

Forum:[Hack Forums](#)

Thread: [\[Easy\] \[pics\] How to Root a Server \[COMPLETE\]](#)

??h™ - October 21, 2011, 8:28 pm

Back before I wrote my crappy, outdated Metasploit tutorial, no one knew what Metasploit was. Now there is a tutoiral being posted on it every other day. I hope the same thing happens with this tutorial. This tutorial explains, IN DEPTH, how to:

1. Set up an IRCd
2. Find VPSs to target
3. Exploit VPSs
4. Setup and use mIRC
5. Use knight.c
6. Rase a powerfull botnet army from scratch

It's a bit of a read, but I hope you enjoy it! Thanks. ?

<http://thebth.org/?p=345>

Edit: Ok, this pdf is the entire text of the post. I'm having some server issues, and the site will be back up as soon as they are resolved.

http://www.4shared.com/document/ysPVhee1/Server_Rooting.html?

zer0day - October 21, 2011, 9:44 pm

Very nice Tutorial, Quality, keep it up.

bgxcdic - October 22, 2011, 12:18 am

Nice in depth tutorial :D Thanks for posting.

Sonic Boom - October 22, 2011, 12:46 am

Thank you very much for this. Bookmarked , so I can read it later. :)

lionkidd - October 22, 2011, 12:51 am

pls fixx this:This Account Has Been Suspended ;D

Alienguy - October 22, 2011, 12:54 am

Error : This Account Has Been Suspended
Please fix that.

andreinescastro - October 22, 2011, 4:44 pm

I'm very interested, please post a new link, thanks ;)

??h™ - October 22, 2011, 6:42 pm

Ok, I fixed it (sort of). You can read about it in the pdf, which is the text of the post. :D

x3r0x3 - October 22, 2011, 9:58 pm

thanks for the tutorial and very interesting ;)

Frostbite™ - October 22, 2011, 10:03 pm

This looks really good, but could you please make it into a thread?

??h™ - October 22, 2011, 10:29 pm

(Oct 22, 2011 10:03 PM)Gu?Rdi?n Wrote: [\[CITE\]](#) This looks really good, but could you please make it into a thread?

I did and it was 400 words to long, so there is now a part I and II floating around. :D

bluebknight - October 23, 2011, 5:43 am

Well, isn't it more concentrated about how to make a DDOS system rather than how to root?

From my experience, Chances of Exploiting linux systems via remote exploits are extremely rare. For example, a nmap scan will show you lots of vulnerable ProFTPd server, for example, but chances of exploiting it is very rare. Hardly any server run as "root" and there's no way to get root via "get system" like in metasploit. You need a local root exploit at this point.

According to your topic, your post should have been something like, how to get a shell in a server via SQL injection/LFI/RFI and then rooting it via a local root exploit. And, then you could have had written about the DDOS setup. Btw, I haven't tried it but I don't think that your "knight.c" requires root permissions at all. r57 shell and most shells already can back-connect via irc.

You also wrote "Be a bawz and make your own exploit. This is VERY easy with the metasploit framework," yeah, right... Have you ever written an exploit in your life? Forget about writing one, have you ever even found a heap/stack or a simple memory address to overflow? If it was "VERY easy" there would be tons of linux exploits. With the implementation of ASLR, it's near impossible to write a exploit cause it's extremely hard to find the exact point that you are overflowing with your fuzzer.

You think of yourself as someone in Stage 5 but you are in Stage 3/4. Other than RATting and DDOSing, there are lots of more stages to hacking, which includes reverse engineering, writing your own exploits, use JTAG/SPI to put exploits in the NAND/FLASH memory. etc...

P.S. I do not hate you or anything but I just think you should correct the name of your topic and you still have a loot more to learn. Take my criticize as a start to learn more and I liked the part about where you explained about how to setup the IRC server. There isn't a very well written tutorial about that anywhere. You should also write a tutorial about how to setup a channel on dalnet or any public channel like that so that people who has trouble port forwarding due to ISP restrictions etc. can use bots and also can have a shell backconnect to an IRC server.

Frostbite™ - October 23, 2011, 6:14 am

(Oct 23, 2011 05:43 AM)bluebknight Wrote: [\[CITE\]](#) Well, isn't it more concentrated about how to make a DDOS system rather than how to root?

From my experience, Chances of Exploiting linux systems via remote exploits are extremely rare. For example, a nmap scan will show you lots of vulnerable ProFTPd server, for example, but chances of exploiting it is very rare. Hardly any server run as "root" and there's no way to get root via "get system" like in metasploit. You need a local root exploit at this point.

According to your topic, your post should have been something like, how to get a shell in a server via SQL injection/LFI/RFI and then rooting it via a local root exploit. And, then you could have had written about the DDOS setup. Btw, I haven't tried it but I don't think that your "knight.c" requires root permissions at all. r57 shell and most shells already can back-connect via irc.

You also wrote "Be a bawz and make your own exploit. This is VERY easy with the metasploit

framework," yeah, right... Have you ever written an exploit in your life? Forget about writing one, have you ever even found a heap/stack or a simple memory address to overflow? If it was "VERY easy" there would be tons of linux exploits. With the implementation of ASLR, it's near impossible to write a exploit cause it's extremely hard to find the exact point that you are overflowing with your fuzzer.

You think of yourself as someone in Stage 5 but you are in Stage 3/4. Other than RATting and DDOSing, there are lots of more stages to hacking, which includes reverse engineering, writing your own exploits, use JTAG/SPI to put exploits in the NAND/FLASH memory. etc...

P.S. I do not hate you or anything but I just think you should correct the name of your topic and you still have a lot more to learn. Take my criticize as a start to learn more and I liked the part about where you explained about how to setup the IRC server. There isn't a very well written tutorial about that anywhere. You should also write a tutorial about how to setup a channel on dalnet or any public channel like that so that people who has trouble port forwarding due to ISP restrictions etc. can use bots and also can have a shell backconnect to an IRC server.

The bits of that I understand of that are very true and the bits I dont sound very legit as well. But yeah this guide is more focused on building a DDoS system, not rooting.

Thementor - October 23, 2011, 6:26 am

wow m8 , ive read it setup my IRC server thing and got 3 vps's things!!! Thanks m8! instead of using them with the irc thing though im using putty and making loads of putty booters to sell.

madhanmech - October 23, 2011, 6:56 am

hey ... thanks for the tutorial mate...

visstee1 - October 23, 2011, 9:08 am

wow nice tutorial mate!

Too bad that I could not give reputation for it:(

The Enforcer - October 23, 2011, 9:30 am

Thank you very much for this. hope it will be use full for me...

6LACK EA6 - October 23, 2011, 12:20 pm

Very useful, Thanks alot, great tutorial. :)

_Gorhax - October 24, 2011, 8:08 am

How the fuck can you say 100 rooted servers are as strong as 100k bots? All goes by the connection speed of the bots etc. You can have a bot with the same or even faster connection speed than some random Linux box..

nbdays0 - October 24, 2011, 4:39 pm

Thanks a lot, I thought it was a great tutorial :D

blady20 - October 24, 2011, 8:00 pm

Thank you. Very nice tutorial. ?

ItsFluffy - October 25, 2011, 8:43 pm

ive been looking for ages for a rooting tut so i hope this will grant me what i seek

The Enforcer - October 25, 2011, 8:51 pm

thanks for the share mate .. thanks hope will be useful for me..

Overdose - October 26, 2011, 4:03 am

Nice High Quality tutorial.

Keep it up.

Greystersting - October 26, 2011, 5:58 pm

Thanks for the tut

Is there a 64bit version of bircd or a similar ircd?

??h™ - October 26, 2011, 6:28 pm

(Oct 26, 2011 05:58 PM)Greystersting Wrote: [\[CITE\]](#) Thanks for the tut

Is there a 64bit version of bircd or a similar ircd?

The 32 bit works on 64 bit computers. :)

Greystersting - October 26, 2011, 7:50 pm

(Oct 26, 2011 06:28 PM)??h™ Wrote: [\[CITE\]](#) The 32 bot works on 64 bit computers. :)

When I open mkpasswd.exe it says

Code The version of this file is not compatible with the version of Windows you're running. Check your computer's system information to see whether you need an x86 (32-bit) or x64 (64-bit) version of the program, and then contact the software publisher. Before you ask I HAVE tried it in compatibility mode.