National Telecommunication Institute

Remote Access Trojan (RAT) Spyware

-

Report

Prepared by: Ahmed Moataz Abdelmonem Elrefaey

National Telecommunication Institute

These are my steps which I did:

- I shared the folder (malware threats) which contains the rat tool and installs & running it in attacker pc (builder/handler) at desktop

- open windows firewall with advanced security then creates new rule from inbound rules then make the port 1337

- Then in NJRat tool I set the builder host 192.168.174.137 and the port 1337 then click build to build the malware and create the file server.exe on desktop

- Now I can make the folder and share it with victim machine (client)

- On victim machine searching about sharing folder (sharing_folder) on windows explorer about \\192.168.174.137\sharing_folder

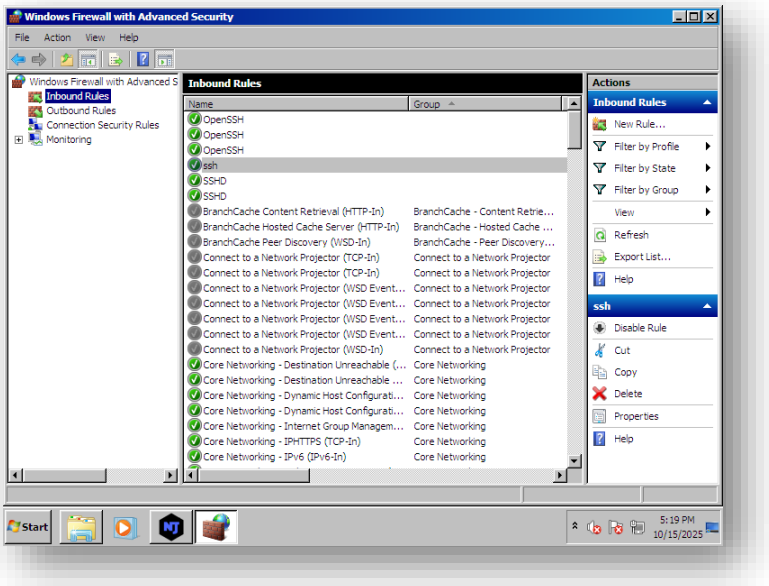
- Then the sharing folder is open, copying the malware and setting it in desktop and double click on it

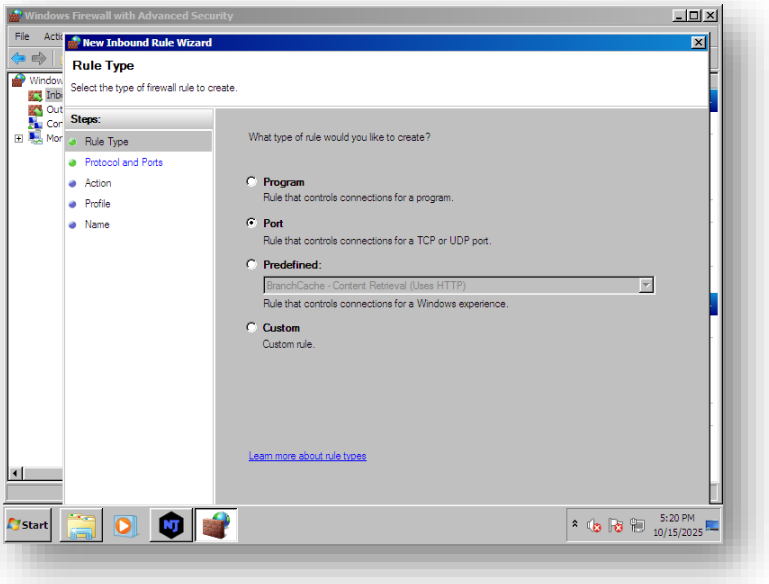
- As you double click on it, the tool (njrat) on attacker machine will listen and now you have access to victim machine (client) and I can use the tool for different usages.

National Telecommunication Institute

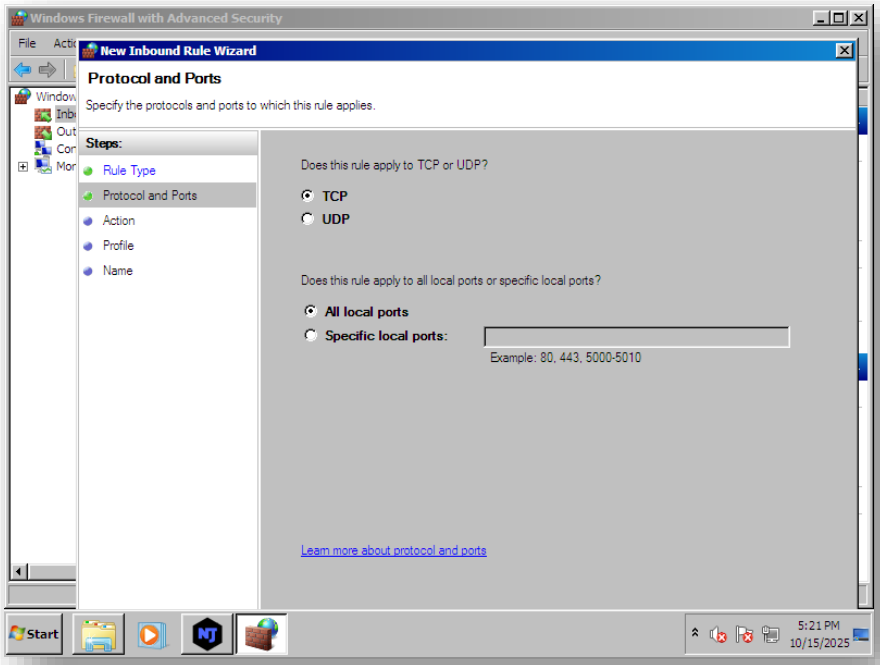
Now I will show the steps which I did it:

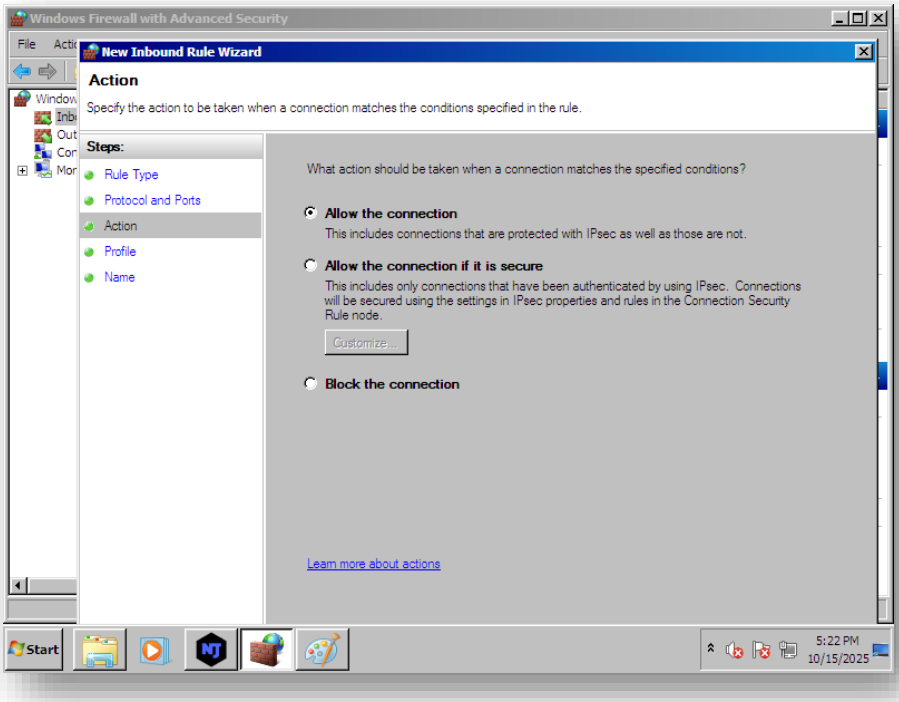
- I shared the folder (malware threats) which contains the rat tool and installs & running it in attacker pc (builder/handler) at desktop.
- open windows firewall with advanced security then creates new rule from inbound rules then make the port 1337.



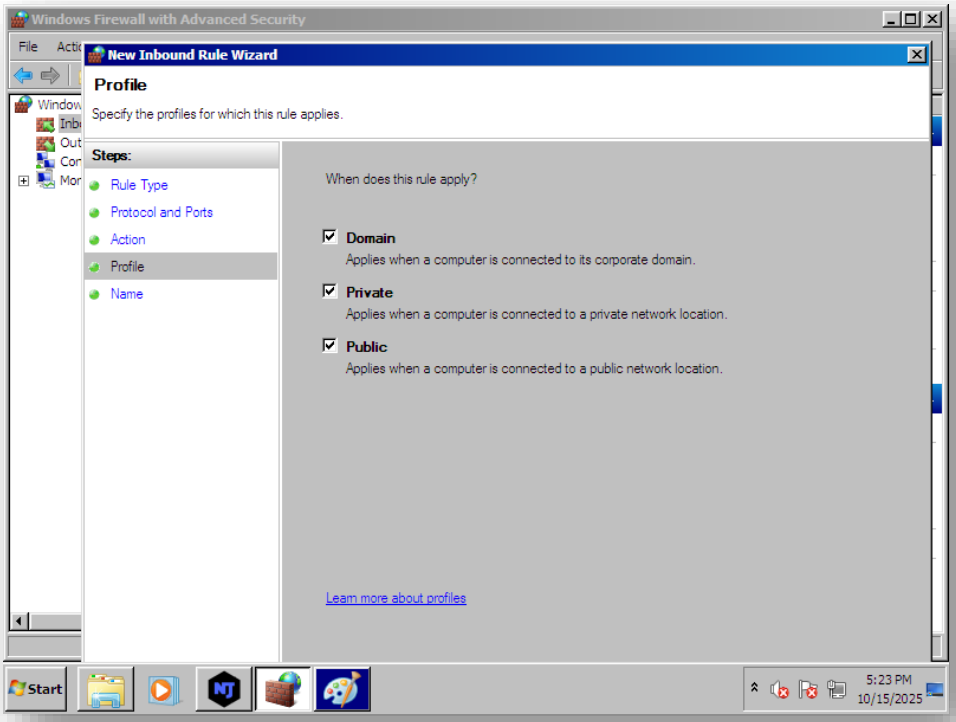


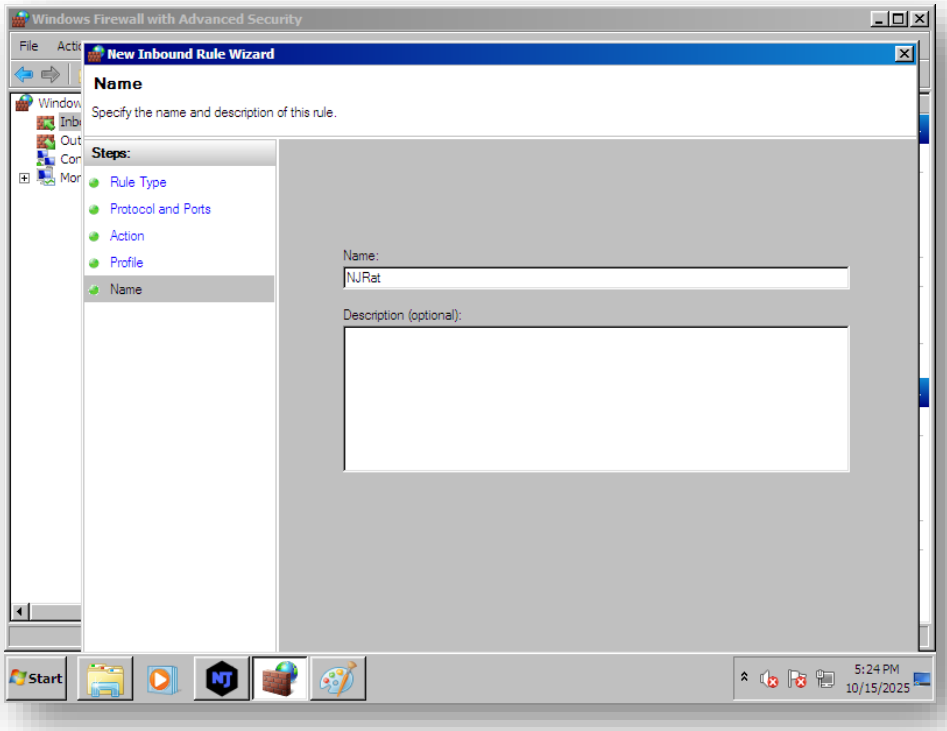
National Telecommunication Institute



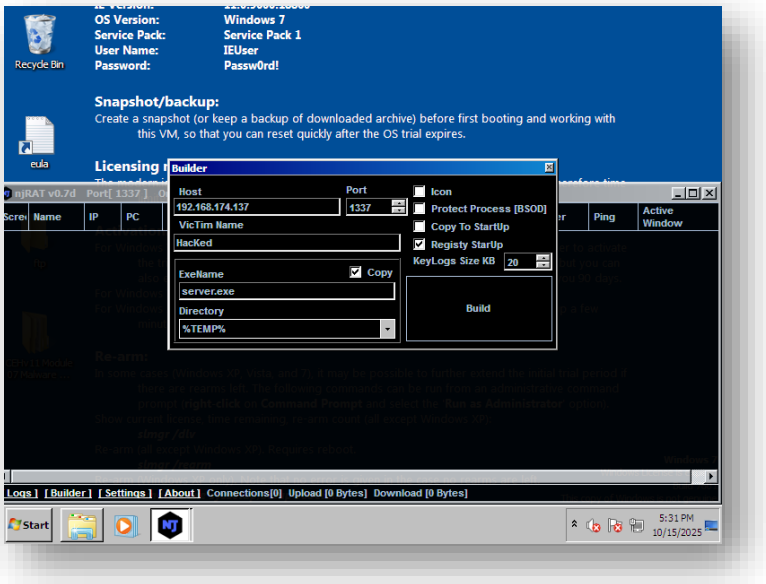


National Telecommunication Institute

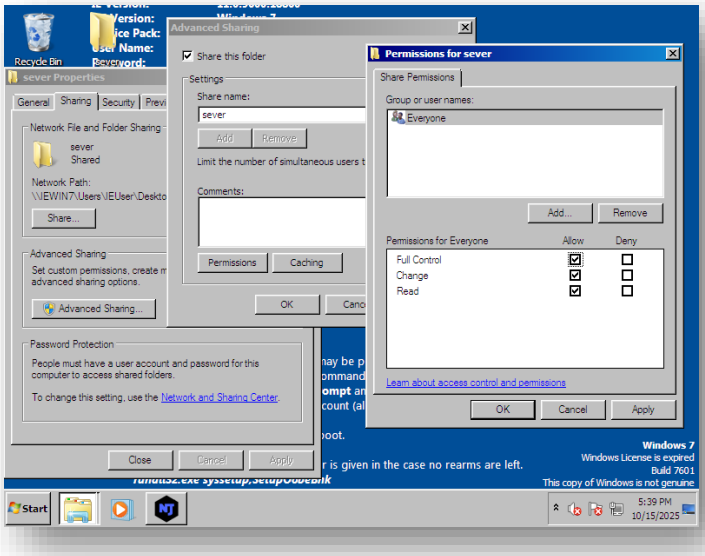




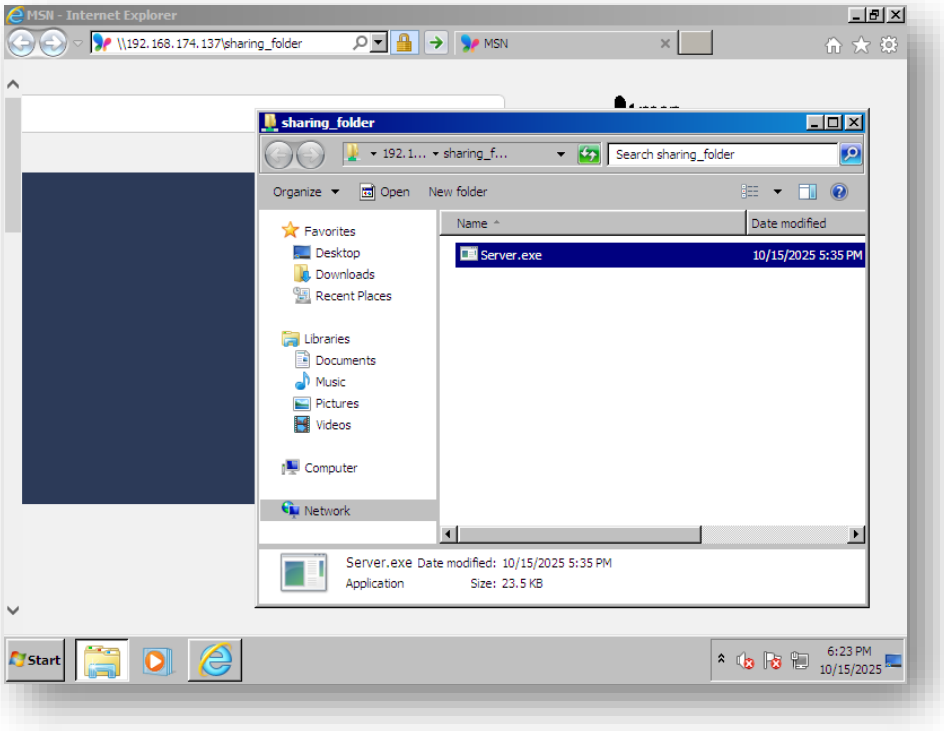
- Then in NJRat tool I set the builder host 192.168.174.137 and the port 1337 then click build to build the malware and create the file server.exe on desktop



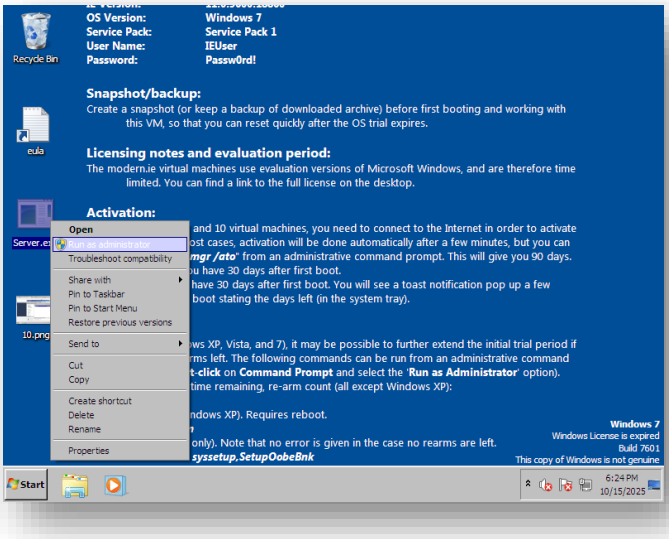
- Now I can make the folder and share it with victim machine (client)



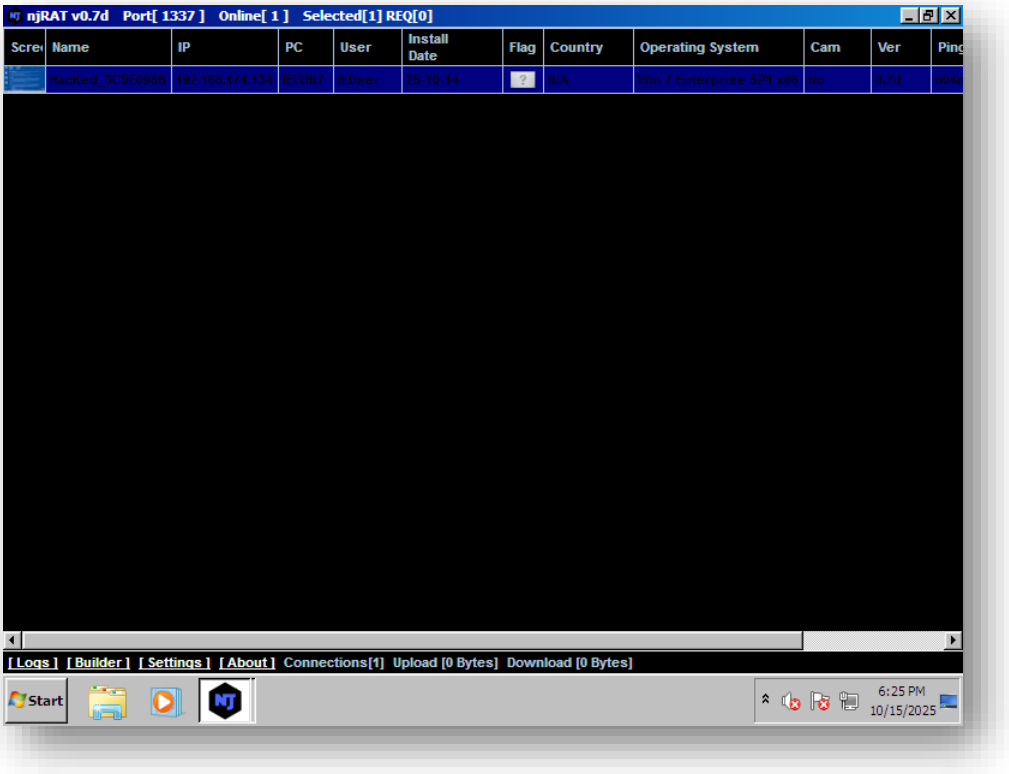
- On victim machine searching about sharing folder (sharing_folder) on windows explorer about \\192.168.174.137\sharing_folder



- Then the sharing folder is open, copying the malware and setting it in desktop and double click on it



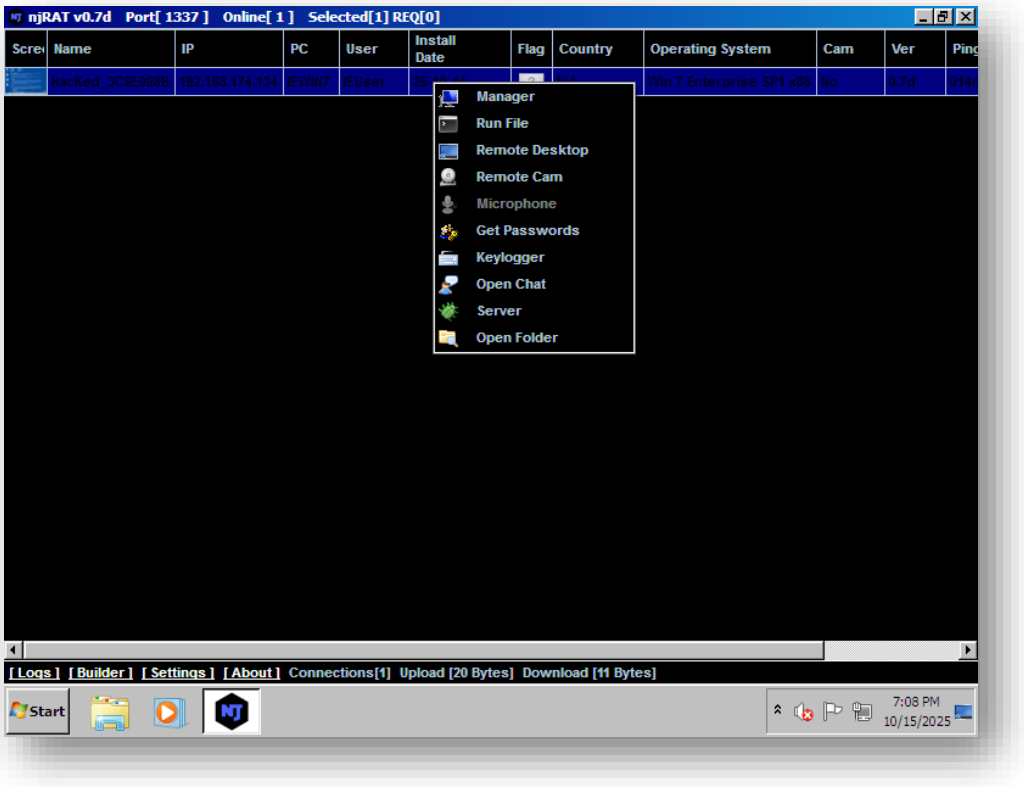
- As you double click on it, the tool (njrat) on attacker machine will listen and now you have access to victim machine (client) and I can use the tool for different usages.



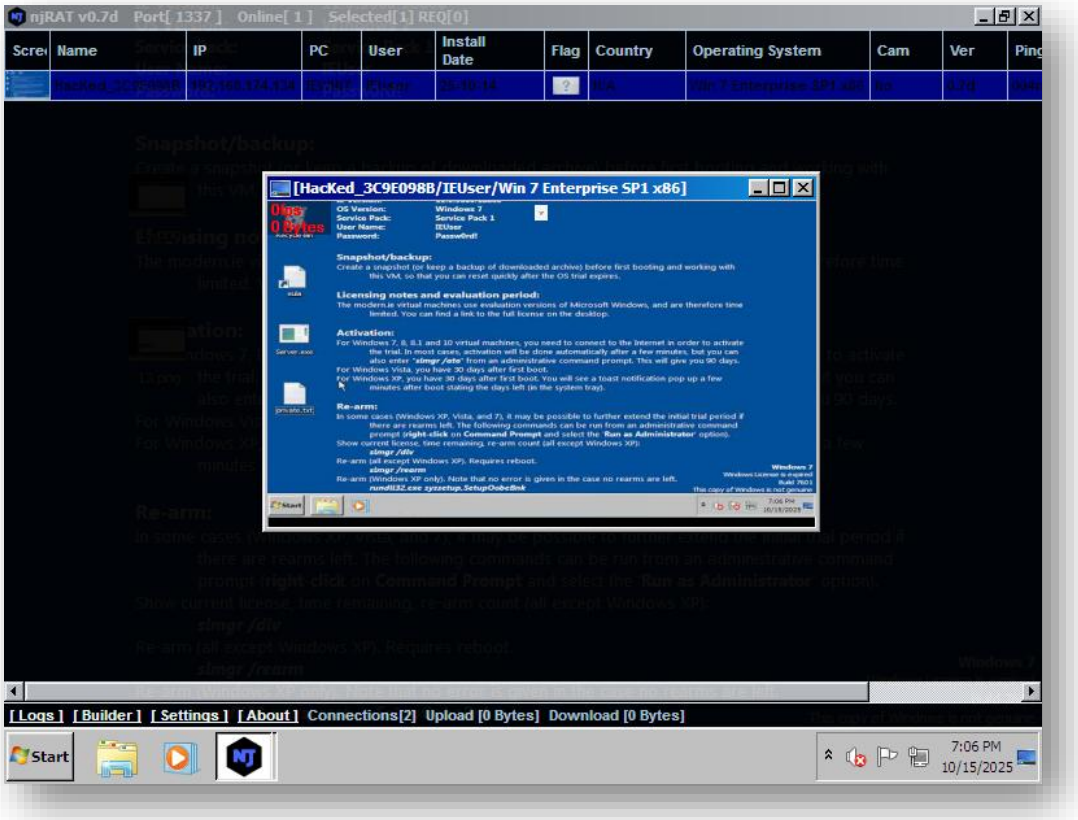
Here we can find the **OS version** and the **username** of the victim machine (client)

- OS version: **Win 7 Enterprise SP1 x86 (0.7d)**
- User: **IEUser**

- Once I double click, it will appear a list of action like (manager, run file, remote desktop, ….) as the image shows and I will try some of these actions at next steps



- I will try remote desktop and keylogger in this step
  - After clicking on remote desktop this will show the victim machine and what he does right now.



- If the victim made a notepad and saved any secret or private strings in it these strings will show on keylogger.
- If the victim visits any website and logs in to any website this will show in keylogger.
- And you can search about any string like (user, pass, secret, private, ….) once you write the specific word in the tap next to **FIND** after this click FIND and will get the filtering.