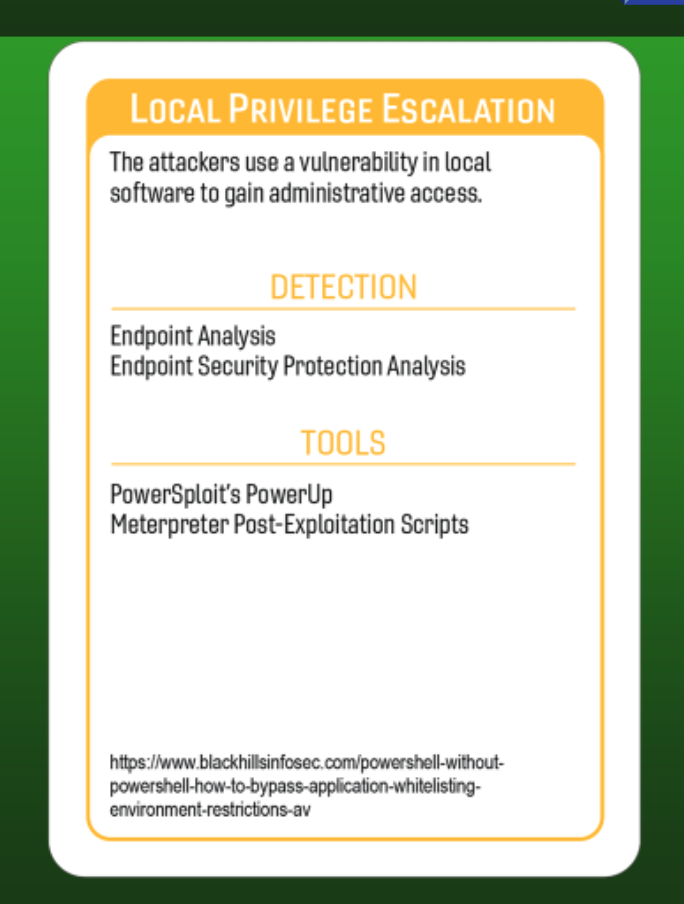
Local Privilege   
Escalation   
(Green)



Summary

Explains:

As we have successfully established backdoor in previous credential stuffing attack, we can use the backdoor to build further escalation from www-data user to root user.

Target Address: 172.26.15.39. Listening Port: 8989

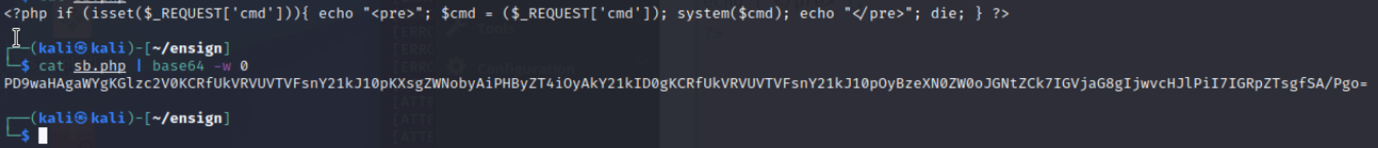
Target Account: [brailee.ogden@windomail.local](mailto:brailee.ogden@windomail.local)

Compromised Account: www-data

System: PHP web server. Account Created: Francis

Tools: Netcat, Revershell, Base64 Encode, Escalation Commands.

This is the backdoor that we implemented last attack.



The is the revershell that we going to establish in our kali linux command line console. The revershell.txt contains the revershell code so we can access via netcat port 8989

And it encode to base64 for stealth purposes.

Text

Description automatically generated

As we put the encode base64 from reverseshell.txt, and put the encode reverseshell into the backdoor url to establish connections.

Graphical user interface, text, application

Description automatically generated

We use kali netcat to start listening the connections port 8989 that we write in the reverseshell.txt

The connections establish successfully and “whoami” command is executed successfully.

And now we need to escalate from www-data user to root user.

Graphical user interface, text

Description automatically generated

As we do some research in the website https://gtfobins.github.io/ to find escalation commands, we found

Using “./dash -p” then “/usr/bin/dash -p” commands can be utilized as escalation commands.

After the escalation, we can see using “whoami” shows we are root.

As a root user we can add users to the system so we can establish persistence.

Graphical user interface, text

Description automatically generated

And then we can establish ssh-keygen to auto-connect to the target server. So we can access the target server via ssh connection without password.

Text

Description automatically generated

Create Francis User, and establish ssh without password with the key-gent

Text

Description automatically generated