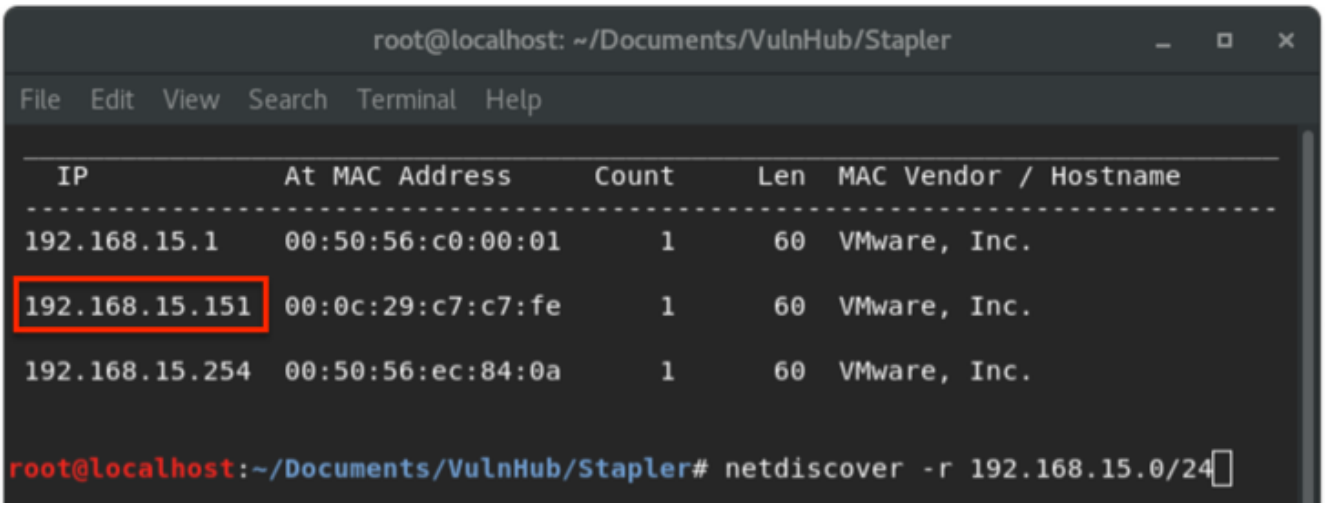
Table of Contents

Summary

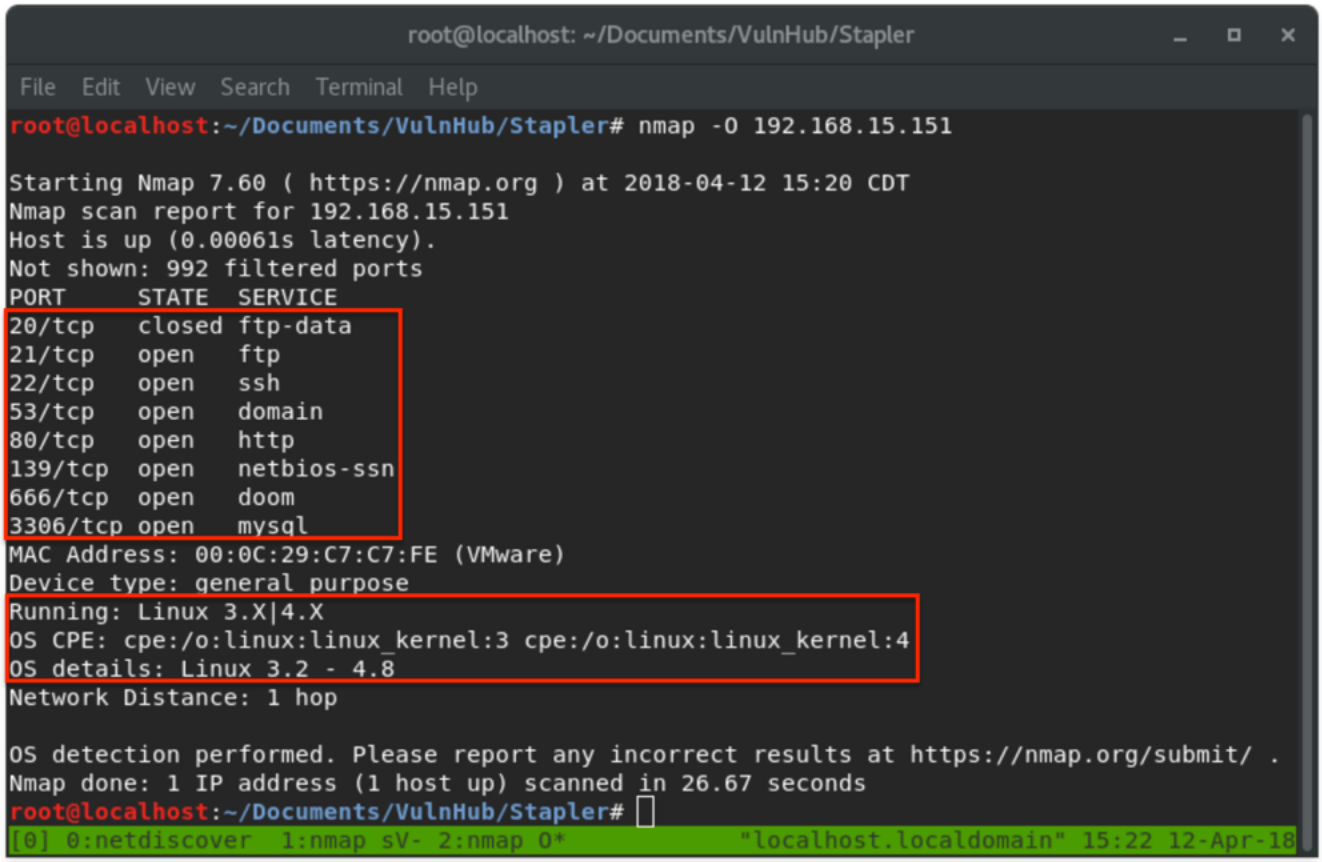
Stapler is an Ubuntu server with multiple services running. This walkthrough will discuss how three of the services were enumerated in order to gain root access to the machine. The services accessed were FTP, SMB, and SSH. The only vulnerabilities exploited was weak user credentials and poor use of strong credentials.

Recon/Scanning

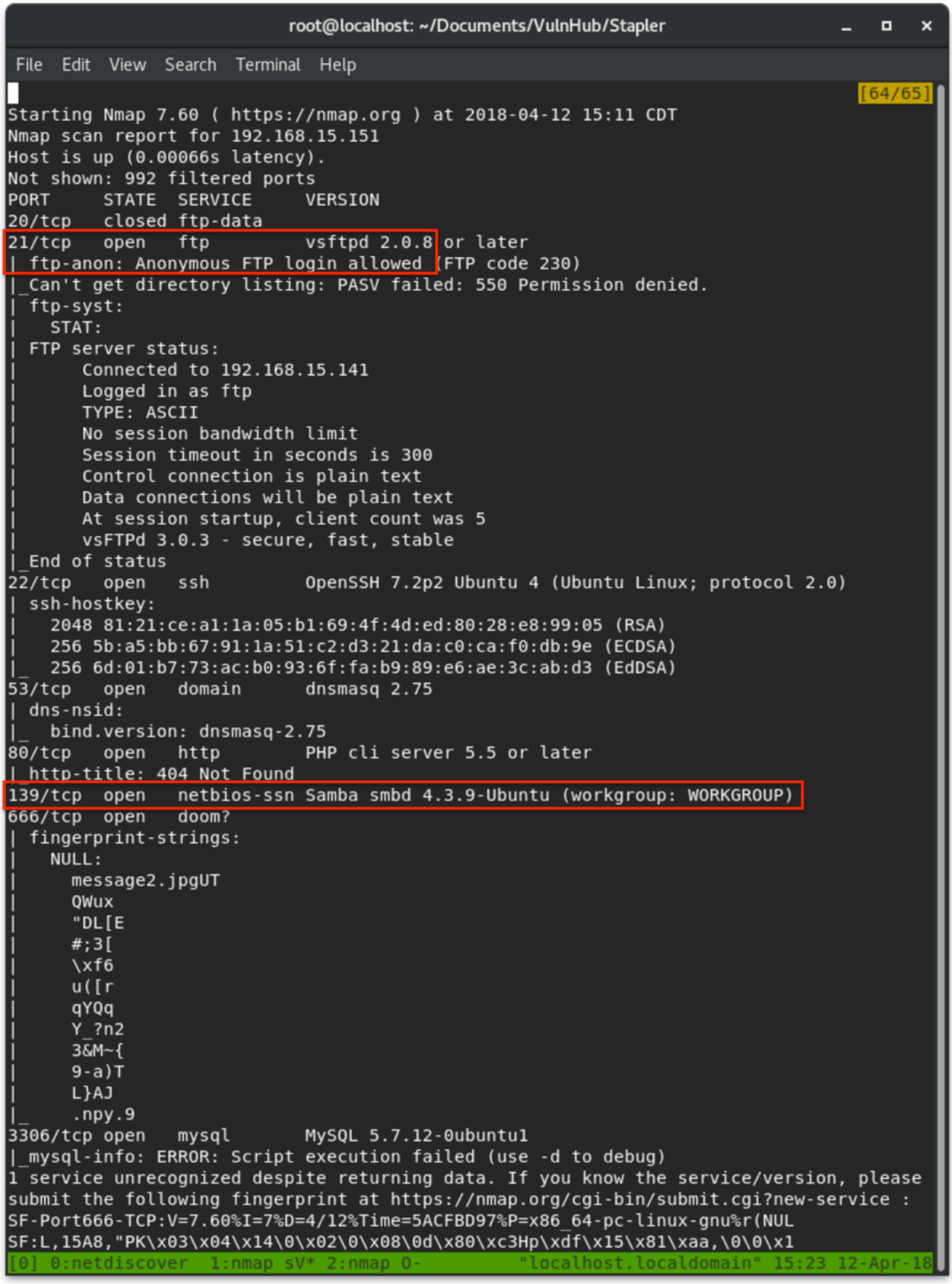
netdiscover of my private range to find host



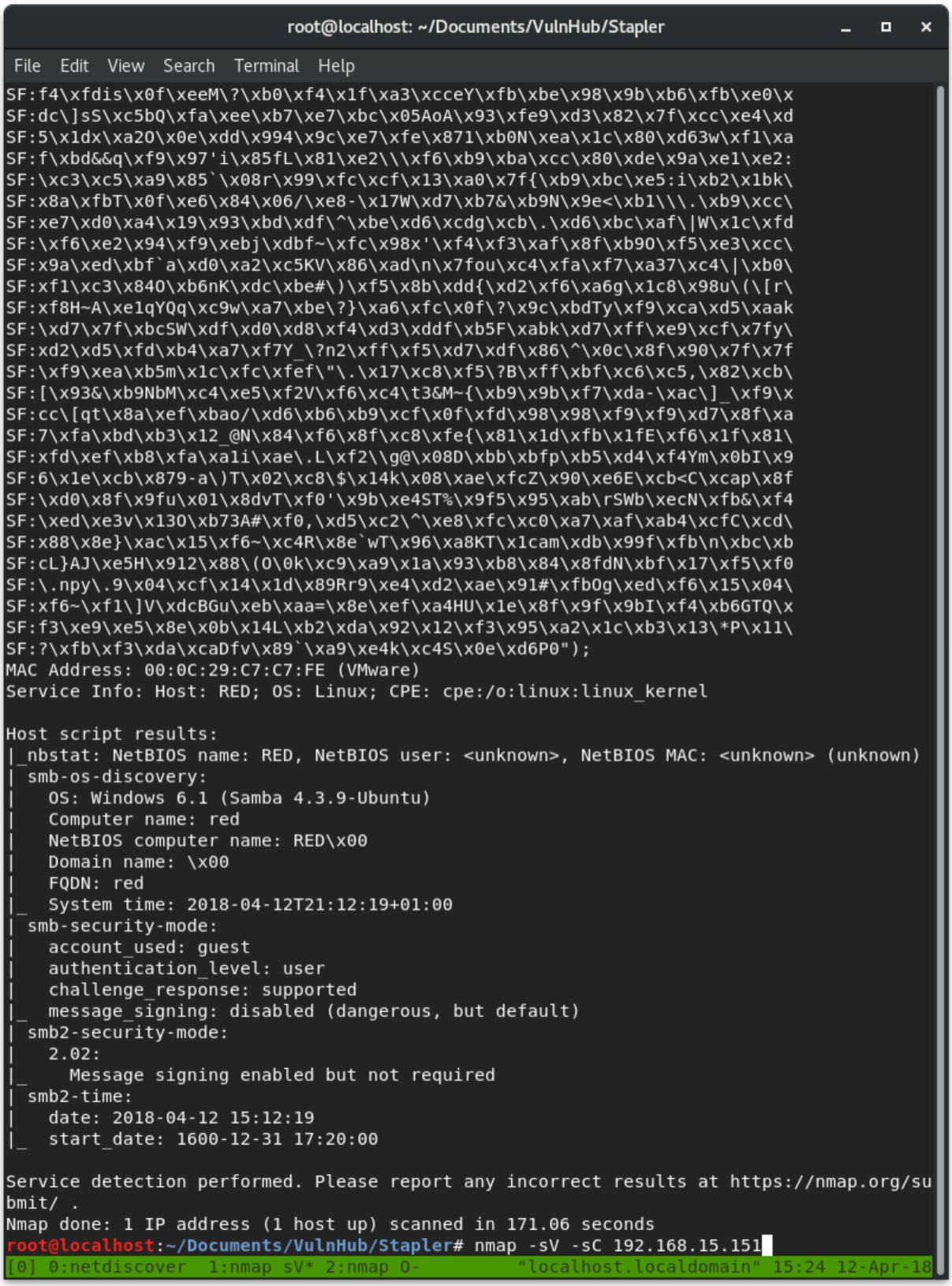
nmap for services and OS detection:



nmap for detailed services and versions:

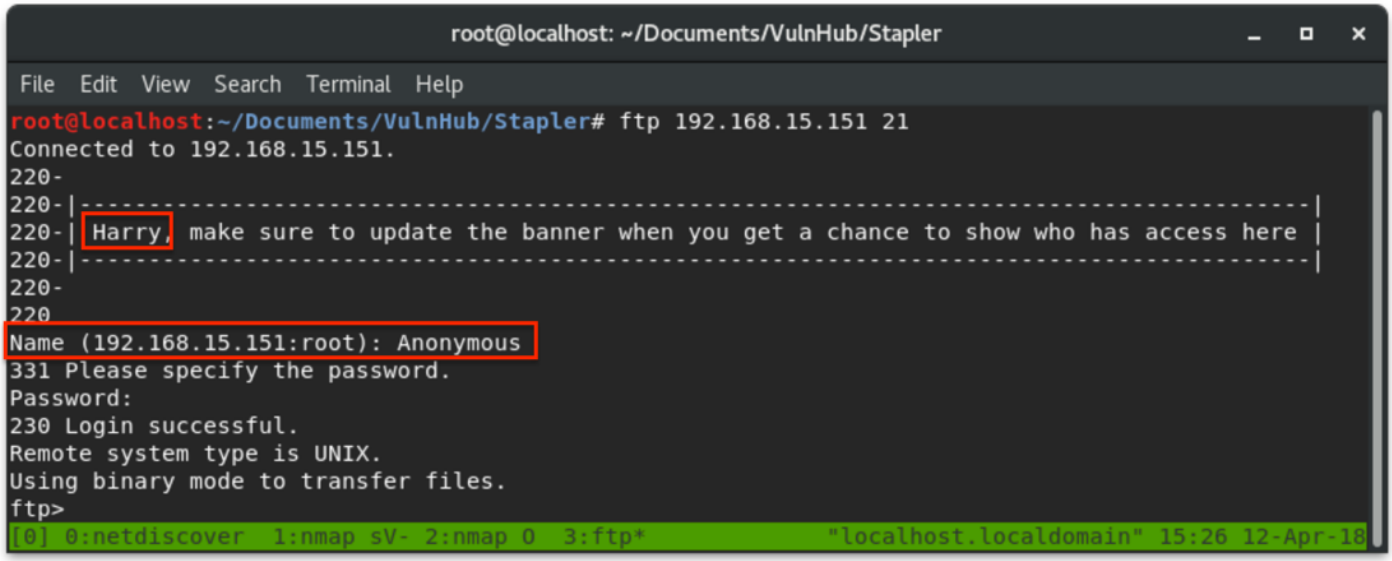


nmap for services and versions continued:

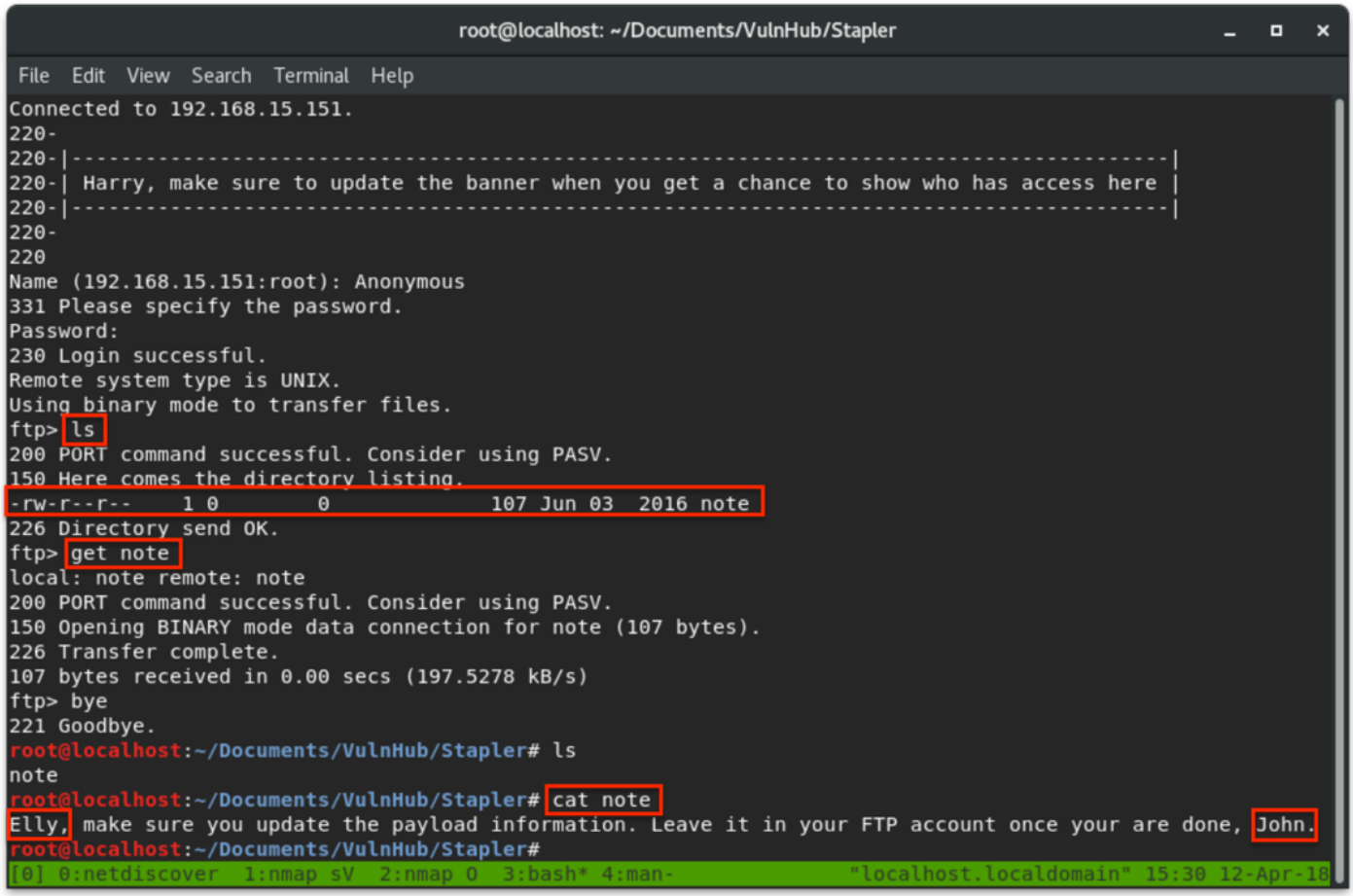


FTP

FTP anonymous access:



Right away we get a user Harry

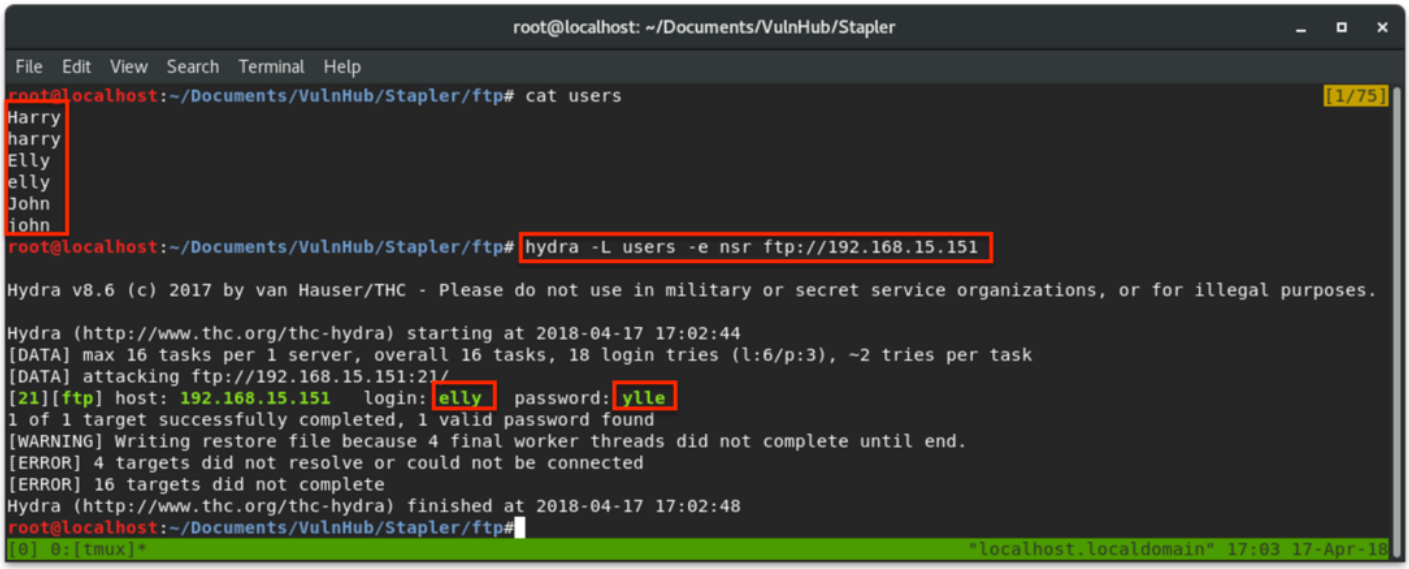


Retrieve the file called "note" and we get two more users, "Elly" and "John"

FTP Credential Audit:

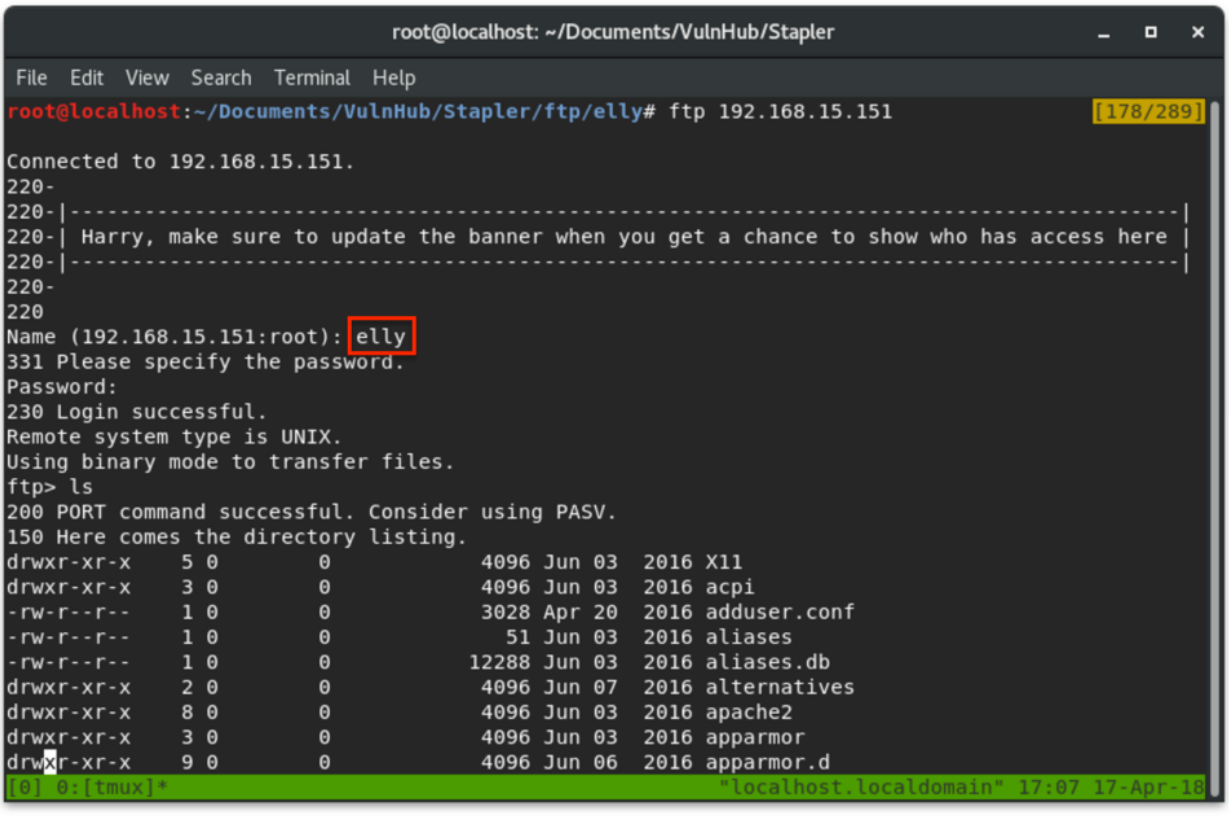
Create a user list w/ capital and lowercase usernames.

Use hydra to bruteforce a null/same-as-username/reverse-username password audit on FTP.

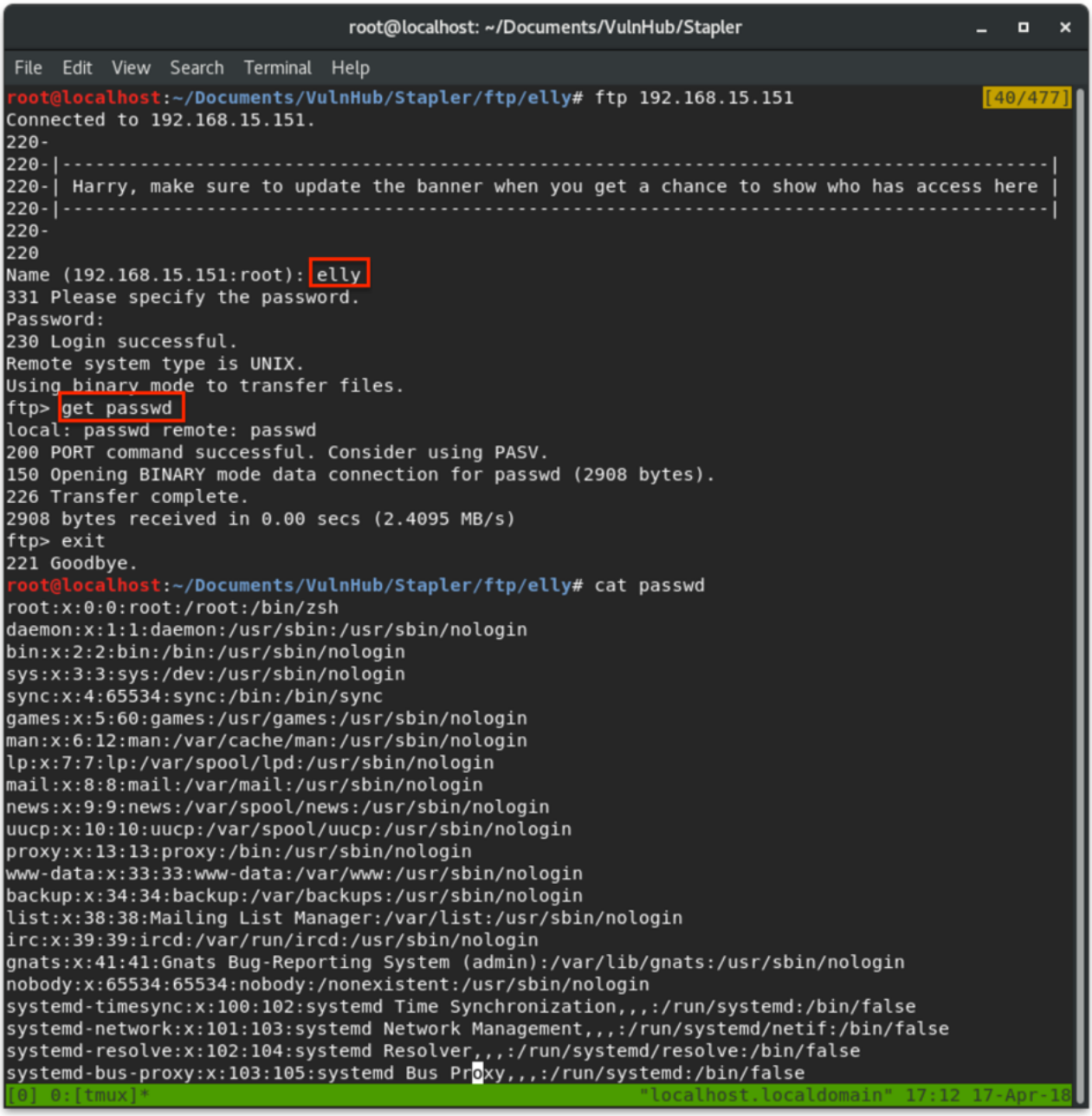


User “elly” used the password “ylle” on FTP.

Lots of files in their FTP directory.



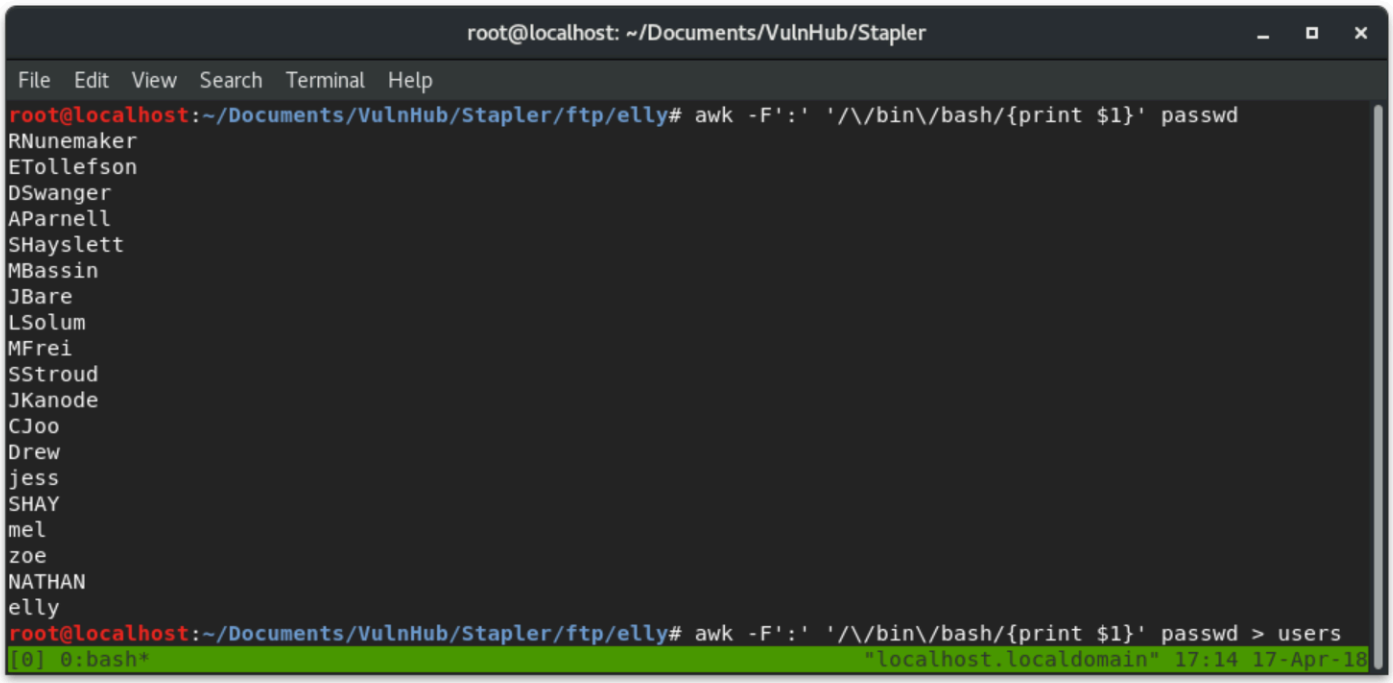
Able to get a retrieve a file called “passwd” from FTP



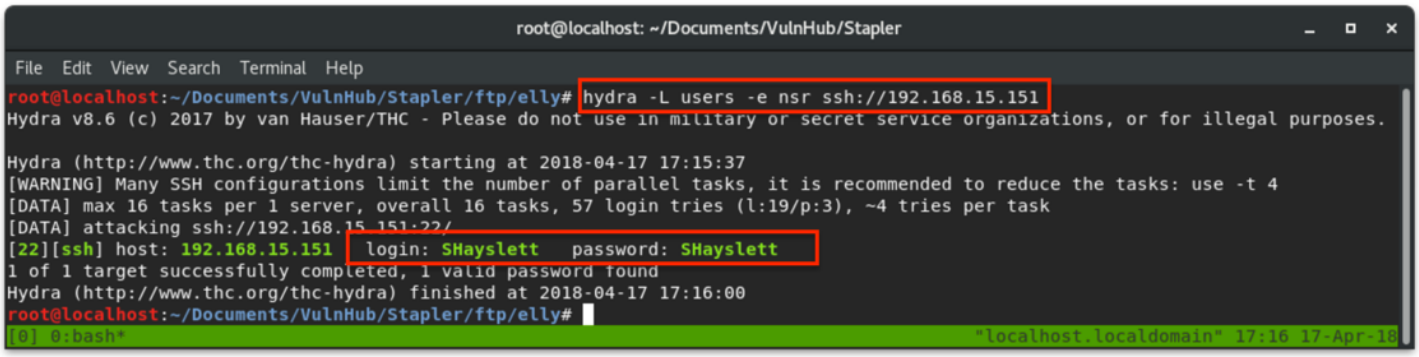
... and the file appears to be a copy of /etc/passwd

SSH Credential Audit

Use awk to parse out a list of users that can log in with /bin/bash



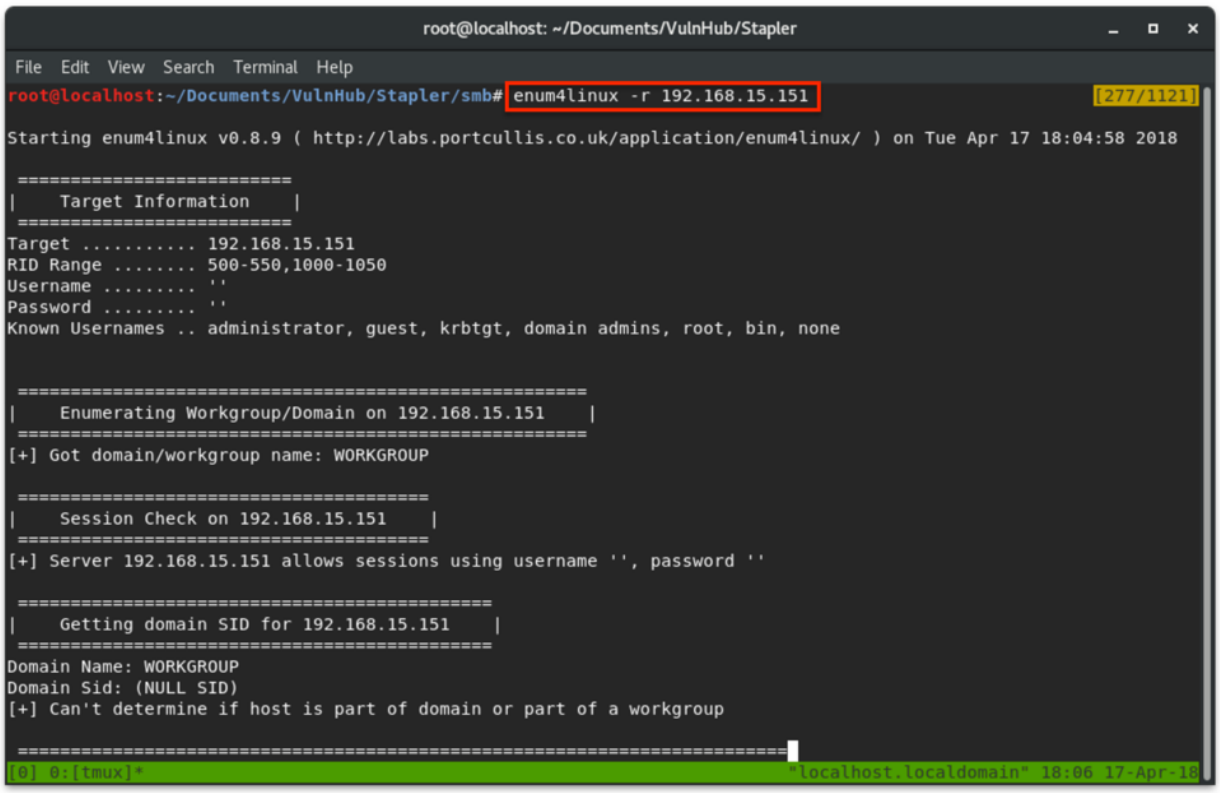
Use hydra and this user list to audit weak ssh credentials

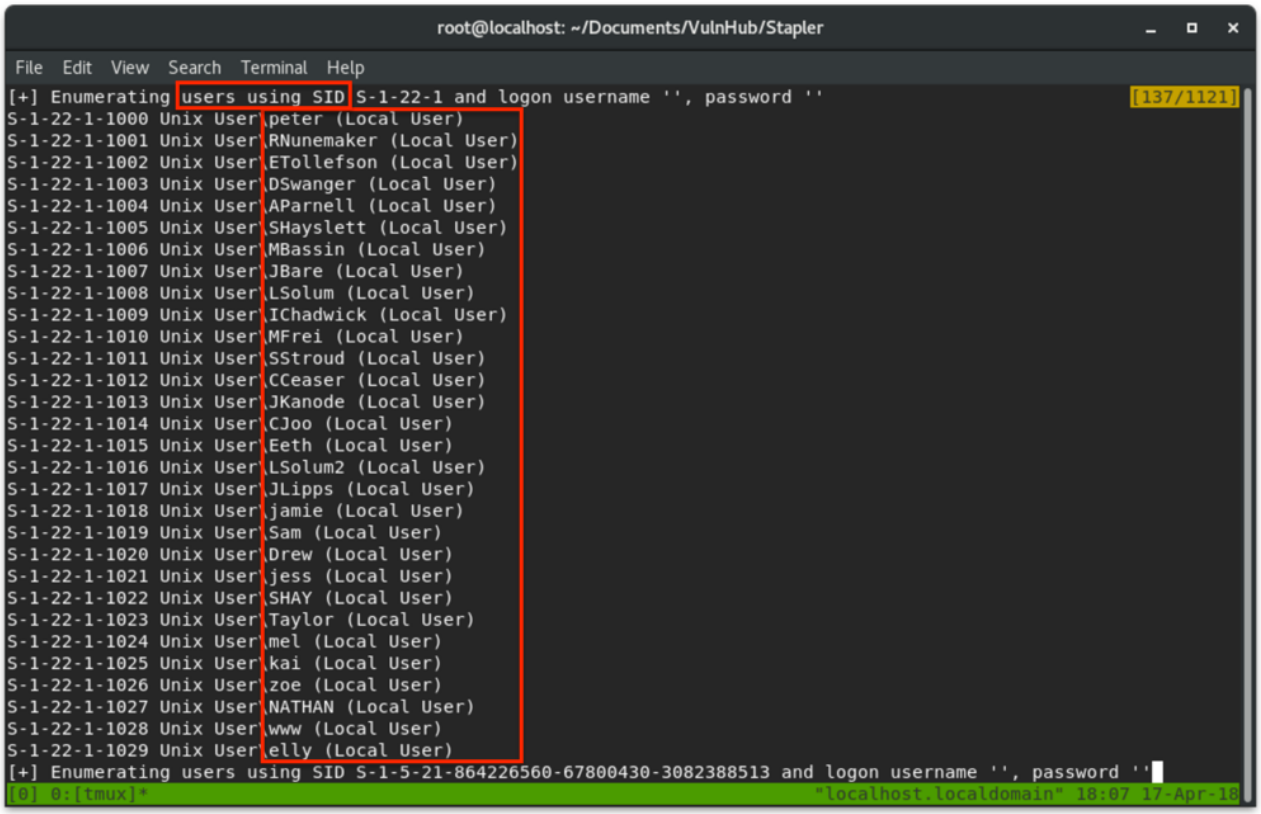


And user “SHayslett” is using their username as their password.

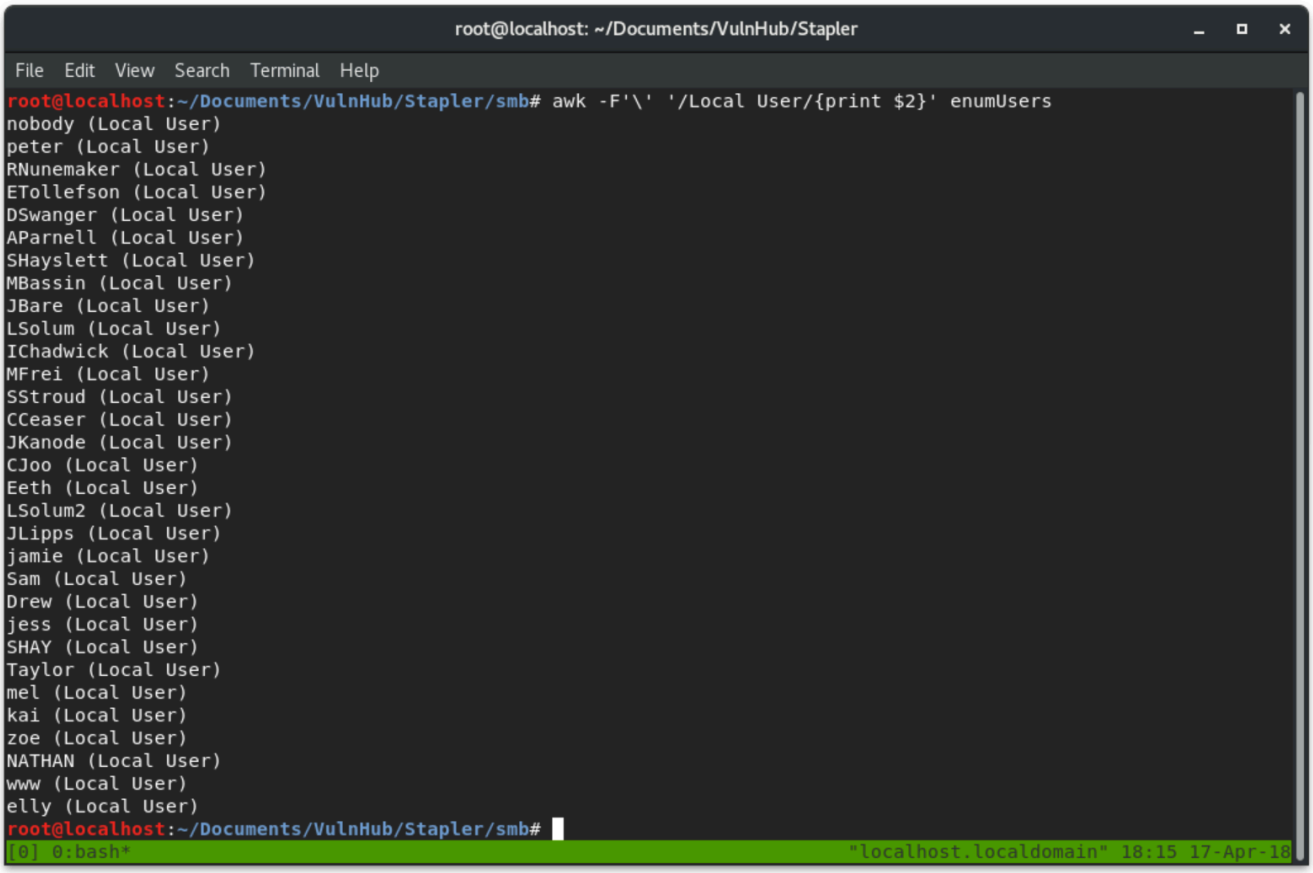
SMB

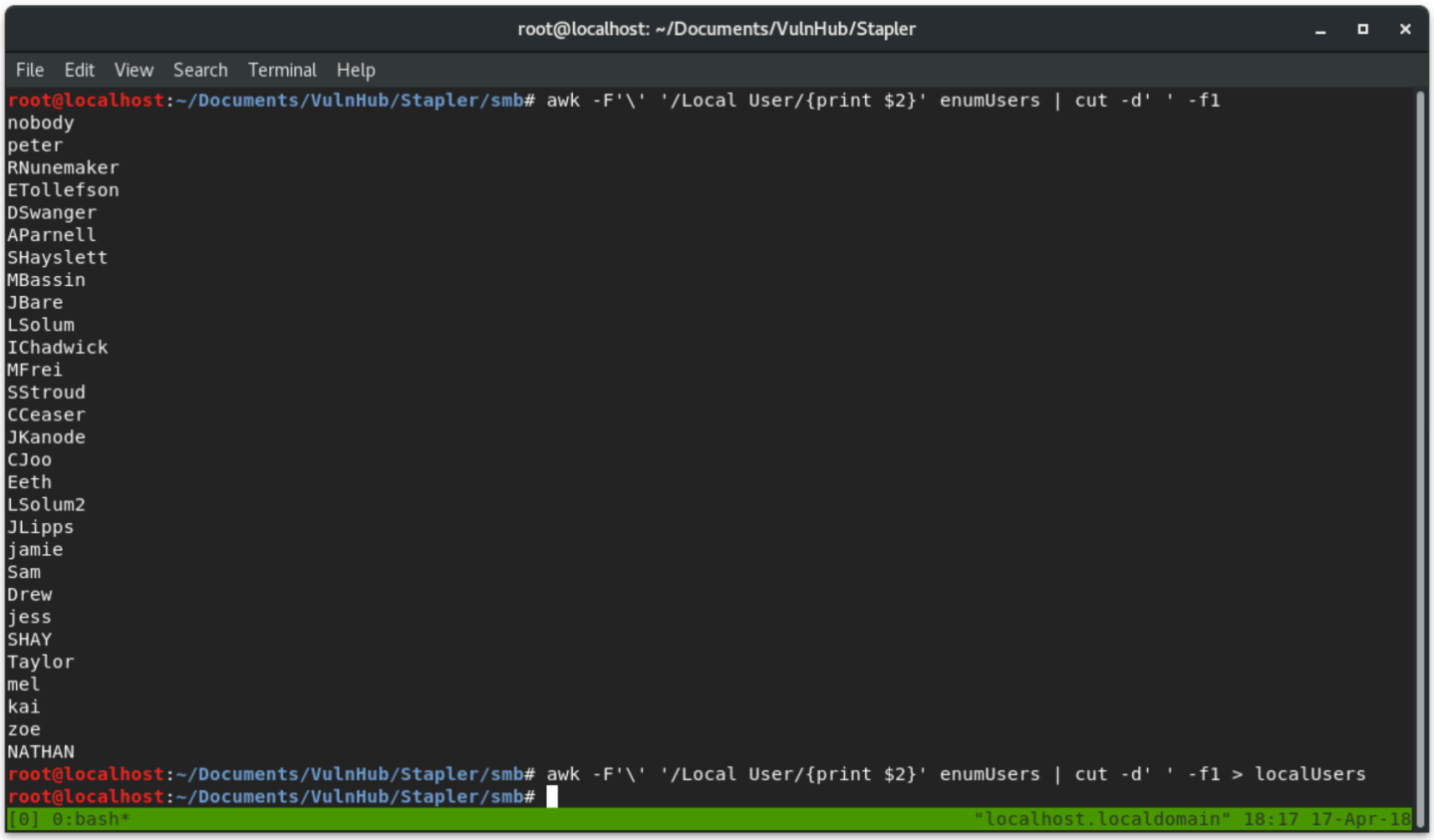
Using SMB to gain a list of local users
enum4linux can bruteforce SIDs to discover local user accounts





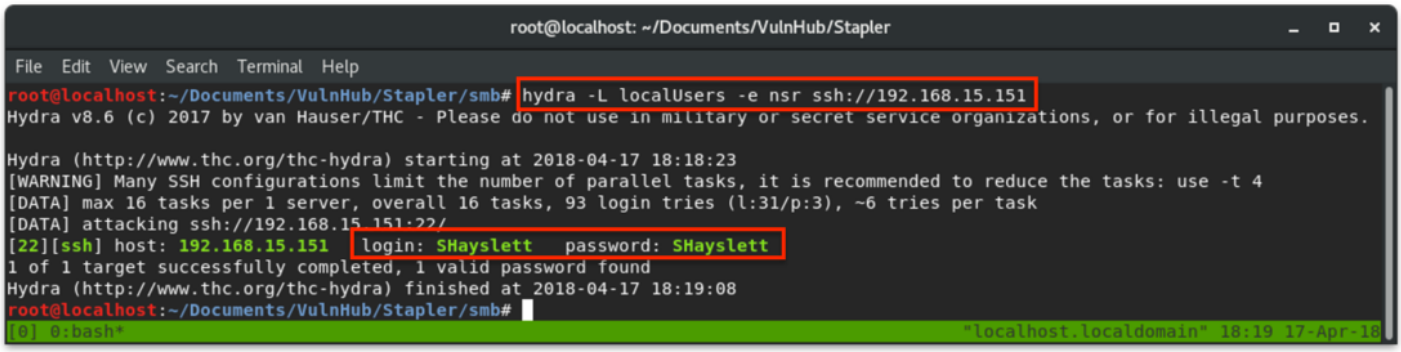
Parse this list with awk and cut to get a list of user accounts



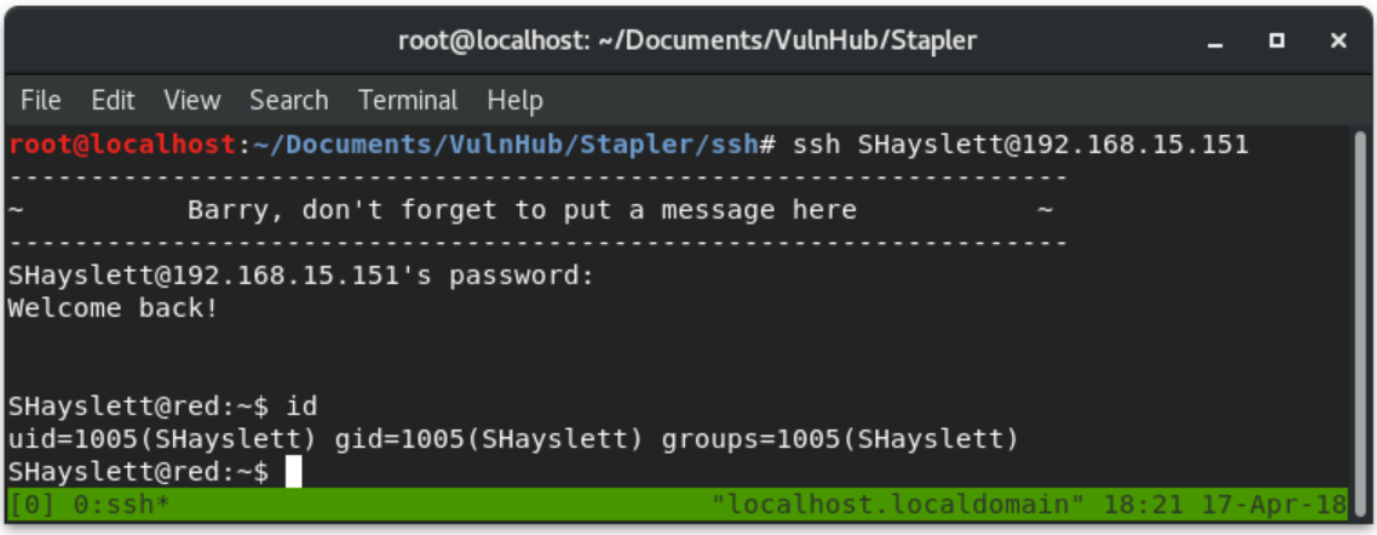


SSH Credential Audit

Use hydra with this user list for the same result as the list from /etc/passwd



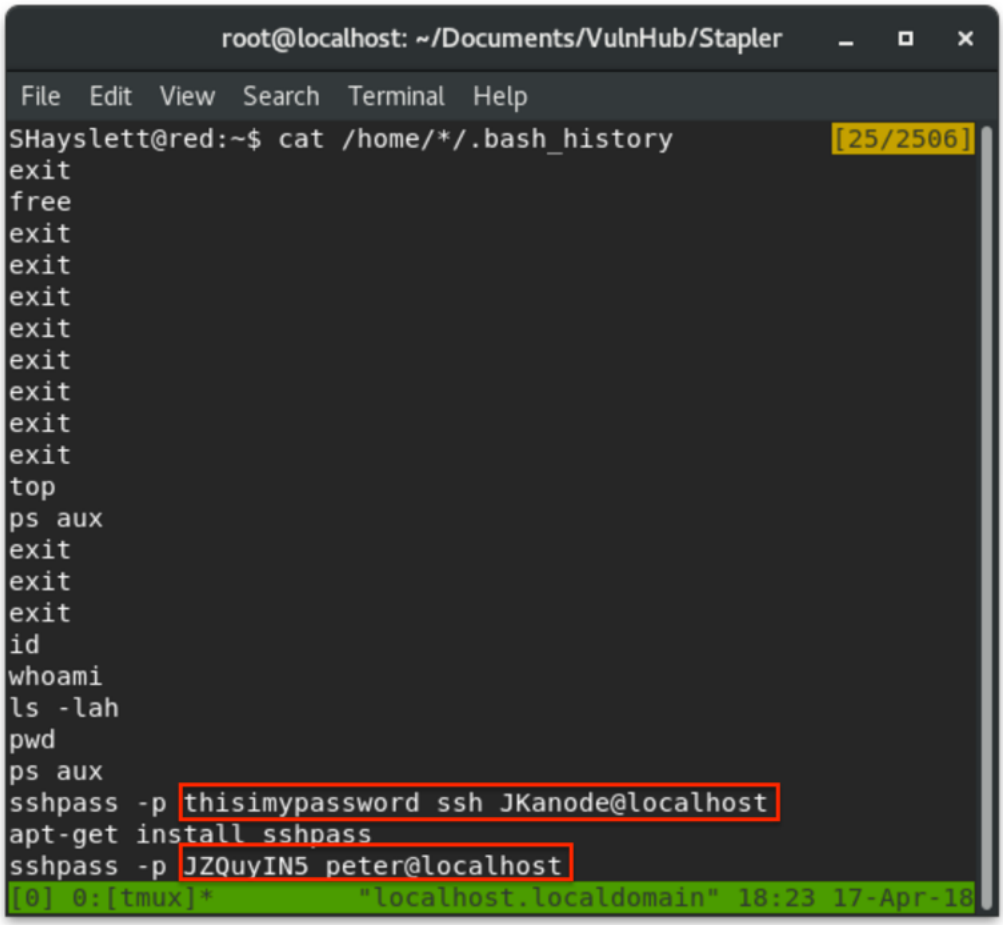
SSH



Not very many files in user directories – both this and other accounts.

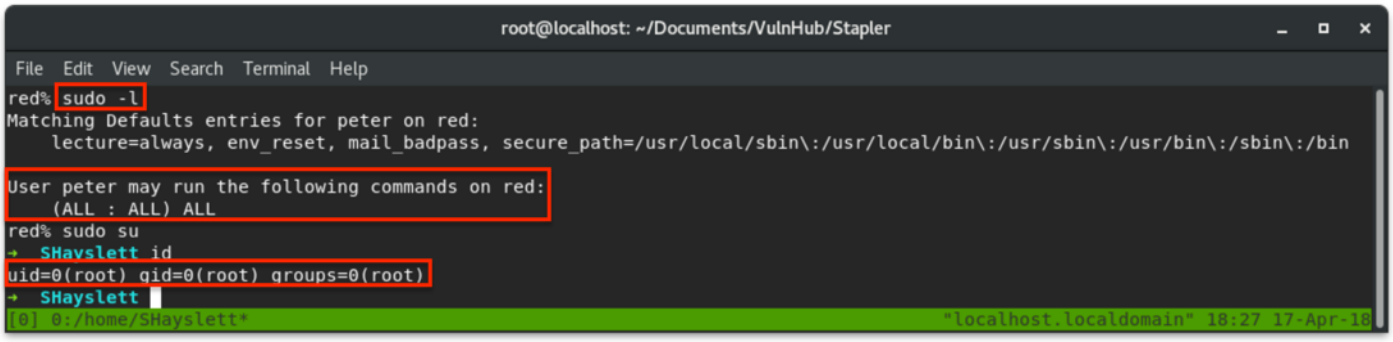
However, we are able to read the .bash_history file of other users...

cat all .bash_history files to see what these users have been up to



Two credentials in plaintext

Privilege Escalation



User “peter” can sudo any command
sudo su returns a root shell in exchange for peter’s password