

Forum: [Hack Forums](#)

Thread: [Linux C++/C DLL injection + Code Injection Tutorial](#)

g4143 - February 17, 2012, 7:12 am

I was planning on making a four part tutorial on DLL/Code injection on a GNU/Linux system. The tutorial would expect some knowledge of DLLs, TCP/IP, threading and general assembler. The breakdown follows:

Part One - DLL injection on a GNU/Linux system.

Part Two - Preparing the injected code for both 32/64 bit GNU/Linux systems.

Part Three - Creating the TCP/IP client to transmit the injected code.

Part Four - Expanding part one code to include a thread executing a TCP/IP server.

Note: The code will be general enough that you could use it for a boiler plate for other purposes.

If your interested, please respond here.

Part One Link - <https://hackforums.net/showthread.php?tid=2222016pid=20043622#pid20043622>

Part Two - <https://hackforums.net/showthread.php?tid=2228260>

Part Three - <https://hackforums.net/showthread.php?tid=2236966>

Part Four - <https://hackforums.net/showthread.php?tid=2237772>

Guaschman - February 17, 2012, 7:30 am

Well, why not?

I just downloaded Ubuntu so that's perfect for me!

madhanmech - February 17, 2012, 8:14 am

this would be great ... i'm really looking forward for this... thanks in advance :)

vive facile - February 17, 2012, 10:55 am

What exactly do you mean by DLL code injection on a GNU system? You're a writing a program that runs on linux that will infect a windows system? Or a program that will infect a GNU library (dll is a windows term)?

g4143 - February 17, 2012, 12:12 pm

(Feb 17, 2012 11:55 AM)mattymatt Wrote: [\[CITE\]](#) What exactly do you mean by DLL code injection on a GNU system? You're a writing a program that runs on linux that will infect a windows system? Or a program that will infect a GNU library (dll is a windows term)?

It has nothing to do with infecting, it has to do with injecting your DLL in favor of the programs default DLL..

oprchniki - February 17, 2012, 12:36 pm

I would be interested. I've never seen a tutorial for non-Windows dll injections, and I expect they're much harder to find.

tulamba - February 17, 2012, 2:06 pm

g4143 is my guru. I have learnt a lot discussing with him (not arguing). Looking forward to your tutorial. If i can do any thing, please feel free to involve me.

Thanks
tulamba

Nichole - February 17, 2012, 2:16 pm

I'm up for any tutorial you have to offer g4143! Learn so much from you on here. Can't wait.

vive facile - February 17, 2012, 2:25 pm

(Feb 17, 2012 01:12 PM)g4143 Wrote: [\[CITE\]](#) It has nothing to do with infecting, it has to do with injecting your Dll in favor of the programs default Dll..

I'm still confused as to whether your injecting a linux library or a windows dll. There are no "DLL"s in linux.

oprchniki - February 17, 2012, 2:34 pm

Linux doesn't use the .dll extension, and obviously the file format would be different. But dynamic linkage is supported by the kernel in what they call shared objects (.so files). I don't know if that's what g4143 is referring to.

betamonkey - February 17, 2012, 3:04 pm

I'd be interested in reading it. I've been doing a lot of security-related programming lately so this would definitely be something I would like to read up on.

g4143 - February 17, 2012, 3:16 pm

To clear up some confusion..I'm creating a tutorial on Dll injection on GNU/Linux systems. I use the term Dll because its used generically for all dynamic libraries.

So to clarify. I'll be giving a tutorial on shared object injection on GNU/Linux systems and eventually code injection.

vive facile - February 17, 2012, 3:22 pm

(Feb 17, 2012 04:16 PM)g4143 Wrote: [\[CITE\]](#) To clear up some confusion..I'm creating a tutorial on Dll injection on GNU/Linux systems. I use the term Dll because its used generically for all dynamic libraries.

So to clarify. I'll be giving a tutorial on shared object injection on GNU/Linux systems and eventually code injection.

I would be interested in seeing that. I was confused because a DLL is not used generically, it's strictly a windows a term, and most of the people here don't run linux or develop mainly on a linux system. This is for C++ I'm assuming?

g4143 - February 17, 2012, 3:57 pm

(Feb 17, 2012 04:22 PM)mattymatt Wrote: [\[CITE\]](#) I would be interested in seeing that. I was confused because a DLL is not used generically, it's strictly a windows a term, and most of the people here don't run linux or develop mainly on a linux system. This is for C++ I'm assuming? Eventually this will be for C/C++/Bash/Python/Perl...etc. It should work for any script/executable that's runnable on a GNU/Linux system. I just check it on a python script and it worked, I also checked it on a bash script and it worked, I also checked on a perl script and it worked and it always worked on a C/C++ executable.

Gh0st-Zer0 - February 17, 2012, 5:25 pm

Just read it from here:

<http://www.codeproject.com/Articles/33340/Code-Injection-into-Running-Linux-Application>

Simply better explanation from an official engineer!

g4143 - February 17, 2012, 5:35 pm

(Feb 17, 2012 06:25 PM)Gh0st-Zer0 Wrote: [\[CITE\]](#) Just read it from here:

<http://www.codeproject.com/Articles/33340/Code-Injection-into-Running-Linux-Application>

Simply better explanation from an official engineer!

Yes I read this, it uses the debugger to inject the code...I use a simpler approach with LD_PRELOAD.