Assignment 4

Due 11:59PM, April 6, 2017

In this assignment, you will have an opportunity to write an exploit to remotely gain control on a host using SEH overwrite technique.

Attack Scenario

The **victim machine** is a Windows 7 machine that has a vulnerable Winamp player installed. This version of Winamp has a vulnerability when parsing a skin file. The Winamp is compiled with stack guard. The structure of a Winamp skin file to trigger the buffer overflow vulnerability is given. You will need to write an exploit generator for this target. Your exploit will be a crafted skin file which will be opened by the victim on the target machine. Upon successful exploit, it will return a shell to the attack machine at IP address: **10.247.49.140 and port 4444**.

You need to develop the exploit on your own laptop like we did in the class. Then submit your working exploit that can return a shell to the attack machine.

Setup Environment

The image of the Windows 7 with the vulnerable Winamp can be downloaded from the following link: https://drive.google.com/open?id=0BzkPm4m1AGy4N3Z4TldfNXRudlU

1. Download the **win7.ova** file and import it to your VMware software.
2. Login to the Windows 7 virtual machine with username: ***victim***, and password: **password**.
3. The Winamp program can be found under path: *C:\Program Files\Winamp* (should also be accessible through the Start Menu)
4. The skin file of Winamp is placed under *C:\Program Files\Winamp\Skins\Bento\scripts*
5. Develop the exploit, make it work on your local laptop.
6. Adjust your exploit to use the payload for returning the shell to the attack machine and submit your program with a report.

You will need a debugger to observe the crashed program and gather important information for developing your exploits. The WinDBG debugger is already installed on the VM. Below are some useful WinDBG commands. In this task, you will need use WinDBG for debugging. You can find WinDBG command-line options from this link: https://msdn.microsoft.com/en-us/library/windows/hardware/ff561306(v=vs.85).aspx

- **r**: show register values
- **db/dd/dc ADDRESS/REG**: dump memory content starting at ADDRESS, or location pointed to by register REG, or dump characters
- **g**: begin/continue execution
- **s ADDRESS l LENGTH PATTERN**: search memory for PATTERN, starting from ADDRESS for LENGTH bytes

- **bp ADDRESS**: set a breakpoint at ADDRESS
- **a/u ADDRESS**: assemble/disassemble instructions starting at ADDRESS
- **!exchain**: show the chain of exception handlers
- **dda ADDRESS**: dynamic dump assembler
- **kb**: show call stack
- **lm**: display address ranges for loaded modules (*e.g.* DLL's)
- **?**: help

The command to execute the NARLY extension in WinDBG for listing all the shared library is:

```
> !load narly
> !nmod
```

You might need to search for the "jump code" in shared library to execute your shellcode. Here is the Metasploit command for searching for jump code:

```
$ msfpescan –j esp [file_to_be_scanned]
$ msfpescan –p [file_to_be_scanned]
```

For generating shellcode, you will need to use Metasploit. Use the payload **windows/shell_reverse_tcp** with encoder **x86/alpha_mixed**.

You might also need tools such as **pattern_create.rb** and **pattern_offset.rb,** which you can find in the following path under Kali: */usr/share/metasploit-framework/tools/exploit/*

Submission

For this assignment, you shall submit the following:

- Source code of the exploit generator.
- A document that shows how to compile/run your exploit generator, and your process of developing the exploit and the thinking behind the conclusions you draw when observing the program's behaviors, so that someone else who has not done it can follow the document to develop the same exploit as well.
- **We will test your exploit on the attacking machine. So please make sure your exploit works there before submitting**. Your reverse shell shall be sent to at the attack machine **under port 4444**.

Note

- Winamp uses a very long buffer for skin file. To crash the buffer you might need to create a string that is around 20000 characters.
- You will need to file a way to copy files from the Windows 7 VM to the Kali box. If you use a Unix-family laptop you can use scp. (http://www.hypexr.org/linux_scp_help.php). If your laptop is Windows, you can use putty (http://www.putty.org/).