

Forum:[Hack Forums](#)

Thread: [Anyone good with Python here?Question:Remove Nullbytes from shellcode?](#)

Nightmare - January 8, 2024, 11:17 pm

Can anyone help me out with this?

I made this code for remove null bytes from shellcode(it's not complete but it is a start),i want to do it kinda like metasploit does?

```
Code # Import necessary modules
import sys
```

```
# Read the shellcode binary file
with open('shellcode.bin', 'rb') as file:
    shellcode = file.read()
```

```
# Filter out null bytes from the shellcode
filtered_shellcode = b''.join(byte for byte in shellcode if byte != b'\x00')
```

```
# Save the filtered shellcode to a new file
with open('filtered_shellcode.bin', 'wb') as file:
    file.write(filtered_shellcode)
```

an4l 1st - January 9, 2024, 5:47 am

Dear honorable and respectable Fallen member,

I am sorry the delay on answering your question. I only saw it now.
I will do my best to help you, my fellow partner.

no, removing null bytes from shellcode requires asm knowledge...
chat gpt cant help you there...

for example:

Code mov eax, 0
this generates null bytes:

Code B800000000
so you need to make eax 0 but without generating null bytes...

Code xor eax, eax
this generates

Code 31C0
no 00 bytes...

or lets say you wanna mov a specific value to a register...

Code mov eax, 0x50

Code B850000000 (no good, null bytes)...

but

Code push 0x50
pop eax
gives

Code 6A5058
no null bytes...

I dont know if there is any automated tool to do that.. I dont know anyone specifically... there must be something...

I find it hard to exist some tool in python that can do this automatically because this will certainly change the offsets and the instructions will need to be recompiled so the calls, jmp and jnc still works...

the change would have to be performed in the source code.. anyway this would be a big project to automate and honestly... for a string buffer overflow with a possible limited number of charactes.. it is easier to edit the shellcode manually...

Nightmare - January 9, 2024, 6:16 am

(Jan 9, 2024 06:47 AM)Threat Actress Wrote: [\[CITE\]](#) Dear honorable and respectable Fallen member,

I am sorry the delay on answering your question. I only saw it now.
I will do my best to help you, my fellow partner.

no, removing null bytes from shellcode requires asm knowledge...
chat gpt cant help you therrere...

for example:

Code mov eax, 0
this generates null bytes:

Code B800000000
so you need to make eax 0 but without generating null bytes...

Code xor eax, eax
this generates

Code 31C0
no 00 bytes...

or lets say you wanna mov a specific value to a register...

Code mov eax, 0x50
Code B850000000 (no good, null bytes)...

but

Code push 0x50
pop eax
gives

Code 6A5058
no null bytes...

I dont know if there is any automated tool to do that.. I dont know anyone specifically... there must be something...

I find it hard to exist some tool in python that can do this automatically because this will certainly change the offsets and the instructions will need to be recompiled so the calls, jmp and jnc still works...

the change would have to be performed in the source code.. anyway this would be a big project to automate and honestly... for a string buffer overflow with a possible limited number of charactes.. it is easier to edit the shellcode manually...

Thank you for your answer to the point,the chat gpt part wasn't needed i think!Thank you anyway for pointing to the ight direction my friend!!

an4l 1st - January 9, 2024, 7:04 am

Indeed, my friend. I am sorry if I sounded rude about "chat gpt".

Nightmare - January 9, 2024, 7:36 am

(Jan 9, 2024 08:04 AM)Threat Actress Wrote: [\[CITE\]](#) Indeed, my friend. I am sorry if I sounded rude about "chat gpt".

No you did not my brother,the opposite you give me a good direction and helped me to see!Thank you very much!Don't worry !