Jonathan Déchaux

Secure Programming

TP: Format String attacks

Goal: The goal of this exercise is:

1) Try different examples of format string on three different systems.

Notation

For this TP, you need to put everything you made and explain everything. You have to make screenshots, good details and explanations.

Summary

Remember the following example

```
#include <stdio.h>
void main(int argc, char **argv)
{
	char outbuf[512];
	char buffer[512];
	sprintf(buffer, "ERR Wrong command: %.400s", user);
	sprintf(outbuf, buffer);
}
```

The bad use of the second *Sprintf* function with a shellcode can allow a bufferoverflow, just by using the wrong prototype of the function.

XP Virtual Machine and Windbg

Memory leak with Printf

Try both following codes:

Example 1:

```
#include <stdio.h>
void main(int argc, char **argv)
{
	printf(argv[1]);
}
```

Example 2:

```
#include <stdio.h>
void main(int argc, char **argv)
{
	printf(“%s\n”, argv[1]);
}
```

Understand the difference

Which code showed above is working? Which is the right format to print the argument?

Crashing your program

By taking the example 1, try your executable with the argument: “%s”.

How many %s do you need to crash your program?

Explain why your program is crashing.

Explain the usage of the argument %s with the *Printf* function.

Verify your informations with WinDBG. Explain your procedure.

Viewing the stack

Now try your executable with the argument: “%08x”.

What is the information displayed on the screen?

How many %08x arguments are needed to view the important informations like SAVED EBP and SAVED EIP?

Explain the usage of the argument %x with the *Printf* function.

Verify your informations with WinDBG. Explain your procedure.

Overwriting the memory

Example 3:

```
#include <stdio.h>
void main(int argc, char **argv){
        int bytes;
        printf(“%s%n\n”, argv[1], &bytes);
        printf(“You input %d characters\n”, bytes);
}
```

Try the example 3 with an argument.

What is the process used by the function *Printf* to overwrite the memory?

Verify your informations with WinDBG. Explain your procedure.

Linux and GCC

Try all previous examples on your Linux environment.

What is the difference with the XP environment? Explain.

Windows 7 and Visual Studio

Try all previous examples on your Windows 7 environment with Visual Studio.

What are the differences with the XP and Linux environments? Explain.