

Forum:[Hack Forums](#)

Thread: [Exploit MSSQL Server Using Kali Linux Metasploit 5](#)

peterboss - May 1, 2019, 7:08 am

I've been trying to exploit a remote MSSQL Server with the help of Metasploit 5 In Kali Linux.

I got following information from the server:

Image Here: [i.imgur.com/IH5xVzG.png](#) (I'm New User And Not Allowed To Add Images ;(

My Questions:

1. The origin IP of website server is : XX.XXX.XX.68

But, Terminal got SQL information from IP: XX.XXX.XX.156 How and Why?

2. How I can proceed further to gain access to the MSSQL Server?

Thanks (New To MSSQL Exploit)

shelled - May 1, 2019, 9:59 am

Maybe don't use metasploit and understand if the mssql server is vulnerable.

jjonglaopi - May 2, 2019, 6:45 am

Two independent server(1.webserver 2.database server)

4444lastgamer - May 3, 2019, 9:07 pm

it's lol question, if you wanna try to hack mysql server then u hv to know if mysql server hv a vulnerability or not

nullcult - May 21, 2019, 7:04 am

(May 1, 2019 07:08 AM)peterboss Wrote: [\[CITE\]](#) I've been trying to exploit a remote MSSQL Server with the help of Metasploit 5 In Kali Linux.

I got following information from the server:

Image Here: [i.imgur.com/IH5xVzG.png](#) (I'm New User And Not Allowed To Add Images ;(

My Questions:

1. The origin IP of website server is : XX.XXX.XX.68

But, Terminal got SQL information from IP: XX.XXX.XX.156 How and Why?

2. How I can proceed further to gain access to the MSSQL Server?

Thanks (New To MSSQL Exploit)

Hi mate, not every MSSQL server will have ready vulnerabilities for you to exploit. Some times you need to look into things like misconfigurations.

1. Enumerate both smb and mssql usernames on your box.
2. Try bruteforce with common names.
3. Look into PowerSQL

Last_viking - May 22, 2019, 10:37 am

I'd suggest you to run nmap scan against the host.

And note down the version or build date

MySQL version 1.0.x has remote backdoor upload vulnerability

icebreacker - May 22, 2019, 2:33 pm

Hello ,

if you have the IP you can brute force the login .

Login: sa

Pass:whatever

Metasploit:

use auxiliary/scanner/mssql/mssql_login

set RHOSTS '127.0.0.1' =your_ip

set username 'sa' =sa=Admin Account for MSSQL_SERVER

set PASS_FILE 'massive_pwd_list.txt' =your PWDLISTE

set STOP_ON_SUCCESS 'true' =PASSWORD GOOD its stopping

set THREADS '5' =its the speed

run =start the tool

Best Regards .