SSH Enumeration

Secure Shell (SSH) is a widely used protocol for securely accessing remote systems over a network. While SSH provides strong encryption and authentication, improper configuration or the use of weak credentials can leave SSH servers vulnerable to enumeration and exploitation.

Version Detection

Lets start with the first technique in which we will enumerate the version of the SSH server.

This can be done very easily with the help of Nmap.

```
sudo nmap -p 22 -sV -sC 192.168.29.141
```

Now that we know the version of our SSH server, we can look for potential exploits related to it.

Another way to find the version of the running FTP server is using Metasploit.

```
use  auxiliary/scanner/ssh/ssh_version
set RHOSTS <TARGET IP>
run
```

User Enumeration

We can find potential SSH usernames using metasploit.

```
use auxiliary/scanner/ssh/ssh_enumusers
set RHOSTS <Target IP>
set USER_FILE user.txt
run
```

Once we have collected the potential usernames, we can perform a bruteforce attack on them like FTP but as i told you before that is on hold till the exploitation section.

Check for SSH login methods

Next we can use Nmap script ssh auth methods to check the authentication scheme used on the target SSH server. This can be a password, a private key or both.

```
sudo nmap -p 22 --script ssh-auth-methods 192.168.29.141
```

Configuration Files

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

```
ssh_config
sshd_config
authorized_keys
ssh_known_hosts
.shosts
```

Along with that, we should also look into the users home directory for the SSH keys which are usually present in .ssh folder.

The authorized keys generally contains the public SSH keys while id_rsa holds the private SSH keys. We need private keys to log into the server from outside, its like a password while the public key checks the private key if it is correct or not.
