ICT & Infrastructure

Week 3 – Chapter 1

Evidence

1. CLI Basics:

Task 1: Getting familiar with CLI

Problem 1:

A close up of text

Description automatically generated

A screenshot of a computer

Description automatically generated

Here I used the command whoami which returned my name.

Problem 2:

A close up of text

Description automatically generated

A screenshot of a computer

Description automatically generated

Here I used the mkdir command which creates a folder which I named PowerSharkFolder.

A screenshot of a computer

Description automatically generated



I used the ls command which showed the files in the current location “Liliya” folder and I have underlined the new folder I made.

Learning outcomes: I learned how to create files and folders as well as look what files and folders are there at any location.

Task 2: File modifications

Problem 1:



A computer screen shot of a black screen

Description automatically generated

With the cd command I go to a specific folder or file in the current folder that I am in. Here I create the folders with the mkdir command.

Problem 2:

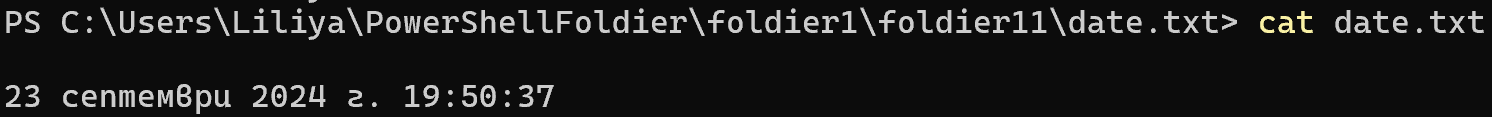


A screen shot of a computer screen

Description automatically generated

Again, I create a file called date.txt with mkdir command, after which I go in it with the cd command. With the “date” command I print the date into the date.txt with the operators “>>”.

Learning outcome: I learned how to write information in a text file through PowerShell.



Here I used the “cat” command for date.txt which is used to display the contents of the file. It displayed the date in my language along with the year and the time.

Problem 3:



A screen shot of a computer screen

Description automatically generated

Here, using the same commands I created another file runningprocesses.txt. This time I used the ps command which shows a list of currently running processes on the computer. I printed this in the runningprocesses.txt file again with the operators “>>”.

A screenshot of a computer program

Description automatically generated

Using the cat command again, the list of currently running processes printed in the runningprocesses.txt file was displayed.

Problem 4:





Here I used the cat command to view the contents of a folder, but to do this while being in another folder, I used the “../” and the path to the date.txt file.

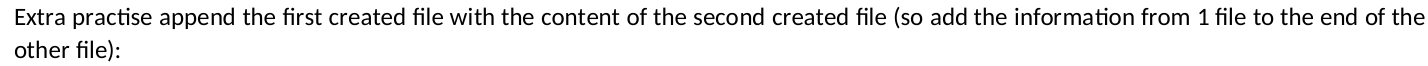
Problem 5:





With the mv command I moved the runninprocesses.txt file from folder12 to folder11.

Problem 6:





While being in the main folder1 where both folder11 and folder12 are, I used the cat command to get the contents of the file date.txt and append them (“>>”) to the runningprocesses.txt file.

Task 3: Networking tools

Problem 1:



A screenshot of a computer

Description automatically generated



Here I used the ipconfig command which displays the IP configuration of my network interfaces. I have underlined the IP address.

Problem 2:



A screenshot of a computer

Description automatically generated

I used the tracert command to find out what route the packets take to reach their destination, followed by another student’s IP.

Problem 3:



A screenshot of a computer

Description automatically generated

Here I did the same thing but with google.com.

1. CLI Chat App:

Problem: Chatting



I downloaded ncat for this assignment. I was home so I did this with two prompts on my own computer.

A screenshot of a computer

Description automatically generated

Here^ in the first prompt I start the ncat server using the ncat command followed by the flag “-l” which tells ncat to operate in “listen mode”. The “-k” allows ncat to keep listening for new connections after a client disconnects. The “-p” specifies the **port number** on which ncat will listen for incoming connections. In this case “1234” is the port number.

A screenshot of a computer

Description automatically generated

In the second prompt I used ncat followed by “localhost” which specifies the hostname to which I want to connect. It refers to the local computer itself. “1234” is the specified port number on which the server is listening for connections. I managed to send messages both from client and from server. They appear on both prompts.

Learning outcomes: I learned how to work with PowerShell and manipulate folders and files through it with commands. I learned how to use Ncat in PowerShell and how to create a chat server.

1. Wireshark

Task 1: Finding the CLI chat

Problem 1:



A screen shot of a computer

Description automatically generated



I have underlined the sent message which I want to see in Wireshark.

A screenshot of a computer

Description automatically generated

To find this in Wireshark I used the filter tcp.port == 1234 so that I see only the packets of the “1234” port. After this I looked for a packet that shows PSH, ACK in the info column. That is how I found the packet where I can see the sent message from the chat in PowerShell.

Problem 2:



A screen shot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

Here I did the same but with a received message.

Problem 3:



I see a difference in the info displayed in Wireshark. The first screenshot shows that the message is sent from the server (1234 -> 30777), 1234 being the port number. The second one shows that the message is sent from the client (30777 -> 1234), so it’s reversed.





Task 2: Dora process

Problem: Start the process

A screenshot of a computer

Description automatically generated

Here I start the process by typing the ipconfig command followed by /release which instruct my computer to drop its current DHCP lease.

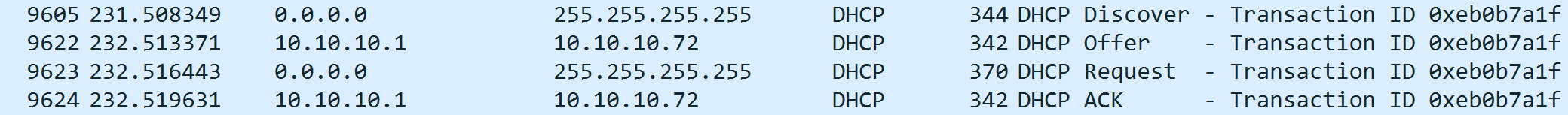
A screenshot of a computer

Description automatically generated

Here I used the command ipconfig followed by /renew which initiates a request to the DHCP server for a new IP address.

Before doing this, I opened Wireshark and started capturing packets. After starting the process, I stopped the capturing and tried to find where Wireshark captured the DORA process. I had to see only DHCP packets. But I did not know how.

Learning outcome: I used the internet and learned that in order to see only DHCP packets in Wireshark I had to use the filter bar and type “bootp”. “This filter works because DHCP uses the BOOTP protocol, and Wireshark recognizes DHCP packets under the BOOTP protocol.”





I looked for DHCP Discover, DHCP Offer, DHCP Request, DHCP ACK packets. This is the DORA process.

Overall learning outcome: I learned how to use PowerShell and manipulate files and folders and modify them through it. I learned how to use Ncat and create a chat. I learned how to use Wireshark to track the messages sent in the chat in PowerShell. I learned how to find my IP address and how to find out what route packets take to reach their destination. I learned about the DORA Process.