Metasploit: Introduction

An introduction to the main components of the Metasploit Framework.

Task 2 Main Components of Metasploit

Question	Answer
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

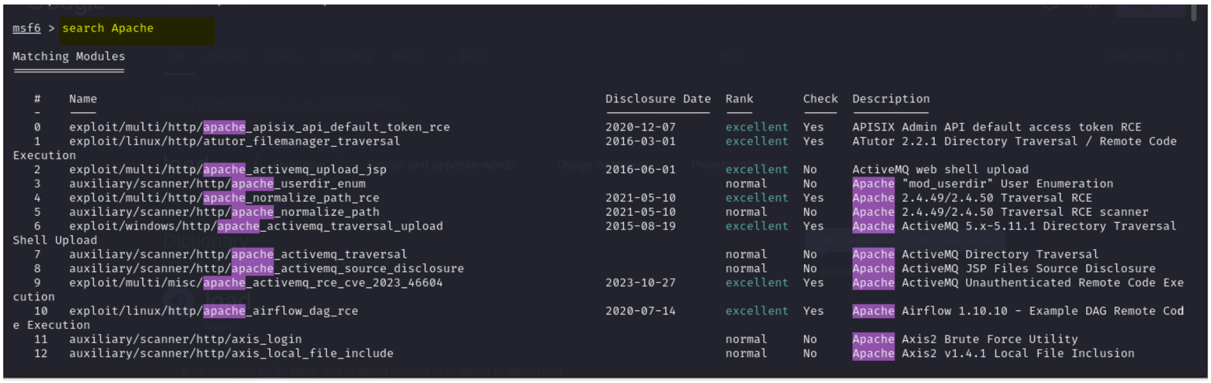
Task 3 Msfconsole

How would you search for a module related to Apache?

- ➔ I launched the Metasploit Framework using the msfconsole command

Command: msfconsole
Command: search Apache

Answer: search Apache



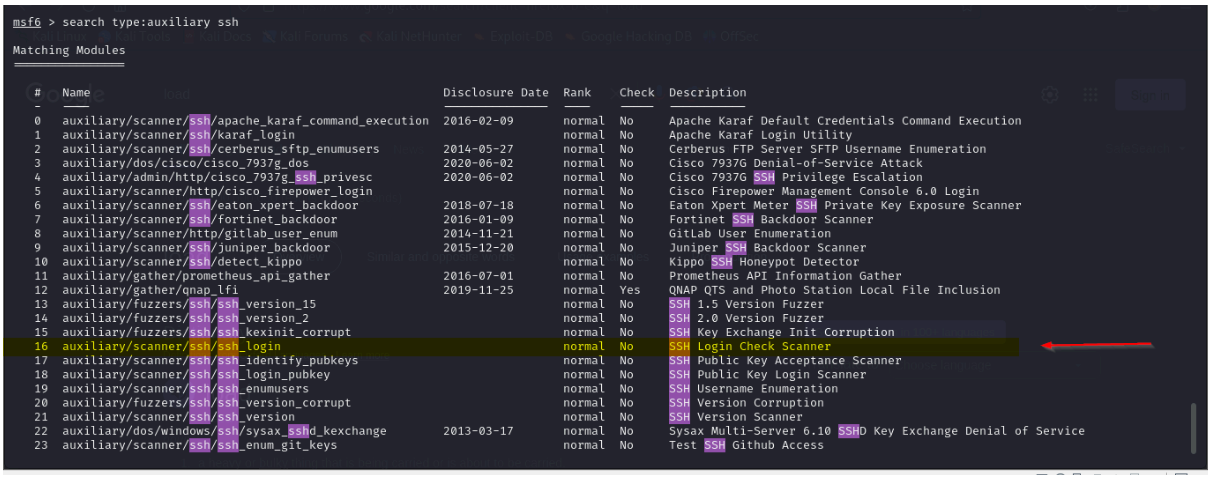
```
msf6 > search Apache

Matching Modules
================

   #    Name                                                                        Disclosure Date  Rank       Check  Description
   -    ----                                                                        ---------------  ----       -----  -----------
   0    exploit/multi/http/apache_apisix_api_default_token_rce                      2020-12-07       excellent  Yes    APISIX Admin API default access token RCE
   1    exploit/linux/http/atutor_filemanager_traversal                             2016-03-01       excellent  Yes    ATutor 2.2.1 Directory Traversal / Remote Code
Execution
   2    exploit/multi/http/apache_activemq_upload_jsp                               2016-06-01       excellent  No     ActiveMQ web shell upload
   3    auxiliary/scanner/http/apache_userdir_enum                                                   normal     No     Apache "mod_userdir" User Enumeration
   4    exploit/multi/http/apache_normalize_path_rce                                2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   5    auxiliary/scanner/http/apache_normalize_path                                2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   6    exploit/windows/http/apache_activemq_traversal_upload                       2015-08-19       excellent  Yes    Apache ActiveMQ 5.x-5.11.1 Directory Traversal
Shell Upload
   7    auxiliary/scanner/http/apache_activemq_traversal                                             normal     No     Apache ActiveMQ Directory Traversal
   8    auxiliary/scanner/http/apache_activemq_source_disclosure                                     normal     No     Apache ActiveMQ JSP Files Source Disclosure
   9    exploit/multi/misc/apache_activemq_rce_cve_2023_46604                       2023-10-27       excellent  Yes    Apache ActiveMQ Unauthenticated Remote Code Exe
cution
   10   exploit/linux/http/apache_airflow_dag_rce                                   2020-07-14       excellent  Yes    Apache Airflow 1.10.10 - Example DAG Remote Cod
e Execution
   11   auxiliary/scanner/http/axis_login                                                            normal     No     Apache Axis2 Brute Force Utility
   12   auxiliary/scanner/http/axis_local_file_include                                               normal     No     Apache Axis2 v1.4.1 Local File Inclusion
```

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

➔ I search for the exact module using the command below

Command: search type:auxiliary ssh

➔ I found different module related to ssh but was able to locate the precise one



```
msf6 > search type:auxiliary ssh

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank    Check  Description
   -   ----                                                 ---------------  ----    -----  -----------
   0   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal  No     Apache Karaf Default Credentials Command Execution
   1   auxiliary/scanner/ssh/karaf_login                                      normal  No     Apache Karaf Login Utility
   2   auxiliary/scanner/ssh/cerberus_sftp_enumusers        2014-05-27       normal  No     Cerberus FTP Server SFTP Username Enumeration
   3   auxiliary/dos/cisco/cisco_7937g_dos                  2020-06-02       normal  No     Cisco 7937G Denial-of-Service Attack
   4   auxiliary/admin/http/cisco_7937g_ssh_privesc         2020-06-02       normal  No     Cisco 7937G SSH Privilege Escalation
   5   auxiliary/scanner/http/cisco_firepower_login                          normal  No     Cisco Firepower Management Console 6.0 Login
   6   auxiliary/scanner/ssh/eaton_xpert_backdoor           2018-07-18       normal  No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   7   auxiliary/scanner/ssh/fortinet_backdoor              2016-01-09       normal  No     Fortinet SSH Backdoor Scanner
   8   auxiliary/scanner/http/gitlab_user_enum              2014-11-21       normal  No     GitLab User Enumeration
   9   auxiliary/scanner/ssh/juniper_backdoor               2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   10  auxiliary/scanner/ssh/detect_kippo                                    normal  No     Kippo SSH Honeypot Detector
   11  auxiliary/gather/prometheus_api_gather               2016-07-01       normal  No     Prometheus API Information Gather
   12  auxiliary/gather/qnap_lfi                            2019-11-25       normal  Yes    QNAP QTS and Photo Station Local File Inclusion
   13  auxiliary/fuzzers/ssh/ssh_version_15                                  normal  No     SSH 1.5 Version Fuzzer
   14  auxiliary/fuzzers/ssh/ssh_version_2                                   normal  No     SSH 2.0 Version Fuzzer
   15  auxiliary/fuzzers/ssh/ssh_kexinit_corrupt                             normal  No     SSH Key Exchange Init Corruption
   16  auxiliary/scanner/ssh/ssh_login                                       normal  No     SSH Login Check Scanner
   17  auxiliary/scanner/ssh/ssh_identify_pubkeys                            normal  No     SSH Public Key Acceptance Scanner
   18  auxiliary/scanner/ssh/ssh_login_pubkey                                normal  No     SSH Public Key Login Scanner
   19  auxiliary/scanner/ssh/ssh_enumusers                                   normal  No     SSH Username Enumeration
   20  auxiliary/fuzzers/ssh/ssh_version_corrupt                             normal  No     SSH Version Corruption
   21  auxiliary/scanner/ssh/ssh_version                                     normal  No     SSH Version Scanner
   22  auxiliary/dos/windows/ssh/sysax_sshd_kexchange       2013-03-17       normal  No     Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
   23  auxiliary/scanner/ssh/ssh_enum_git_keys                               normal  No     Test SSH Github Access
```

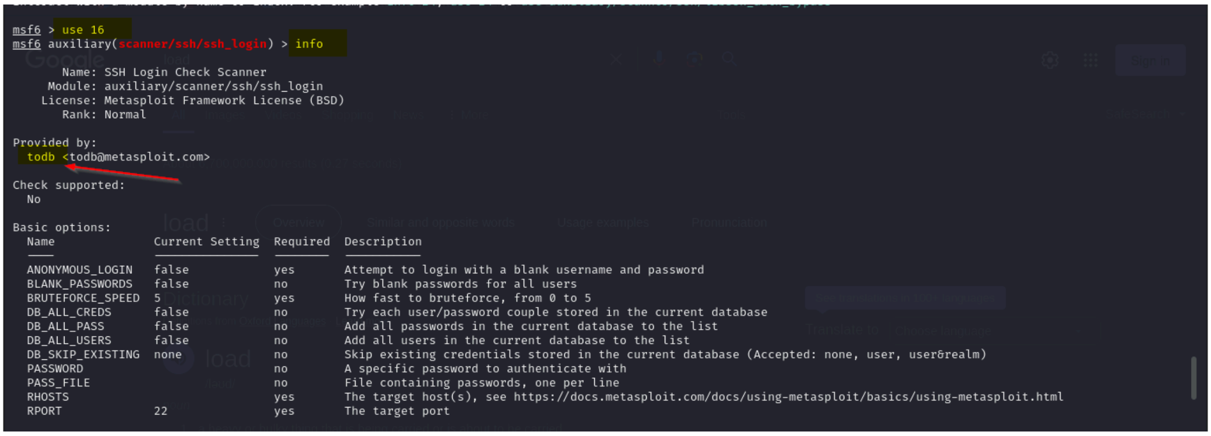
➔ To access the module

Command: use 16

➔ To access the information on the module

Command: info

Answer: todb



```
msf6 > use 16
msf6 auxiliary(scanner/ssh/ssh_login) > info

       Name: SSH Login Check Scanner
     Module: auxiliary/scanner/ssh/ssh_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No

Basic options:
  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
  BLANK_PASSWORDS   false            no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
  DB_ALL_PASS       false            no        Add all passwords in the current database to the list
  DB_ALL_USERS      false            no        Add all users in the current database to the list
  DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
  PASSWORD                           no        A specific password to authenticate with
  PASS_FILE                          no        File containing passwords, one per line
  RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT             22               yes       The target port
```

Task 4 Working with modules

Question	Answer
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 ?	set 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

END!!!