Secure Programming Laboratory 1: Introduction

SP Demonstrators: Arthur, Margus, Connie, David

23rd January 2018
This is the first Laboratory Session for **Secure Programming**

It is convened by Arthur, Margus, Connie and David.

Please take a copy of the **handout**. It is also available online via the **course web page**.
What is this lab about?

There are 3 exercises showing some basic stuff and tools in security plus 1 simple buffer overflow exercise at last to prepare you for the next lab.

- **Exercise 1.** Unix Permissions.
- **Exercise 2.** Tools and GDB Debugger.
- **Exercise 3.** Memory Allocation.
- **Exercise 4.** Simple Buffer Overflow.

The exercises are based on executable and source files provided in a Virtual Machine running Linux.
What do we hope you will learn?

- Understanding (or revising) the permission model of Unix/Linux
- Use of some simple tools to help investigate or find flaws
- Investigate memory allocation and crashing of programs
- Understanding basic vulnerability analysis and prepare yourself for the future labs
Resources

➢ Use **anything**! You are encouraged to search on the web for help, tutorials, manuals, etc.

➢ You can get plenty of help this way. But it is probably more rewarding to try to solve the exercises for yourself first. Make sure to spend time experimenting, not only reading.

➢ **Warning**: experiment with care! If you download sample exploits, generation tools, etc, install and run these in the Virtual Machine, **not on the host DICE environment**. The VM already has several interesting tools provided.

➢ **Ask us!** We are here to help, as much as we can.

➢ **Ask each other!** There may be expert x86 programmers, C hackers, exploit developers(?) among you...
You may not have time to complete all exercises in this lab session.

▶ Don’t worry!
▶ Try attempting and understanding all the checkpoint questions before skipping sections.
▶ Exercise 2 involves knowledge of different tools which will be handy in future labs
▶ Of course, you can spend more of your own time later if you are interested. Completing the lab is desirable but not essential: at least, try to look at each exercise a little bit, and review the solutions when they are released. The important thing is to understand the concepts well.
Recording your work

Each exercise has a series of Checkpoints which are questions that you can provide brief answers to. A plain text file checkpoints.md is provided, please fill this in as a record of your work.

The main point of the checkpoints is for you to check your own understanding, so please don’t spent time writing long or very polished answers!

You may continue working on the lab in your own time. We will publish the solutions on the lab page on Monday 29th Jan.

In later labs we will accept checkpoint files submitted with the submit command and provide feedback on them at the next lab.
During the lab we will provide individual help and guidance, and also make announcements during the lab with hints and tips.

We will review and discuss the checkpoint answers with you as we go round the lab.
Good Luck!

We hope you enjoy the lab.