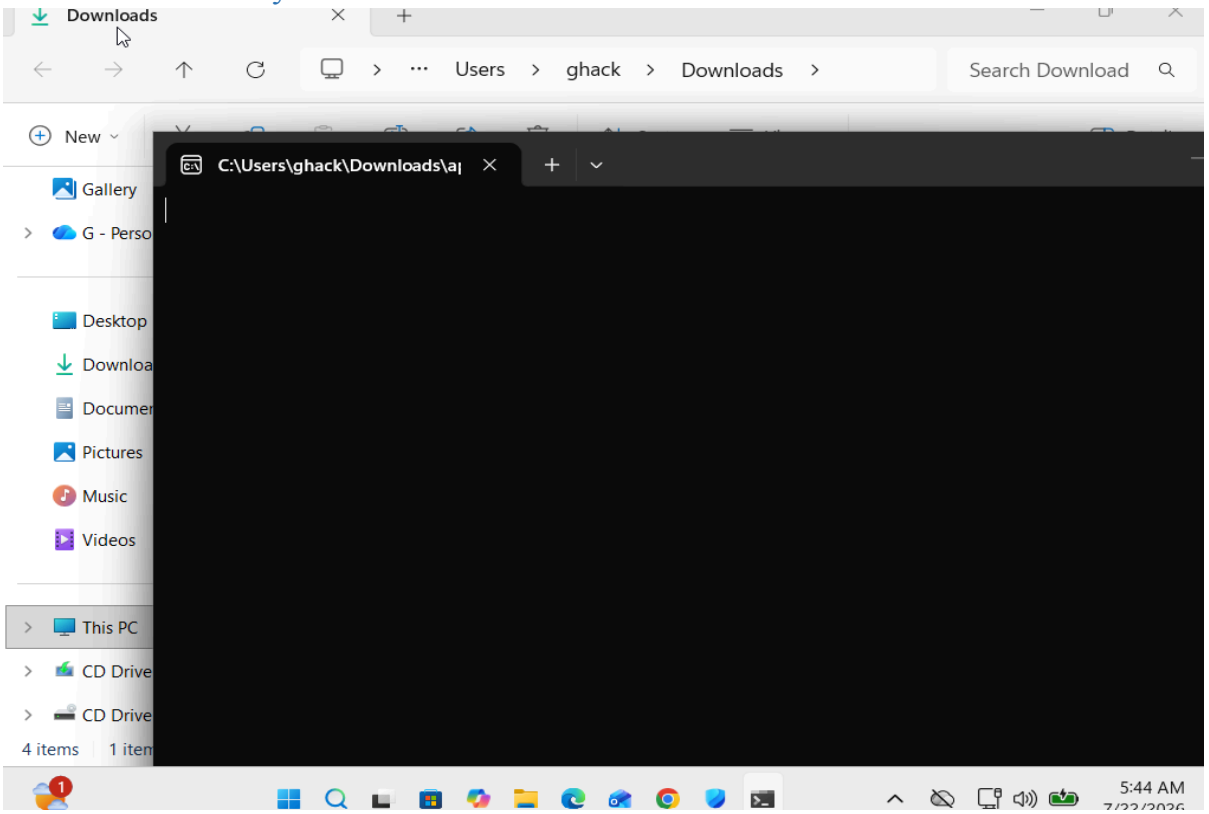
Its a bit old fashion throwing it up on a python server but its just about learning new tools at this point.

6. Downloading Payload on Windows Target



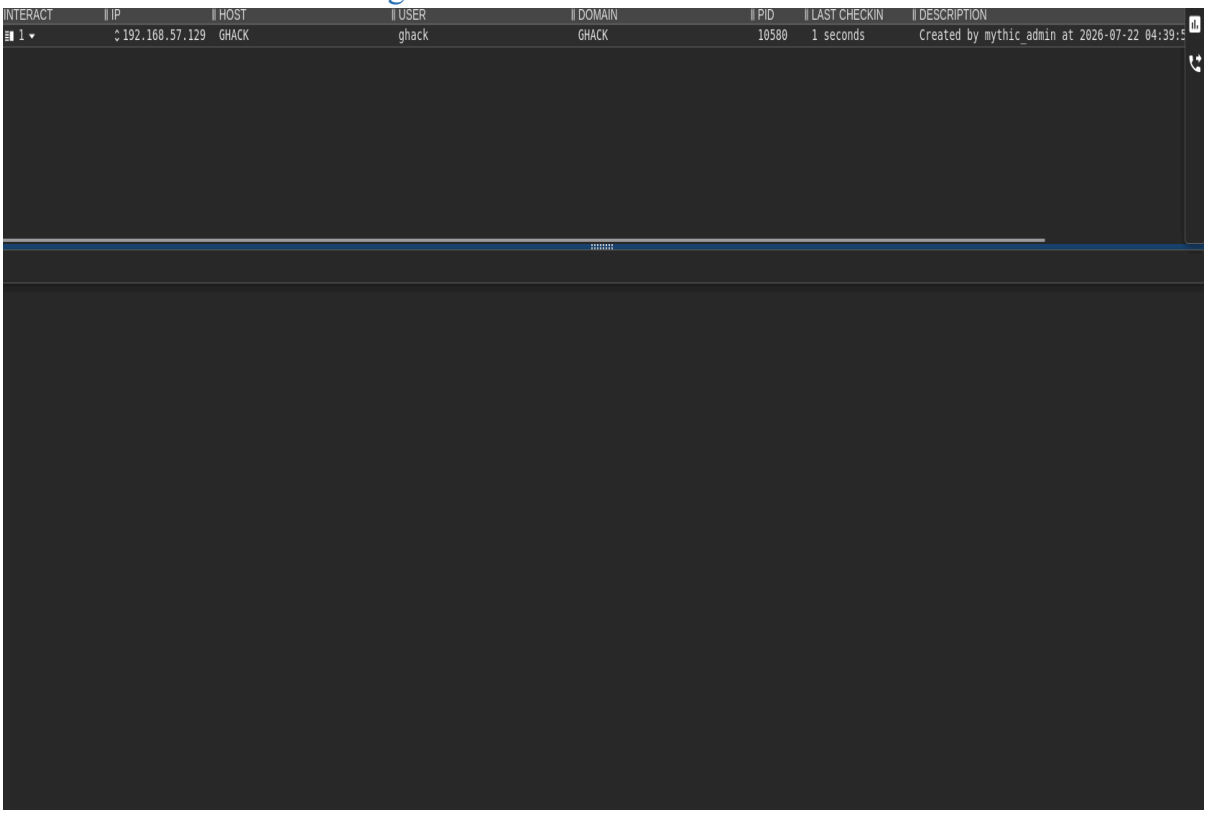
So as expected windows and browser firewall blocked but just for now prententing to be a unsafe user I stop all antivirus and continued to download the payload

7. Windows Security Alerts



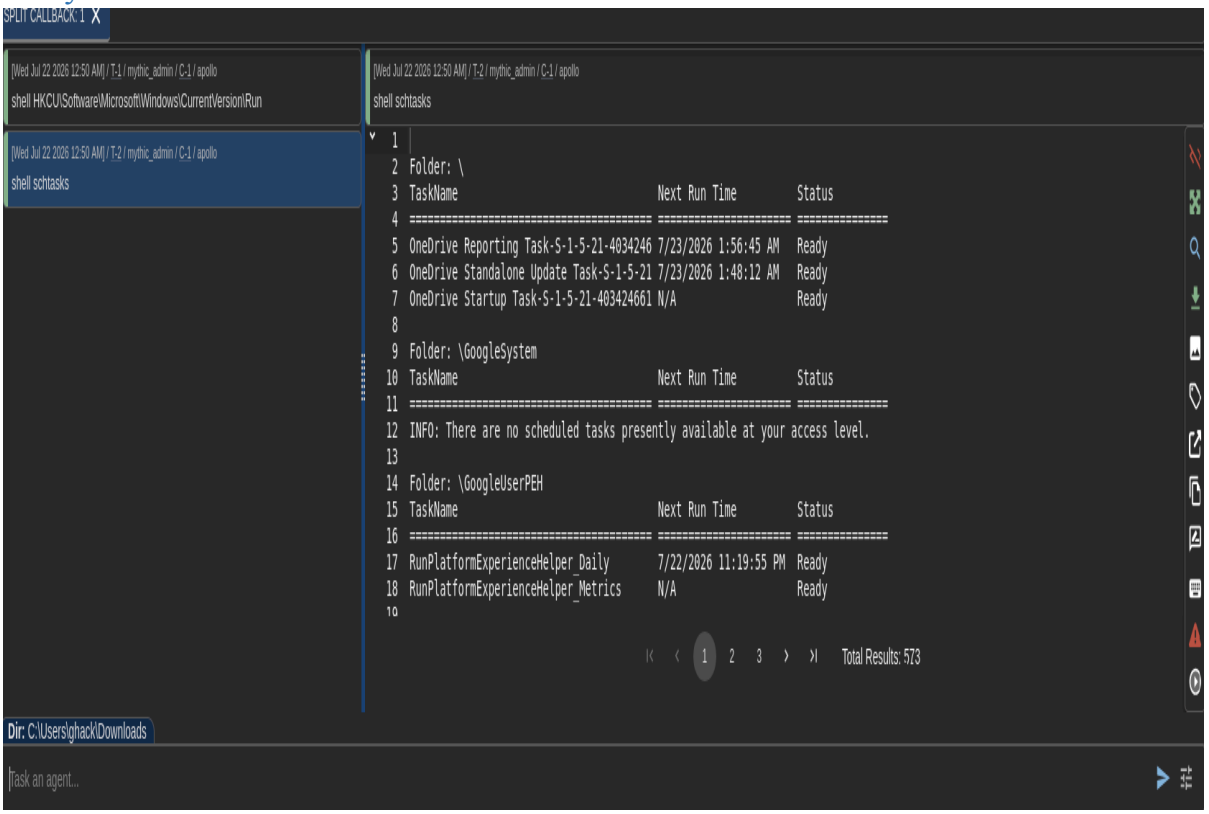
Now this led me to believe it failed as normally I might see something and then it would close the window in a flash however…

8. Downloads Folder on Target

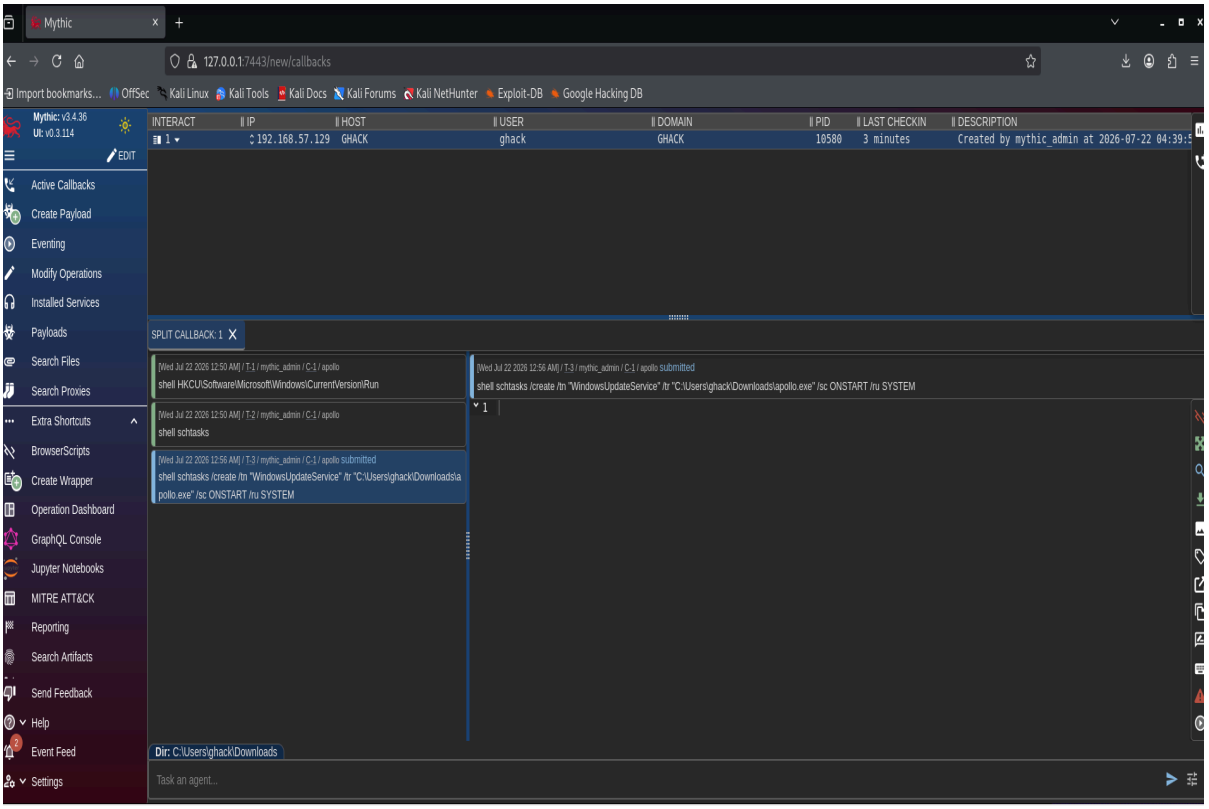


Bingo I got a hooker now to see how to use this C2

9. Mythic Callback Established



10. Persistence via Scheduled Task



After some messing around and some research each command that I want to send to windows needs the shell before it. I tried some typical scheduling persistence but not much luck. It would be easier to just make a user but that would stick out like a saw thumb. But getting in with method did quite well just need a way to obscate the payload so it wont get blocked or deleted by anit virus. Which is constant theme.