Malicious Service   
with systemd   
(Green)

Graphical user interface, text, application

Description automatically generated

Summery

Vulnerabilities Explains:

For the malicious service we are going to hide is piwigoMonitor.php. it amongst the web server files that exist under /var/www/html in the piwigo webserver.

At first, we are going to test it out in the kali linux.  
Then we are going to disguise it as a service monitoring script for the site Piwigo

Finally, we will execute as systemd service as a legitimate service.

Target Address: 172.26.15.39. Target Testing: 127.0.0.1 (KALI)

System: PHP webserver System Software: Piwigo

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

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

Using php to start the connections to the UDP port 10000

Text

Description automatically generated

We are using netcat to listen to the internal address 127.0.0.1 and port 10000 as the same port we put in the malicious script.

Then we are going to listen to 8989 which is my reverse shell established port.

Graphical user interface, text

Description automatically generated

Executed and connection has established successfully, we can see the second USER

“Kali pts/2” connected from ssh vpn and port 8989 as reverse shell.Text

Description automatically generated