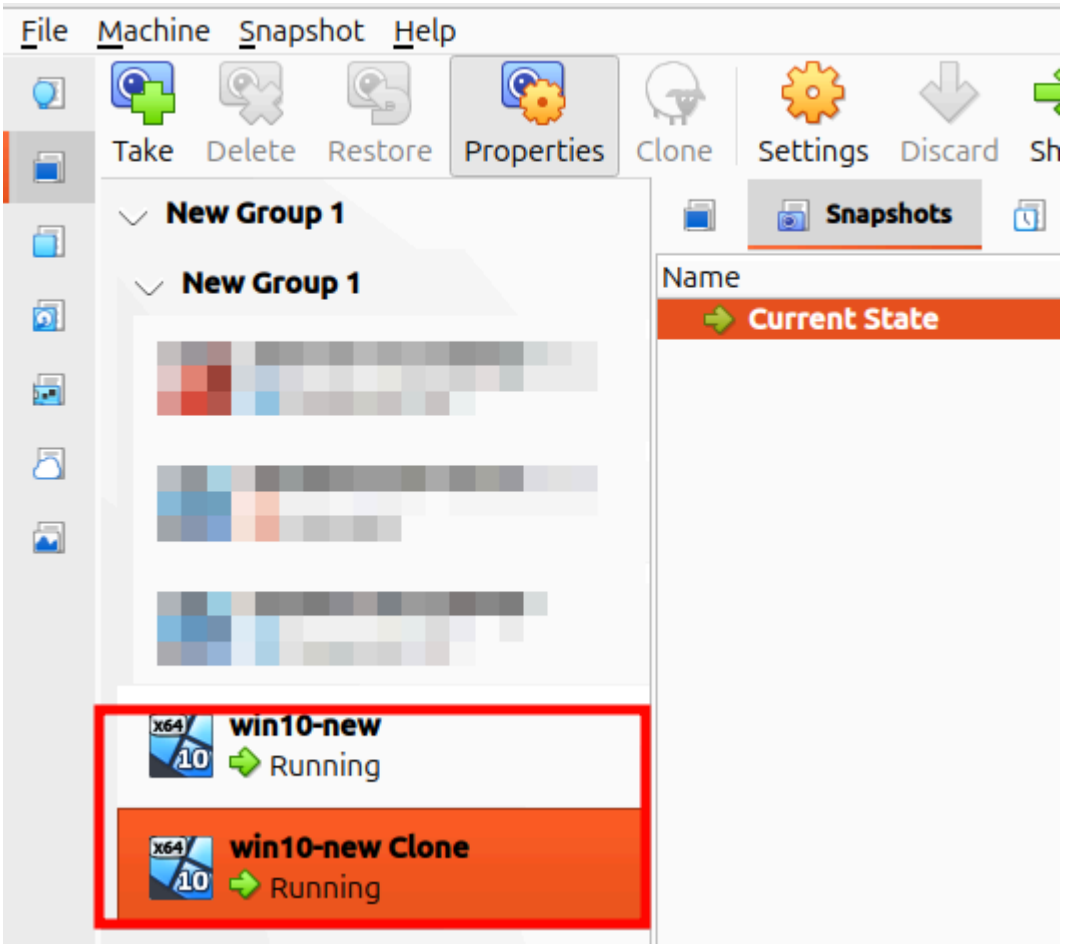
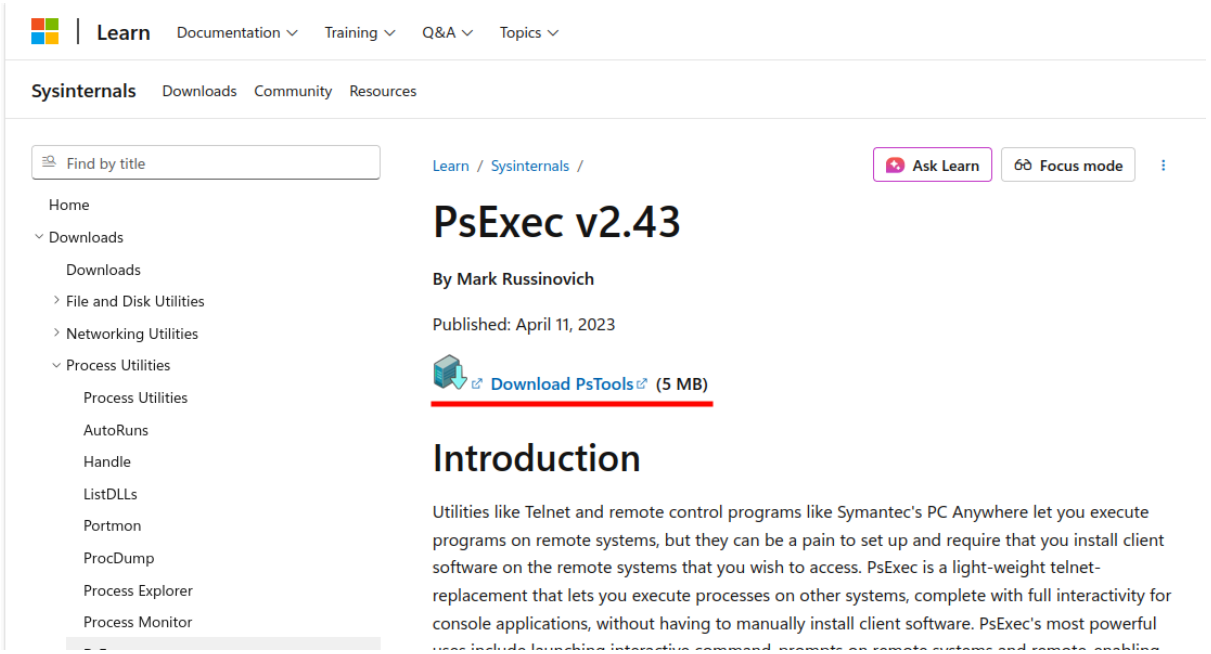
Brandon Gracy *10/01/2026*

In this lab we are going to see how to detect and analyse lateral movement using PsExec, a legitimate Windows sysinternals tool often exploited by attackers.

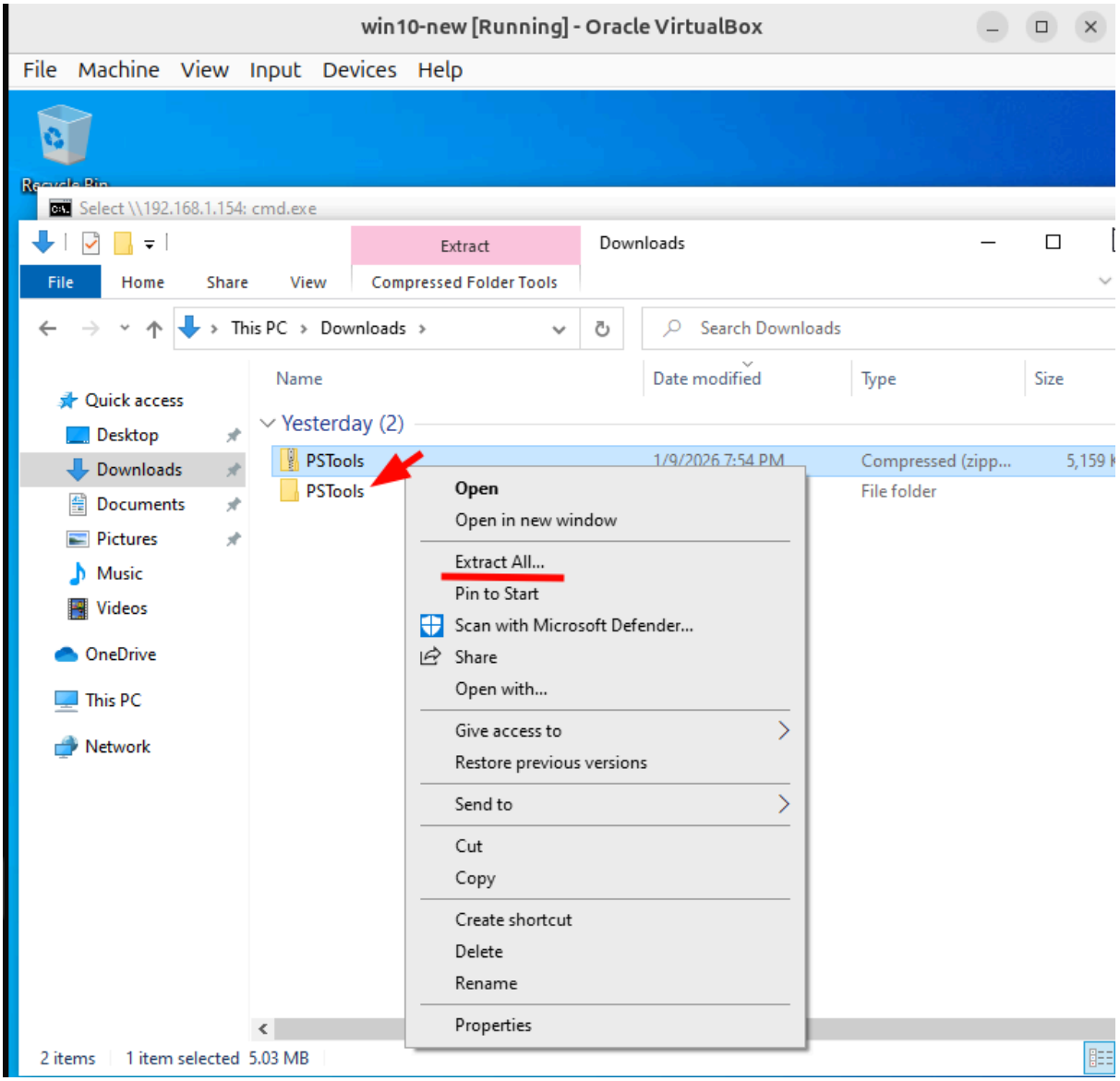
Now we are going to start from using two windows VMs, one going to be the machine that we are using to exploit and other that will be the target.



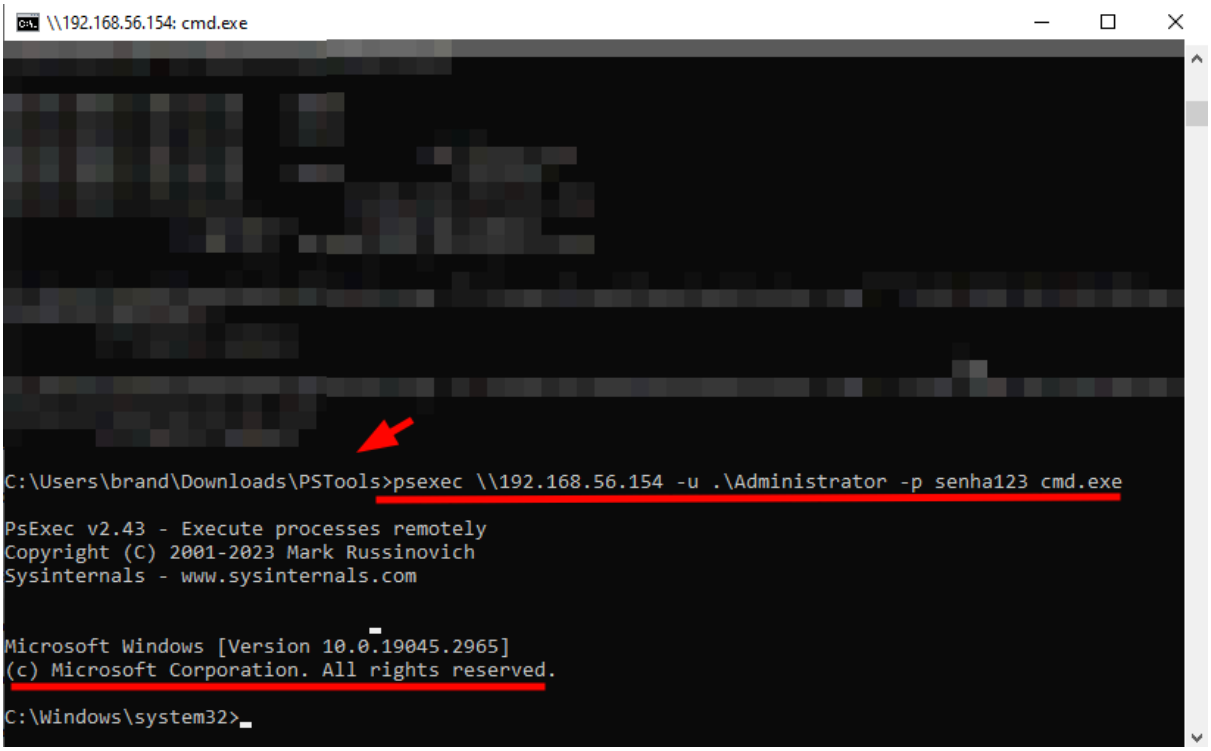
Win10-new will be our machine to exploit and the win10-new clone will be our target.



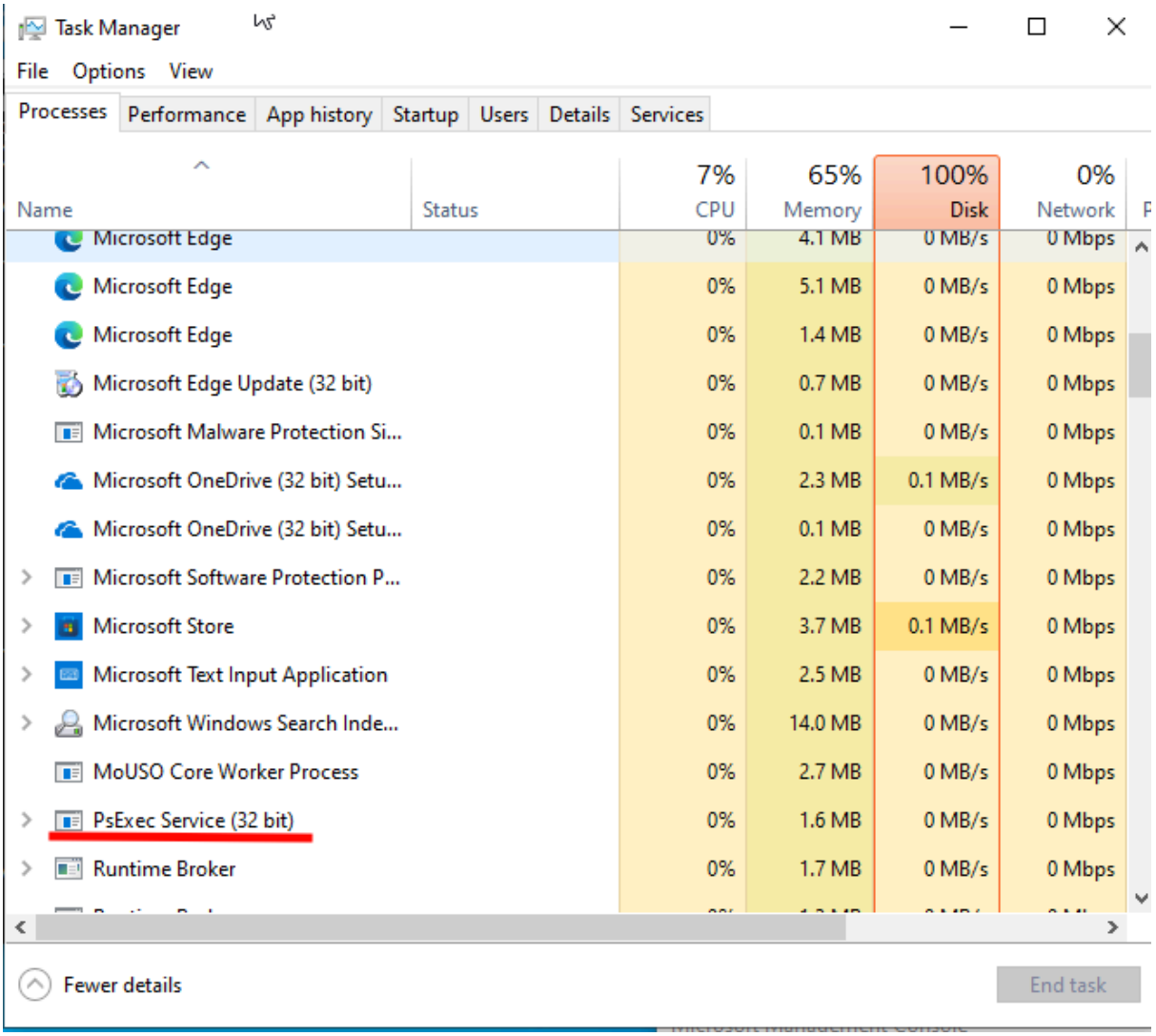
To use the PsExec, we have to enter in the site of Microsoft and downloaded the file PsExec v2.43.



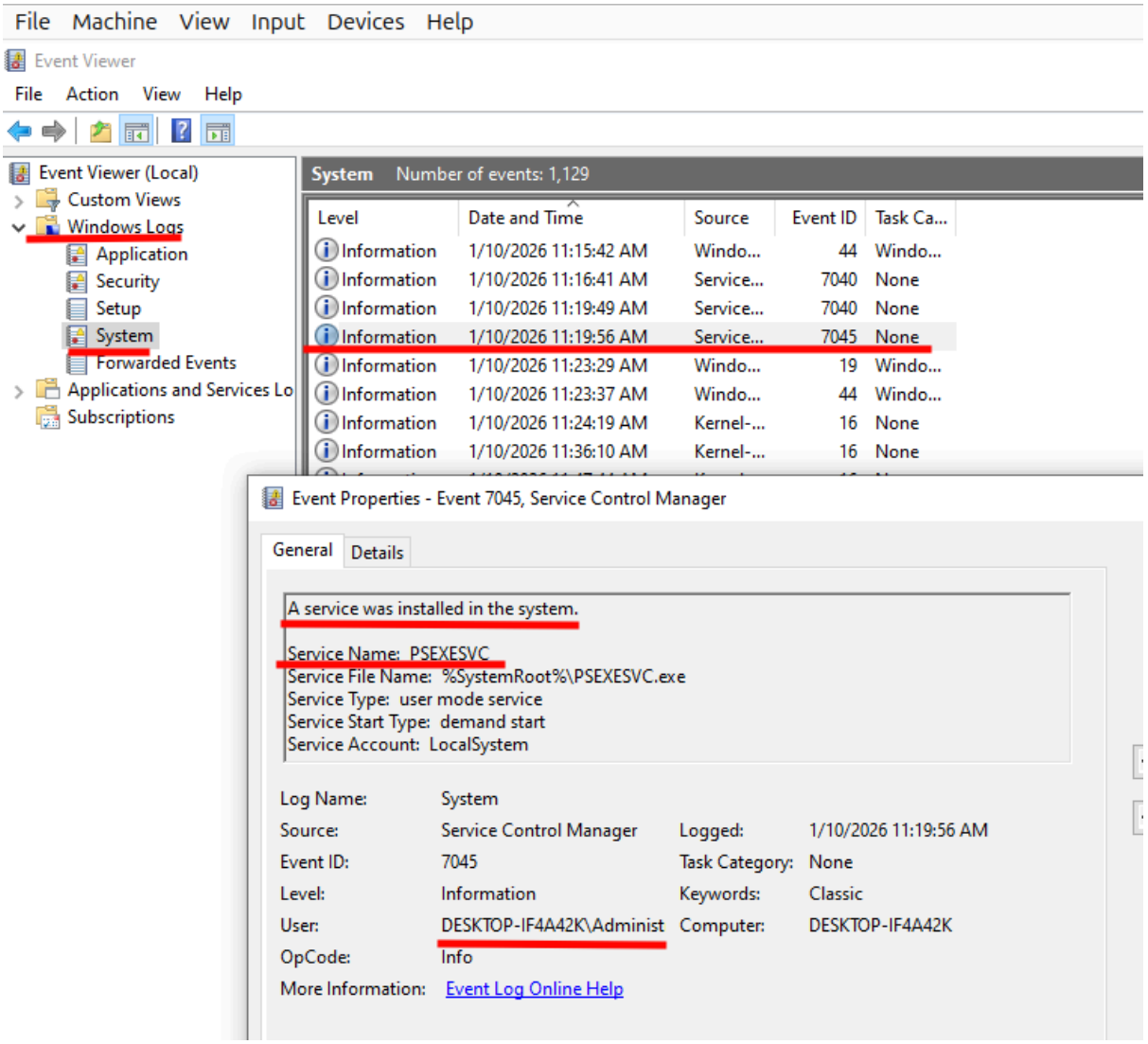
After downloading, we just need to extract the contents of the folder.



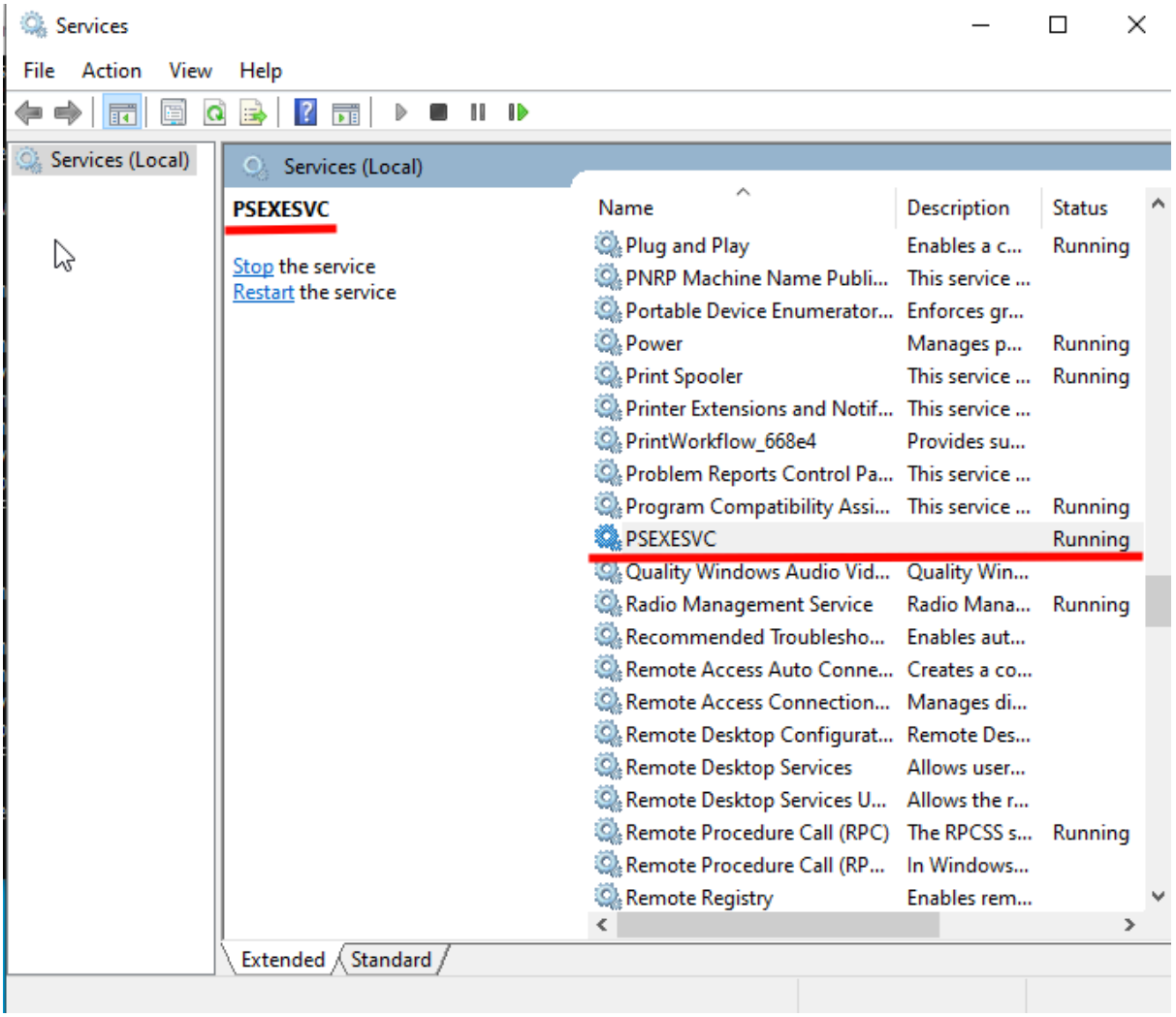
Now, when we ran this command, if successful, this opens a remote shell on our target.



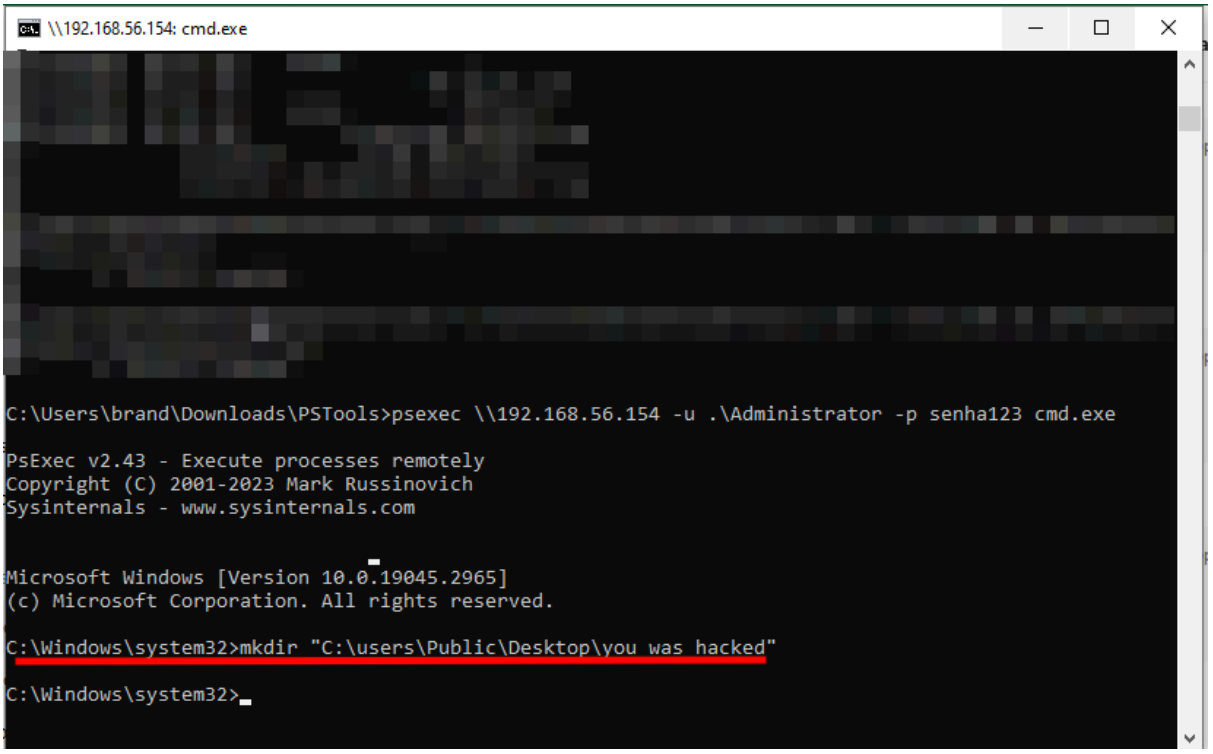
If we enter in the task manager, of course in the target machine, we can see the PsExec running in the second plan.



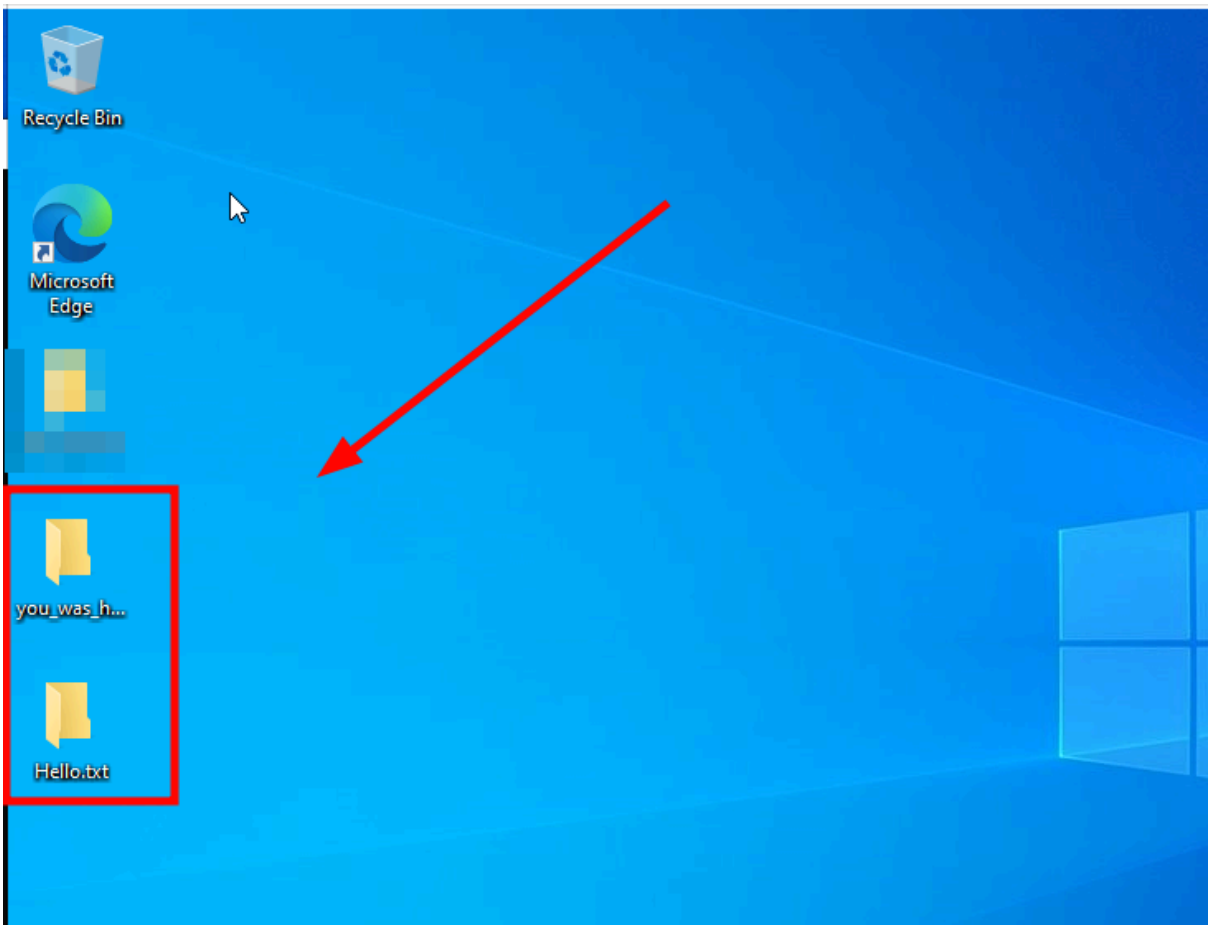
If we enter in the event viewer, we can notice that a service was installed in the system, the PSEXESVC.



If we press the win + r and write service.msc, we can check the PSEXESVC running.

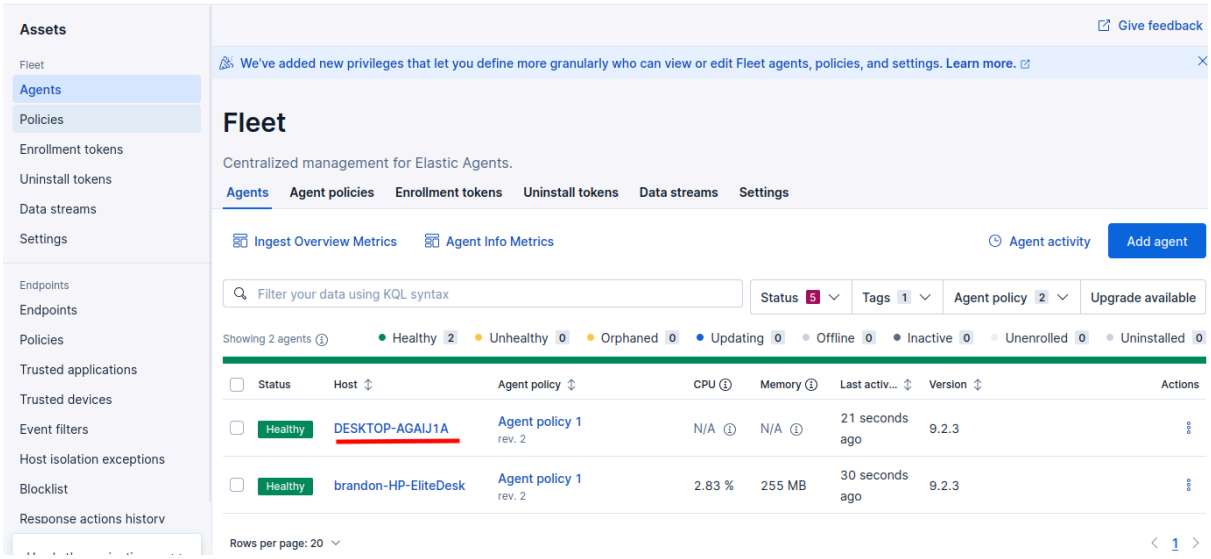


Now, let's run this command to create a file in our target.

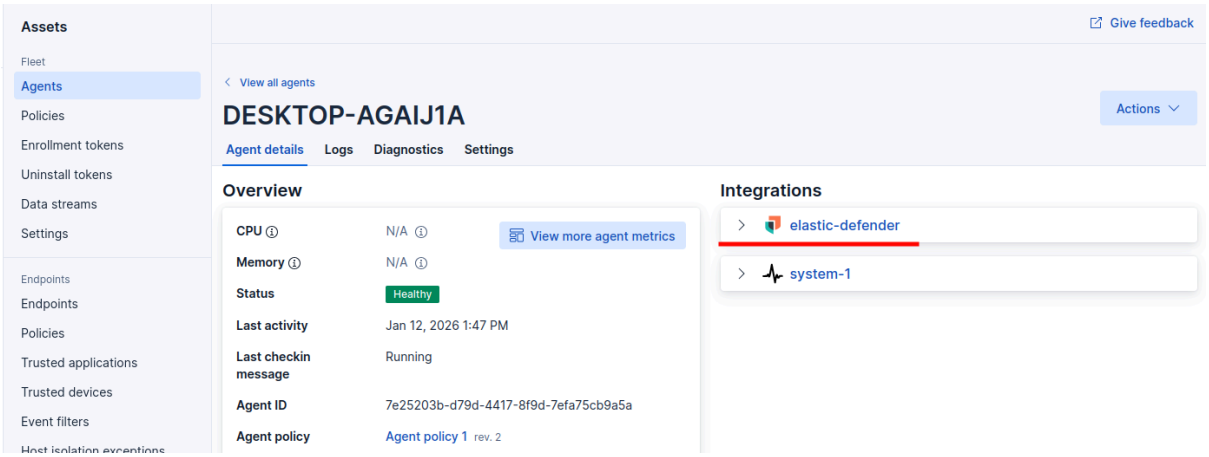


Here we can check that the file was created successfully.

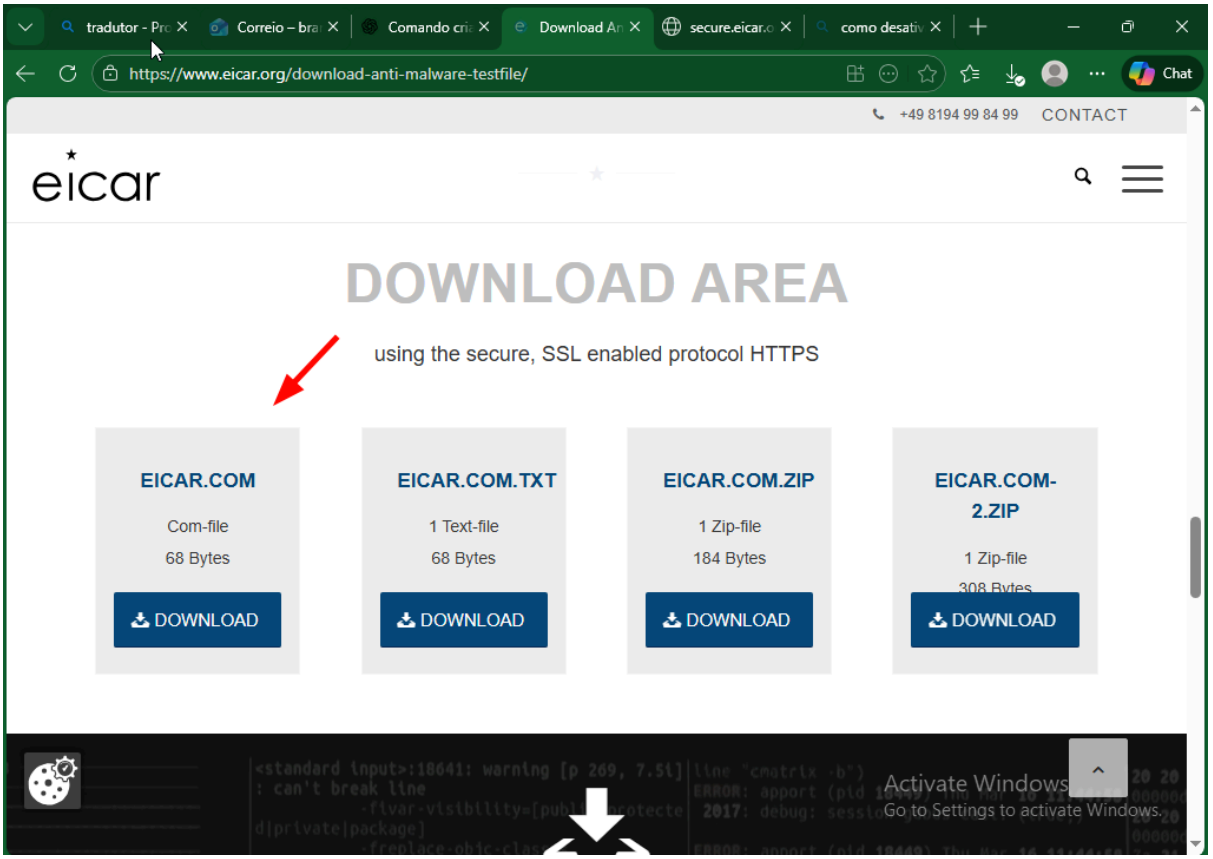
Now we are going to use the elastic cloud to watch our target machine.



Lets start installing the agent in the machine target.

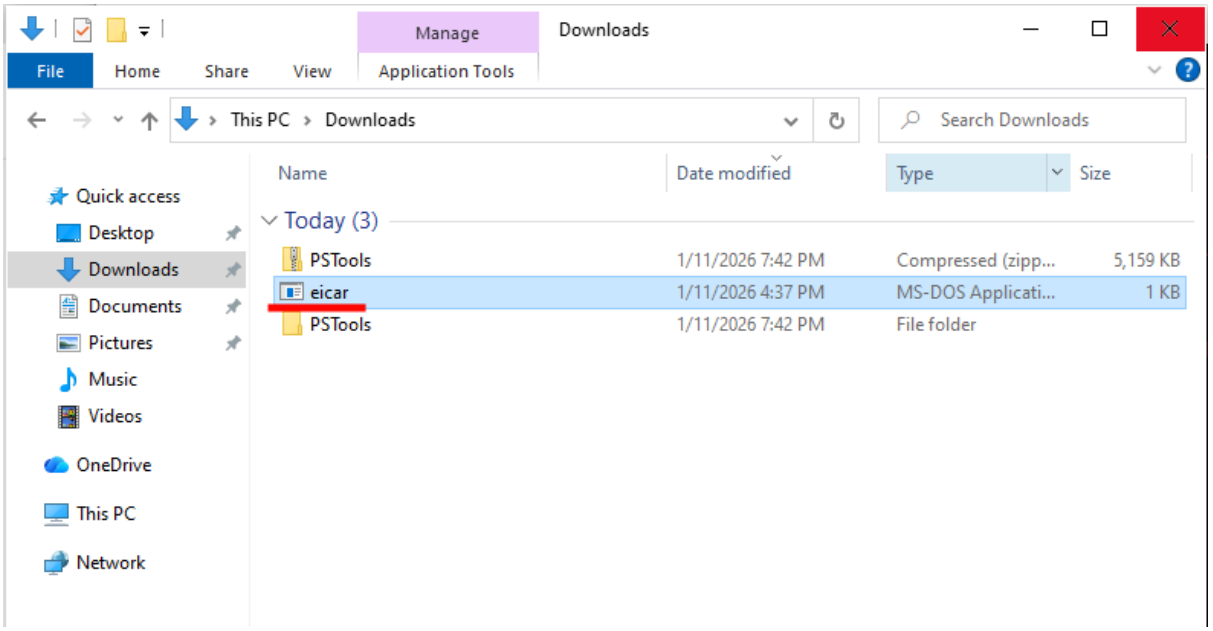


Let's add the integration elastic-defender to obtain information if something wrong happens.

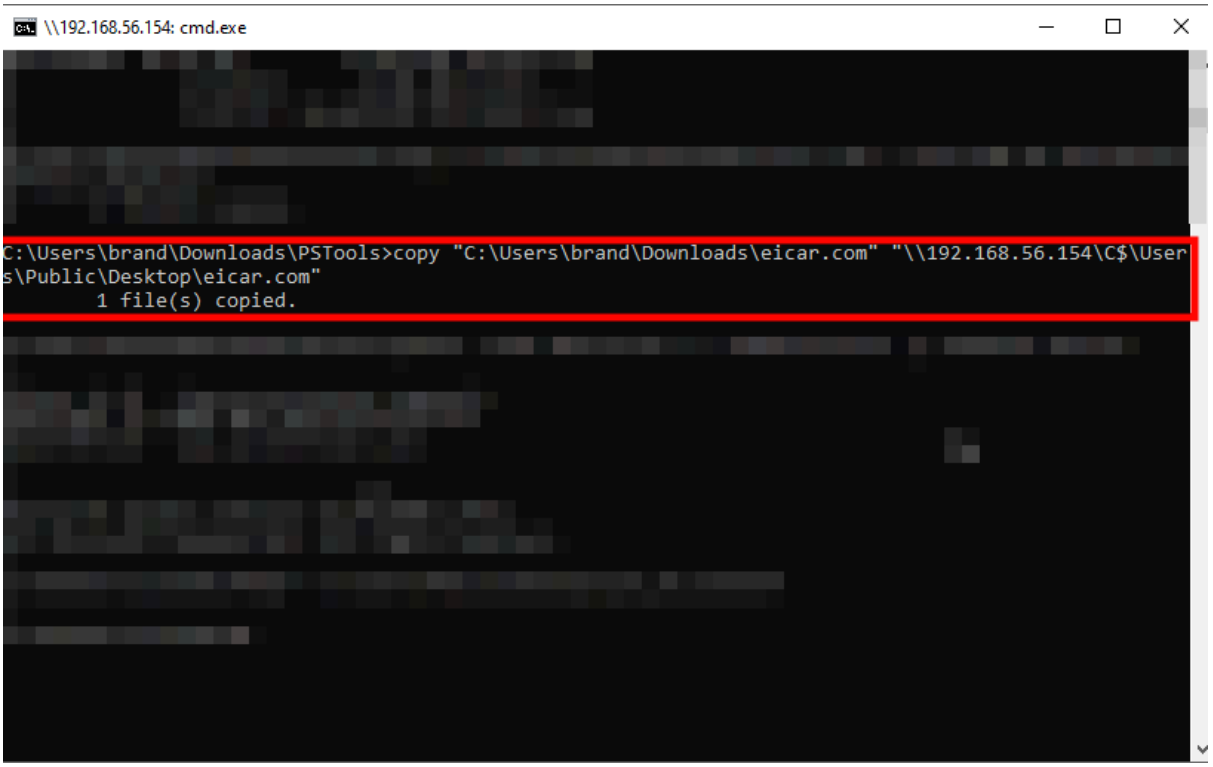


Now, in the machine that you are running the PsExec, let's download the Eicar test, it is a malware test.

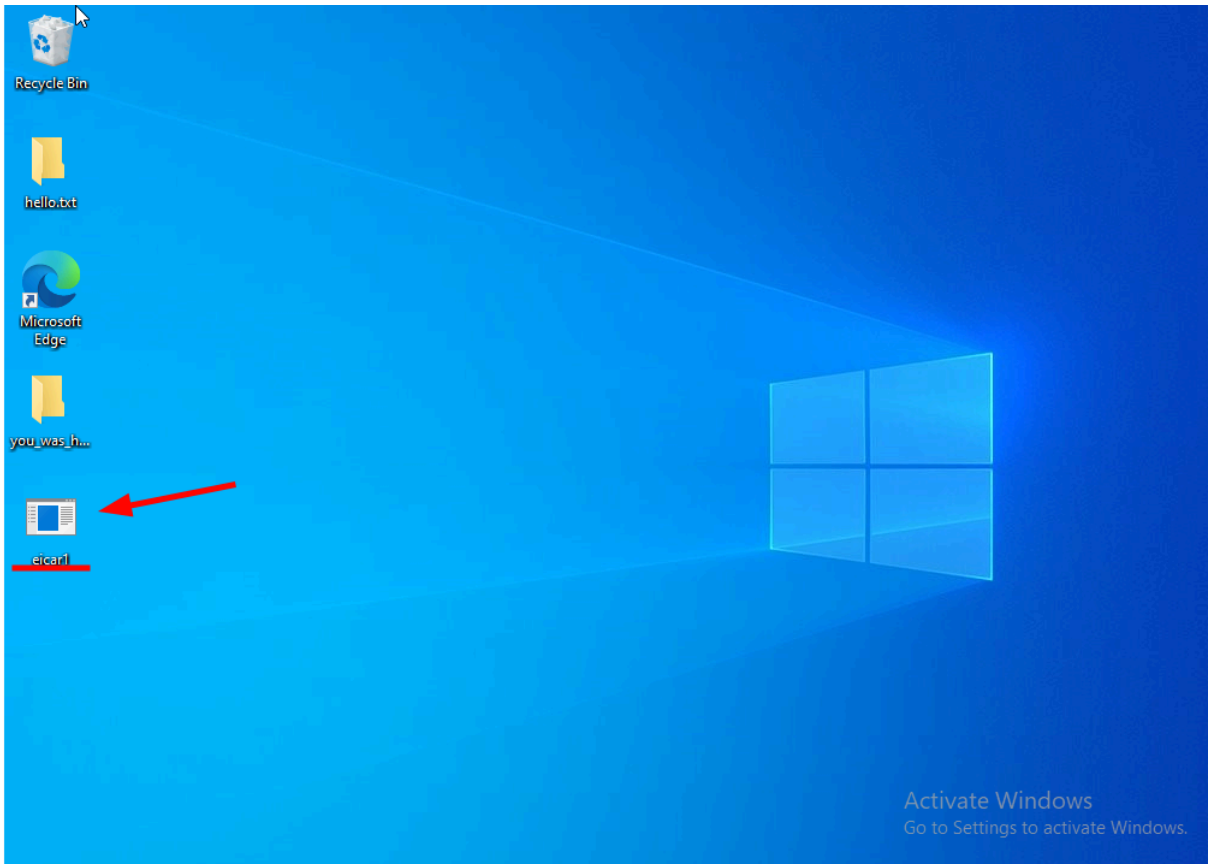
To download the Eicar test, I have to turn off the windows defender.



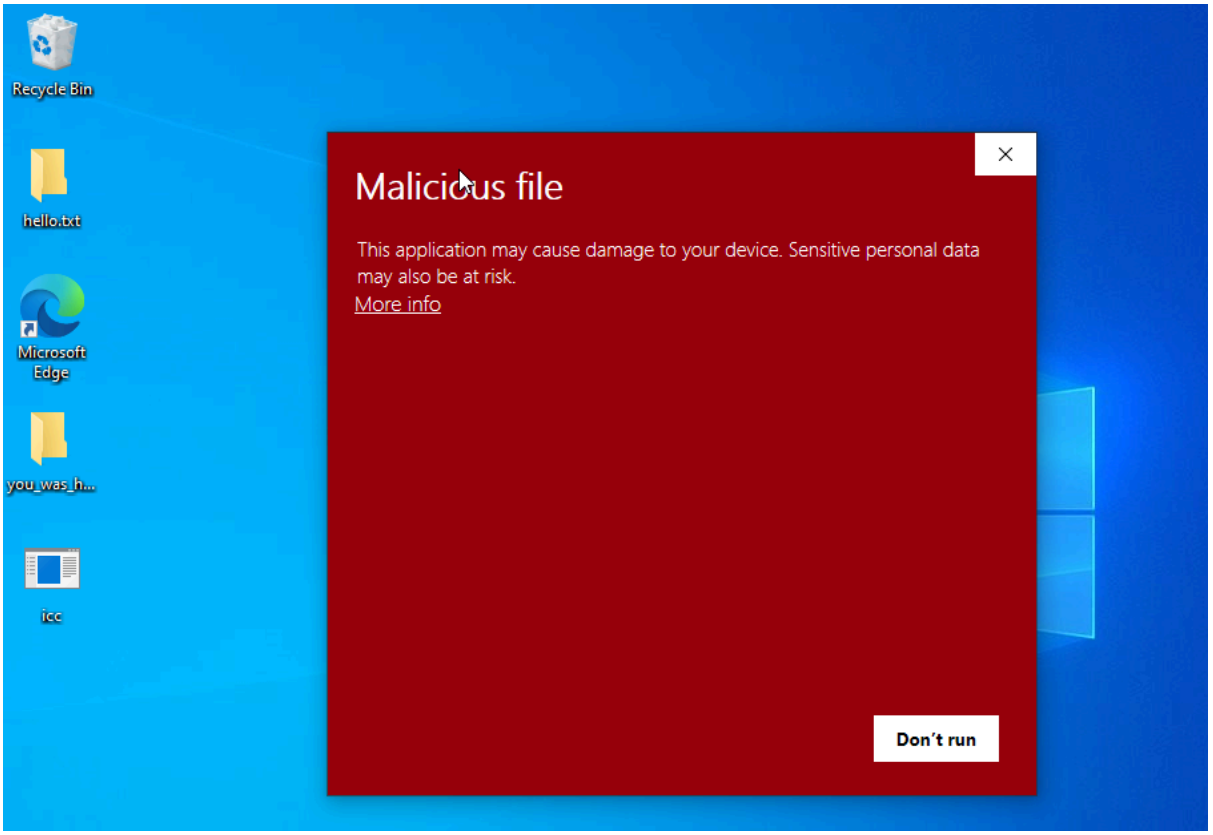
It is here, in the downloads.



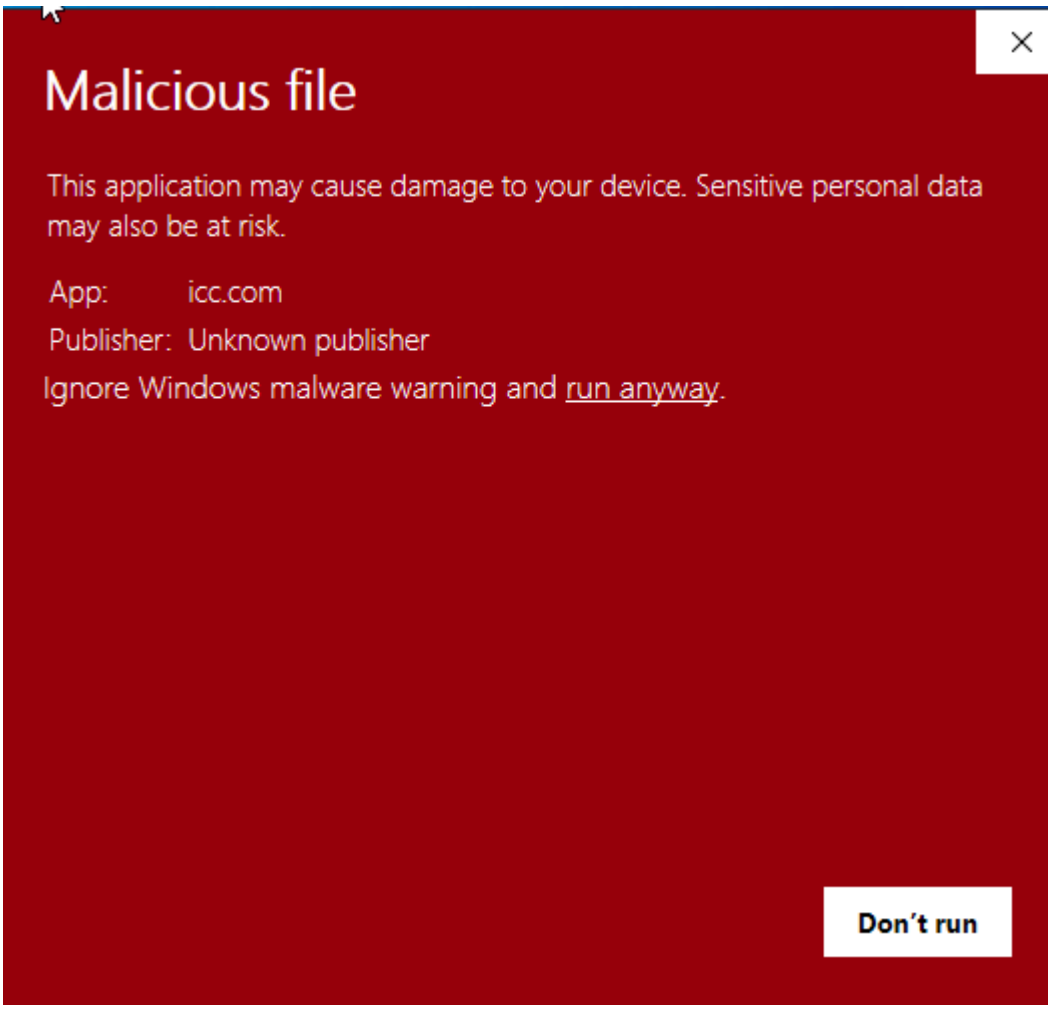
Now, we have to do this command to send this eicar test file to our target.



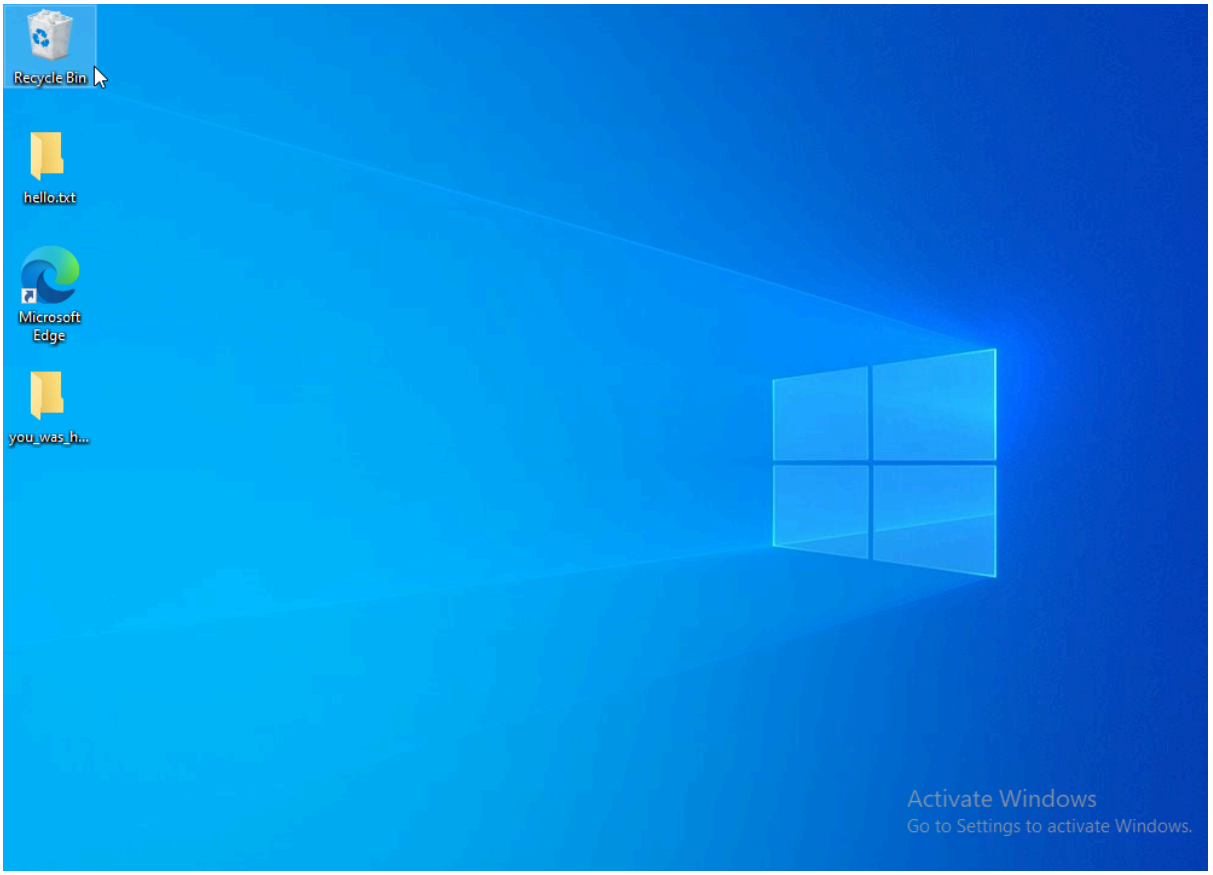
Now, in the target machine, we can see the Eicar file.



If we click in there, we will see this danger warning.

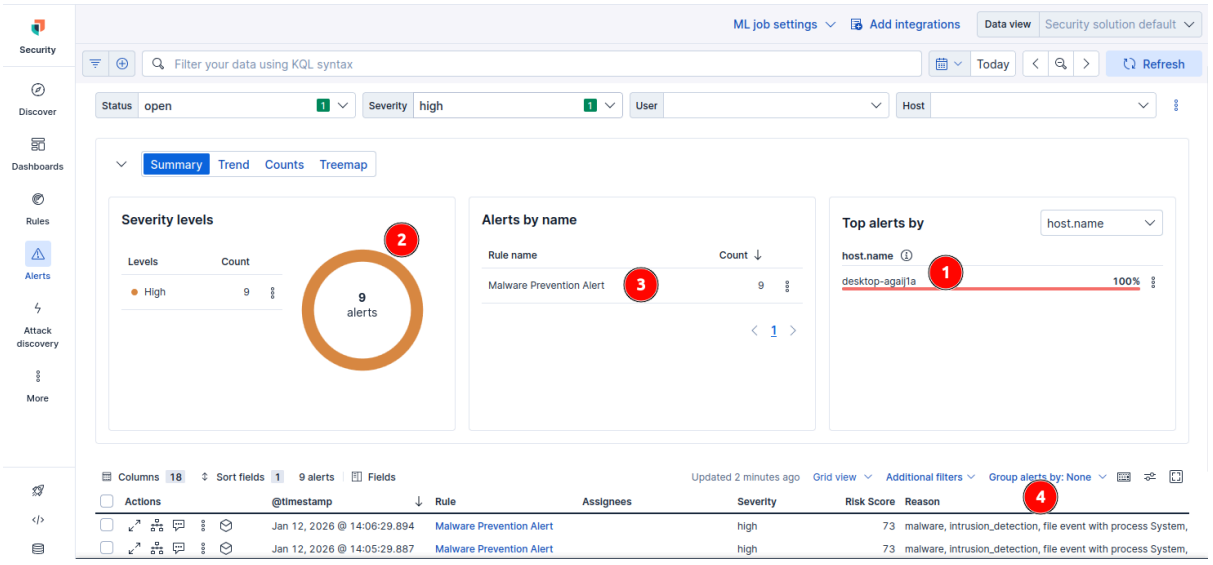


Let's click in run anyway to see what happens.



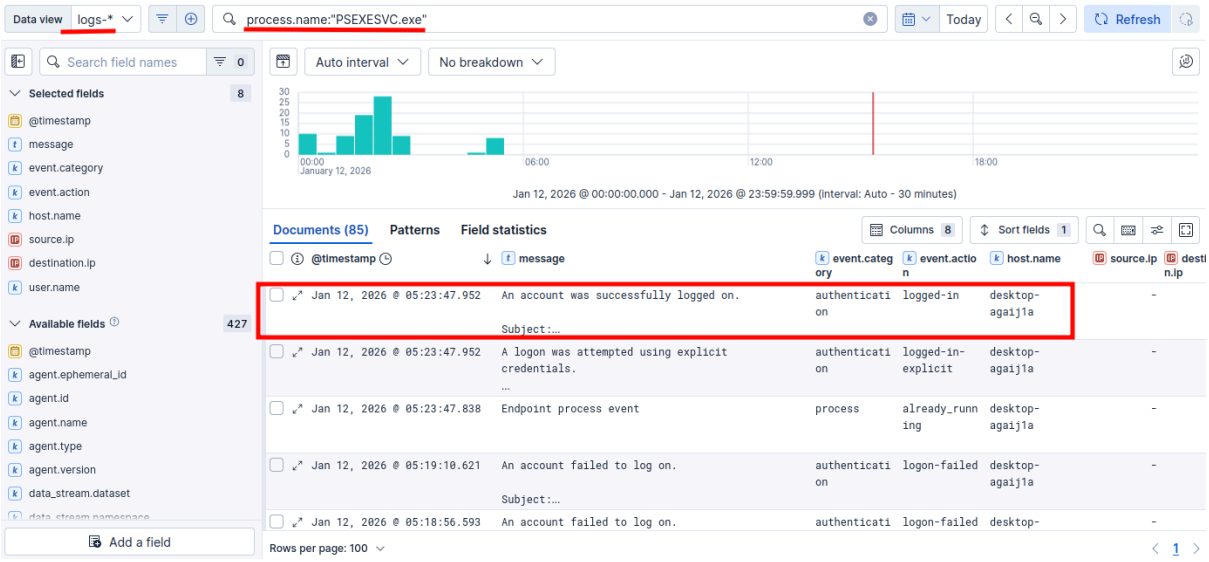
It was deleted.

Now, let’s go to the Elastic cloud to see the alerts.



When we open the alerts, we can notice a lot of new advises. The number 1 means the name of our target machine, the

number 2 means how many alerts happen, the number 3 means alert by name and number 4 means the reason.



If we go to Discover, and in data view put logs-*, and write “process.name:”PSEXESVC.exe”” we can check that someone successfully logged in our target machine.