# STEPS :

1. Always check nmap

***Nmap -T4 -sC -sV -Pn -oN nmap/initial TARGETIPADDRESS***

1. Once you find the ports that are running on the target host we can then gather more information based on the ports that are open on the remote host

***nmap -A -Pn -T4 -p21,80,2222 TARGET\_IP***

1. Navigate to the web app itself in the browser and check what all information can you gather
2. Run Gobuster with different username lists to check what all sub domains might be available on the web app

***gobuster dir -w /usr/share/wordlists/dirb/common.txt -u <ip>***

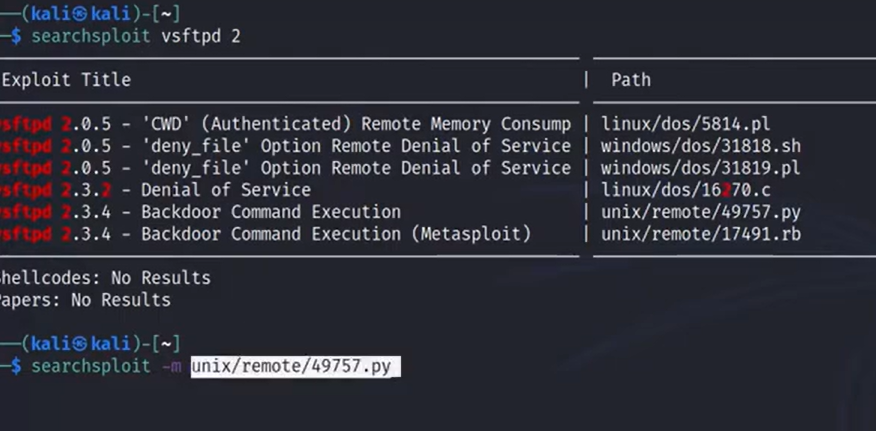
1. We can also user the search sploit to find if there are current vulnerabilities that are known about the services that are currently running on the server

***python2 exploit.py -u <url> -c -w /usr/share/wordlists/rockyou.txt***

**NOTE** : Make sure that we have confirmed if the downloaded exploit is supposed to be ran using python or python2

1. Run nmap with -sV and -sC flag
2. This will give you all the services running on the target machine
3. Use the command

### Searchsploit openssh



1. In order to mirror the python script we can simply use

Searchsploit -m

-m flag is for mirroring the python script