HTTP Exfil  
(Orange)

Summary

Using HTTP protocol and web to disguise like a internet traffic to upload malicious file in the webserver. So the webserver can be exploits

Target Address: 172.26*.1.229* Target Account: vagrant

Target OS: qdpm, Linux

Techniques/Tools: Ssh reverse tunnel, VPN, Metasploit, php.

Establish reverse shell tunnel in qdpm server

Text

Description automatically generated

Use proxychains to hide your connections.

Graphical user interface, chart

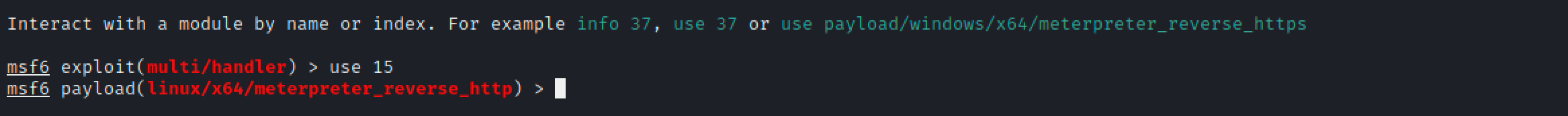
Description automatically generated

We establish revers\_http using multi handler.

A screenshot of a computer

Description automatically generated with medium confidence

And set up the configurations



Using 9900 as Local Host to listen and put your kali address

And exploit -j to start to listen in the backgrond

Text

Description automatically generated

Create a http payload using the msfvenom and put in your lport 9900 and lhost to kali address

Text

Description automatically generated

Verify the payload is creaded

A screen shot of a computer

Description automatically generated with low confidence

Put in your html directory

Chart

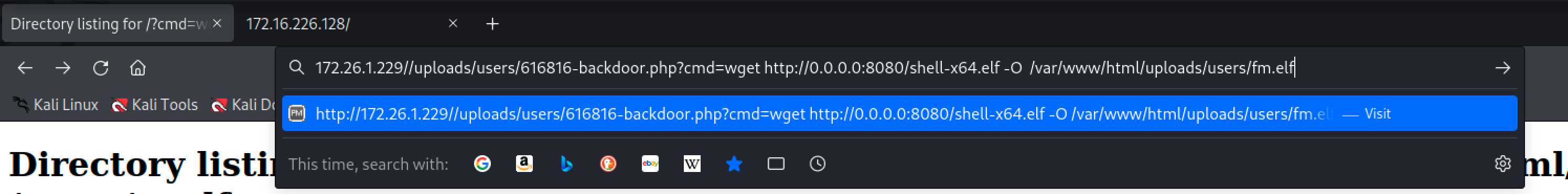
Description automatically generated with low confidence

Establish http 8080 port webserver using python3

Graphical user interface, text

Description automatically generated

Download the payload using web shell.



Verify the payload is downloading. And the privilege for executable.

Graphical user interface, text

Description automatically generated