

Forum:[Hack Forums](#)

Thread: [Need some help with a buffer overflow exploit](#)

ernestmiller - September 29, 2019, 2:00 pm

I need some help creating an exploit for a buffer overflow.

Message me for the application or scripts source code.

The code is very simple its nothing complex at all im just a complete beginner in this aspect of pen testing

Abducted - September 30, 2019, 6:00 am

I guess I could help you with that.

ernestmiller - September 30, 2019, 6:45 am

Cool thanks bud mind if i send you the C code as well as the exploit im working on as well

Abducted - September 30, 2019, 7:26 am

(Sep 30, 2019 06:45 AM)ernestmiller Wrote: [\[CITE\]](#) Cool thanks bud mind if i send you the C code as well as the exploit im working on as well

Sure, go ahead.

ernestmiller - September 30, 2019, 7:27 am

im pretty sure i messaged you already with it, although its not in my sent messages have a check of your inbox

Dont worry I have now managed to compile the source code however if you would like to help me write a exploit for it id be grateful :)

Abducted - September 30, 2019, 11:46 pm

(Sep 30, 2019 07:27 AM)ernestmiller Wrote: [\[CITE\]](#) im pretty sure i messaged you already with it, although its not in my sent messages have a check of your inbox

Dont worry I have now managed to compile the source code however if you would like to help me write a exploit for it id be grateful :)

Yeah sure go ahead.

ernestmiller - October 1, 2019, 5:45 am

I have managed to pop a calculator but cant seem to get my reverse shell to work from my kali vm
Done it everyone!!! First buffer overflow exploited with a reverse meterpreter payload!!! woohoo
Got damn it the exploit worked fine in Windows but on the Linux machine I get

```
root@kali:~/Desktop# proxychains python exploit.py
```

```
ProxyChains-3.1 (http://proxychains.sf.net)
```

```
[S-chain]-<>-127.0.0.1:1080-<><>-10.185.10.55:42424-<--denied
```

```
Traceback (most recent call last):
```

```
File "exploit.py", line 8, in <module>
```

```
s.connect((ServiceManagerIP, ServiceManagerPort))
```

```
File "/usr/lib/python2.7/socket.py", line 228, in meth
```

```
return getattr(self._sock,name)(*args)
```

```
socket.error: [Errno 111] Connection refused
```

