Cyber Defense Overview
Lab 2

Raghu Pusapati

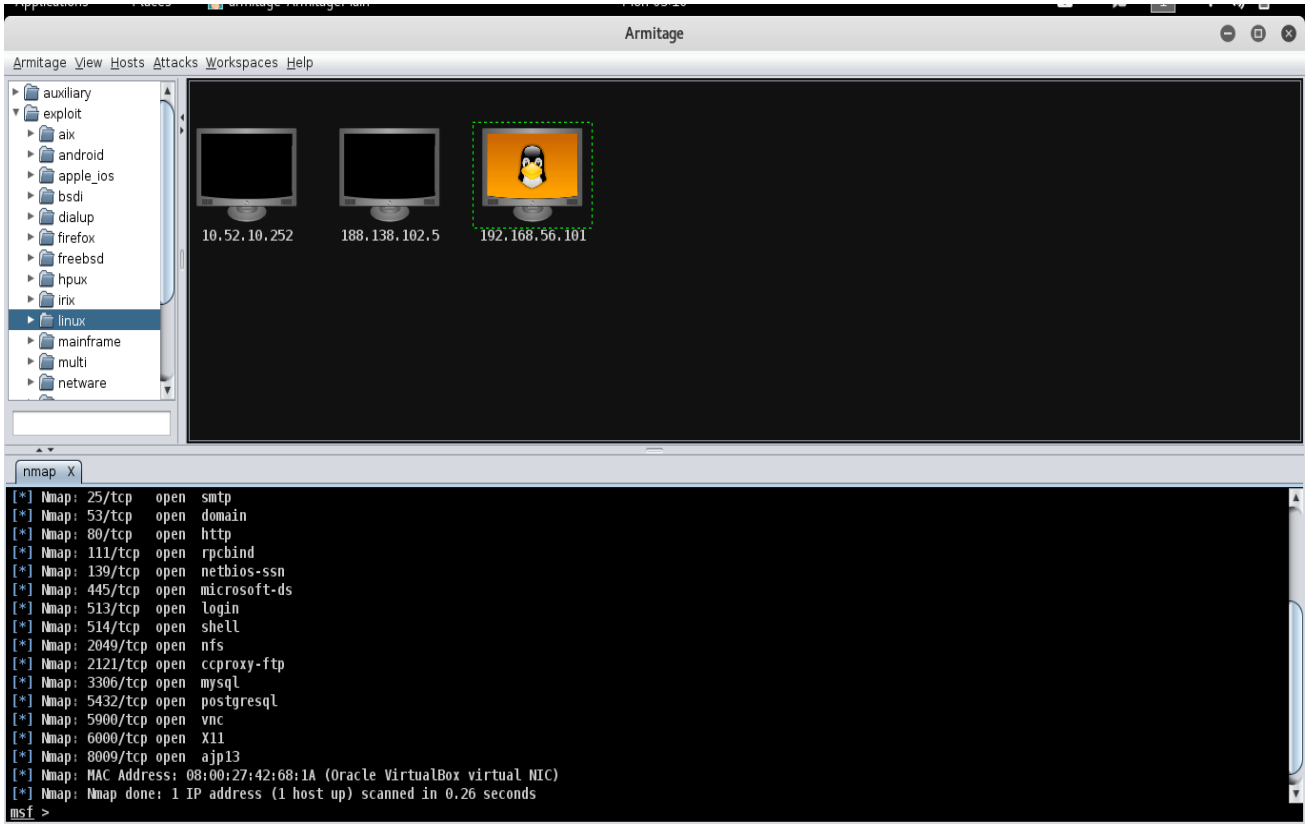
pusaparv@mail.uc.edu

Environment setup:

1. Metasploitable appliance is downloaded and imported into the virtual box.
2. My host machine is Kali Linux itself
3. Metasploitable is powered on.

Exercise:

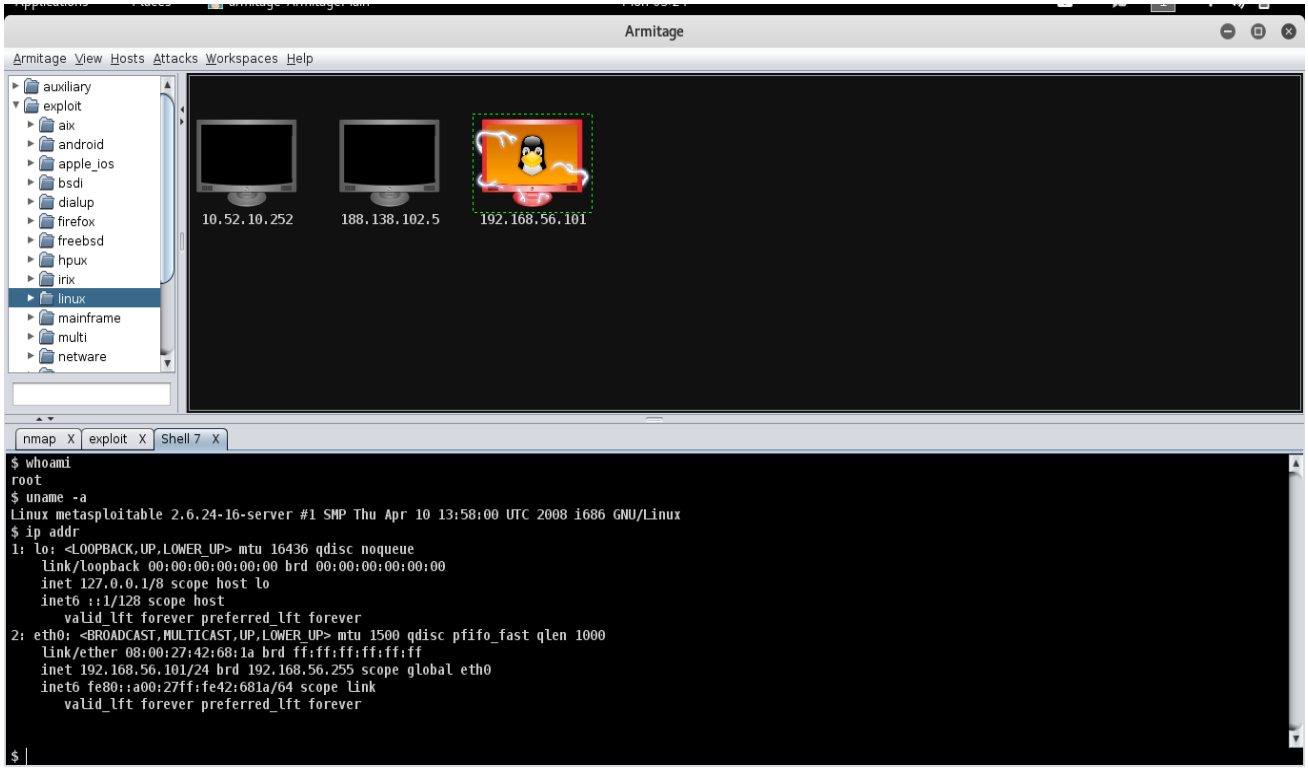
To start postgresql, 'sudo service postgresql start' command is issued on the console. Then Armitage is fired up using 'sudo armitage'. IP address of the guest machine is 192.168.56.101 while the IP address of the vboxnet0 interface on the host machine is 192.168.56.1. The guest host is added manually onto Armitage since the IP address is known. It can be done by clicking on Hosts => Add host. Then a monitor with the IP address used while adding will show up.



Once, all attacks are found using Attacks => Find attacks, a tab appears when we right click on our target host – 'Attacks'. We can then click on any of those to launch an attack. The status of the attack and/or the final result is displayed on the console at the bottom. Since Kali is my host machine, I had to change the default LHOST address from the eth0's address to vboxnet0's address. There are hundreds of modules available to attack, but the following are some of the vulnerabilities found pretty much directly (without necessarily altering default parameters).

1. ftp/vsftpd_234_backdoor:

This module exploits a backdoor that vsftpd version 2.3.4 has.

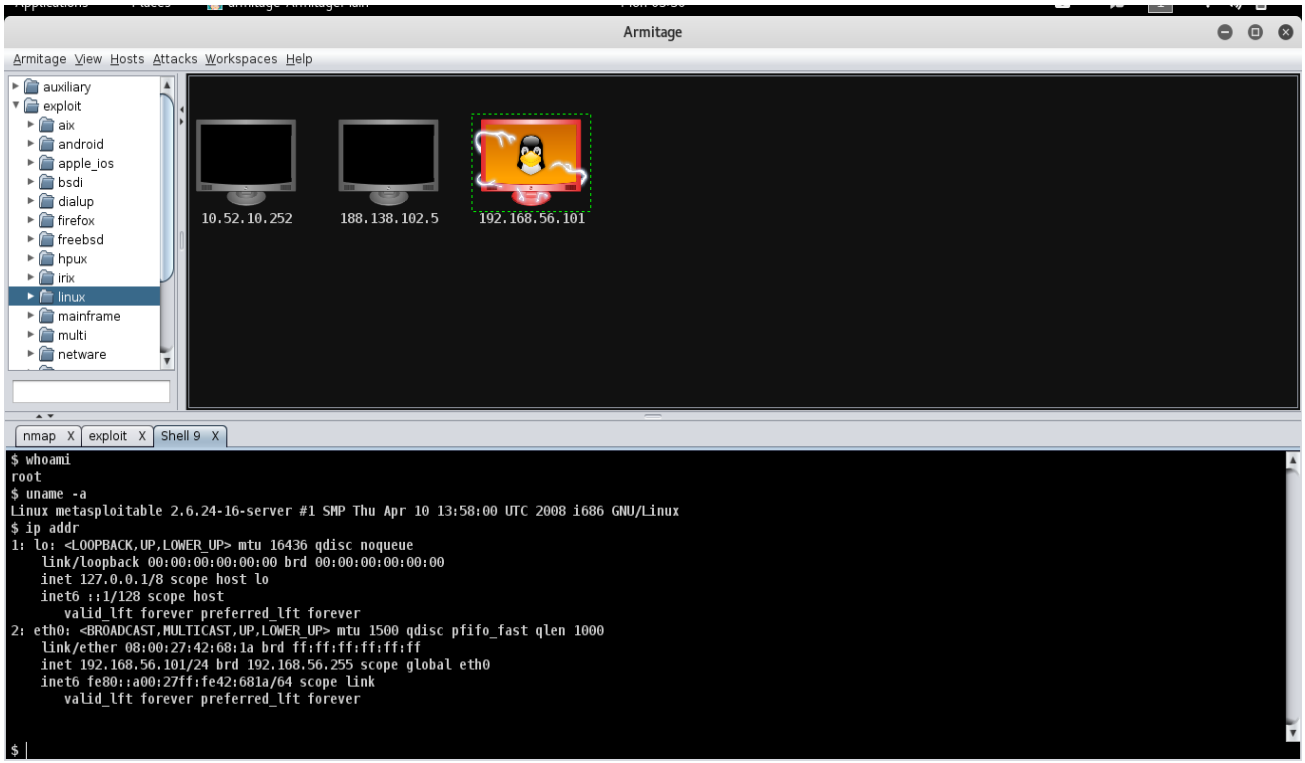


The attack opened a shell session (number 7). To show that it worked, I did whoami, uname -a and ip addr. We could root into the guest host from this exploit.

Fix: Updating to newer version fixes it.

2. irc/unreal_ircd_3281_backdoor:

This module exploits the backdoor in the unreal ircd version 3.2.8.1.

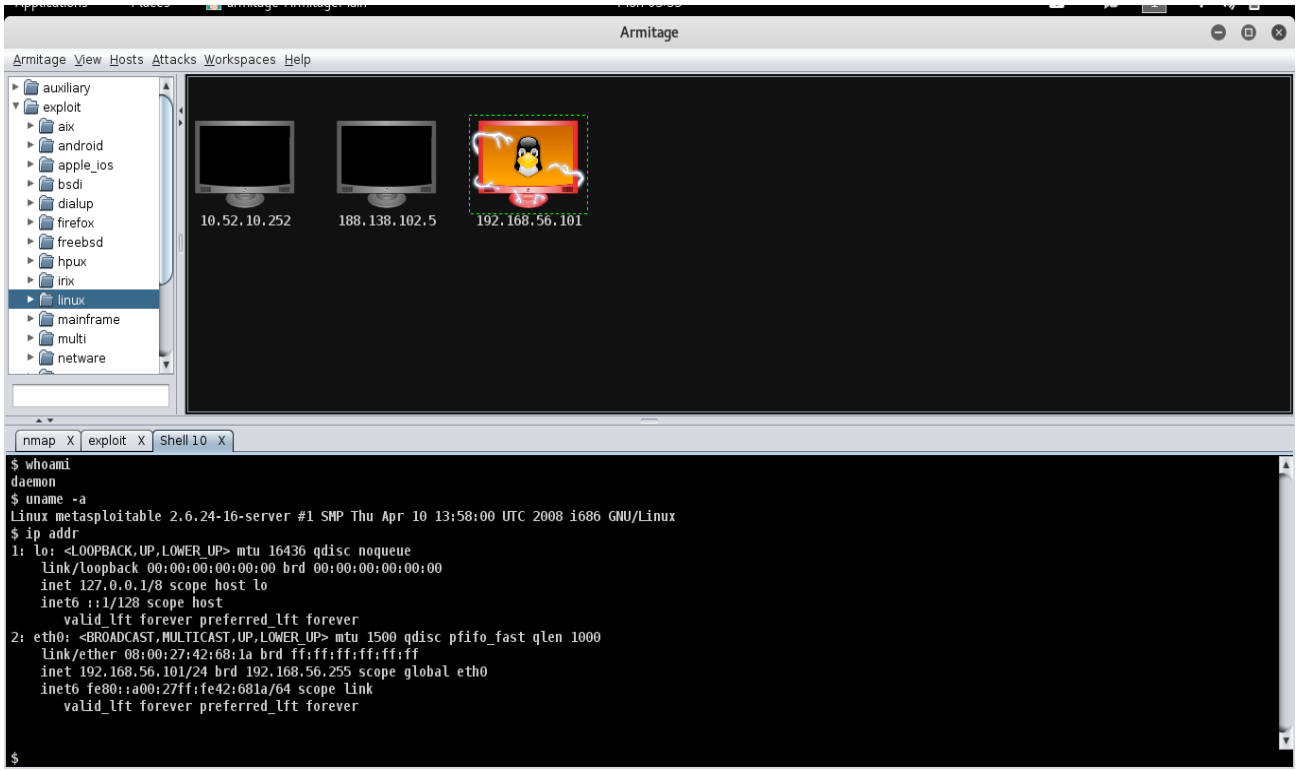


The result of the exploit is a new shell session (number 9 in the image). We got root access to the guest host.

Fix: Updating to newer version should fix this exploit.

3. misc/distcc_exec

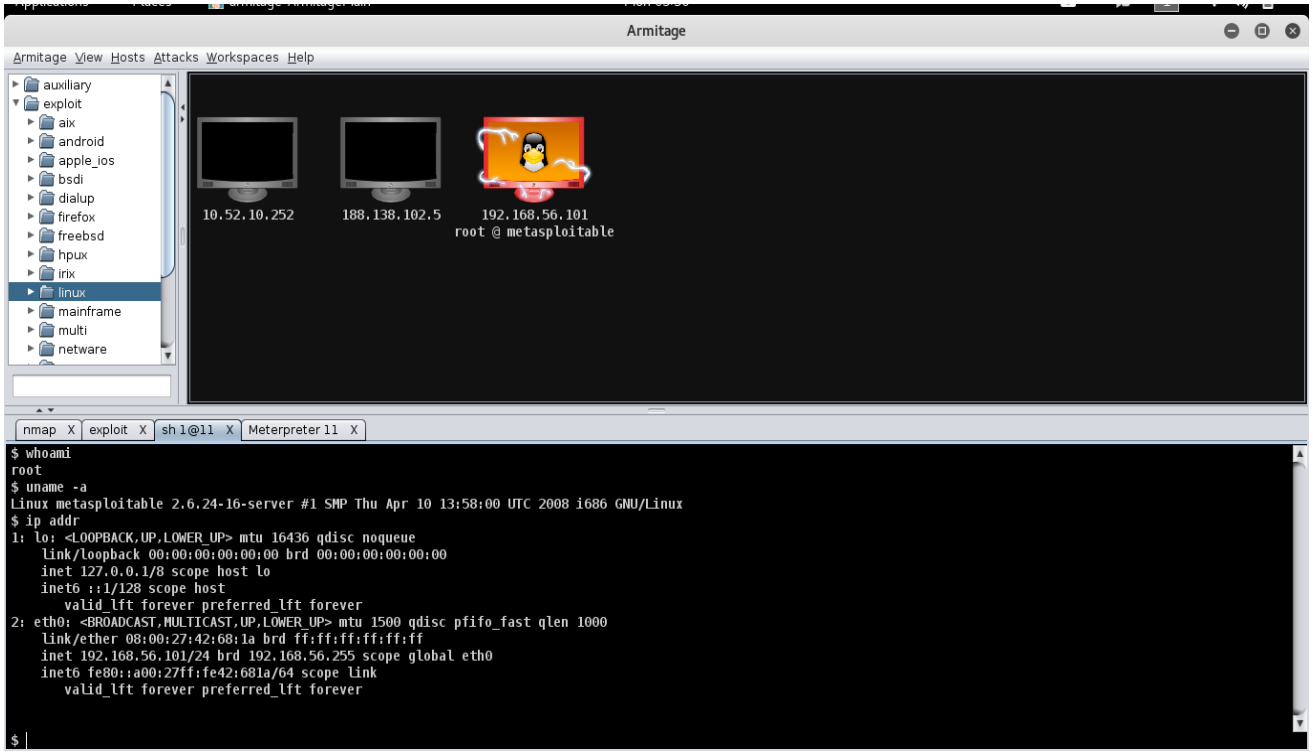
This module uses documented security weakness to get into the target system.

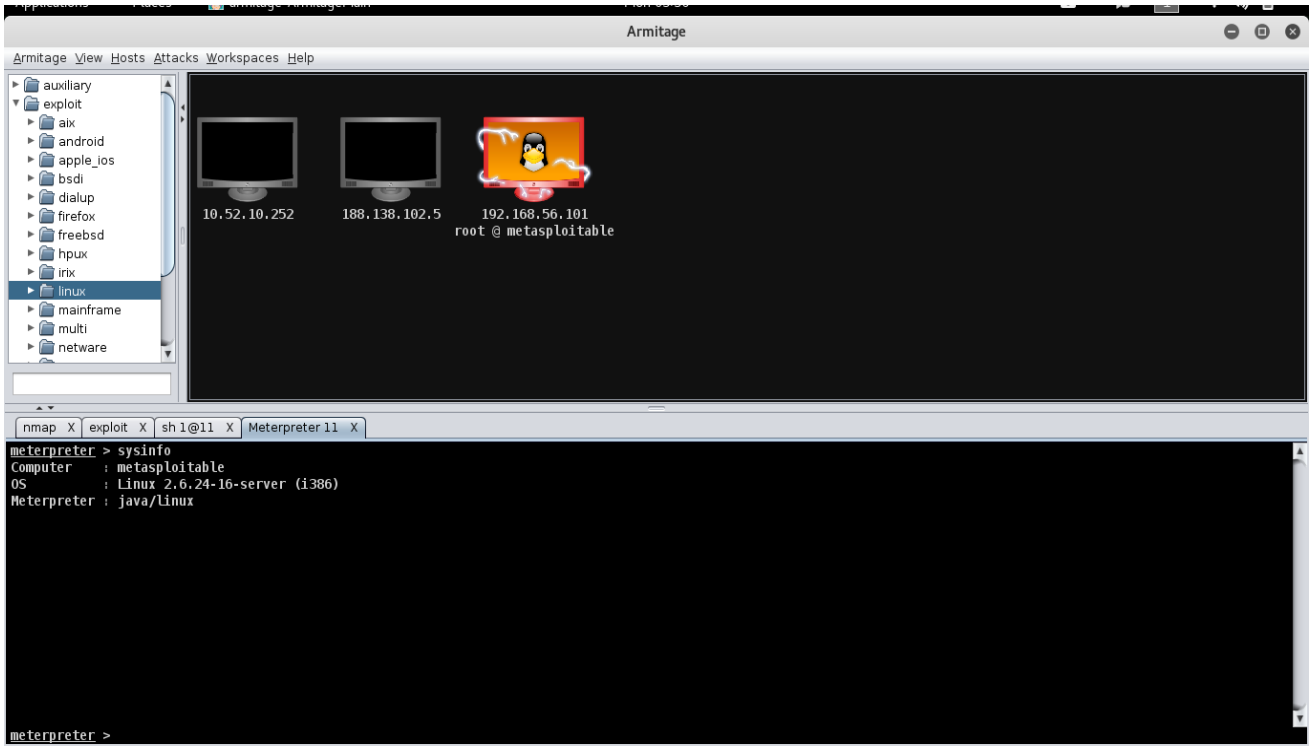


We could get in as a daemon user.

4. misc/java_rmi_server

The default java configuration allows for loading a remote class through web. This module exploits this misconfiguration. The result of the exploitation is a meterpreter session along with a shell session.



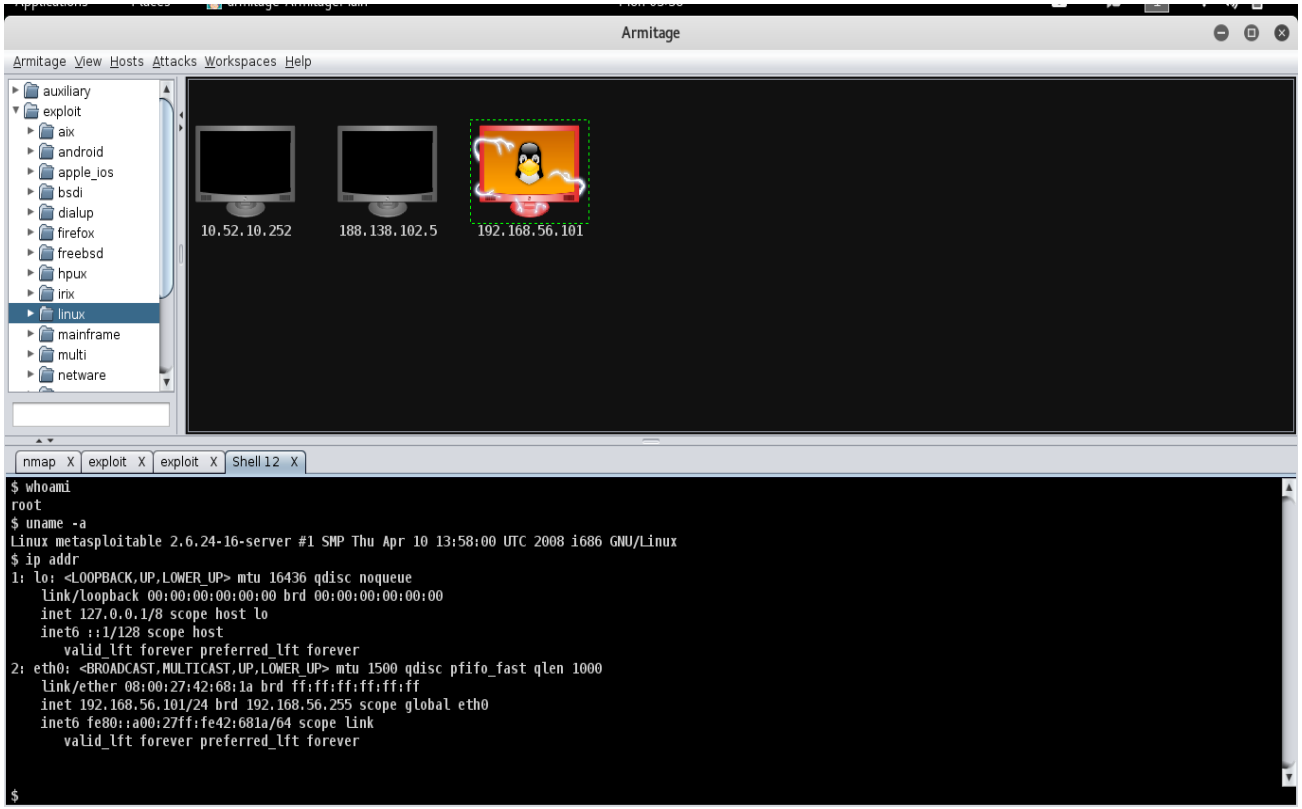


I could get root access using this module.

Fix: Changing default settings should fix this.

5. samba/usermap_script

The module works on Samba versions 3.0.20 through 3.0.25rc3. It exploits a command execution vulnerability found in this Samba version.

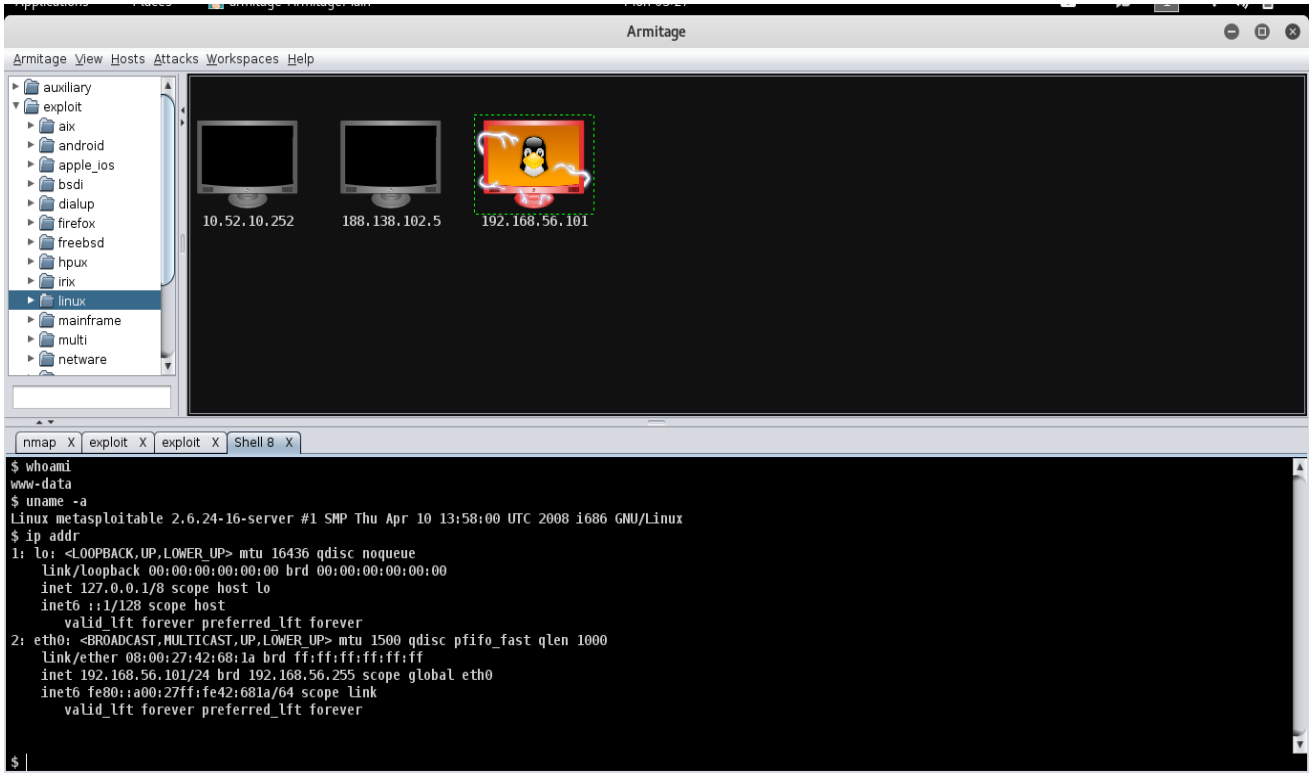


I could gain root access through this exploit.

Fix: Updating to newer version.

6. http/php_cgi_arg_injection:

This module works on PHP versions from 5.3.12 to 5.4.2. These versions are vulnerable to argument injection.



I could get into system as www-data user.

Fix: Updating to newer version.