Telnet Enumeration

Telnet is an older protocol used for remote access to systems over a network. While it has largely been replaced by more secure protocols like SSH, some legacy systems and devices still use Telnet.

Service Enumeration

We can use nmap's service and script based scans to gather information about the running telnet server.

```
sudo nmap -p 23 -sV --script telnet-encryption,telnet-ntlm-info
192.168.29.141
```

Capturing telnet creds using Wireshark

As we know that, telnet is an old protocol and it has no encryption. That means, whatever data is sent through it, including username and password, travel in clear text.

We can use packet sniffing tool like Wireshark to capture these clear text credentials

```
sudo wireshark&
```

- Apply telnet filter

MITM Attack to capture Telnet creds

Next, we can also perform an MITM attack on the network using metasploit to capture telnet creds. So, basically we will create a fake telnet server that will be pointing to our Ip address and if the user mistakenly logged into it like it does with the real telnet server, we will get his credentails.

To set up this, we need to do this with root.

```
use auxiliary/server/capture/telnet
set srvhost 192.168.0.102
set banner Welcome to Invent Your Shit Server
exploit
```

Configuration Files

If we land on the server somehow, then we can look into some sensitive SSH configuration files.

```
/etc/inetd.conf
/etc/xinetd.d/telnet
/etc/xinetd.d/stelnet
```

We can also perform bruteforce attack on telnet with a username and password list. Along with that, we can have full control over a server by uploading our payload on the telenet server and executing it.
