



Name : [Ahmed Alzahrani](#) || **Email :** You-187@hotmail.com

IR Writing Assignment

For this lab we will attack the machine named Lazsysadmin then analysis the image after the attack using autopsy 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 the system "togie".



Hello world!

Please dont make me setup wp again 😞

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.

```
-$ ssh togie@192.168.56.12
#####
                        Welcome to Web TR1
                        All connections are monitored and recorded
                        Disconnect IMMEDIATELY if you are not an authorized user!
#####
togie@192.168.56.12's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/
 * 0 updates can be updated.
 * updates are security updates.

System information as of Wed Oct  6 21:25:14 AEST 2021

System load:  0.0      Processes:    178
Usage of /:   46.5% of 2.89GB   Users logged in:  0
Memory usage: 34%      IP address for eth0: 192.168.56.12
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

togie@LazySysAdmin:~$ sudo -l
[sudo] password for togie:
Matching Defaults entries for togie on LazySysAdmin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User togie may run the following commands on LazySysAdmin:
    (ALL : ALL) ALL
togie@LazySysAdmin:~$ sudo su
root@LazySysAdmin:/home/togie# cat /r
root/ run/
root@LazySysAdmin:/home/togie# cat /r
root/ run/
root@LazySysAdmin:/home/togie# cat /root/.profile
bash_history .bashrc .cache/.profile
root@LazySysAdmin:/home/togie# cat /root/.proof.txt
X6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851
#####
```

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

```
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>vboxmanage clonehd D:\Vbox\vm\LazySysAdmin-disk1.vdi D:\image.img --format raw
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone medium created in format 'raw'. UUID: 11cce127-bf52-4d6d-b2b5-fead61178bbb

C:\Windows\system32>
```


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	btmpt	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)
r	/	r	dmesg_3.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 - report)
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 unsuccessfully to the root.

Username: **togie** Password: **12345**

Accepted password for togie from **192.168.56.10** port **51366** SSH.