

Forum:[Hack Forums](#)

Thread: [I Would Like To Learn How To Exploit Software Via Memory Corruption -Buffer Overflows](#)

Demoralise - February 12, 2014, 12:09 am

I want to learn how to manually penetrate software and make a command/instruction be run outside of the default sandbox by corrupting/confusing the sandbox and making the command/instruction be ran in a vulnerable area of the software's memory by overflowing it into a different stack/buffer where it will be executed and injected on the computer with the software installed.

herpface - February 12, 2014, 12:45 am

Is there a question in there somewhere? I'm confused.

Goodies - February 12, 2014, 12:49 am

Some I've written:

Simple BOF + ASLR Bypass via Brute Force:

<https://hackforums.net/showthread.php?tid=3997977>

BOF Using Ret2Reg:

<https://hackforums.net/showthread.php?tid=3999106>

I also have some on writing linux shellcode.

Demoralise - February 13, 2014, 9:06 pm

(Feb 12, 2014 01:49 AM)Goodies Wrote: [\[CITE\]](#) Some I've written:

Simple BOF + ASLR Bypass via Brute Force:

<https://hackforums.net/showthread.php?tid=3997977>

BOF Using Ret2Reg:

<https://hackforums.net/showthread.php?tid=3999106>

I also have some on writing linux shellcode.Thank you Goodies :) Much appreciated.