COMP8053 Embedded Software Security – Assignment 1

Answer **all** questions. Submit your answers in a single pdf file through the submission facility on Canvas in "Assignments -> Assignment 1 Submission". The assignment is due at 23:59 on November 15th. Penalty-free late submission allowed until 23:59 November 29th. **Note that submissions from Nov 30th onwards will receive a mark of 0.**

For questions 1-4 you **must provide a description of the process taken to solve the problem**. This description should explain what actions you took and why you did them. Start by giving an overview of the approach you intend to take, then provide step-by-step descriptions of the actions taken to achieve that approach. Write as if your target audience is a computer scientist but with no security background (i.e. they know how to operate a computer and what the stack/heap are, but not what a buffer overflow attack is).

It is **required** that you use **screenshots** to help illustrate this description. In the Lab computers on Windows, the "Snipping Tool" can be used to take pictures of part of the screen.

For example:

Sample Command (should be screenshotted along with the relevant output included in the image): x\24x $esp

Sample explanations for why:

I used it to show the stack. **(BAD – this is what you did, not why you did it)**

I used it to show the contents of the top 24 addresses on the stack, in order to identify the exact location of the buffer and calculate how much overflow was necessary to write over the return address. Changing the return address allowed me to redirect the program execution and…. **(GOOD! – here the purpose of using a command to show the stack is explained!)**

Question 1 – [10 Marks]

Download the 3 Firmware binaries, named “Firmware1.bin”, “Firmware2.bin” and “Firmware3.bin” in “Units -> Marked Assignment” on Canvas. For these 3 binaries, you must do the following:

1. Locate a private cryptographic key stored as plaintext in 2 of the firmware binaries.
2. Locate login credentials for a remote connection (e.g. ssh, telnet, https, etc..) in one of the firmwares. Note that you must make sure you find the full login name and password combination (not merely a variable for either of them, if it is part of a script).

You may use any of the tools we used in the labs to assist in your search. You may also use any of linux’s built-in commands to assist you (e.g. ‘grep’ to search files). Remember you can type “man <linux command>” to get instructions on how to use linux commands if you are unsure. You may not use any other types of tools than these.

For questions 2-4, you will need to download the relevant C program file and copy it into the Protostar virtual machine. This can be done on Linux machines by using the "scp" (secure copy) command. For the Windows machines in the lab, PuTTY includes its own version of "scp" in the file "pscp.exe" located in the PuTTY installation directory. To use it, open a command prompt (start menu -> type in "cmd.exe") and navigate to the PuTTY installation directory. From there, type the following command:

```
pscp <filename> user@<ip address>:/home/user/
```

Where <filename> is the name of the C program file you are copying over, and <ip address> is the IP Address of the Protostar VM you are running (get it by typing "ip addr" inside the Protostar VM). This will create a copy of the file inside the /home/user/ directory on Protostar (the default starting directory).

Next you must compile the C program, with the following command:

```
gcc <filename> -o <outfile name>
```

Where <filename> is the name of the C program file, and <outfile name> is your name for the compiled binary. You can then run the compiled binary by typing:

```
./<outfile name>
```

Contact me if you have any difficulties in copying over and compiling the C programs!

Question 2 – [25 Marks]

For this question, you will use the program "Question2.c" available in "Units -> Marked Assignment". You must make the program output **both** "Achieved 1/2!" and "Achieved 2/2!" in a **single run** of the program.

Question 3 – [25Marks]

For this question, you will use the program "Question3.c" available in "Units -> Marked Assignment". You must overcome the cruel marking scheme and make the program output "Grade of 100 assigned." (Note: making it output "Grade of 100 assigned" does not guarantee you will get 100% on this assignment).

Question 4 – [25Marks]

For this question, you will use the program "Question4.c" available in "Units -> Marked Assignment". You must cause the program to execute the printf() function on line 16 in the goal() function, and output "You reached the goal!".

Question 5 – [15Marks]

a) *Buffer Overflow Attacks* (or Stack Smashing) are a type of attack in which an attacker injects shellcode onto the stack (probably utilising a NOP slide too), and then redirects the flow of the program to execute the shellcode. **Describe** what is meant by *Canaries* and give a **detailed explanation** of how canaries might mitigate or prevent a buffer overflow attack of the type described.

b) *Format String Exploits* take advantage of improperly used function calls for format strings. They allow an attacker to read and write from memory, potentially leading to complete compromise of a system. **Describe** what is meant by *ASLR* and give a **detailed explanation** of how it might mitigate or prevent a Format String Exploit, *in the context of embedded devices*.