

Forum:[Hack Forums](#)

Thread: [\[Share\] Root Exploiter with out Back Connect - \[New Methods\]](#)

blingbling - September 30, 2015, 9:15 am

[img=555x347]http://mukarramkhalid.com/wp-content/uploads/2015/09/main_screen.png[/img]

Hello Hackforums.

My first post here.

I want to share these articles written by a friend.

From the BlogPost

Introduction:

Have you ever had any of the following issues? Shell access to a vulnerable (Rootable) server with a known root exploit but no reverse or back connection.

Shell access to a server and you know the root login credentials but no SSH or any other means to connect.

Issues with port forwarding and back connect.

This article has 2 parts.

Part 1 - [\[PHP\]\[Python\] Root Exploiter – No Back-Connect](#)

Part 2 - [\[PHP\]\[C++\] Root Exploiter \(Part 2\) – No Back-Connect](#)

Video Demos:

[Part 1](#)

[Part 2](#)

Credits to the author of : <http://mukarramkhalid.com>

CIA Insider - September 30, 2015, 9:34 am

Surprised that this gets no love. Seems like quality. Great post.

EbonCipher - September 30, 2015, 11:27 am

Tested it out. Works well. Thanks for the share.

Aur3xis - September 30, 2015, 11:34 am

Wow, a quality share from a newb on here?

Stay HQ my friend.

HaxOr? - September 30, 2015, 12:34 pm

Nice share mate, thanks for posting.

Im gone brah - September 30, 2015, 1:45 pm

If really doesn't have the resources or can't bother to back-connect. You are still able to run commands through the shell as root and by using a pipe.

```
Code Root@doge:~# echo 'exploit goes here, hello, hello, hello' | ./exploitname123
```

Do demonstrate the use of the pipe.

```
Code root@doge:~# echo zeroisabeaver | base64  
emVyb2lzYWJlYXZlcgo=
```

Hell you can even add another pipe if you want to run something else. A stupid example of first encoding the string in base64 then decode it.

```
Code root@doge:~# echo zeroisabeaver | base64 | base64 --decode  
zeroisabeaver
```

Another example of using the pipe operator.

```
Code root@doge:~# echo zeroisabeaver | base64 | cat logfile.log  
zeroisabeaver  
64 bytes from 6.6.6 (127.0.0.1): icmp_req=31359 ttl=50 time=10.4 ms
```

blingbling - September 30, 2015, 4:15 pm

(Sep 30, 2015 01:45 PM)Zayne Wrote: [\[CITE\]](#) If really doesn't have the resources or can't bother to back-connect. You are still able to run commands through the shell as root and by using a pipe.

...

...

...

Thanks for the info. ?. The Part 1 of this article covers another aspect. What if we have login credentials of the root user or any other user and we don't have any means to connect to the server, just a php interface. Can we do something like this with pipes?

```
Code su - someUser  
passwd: pass_of_someUser  
Successfully logged in.  
someUser@mylinuxBox~# (Waiting for the next command as someUser)I guess no.
```

hahdbwoannniabs - September 30, 2015, 8:56 pm

Nice share. I've given up several boxes in the past because I couldn't obtain a shell.

Meowie - October 1, 2015, 7:50 am

(Sep 30, 2015 01:45 PM)Zayne Wrote: [\[CITE\]](#) If really doesn't have the resources or can't bother to back-connect. You are still able to run commands through the shell as root and by using a pipe.

```
Code Root@doge:~# echo 'exploit goes here, hello, hello, hello' | ./exploitname123
```

Do demonstrate the use of the pipe.

```
Code root@doge:~# echo zeroisabeaver | base64  
emVyb2lzYWJlYXZlcgo=
```

Hell you can even add another pipe if you want to run something else. A stupid example of first encoding the string in base64 then decode it.

```
Code root@doge:~# echo zeroisabeaver | base64 | base64 --decode  
zeroisabeaver
```

Another example of using the pipe operator.

```
Code root@doge:~# echo zeroisabeaver | base64 | cat logfile.log  
zeroisabeaver
```

64 bytes from 6.6.6 (127.0.0.1): icmp_req=31359 ttl=50 time=10.4 msYou cannot interact with a process via PHP (at least to my knowledge).

If you want to, you can go ahead and try executing gdb and inputting something via PHP.

@OP, Nice! I really like this.
Finally something new in here.

Im gone brah - October 1, 2015, 7:57 am

(Oct 1, 2015 07:50 AM)Meowie Wrote: [\[CITE\]](#) You cannot interact with a process via PHP (at least to my knowledge).

If you want to, you can go ahead and try executing gdb and inputting something via PHP.

@OP, Nice! I really like this.
Finally something new in here.

Where the hell did I mention anything regarding PHP completely not relevant to what I posted?

Meowie - October 1, 2015, 8:03 am

(Oct 1, 2015 07:57 AM)Zayne Wrote: [\[CITE\]](#) Where the hell did I mention anything regarding PHP completely not relevant to what I posted?

You mentioned piping, I just mentioned PHP.

Piping happens to be exactly like PHP in the regard that you cannot interact with a program.

Im gone brah - October 1, 2015, 8:49 am

(Oct 1, 2015 08:03 AM)Meowie Wrote: [\[CITE\]](#) You mentioned piping, I just mentioned PHP.

Piping happens to be exactly like PHP in the regard that you cannot interact with a program.

I told him another way to possibly gain root without using a back-connection and neither a reverse-connection. (relying on that the exploit works)

You on the other hand mentioned this and quoted me on it.

Quote:You cannot interact with a process via PHP

Quote:Piping happens to be exactly like PHP in the regard that you cannot interact with a program.

However, I never stated that you can interact with a process through either php or a pipe. What I did state here is that bin/sh will allow the individual to redirect an output of commands into other commands through a pipe.

Quote:interact

Int?r'akt

verb

act in such a way as to have an effect on each other.

"all the stages in the process interact"

communicate or be involved directly.

"the user interacts directly with the library"

You can actually have an effect on a process for example by killing it through using the php function `posix_kill()`

`Posix_kill` will send a signal to the proccess

Meowie - October 1, 2015, 9:00 am

(Oct 1, 2015 08:49 AM)Zayne Wrote: [\[CITE\]](#) I told him another way to possibly gain root without using a back-connection and neither a reverse-connection. (relying on that the exploit works)

You on the other hand mentioned this and quoted me on it.

However, I never stated that you can interact with a process through either php or a pipe. What I did state here is that bin/sh will allow the individual to redirect an output of commands into other commands through a pipe.

You can actually have an effect on a process for example by killing it through using the php function `posix_kill()`

`Posix_kill` will send a signal to the process I said interact

And have you tested what happens if you run a local root exploit without a reverse or bind shell?

Yeah, it doesn't really work unless you make the exploit do something like write an suid root file.

Im gone brah - October 1, 2015, 9:04 am

(Oct 1, 2015 09:00 AM)Meoww wrote: [\[CITE\]](#) I said interact

And have you tested what happens if you run a local root exploit without a reverse or bind shell?

Yeah, it doesn't really work unless you make the exploit do something like write an suid root file.

You said interact and I gave you the definition of it with an example. I also never stated anything about a local root exploit now did I?

Meoww - October 1, 2015, 9:36 am

(Oct 1, 2015 09:04 AM)Zayne wrote: [\[CITE\]](#) You said interact and I gave you the definition of it with an example. I also never stated anything about a local root exploit now did I?

Haha, okay okay.

I'll let you have this one.

FITSD - October 1, 2015, 10:18 am

Another awesome thread + Video Demo!

Thanks buddy

JaNuS18 - October 2, 2015, 3:31 am

(Sep 30, 2015 09:15 AM)blingbling wrote: [\[CITE\]](#) I want to share these articles written by a friend.

...

As far as I know makman is member here on HF. I am not sure why did you post this instead of him ?

blingbling - October 2, 2015, 3:38 am

(Oct 2, 2015 03:31 AM)JaNuS18 wrote: [\[CITE\]](#) As far as I know makman is member here on HF. I am not sure why did you post this instead of him ?

Sorry dude. I didn't know. ?

zero.py - October 4, 2015, 10:05 pm

HQ thread indeed and very innovative. This helped me a lot. Thanks for sharing.

m115 - October 5, 2015, 5:32 pm

can it work in kernel 2.6.18-398.el5 #1 SMP Tue Sep 16 20:50:52 EDT 2014 x86_64 ?

or can u help me to root the kernel :D

Learner Boy - October 5, 2015, 8:23 pm

Nice share OP

Thanks for this

Wireless Network - *October 6, 2015, 1:11 pm*

Thanks for sharing this! Stay HQ!

LeadGenerator - *October 7, 2015, 4:40 pm*

Really high quality - thanks so much. Loved watching the video demo.

makmaniac - *October 28, 2015, 6:03 am*

? .. Thanks for sharing my work .. ?

limainfinita - *October 28, 2015, 6:21 pm*

awsome

i was looking for something like this for a while now

great work

(Oct 28, 2015 06:03 AM)makmaniac Wrote: [\[CITE\]](#) ? .. Thanks for sharing my work .. ?