CSFCL IA2: Metasploit

Contributors:

i. Devansh Dang: 16010122035
ii. Arya Dhamale:16010122045

Introduction:

Metasploit stands as an open-source framework devised to enable penetration testers and security researchers in uncovering and exploiting vulnerabilities within computer systems and networks. Originally crafted by H.D. Moore in 2003, it served as a tool for both testing and refining exploits. Metasploit empowers users to assess the security of networks and applications while offering the capability to tailor custom payloads and exploit codes. Its architecture relies on modularity, granting users the flexibility to construct their own modules and plugins. Featuring an extensive library of pre-assembled modules, the framework facilitates the execution of attacks on susceptible systems. These modules are engineered to target specific vulnerabilities, allowing for personalized adjustments to meet user requirements. Accessible through a command-line interface, the Metasploit Framework enables users to interact with the system and initiate attacks. Additionally, it encompasses a graphical user interface (GUI) named Armitage, which furnishes a visual depiction of the network, streamlining navigation and the execution of attacks.

i. Functionalities Implemented:

ii. Metasploit offers a suite of capabilities tailored for penetration testing, vulnerability assessment, and exploitation. Here are some key functionalities that have been implemented:

iii. Exploitation: Metasploit is equipped to exploit vulnerabilities found within computer systems and networks. It boasts an extensive repository of pre-assembled exploits spanning various operating systems and applications.

iv. Payloads: Within Metasploit, users have access to a diverse array of payloads designed to facilitate remote access to targeted systems. These payloads encompass options like establishing a reverse shell or initiating a meterpreter session.

v. Reconnaissance: Metasploit aids in the collection of intelligence concerning a target system or network. This includes identifying open ports, deciphering active services, and discerning details about the operating system in use.

vi. Exploit Development: Metasploit supports the development of exploits, empowering users to craft custom solutions tailored to specific vulnerabilities.

vii. Metasploit includes tools for developing custom exploits and payloads.

i. Advantages of Metasploit:

ii. Open-source Nature: Metasploit operates as an open-source platform, offering users the

freedom to utilize it without cost and adapt it to suit individual requirements or preferences.

iii. Comprehensive Capabilities: With its wide array of functionalities tailored for penetration testing, vulnerability assessment, and exploitation, Metasploit emerges as a versatile tool, catering to the diverse needs of security professionals.

iv. User-Friendly Interface: Metasploit boasts an intuitive interface that simplifies navigation and offers clear, step-by-step instructions for executing various attacks, ensuring accessibility even for those with limited experience in cybersecurity.

v. Vibrant Community Support: The Metasploit community thrives with a significant number of engaged users and developers. This community actively contributes by offering assistance, regular updates, and the development of new modules, fostering a collaborative environment for learning and improvement.

vi. Integration with other tools: Metasploit can be easily integrated with other tools such as Nmap and Wireshark to provide a more comprehensive approach to penetration testing.

i. Disadvantages of Metasploit:

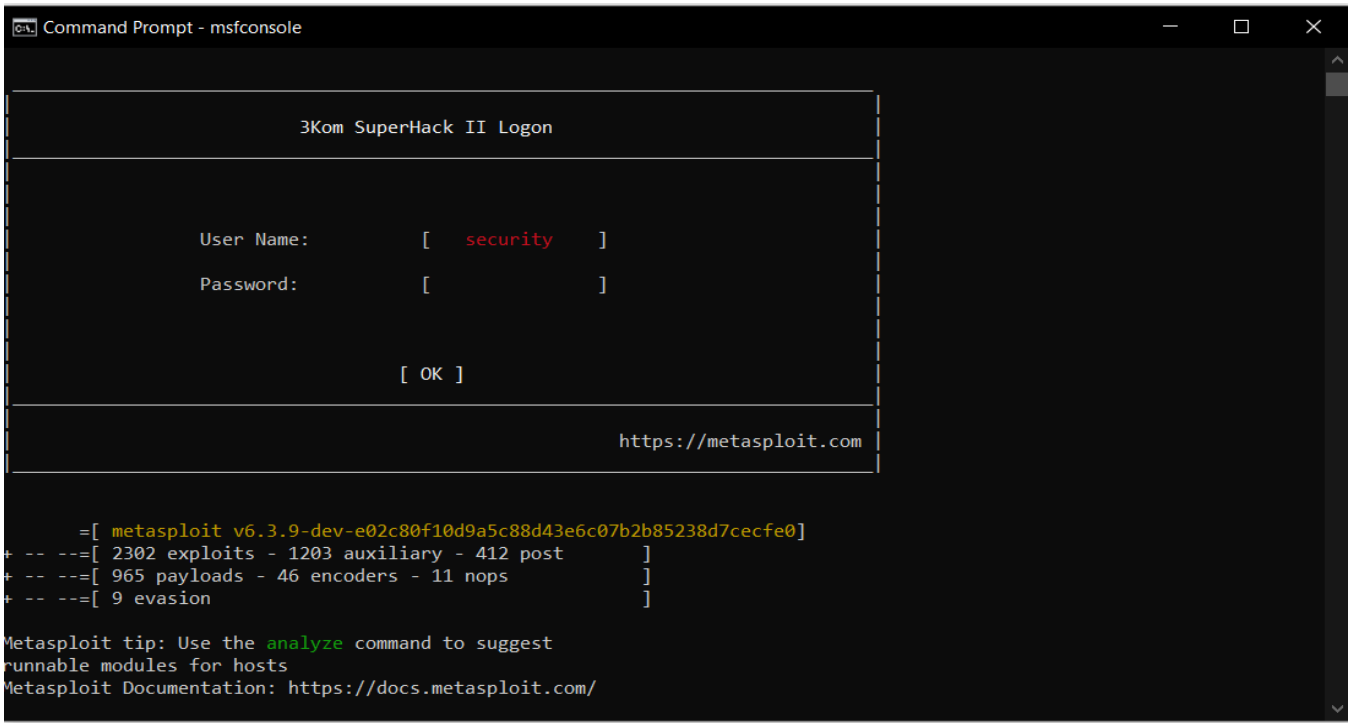
ii. Potential for Misuse: While Metasploit is a powerful tool for cybersecurity professionals, its capabilities can also be exploited by malicious actors. It's crucial to use Metasploit responsibly and only in authorized settings to prevent misuse.

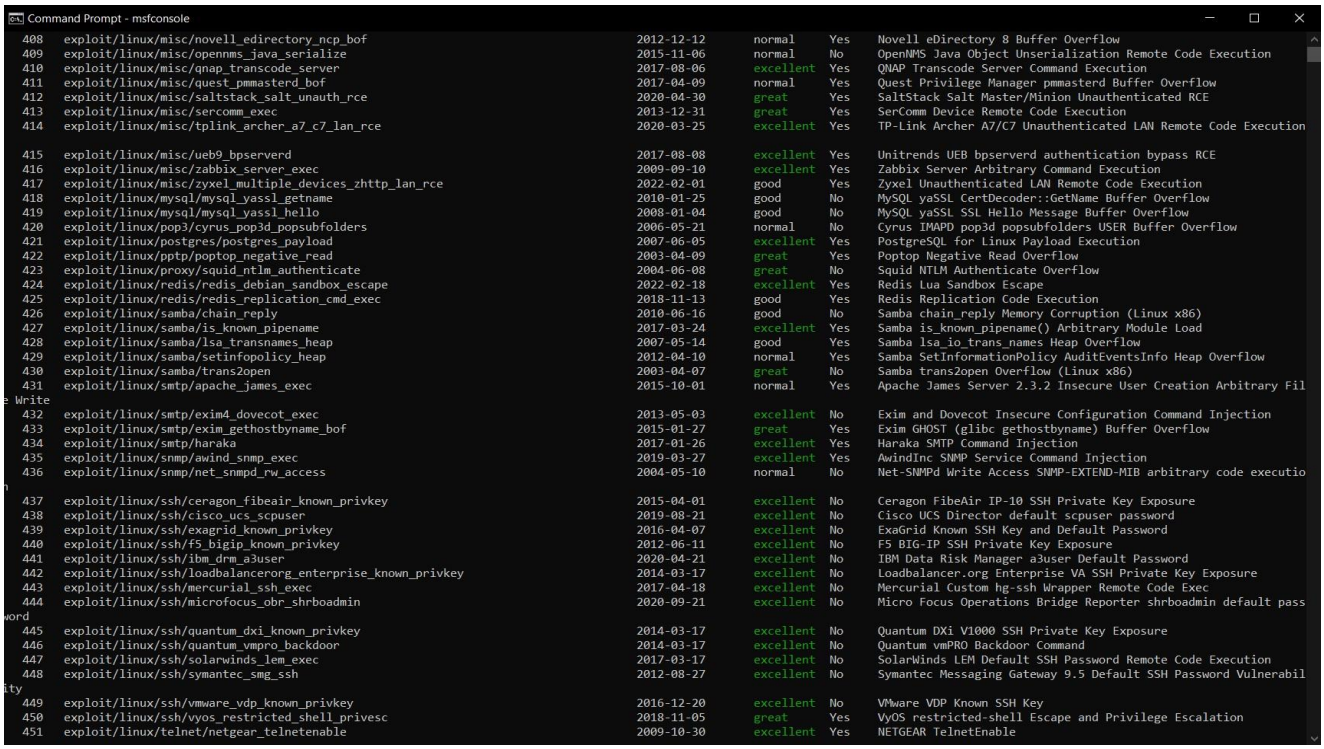
iii. Detection by Antivirus: Some payloads and exploits generated by Metasploit may trigger alerts from antivirus software, diminishing their effectiveness in bypassing security measures.

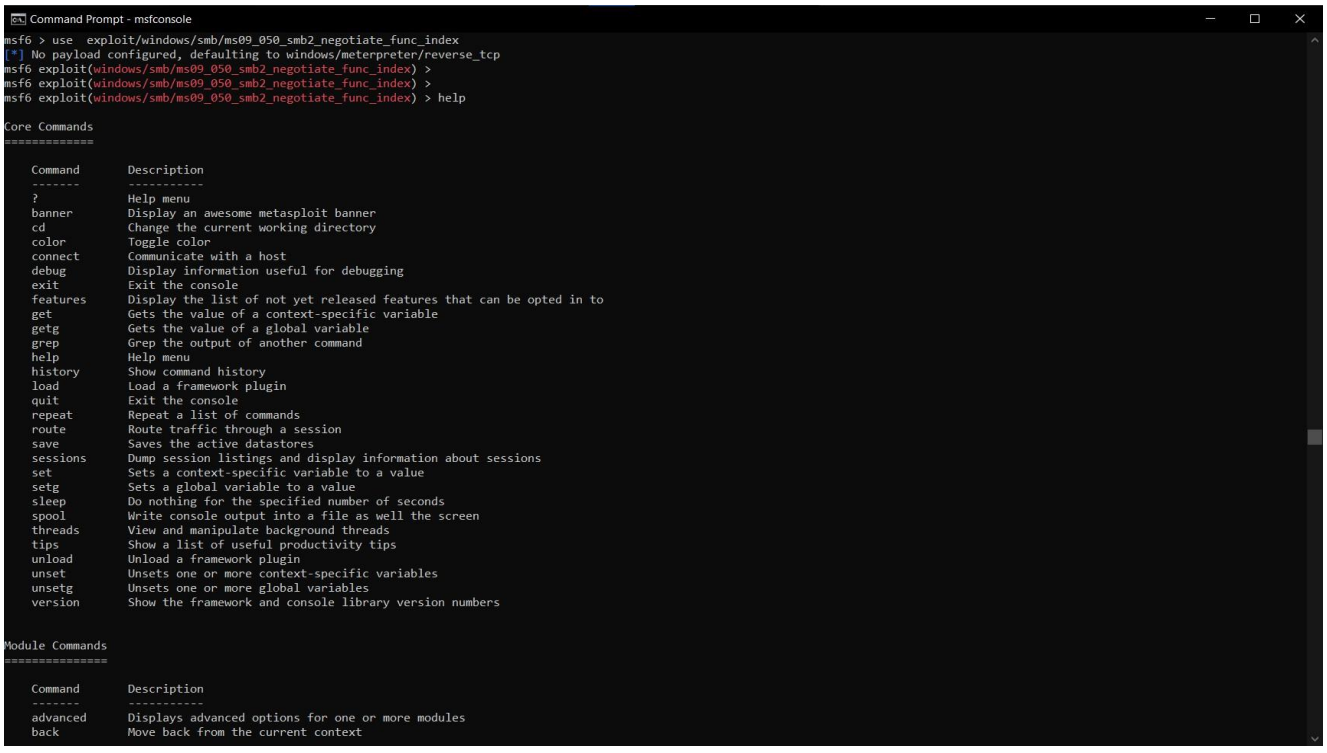
iv. Limited Scope: Metasploit's effectiveness can be limited when dealing with complex or custom-built systems. It may not always be suitable for exploiting certain types of vulnerabilities, which could restrict its applicability in certain scenarios.

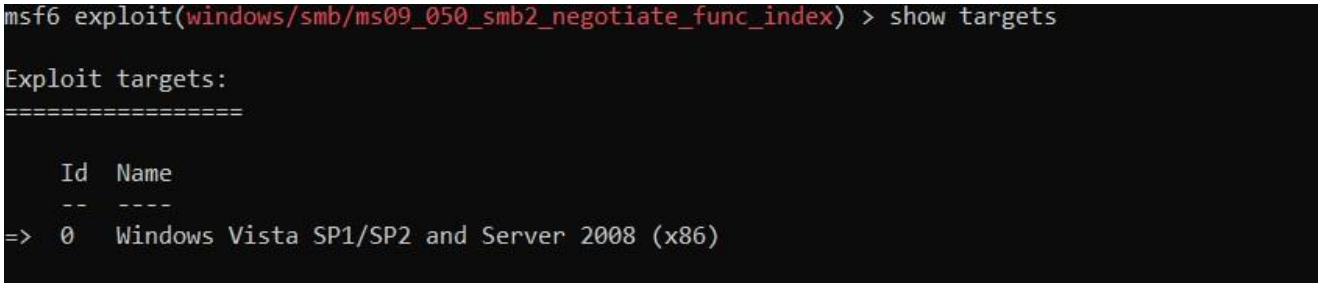
v. Skill and Knowledge Requirements: Utilizing Metasploit effectively demands a certain level of technical proficiency and understanding. Beginners may encounter challenges in mastering its functionalities and may require comprehensive training to navigate its complexities.

Implementation Screenshots:



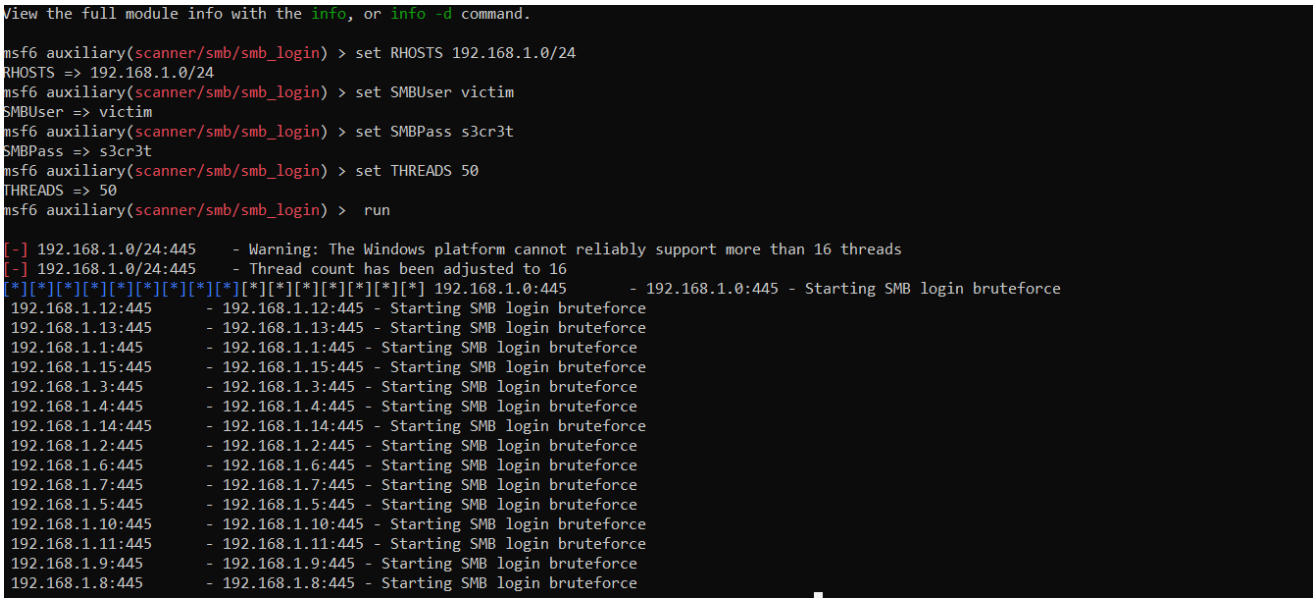

Command Prompt - msfconsole
408 exploit/linux/misc/novell_edirectory_ncp_bof 2012-12-12 normal Yes Novell eDirectory 8 Buffer Overflow
409 exploit/linux/misc/opennms_java_serialize 2015-11-06 normal No OpenNMS Java Object Unserialization Remote Code Execution
410 exploit/linux/misc/qnap_transcode_server 2017-08-06 excellent Yes QNAP Transcode Server Command Execution
411 exploit/linux/misc/quest_pmmasterd_bof 2017-04-09 normal Yes Quest Privilege Manager pmmasterd Buffer Overflow
412 exploit/linux/misc/saltstack_salt_unauth_rce 2020-04-30 great Yes SaltStack Salt Master/Minion Unauthenticated RCE
413 exploit/linux/misc/sercomm_exec 2013-12-31 great Yes SerComm Device Remote Code Execution
414 exploit/linux/misc/tplink_archer_a7_c7_lan_rce 2020-03-25 excellent Yes TP-Link Archer A7/C7 Unauthenticated LAN Remote Code Execution
415 exploit/linux/misc/ueb9_bpserverd 2017-08-08 excellent Yes Unitrends UEB bpserverd authentication bypass RCE
416 exploit/linux/misc/zabbix_server_exec 2009-09-10 excellent Yes Zabbix Server Arbitrary Command Execution
417 exploit/linux/misc/zyxel_multiple_devices_zhttp_lan_rce 2022-02-01 good Yes Zyxel Unauthenticated LAN Remote Code Execution
418 exploit/linux/mysql/mysql_yassl_getname 2010-01-25 good No MySQL yaSSL CertDecoder::GetName Buffer Overflow
419 exploit/linux/mysql/mysql_yassl_hello 2008-01-04 good No MySQL yaSSL SSL Hello Message Buffer Overflow
420 exploit/linux/pop3/cyrus_pop3d_popsubfolders 2006-05-21 normal No Cyrus IMAPD pop3d popsubfolders USER Buffer Overflow
421 exploit/linux/postgres/postgres_payload 2007-06-05 excellent Yes PostgreSQL for Linux Payload Execution
422 exploit/linux/pptp/poptop_negative_read 2003-04-09 great Yes Poptop Negative Read Overflow
423 exploit/linux/proxy/squid_ntlm_authenticate 2004-06-08 great No Squid NTLM Authenticate Overflow
424 exploit/linux/redis/redis_debian_sandbox_escape 2022-02-18 excellent Yes Redis Lua Sandbox Escape
425 exploit/linux/redis/redis_replication_cmd_exec 2018-11-13 good Yes Redis Replication Code Execution
426 exploit/linux/samba/chain_reply 2010-06-16 good No Samba chain_reply Memory Corruption (Linux x86)
427 exploit/linux/samba/is_known_pipename 2017-03-24 excellent Yes Samba is_known_pipename() Arbitrary Module Load
428 exploit/linux/samba/lsa_transnames_heap 2007-05-14 good Yes Samba lsa_io_trans_names Heap Overflow
429 exploit/linux/samba/setinfopolicy_heap 2012-04-10 normal Yes Samba SetInformationPolicy AuditEventsInfo Heap Overflow
430 exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
431 exploit/linux/smtp/apache_james_exec 2015-10-01 normal Yes Apache James Server 2.3.2 Insecure User Creation Arbitrary Fil
e Write
432 exploit/linux/smtp/exim4_dovecot_exec 2013-05-03 excellent No Exim and Dovecot Insecure Configuration Command Injection
433 exploit/linux/smtp/exim_gethostbyname_bof 2015-01-27 great Yes Exim GHOST (glibc gethostbyname) Buffer Overflow
434 exploit/linux/smtp/haraka 2017-01-26 excellent Yes Haraka SMTP Command Injection
435 exploit/linux/snmp/awind_snmp_exec 2019-03-27 excellent Yes AwindInc SNMP Service Command Injection
436 exploit/linux/snmp/net_snmpd_rw_access 2004-05-10 normal No Net-SNMPd Write Access SNMP-EXTEND-MIB arbitrary code executio
n
437 exploit/linux/ssh/ceragon_fibeair_known_privkey 2015-04-01 excellent No Ceragon FibeAir IP-10 SSH Private Key Exposure
438 exploit/linux/ssh/cisco_ucs_scpuser 2019-08-21 excellent No Cisco UCS Director default scpuser password
439 exploit/linux/ssh/exagrid_known_privkey 2016-04-07 excellent No ExaGrid Known SSH Key and Default Password
440 exploit/linux/ssh/f5_bigip_known_privkey 2012-06-11 excellent No F5 BIG-IP SSH Private Key Exposure
441 exploit/linux/ssh/ibm_drm_a3user 2020-04-21 excellent No IBM Data Risk Manager a3user Default Password
442 exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey 2014-03-17 excellent No Loadbalancer.org Enterprise VA SSH Private Key Exposure
443 exploit/linux/ssh/mercurial_ssh_exec 2017-04-18 excellent No Mercurial Custom hg-ssh Wrapper Remote Code Exec
444 exploit/linux/ssh/microfocus_obr_shrboadmin 2020-09-21 excellent No Micro Focus Operations Bridge Reporter shrboadmin default pass
word
445 exploit/linux/ssh/quantum_dxi_known_privkey 2014-03-17 excellent No Quantum DXi V1000 SSH Private Key Exposure
446 exploit/linux/ssh/quantum_vmpro_backdoor 2014-03-17 excellent No Quantum vmPRO Backdoor Command
447 exploit/linux/ssh/solarwinds_lem_exec 2017-03-17 excellent No SolarWinds LEM Default SSH Password Remote Code Execution
448 exploit/linux/ssh/symantec_smg_ssh 2012-08-27 excellent No Symantec Messaging Gateway 9.5 Default SSH Password Vulnerabil
ity
449 exploit/linux/ssh/vmware_vdp_known_privkey 2016-12-20 excellent No VMware VDP Known SSH Key
450 exploit/linux/ssh/vyos_restricted_shell_privesc 2018-11-05 great Yes VyOS restricted-shell Escape and Privilege Escalation
451 exploit/linux/telnet/netgear_telnetenable 2009-10-30 excellent Yes NETGEAR TelnetEnable


Command Prompt - msfconsole
msf6 > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) >
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) >
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > help
Core Commands
Command Description
? Help menu
banner Display an awesome metasploit banner
cd Change the current working directory
color Toggle color
connect Communicate with a host
debug Display information useful for debugging
exit Exit the console
features Display the list of not yet released features that can be opted in to
get Gets the value of a context-specific variable
getg Gets the value of a global variable
grep Grep the output of another command
help Help menu
history Show command history
load Load a framework plugin
quit Exit the console
repeat Repeat a list of commands
route Route traffic through a session
save Saves the active datastores
sessions Dump session listings and display information about sessions
set Sets a context-specific variable to a value
setg Sets a global variable to a value
sleep Do nothing for the specified number of seconds
spool Write console output into a file as well the screen
threads View and manipulate background threads
tips Show a list of useful productivity tips
unload Unload a framework plugin
unset Unsets one or more context-specific variables
unsetg Unsets one or more global variables
version Show the framework and console library version numbers
Module Commands
Command Description
advanced Displays advanced options for one or more modules
back Move back from the current context


msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > show targets
Exploit targets:
Id Name
-- ----
=> 0 Windows Vista SP1/SP2 and Server 2008 (x86)

```
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > show payloads

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

   #    Name                                                Disclosure Date  Rank    Check  Description
   -    ----                                                ---------------  ----    -----  -----------
   0    payload/generic/custom                                               normal  No     Custom Payload
   1    payload/generic/debug_trap                                           normal  No     Generic x86 Debug Trap
   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/generic/tight_loop                                           normal  No     Generic x86 Tight Loop
   6    payload/windows/adduser                                              normal  No     Windows Execute net user /ADD
   7    payload/windows/custom/bind_hidden_ipknock_tcp                       normal  No     Windows shellcode stage, Hidden Bind Ipknock TCP Stager
   8    payload/windows/custom/bind_hidden_tcp                               normal  No     Windows shellcode stage, Hidden Bind TCP Stager
   9    payload/windows/custom/bind_ipv6_tcp                                 normal  No     Windows shellcode stage, Bind IPv6 TCP Stager (Windows x86)
   10   payload/windows/custom/bind_ipv6_tcp_uuid                            normal  No     Windows shellcode stage, Bind IPv6 TCP Stager with UUID Support (Windows x86)
   11   payload/windows/custom/bind_named_pipe                               normal  No     Windows shellcode stage, Windows x86 Bind Named Pipe Stager
   12   payload/windows/custom/bind_nonx_tcp                                 normal  No     Windows shellcode stage, Bind TCP Stager (No NX or Win7)
   13   payload/windows/custom/bind_tcp                                      normal  No     Windows shellcode stage, Bind TCP Stager (Windows x86)
   14   payload/windows/custom/bind_tcp_rc4                                  normal  No     Windows shellcode stage, Bind TCP Stager (RC4 Stage Encryption, Metasm)
   15   payload/windows/custom/bind_tcp_uuid                                 normal  No     Windows shellcode stage, Bind TCP Stager with UUID Support (Windows x86)
   16   payload/windows/custom/reverse_hop_http                              normal  No     Windows shellcode stage, Reverse Hop HTTP/HTTPS Stager
   17   payload/windows/custom/reverse_http                                  normal  No     Windows shellcode stage, Windows Reverse HTTP Stager (wininet)
   18   payload/windows/custom/reverse_http_proxy_pstore                     normal  No     Windows shellcode stage, Reverse HTTP Stager Proxy
   19   payload/windows/custom/reverse_https                                 normal  No     Windows shellcode stage, Windows Reverse HTTPS Stager (wininet)
   20   payload/windows/custom/reverse_https_proxy                           normal  No     Windows shellcode stage, Reverse HTTPS Stager with Support for Custom Proxy
   21   payload/windows/custom/reverse_ipv6_tcp                              normal  No     Windows shellcode stage, Reverse TCP Stager (IPv6)
   22   payload/windows/custom/reverse_named_pipe                            normal  No     Windows shellcode stage, Windows x86 Reverse Named Pipe (SMB) Stager
   23   payload/windows/custom/reverse_nonx_tcp                              normal  No     Windows shellcode stage, Reverse TCP Stager (No NX or Win7)
   24   payload/windows/custom/reverse_ord_tcp                               normal  No     Windows shellcode stage, Reverse Ordinal TCP Stager (No NX or Win7)
   25   payload/windows/custom/reverse_tcp                                   normal  No     Windows shellcode stage, Reverse TCP Stager
   26   payload/windows/custom/reverse_tcp_allports                          normal  No     Windows shellcode stage, Reverse All-Port TCP Stager
   27   payload/windows/custom/reverse_tcp_dns                               normal  No     Windows shellcode stage, Reverse TCP Stager (DNS)
   28   payload/windows/custom/reverse_tcp_rc4                               normal  No     Windows shellcode stage, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   29   payload/windows/custom/reverse_tcp_rc4_dns                           normal  No     Windows shellcode stage, Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
   30   payload/windows/custom/reverse_tcp_uuid                              normal  No     Windows shellcode stage, Reverse TCP Stager with UUID Support
   31   payload/windows/custom/reverse_udp                                   normal  No     Windows shellcode stage, Reverse UDP Stager with UUID Support
   32   payload/windows/custom/reverse_winhttp                               normal  No     Windows shellcode stage, Windows Reverse HTTP Stager (winhttp)
   33   payload/windows/custom/reverse_winhttps                              normal  No     Windows shellcode stage, Windows Reverse HTTPS Stager (winhttp)
   34   payload/windows/dllinject/bind_hidden_ipknock_tcp                    normal  No     Reflective DLL Injection, Hidden Bind Ipknock TCP Stager
   35   payload/windows/dllinject/bind_hidden_tcp                            normal  No     Reflective DLL Injection, Hidden Bind TCP Stager
   36   payload/windows/dllinject/bind_ipv6_tcp                              normal  No     Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86)
   37   payload/windows/dllinject/bind_ipv6_tcp_uuid                         normal  No     Reflective DLL Injection, Bind IPv6 TCP Stager with UUID Support (Windows x86)
   38   payload/windows/dllinject/bind_named_pipe                            normal  No     Reflective DLL Injection, Windows x86 Bind Named Pipe Stager
   39   payload/windows/dllinject/bind_nonx_tcp                              normal  No     Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
   40   payload/windows/dllinject/bind_tcp                                   normal  No     Reflective DLL Injection, Bind TCP Stager (Windows x86)
```

```
msf6 >  use auxiliary/scanner/smb/smb_login
msf6 auxiliary(scanner/smb/smb_login) > show options

Module options (auxiliary/scanner/smb/smb_login):

   Name               Current Setting  Required  Description
   ----               ---------------  --------  -----------
   ABORT_ON_LOCKOUT   false            yes       Abort the run when an account lockout is detected
   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)
   DETECT_ANY_AUTH    false            no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN  false            no        Detect if domain is required for the specified user
   PASS_FILE                           no        File containing passwords, one per line
   PRESERVE_DOMAINS   true             no        Respect a username that contains a domain name.
   Proxies                             no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST       false            no        Record guest-privileged random logins to the database
   RHOSTS                              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT              445              yes       The SMB service port (TCP)
   SMBDomain          .                no        The Windows domain to use for authentication
   SMBPass                             no        The password for the specified username
   SMBUser                             no        The username to authenticate as
   STOP_ON_SUCCESS    false            yes       Stop guessing when a credential works for a host
   THREADS            1                yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                       no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS       false            no        Try the username as the password for all users
   USER_FILE                           no        File containing usernames, one per line
   VERBOSE            true             yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.
```



Conclusion:

In conclusion, Metasploit emerges as a potent asset for both probing security vulnerabilities and fortifying system defenses. Its extensive arsenal of exploits and payloads enables thorough security testing and vulnerability identification. Nevertheless, its robust capabilities entail a responsibility to wield it ethically and conscientiously, given its potential for misuse. Effective utilization of Metasploit mandates a deep understanding of the target system and its vulnerabilities, alongside obtaining explicit permission from system owners before conducting tests or exploits. Failure to adhere to ethical guidelines can lead to legal repercussions and harm to both the tester and the targeted system. Despite the risks, Metasploit remains a cornerstone in cybersecurity, empowering professionals to preemptively address weaknesses and thwart potential threats. Its value lies in its ability to bolster defenses against malicious actors, underscoring the importance of responsible and ethical use at all times.