

Forum:[Hack Forums](#)

Thread: [Laying low in exploited root box with new user and root privilege \[TUT\]](#)

Dimeblade - November 24, 2018, 6:02 am

Hello guys

Since I receive - negative reputation for what I think was good to express, here today I will teach you how to stay hidden in and lay low for longer in r00t servers. BTW I am not asking anyone to give a good rep + for me just here to help all I can with some knowledge.

After so long I decided to create a new thread which I think is going to benefit some members here. I hope everyone enjoys this ?

In this demonstration I will be using Ubuntu box for showing what need to be done.

First of all lets say you have used an public or private exploit for getting root access. Like in below pic I have already exploited and owned a server with root access.

Now we will want to create a new user in root box. But we will not be using just any username for this purpose.

For this tutorial we will be just using "..." as our user name and we will have to force the username to be added to the users.

This is because just using "adduser ..." is not going to work so we need to force it, just like the pic below:

Quote:Command used for above pic:

```
r00t:/# useradd ... --force-badname
```

After executing above command enter your desired password. Then press enter 5 times and at last type Y

Now you must be wondering why I specifically chose "..." to be added to user.

It is because when we do a simple "ls" in directory /home our user "..." will not be listed just like the rest of normal users added.

Ofcourse user "..." can be seen when we do "ls -lia" in direcotry /home we see our user there. But when owner of box is dumb they mostly goes unnoticed and this way its better than adding users such as "john" "l33t" you see.

Pic below will show executing 2 commands

Quote:Command 1: ls /home

Command 2: ls /home -lia

As you can see I have highlighted ... in by doing command 2 for demonstration purpose.

So now just adding wont be enough you need the user "..." you created to be with root privileges.

We need to add our user "..." to be in sudoers file.

To do this need to edit file which is located in "/etc/sudoers" and add our user there just like this:

NOTE: I am using vi for editing the lines and saving since its already installed with every unix operating sys. But you can use nano if its already installed.

Before giving root privileges you will notice just root is listed mostly under "#user privilege specification"

This is after editing "/etc/sudoers" and adding our newly created "..." user and giving same privilege as root

as you can see above I have edited and added below line under root :

```
... ALL=(ALL:ALL) ALL
```

Now restart root box:

```
exec /sbin/init
```

login with new user ... and password

then use command : `sudo su`

when prompt to enter password enter it.

With above command "sudo su" you can execute commands without typing sudo in every command you execute in that session.

Now at last you will want to remove all logs from the server and never leave any trace.

SORRY FOR MY BAD ENGLISH. I hope everyone learned something new today.

That is all for today. My next thread I will showing demonstration of creating a secondary user with name root and is also hidden. ?

? Thank you ?

VoIPv2 - November 24, 2018, 8:20 am

Oh, I get what you are doing with that.

Thanks for the share.

Dimeblade - November 24, 2018, 8:25 am

(Nov 24, 2018 09:20 AM)VoIPv2 Wrote: [\[CITE\]](#) Oh, I get what you are doing with that.

Thanks for the share.

Thanks for the first post to my thread :)

I hope it helped ya ?