Registry Keys for   
Persistence   
(Blue)

Graphical user interface

Description automatically generated

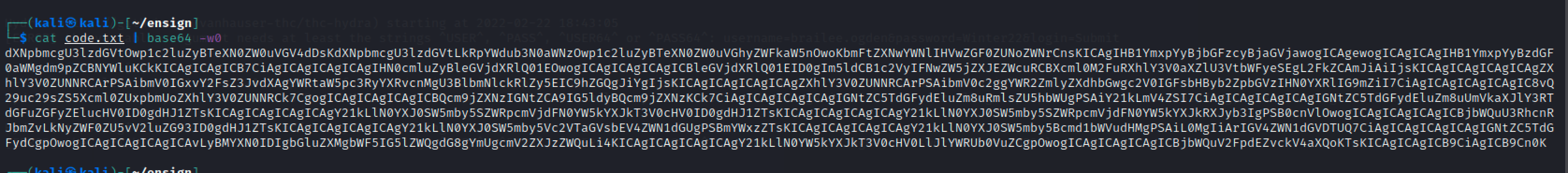
Explain:

This persistence attack is to maintain login/connection into the system, and by using the register the mailouts script and encode to base64 that can be a register keys. Then upload to the server.

As we can see the script I created the script to add user name “SpecnerDeg.D” this script will add user to the server in order to use it for persistence attack in case the brailee.ogden user being defended by the blue team.

Graphical user interface

Description automatically generated



Using crackmapexec with smb protocol from previous technic and use -x command to upload and execute the malicious code to the server. And it executed successfully.

A picture containing graphical user interface

Description automatically generated

This schTask.xml to create schedule task to take advantage of Windows Autoruns so the malicious code can be run on the schedule tasks in the system, this can let the payloads be execute with persistence without using credential again.

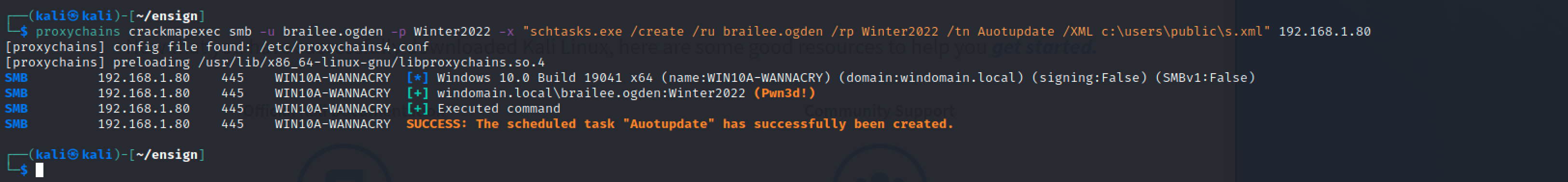
Graphical user interface, text

Description automatically generated

Using credentials derivde from orange attack path to upload and execute the schTask.xml to the server using “—put-file” command through crackmapexec with smb protocol. And the AUTORUNS executed successfully with “-x schtasks.exe command …” command into the target address 192.168.1.80

Text

Description automatically generated



To test out the persistence attack runs successfully, and see the username that created in the malicious in the script “SpecnerDeg.D” is properly added into the server. try to execute “net user” to see the user is added. As we can see “SpecnerDeg.D” is added successfully.

Graphical user interface, website

Description automatically generated

In case If the persistence username is compromise by the blue team, we can use “-x schetasks.exe” command again by using crackmapexec.

Text

Description automatically generated