1Traffic Signaling   
(Green)

Graphical user interface, application

Description automatically generated

Summary

Attack Explains:

We are using the malicious server that we created in the last attack and put it in the piwigo webserver. By executing the malicious server inside, it will connect to kali linux and have root privilege.

Target Address: 172.26.15.39. Listening Port: 8989

System: PHP webserver System Software: Piwigo

Account: [brailee.odgen@windoain.local](mailto:brailee.odgen@windoain.local), [vagran@172.26.1.229](mailto:vagran@172.26.1.229)

Passwords: “Winter2022”, “vagrant”

Techniques: PHP-Reverse-shell, Netcat, PHP scripting, SSH Reverse-Shell

**First service testing on Kali Host:**

We are establishing reverse shell 172.16.1.229 and port as a pivot to the webserver to hide our connections.

Text

Description automatically generated

Below is the php malicious script that we will put in the Piwigo server, and it has been modified and added payload “php-reverse-shell.php” inside the script. The socket as modified to UDP 1000 port that we are going to connect and listen.

Text

Description automatically generated

I rename the php malicious file to moniotr123.php for disguise.

And test it again with “sudo php”, and see if it works

Graphical user interface, application

Description automatically generated

Go on this website to see how to establish a linux service to auto-connect to malicious php file.

<https://medium.com/@benmorel/creating-a-linux-service-with-systemd-611b5c8b91d6>

Modify the path of ExecStart which is the malicious php service.

Text

Description automatically generated

Tried to executed and rot13.service to connect and start the monitor123.php

Text

Description automatically generated

To connect malicious, start listening to the port 10000 which I put in the php script.

And set the port 8989 so I can gain access to the server

Graphical user interface, text

Description automatically generated

As we see, we have gain access to the kali php web server as root.

Graphical user interface, text

Description automatically generated

Now we put all these technique to the target address 172.26.15.39 web server.

Execution in PHP webserver:

Access to the francis account that we created in previous attack; I have the authorized key so I do not have enter password.

Text

Description automatically generated

Verifying the account that I created, and there’s “francus user”

Graphical user interface, text, website

Description automatically generated

Copy and create the rot13.service and monitor123.php in the right directory. Which are the malicious service and script.

Text

Description automatically generated

Enable the rot13.server by executing “sudo systemclt restart/enable rot13”

And we have modified the rot13 scrip “after=sshd.service” and the ExecStart Path.

Text

Description automatically generated

We shall start the to listen to the target address and its port 10000 which is UDP

And set the 172.26.1.229 and 8989 for the reverse-shall address and port to pivot to our host kali

Then Start listen 8989, the reverse-shell port and we gain access to the web server successfully, and we can verify by executing “whoami” and we got the root access.

Graphical user interface, text

Description automatically generated