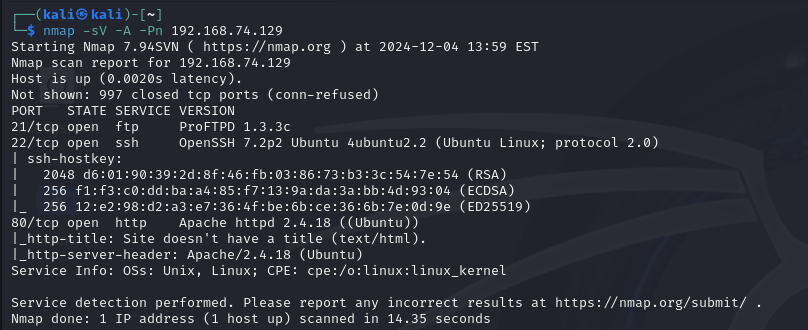
**Kabelo Modimoeng**

**Capstone Project – Case Study for Local VM**

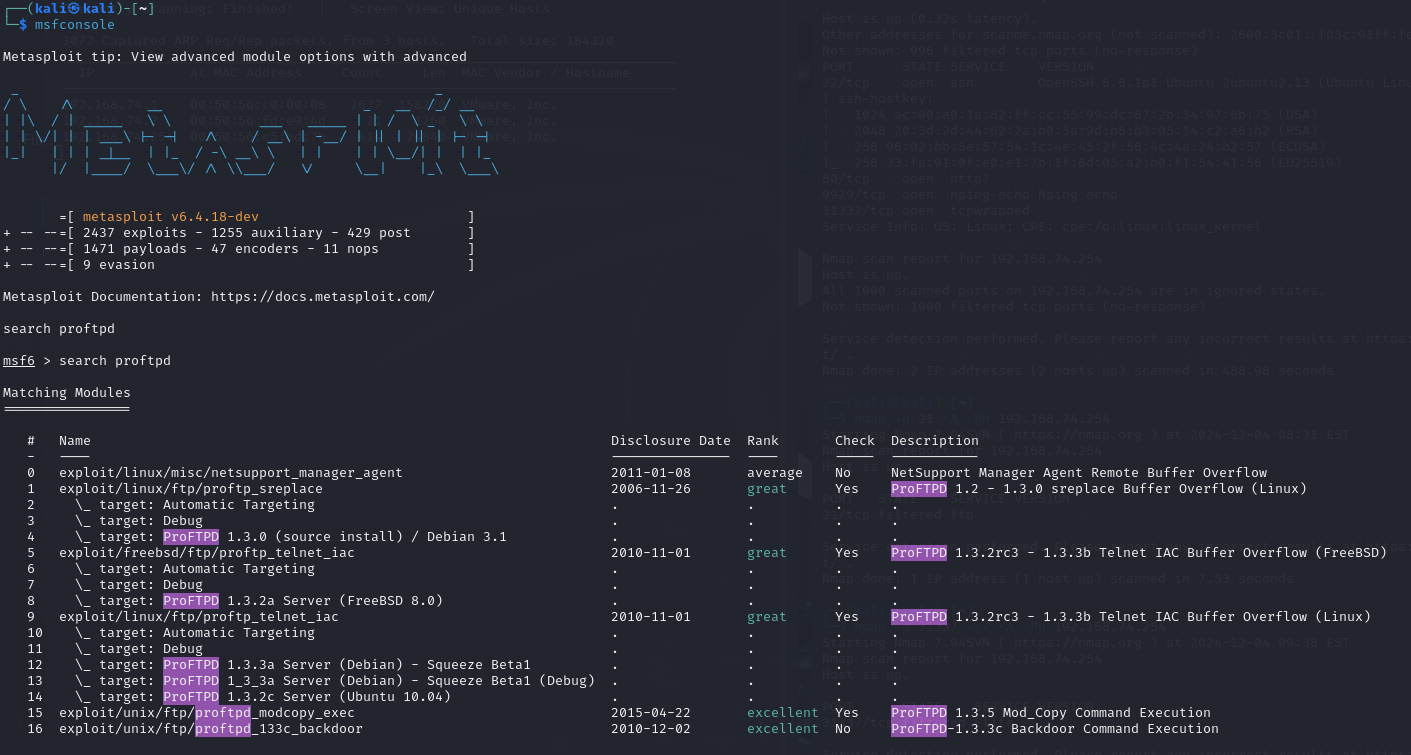
**Stage 1**

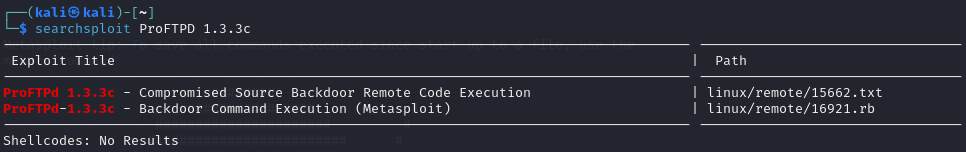
****

* Port 21/tcp – ftp – (ProFTPD 1.3.3c)
* Port 22/tcp – ssh – (OpenSSH 7.2p2 Ubuntu)
* Port 80/tcp – http – (Apache httpd 2.4.18)

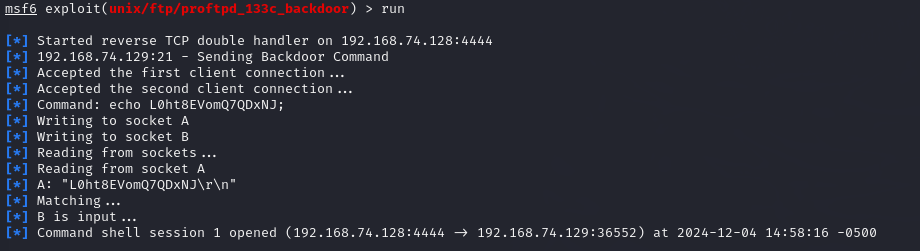
**Stage 2**

On port 21, the service “ftp” being ran refers to the File Transfer Protocol. The service has backdoor vulnerabilities which include: Anonymous Login, Weak Passwords, Unencrypted Data Transfer, Outdated software, etc. The particular backdoor vulnerability I found is associated with the ProFTPD server which was used to grant unauthenticated remote root access to systems running the compromised version of ProFTPD (1.3.3c).



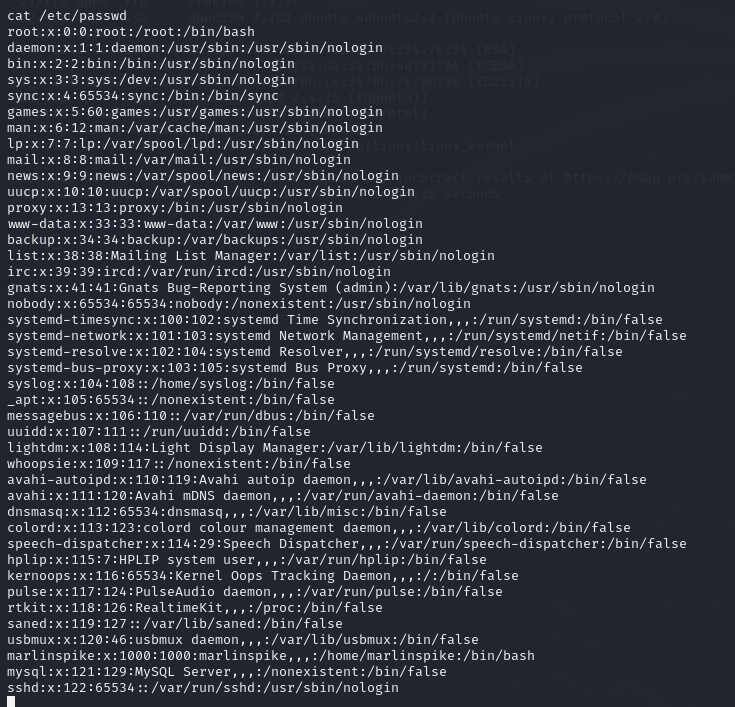


**Stage 3**

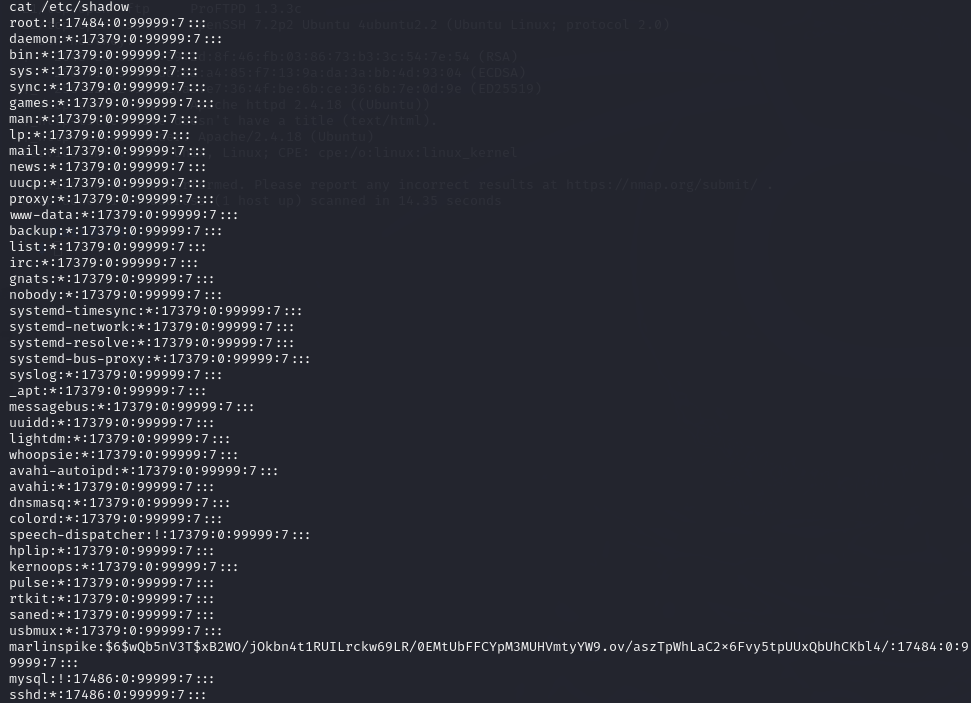


**Stage 4**

* The password file can be extracted using **cat /etc/passwd**. This command will display the contents of the /etc/passwd file, which contains user account information.



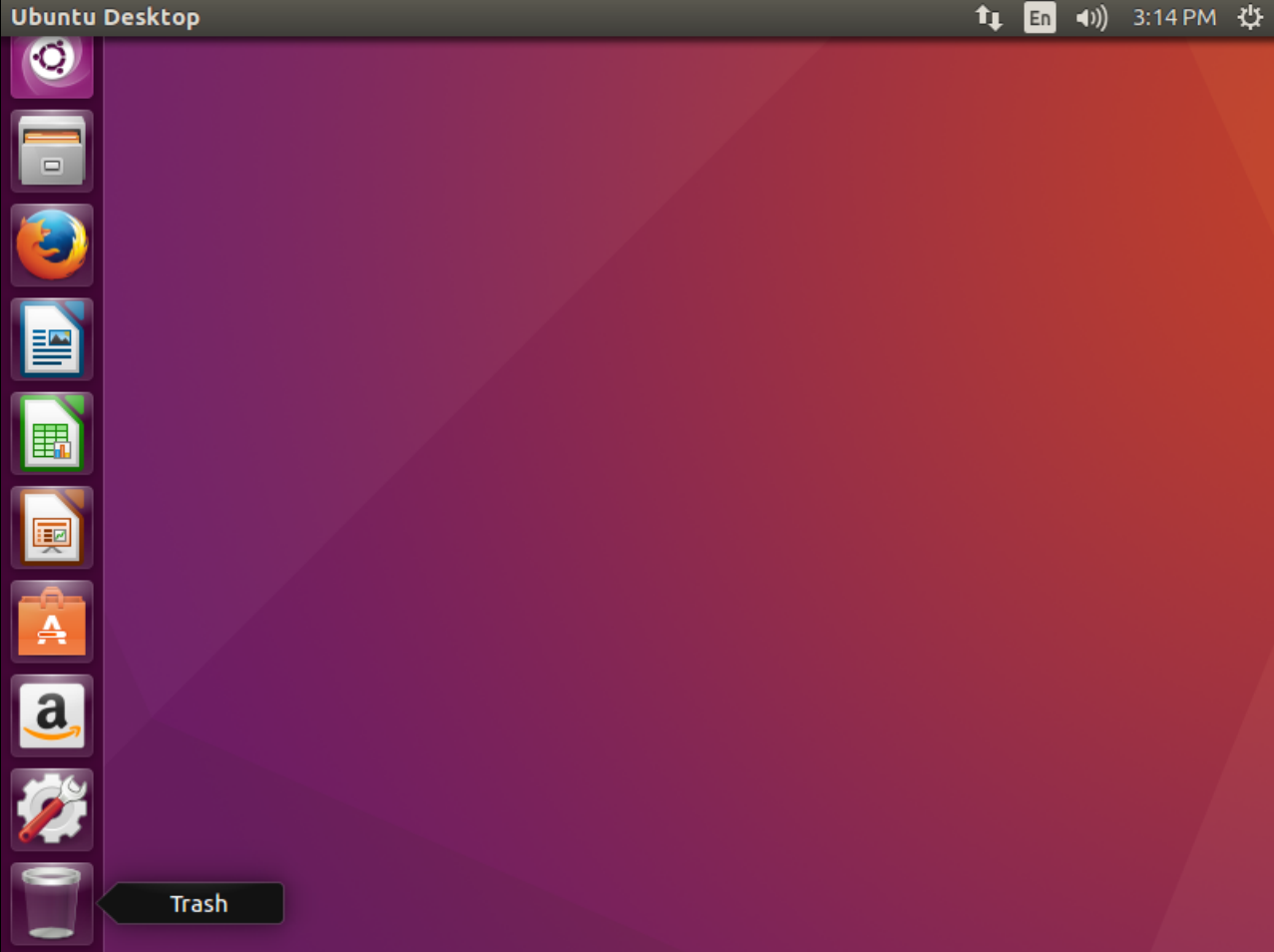
To view the hashed password file: **cat /etc/shadow**

****

The hashed password is: **$6$wQb5nV3T$xB2WO/joknb4t1RtULrckw69LR/0EMtUbFFCYpM3MUhYmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbL4**

* Username: **marlinspike**

password: **marlinspike**

****