Logon Scripts  
(Orange)

Summary

Target Address: 172.26.1.229

Target Account: vagrant Password: vagrant

Techniques/tools: SSh, SSh-keygen, Sha256 encoding, crontab, PHP backdoor.

SSH Auto Login

Use the ssh-keygen to create public keys for my own kali

Text

Description automatically generated

This the sha256 for my public keys to insert to the script

A picture containing text

Description automatically generated

Go to the vagrant to see in the authorized\_keys to if it does have the keys so we can insert the keys through script

Text

Description automatically generated

Use the malicious auto insert the public keys using the public keys and sha256sum and execute.

Text

Description automatically generated

After login without password mean its successful.

Text

Description automatically generated

PHP backdoor script auto execute using crobtab

Find crontab in /etc directory

Graphical user interface, application, website

Description automatically generated

We are going to us hourly crontab/

Text

Description automatically generated

We are going to use this php-reverse-shell.php in side of the kali linux. To establish backdoor.

Graphical user interface, text, application, website

Description automatically generated

We are going to rename this php into sb.php

Graphical user interface

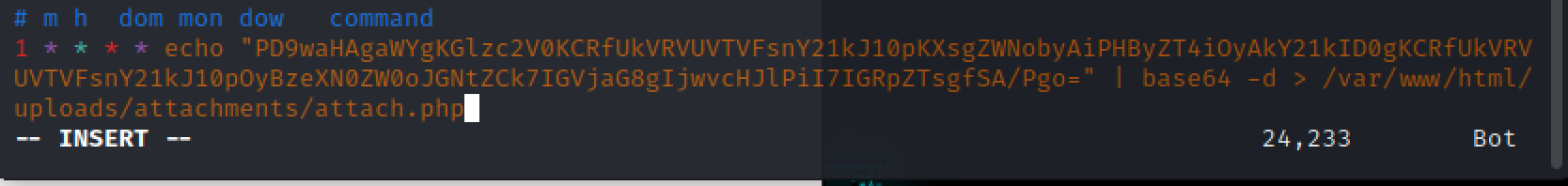
Description automatically generated with medium confidence

We are going to encode this in base64 to hide the malicious code.

Text

Description automatically generated

We are going to execute this in 1 \* \* \* \* meaning every one minutes going to execute the code into attach.php. attach.php is a empty file



After one minutes, We are going to execute the attach.php, it and it works and shows the root directory.

Text

Description automatically generated