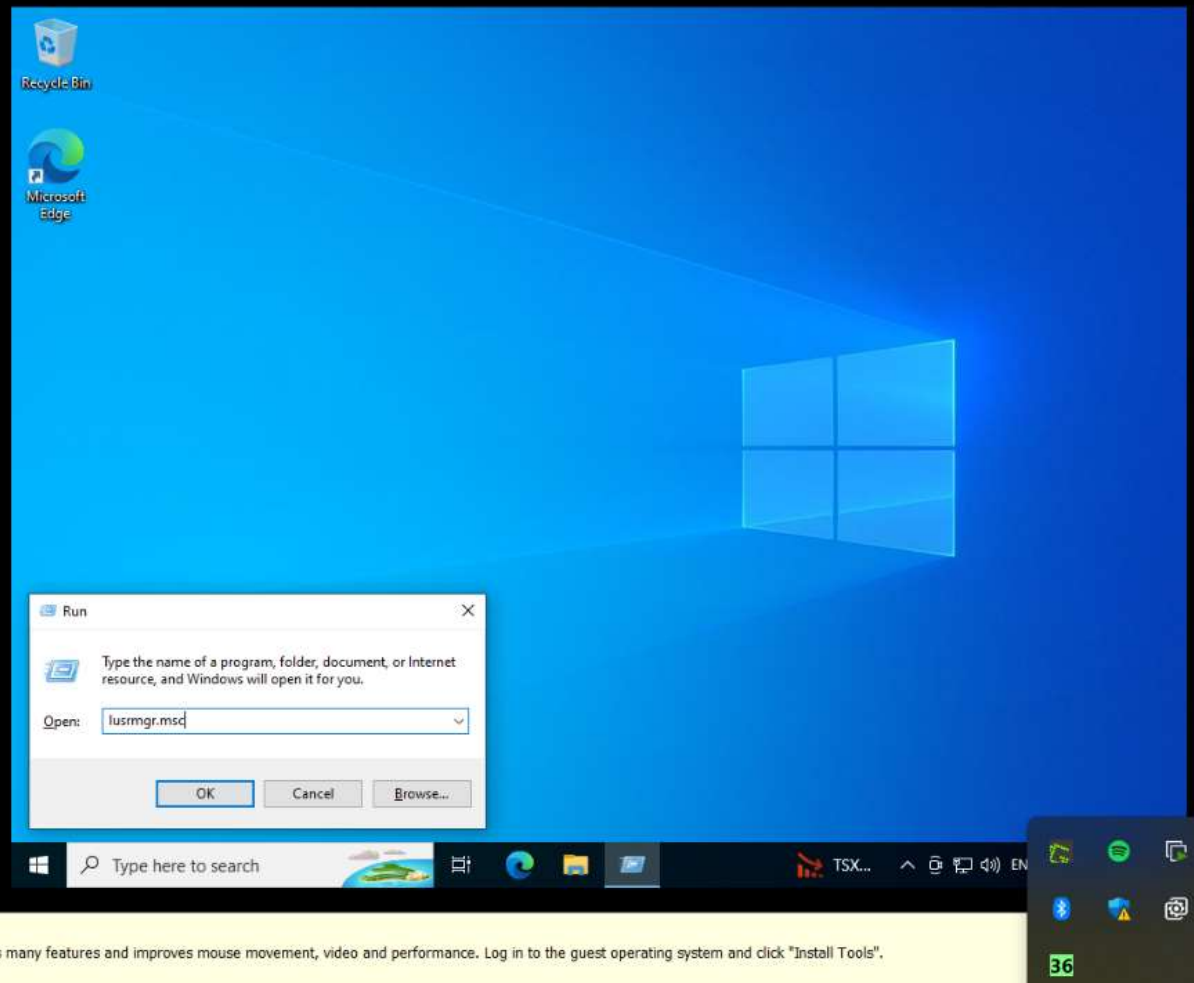
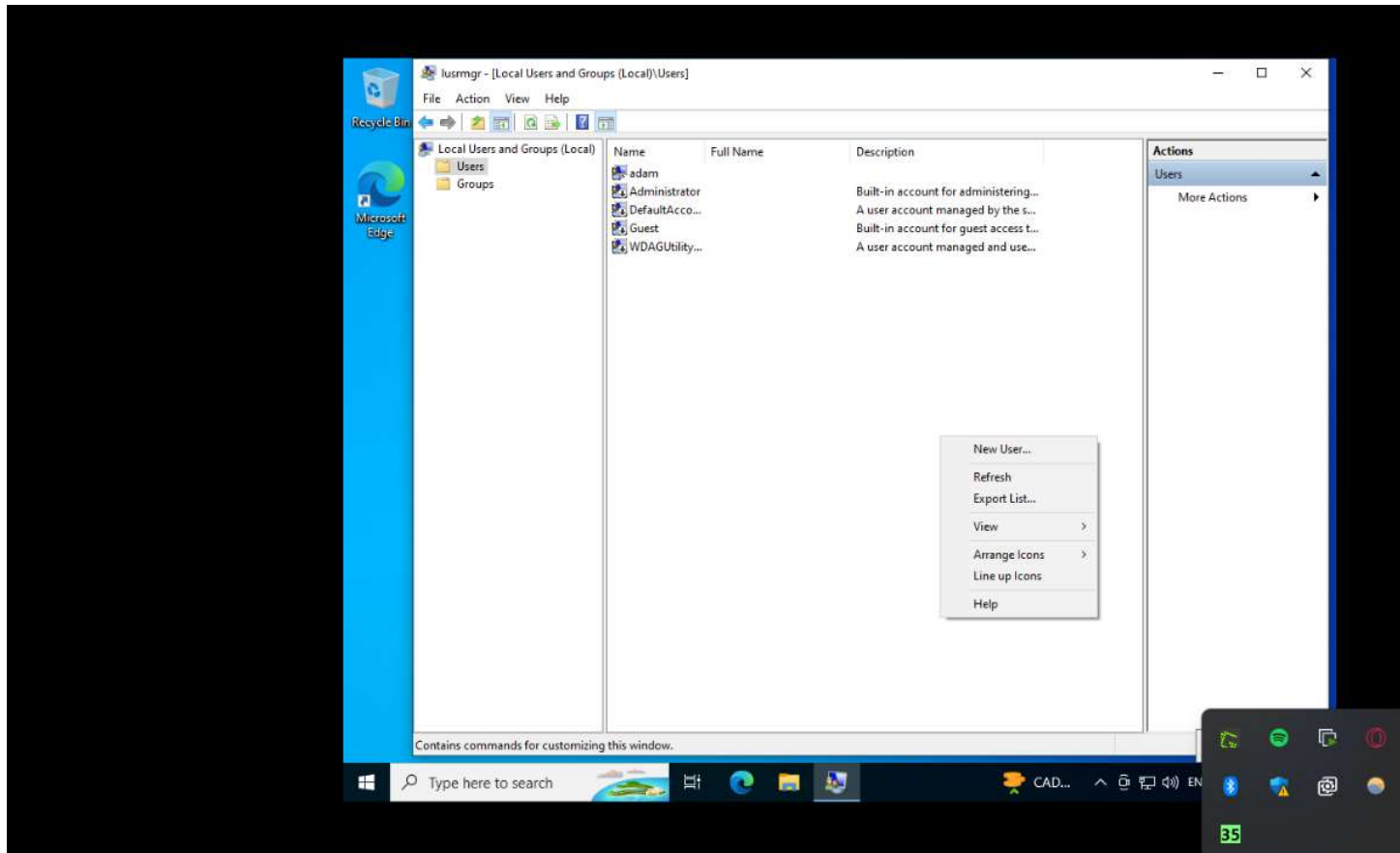


Lab 1 – Windows 10 User Management Lab

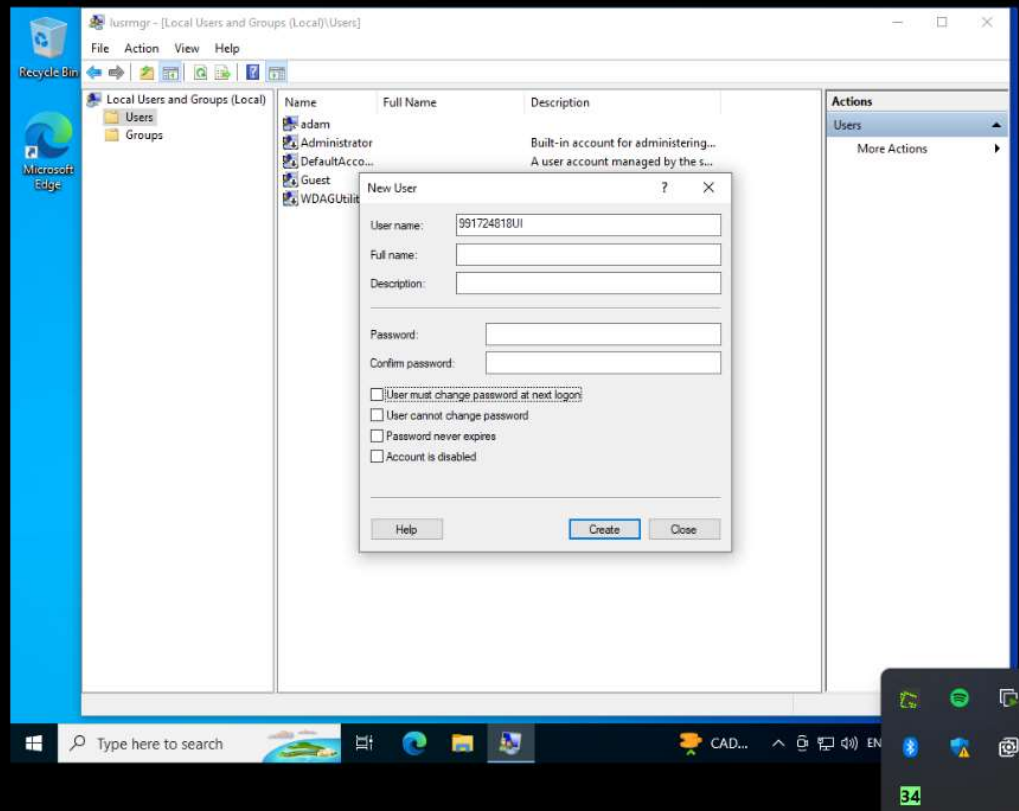
Adam Magdziak



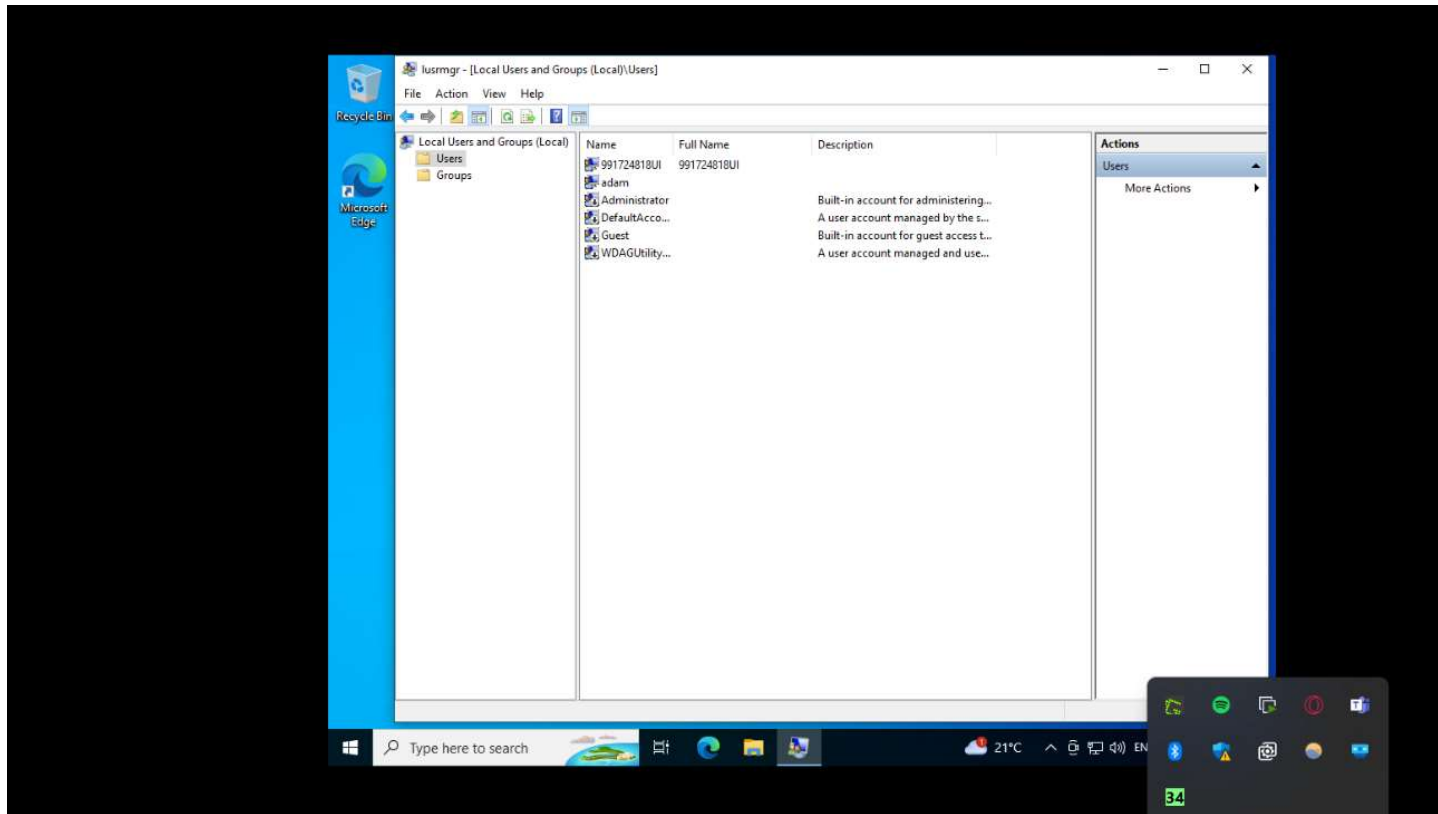
Opening lusrmgr.msc to create an account using the GUI method



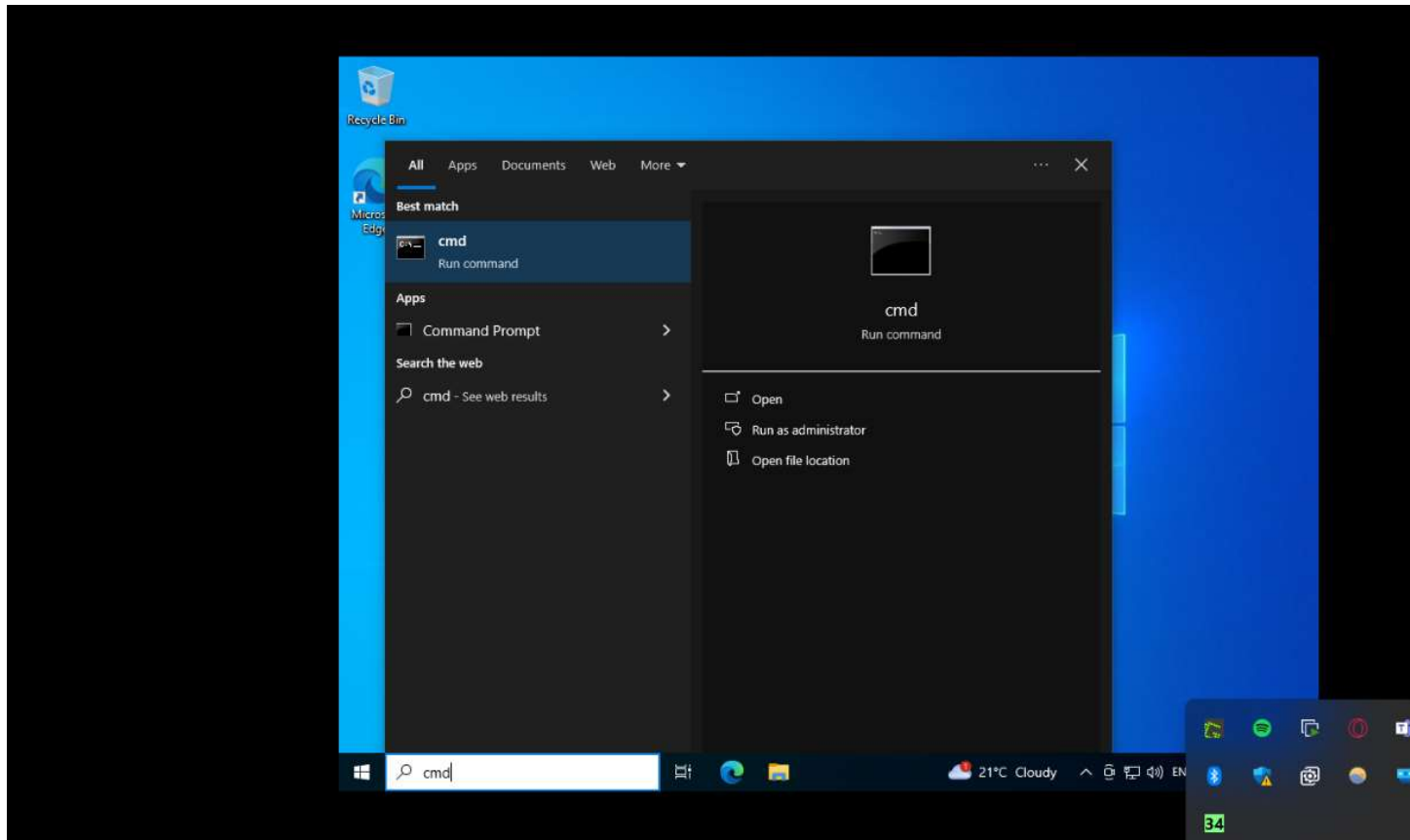
Right clicking in lusrmgr.msc to click on new user



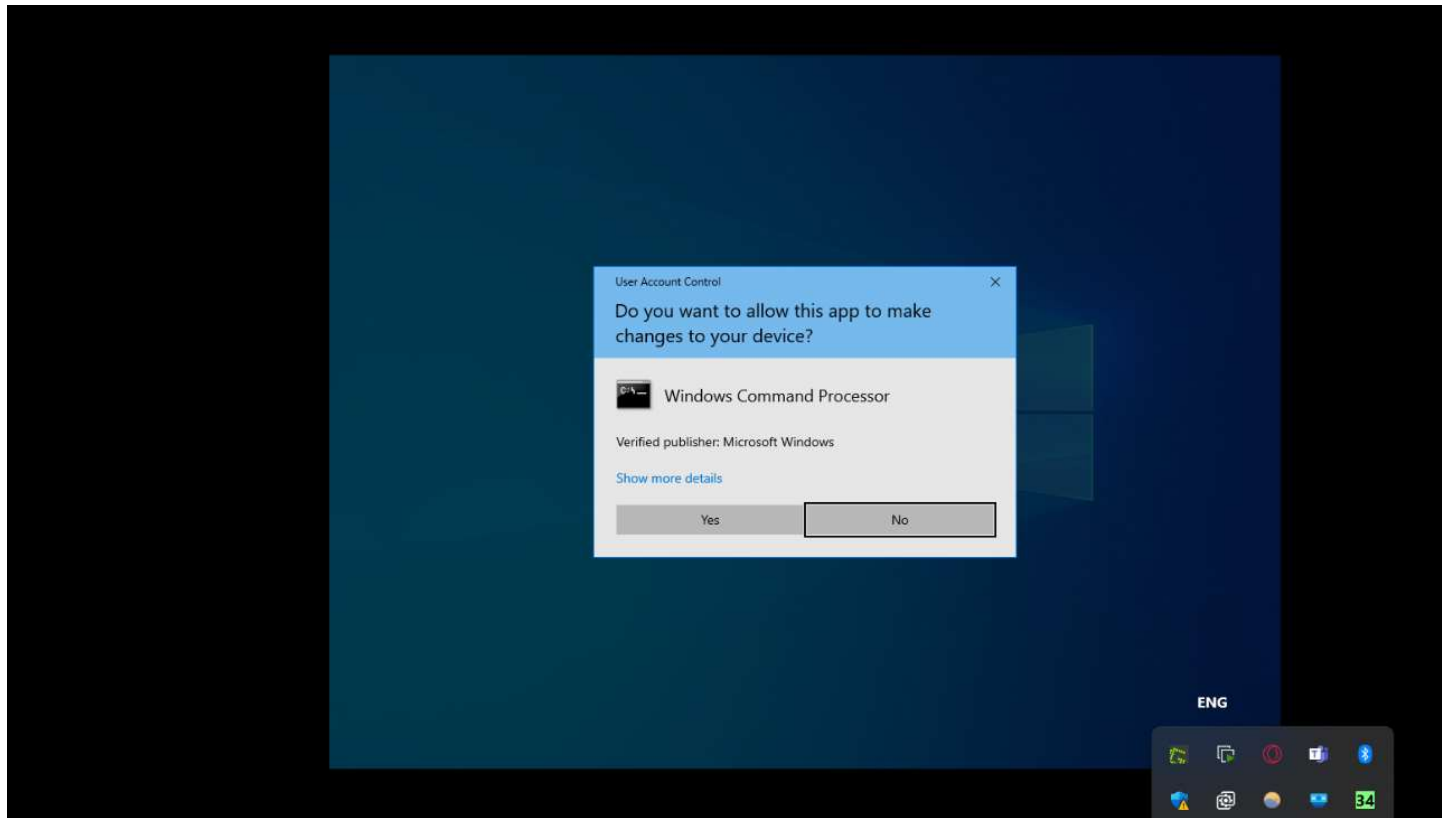
Creating the new user with the username – “991724818UI”



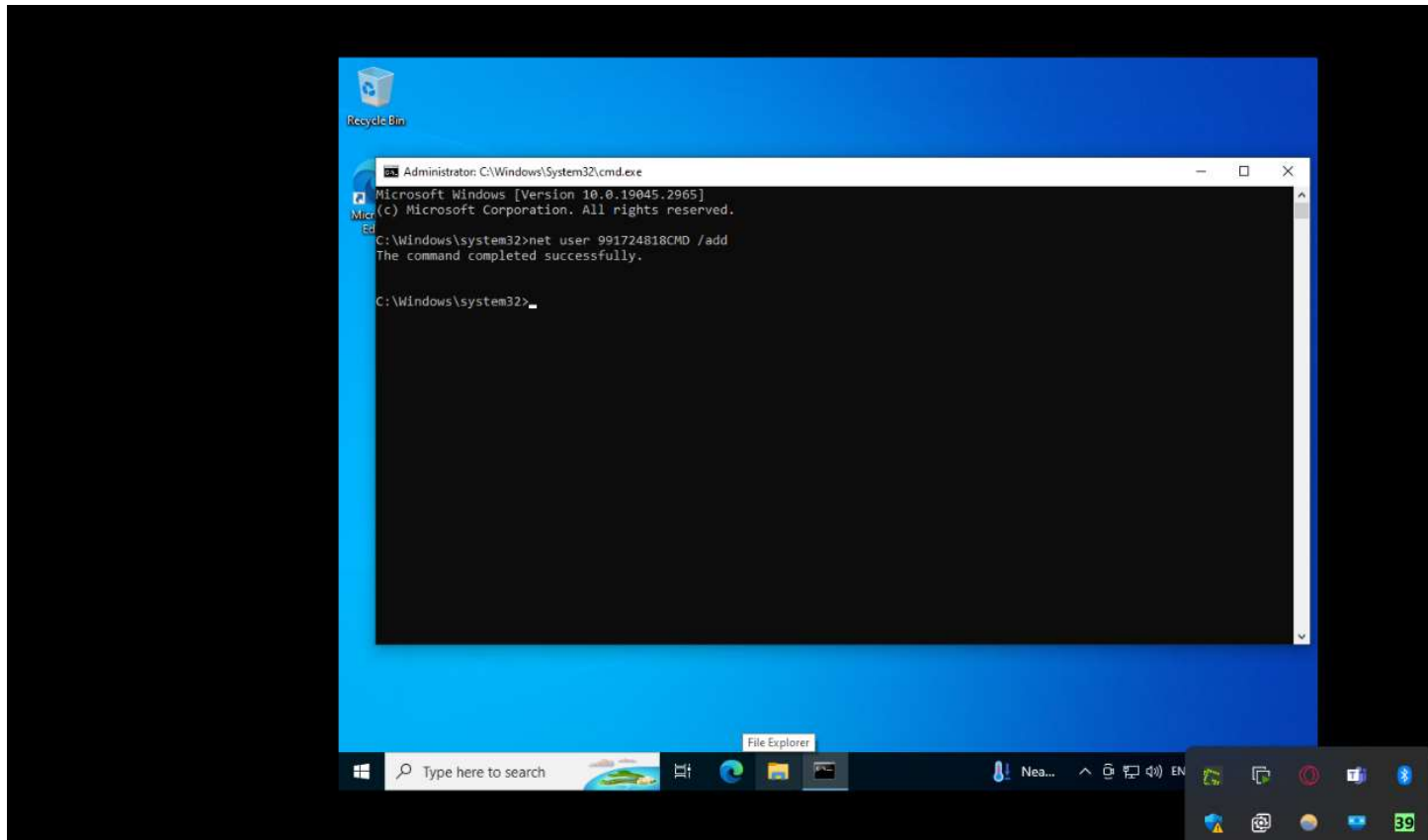
Confirming that 991724818UI is in the Local Users and Groups



Searching “cmd” in the search button and clicking on ‘*run as administrator*’

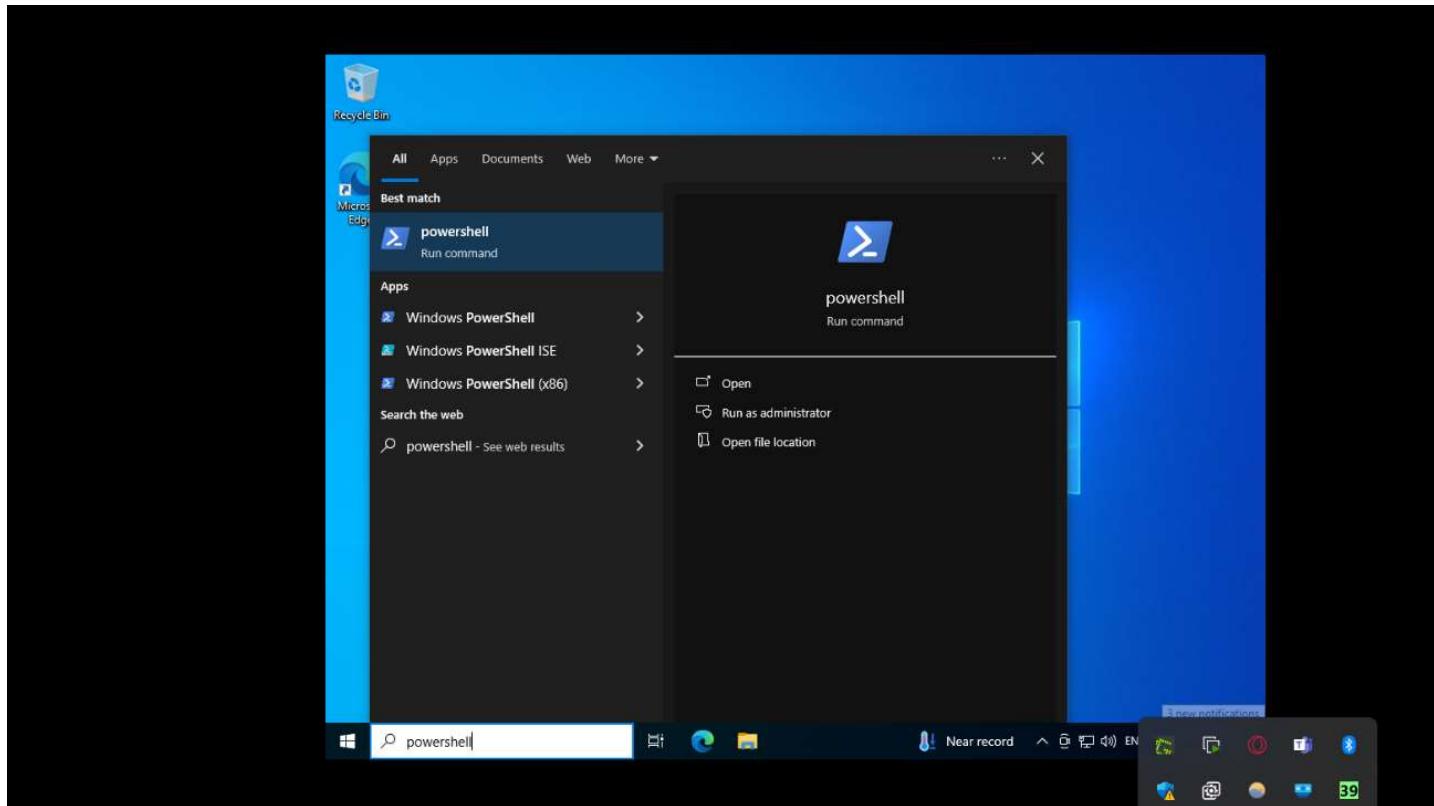


Confirming to run cmd as administrator by clicking 'yes'

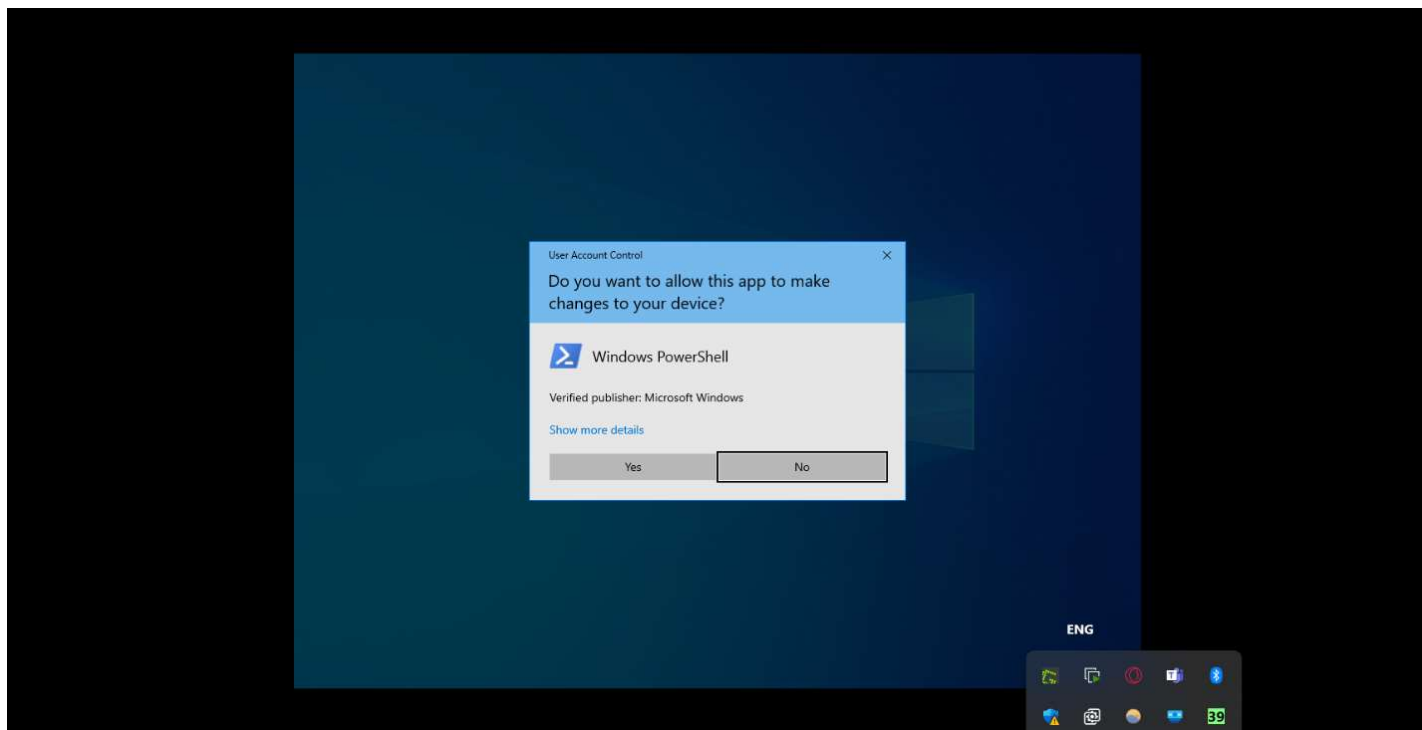


Using the command “net user username /add” to create the 991724818CMD user

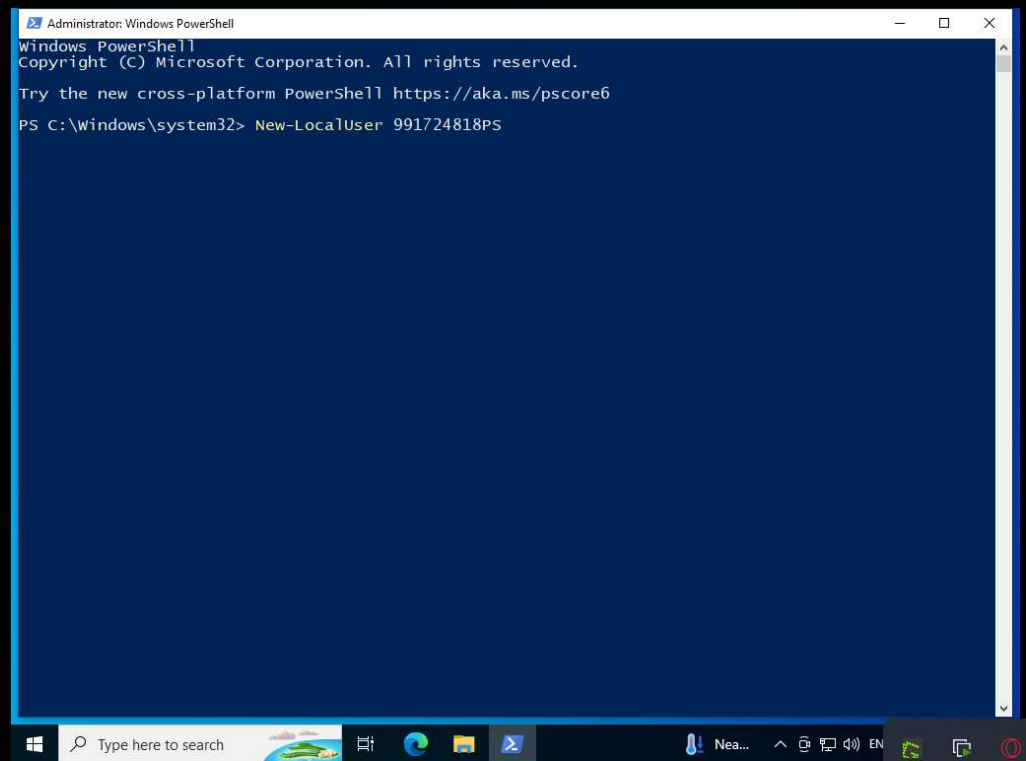
Windows response: “the command completed successfully”



Searching “PowerShell” in the search button and clicking *“run as administrator”*



Confirming to run PowerShell as administrator by clicking ‘yes’

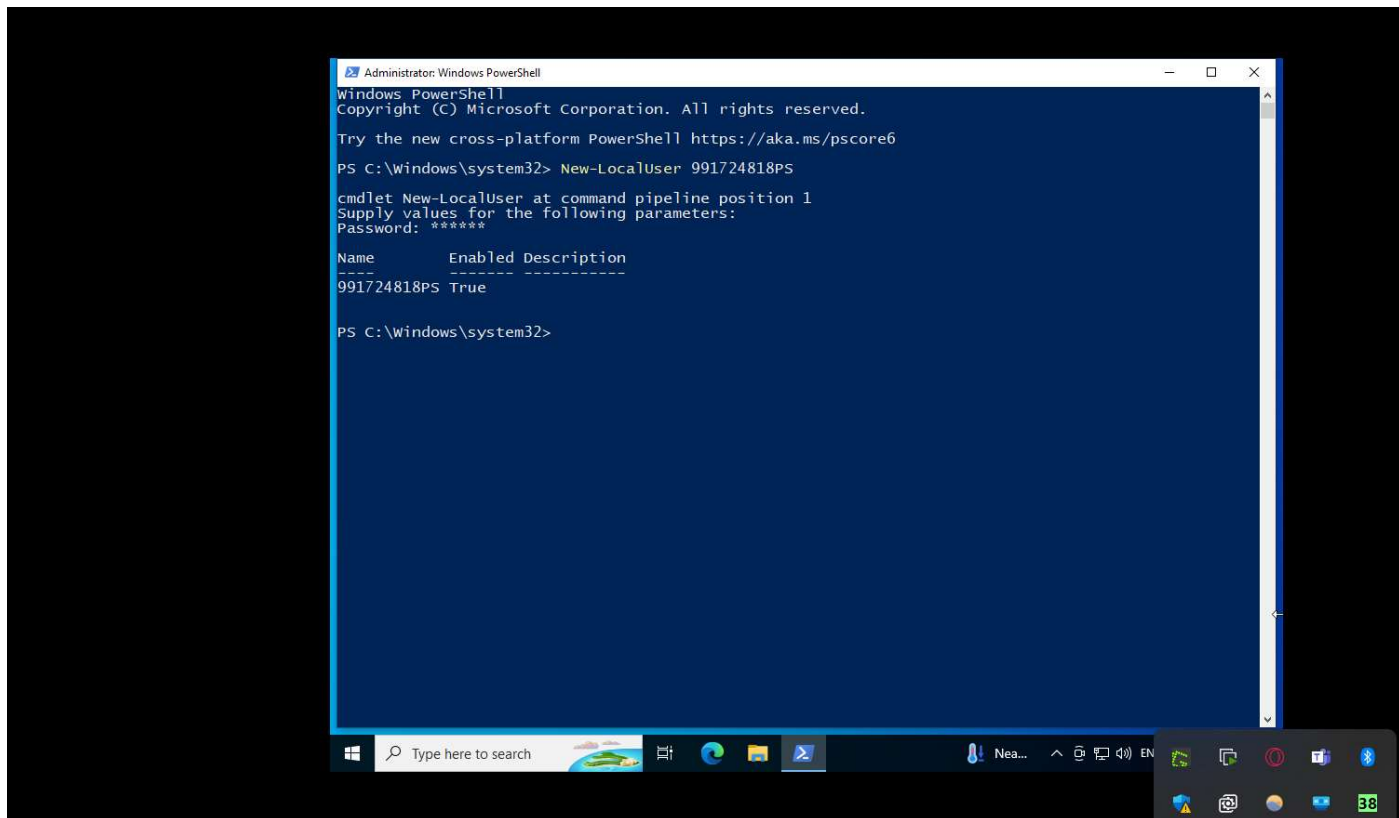


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

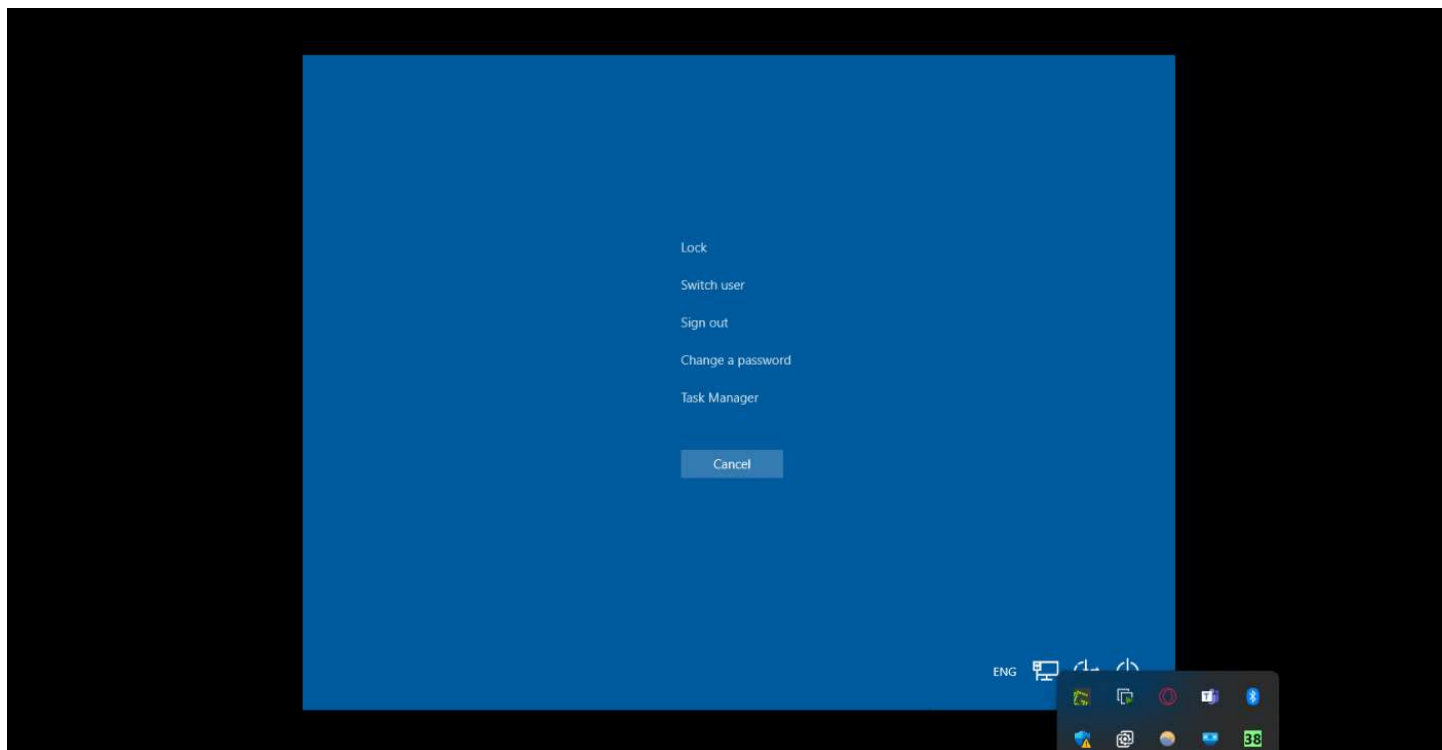
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> New-LocalUser 991724818PS
```

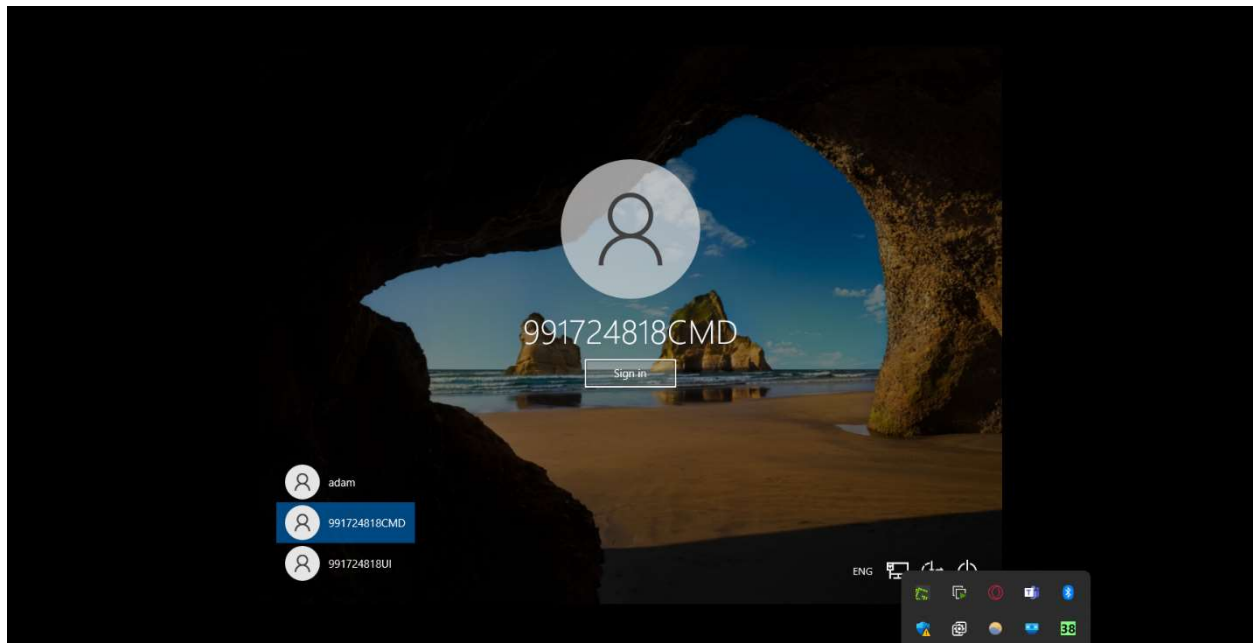
Using the command “New-LocalUser username” to create the user 991724818PS



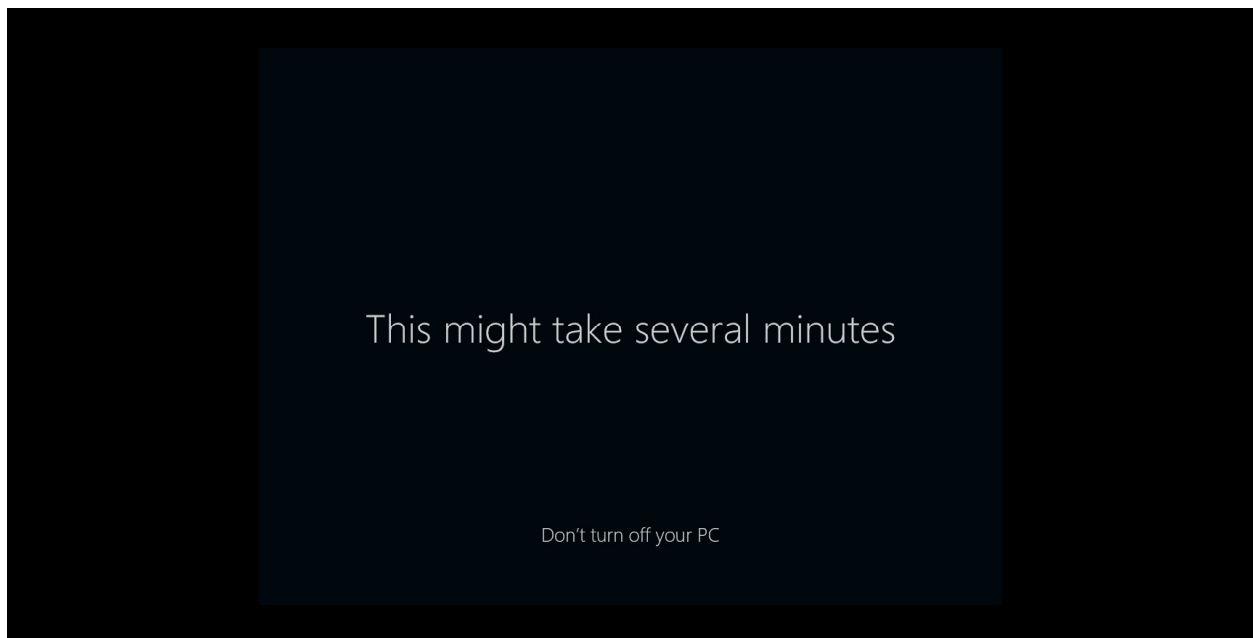
The windows response to creating a new user in PowerShell



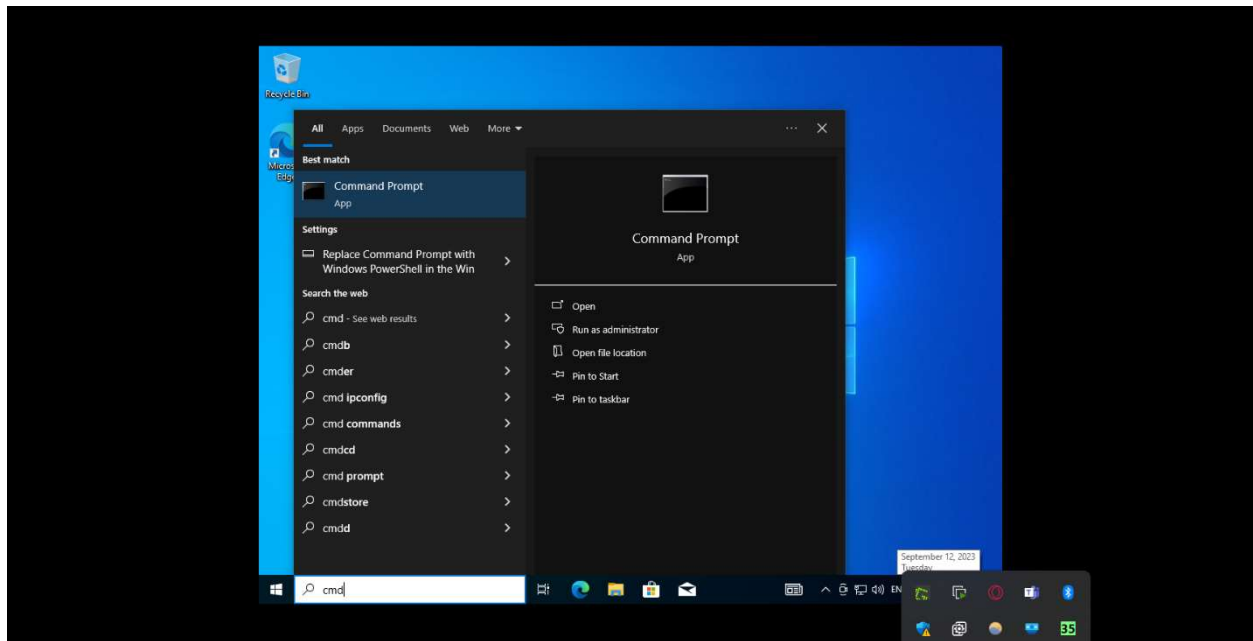
Switching into a new user by pressing “ctrl-alt-del”



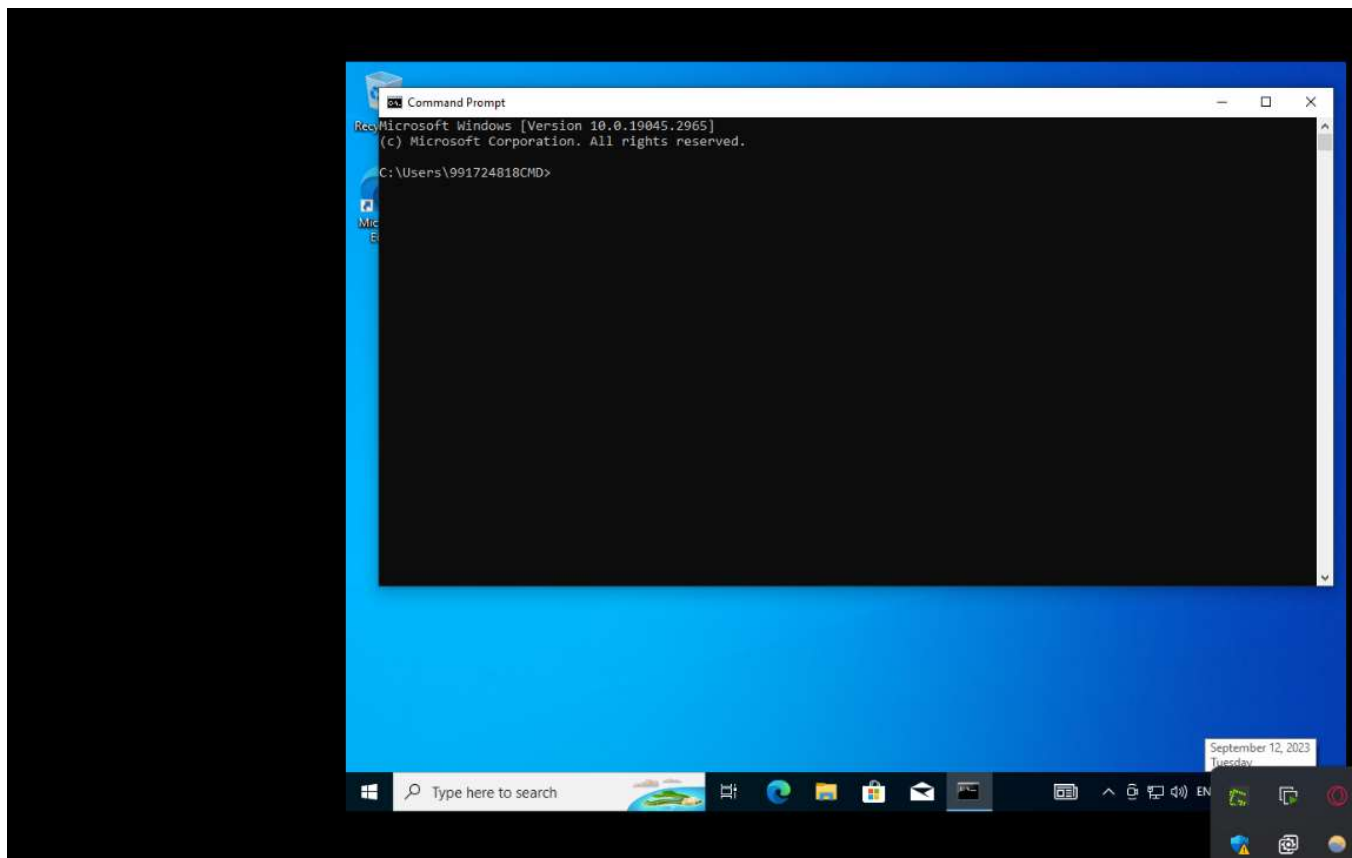
Switching into the CMD user



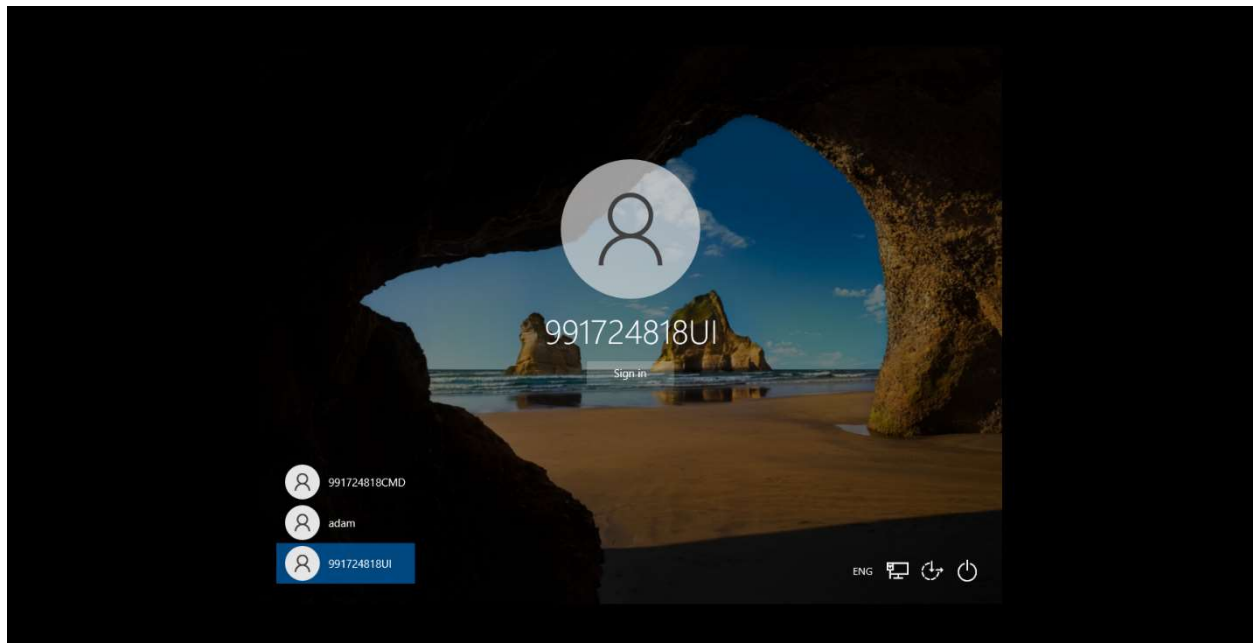
Receiving a windows update to boot up the new user



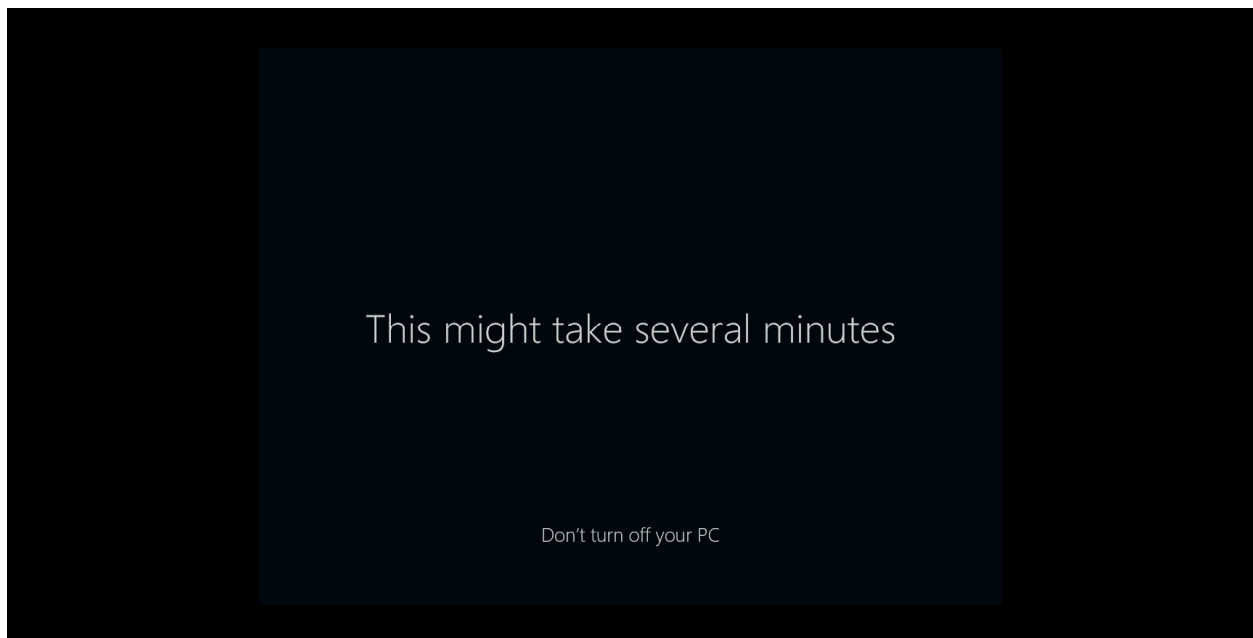
Searching cmd and opening it to see which user is currently logged in



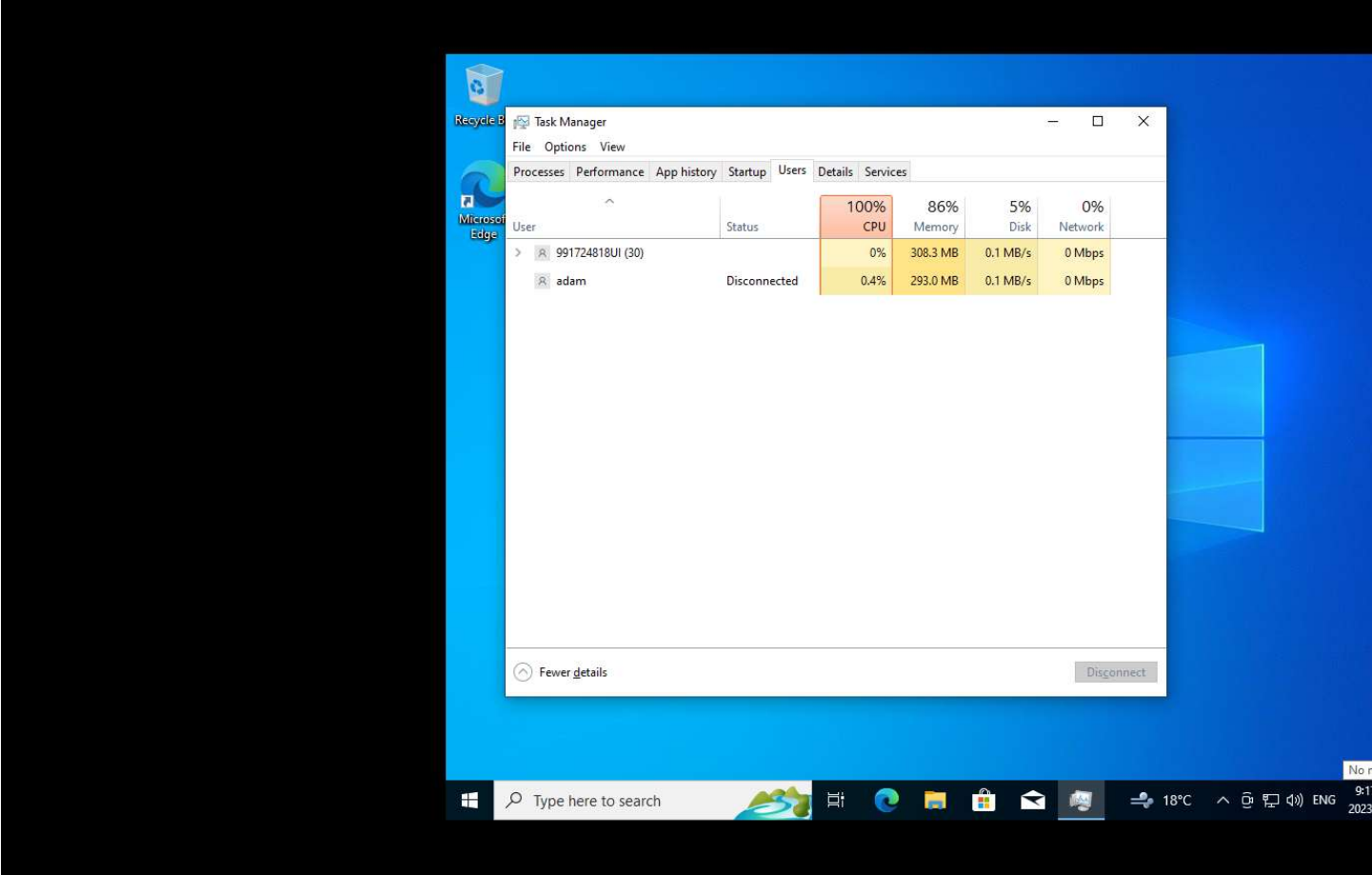
Confirming that the CMD user is logged in through “C:\Users\991724818CMD>” prompt



Switching into the UI user

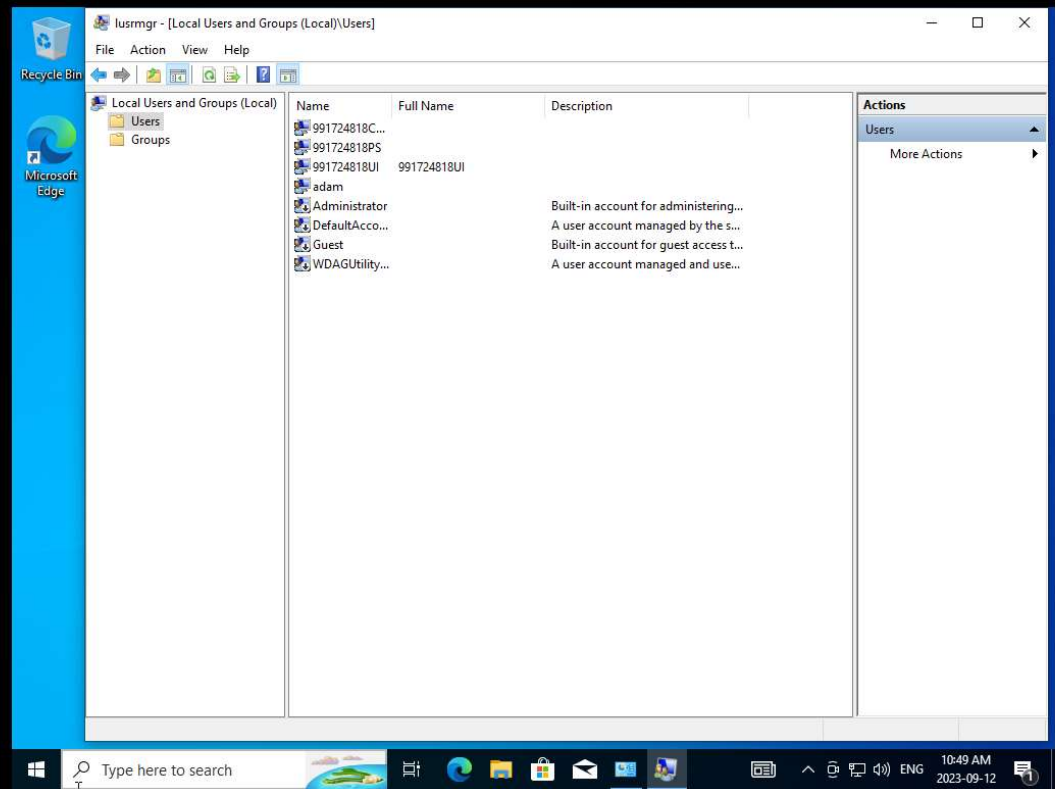


Receiving a windows update to boot up the new user

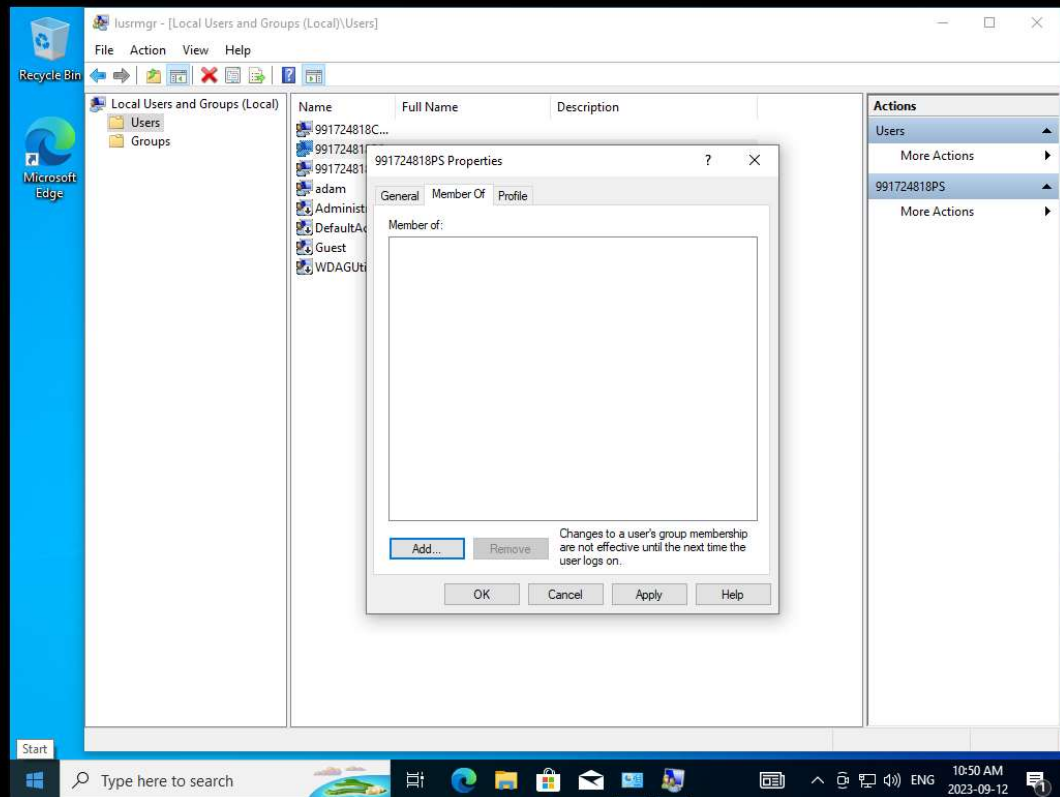


Loaded task manager and confirmed the UI user is logged in through the 991724818UI being active

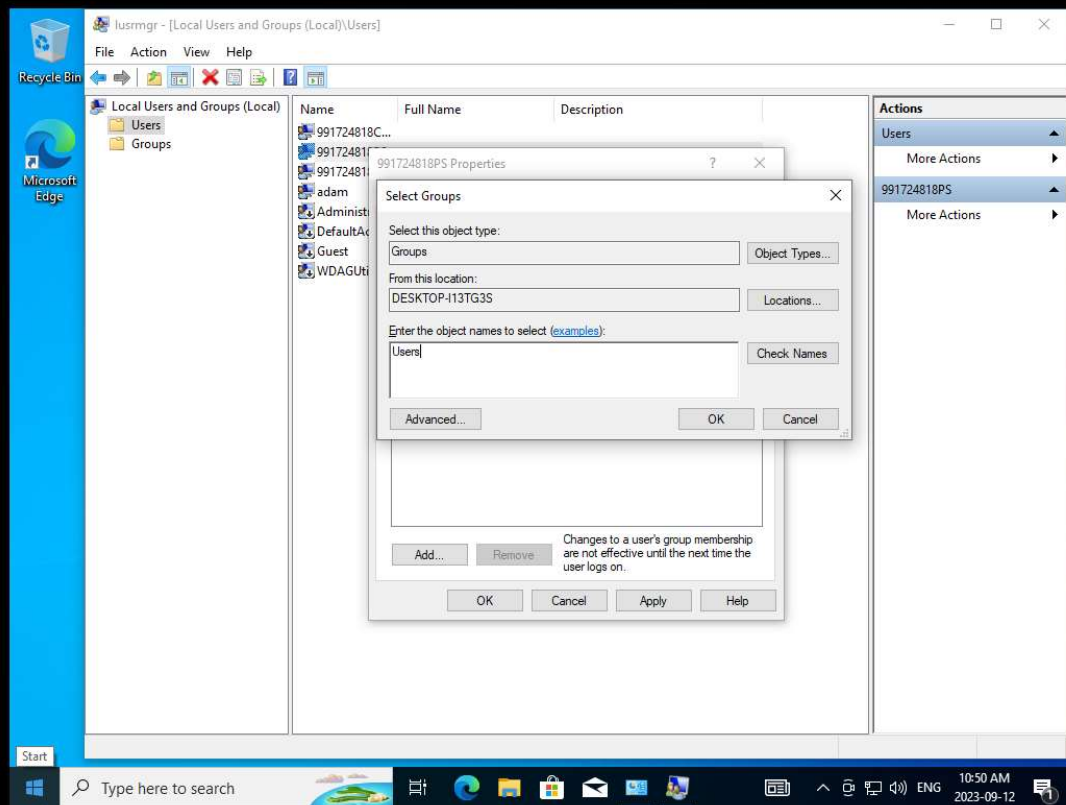
When attempting to log into the PowerShell user, I noticed it wasn't in the menu of choosing users.



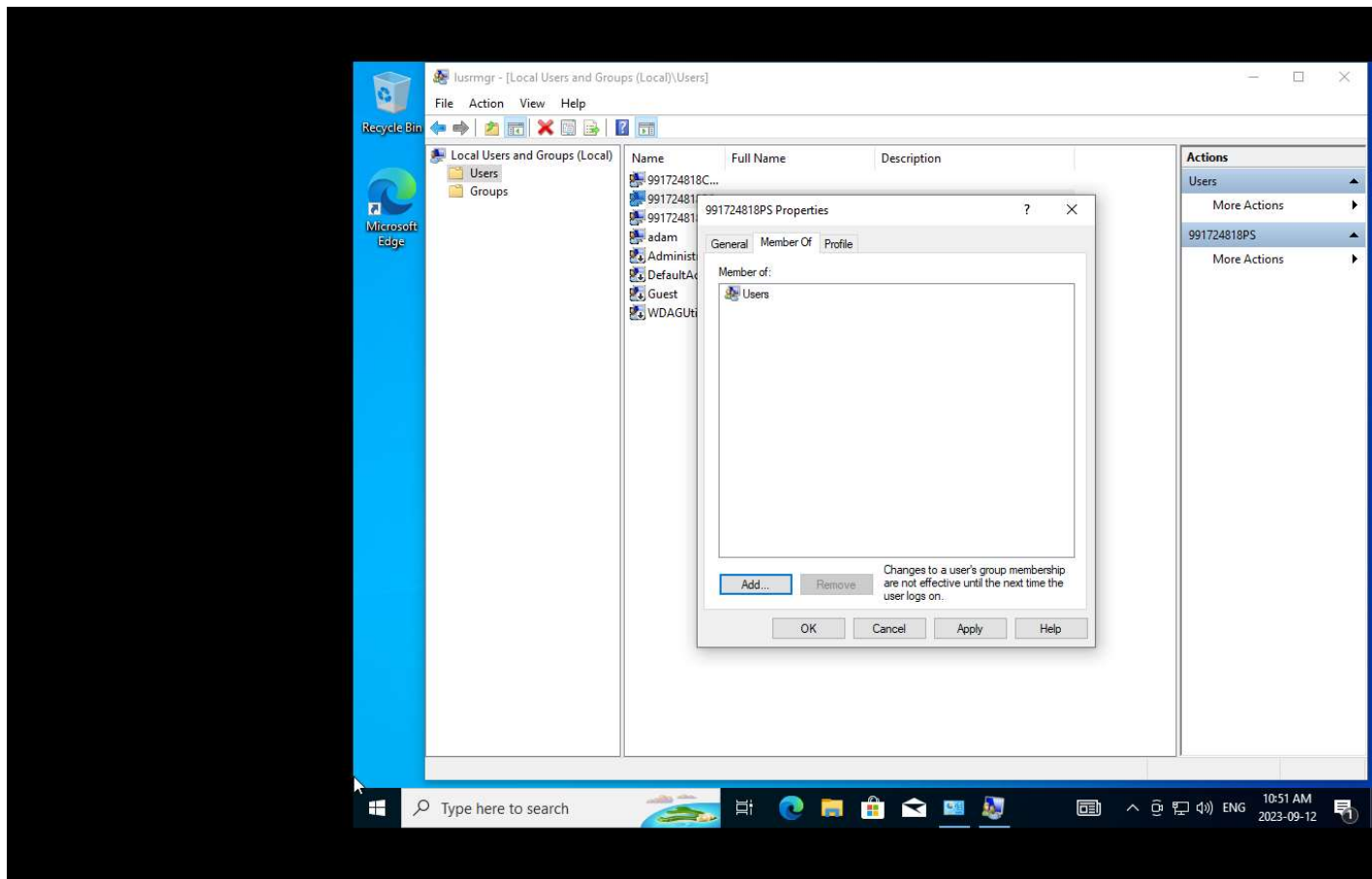
Opening lusrmgr.msc to double-check the status of the 991724818PS user



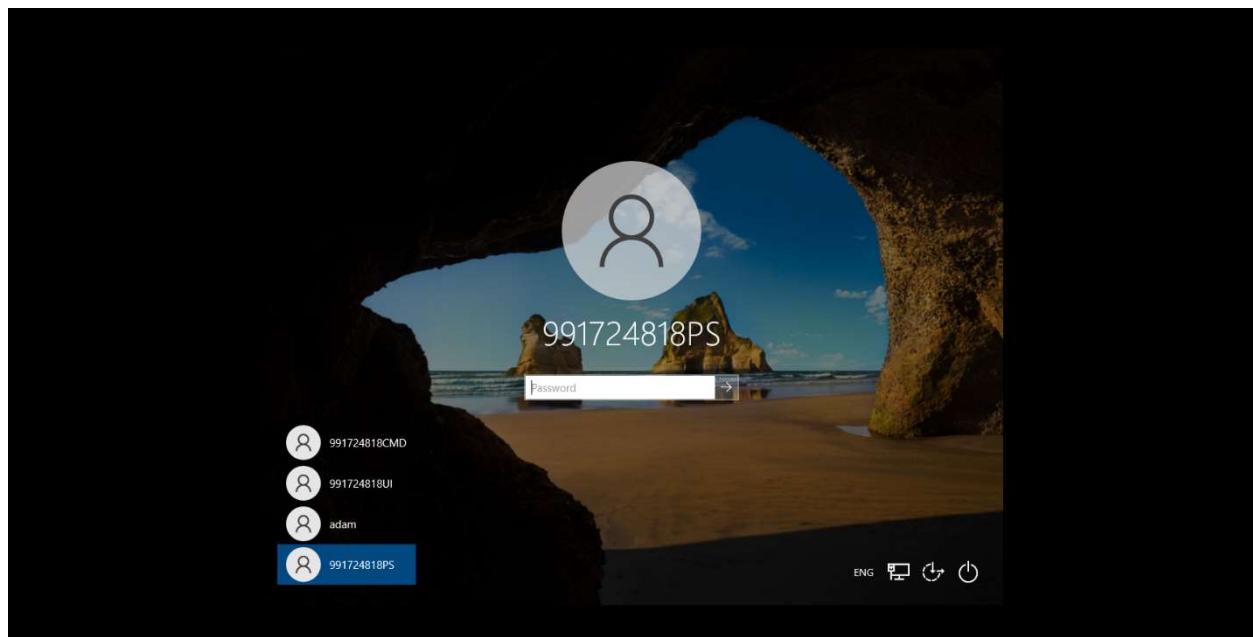
Clicking on the 991724818PS properties and going under the “member of” tab; the issue was with the user not being assigned to any of the groups



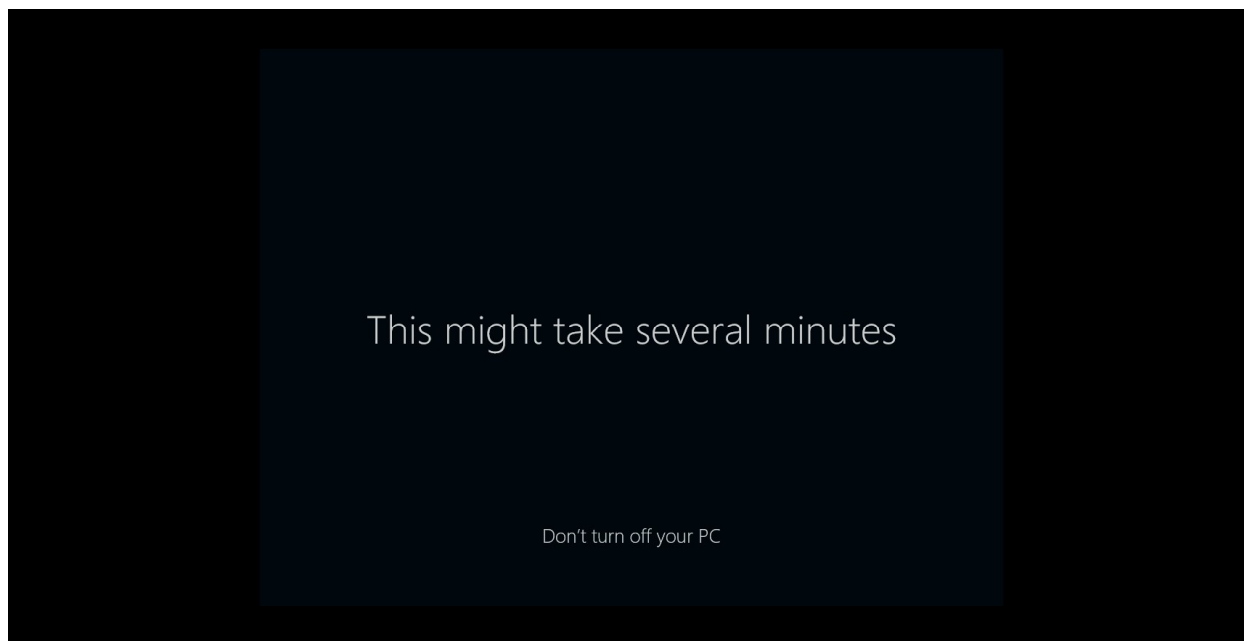
Assigning the 991724818PS user into the “Users” group



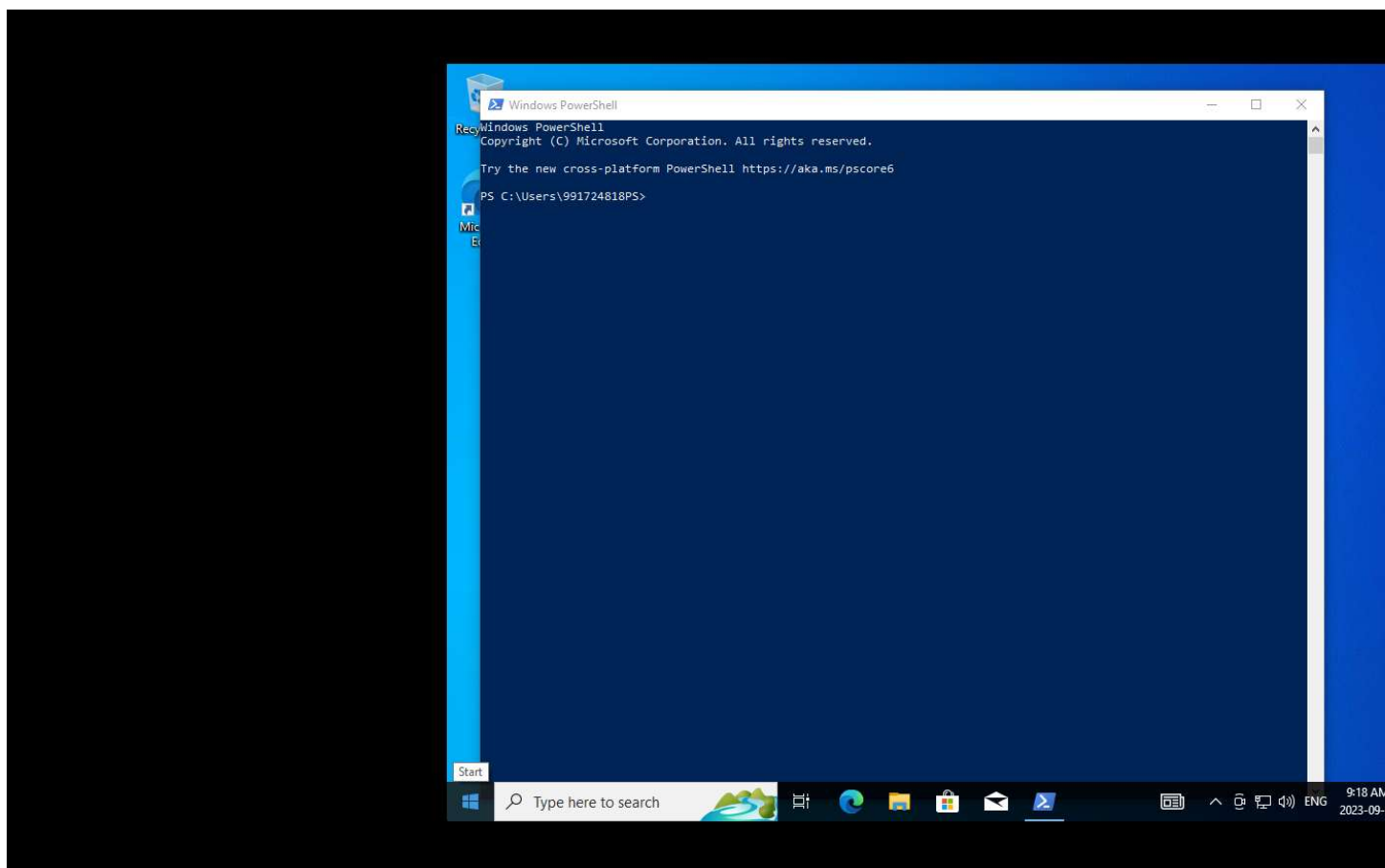
Confirming that 991724818PS is now apart of the “Users” group



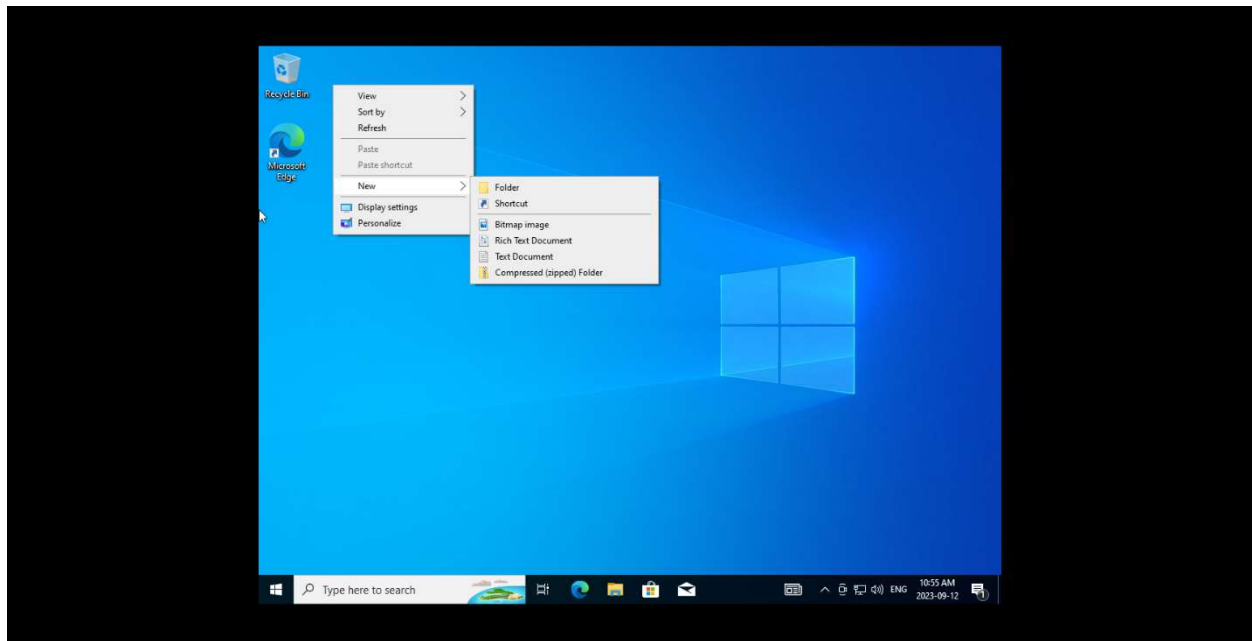
Switching into the 991724818PS user



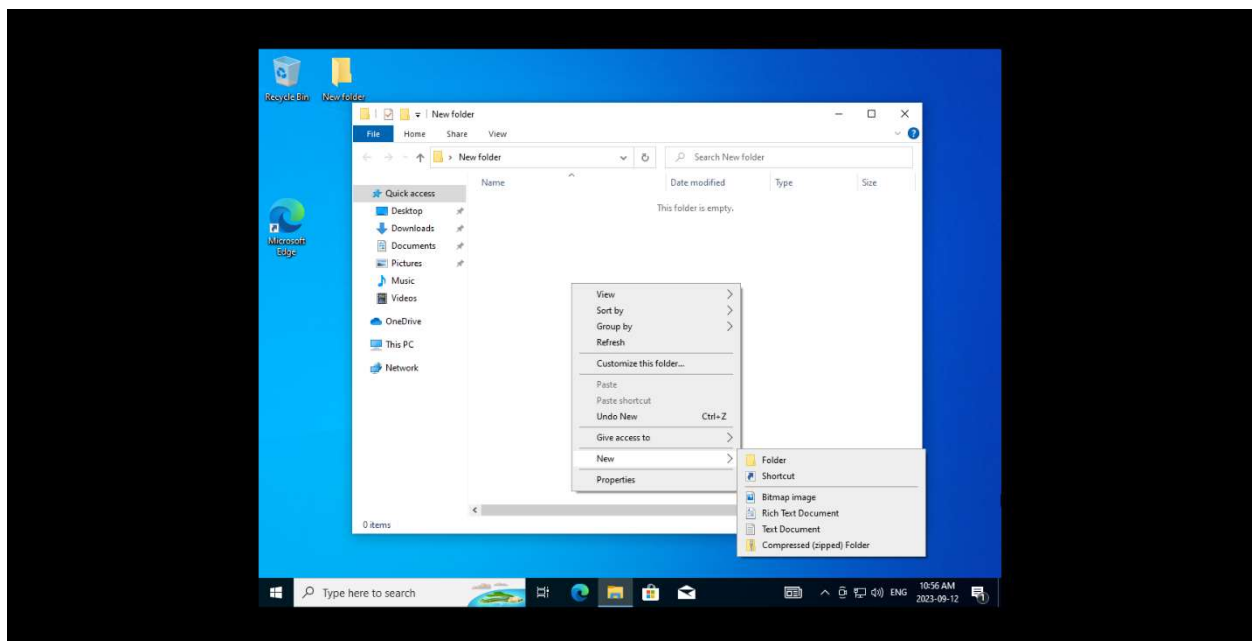
Receiving a windows update to boot up the new user



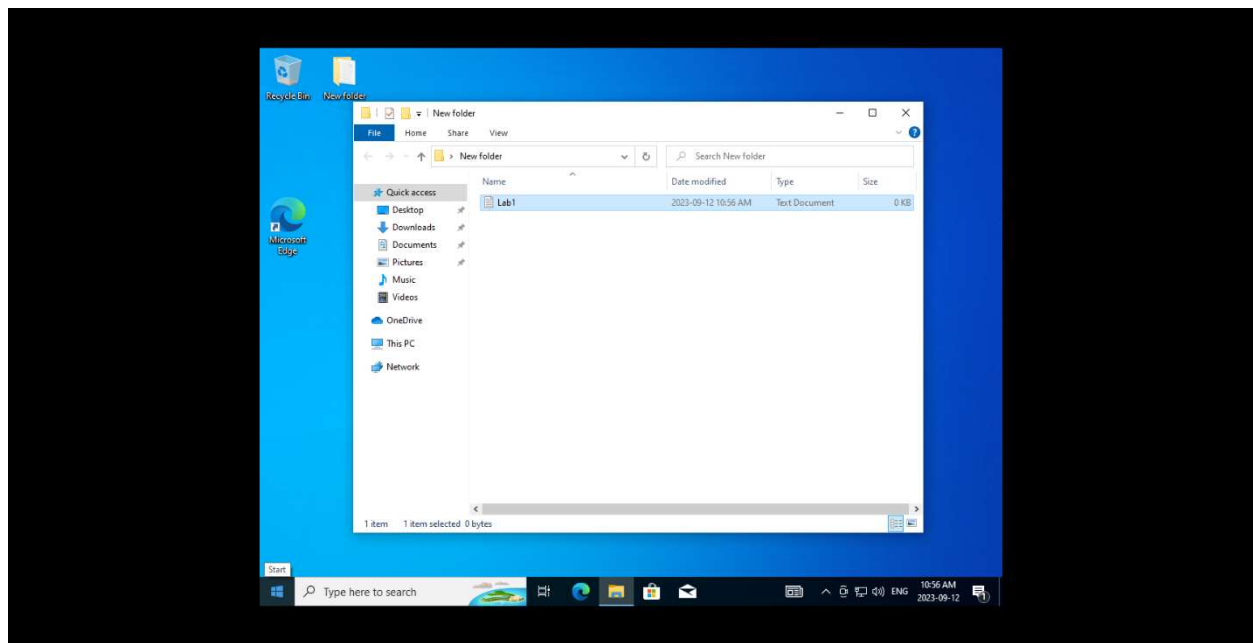
Loading ps to confirm the PowerShell user is logged in through the “C:\Users\991724818PS>” prompt



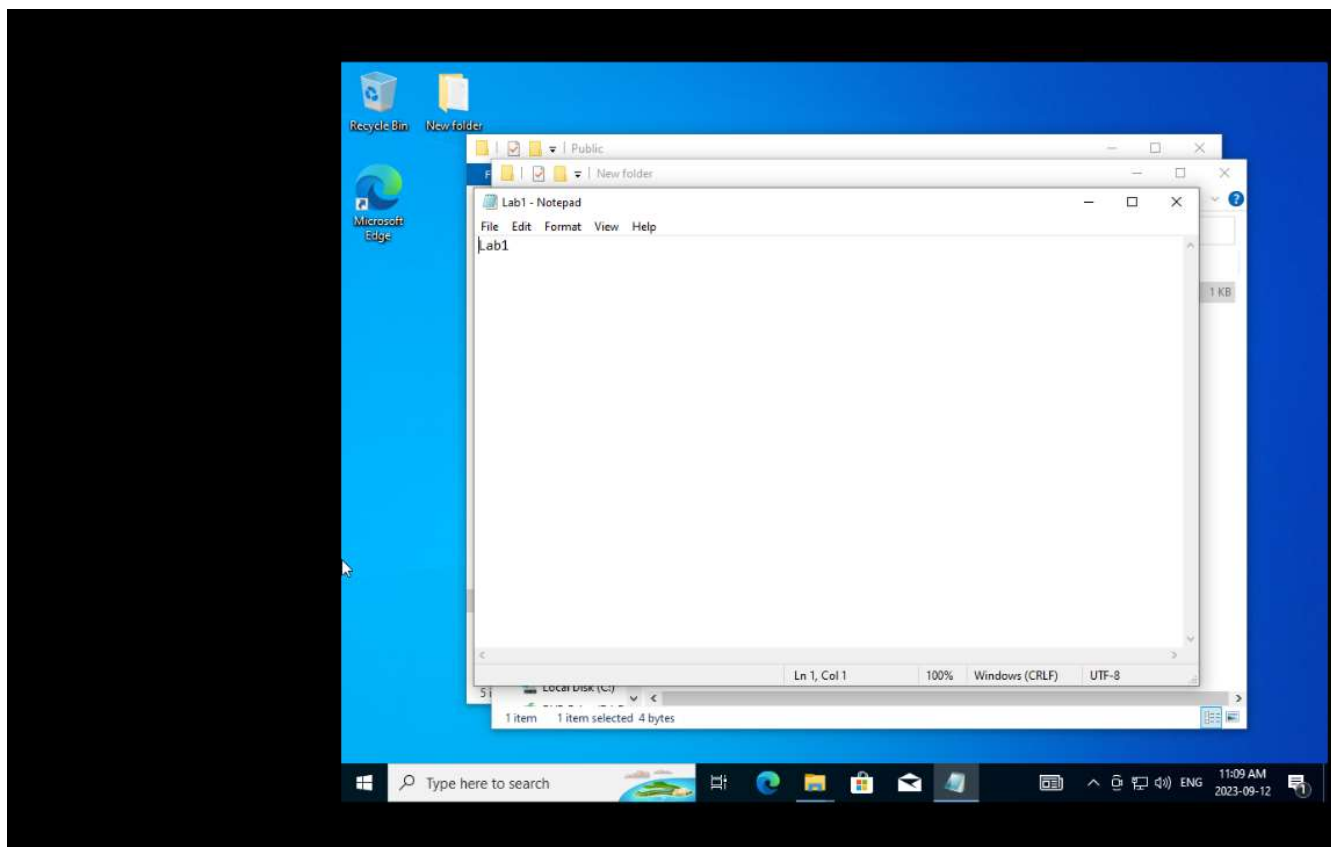
Creating a new folder on the desktop under the 991724818PS user



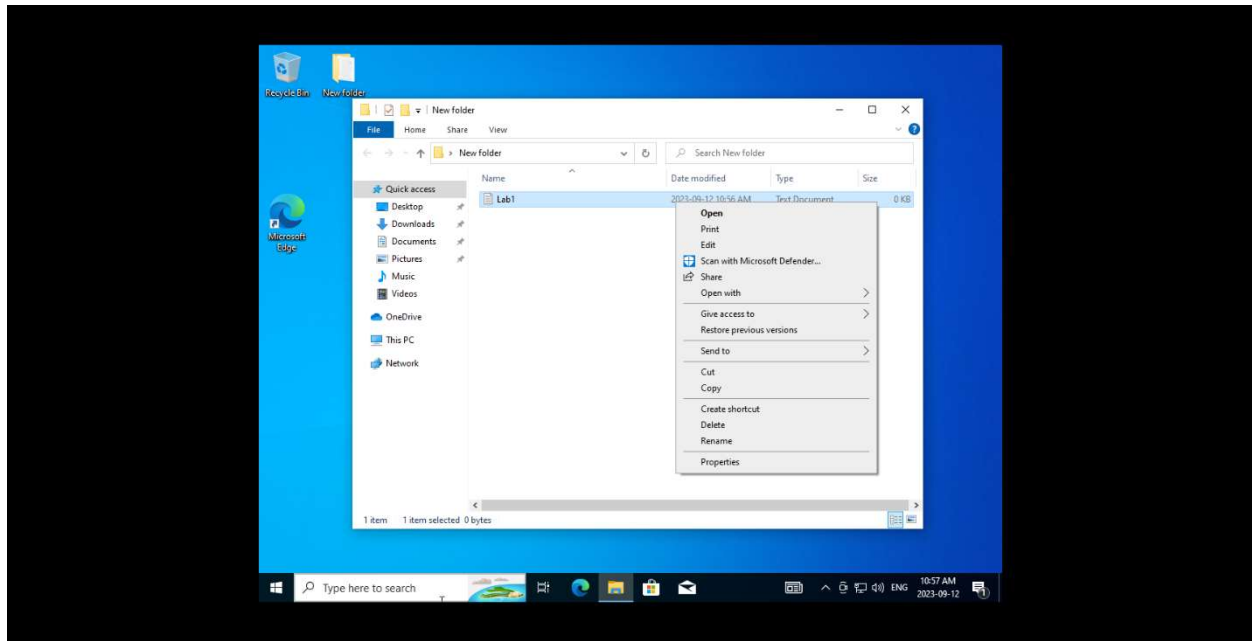
Creating a new text document



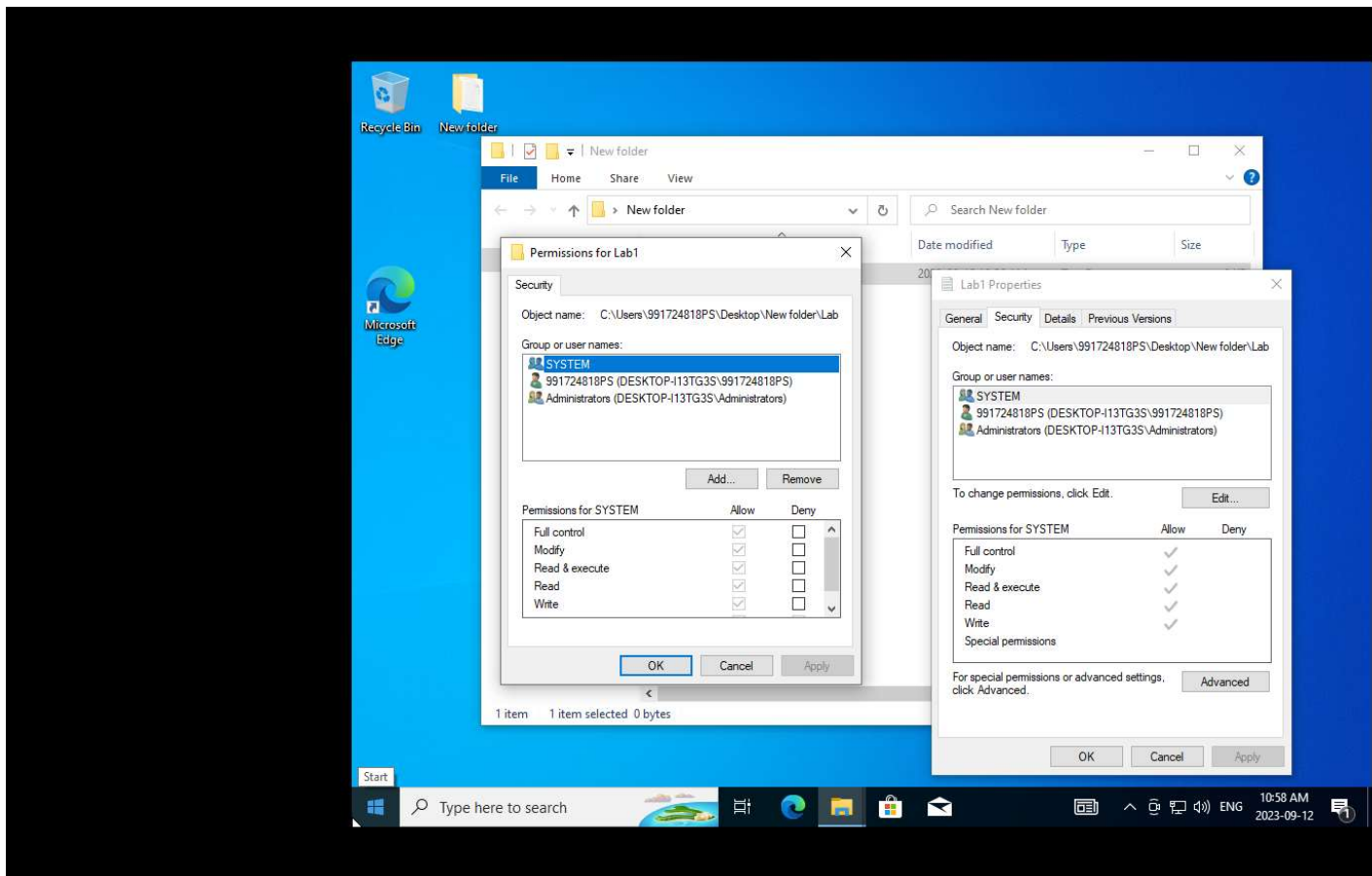
Titling the text document “Lab 1”



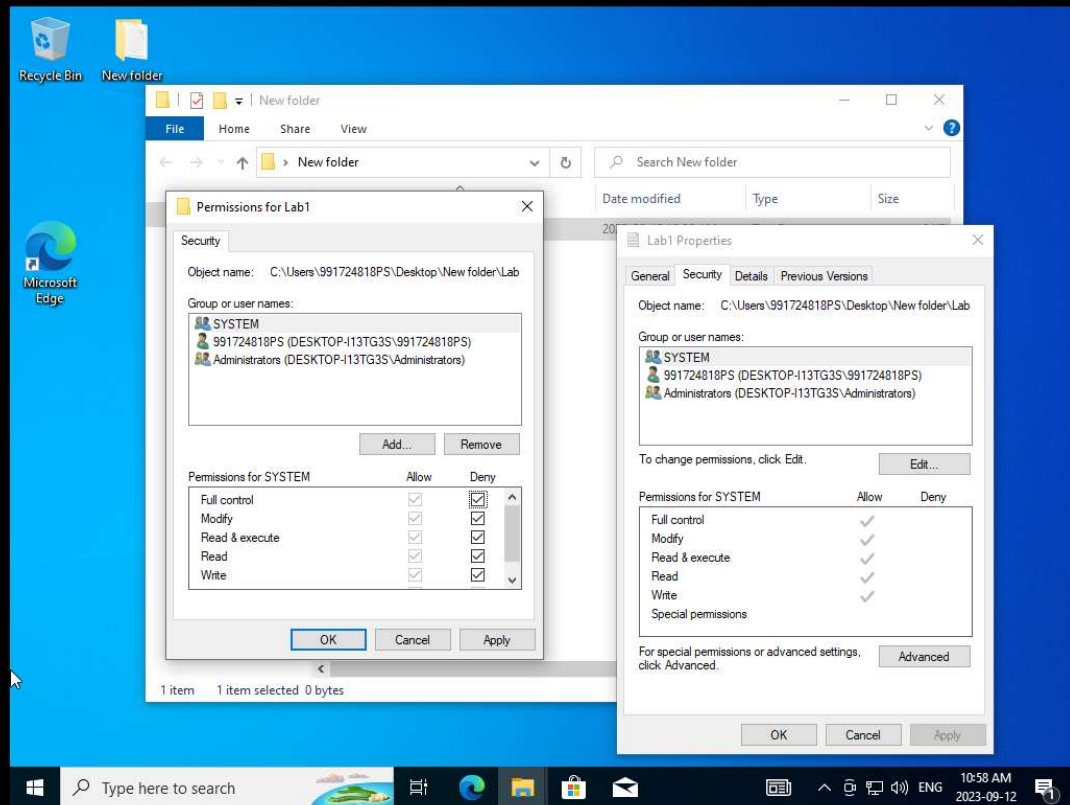
Typing “Lab 1” in the document



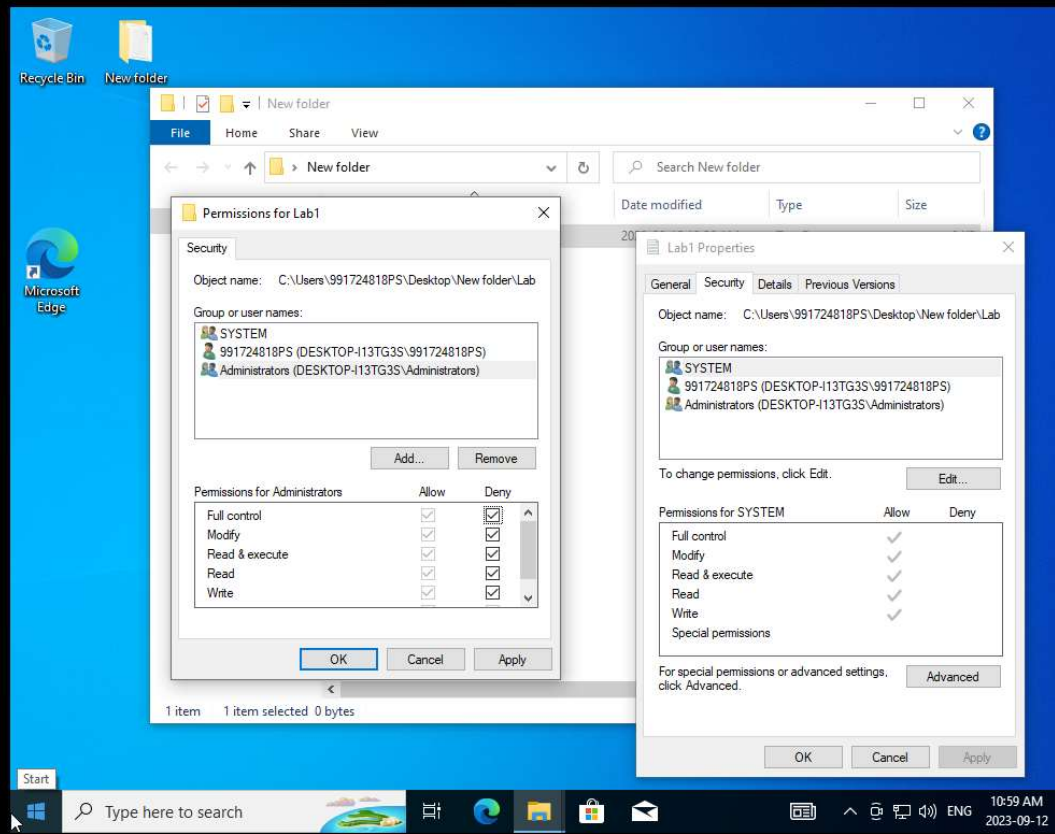
Right clicking the document to enter it's security properties



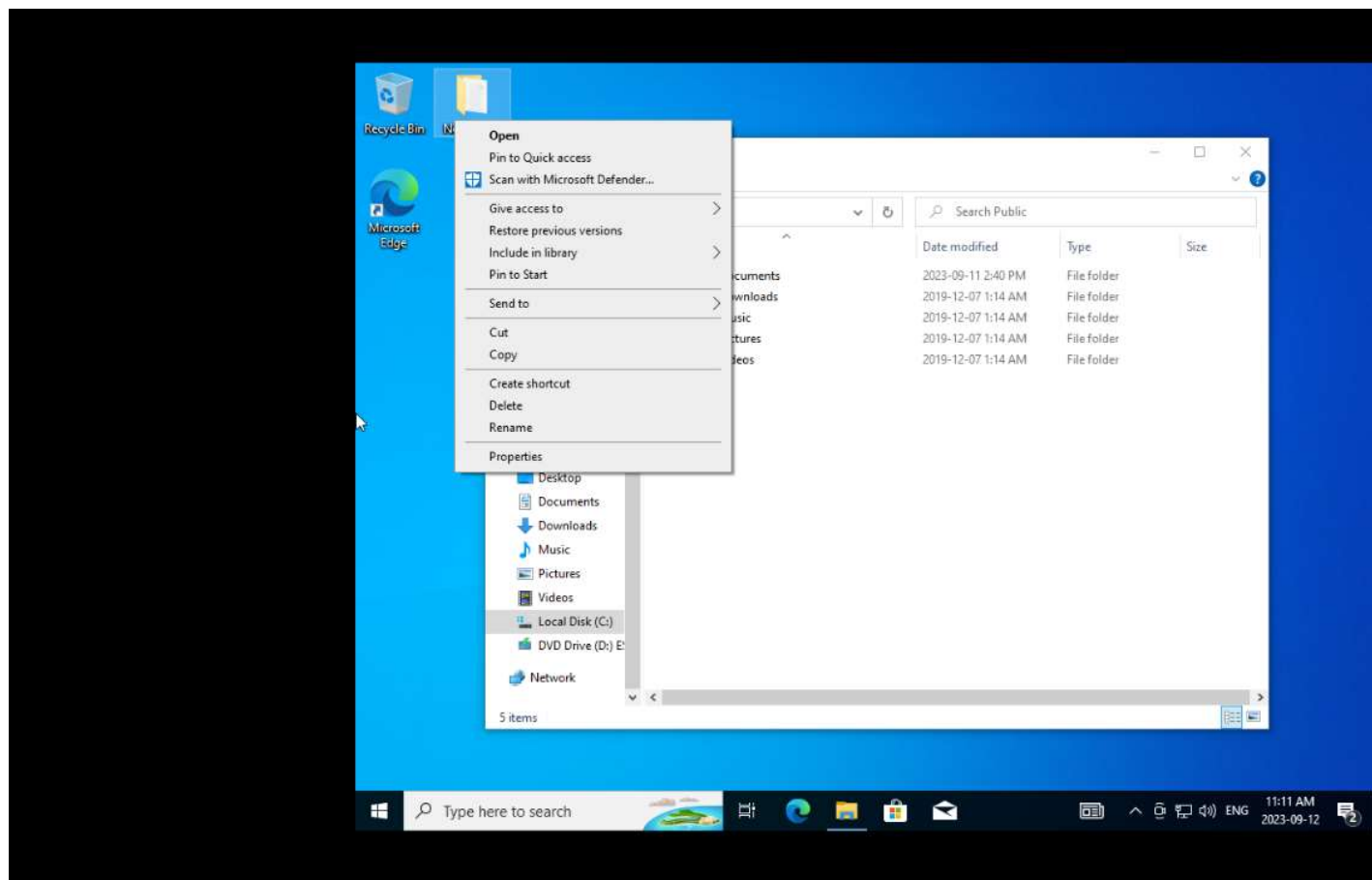
Locating the properties of the permissions of the different groups



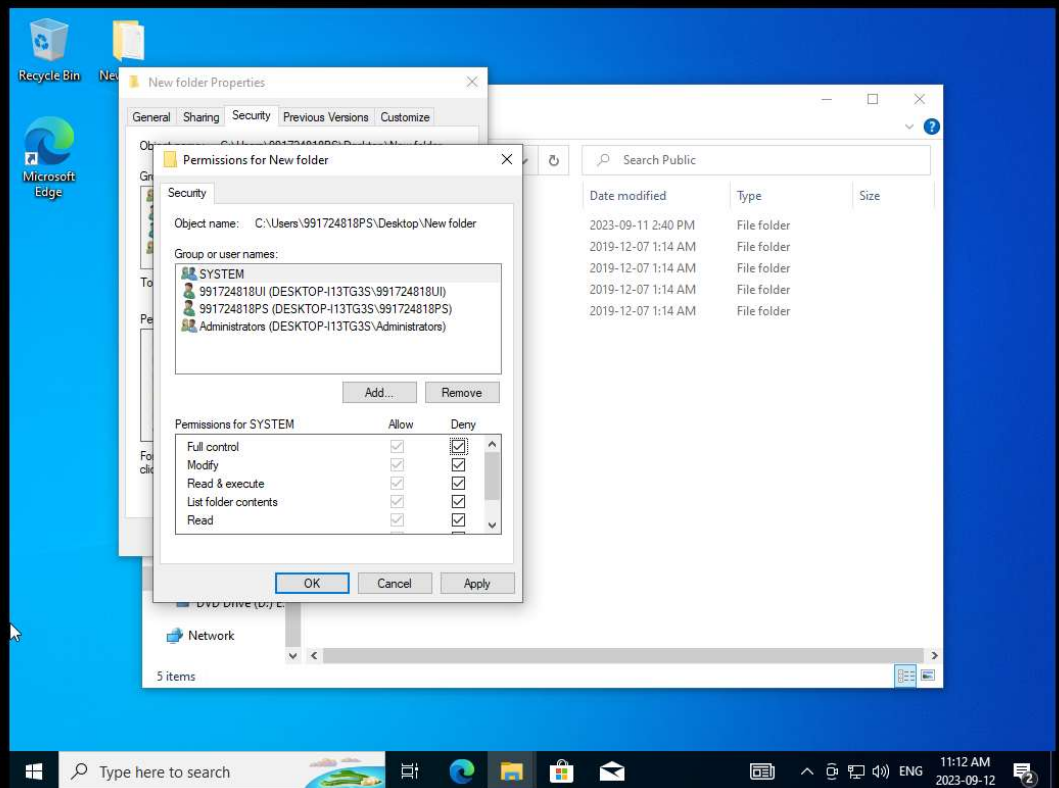
Setting system users to denied access to the text document



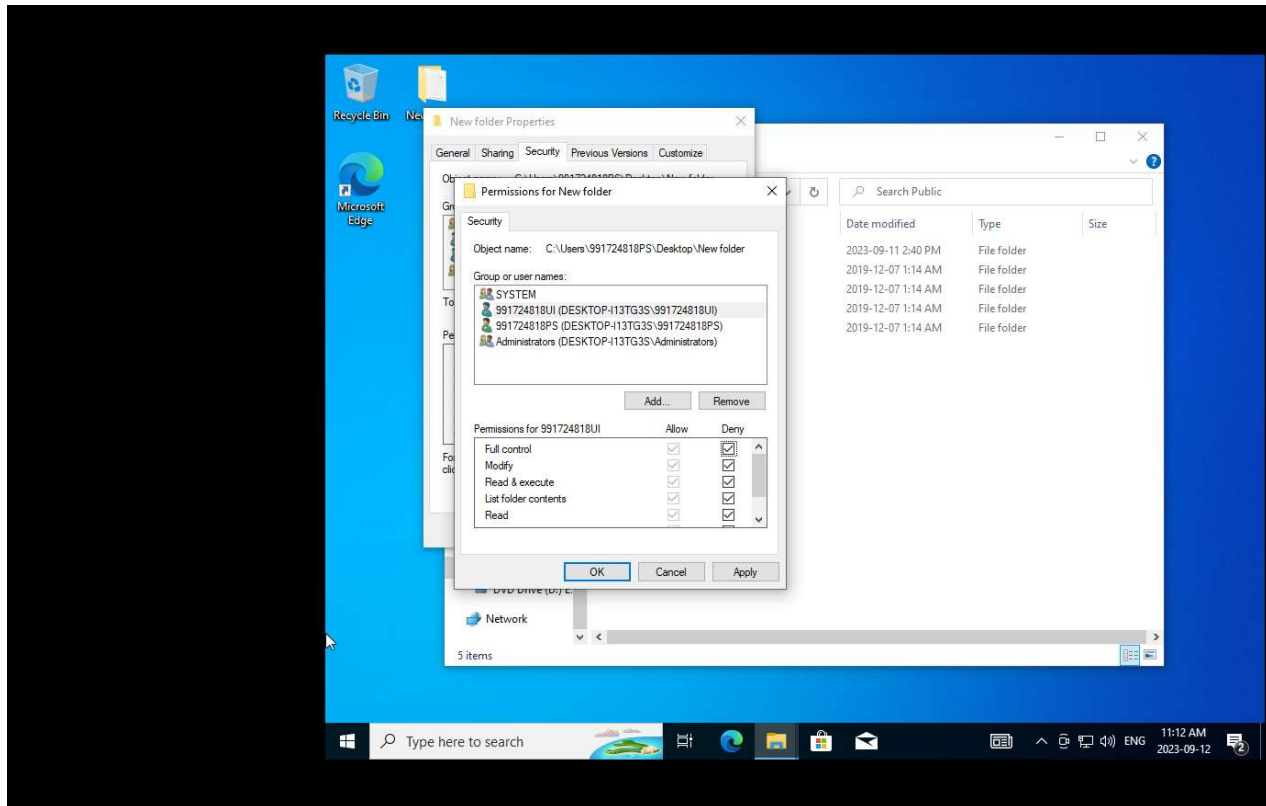
Setting administrators to denied access to the text document



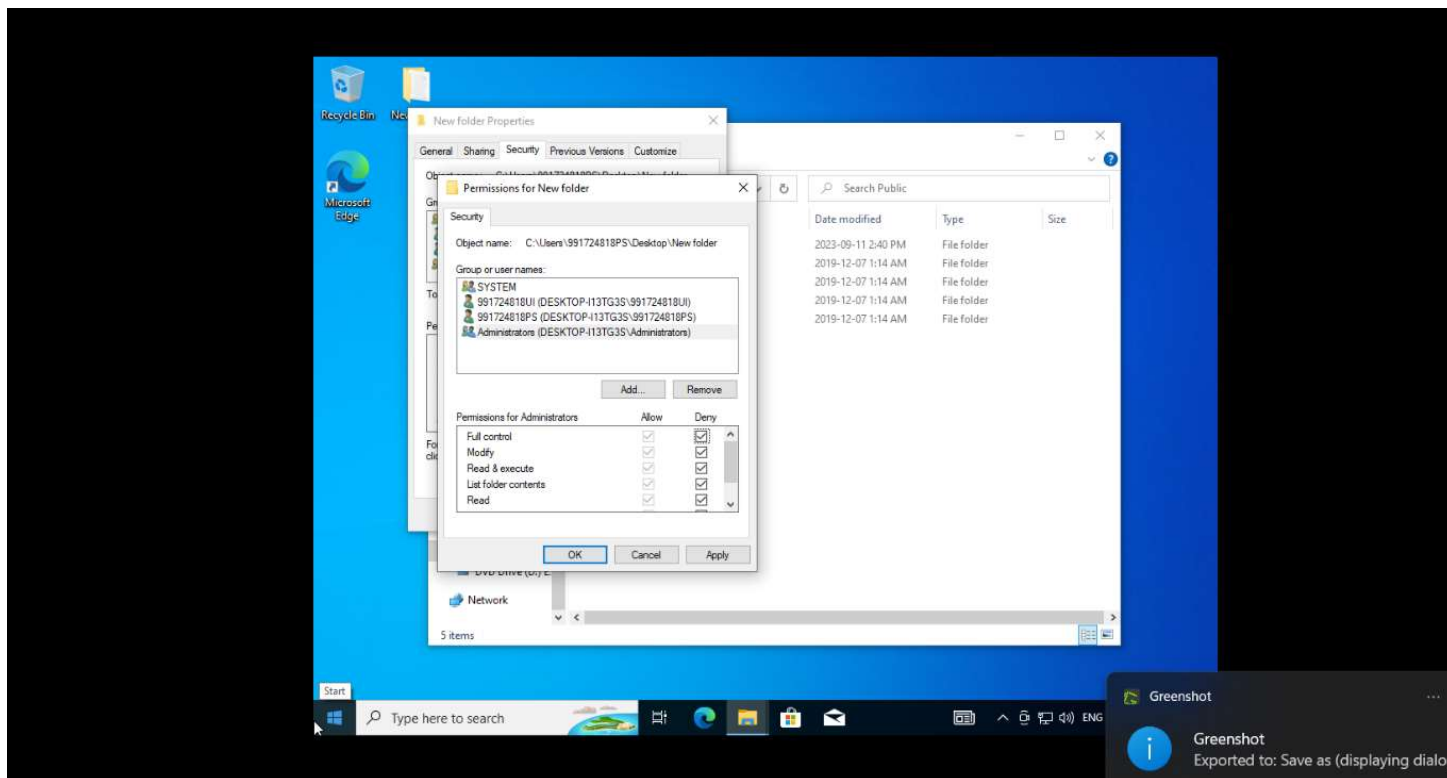
Opening the folder's properties to deny permissions for other users



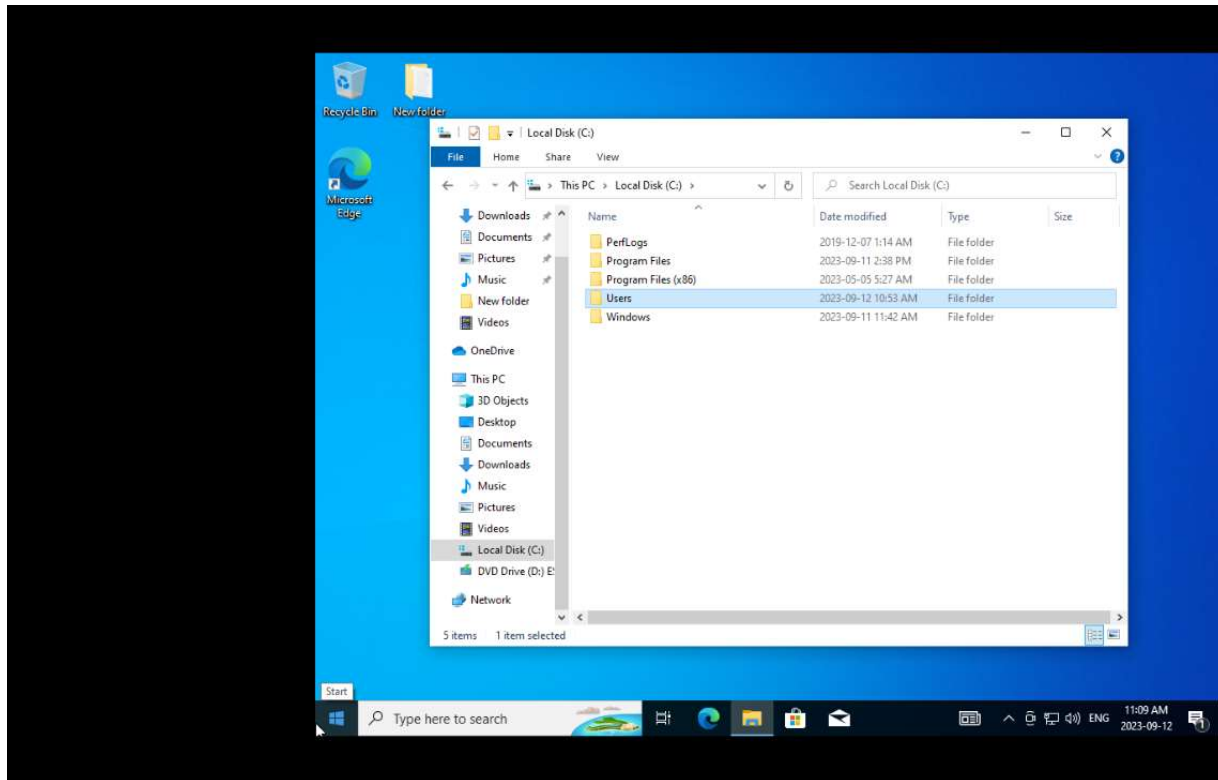
Setting system users to denied access to the folder



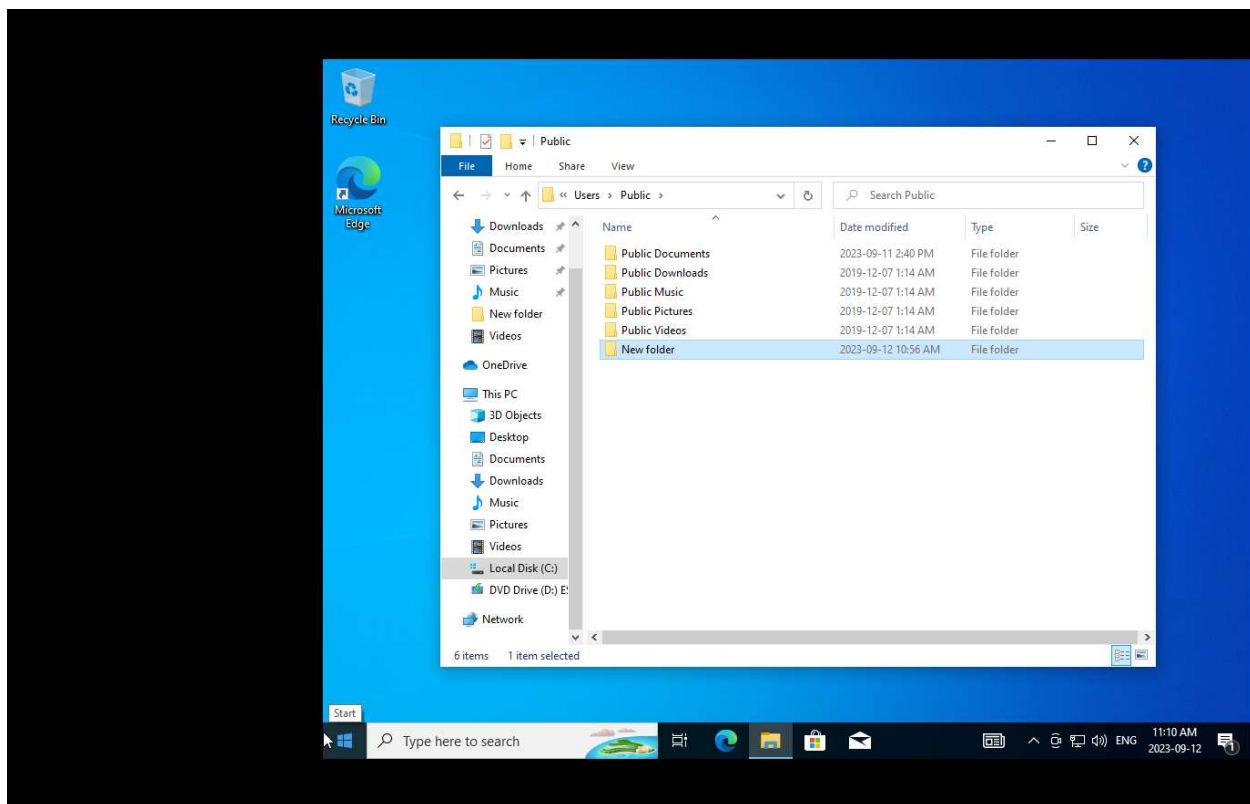
Setting 991724818UI to denied access to the folder



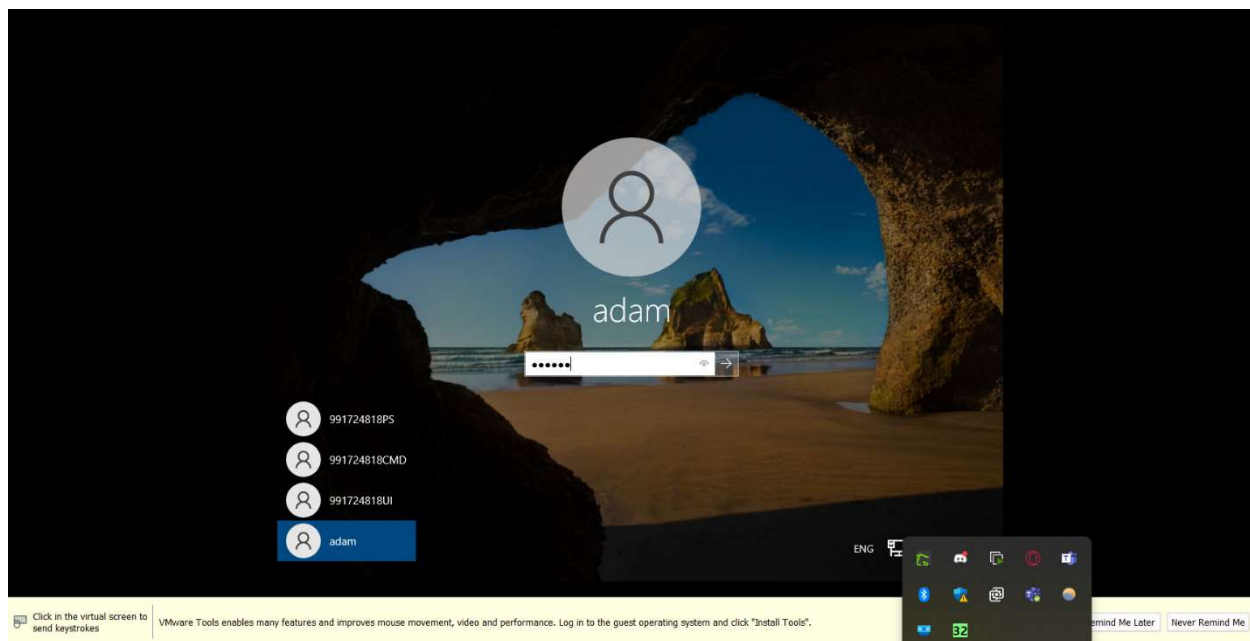
Setting administrators to denied access to the folder



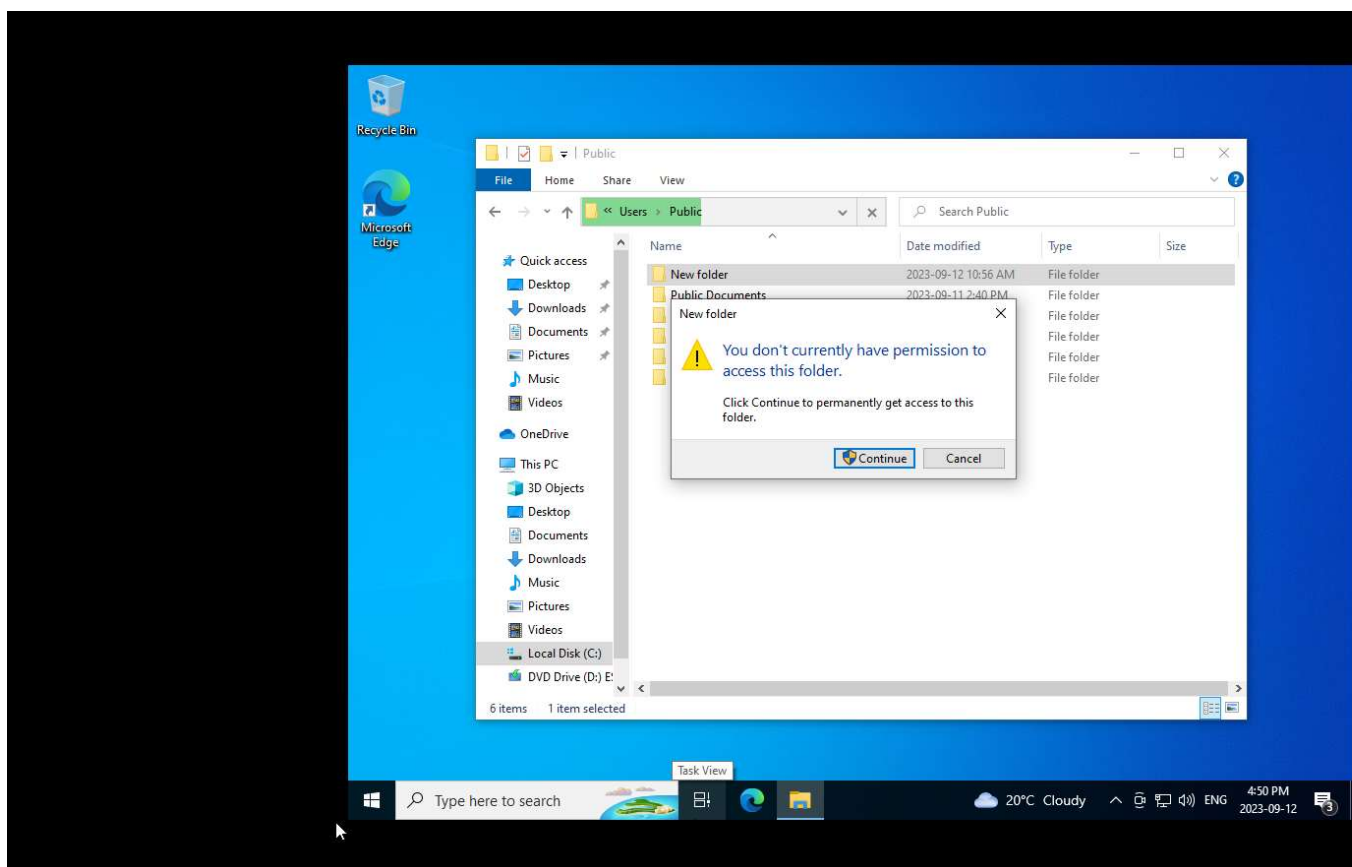
Opening the C:\ drive in order to put the folder into the public folder



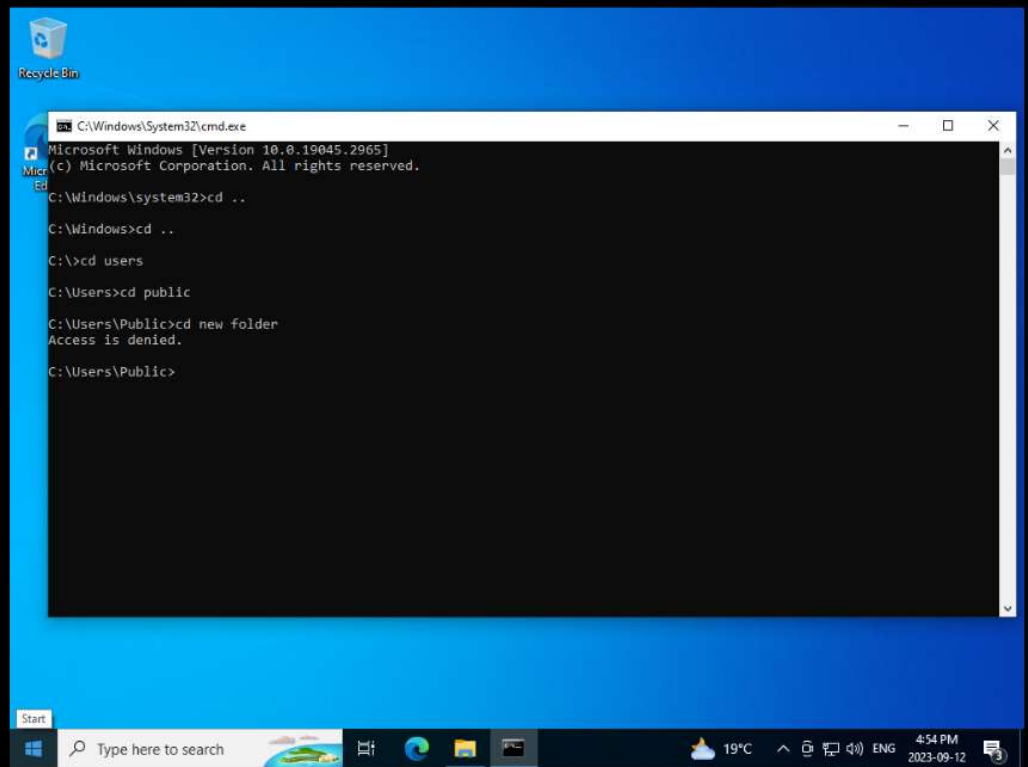
Placed the folder into C:\Users\Public in order for all users to be able to see and open the folder



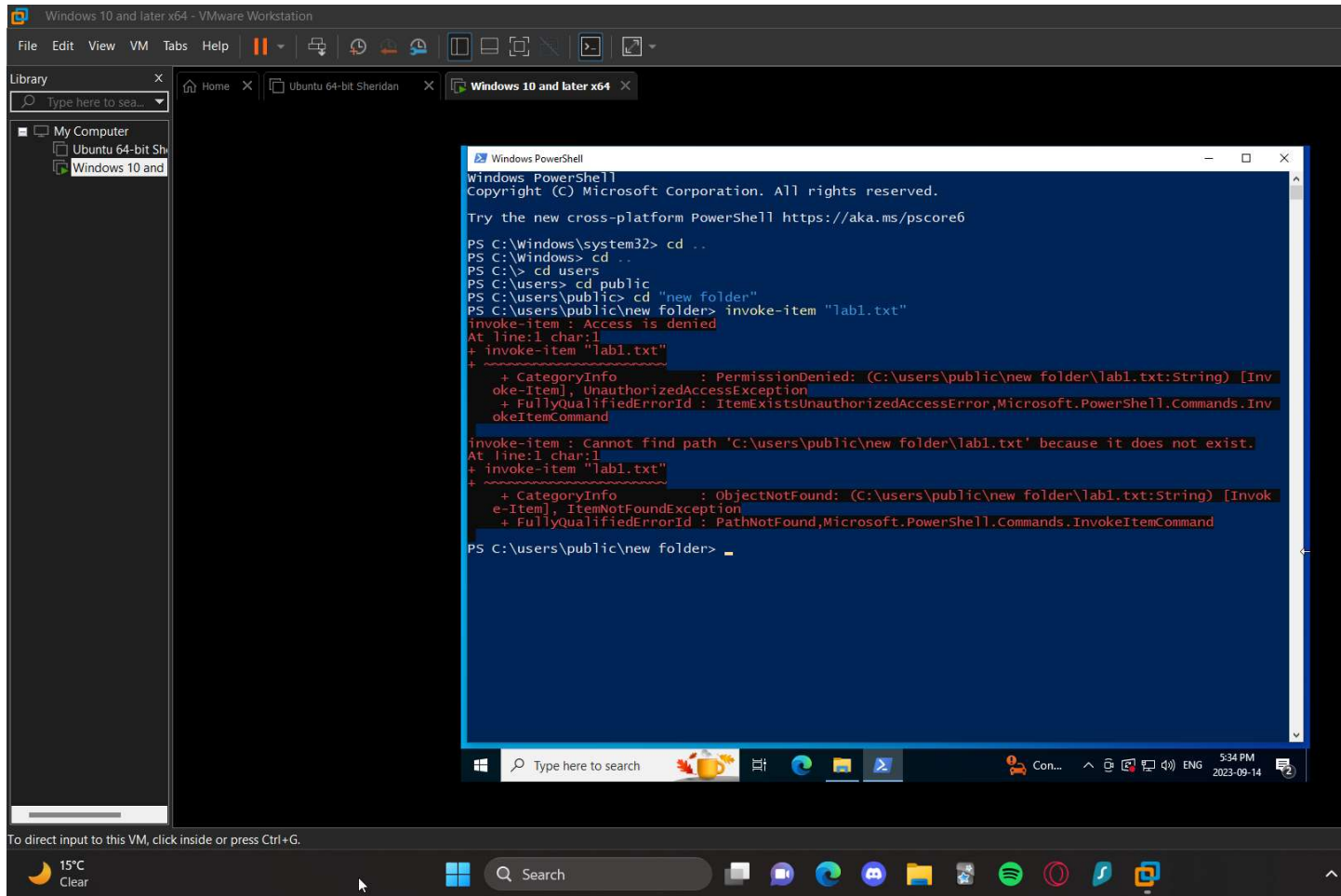
Switching to the administrator account



Attempting to open the folder within the UI option: Through the UI, it outlines that only administrators with elevated permissions can access the folder and prompts me to allow access to permanently gain those elevated permissions in regards to opening the folder



Attempting to open the folder within the cmd option: Through the cmd option, it simply outlines that access is denied and does not provide any extra options to gain administrative action to permanently gain elevated permissions in opening the file.



Attempting to open the folder within the PowerShell option: Through the PowerShell option, it allows me access to the folder which the GUI and cmd option didn't; however, it still doesn't allow access into the lab1.txt file. It outlines that access is denied due to having denied permissions. It also states that PowerShell cannot find the item path because it does not exist, even though it outlined that it recognized lab1.txt in the new folder and couldn't open it due to a lack of permissions.

Questions:

7. Although there the permission levels between administrator groups and standard users/guests can vary depending on the environment, OS, and software, there are universal settings that differ between the three. Initially, users in the administrators group typically have full control over a system with access and authorization to most services. They can review logs, configurations, and manage settings that are considered to be confidential and crucial to the functioning of the network/system. Standards users and guests don't have the ability to access these services and configurations, and furthermore, they have limited access to the OS itself. Standard users typically have partial system control and can modify files, folders, etc... and run the account as a normal computer, except won't have the privilege of elevated permissions. Depending on the environment, standard users may have access to certain permissions that allow software installation, changing system configuration, etc... but not as vast as administrators. Guests typically have very limited access; they can't modify or delete files, and instead just browse the OS. They would not have access to any setting that would change, update, or modify the OS.

8. User level settings are defined as personalized settings specific to that user such as user profile information, types of notification pop-ups, personalization settings such as time zone and data format, accessibility features, and contact settings. System level settings are defined as the settings that are configured for the entire system, regardless of the user logged on such as firewall configuration settings, security policies such as password complexity, data retention policies, backup settings, and patch management. These separations of settings can be beneficial in varying situations; however, can be most beneficial in system administration. System administrators would have the access to system-level settings and create changes across a computer network instead of going to each user's computer and creating these changes one by one. Another situation this separation would be beneficial in would be computer network safety. One system-level setting listed previously are firewall configurations that affect an entire network. Since these system-level settings are permissions that not everyone can access, if people did have access, it can jeopardize the safety of the network.

9. A computer would need different levels of permissions based on their authorization/responsibility status. For example, a company could implement the least-privilege policy. The least-privilege policy outlines that users should only receive the adequate amount of permissions based on the responsibilities they have and the tasks they must complete. These users, although may have specific elevated permissions, don't need to the same permissions as a superuser or a systems administrator. These unnecessary allocated permissions could also breach a safety issue; regular users could have access to private information, networking information, etc... which can potentially harm the company's business proceedings and safety. Another example of why computers need different levels of permissions can revolve around a family environment. If a parent wants to set a certain screen time limit, they can configure it so their child's user cannot change that limit. Ultimately, different levels of permissions prevent breaching safety, privacy, and unauthorized control.