

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 Thus, in many applications and services, Telnet has been replaced by SSH in most implementations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)
```

```
(root@kali)-[~]
└─# sudo nmap -sS -sV -p- -O 10.10.5.166
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-09 15:29 UTC
Nmap scan report for ip-10-10-5-166.eu-west-1.compute.internal (10.10.5.166)
Host is up (0.00050s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8012/tcp  open  unknown
1 service unrecognized despite returning data. If you know the service/version, p
ngerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8012-TCP:V=7.93%I=7%D=3/9%Time=6409FB80%P=x86_64-pc-linux-gnu%r(NUL
```

Connecting with telnet

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

```
telnet $IP $PORT
```

```
(root@kali)-[~]  
└─# telnet 10.10.5.166 8012  
Trying 10.10.5.166 ...  
Connected to 10.10.5.166.  
Escape character is '^]'.  
SKIDY'S BACKDOOR. Type .HELP to view commands
```

DEMO



THANKS