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' .

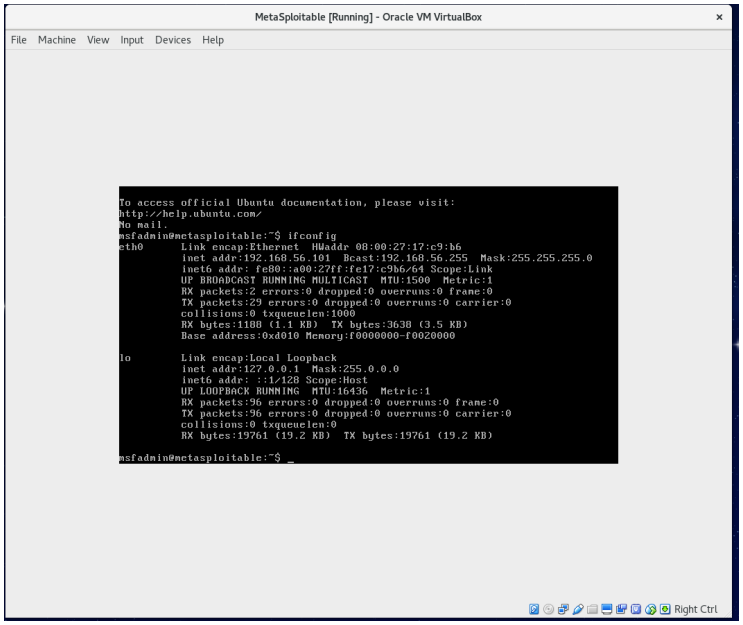
Solution:

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



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 in msf console.
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:

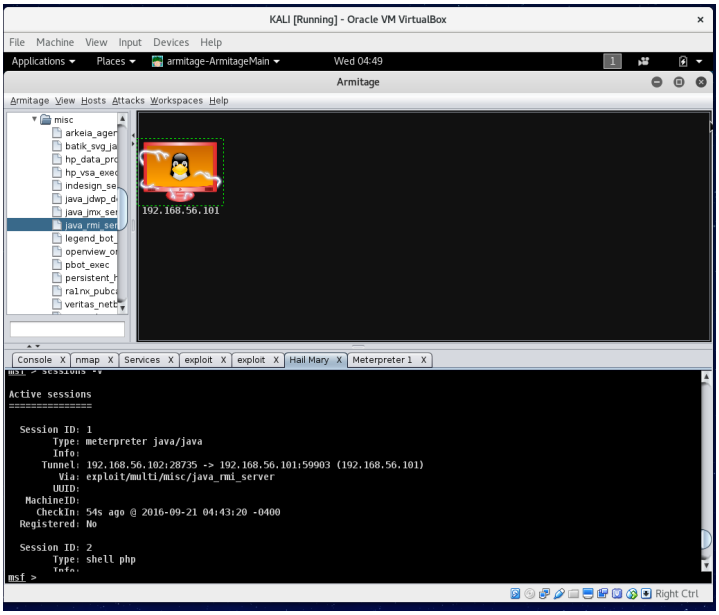
(1) exploit/multi/misc/java_rmi_server
(2) exploit/multi/http/php_cgi_org_injection
(3) exploit/linux/postgres/postgres_payload
(4) exploit/unix/irc/unreal_ircd_3281_backdoor

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

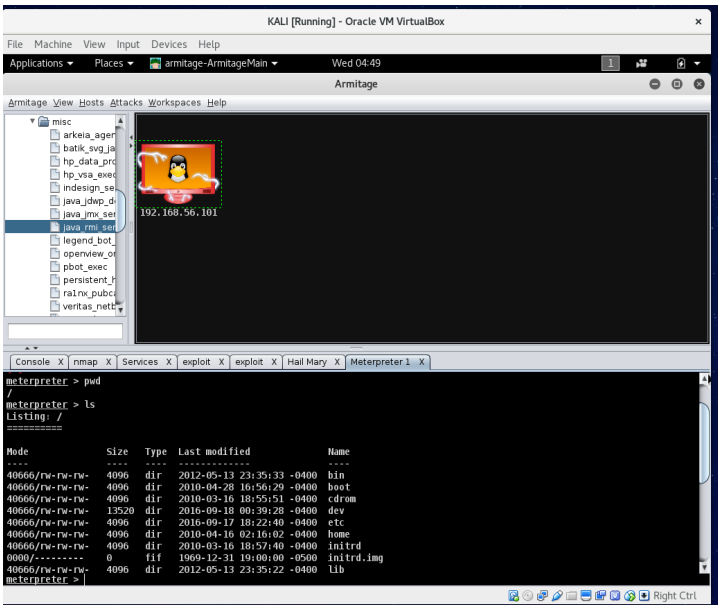
Step 6: After launching flood of exploits we will have sessions opened for each vulnerability and we can interact with the target host using shell once the exploitation is successful.

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



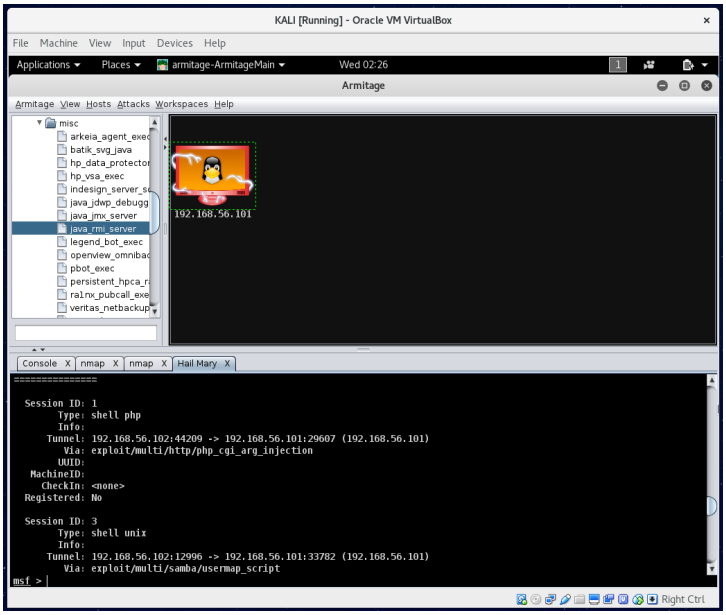
we can open the shell 1 by right click on the host icon and start interacting with the target machine:

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 as shown in screenshots below:

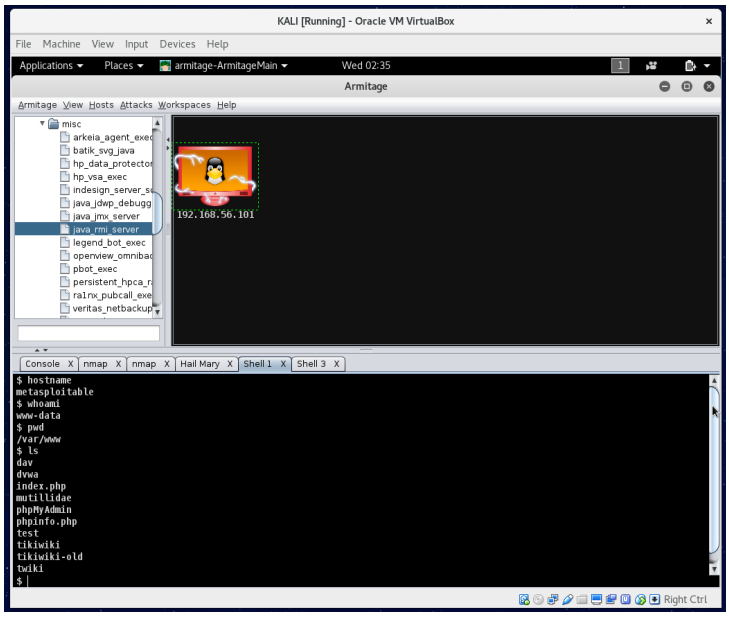


same is done for all the exploits as shown below:

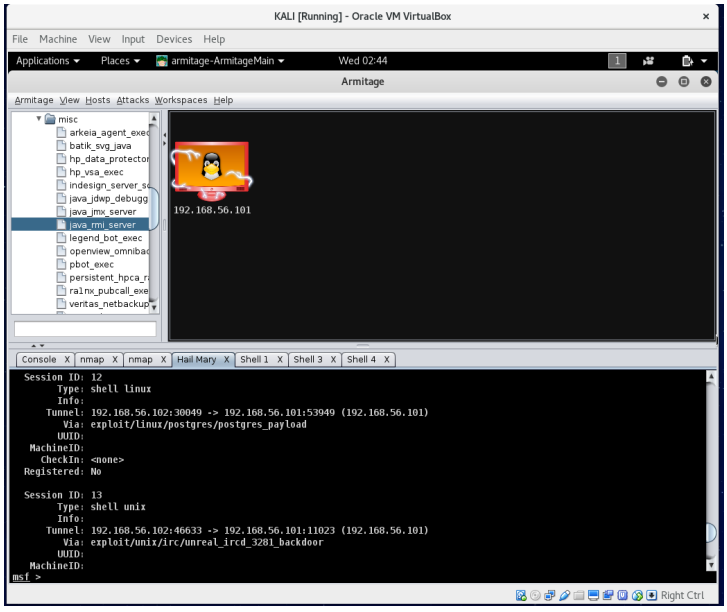
(2) second vulnerability is exploit/multi/http/php_cgi_org_injection .The screenshot of launching exploit is



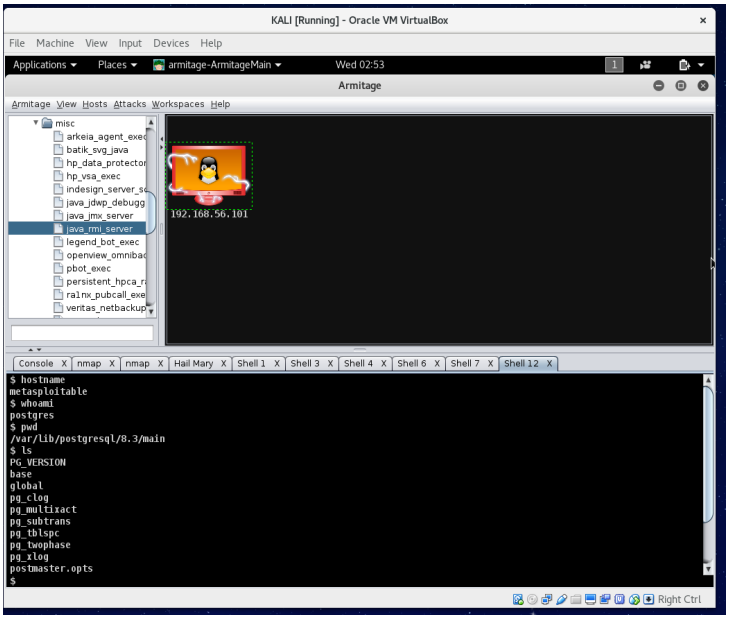
The shell for interacting with target machine is :



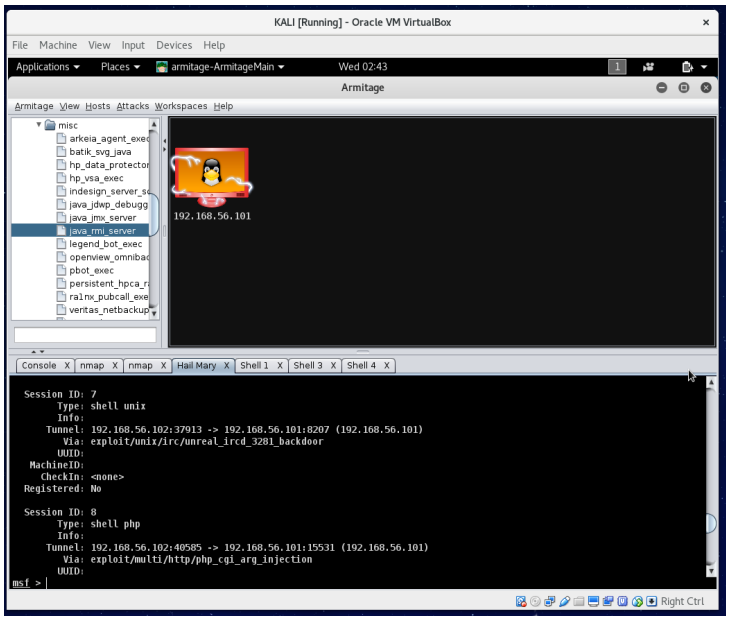
(3) third vulnerability is exploit/linux/postgres/postgres_payload .The screenshot of launching exploit is:



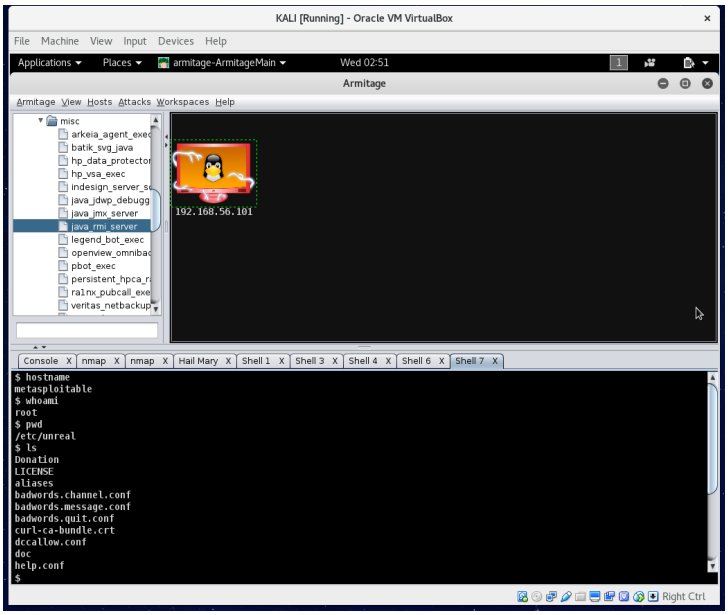
The shell for interacting with target machine is :



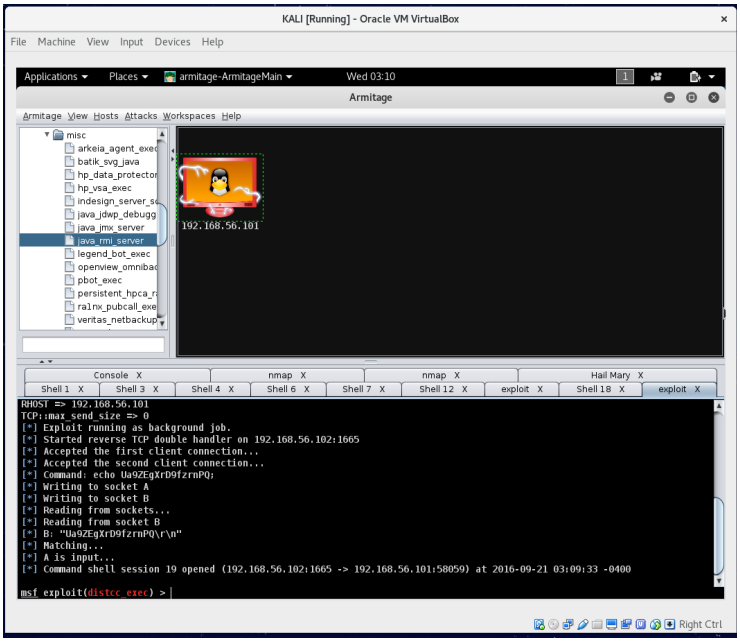
(4) fourth vulnerability is exploit/unix/irc/unreal_ircd_3281_backdoor. The screenshot of launching exploit is:



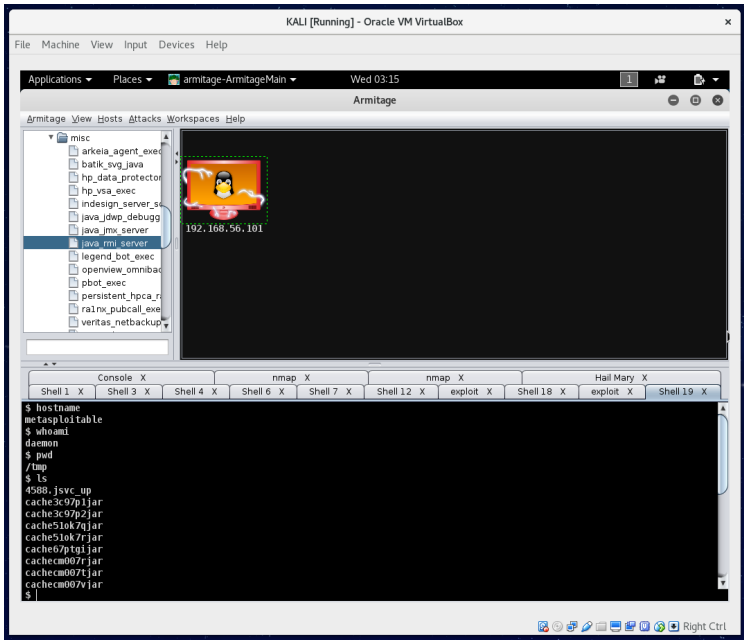
The shell for interacting with target machine is :



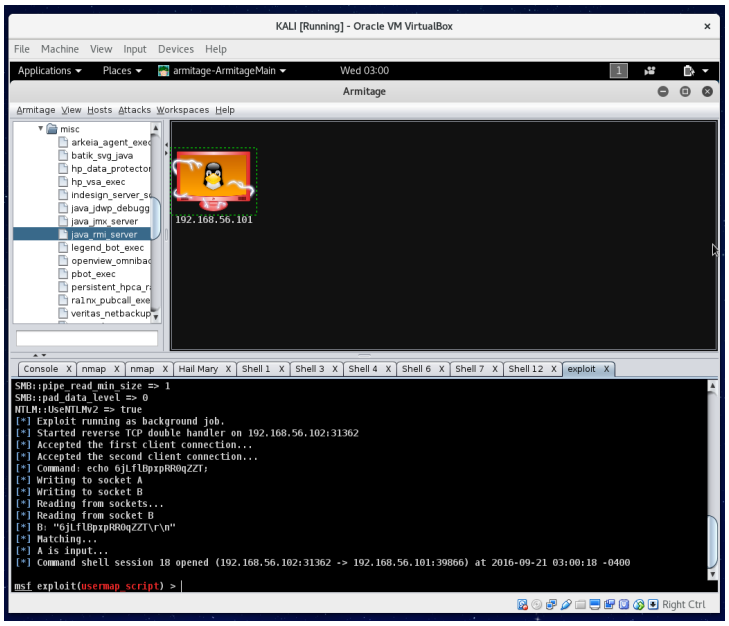
(5) fifth vulnerability is exploit/unix/misc/distcc_exec . The screenshot of launching exploit is:



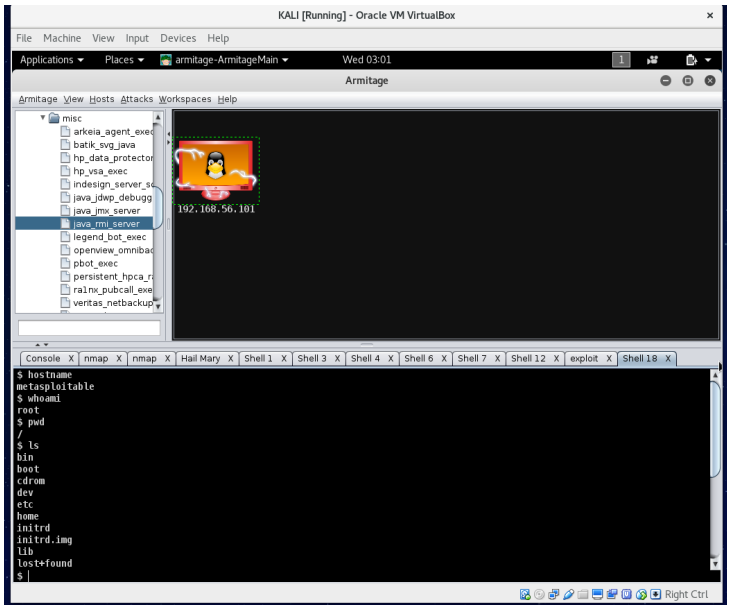
The shell for interacting with target machine is :



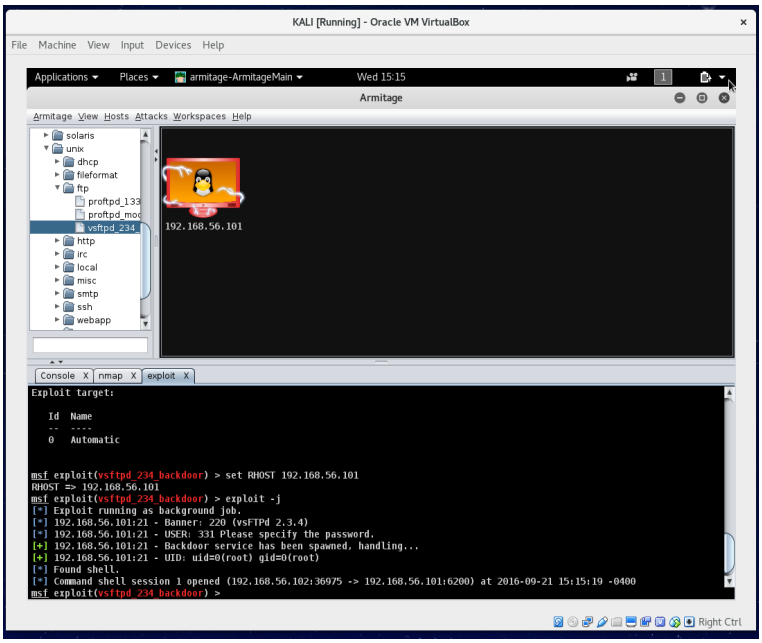
(6)sixth vulnerability is exploit/multi/samba/usermap_script . The screenshot of launching exploit is:



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)