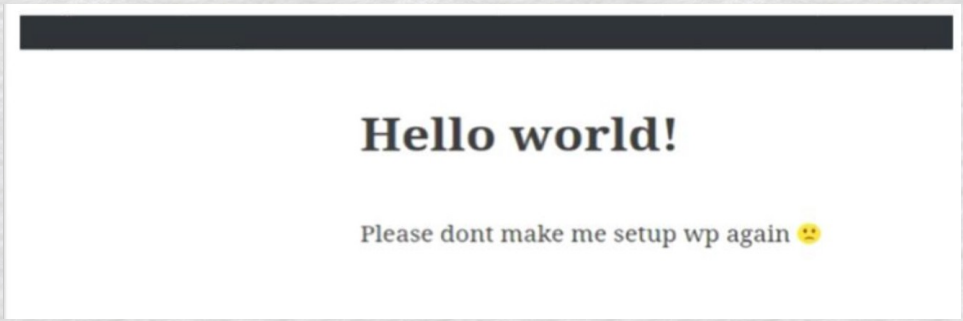
Name : Ahmed Alzahrani **|| Email** : You-187@hotmail.com

IR Writing Assignment

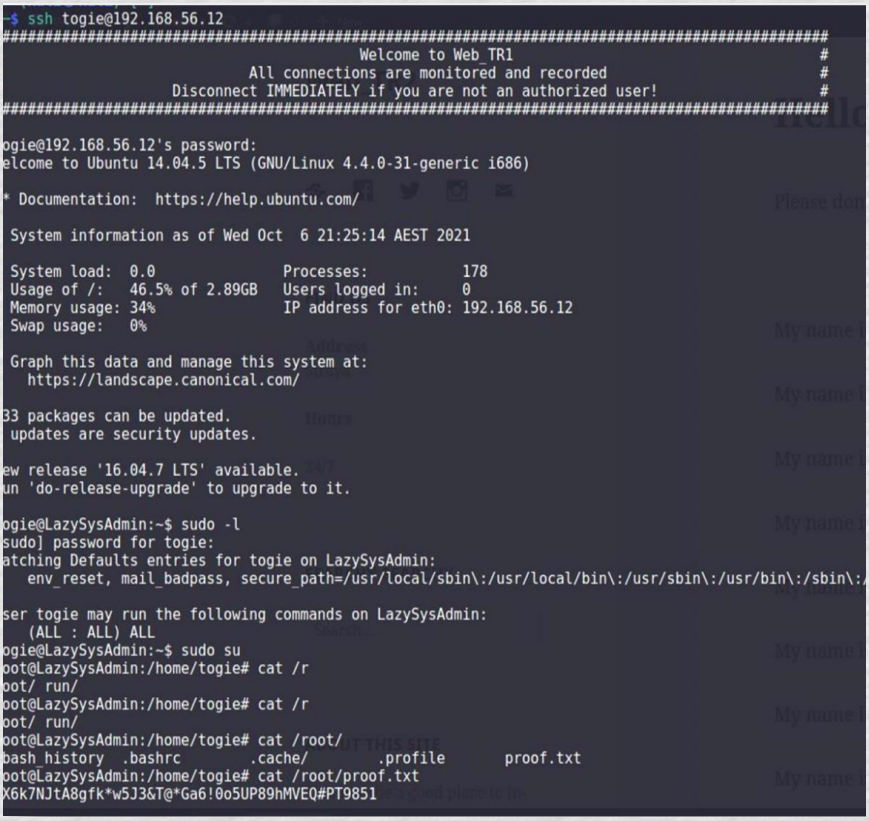
For this lab we will attack the machine named Lazysysadmin then analysis the image after the attack usingautopsy to see if their suspicious activities in the logs 1.
The attack part: I use Nessus to scan for the system We see there 6 ports open in system

1) 22 for SSH
2) 80 for http
3) 139 for SMB
4) 445 for CIFS
5) 3306 for MySQL
6) 6667 for IRC

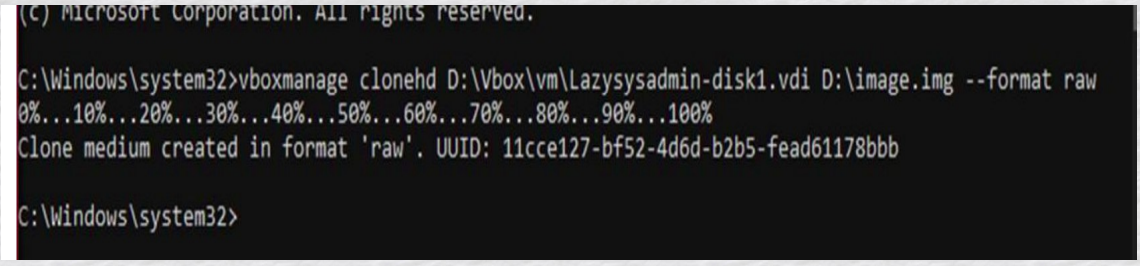
There is a vulnerability we see about folder in SMB called "share" that is do not have privileged AccessSo, we can access to the content of the folder without username or password. This folder has files or folder that we can access them with http with the browser.The more interesting file and folder is: The "deets.txt" file that have a password. The "wordpress" folder have WordPress webpages.
In the wordpress there is a post have the name of the user that could be the username of thesystem" togie".

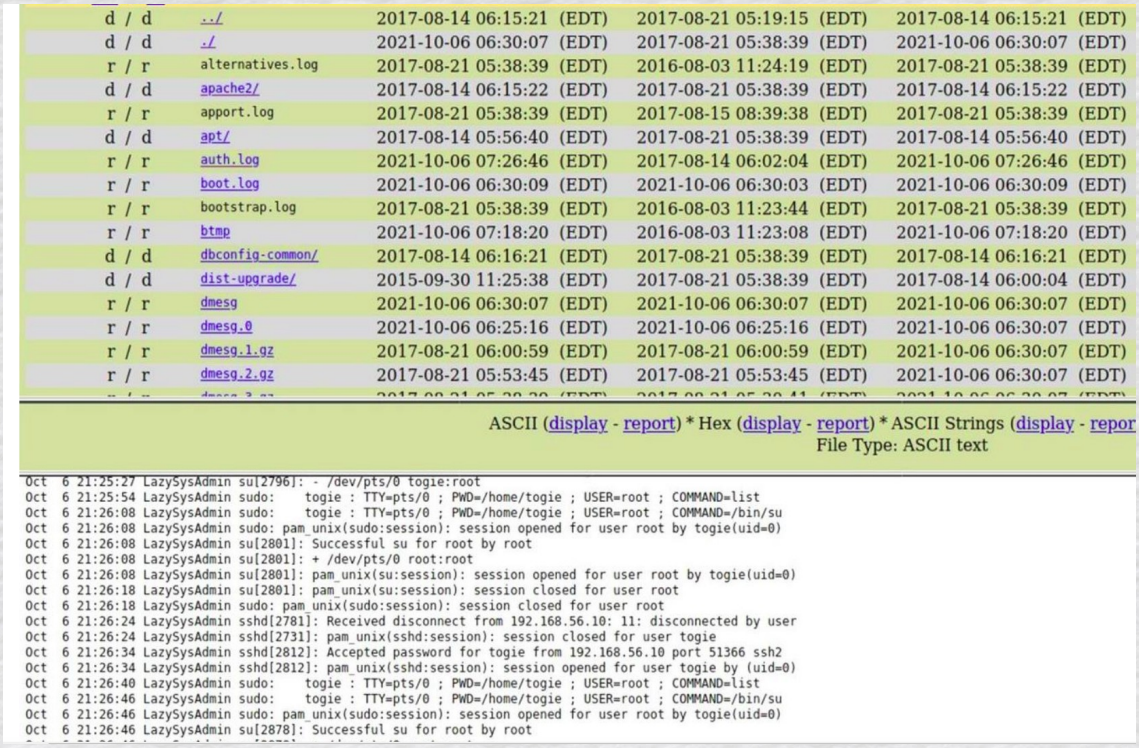


And the password in the "deet.txt" file could be the password. I tried to connect to the system Through SSH service by using the name and password.
I get and Isuccessfully login to the system.



After that I create an image of the system to analyses it with "Autopsy" by using VboxManage.





d / d	../	2017-08-14 06:15:21 (EDT)	2017-08-21 05:19:15 (EDT)	2017-08-14 06:15:21 (EDT)
d / d	./	2021-10-06 06:30:07 (EDT)	2017-08-21 05:38:39 (EDT)	2021-10-06 06:30:07 (EDT)
r / r	alternatives.log	2017-08-21 05:38:39 (EDT)	2016-08-03 11:24:19 (EDT)	2017-08-21 05:38:39 (EDT)
d / d	apache2/	2017-08-14 06:15:22 (EDT)	2017-08-21 05:38:39 (EDT)	2017-08-14 06:15:22 (EDT)
r / r	apport.log	2017-08-21 05:38:39 (EDT)	2017-08-15 08:39:38 (EDT)	2017-08-21 05:38:39 (EDT)
d / d	apt/	2017-08-14 05:56:40 (EDT)	2017-08-21 05:38:39 (EDT)	2017-08-14 05:56:40 (EDT)
r / r	auth.log	2021-10-06 07:26:46 (EDT)	2017-08-14 06:02:04 (EDT)	2021-10-06 07:26:46 (EDT)
r / r	boot.log	2021-10-06 06:30:09 (EDT)	2021-10-06 06:30:03 (EDT)	2021-10-06 06:30:09 (EDT)
r / r	bootstrap.log	2017-08-21 05:38:39 (EDT)	2016-08-03 11:23:44 (EDT)	2017-08-21 05:38:39 (EDT)
r / r	btmp	2021-10-06 07:18:20 (EDT)	2016-08-03 11:23:08 (EDT)	2021-10-06 07:18:20 (EDT)
d / d	dbconfig-common/	2017-08-14 06:16:21 (EDT)	2017-08-21 05:38:39 (EDT)	2017-08-14 06:16:21 (EDT)
d / d	dist-upgrade/	2015-09-30 11:25:38 (EDT)	2017-08-21 05:38:39 (EDT)	2017-08-14 06:00:04 (EDT)
r / r	dmesg	2021-10-06 06:30:07 (EDT)	2021-10-06 06:30:07 (EDT)	2021-10-06 06:30:07 (EDT)
r / r	dmesg.0	2021-10-06 06:25:16 (EDT)	2021-10-06 06:25:16 (EDT)	2021-10-06 06:30:07 (EDT)
r / r	dmesg.1.gz	2017-08-21 06:00:59 (EDT)	2017-08-21 06:00:59 (EDT)	2021-10-06 06:30:07 (EDT)
r / r	dmesg.2.gz	2017-08-21 05:53:45 (EDT)	2017-08-21 05:53:45 (EDT)	2021-10-06 06:30:07 (EDT)

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - repor
File Type: ASCII text

```
Oct  6 21:25:27 LazySysAdmin su[2796]: - /dev/pts/0 togie:root
Oct  6 21:25:54 LazySysAdmin sudo:    togie : TTY=pts/0 ; PWD=/home/togie ; USER=root ; COMMAND=list
Oct  6 21:26:08 LazySysAdmin sudo:    togie : TTY=pts/0 ; PWD=/home/togie ; USER=root ; COMMAND=/bin/su
Oct  6 21:26:08 LazySysAdmin sudo: pam_unix(sudo:session): session opened for user root by togie(uid=0)
Oct  6 21:26:08 LazySysAdmin su[2801]: Successful su for root by root
Oct  6 21:26:08 LazySysAdmin su[2801]: + /dev/pts/0 root:root
Oct  6 21:26:08 LazySysAdmin su[2801]: pam_unix(su:session): session opened for user root by togie(uid=0)
Oct  6 21:26:18 LazySysAdmin su[2801]: pam_unix(su:session): session closed for user root
Oct  6 21:26:18 LazySysAdmin sudo: pam_unix(sudo:session): session closed for user root
Oct  6 21:26:24 LazySysAdmin sshd[2781]: Received disconnect from 192.168.56.10: 11: disconnected by user
Oct  6 21:26:24 LazySysAdmin sshd[2731]: pam_unix(sshd:session): session closed for user togie
Oct  6 21:26:34 LazySysAdmin sshd[2812]: Accepted password for togie from 192.168.56.10 port 51366 ssh2
Oct  6 21:26:34 LazySysAdmin sshd[2812]: pam_unix(sshd:session): session opened for user togie by (uid=0)
Oct  6 21:26:40 LazySysAdmin sudo:    togie : TTY=pts/0 ; PWD=/home/togie ; USER=root ; COMMAND=list
Oct  6 21:26:46 LazySysAdmin sudo:    togie : TTY=pts/0 ; PWD=/home/togie ; USER=root ; COMMAND=/bin/su
Oct  6 21:26:46 LazySysAdmin sudo: pam_unix(sudo:session): session opened for user root by togie(uid=0)
Oct  6 21:26:46 LazySysAdmin su[2878]: Successful su for root by root
```

Then create a case in autopsy and search for the logs:
He got the password and username by using Python coding.
Then he logged insuccessfully to the root.
Username: togie Password: 12345
Accepted password for togie from 192.168.56.10 port 51366 SSH.