

Forum:[Hack Forums](#)

Thread: [\[TUT\] Mac OS X 10.9.5 Root Exploit \[TUT\]](#)

h?ck?r - October 27, 2015, 8:42 pm

Hi guys, today I am going to show you how spawn a root shell on OS X Mavericks 10.9.5, in which you can run any command with root privileges ?

What You Will Need:

Mac running OS X Mavericks 10.9.5

Access to Terminal

NOTE: If you do not have these you will not be able to get root

Step One

Download my script from [here](#) and save it to your Desktop as exploit.py (or whatever you want the filename to be).

NOTE: Must be saved as a python script!!

Step Two

Open Terminal and type cd Desktop. Then type

Code python exploit.py

or whatever you named the file.

Step Three

Let my script execute, it may take up to a minute or two. Once completed you will get something like this. You now have a root shell in which you can execute root commands!

Spoiler [\(Click to View\)](#)

What Can I Do With This?

1.) Steal the passwords of any account on your computer!

Download my keychaindumper.sh script and run it! Download by [clicking here](#)

2.) Make any normal user account an admin account Click spoiler for code. Spoiler [\(Click to View\)](#)

Code sudo dseditgroup -o edit -a UsernameToAdd -t user admin

3.) Anything you want ?

Hope you enjoyed my tutorial! Post your thoughts!

NyQuil - October 27, 2015, 8:43 pm

cool will check it out in a bit, least its not another tutorial on how to exploit something without using metasploit.

DrakkarLevi - October 27, 2015, 10:53 pm

Does this work only on 10.9.5? I have 10.11.1 El Capitan ;(

h?ck?r - October 27, 2015, 10:57 pm

It only works on 10.9.5 I think. I haven't tried it on anything else

DrakkarLevi - October 27, 2015, 11:02 pm

Dang. Well, I have a quick question either way.

Someone ssh'd into a server on this Mac, but I guess the password wasn't saved (when you ssh into servers, typing in the password is invisible). Would this exploit allow me to obtain this password?

h?ck?r - October 27, 2015, 11:07 pm

Probably not, but if you were running 10.9.5 you could get admin privileges and install a keylogger.

SWCR - October 28, 2015, 11:13 pm

Someone try it on 10.11.1?

h?ck?r - October 28, 2015, 11:26 pm

Got you guys something :D

<https://github.com/kpwn/tpwn>

Works for 10.11.5>

SOSA_ - October 29, 2015, 7:09 pm

(Oct 27, 2015 11:02 PM)awric Wrote: [\[CITE\]](#) Dang. Well, I have a quick question either way.

Someone ssh'd into a server on this Mac, but I guess the password wasn't saved (when you ssh into servers, typing in the password is invisible). Would this exploit allow me to obtain this password?

Assuming that the keypairs are stored on that computer and the password is in the keychain, yes. But you need a separate keychain stealer

OP, did you write this yourself?

h?ck?r - October 29, 2015, 7:29 pm

Write what exactly? haha there's like 4 different codes included :D

SOSA_ - October 30, 2015, 12:48 pm

(Oct 29, 2015 07:29 PM)greyhatphantom Wrote: [\[CITE\]](#) Write what exactly? haha there's like 4 different codes included :D

The main exploit script

h?ck?r - October 30, 2015, 12:56 pm

Found part of a script then modified :D

Did it work for you? The script was pretty complicated, so I shortened it up and made it user friendly :D

Tr0janVirus - October 31, 2015, 1:34 pm

Will this work for el capitan?

WiiSport - October 31, 2015, 1:36 pm

Really nice OP! Will try this on my old iMac. Needed this for a long time a time ago. Still going to do the idea because of your thread. Thanks :)

Kind and regards,

- WiiSport

? Eugtique ? - October 31, 2015, 2:06 pm

I'll need to try :o haha thanks ^^

h?ck?r - October 31, 2015, 2:58 pm

(Oct 31, 2015 01:34 PM)Tr0janVirus Wrote: [\[CITE\]](#) Will this work for el capitan?No, but look at tpwn on GitHub. That should work for you.

(Oct 31, 2015 01:36 PM)WiiSport Wrote: [\[CITE\]](#) Really nice OP! Will try this on my old iMac. Needed this for a long time a time ago. Still going to do the idea because of your thread. Thanks :)

Kind and regards,
- WiiSport
Good luck! Hope it works for you.

(Oct 31, 2015 02:06 PM)? Eugtique ? Wrote: [\[CITE\]](#) I'll need to try :o haha thanks ^^Welcome!

Tr0janVirus - October 31, 2015, 5:56 pm

Okay after getting tpwn can i still run that and use the same codes on terminal?

h?ck?r - October 31, 2015, 7:45 pm

Yes. Just the initial root exploit won't work. The other codes will/should

ng-Coder - November 1, 2015, 11:30 pm

(Oct 28, 2015 11:26 PM)Menist Wrote: [\[CITE\]](#) Got you guys something :D

<https://github.com/kpwn/tpwn>

Works for 10.11.5>

That's smart thx, but vulnerability got burnt in 10.11.?

Apple are like forcing update on you now.?

h?ck?r - November 2, 2015, 6:14 am

Yep. I know that. If there was a vulnerability, they would want to patch it.

Frave - November 10, 2015, 12:41 am

Will this work for 10.11?

h?ck?r - November 10, 2015, 1:00 pm

(Nov 10, 2015 01:41 AM)Frave Wrote: [\[CITE\]](#) Will this work for 10.11?No, but tpwn should. The link is in the tutorial

thehappydino - December 17, 2015, 7:55 am

Hey, I actually did something similar for 10.10.3 by using (whoami) and DYLD_PRINT_TO_FILE. Check out my posts for more info. And if you don't have access to Terminal.app you can right click on the app copy the Resource folder into a new folder called term. After that rename the new folder to term.app. Hope that helped someone. ?

?? ?????? ????? ??? ?????? ?????? ?????? ?????? ?????? ??? ?????? ?????
?? ?????? ?????? ??? ?????? ?????? ?????? ?????? ?????? ?????? ??? ?????? ?????
?? ?????? ?????? ??? ?????? ?????? ?????? ?????? ?????? ?????? ??? ?????? ?????

h?ck?r - December 21, 2015, 6:28 pm

(Dec 17, 2015 08:55 AM)thehappydino Wrote: [\[CITE\]](#) Hey, I actually did something similar for 10.10.3 by using (whoami) and DYLD_PRINT_TO_FILE. Check out my posts for more info. And if you don't have access to Terminal.app you can right click on the app copy the Resource folder into a new

?? ????? ???? ???? ???? ???? ???? ???? ???? ???? ???? ????
 ?? ????? ???? ???? ???? ???? ???? ???? ???? ???? ???? ????
 ?? ????? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ????

(Jan 2, 2016 04:29 AM)axmaxmax Wrote: [\[CITE\]](#) thanks man good working 10.9.5 :DAwesome!!
Enjoy :D