

Forum:[Hack Forums](#)

Thread: [\[TuT\] - Hack a site through FTP - \[TuT\]](#)

zer0pwn - October 10, 2011, 12:47 am

Hello there HackForums, here I am again, posting a tutorial on web-penetration. I will be explaining how to crack and hack an FTP server.

What is "FTP"?

FTP stands for File Transfer Protocol. As you can see by the name, you can manage files through the FTP. The FTP port, is very-well known, but is rarely open on big websites. The FTP port is Port 21. There are multiple ways to connect to an FTP server/port, especially thanks to technology, such as FileZilla.

There are of course other ways, which are the manual ways. Which is connecting to the FTP through a DOS Command line. You can do this from Ubuntu, Backtrack, (All linux), and also Windows. I've never tried it on Mac, but I'm sure it's possible.

When you have access to the FTP, you're the king of the website. Mostly because you can manage all of the files and directories on the site. So you can upload and delete. If you upload your PHP or ASP shell, you could root the server, and possibly hack other sites.

How do I know if the FTP port is open?

Well, you don't know until you scan. The most popular port scanner would be Nmap. You can download Nmap at <http://www.nmap.org/>

How do I connect to FTP?

Like I said, there are a couple options. Personally, I would choose the command line first, because you learn from it. In a program like FileZilla, with all the fancy shit, it's got it all. Easy to work with, etc. But the method we will be using to connect, is with "Telnet".

Telnet is a network protocol that you can use to connect to certain ports on hosts. You would either need the website name, or IP to connect. You would also have to make sure the port that you want to connect to, is open.

To do that, we need a program called "Nmap". Nmap is a free Port-Scanner tool, it is very useful to many hackers for multiple reasons.

To connect to FTP on a site, an IP, or a computer, you need to have Telnet installed. Telnet is already installed on all Windows and Linux operating systems. But in Windows 7 & Vista, you have to change some settings.

This can be done very easily, simply go to Control Panel ==> Programs and Features ==> Turn windows features on or off ==> Check off the Telnet Client.

Now we can successfully connect to a port through Telnet.

So open CMD (Command Prompt(Start => Run => CMD)). Now in the command prompt, type:

Code telnet

And hit enter. Now we're on Telnet, so we can connect to a port. If you would like to get familiar with the commands, simply type in "HELP" in the command prompt.

Now, let's connect to our site (First make sure the FTP port is open (Port 21). Now, let's type in:

Code o www.sitename.com 21

Now it should display some information on the FTP, we can use that information against the site, by simply googling some exploits for it.

Example: "ProFTPD 1.3.3c Exploit".

How do I hack a site through FTP?

There are a couple ways to do this, my favorites are looking for exploits in the FTP client and version, and Bruteforcing/Dictionary attack. The first method is very simple, just read the above section to figure out how to do it.

Bruteforcing is when you attack a target by using sometimes MILLIONS of passwords. Bruteforce uses random combinations, whereas a Dictionary Attack uses words. The Dictionary Attack goes MUCH faster, but will not always work. I only bruteforce when I have no other choice.

The second way, is still pretty easy, but requires a little bit more brain :P. If you want to do it more "Advanced-ly" then download "Hydra". Hydra is a program that will perform a dictionary attack on any open port on your target site, or IP.

The easy way to do it, is by downloading "Brutus". It does the same thing, but it's easier to navigate and use. You can get both programs by googling them. If you can't find any, PM me and I'll send you a good link.

If you already have the credntials, you can login to the FTP over Telnet, by doing the following:

Code o www.site.com 21

-

PASV

-

USER -USERNAMEHERE-

PASS -PASSWORDHERE-

Epilogue

This is a tutorial for beginners, but if I missed something PLEASE notify me by PM or by replying in the comment section. This tutorial does seem very brief to me, but I can't explain EVERY exploit there is for FTP, otherwise the tutorial would be too long and boring.

If you require any assistance, be sure to contact me by PM. I ALWAYS read my PMs, and I 90% of the time reply to all of them.

I really hope this tutorial helped, but if it didn't, please tell me what I did wrong on this tutorial, so that I can fix it for you. :)

kobez - October 10, 2011, 12:51 am

Good tutorial you have here zeropwn, very helpful to the beginners.

zer0pwn - October 10, 2011, 12:56 am

(Oct 10, 2011 12:51 AM)kobez Wrote: [\[CITE\]](#) Good tutorial you have here zeropwn, very helpful to the beginners.

Thanks kobez, that's what I was aiming for :)

raX0r - October 10, 2011, 1:05 am

Well explained good work man.... tnx for this....

~!White!~ - October 10, 2011, 1:11 am

Nice tutorial keep up the good work cant wait for future tuts

mudkipize - October 10, 2011, 2:15 am

yeah i learnt this a while ago, must make mad logs on the server, also, a lot of FTP's will ban you after a certain ammount of incorrect trys but...not all of them i guess.

Isolate - October 10, 2011, 3:23 am

Great tutorial i have been looking for some ftp exploit's and this is perfect thanks!

Darkalias - October 10, 2011, 4:02 am

for people that have trouble with ProFTPD 1.3.3c Exploit and it says no backdoor planted or something like that

and you have the correct version just keep trying sometimes it won't work and when you do it a next time it works ok

zer0pwn - October 10, 2011, 4:05 am

(Oct 10, 2011 04:02 AM)Darkalias Wrote: [\[CITE\]](#) for people that have trouble with ProFTPD 1.3.3c Exploit and it says no backdoor planted or something like that

and you have the correct version just keep trying sometimes it won't work and when you do it a next time it works ok

Yeah, that vulnerability is the same as SQLi. Some are vulnerable, and some are not.

noober1001 - October 10, 2011, 4:54 am

Thank you so much for this.

It helped me.

Pro-Hackers - October 10, 2011, 4:58 am

i wrote in telnet:

o www.MYSIETEHERE.com 21

And then there comes this message:

220 ::ffff:87.230.106.64 FTP server ready

What should i do now?

markerr - October 10, 2011, 5:29 am

Very nice tutorial, what i was looking for, thank you!!!

Razor4x 5_0 - October 10, 2011, 5:42 am

Useful but you can spend 2 more words about telnet command for newbies ;)

Techie??? - October 10, 2011, 6:11 am

Nice tutorial. Will be helpful for many.

[H]ell - October 10, 2011, 6:33 am

Almost same as I posted a while back o_O

<http://www.exploit-news.com/2011/09/list-of-vulnerable-ftp-applications.html>

Hooded Robin - October 10, 2011, 6:40 am

You can also do this with ncat which comes installed with NMAP if you dont like messing with telnet or having to install additional services in W7 (just swap all instances of telnet for ncat in tut and you should be fine). Good tut for beginners!

zer0pwn - October 10, 2011, 9:46 am

(Oct 10, 2011 06:40 AM)Hooded Robin Wrote: [\[CITE\]](#) You can also do this with ncat which comes installed with NMAP if you dont like messing with telnet or having to install additional services in W7 (just swap all instances of telnet for ncat in tut and you should be fine). Good tut for beginners!

Ah, forgot about Netcat. I'll think about adding that :)

Crying - October 10, 2011, 1:06 pm

Really well explained,i already tried on some sites ,and these people dont seem to close 21port.Which is so bad.

Anything else besides Dictionary attack can be done?

LOL_KRIS - October 10, 2011, 4:58 pm

When im trying to connect it says Connection to host lost. Does that mean that the port inst open>?

Thunderwolf999 - October 10, 2011, 5:28 pm

Good job man very good tutorial for your new ones here at HF:)

unknown2 - October 16, 2011, 11:54 am

i founded a exploit of vsftpd 2.0.5,its in text form means codes,how to use it?

M0D3M - October 19, 2011, 3:01 pm

Yes, excellent tutorial. I definitely look forward to more of them.

jakesahir - October 23, 2011, 5:17 am

nice tutorial yaar...this is very helpful to me..

zer0pwn - November 3, 2011, 4:35 pm

Thanks guys!

I've seen a lot of questions regarding FTP Hacking, unfortunately nobody has seen this tutorial (At least, no one who NEEDS to see it). Hopefully this thread will get a little more popular, so there will be less questions.

viruzkillz23 - November 3, 2011, 6:24 pm

Thanks for this one Zer0, I'm actually learning this atm very helpful!

M0D3M - November 3, 2011, 6:57 pm

Excellent tutorial. I will be reading it more extensively tomorrow.

The Ion - November 3, 2011, 10:00 pm

very nice tut bookmarked it for furthur ones

this is a fantastic guide thank you alot if i could rep you i would brilliant tut for such good exploits

nice tutorial really nice :D<><><><><><><><><><>

Good tutorial for beginners. Keep it up. ?

Nice tutorial but thats why you need to ROOT the server using SSH Backtrack which can basically come through any firewall once doing that you can steal their source code , and passwords list if they have it in there database. Or you could always socially engineer the admin of the site and get his e-mail and get his HASH and try decrypting it to get his password anyways nice guide.

Good luck bruteforcing a secured server.

My server will nullroute your IP once you hit 7-8 wrong passwords. Currently going through the logs, taking the chinese out of the equation, I see atleast 5 nullrouted IPs per day, excluding the hundreds of attempts that come from China..

Also rooting is not as easy as some of try to make it.

Nice, well put together tutorial, thanks.

Well nice tutorial for beginners!
thanks!

Thanks for the tutorial
Very helpful

thanks for sharing this