# Telnet Exploitation

@mmar

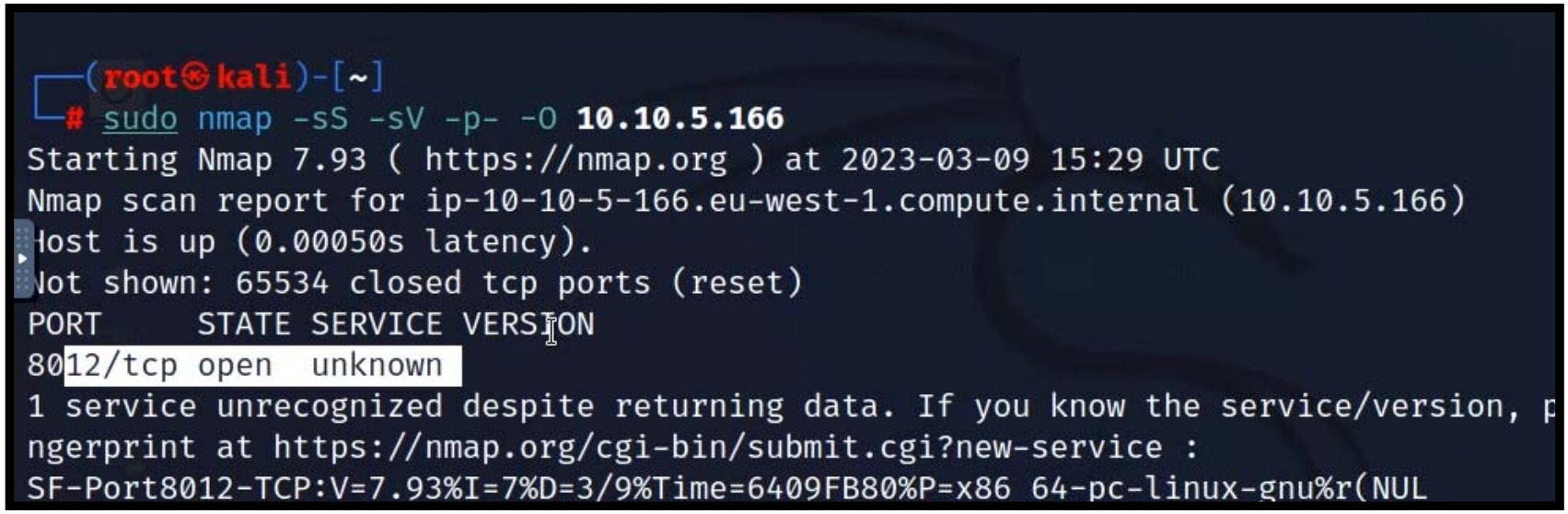
Telnet is an application protocol which allows you, with the use of a telnet client, to connect to and execute commands on a remote machine that's hosting a telnet server.

The telnet client will establish a connection with the server. The client will then become a virtual terminal- allowing you to interact with the remote host. Telnet sends all messages in clear text and has no specific security mechanisms. Thus, in many applications and services, Telnet has been replaced by SSH in most implementations

# Scanning

- Nmap can be used to scan for the telnet port

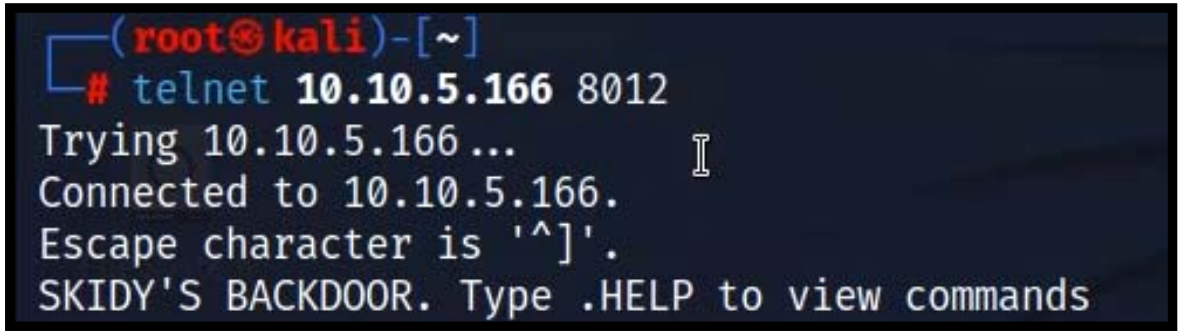
Nmap –sS –T4 -p- 10.10.50.26  (normally port 23)



# Connecting with telnet

- Connection with telnet is very easy. You can use the following command to connect to a telnet port

```
telnet $IP $PORT
```



# DEMO

# THANKS