

Forum:[Hack Forums](#)

Thread: [MSSQL | Attack Script | Scanner | Filter | Lists | FREE |](#)

vercenta - December 4, 2014, 6:26 pm

MSSQL | Attack Script | Scanner | Filter | Lists |
FREE

Introduction

Hi, I am releasing my MSSQL scripts to everyone for free, I am unsure of the payload of the public MSSQL script out there or if it works the same but I in no way stole anything from it as I have never even used that script before.

That being said, I wouldn't trust it either especially it being leaked.

So after seeing threads about people selling MSSQL for \$200-\$500 I decided to look up the protocol, turns out this exploit has been around since 2003 just seems to have been forgotten. I found the payload in about 10 minutes just browsing through pages... No packet sniffing required.

The payload is only 1 byte long:

Code x02

And it can receive a response up to 1300 bytes... Yup thats a 1300x AMP if you are lucky enough to find these servers.

There is not many of them so the odds of achieving that globally with a large list is pretty much impossible, most servers respond about 250 bytes.

So its roughly a 250x amplification method.

About The Scripts

I have included my Attack Script [C], Scanner [C] and Filter [PHP]

I have also thrown in some filtered and unfiltered lists.

There are really not many MSSQL servers in the world, they are about as rare as CHARGEN so you will need to scan for a long time, this list I provided should last a while though.

Don't forget to give permissions to binary files.

Code chmod 777 mssql

chmod 777 mssqlscan

Attack Script Usage

Code Usage: ./mssql [IP] [Port] [List] [Threads] [Time]

Scanner Usage

Code Usage: ./mssqlscan [Start Range] [End Range] [List] [Threads] [Scan Delay]

Filter Usage

Code Usage: php filter.php [Input.txt] [Output.txt] [Response Size]

-For educational purposes only!

Credits to LightSpeed for the original C scripts, I modified them for MSSQL payload.

[Download Here](#)

nbc_ - December 4, 2014, 6:51 pm

First post does this make me special? Will you love me now?

R?eece? - December 4, 2014, 6:56 pm

Not a 1300x amp.

This script is 10x amp. Ask anyone with common knowledge.

Hopefully they're not backdoored. Thanks though

It will amplify any attack 10x. 100Mbps to 1Gbps.

Yes it will amp that byte to 1300x IF you get 1300bytes. Thats why we dont say its a 1300x amp.

We put it all together. 10x amp.

Technically you're right with the 1 byte thing but thats just going to confuse people.

vercenta - December 4, 2014, 7:01 pm

(Dec 4, 2014 07:56 PM)R?eece? Wrote: [\[CITE\]](#) Not a 1300x amp.

This script is 10x amp. Ask anyone with common knowledge.

Hopefully they're not backdoored. Thanks though

It will amplify any attack 10x. 100Mbps to 1Gbps.

Actually If a packet is 1 byte and a response is 1300 bytes that makes it 1300x larger then the original request, being 1300x amplification for that particular server?

R?eece? - December 4, 2014, 7:02 pm

(Dec 4, 2014 08:01 PM)AncientMidgets Wrote: [\[CITE\]](#) Actually If a packet is 1 byte and a response is 1300 bytes that makes it 1300x larger then the original request, being 1300x amplification for that particular server?

Yes that is correct for that one byte. BUT overall its a 10x amp.

It will not amplify a 100Mbps server 1300 times.

vercenta - December 4, 2014, 7:02 pm

(Dec 4, 2014 07:51 PM)Nbc_ Wrote: [\[CITE\]](#) First post does this make me special? Will you love me now?

I've sent you the scripts enjoy?

(Dec 4, 2014 08:02 PM)R?eece? Wrote: [\[CITE\]](#) Yes that is correct for that one byte. BUT overall its a 10x amp.

It will not amplify a 100Mbps server 1300 times.

I never said it would lol

?

R?eece? - December 4, 2014, 7:04 pm

(Dec 4, 2014 08:02 PM)AncientMidgets Wrote: [\[CITE\]](#) I've sent you the scripts enjoy?

I never said it would lol

?

Then call it a damn 10x amplification otherwise people will think you will get 130Gbps out of a 100Mbps server.

ablationvector - December 4, 2014, 7:13 pm

If you can hook me up with this new fancih scriptz i would luv u with all my vagina

<3

nbc_ - December 4, 2014, 7:18 pm

Vouch for Ancient's scripts, works properly, etc etc etc.

Phenomite - December 4, 2014, 7:21 pm

Nice release but Post to PM is against forum rules.

Change this please.

vercenta - December 4, 2014, 7:24 pm

(Dec 4, 2014 08:21 PM)Phenomite Wrote: [\[CITE\]](#) Nice release but Post to PM is against forum rules.

Change this please.

Did not know that, I put the download link in the thread now?

R?eece? - December 4, 2014, 7:30 pm

Will you be giving out the .c version of the attack script?

Taranis - December 5, 2014, 12:56 am

You are mistaken in some of your assumptions, I have a list of millions and it works very well .

And ... 1300x amp ? Lol Hilarious ...

Furthermore, this is not the same payload of my script at all .

I will test it though and update soon about it

vercenta - December 5, 2014, 7:16 am

(Dec 5, 2014 01:56 AM)Transe Wrote: [\[CITE\]](#) You are mistaken in some of your assumptions, I have a list of millions and it works very well .

And ... 1300x amp ? Lol Hilarious ...

Furthermore, this is not the same payload of my script at all .

I will test it though and update soon about it

- 1) Go into calculator
- 2) Divide 13,000 by 1
- 3) Answer is 1300x

Hope I helped?

By the way, if you use a different payload that makes it less amplification because my payload is only 1 byte :)

Taranis - December 5, 2014, 7:22 am

(Dec 5, 2014 08:16 AM)AncientMidgets Wrote: [\[CITE\]](#) 1) Go into calculator

- 2) Divide 13,000 by 1
- 3) Answer is 1300x

Hope I helped?

As other ppl already stated, you show you totally lack understanding of how amplification works.

Furthermore, this script is not even using the right payload that will match both my script and Horny

method.

Go research again and come up with a new one plz :) You got it totally wrong sorry to tell you

Lmk when it s working

Btw, the method isn t really about the amp factor ...

vercenta - December 5, 2014, 7:48 am

(Dec 5, 2014 08:22 AM)Transe Wrote: [\[CITE\]](#) As other ppl already stated, you show you totally lack understanding of how amplification works.

Furthermore, this script is not even using the right payload that will match both my script and Horny method.

Go research again and come up with a new one plz :) You got it totally wrong sorry to tell you

Lmk when it s working

Btw, the method isn t really about the amp factor ...

Hi Transe, since you don't seem to be very educated in the SST I will help you out.

What is amplification?

The ratio of the sized response compared to the sized request.

Why are you so confused by that? You think 1300x potential from a few servers automatically means 130Gbps? You have no idea what you are talking about.

Please read a book.

Also I'm not using the same payload??? thats fine, if your payload is anything more then 1 byte then it is mathematically a worse amplification ratio then mine.

Enjoy my scripts though bro.

ablationvector - December 5, 2014, 8:45 am

Transe seems to go butthurt on people who post this MSSQL attack method out.

"Oh this isn't my method, mine is better"

Anyone can tell thats BS.

@OP

Thanks for your generosity, keep up the work.

??s†??B?? ? - December 5, 2014, 8:56 am

Vouch for AncientMidgets!

Well working product. Well done mate... ?

B?wseR - December 5, 2014, 9:34 am

Thanks for the scripts will post back when i get to test them on how well they do.

vercenta - December 5, 2014, 9:34 am

(Dec 5, 2014 09:45 AM)Dominate Humbly Wrote: [\[CITE\]](#) Transe seems to go butthurt on people who

post this MSSQL attack method out.

"Oh this isn't my method, mine is better"
Anyone can tell that's BS.

@OP

Thanks for your generosity, keep up the work.

I feel kind of bad for Transe honestly, he paid \$300 to have a MSSQL script modified for him (and probably hoping to make some profit on it) and then it was leaked. So that does suck for him, I don't see why he has to hate on EVERYONE though.

But his version can't be 'better' because if the max byte response for a MSSQL server is 1300, and he has a different request payload, that means he's sending more data that was not even needed to be sent creating a lower amp factor.

?icK - December 5, 2014, 9:35 am

thakns for this op going to use this right now.

vercenta - December 7, 2014, 12:22 pm

Let me know if you guys need help with the scripts?

Dwynr - December 8, 2014, 5:03 am

Thanks dude, this is awesome! Really helpfull, gonna try this out..

ItsFluffy - December 8, 2014, 4:48 pm

i just want to say i appreciate threads like this
you explain what it is, offer the item and explain how to use it
it's very much appreciated so thanks

ReaperRowRead - December 9, 2014, 8:42 pm

awesome this will do thanks Op.....

askarne - December 11, 2014, 1:38 pm

The link seems to be dead. Reupload please?

vercenta - December 15, 2014, 1:24 am

(Dec 11, 2014 02:38 PM)askarne Wrote: [\[CITE\]](#) The link seems to be dead. Reupload please?
I have re-uploaded the scripts enjoy!

vercenta - December 17, 2014, 8:33 pm

Here is a MSSQL list I scanned recently, has over 110k lines.

<https://www.dropbox.com/s/9g4ymjh7mtx58nk/mssql.txt?dl=0>

BlackLayer - January 8, 2015, 12:20 pm

T Th Tha Than Thank Thanks 1000x

[img]<http://e.deviantart.net/emoticons/moods/love/lust/passionate.gif>[/img]

vercenta - January 8, 2015, 11:46 pm

(Jan 8, 2015 01:20 PM)0011101000101001 Wrote: [\[CITE\]](#) T Th Tha Than Thank Thanks 1000x
[img]<http://e.deviantart.net/emoticons/moods/love/lust/passionate.gif>[/img]

No problem, enjoy the scripts bud ?

ItsFluffy - January 9, 2015, 12:49 am

(Jan 9, 2015 12:46 AM)AncientMidgets Wrote: [\[CITE\]](#) No problem, enjoy the scripts bud ?
just wish this wasn't patched on so many servers you know

Taranis - January 9, 2015, 1:33 am

(Jan 9, 2015 01:49 AM)ItsFluffy Wrote: [\[CITE\]](#) just wish this wasn't patched on so many servers you know

Say thanks to all the idiots leaking it ?

People don't understand basic things such as certain kind of information being leaked is not gonna help anyone except ppl outside forum .

Same for the host killed by Clubs idiot lol

ItsFluffy - January 9, 2015, 1:41 am

(Jan 9, 2015 02:33 AM)Transe Wrote: [\[CITE\]](#) Say thanks to all the idiots leaking it ?

People don't understand basic things such as certain kind of information being leaked is not gonna help anyone except ppl outside forum .

Same for the host killed by Clubs idiot lol

clubs arrogance far surpasses that of this script being released, just saying

vercenta - January 9, 2015, 10:34 am

(Jan 9, 2015 02:33 AM)Transe Wrote: [\[CITE\]](#) Say thanks to all the idiots leaking it ?

People don't understand basic things such as certain kind of information being leaked is not gonna help anyone except ppl outside forum .

Same for the host killed by Clubs idiot lol

This was a release not a leak.

And did you really think MSSQL would still be effective on OVH even if only some stressers used it? You realize that when these servers gets hit there is logs that will indicate what port the attack came from revealing it's MSSQL/NTP/SSDP.

You can also just look at the STS and 99% of owners will put the "fancy" methods in there thread title for advertisement purposes, OVH admins could easily look at HF and save time instead of going through logs.

If you really want a unused method then find another payload, there are a lot of UDP ports out there.

ItsFluffy - January 9, 2015, 7:38 pm

midgets is quite accurate in his reply

one thing ovh dos well, better than others is adapt

their I7 is probably the worst in the market but their adaptation and I4 protection in general is superb hence them being top dog for the most part

every method gets leaked at some point but it's whether the leak has purpose or it's to be a "vigilante" leak of sorts

darkreign - January 13, 2015, 3:10 pm

could we get this compiled for 32bit? seems to only run on 64bit systems!

BlackLayer - January 13, 2015, 5:09 pm

(Jan 13, 2015 04:10 PM)darkreign Wrote: [\[CITE\]](#) could we get this compiled for 32bit? seems to only

run on 64bit systems!

Recommend using CentOS 6.6 final x86_x64 without problems.

darkreign - January 13, 2015, 9:44 pm

(Jan 13, 2015 06:09 PM)0011101000101001 Wrote: [\[CITE\]](#) Recommend using CentOS 6.6 final x86_x64 without problems.

I know it works on 64bit systems, as I said, I was hoping for the 32bit binary because not every root that spoofs runs a 64bit OS lol..

BlackLayer - January 14, 2015, 5:34 am

(Jan 13, 2015 10:44 PM)darkreign Wrote: [\[CITE\]](#) I know it works on 64bit systems, as I said, I was hoping for the 32bit binary because not every root that spoofs runs a 64bit OS lol..

I knew, him should complie compatibly 32bit and 64bit stable. or anyway always 64 bit ?

pwn4life - January 14, 2015, 5:56 am

Exec format error need help im running lubuntu

BlackLayer - January 14, 2015, 5:59 am

(Jan 14, 2015 06:56 AM)pwn4life Wrote: [\[CITE\]](#) Exec format error need help im running lubuntu Ubuntu are shit because not stable programming C, recommend using CentOS or Red Hat or Fedora.

vercenta - January 14, 2015, 7:41 am

(Jan 14, 2015 06:56 AM)pwn4life Wrote: [\[CITE\]](#) Exec format error need help im running lubuntu As 0011101000101001 has already stated, use Centos 64bit ?

BlackLayer - January 14, 2015, 7:48 am

(Jan 14, 2015 08:41 AM)AncientMidgets Wrote: [\[CITE\]](#) As 0011101000101001 has already stated, use Centos 64bit ?

Yea that's good CentOS 64 bit. 

J?son - March 15, 2015, 8:40 am

(Jan 13, 2015 04:10 PM)darkreign Wrote: [\[CITE\]](#) could we get this compiled for 32bit? seems to only run on 64bit systems!

Ever since i heard you could modify the chargen script and turn it into the MSSQL flooder, i switched out the payloads

<http://pastebin.com/RsYN9wYs>

vercenta - March 15, 2015, 2:01 pm

(Mar 15, 2015 08:40 AM)Laertes Wrote: [\[CITE\]](#) Ever since i heard you could modify the CHARGEN.c amplification ddos script and turn it into the MSSQL flooder, i began to tinker around with the chargen sauce and BEHOLD I MADE A .C VERSION YOU CAN COMPILE EVERYWHERE. NOBODY SHOULD BE PAYING MONEY FOR THIS SCRIPT AND I WILL SHARE IT FOR EVERYONE TO USE. MUAHAHAHA. ?

pastebin.com/RsYN9wYs

Congrats but nobody has been paying for MSSQL for a very long time so idk what you're talking about.

J?son - March 15, 2015, 2:05 pm

(Mar 15, 2015 02:01 PM)ArchNME Wrote: [\[CITE\]](#) Congrats but nobody has been paying for MSSQL for a very long time so idk what you're talking about.

Good and im glad to hear it, last I saw on IRC, people were paying 10-30\$ for this script and that just makes me sad.

mrxd - *November 29, 2017, 2:39 pm*

no work for download linke