Metasploit Framework

MSFConsole

Agenda

- MSFconsole
  - MSFConsole Basics
    - Core Commands
      - Search, Use, set/unset, show, info, route, quit/ exit
    - Database Backend Commands
    - Exploit Commands
    - Payload Commands
    - Auxiliary Commands
    - Post Commands

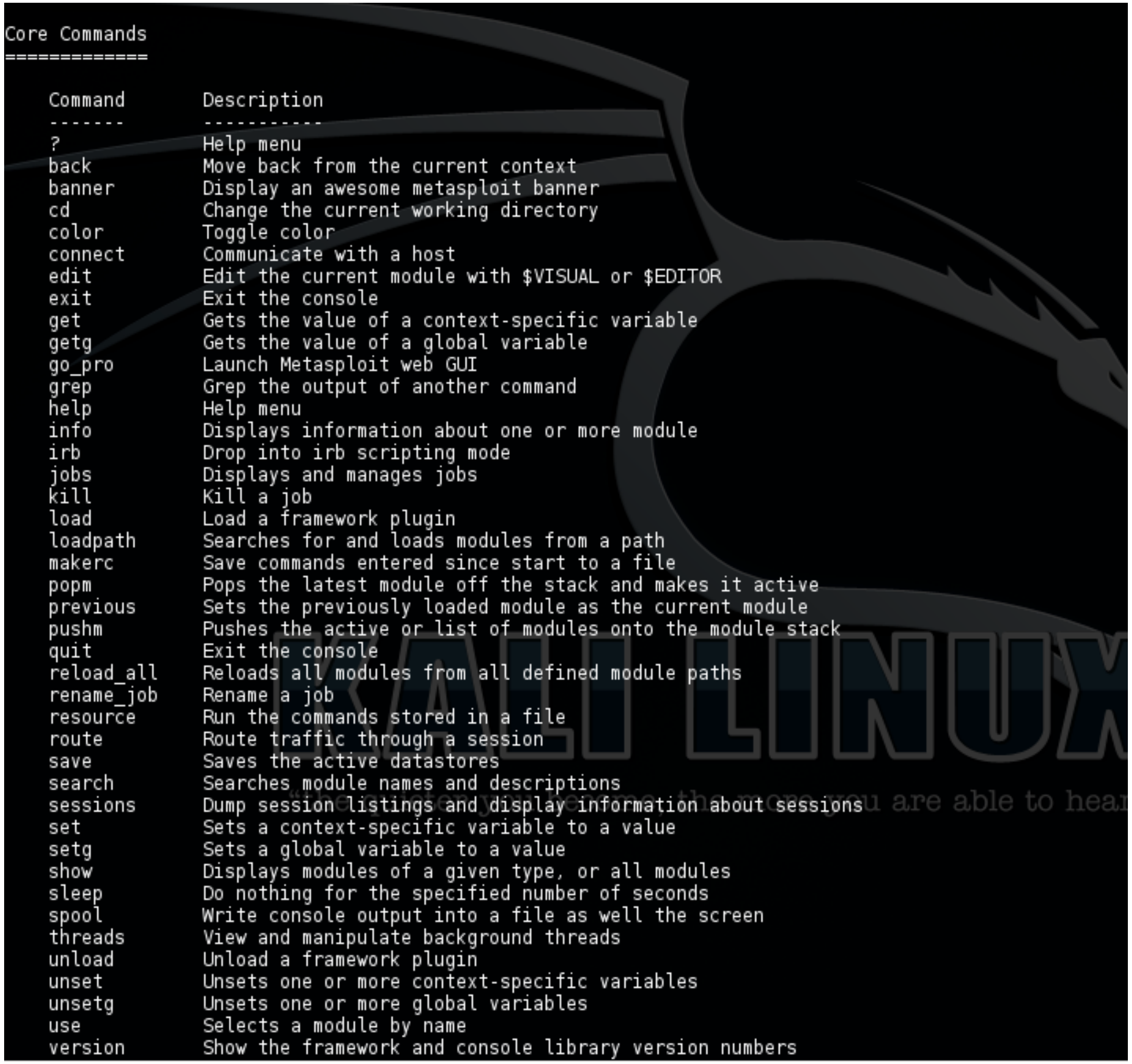
MSFConsole

- Core Commands
- Database Backend Commands
- Exploit Commands
- Payload Commands
- Auxiliary Commands
- Post Commands

Core Commands

MSFCONSOLE

MSFConsole: Core



```
Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    edit          Edit the current module with $VISUAL or $EDITOR
    exit          Exit the console
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    go_pro        Launch Metasploit web GUI
    grep          Grep the output of another command
    help          Help menu
    info          Displays information about one or more module
    irb           Drop into irb scripting mode
    jobs          Displays and manages jobs
    kill          Kill a job
    load          Load a framework plugin
    loadpath      Searches for and loads modules from a path
    makerc        Save commands entered since start to a file
    popm          Pops the latest module off the stack and makes it active
    previous      Sets the previously loaded module as the current module
    pushm         Pushes the active or list of modules onto the module stack
    quit          Exit the console
    reload_all    Reloads all modules from all defined module paths
    rename_job    Rename a job
    resource      Run the commands stored in a file
    route         Route traffic through a session
    save          Saves the active datastores
    search        Searches module names and descriptions
    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
    show          Displays modules of a given type, or all modules
    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
    unload        Unload a framework plugin
    unset         Unsets one or more context-specific variables
    unsetg        Unsets one or more global variables
    use           Selects a module by name
    version       Show the framework and console library version numbers
```

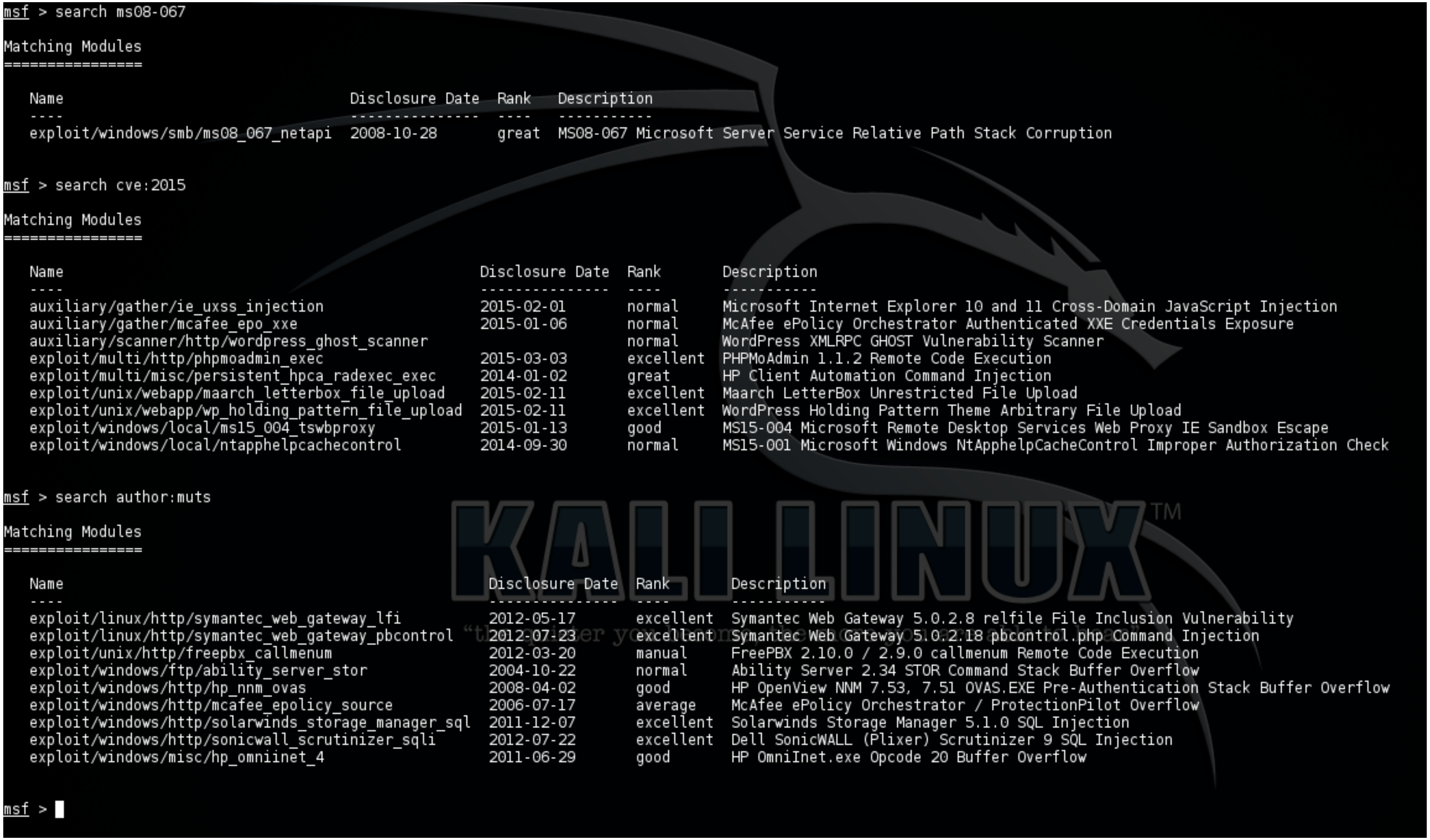
MSFConsole

- List of Commands that very often to use in core:
  - Search
  - Use
  - set/unset
  - show
  - info
  - route
  - quit/exit

MSFConsole

```
msf > search -h
Usage: search [keywords]

Keywords:
  app       :  Modules that are client or server attacks
  author    :  Modules written by this author
  bid       :  Modules with a matching Bugtraq ID
  cve       :  Modules with a matching CVE ID
  edb       :  Modules with a matching Exploit-DB ID
  name      :  Modules with a matching descriptive name
  osvdb     :  Modules with a matching OSVDB ID
  platform  :  Modules affecting this platform
  ref       :  Modules with a matching ref
  type      :  Modules of a specific type (exploit, auxiliary, or post)

Examples:
  search cve:2009 type:exploit app:client
```

MSFConsole



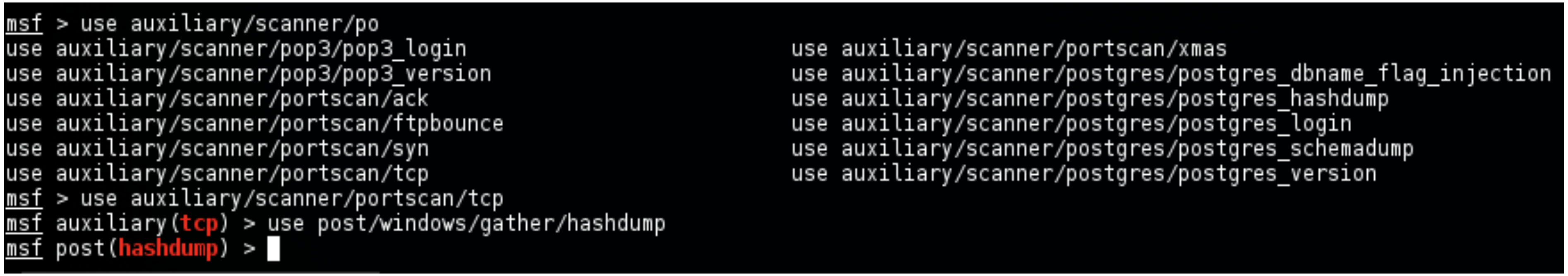
```
msf > search ms08-067

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

   Name                           Disclosure Date  Rank   Description
   ----                           ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  MS08-067 Microsoft Server Service Relative Path Stack Corruption


msf > search cve:2015

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

   Name                                         Disclosure Date  Rank       Description
   ----                                         ---------------  ----       -----------
   auxiliary/gather/ie_uxss_injection           2015-02-01       normal     Microsoft Internet Explorer 10 and 11 Cross-Domain JavaScript Injection
   auxiliary/gather/mcafee_epo_xxe              2015-01-06       normal     McAfee ePolicy Orchestrator Authenticated XXE Credentials Exposure
   auxiliary/scanner/http/wordpress_ghost_scanner                normal     WordPress XMLRPC GHOST Vulnerability Scanner
   exploit/multi/http/phpmoadmin_exec           2015-03-03       excellent  PHPMoAdmin 1.1.2 Remote Code Execution
   exploit/multi/misc/persistent_hpca_radexec_exec  2014-01-02   great      HP Client Automation Command Injection
   exploit/unix/webapp/maarch_letterbox_file_upload  2015-02-11  excellent  Maarch LetterBox Unrestricted File Upload
   exploit/unix/webapp/wp_holding_pattern_file_upload  2015-02-11  excellent  WordPress Holding Pattern Theme Arbitrary File Upload
   exploit/windows/local/ms15_004_tswbproxy     2015-01-13       good       MS15-004 Microsoft Remote Desktop Services Web Proxy IE Sandbox Escape
   exploit/windows/local/ntapphelpcachecontrol  2014-09-30       normal     MS15-001 Microsoft Windows NtApphelpCacheControl Improper Authorization Check


msf > search author:muts

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

   Name                                          Disclosure Date  Rank       Description
   ----                                          ---------------  ----       -----------
   exploit/linux/http/symantec_web_gateway_lfi   2012-05-17       excellent  Symantec Web Gateway 5.0.2.8 relfile File Inclusion Vulnerability
   exploit/linux/http/symantec_web_gateway_pbcontrol  2012-07-23  excellent  Symantec Web Gateway 5.0.2.18 pbcontrol.php Command Injection
   exploit/unix/http/freepbx_callmenum           2012-03-20       manual     FreePBX 2.10.0 / 2.9.0 callmenum Remote Code Execution
   exploit/windows/ftp/ability_server_stor       2004-10-22       normal     Ability Server 2.34 STOR Command Stack Buffer Overflow
   exploit/windows/http/hp_nnm_ovas              2008-04-02       good       HP OpenView NNM 7.53, 7.51 OVAS.EXE Pre-Authentication Stack Buffer Overflow
   exploit/windows/http/mcafee_epolicy_source    2006-07-17       average    McAfee ePolicy Orchestrator / ProtectionPilot Overflow
   exploit/windows/http/solarwinds_storage_manager_sql  2011-12-07  excellent  Solarwinds Storage Manager 5.1.0 SQL Injection
   exploit/windows/http/sonicwall_scrutinizer_sqli  2012-07-22    excellent  Dell SonicWALL (Plixer) Scrutinizer 9 SQL Injection
   exploit/windows/misc/hp_omniinet_4            2011-06-29       good       HP OmniInet.exe Opcode 20 Buffer Overflow


msf >
```

MSFConsole

```
msf > use
Usage: use module_name
```

The use command is used to interact with a module of a given name.

MSFConsole



```
msf > use auxiliary/scanner/po
use auxiliary/scanner/pop3/pop3_login                          use auxiliary/scanner/portscan/xmas
use auxiliary/scanner/pop3/pop3_version                        use auxiliary/scanner/postgres/postgres_dbname_flag_injection
use auxiliary/scanner/portscan/ack                             use auxiliary/scanner/postgres/postgres_hashdump
use auxiliary/scanner/portscan/ftpbounce                       use auxiliary/scanner/postgres/postgres_login
use auxiliary/scanner/portscan/syn                             use auxiliary/scanner/postgres/postgres_schemadump
use auxiliary/scanner/portscan/tcp                             use auxiliary/scanner/postgres/postgres_version
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > use post/windows/gather/hashdump
msf post(hashdump) > 
```

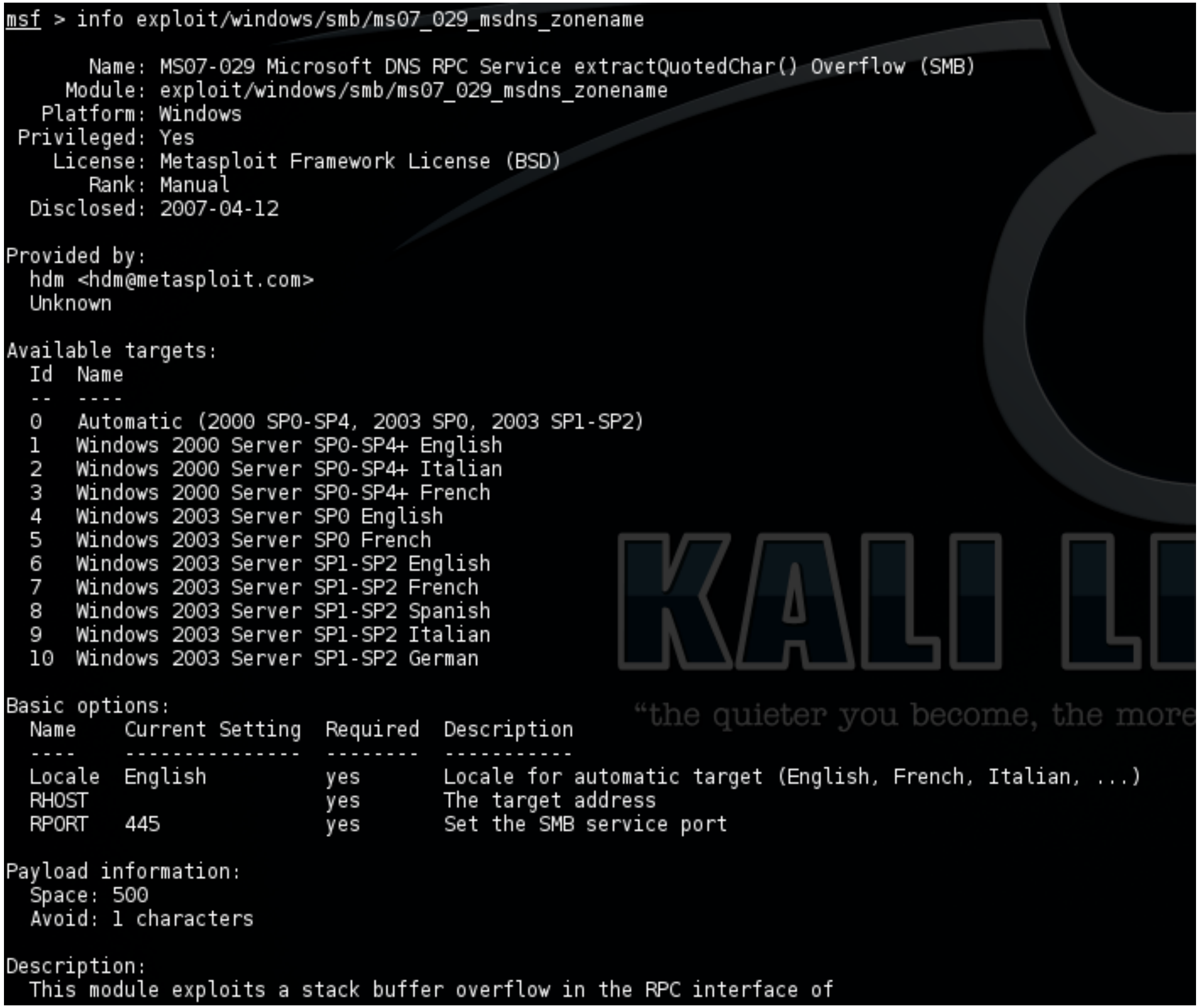
MSFConsole

```
msf > info
Usage: info <module name> [mod2 mod3 ...]
```

Queries the supplied module or modules for information. If no module is given,

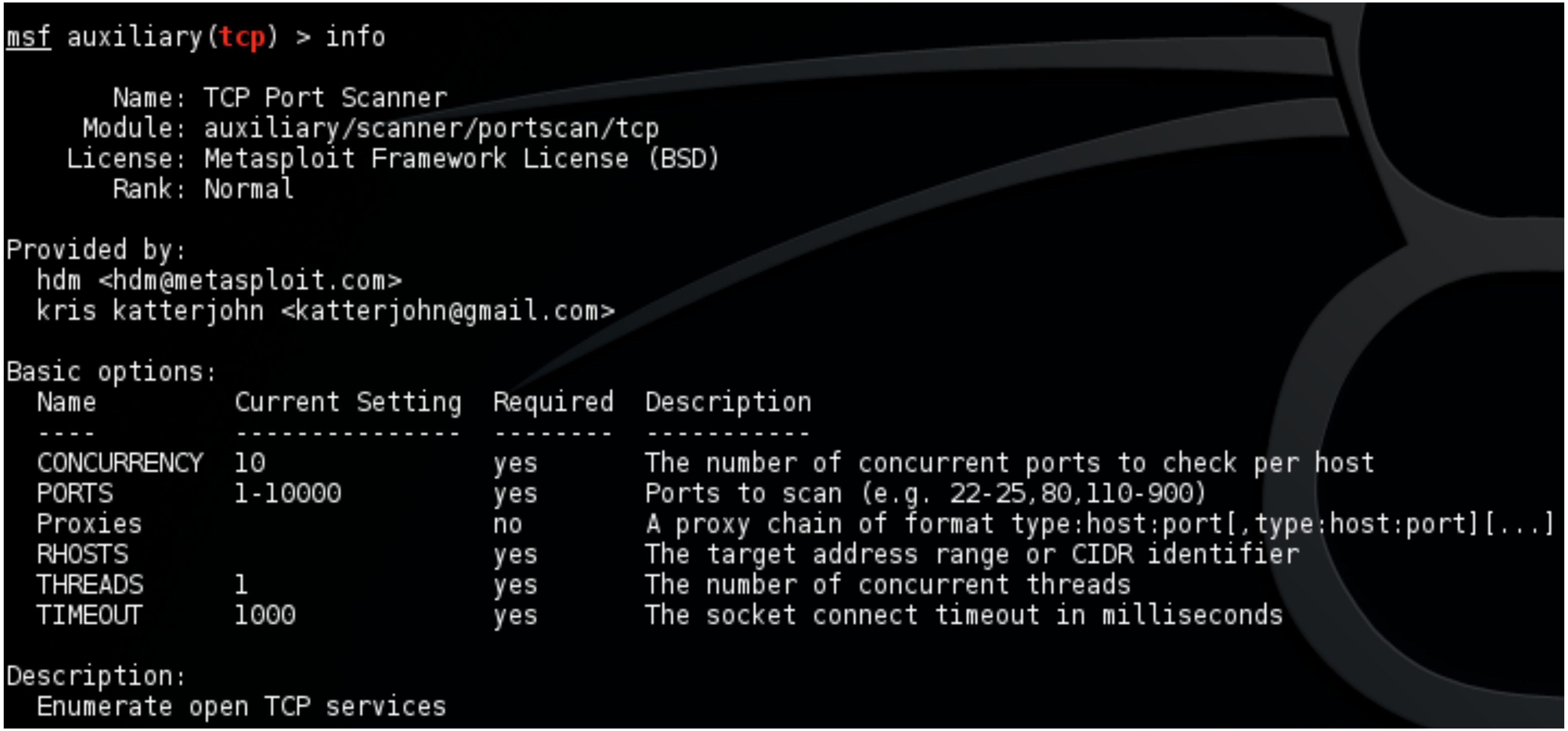
show info for the currently active module.

MSFConsole



```
msf > info exploit/windows/smb/ms07_029_msdns_zonename

       Name: MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
     Module: exploit/windows/smb/ms07_029_msdns_zonename
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2007-04-12

Provided by:
  hdm <hdm@metasploit.com>
  Unknown

Available targets:
  Id  Name
  --  ----
  0   Automatic (2000 SP0-SP4, 2003 SP0, 2003 SP1-SP2)
  1   Windows 2000 Server SP0-SP4+ English
  2   Windows 2000 Server SP0-SP4+ Italian
  3   Windows 2000 Server SP0-SP4+ French
  4   Windows 2003 Server SP0 English
  5   Windows 2003 Server SP0 French
  6   Windows 2003 Server SP1-SP2 English
  7   Windows 2003 Server SP1-SP2 French
  8   Windows 2003 Server SP1-SP2 Spanish
  9   Windows 2003 Server SP1-SP2 Italian
  10  Windows 2003 Server SP1-SP2 German

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  Locale  English          yes       Locale for automatic target (English, French, Italian, ...)
  RHOST                    yes       The target address
  RPORT   445              yes       Set the SMB service port

Payload information:
  Space: 500
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the RPC interface of
```

MSFConsole

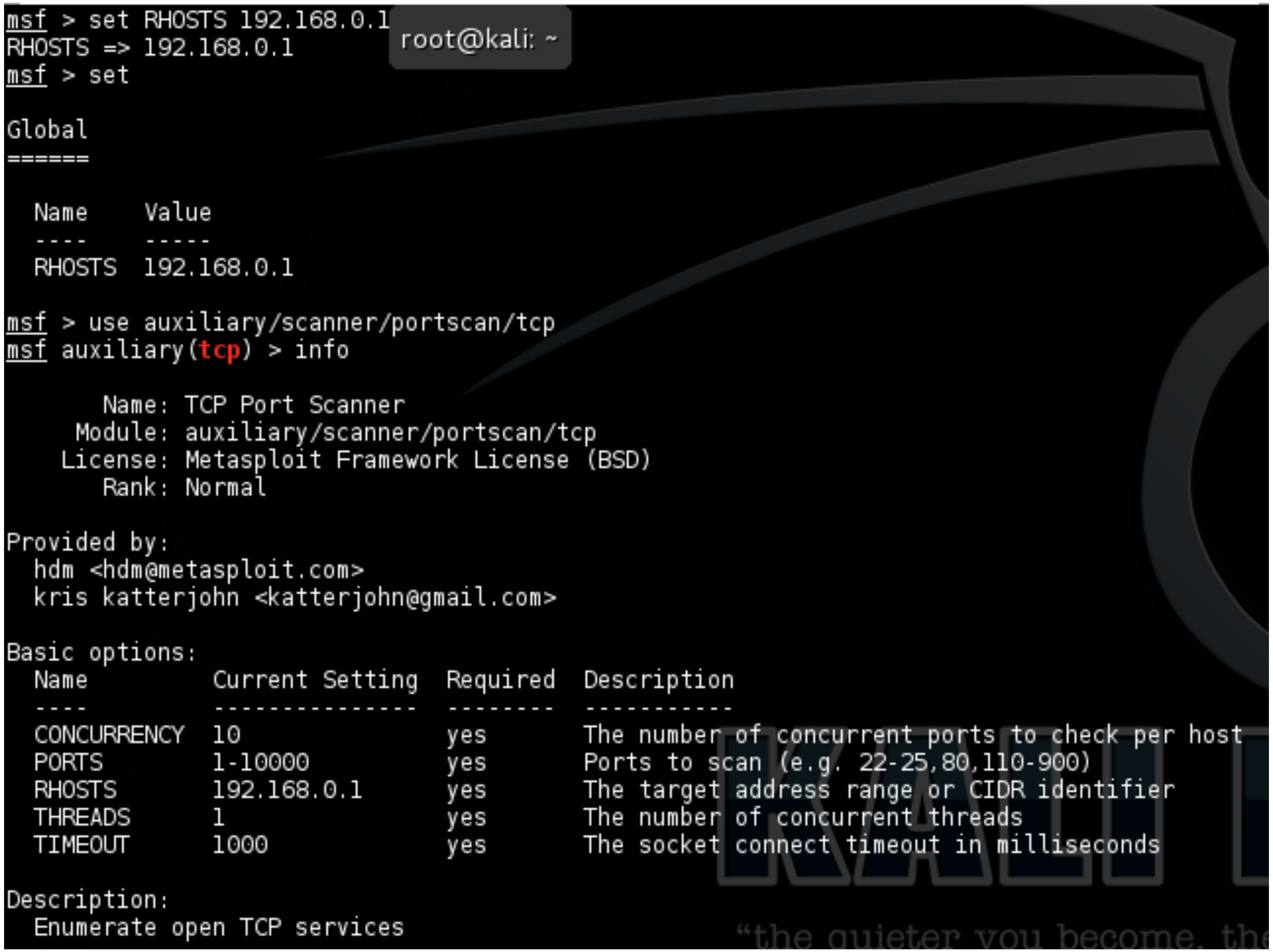


```
msf auxiliary(tcp) > info

       Name: TCP Port Scanner
     Module: auxiliary/scanner/portscan/tcp
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <hdm@metasploit.com>
  kris katterjohn <katterjohn@gmail.com>

Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  CONCURRENCY  10               yes       The number of concurrent ports to check per host
  PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
  Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                        yes       The target address range or CIDR identifier
  THREADS      1                yes       The number of concurrent threads
  TIMEOUT      1000             yes       The socket connect timeout in milliseconds

Description:
  Enumerate open TCP services
```

MSFConsole

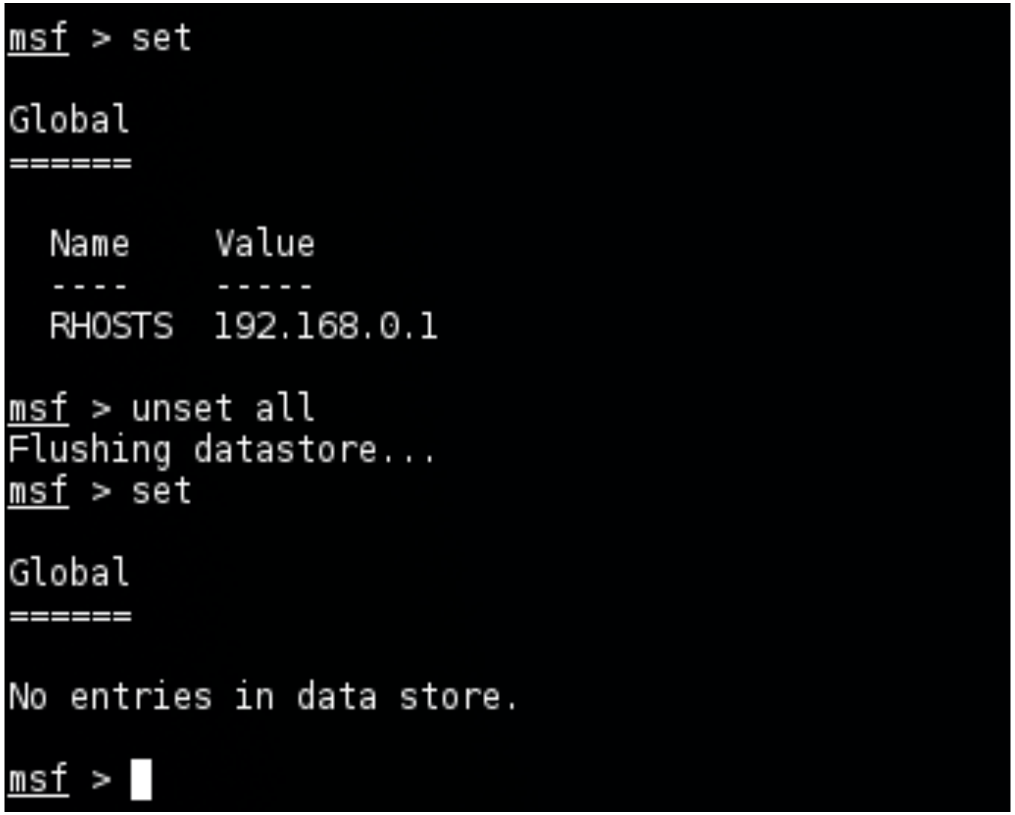
```
msf > set -h
[-] Unknown variable
Usage: set [option] [value]

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

msf > unset
Usage: unset [-g] var1 var2 var3 ...

The unset command is used to unset one or more variables.
To flush all entires, specify 'all' as the variable name.
With -g, operates on global datastore variables.
```

MSFConsole



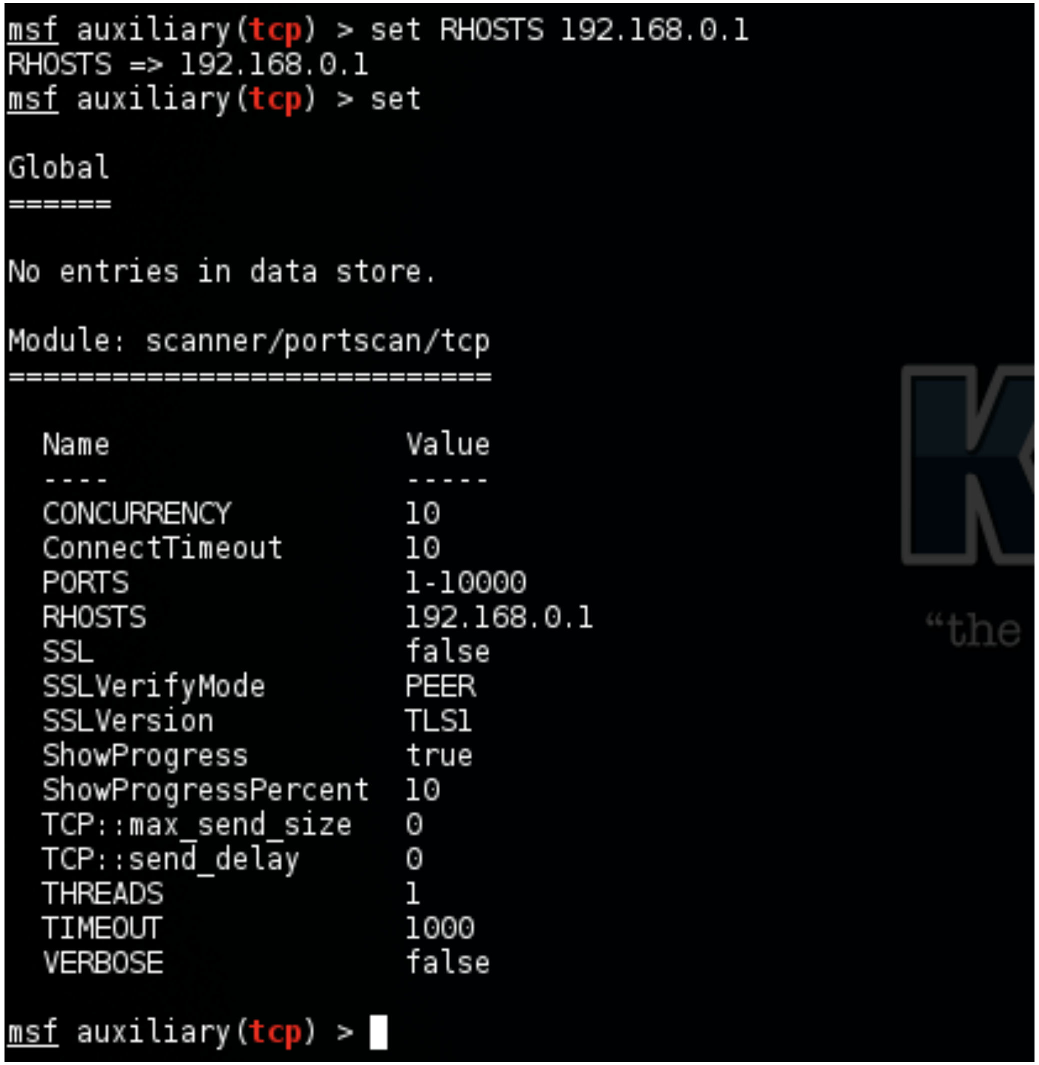
```
msf > set RHOSTS 192.168.0.1
RHOSTS => 192.168.0.1
msf > set

Global
======

  Name     Value
  ----     -----
  RHOSTS   192.168.0.1

msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > info

       Name: TCP Port Scanner
     Module: auxiliary/scanner/portscan/tcp
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <hdm@metasploit.com>
  kris katterjohn <katterjohn@gmail.com>

Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  CONCURRENCY  10               yes       The number of concurrent ports to check per host
  PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS       192.168.0.1      yes       The target address range or CIDR identifier
  THREADS      1                yes       The number of concurrent threads
  TIMEOUT      1000             yes       The socket connect timeout in milliseconds

Description:
  Enumerate open TCP services
```

MSFConsole



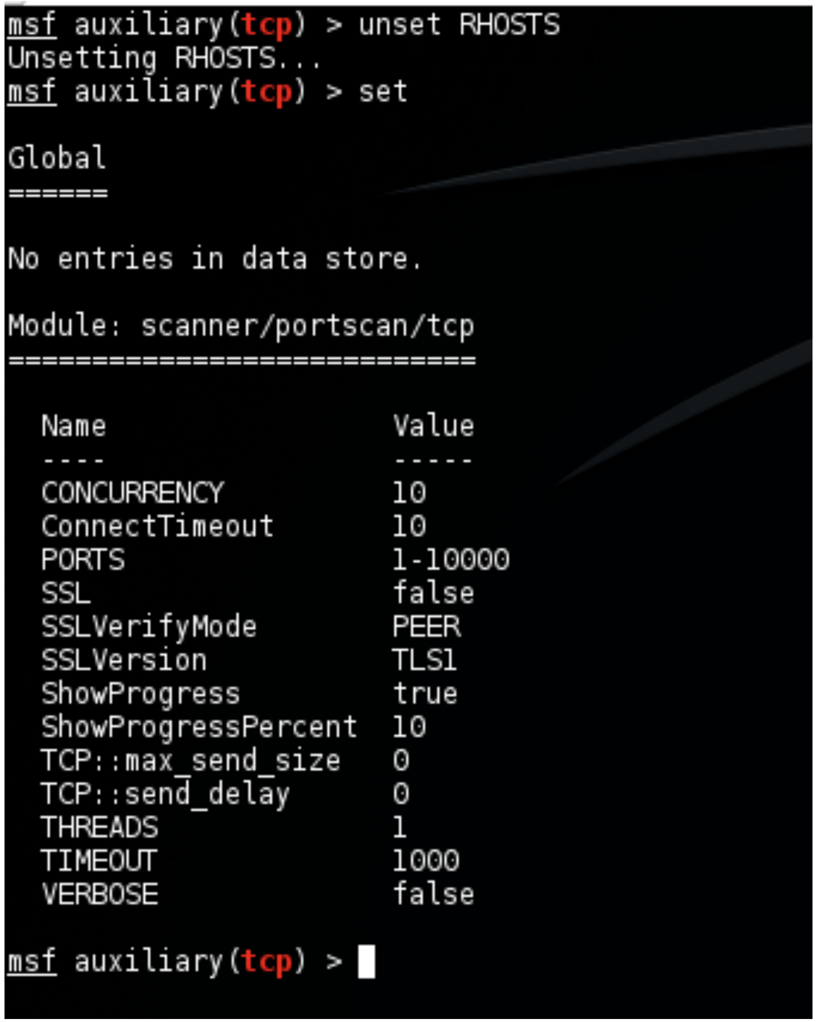
```
msf > set

Global
======

  Name    Value
  ----    -----
  RHOSTS  192.168.0.1

msf > unset all
Flushing datastore...
msf > set

Global
======

No entries in data store.

msf > 
```

MSFConsole



```
msf auxiliary(tcp) > set RHOSTS 192.168.0.1
RHOSTS => 192.168.0.1
msf auxiliary(tcp) > set

Global
======

No entries in data store.

Module: scanner/portscan/tcp
============================

  Name                   Value
  ----                   -----
  CONCURRENCY            10
  ConnectTimeout         10
  PORTS                  1-10000
  RHOSTS                 192.168.0.1
  SSL                    false
  SSLVerifyMode          PEER
  SSLVersion             TLS1
  ShowProgress           true
  ShowProgressPercent    10
  TCP::max_send_size     0
  TCP::send_delay        0
  THREADS                1
  TIMEOUT                1000
  VERBOSE                false

msf auxiliary(tcp) > 
```

MSFConsole

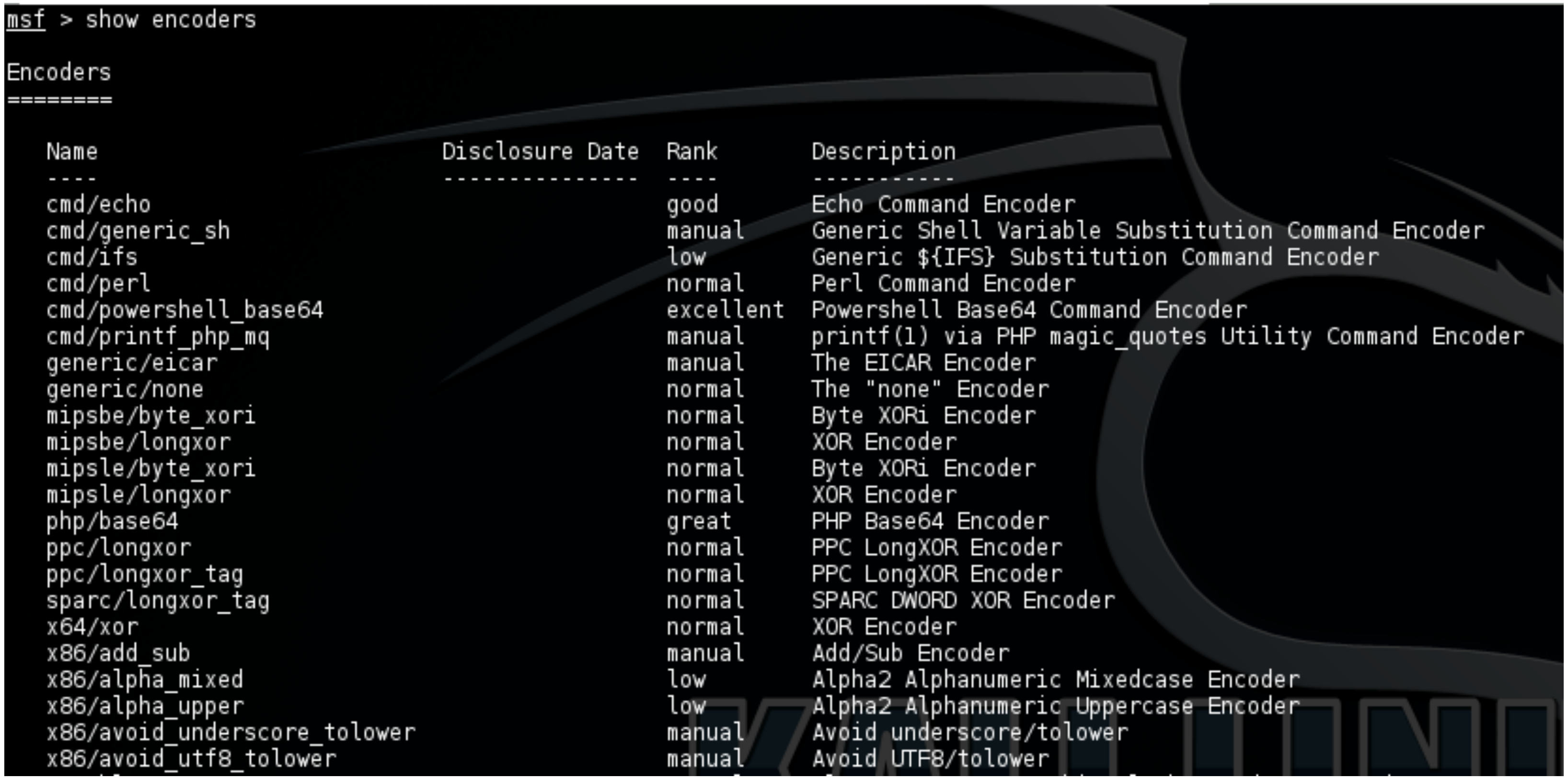


```
msf auxiliary(tcp) > unset RHOSTS
Unsetting RHOSTS...
msf auxiliary(tcp) > set

Global
======

No entries in data store.

Module: scanner/portscan/tcp
============================

  Name                   Value
  ----                   -----
  CONCURRENCY            10
  ConnectTimeout         10
  PORTS                  1-10000
  SSL                    false
  SSLVerifyMode          PEER
  SSLVersion             TLS1
  ShowProgress           true
  ShowProgressPercent    10
  TCP::max_send_size     0
  TCP::send_delay        0
  THREADS                1
  TIMEOUT                1000
  VERBOSE                false

msf auxiliary(tcp) > 
```

MSFConsole

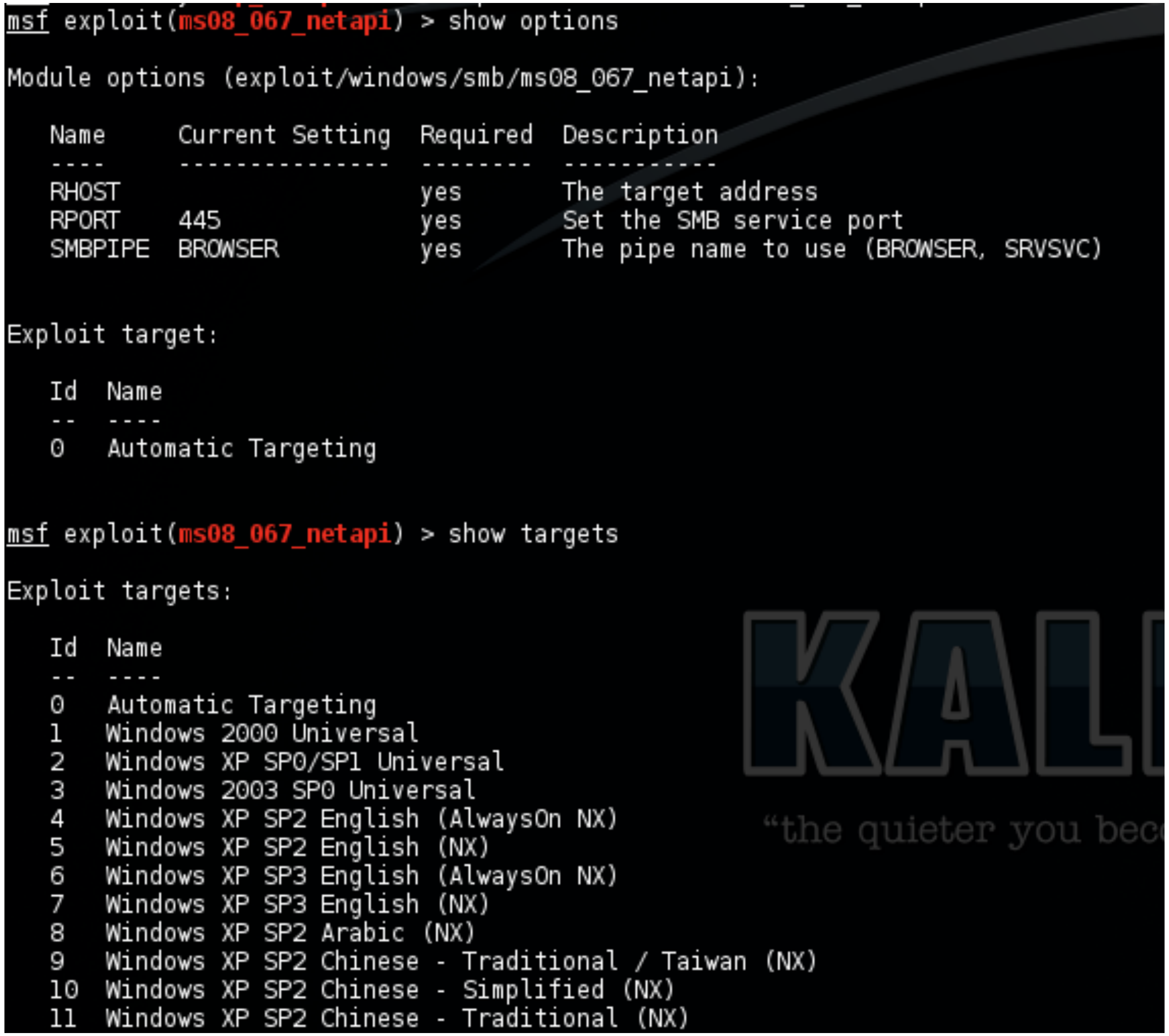
```
msf > show -h
[*] Valid parameters for the "show" command
are: all, encoders, nops, exploits, payloads,
auxiliary, plugins, options
[*] Additional module-specific parameters are:
missing, advanced, evasion, targets, actions
```

MSFConsole



```
msf > show encoders

Encoders
========

   Name                          Disclosure Date  Rank       Description
   ----                          ---------------  ----       -----------
   cmd/echo                                       good       Echo Command Encoder
   cmd/generic_sh                                 manual     Generic Shell Variable Substitution Command Encoder
   cmd/ifs                                        low        Generic ${IFS} Substitution Command Encoder
   cmd/perl                                       normal     Perl Command Encoder
   cmd/powershell_base64                          excellent  Powershell Base64 Command Encoder
   cmd/printf_php_mq                              manual     printf(1) via PHP magic_quotes Utility Command Encoder
   generic/eicar                                  manual     The EICAR Encoder
   generic/none                                   normal     The "none" Encoder
   mipsbe/byte_xori                               normal     Byte XORi Encoder
   mipsbe/longxor                                 normal     XOR Encoder
   mipsle/byte_xori                               normal     Byte XORi Encoder
   mipsle/longxor                                 normal     XOR Encoder
   php/base64                                     great      PHP Base64 Encoder
   ppc/longxor                                    normal     PPC LongXOR Encoder
   ppc/longxor_tag                                normal     PPC LongXOR Encoder
   sparc/longxor_tag                              normal     SPARC DWORD XOR Encoder
   x64/xor                                        normal     XOR Encoder
   x86/add_sub                                    manual     Add/Sub Encoder
   x86/alpha_mixed                                low        Alpha2 Alphanumeric Mixedcase Encoder
   x86/alpha_upper                                low        Alpha2 Alphanumeric Uppercase Encoder
   x86/avoid_underscore_tolower                   manual     Avoid underscore/tolower
   x86/avoid_utf8_tolower                         manual     Avoid UTF8/tolower
```

MSFConsole

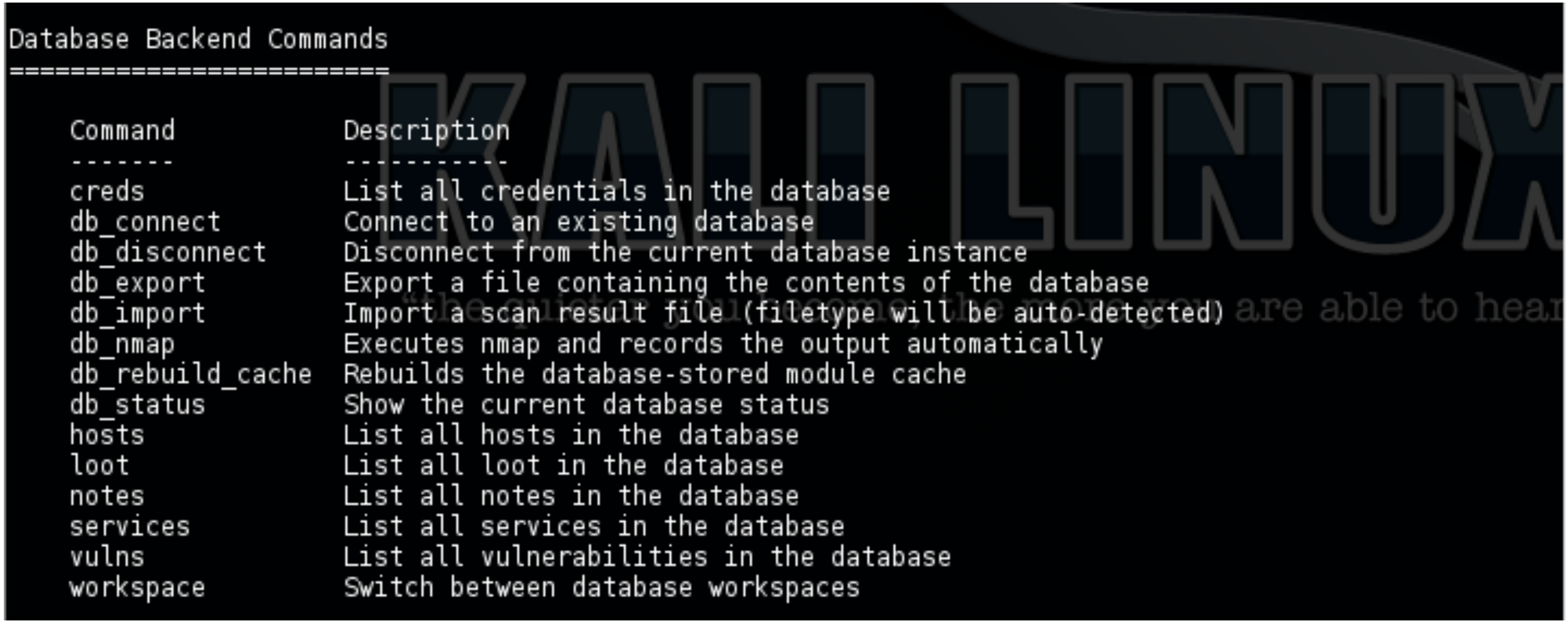


```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows 2003 SP0 Universal
   4   Windows XP SP2 English (AlwaysOn NX)
   5   Windows XP SP2 English (NX)
   6   Windows XP SP3 English (AlwaysOn NX)
   7   Windows XP SP3 English (NX)
   8   Windows XP SP2 Arabic (NX)
   9   Windows XP SP2 Chinese - Traditional / Taiwan (NX)
   10  Windows XP SP2 Chinese - Simplified (NX)
   11  Windows XP SP2 Chinese - Traditional (NX)
```

Database Commands

MSFCONSOLE

MSFConsole: Database



```
Database Backend Commands
=========================

    Command           Description
    -------           -----------
    creds             List all credentials in the database
    db_connect        Connect to an existing database
    db_disconnect     Disconnect from the current database instance
    db_export         Export a file containing the contents of the database
    db_import         Import a scan result file (filetype will be auto-detected)
    db_nmap           Executes nmap and records the output automatically
    db_rebuild_cache  Rebuilds the database-stored module cache
    db_status         Show the current database status
    hosts             List all hosts in the database
    loot              List all loot in the database
    notes             List all notes in the database
    services          List all services in the database
    vulns             List all vulnerabilities in the database
    workspace         Switch between database workspaces
```

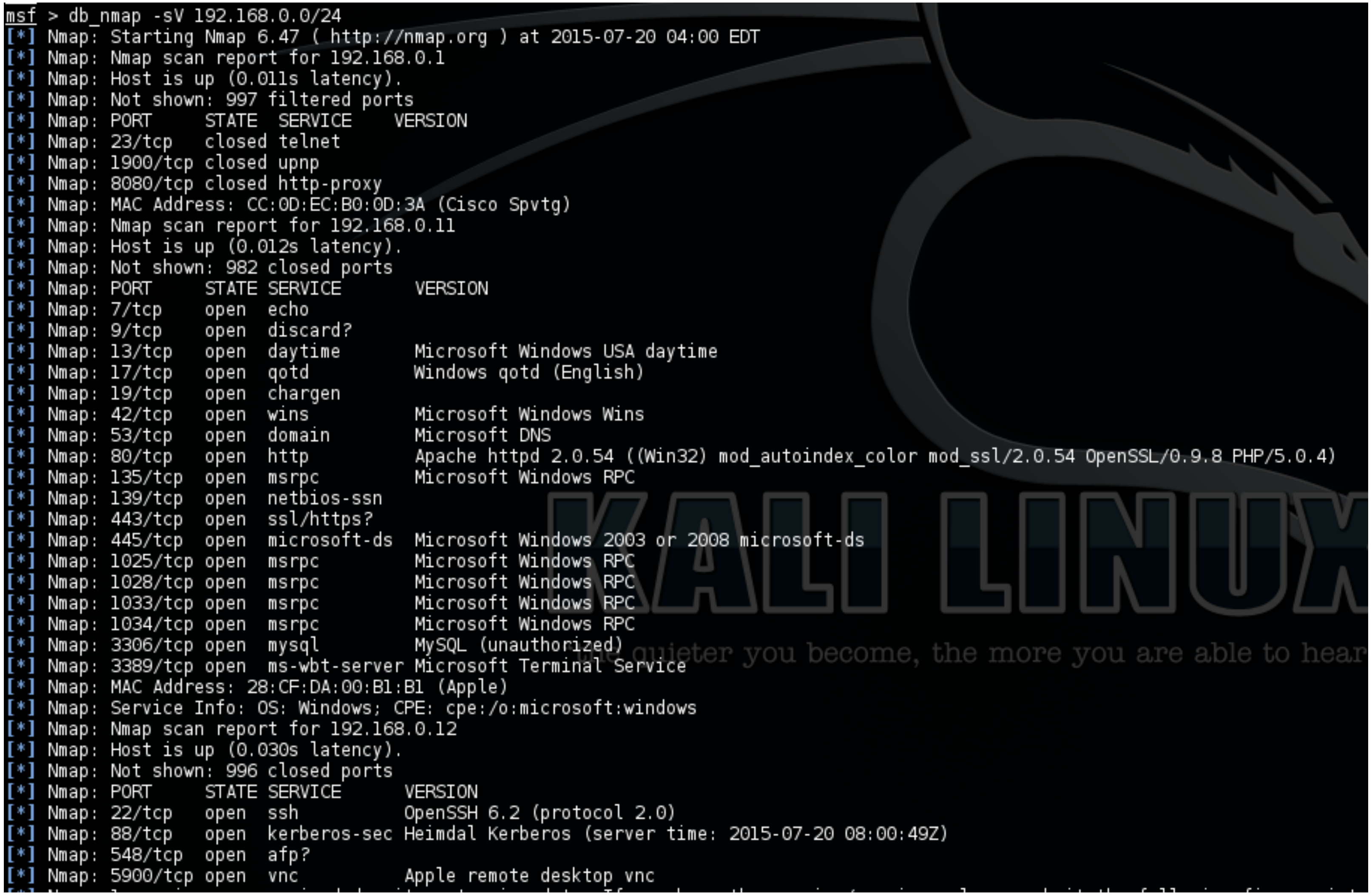
MSFConsole

- List of Databases Commands that very often to use:
  - db_nmap
  - hosts
  - services

Database: db_nmap

```
msf > db_nmap --help
[*] Nmap: Nmap 6.47 ( http://nmap.org )
[*] Nmap: Usage: nmap [Scan Type(s)] [Options] {target specification}
[*] Nmap: TARGET SPECIFICATION:
[*] Nmap: Can pass hostnames, IP addresses, networks, etc.
[*] Nmap: Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
[*] Nmap: -iL <inputfilename>: Input from list of hosts/networks
[*] Nmap: -iR <num hosts>: Choose random targets
[*] Nmap: --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
[*] Nmap: --excludefile <exclude_file>: Exclude list from file
[*] Nmap: HOST DISCOVERY:
[*] Nmap: -sL: List Scan - simply list targets to scan
[*] Nmap: -sn: Ping Scan - disable port scan
[*] Nmap: -Pn: Treat all hosts as online -- skip host discovery
[*] Nmap: -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
… truncated….
```

Database: db_nmap

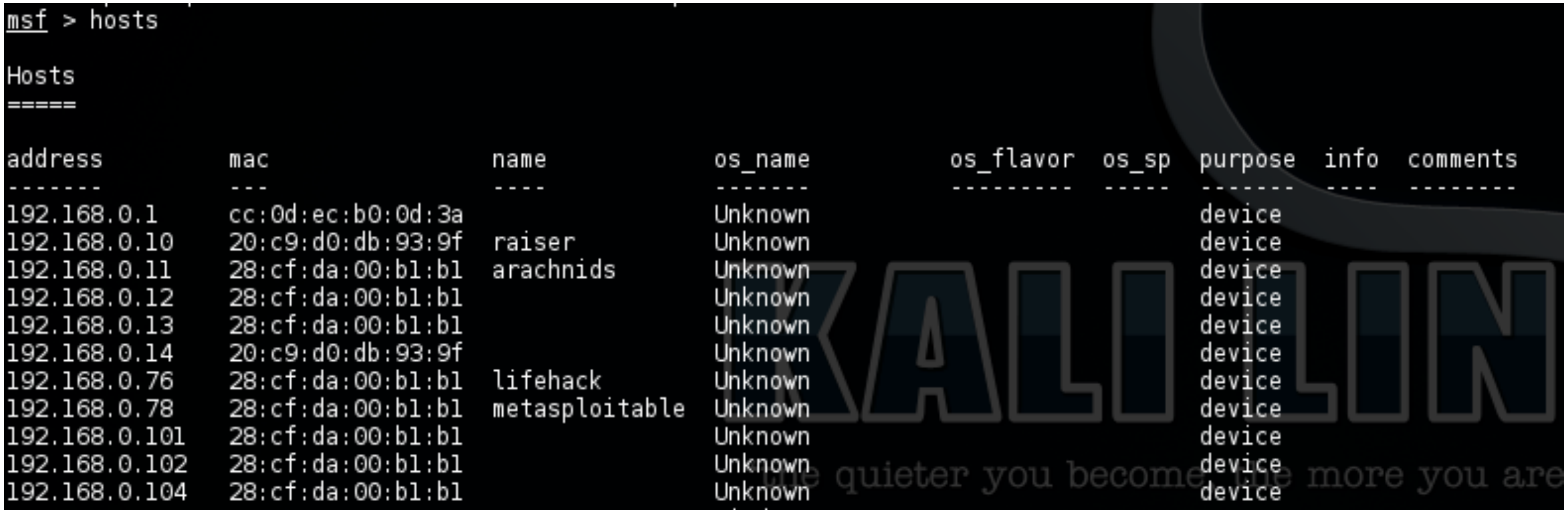


```
msf > db_nmap -sV 192.168.0.0/24
[*] Nmap: Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-20 04:00 EDT
[*] Nmap: Nmap scan report for 192.168.0.1
[*] Nmap: Host is up (0.011s latency).
[*] Nmap: Not shown: 997 filtered ports
[*] Nmap: PORT     STATE  SERVICE    VERSION
[*] Nmap: 23/tcp   closed telnet
[*] Nmap: 1900/tcp closed upnp
[*] Nmap: 8080/tcp closed http-proxy
[*] Nmap: MAC Address: CC:0D:EC:B0:0D:3A (Cisco Spvtg)
[*] Nmap: Nmap scan report for 192.168.0.11
[*] Nmap: Host is up (0.012s latency).
[*] Nmap: Not shown: 982 closed ports
[*] Nmap: PORT     STATE SERVICE       VERSION
[*] Nmap: 7/tcp    open  echo
[*] Nmap: 9/tcp    open  discard?
[*] Nmap: 13/tcp   open  daytime       Microsoft Windows USA daytime
[*] Nmap: 17/tcp   open  qotd          Windows qotd (English)
[*] Nmap: 19/tcp   open  chargen
[*] Nmap: 42/tcp   open  wins          Microsoft Windows Wins
[*] Nmap: 53/tcp   open  domain        Microsoft DNS
[*] Nmap: 80/tcp   open  http          Apache httpd 2.0.54 ((Win32) mod_autoindex_color mod_ssl/2.0.54 OpenSSL/0.9.8 PHP/5.0.4)
[*] Nmap: 135/tcp  open  msrpc         Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 443/tcp  open  ssl/https?
[*] Nmap: 445/tcp  open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
[*] Nmap: 1025/tcp open  msrpc         Microsoft Windows RPC
[*] Nmap: 1028/tcp open  msrpc         Microsoft Windows RPC
[*] Nmap: 1033/tcp open  msrpc         Microsoft Windows RPC
[*] Nmap: 1034/tcp open  msrpc         Microsoft Windows RPC
[*] Nmap: 3306/tcp open  mysql         MySQL (unauthorized)
[*] Nmap: 3389/tcp open  ms-wbt-server Microsoft Terminal Service
[*] Nmap: MAC Address: 28:CF:DA:00:B1:B1 (Apple)
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Nmap scan report for 192.168.0.12
[*] Nmap: Host is up (0.030s latency).
[*] Nmap: Not shown: 996 closed ports
[*] Nmap: PORT     STATE SERVICE      VERSION
[*] Nmap: 22/tcp   open  ssh          OpenSSH 6.2 (protocol 2.0)
[*] Nmap: 88/tcp   open  kerberos-sec Heimdal Kerberos (server time: 2015-07-20 08:00:49Z)
[*] Nmap: 548/tcp  open  afp?
[*] Nmap: 5900/tcp open  vnc          Apple remote desktop vnc
```

Database: Hosts

```
msf > hosts --help
Usage: hosts [ options ] [addr1 addr2 ...]

OPTIONS:
  -a,--add          Add the hosts instead of searching
  -d,--delete       Delete the hosts instead of searching
  -c <col1,col2>    Only show the given columns (see list below)
  -h,--help         Show this help information
  -u,--up           Only show hosts which are up
  -o <file>         Send output to a file in csv format
  -R,--rhosts       Set RHOSTS from the results of the search
  -S,--search       Search string to filter by

Available columns: address, arch, comm, comments, created_at, cred_count, detected_arch,
exploit_attempt_count, host_detail_count, info, mac, name, note_count, os_flavor, os_lang,
os_name, os_sp, purpose, scope, service_count, state, updated_at, virtual_host, vuln_count
```

Database: Hosts

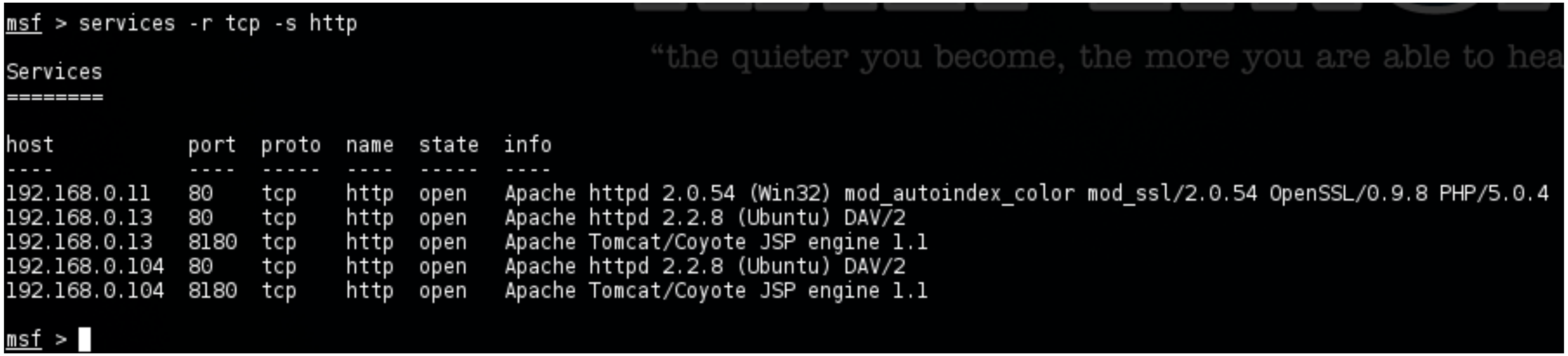


```
msf > hosts

Hosts
=====

address         mac                name            os_name          os_flavor  os_sp  purpose  info  comments
-------         ---                ----            -------          ---------  -----  -------  ----  --------
192.168.0.1     cc:0d:ec:b0:0d:3a                  Unknown                            device
192.168.0.10    20:c9:d0:db:93:9f  raiser          Unknown                            device
192.168.0.11    28:cf:da:00:b1:b1  arachnids       Unknown                            device
192.168.0.12    28:cf:da:00:b1:b1                  Unknown                            device
192.168.0.13    28:cf:da:00:b1:b1                  Unknown                            device
192.168.0.14    20:c9:d0:db:93:9f                  Unknown                            device
192.168.0.76    28:cf:da:00:b1:b1  lifehack        Unknown                            device
192.168.0.78    28:cf:da:00:b1:b1  metasploitable  Unknown                            device
192.168.0.101   28:cf:da:00:b1:b1                  Unknown                            device
192.168.0.102   28:cf:da:00:b1:b1                  Unknown                            device
192.168.0.104   28:cf:da:00:b1:b1                  Unknown                            device
```

Database: Services

```
msf > services --help

Usage: services [-h] [-u] [-a] [-r <proto>] [-p <port1,port2>] [-s <name1,name2>] [-o <filename>] [addr1
addr2 ...]

  -a,--add          Add the services instead of searching
  -d,--delete       Delete the services instead of searching
  -c <col1,col2>    Only show the given columns
  -h,--help         Show this help information
  -s <name1,name2>  Search for a list of service names
  -p <port1,port2>  Search for a list of ports
  -r <protocol>     Only show [tcp|udp] services
  -u,--up           Only show services which are up
  -o <file>         Send output to a file in csv format
  -R,--rhosts       Set RHOSTS from the results of the search
  -S,--search       Search string to filter by

Available columns: created_at, info, name, port, proto, state, updated_at
```

Database: Services

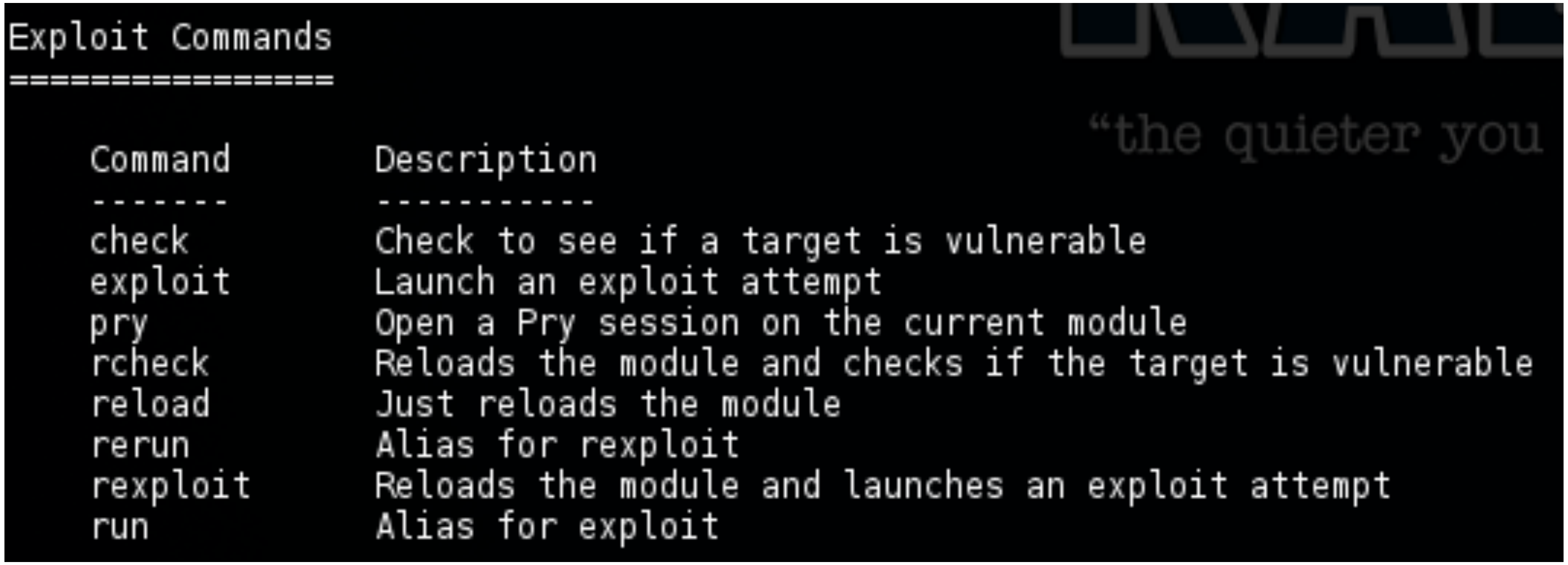


```
msf > services -r tcp -s http

Services
========

host           port  proto  name  state  info
----           ----  -----  ----  -----  ----
192.168.0.11   80    tcp    http  open   Apache httpd 2.0.54 (Win32) mod_autoindex_color mod_ssl/2.0.54 OpenSSL/0.9.8 PHP/5.0.4
192.168.0.13   80    tcp    http  open   Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.0.13   8180  tcp    http  open   Apache Tomcat/Coyote JSP engine 1.1
192.168.0.104  80    tcp    http  open   Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.0.104  8180  tcp    http  open   Apache Tomcat/Coyote JSP engine 1.1

msf >
```

Exploit Commands

MSFCONSOLE

MSFConsole: Exploit



```
Exploit Commands
================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       Launch an exploit attempt
    pry           Open a Pry session on the current module
    rcheck        Reloads the module and checks if the target is vulnerable
    reload        Just reloads the module
    rerun         Alias for rexploit
    rexploit      Reloads the module and launches an exploit attempt
    run           Alias for exploit
```

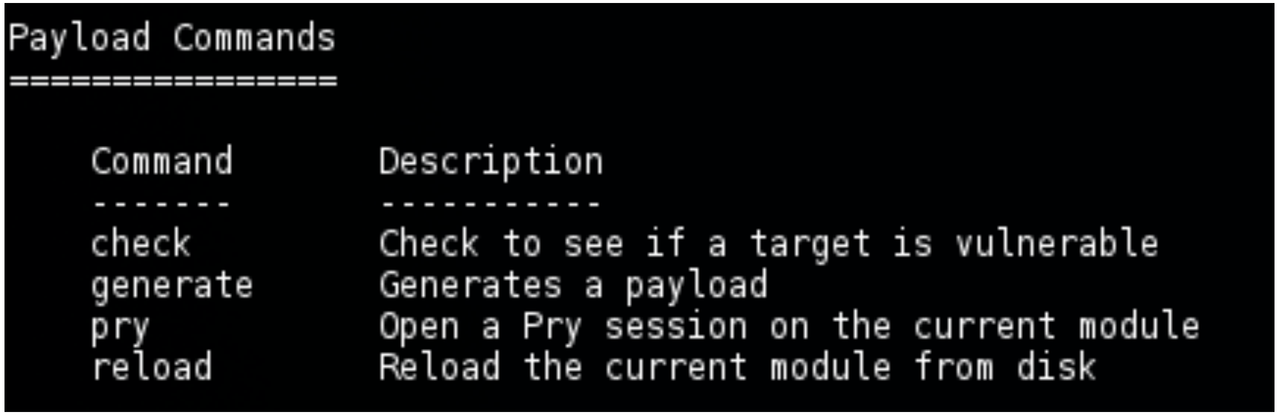
MSFConsole

- List of Commands that very often to use in modules:
  - exploit
  - check
  - run

Payloads Commands

MSFCONSOLE

MSFConsole: Payload

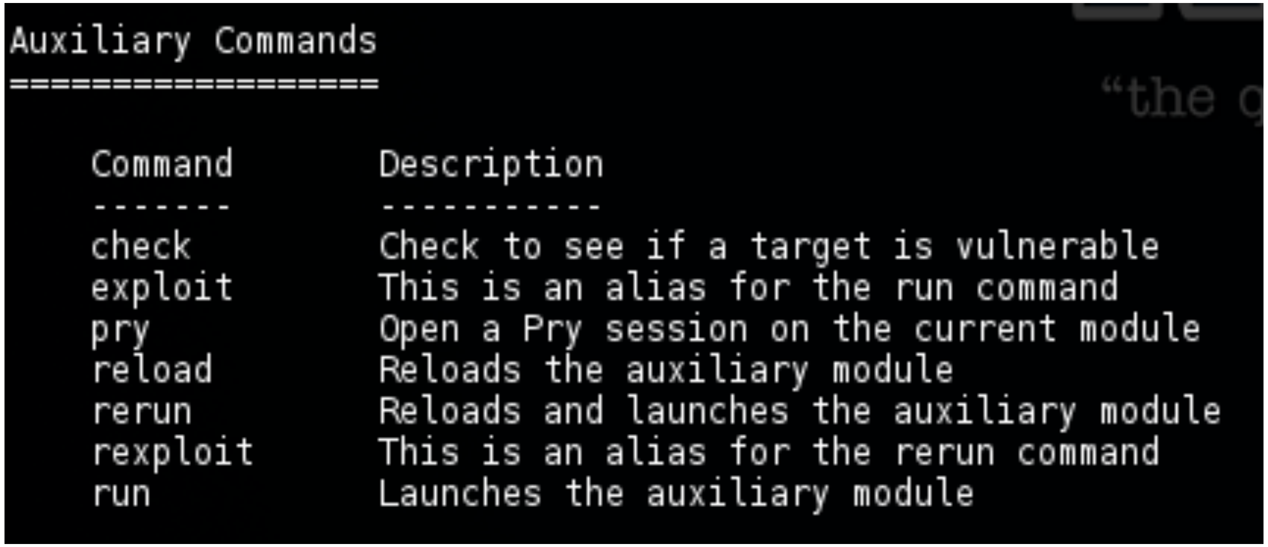


```
Payload Commands
================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    generate      Generates a payload
    pry           Open a Pry session on the current module
    reload        Reload the current module from disk
```

Auxiliary Commands

MSFCONSOLE

MSFConsole: Auxiliary

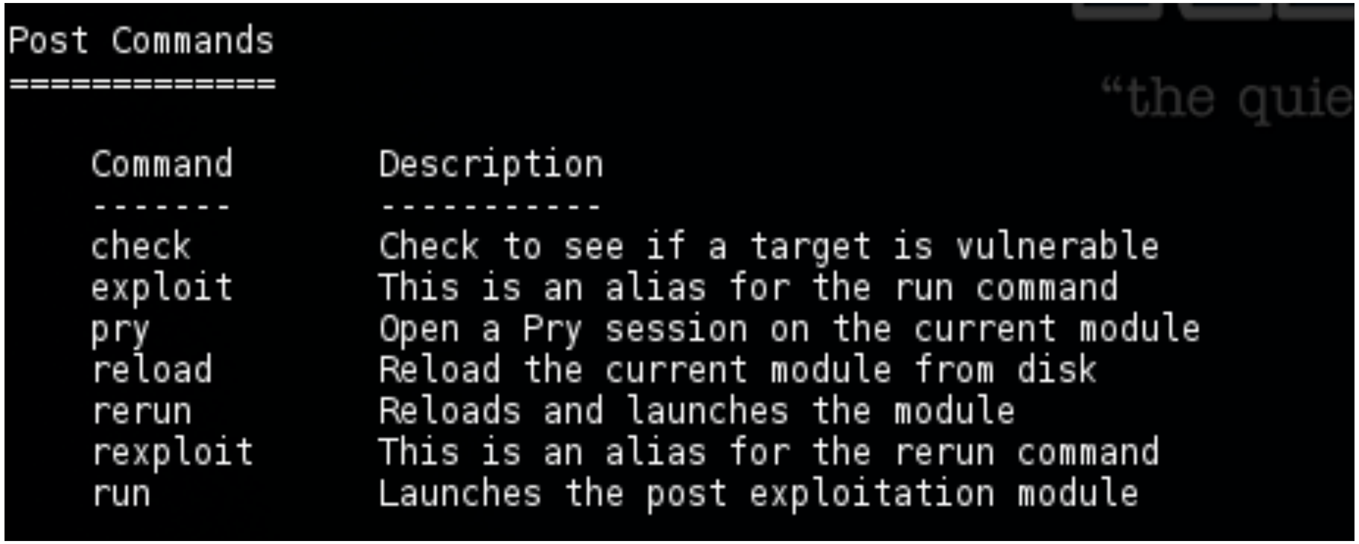


```
Auxiliary Commands
==================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       This is an alias for the run command
    pry           Open a Pry session on the current module
    reload        Reloads the auxiliary module
    rerun         Reloads and launches the auxiliary module
    rexploit      This is an alias for the rerun command
    run           Launches the auxiliary module
```

Post Exploitation Commands

MSFCONSOLE

MSFConsole: Post



```
Post Commands
=============

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       This is an alias for the run command
    pry           Open a Pry session on the current module
    reload        Reload the current module from disk
    rerun         Reloads and launches the module
    rexploit      This is an alias for the rerun command
    run           Launches the post exploitation module
```

Questions?

MSFConsole