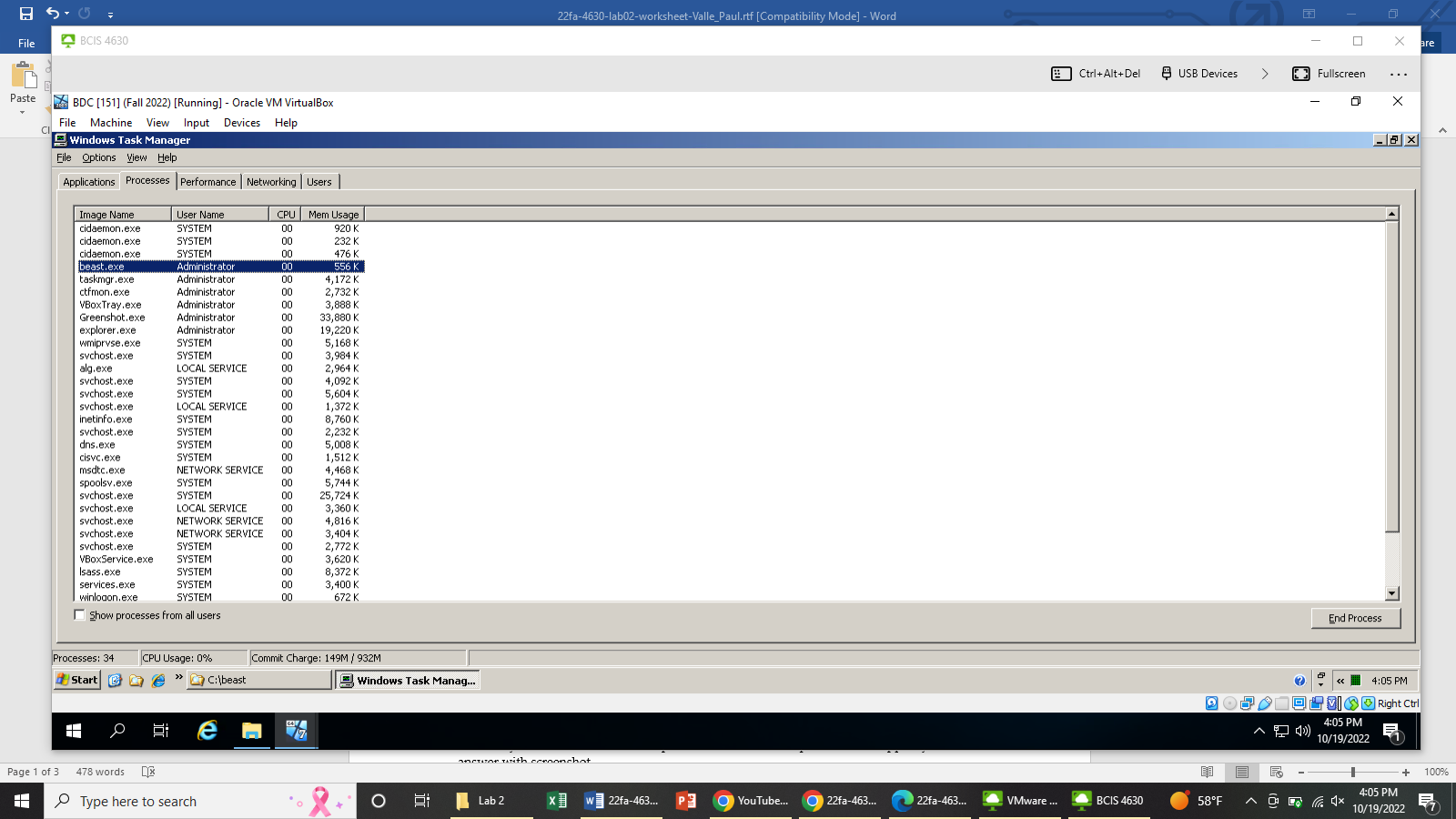
Name: Paul Valle

**BCIS 4630 Lab 2 Worksheet**

***Important hint***: In this lab, you’ll report outcome from running Task Manager, netstat, and File Explorer multiple times. Some processes, ports, and folders/files appear in the output at some points but may not at other times, depending on whether the Trojan and/or rootkit is running. Therefore, take screenshots and answer the questions **based on what you actually see but not on what you think you should see**. Some questions below ask you to compare the output from different points in time so that you can see the effects of Trojan and rootkit. That said, if a process, port, or folder/file is missing from the output throughout the entire lab, then something is amiss, and you want to contact your instructor about it.

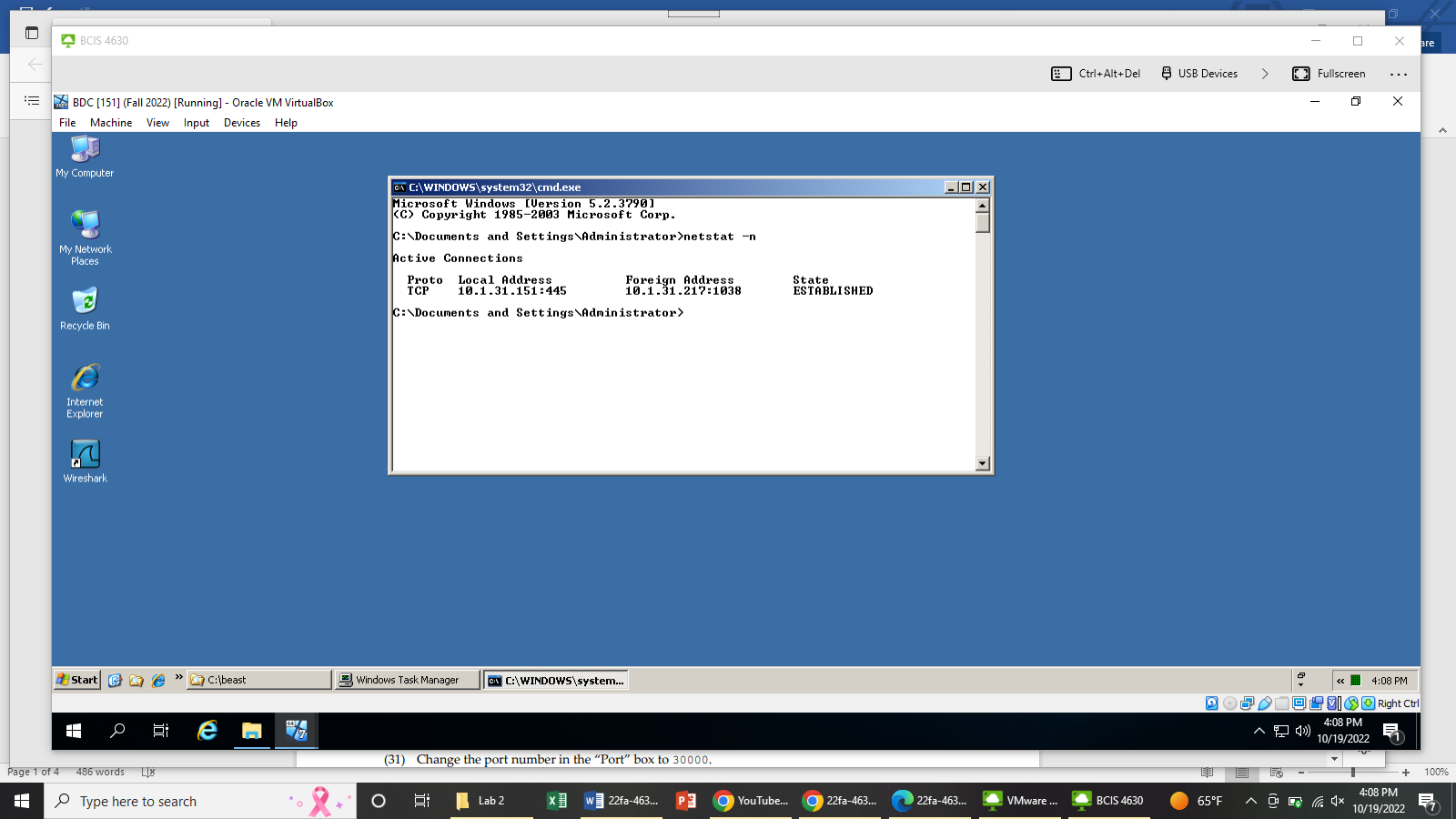
**Question 2.1**

2.1.1. Do you see “beast” in the process list? Support your answer with screenshot.



Yes, “beast” did show in the process list.

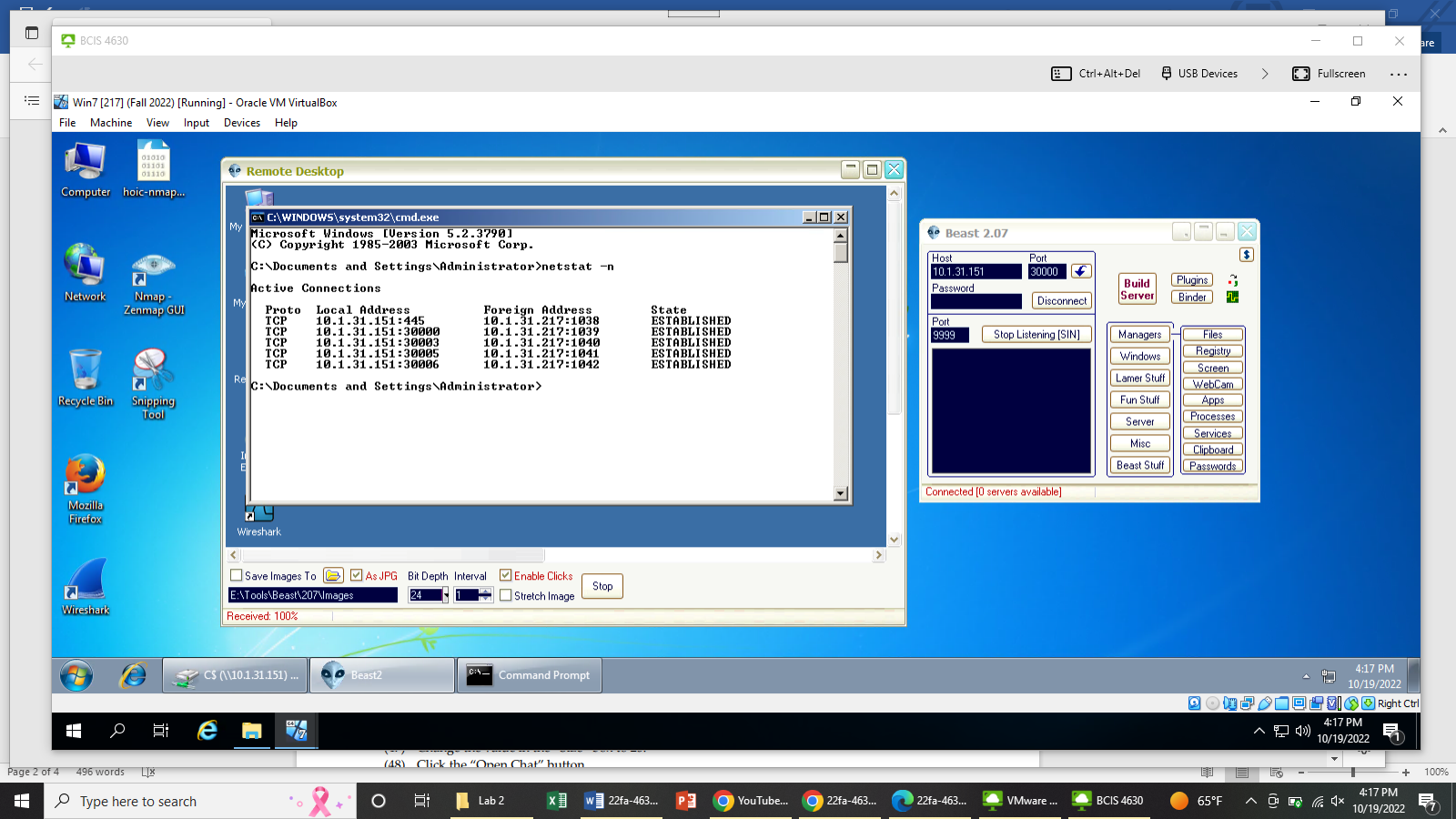
2.1.2. What are the open ports on the victim computer now? Support your answer with screenshot. Focus on only those entries starting with TCP and the 10.1.xx.151 address.



The open port on the victim computer is Port #445.

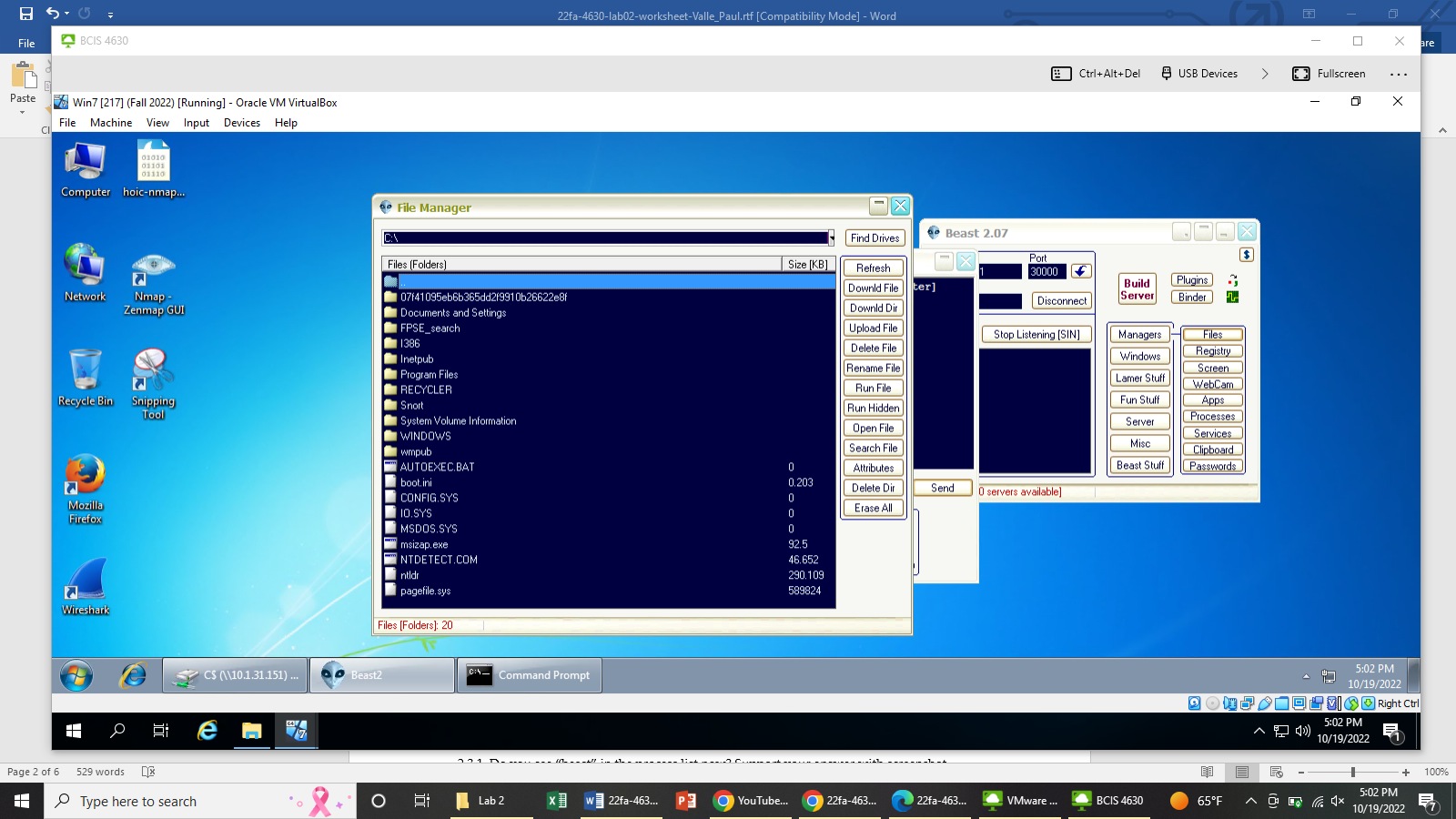
**Question 2.2**

2.2.1. Do you see the victim’s desktop in the “Remote Desktop” window? Support your answer with screenshot.



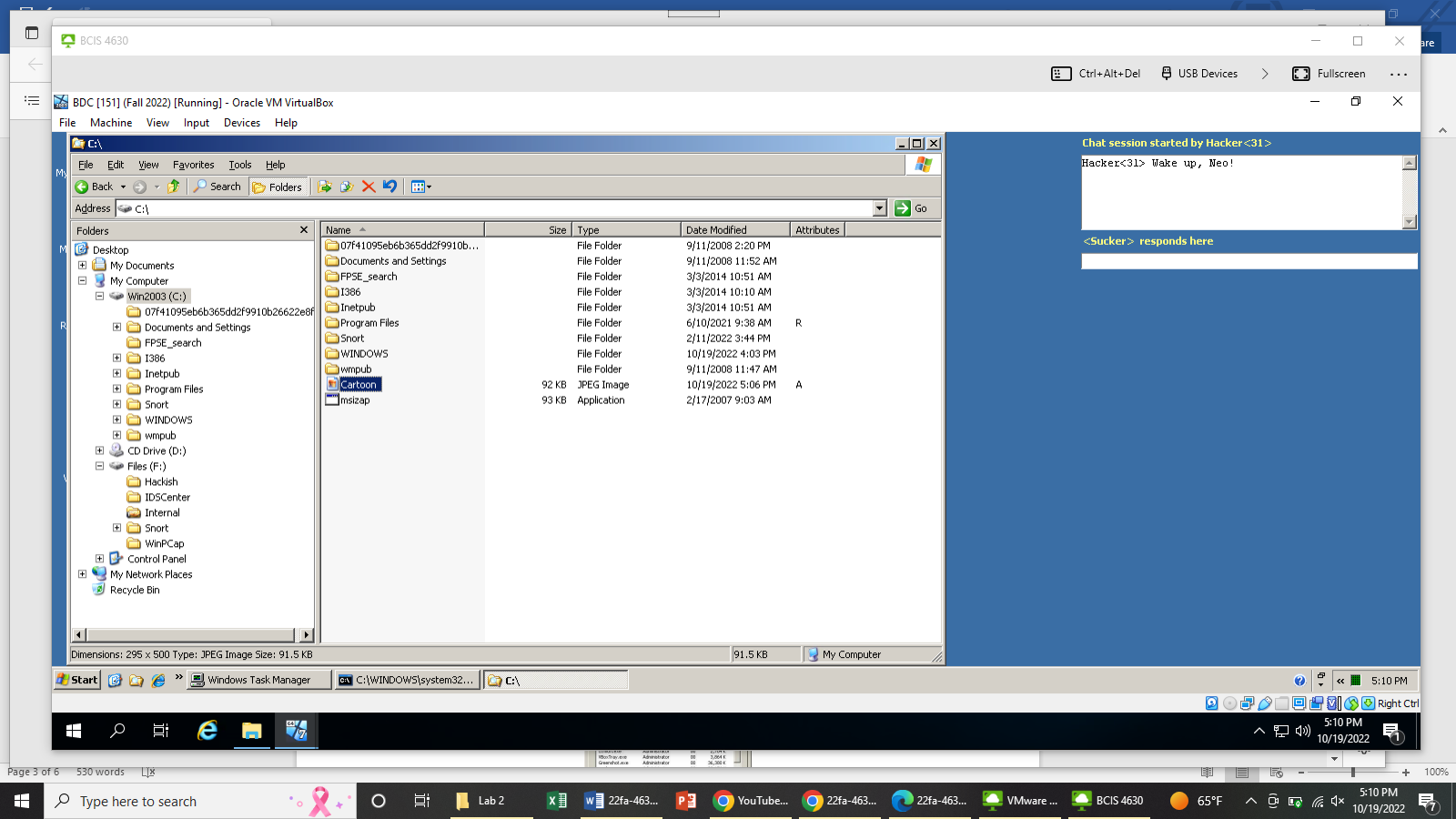
Yes I did the see the victim’s desktop in the “Remote Desktop” window.

2.2.2. Do you see the contents of the C: drive on the victim machine? Support your answer with screenshot.

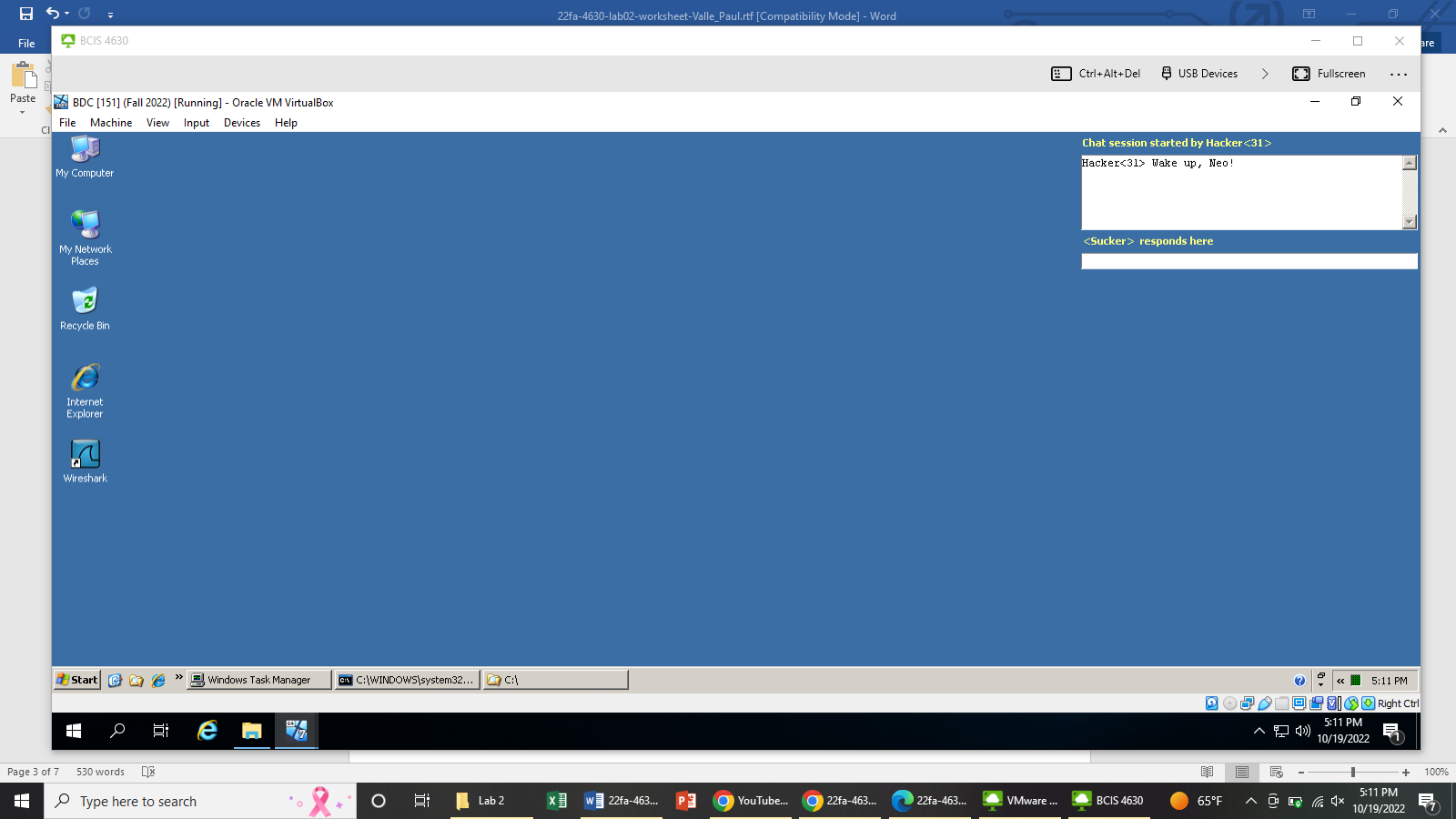


Yes.

2.2.3. Show the success of uploading Cartoon.jpg with the Windows Explorer screenshot you took.

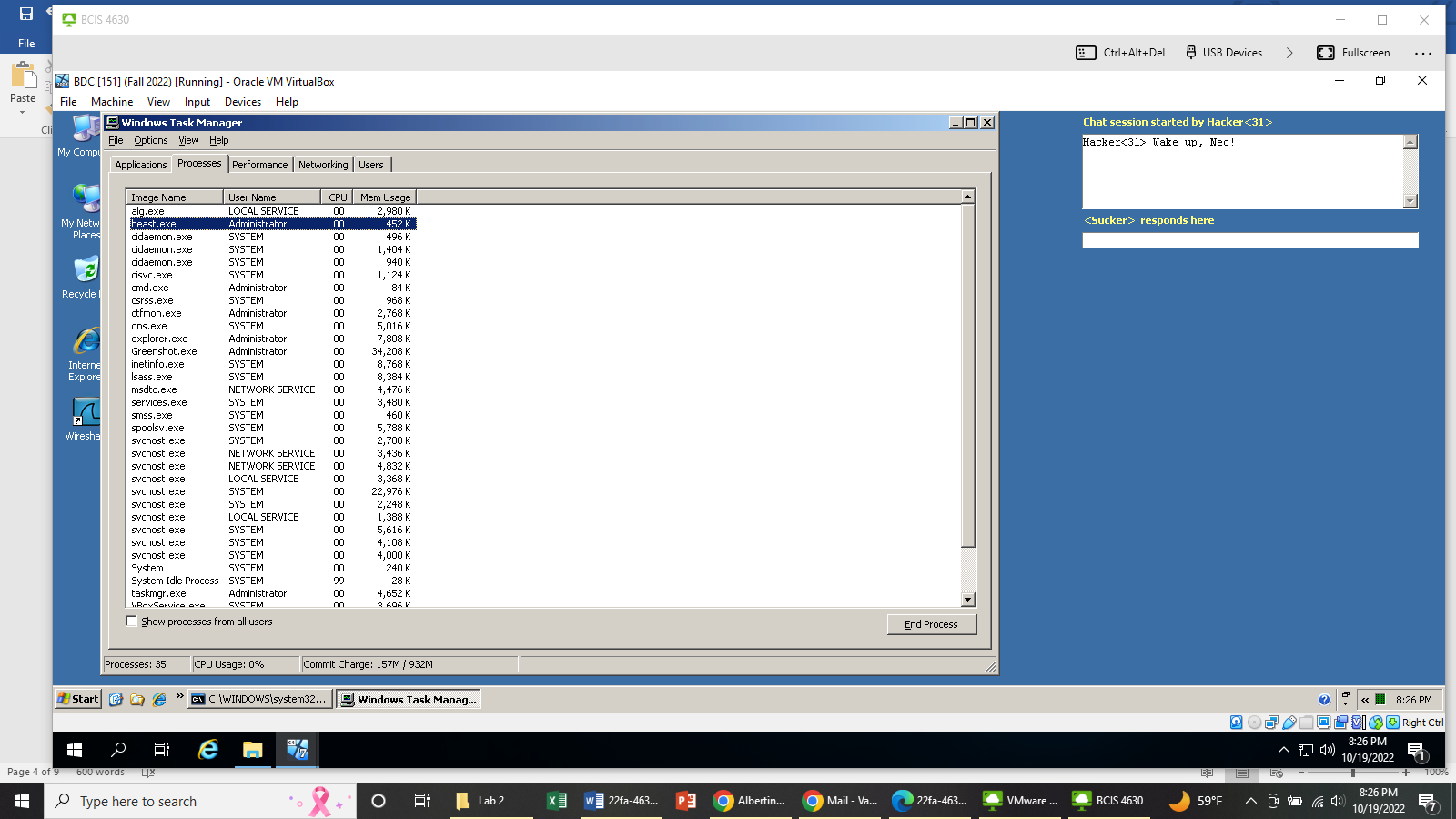


2.2.4. Insert the screenshot of the chat window below.



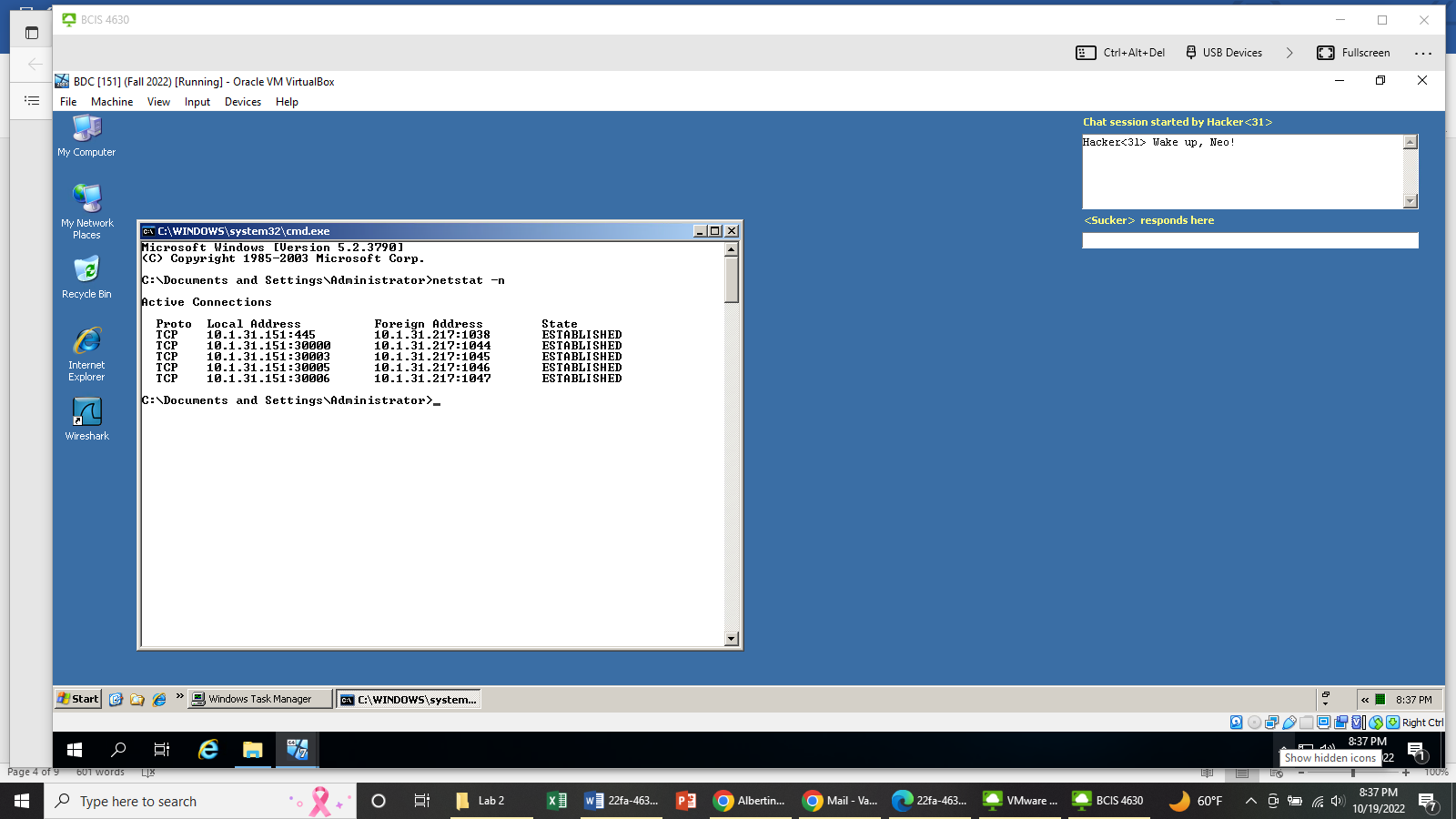
**Question 2.3**

2.3.1. Do you see “beast” in the process list now? Support your answer with screenshot.



Yes.

2.3.2. Compared with 2.1.2, what new open ports do you see on the victim computer now? What is the IP of the remote computer that is connected to those newly-opened ports? Support your answer with screenshot.



Ports 30000, 30003, 30005, and 30006 are new open ports. The IP address of the remote computer that is connected to the newly opened ports is 10.1.31.217.

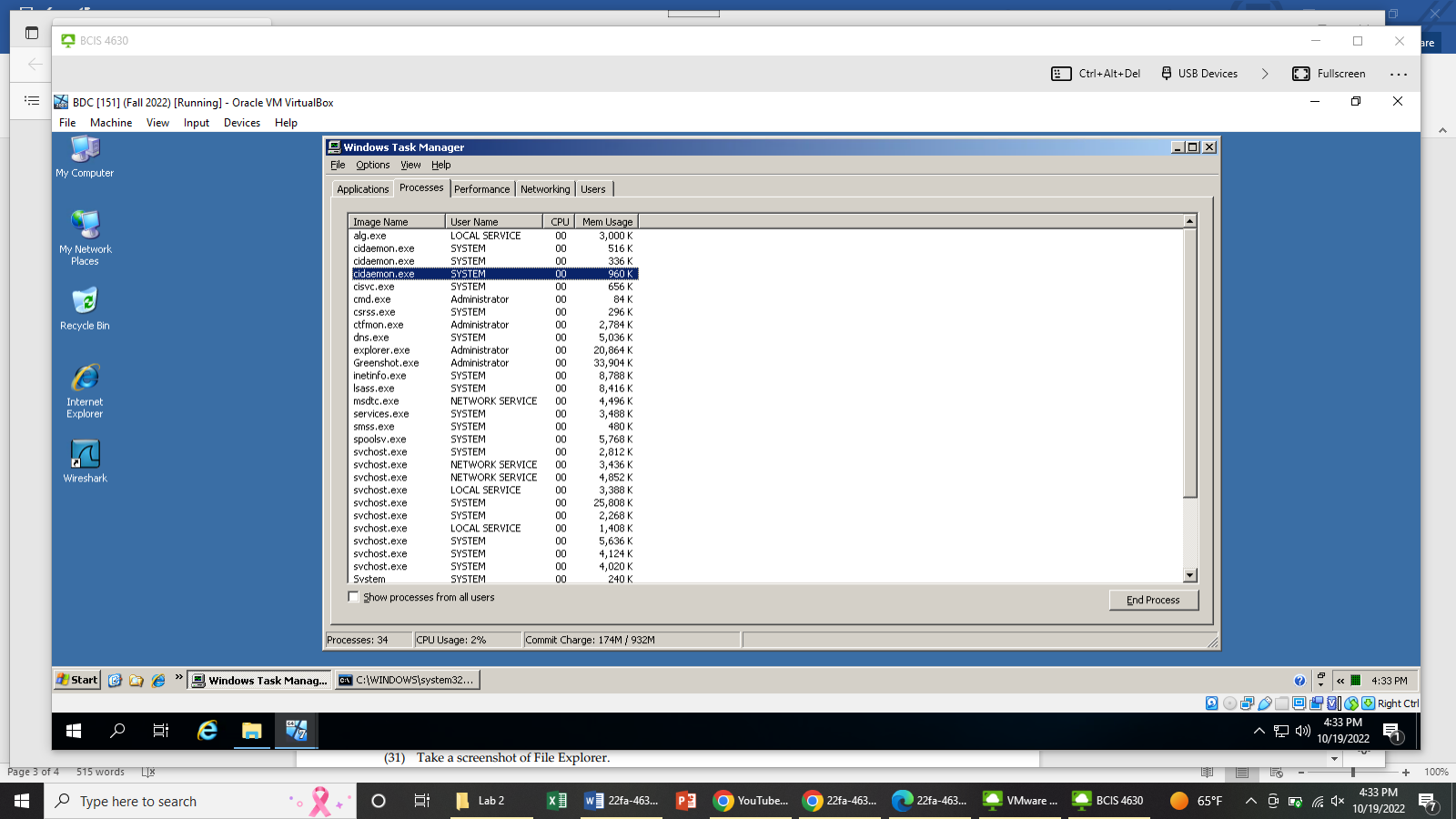
**Question 2.4**

2.4.1. Do you see beast.exe in Task Manager’s process list?

Yes

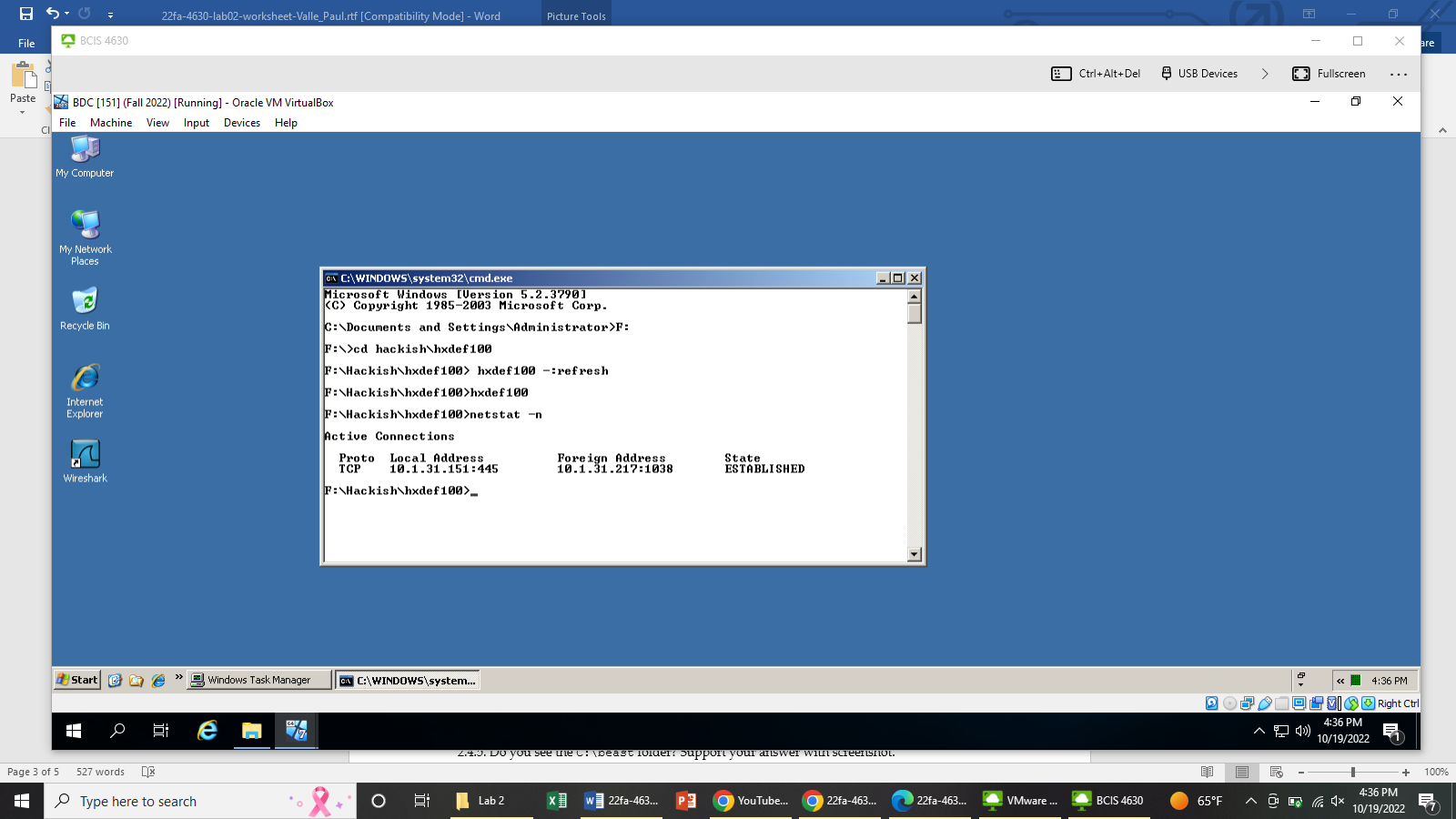
2.4.2. What ports are open for the Beast Trojan?

30000, 30003, 30005, 30006

2.4.3. Do you see beast.exe in Task Manager’s process list now? Support your answer with screenshot. 

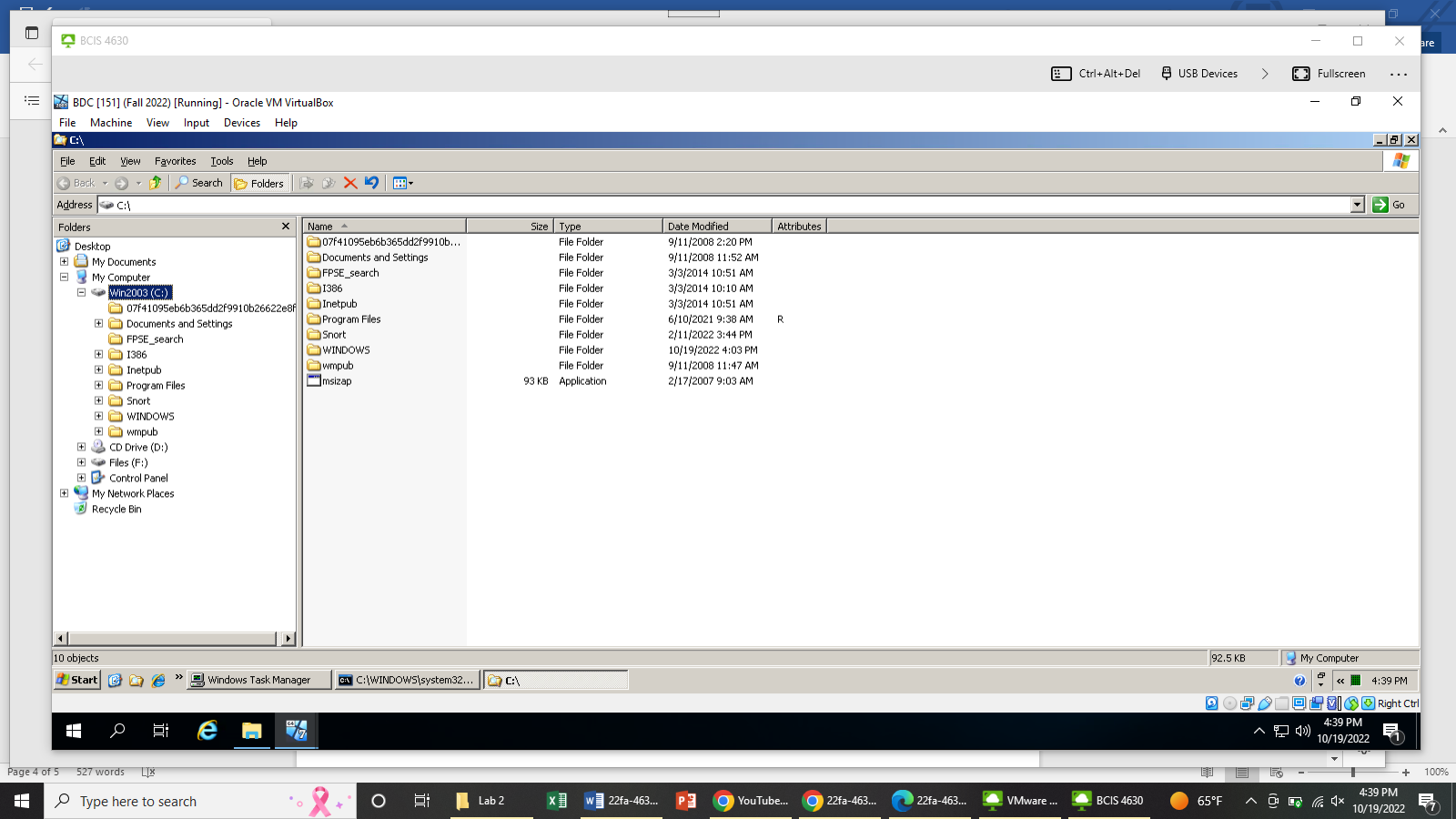
No I did not see beast.exe in the Task Manager’s process list.

2.4.4. Do you see those open ports you saw in 2.4.2? Support your answer with screenshot.

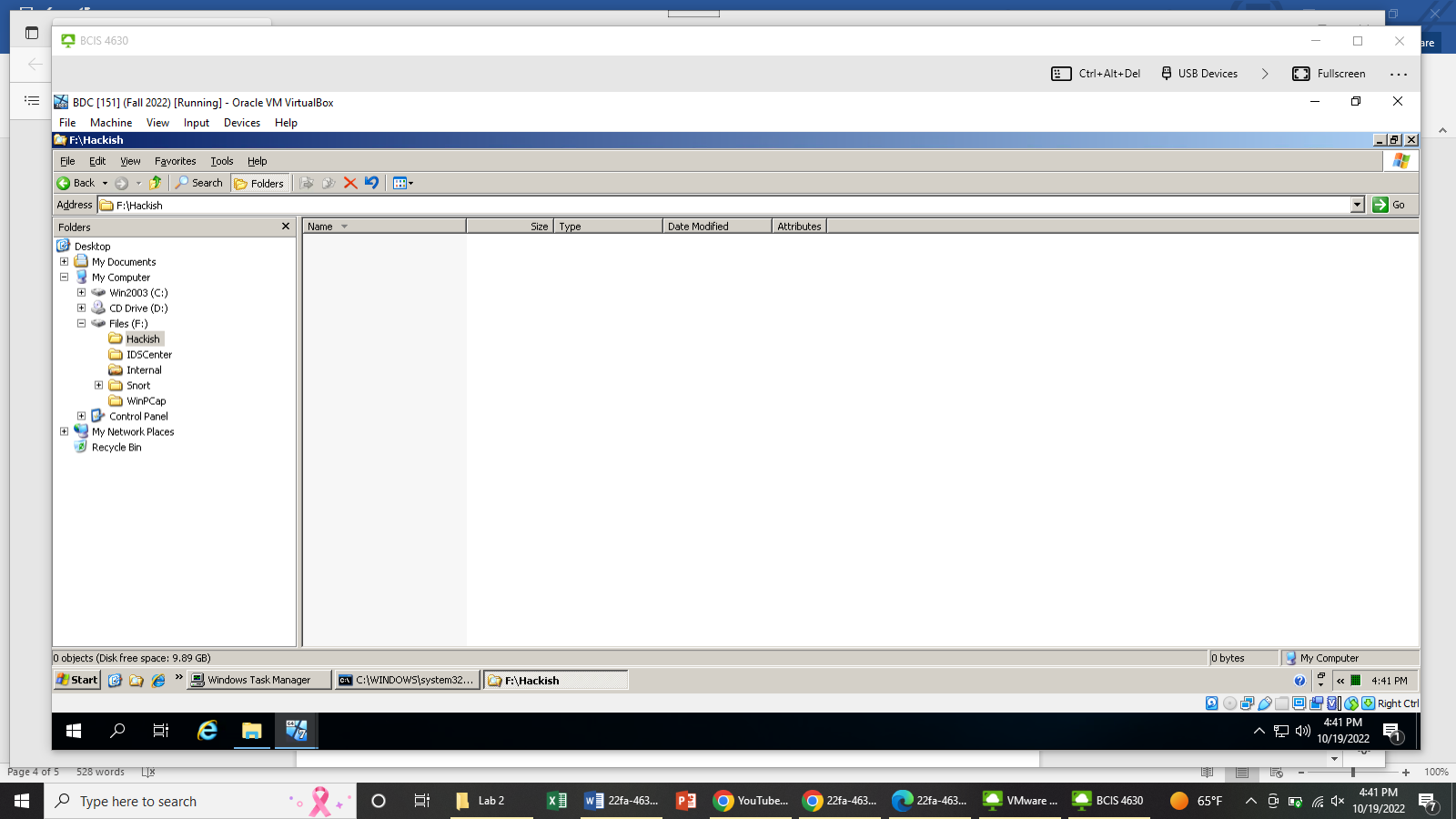


No.

2.4.5. Do you see the C:\beast folder? Support your answer with screenshot.

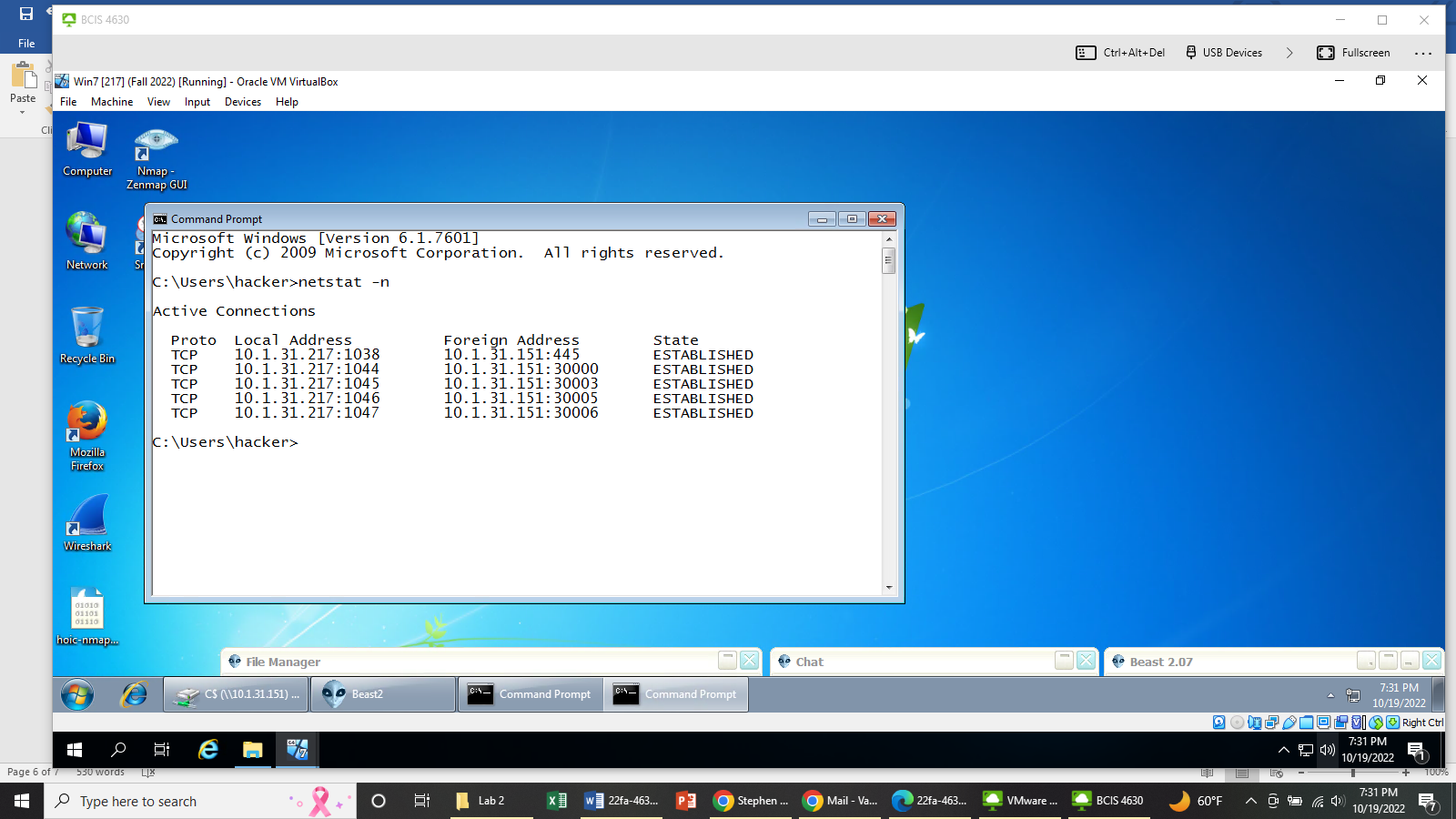


No.

2.4.6. Inside F:\Hackish, do you see the \hxdef100 subfolder? Support your answer with screenshot. 

No.

2.4.7. What ports on 10.1.xx.151 (the victim) is your attacker machine connected to? Are they the same as those you saw in 2.4.2? Support your answer with screenshot.



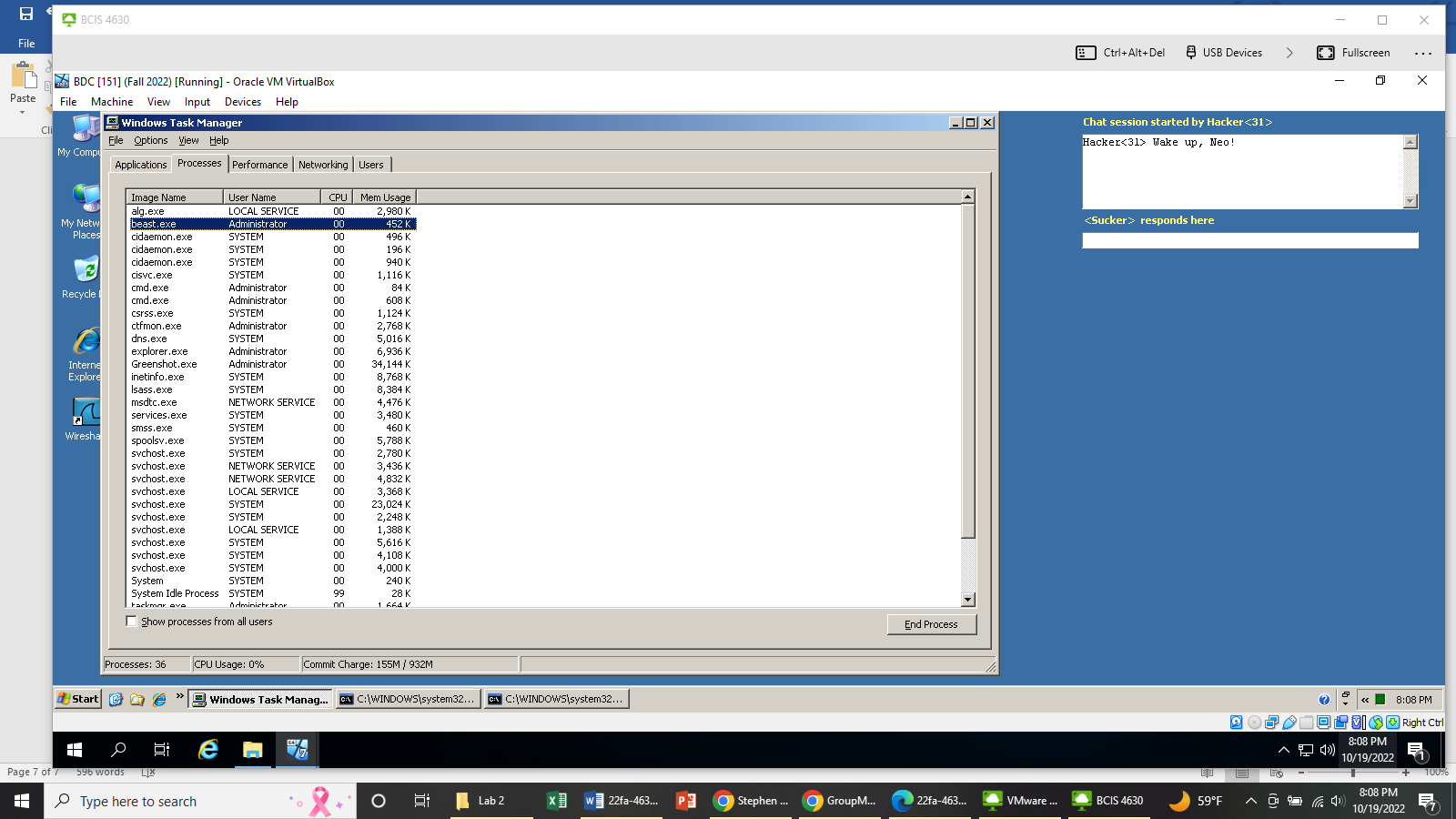
The ports are the same as I saw in 2.4.2.

2.4.8. Based on your answers to Question 2.4.1-2.4.7, what do you think are the effects of running the hxdef100 rootkit?

The effects of the hxdef100 rootkit allow the hacker to hide the presence of “beast.exe” inside of the victim machine. If the user in the victim machine uses task manager, “beast.exe” is hidden. It is also hidden in file explorer. The user in the victim cannot detect see which ports are open for the beast Trojan.

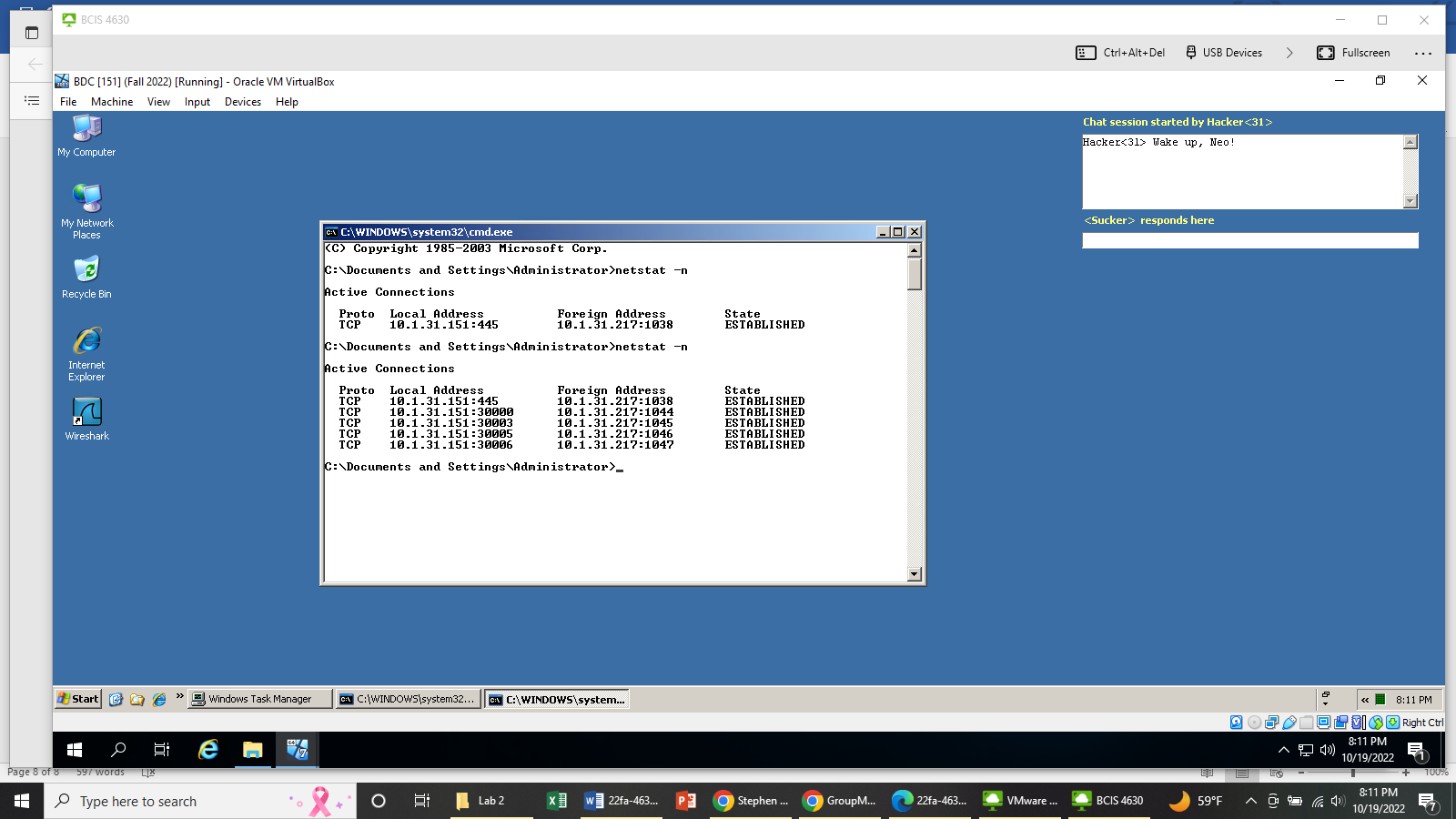
**Question 2.5**

2.5.1. Can you see the “beast” process in the Task Manager process list now? Support your answer with screenshot.



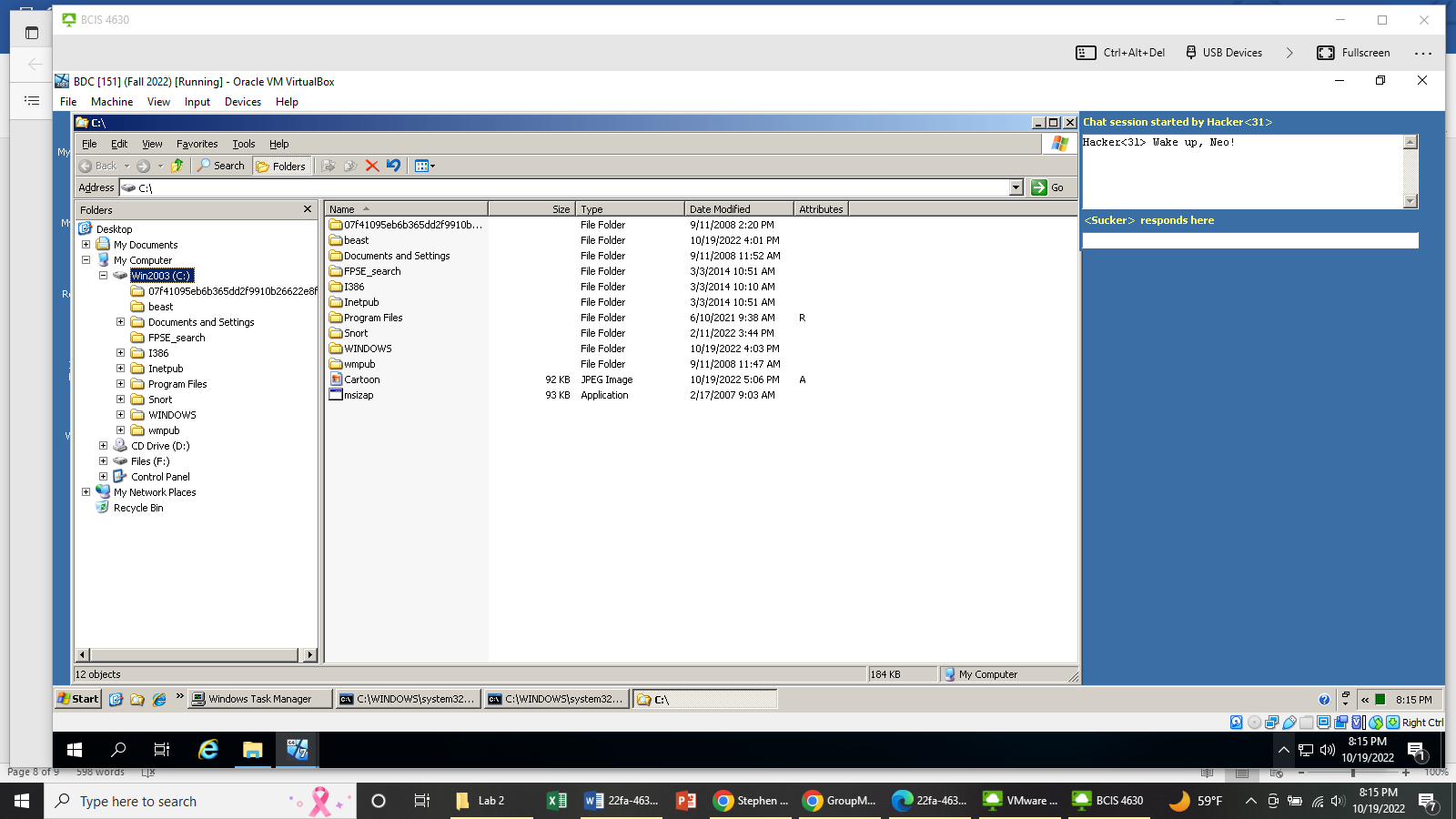
Yes.

2.5.2. Do you see those ports you saw in 2.4.2 in the list now? Support your answer with screenshot.



Yes.

2.5.3. Do you see the C:\beast folder now? Support your answer with screenshot.



Yes.

2.5.4. Inside F:\Hackish, do you see the \hxdef100 subfolder now?

Yes