

[REVS] Introduction to Shellcoding for Overflows Exploiting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0039.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/15/04

To: list@securiteam.com

Date: 15 Mar 2004 09:45:22 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Introduction to Shellcoding for Overflows Exploiting

SUMMARY

This paper will introduce the reader to the shellcoding and the study of buffer overflows; are required a Linux system (with GCC and GDB), and a superficial knowledge of C and ASM programming. We will talk about shellcodes x86 for Linux and we will explain to you how to write a simple rootshell (Note: shellcodes for Linux are different from BSD or Windows shellcodes, so they will be used only on Linux systems).

DETAILS

The document linked below will guide the reader in the creation of a shell code from the source C code to a string ready to use in exploits. The document requires no prior knowledge of shellcoding, and basic C and assembler knowledge.

Abstract:

General knowledge:

A buffer is a static array (with a prefixed size) that is loaded on the stack. A buffer overflow occurs when there is an array's data discharge; that happens when there are programming errors. In fact a lot of programs

Securiteam: [REVS] Introduction to Shellcoding for Overflows Exploiting

don't check variables size. We will insert the shellcode in the stack with a strings copy function, called STRCPY and we will execute /BIN/SH with the function EXECVE. (Note: String based shellcodes can't use the character 0 (NULL), because for the STRCPY function, the end of a string is identified by a 0, and if the 0 appears in the middle of the shellcode, only part of it will be loaded to the memory).

ADDITIONAL INFORMATION

The information has been provided by <mailto:nemesis@blackangels.it > Nemesis.

The complete papaer can be found at:

<<http://www.blackangels.it/Files/Papers/introshellcoding.txt>>
<http://www.blackangels.it/Files/Papers/introshellcoding.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.