**CYBR430, Penetration Testing and Incident Response  
Week 5 Lab – grep and regular expressions**

Chad Ballay

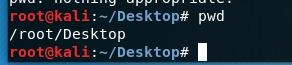
CYBR 430-342

Week 5

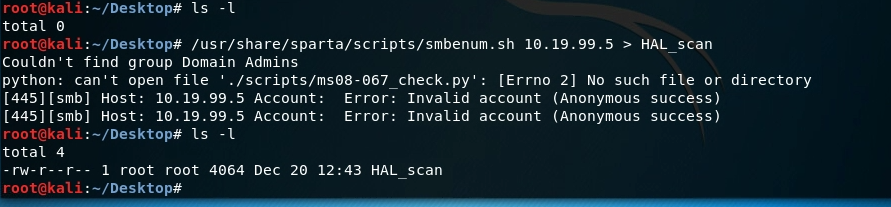
12/20/2020

**What is returned by the pwd command?**

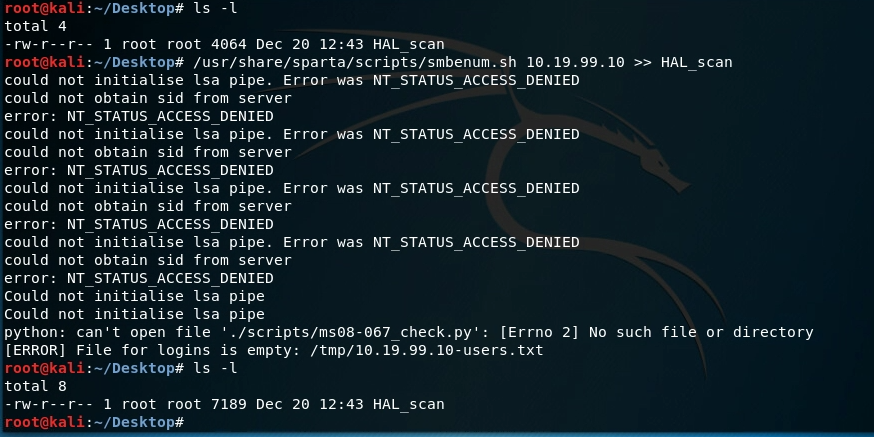
Present working directory. Lists the current directory that the running process has context in.



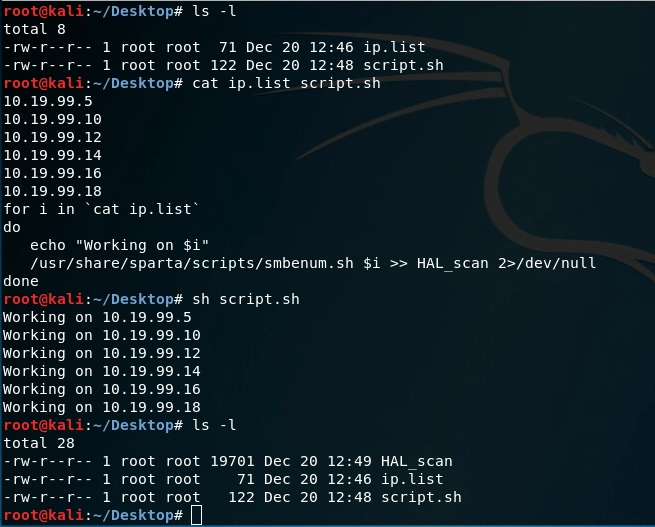
**Provide a screen shot of your directory listing showing the HAL\_scan file**



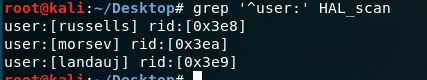
**Provide another screen shot of your directory listing showing the HAL\_scan file and its file size. You should note the file size has gotten larger.**



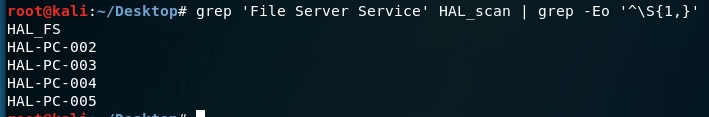
**Provide another screen shot of your directory listing showing the HAL\_scan file and its file size. You should note the file size has gotten larger again.**



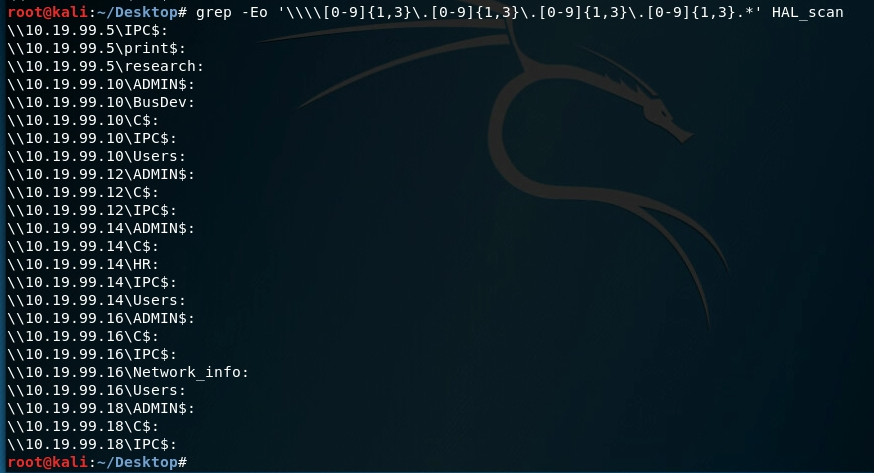
**Enter the command to search your scan file for usernames and provide a screen shot of the results.**



**Enter the above combination grep command and provide a screen shot of your results**



**Complete the regex and execute the completed grep command. Provide a screen shot of the completed command and output. There are several regex which will return the correct results for this assignment, maybe looking for only a partial IP address. Write a paragraph discussing if this is or isn’t good and for what weaknesses (e.g. patterns that may be missed) your particular regex may have?**



Not sure when nmap’s smb-enum-shares script will output IPv6 addresses but my regular expression will fail at that point. My regular expression just looks for 0-999.0-999.0-999.0-999 formatted IP addresses. While that is a proper format that is by no way valid. 333.444.0.0 would pass my expression but that is not a valid IP address.

A better long term solution would be to pick apart smb-enum-shares.nse and possibly see if it’s output could be tweaked to make things more machine readable instead of human readable. JSON or XML based output with rich metadata for contextualizing the information.