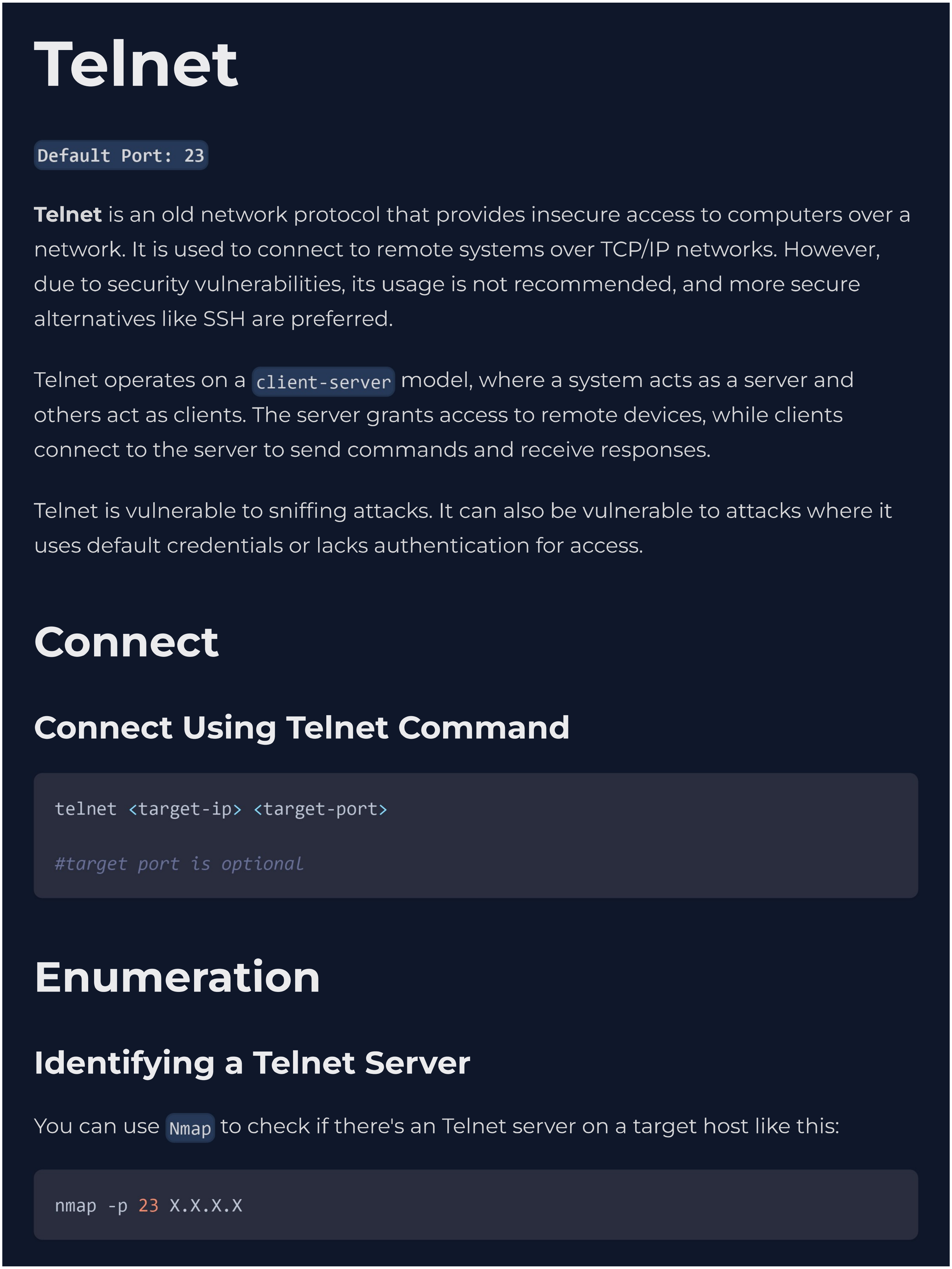

Telnet

`Default Port: 23`

Telnet is an old network protocol that provides insecure access to computers over a network. It is used to connect to remote systems over TCP/IP networks. However, due to security vulnerabilities, its usage is not recommended, and more secure alternatives like SSH are preferred.

Telnet operates on a `client-server` model, where a system acts as a server and others act as clients. The server grants access to remote devices, while clients connect to the server to send commands and receive responses.

Telnet is vulnerable to sniffing attacks. It can also be vulnerable to attacks where it uses default credentials or lacks authentication for access.

Connect

Connect Using Telnet Command

```
telnet <target-ip> <target-port>

#target port is optional
```

Enumeration

Identifying a Telnet Server

You can use `Nmap` to check if there's an Telnet server on a target host like this:

```
nmap -p 23 X.X.X.X
```

Assessing Encryption on Telnet Server

The `telnet-encryption` script of Nmap is designed to assess the presence of encryption support on Telnet servers. It should be noted that incorrect implementations in certain systems may result in security vulnerabilities. This script solely evaluates the availability of encryption support.

```
nmap -p 23 --script telnet-encrpytion X.X.X.X
```

Extracting NTLM Authentication Details on Telnet Server

The `telnet-ntlm-info` script of Nmap is designed to gather information from remote Microsoft Telnet services that have NTLM authentication enabled. By initiating a MS-TNAP NTLM authentication request using null credentials, the script prompts the remote service to return a NTLMSSP message. This response reveals critical information, including the NetBIOS name, DNS name, and the operating system's build version.

```
nmap -p 23 --script telnet-ntlm-info X.X.X.X
```

Banner Grabbing

You can use `Netcat` to find out what service is running and its version by looking at the welcome message it shows when you connect. This method is called Banner Grabbing.

```
nc -nv X.X.X.X 23
```

Attack Vectors

Passwordless Authentication

Telnet allows users to connect to a server without needing a specific identity by utilizing a `passwordless` login feature. This method is commonly employed for accessing or downloading public files.

```
telnet X.X.X.X

#provide username
#do not provide any password
```

Common Credentials

If anonymous login is disabled on the Telnet server, trying common usernames and passwords like `admin`, `administrator` , `root` , `user`, or `test` can be a good initial step. This approach is less aggressive than attempting to guess passwords through brute force and is recommended to try first when accessing a server.

```
telnet X.X.X.X

#provide a common username
#provide a common password
```

Bruteforcing Credentials

A brute-force attack involves trying many passwords or usernames to find the right one for accessing a system.

Tools like Hydra are designed for cracking into networks and can be used on services like Telnet, HTTP, SMB, etc. For Telnet, Hydra often carries out a dictionary attack, which means it uses a list of possible usernames and passwords from a file to try and log in.

Bruteforcing with Hydra

To use `Hydra` for brute-forcing Telnet login credentials, you would use a command structured for this purpose:

```
hydra [-L users.txt or -l user_name] [-P pass.txt or -p password] -f [-S port]
telnet://X.X.X.X
```

```
nmap -p 23 --script telnet-brute X.X.X.X
```

Bruteforcing with Metasploit

It is also possible to apply brute force with `Metasploit` modules on Telnet:

```
use auxiliary/scanner/telnet/telnet_login
msf auxiliary(telnet_login) > set rhosts X.X.X.X
msf auxiliary(telnet_login) > set user_file /path/to/user.txt
msf auxiliary(telnet_login) > set pass_file /path/to/pass.txt
msf auxiliary(telnet_login) > set stop_on_success true
msf auxiliary(telnet_login) > exploit
```

MITM: Telnet Spoofing with Metasploit

A man-in-the-middle attack to capture Telnet login credentials can be performed using the `Metasploit` module.

```
use auxiliary/server/capture/telnet
set srvhost X.X.X.X
set banner Hackviser Telnet Server
exploit
```

Post-Exploitation

Common Telnet Commands

Command	Description	Usage

Command	Description	Usage
`open`	Connects to a specified remote host	`telnet open example.com 23`
`close`	Closes the current connection	`telnet> close`
`quit`	Exits telnet	`telnet> quit`
`status`	Shows the current status of the telnet client	`telnet> status`
`z`	Suspends telnet (on Unix/Linux systems)	`telnet> z`
`set`	Sets Telnet options (like terminal type)	`telnet> set term vt100`
`unset`	Unsets Telnet options	`telnet> unset term`
`display`	Displays current settings of Telnet options	`telnet> display`
`send`	Sends special characters or sequences (like break)	`telnet> send break`
`mode`	Sets the mode of operation (e.g., line by line or character)	`telnet> mode character`
`logout`	Logs out from the remote system (not available on all systems)	`telnet> logout`