DOTA: Introductory Laboratory

1 Lab intro, part 1: How to submit laboratory results

Let us see if we are alive. Access the DOTA grading website, and enter your username, password, and whatever you want to give yourself as a mark[1]:

`https://hugh.comp.nus.edu.sg/DOTA/introlab1/gradesintrolab1-1.php`

You can give yourself whatever mark you want. Including pictures if you really want. Please be nice.

2 Lab intro, part 2: Getting started with SEED UNIX

Some of the laboratory exercises will be using SEED Labs 2.0. You should follow the instructions at `https://seedsecuritylabs.org/labs.html`. There are two things to do:

1. Install VirtualBox on your machine, so that you can run the Ubuntu 20.04 virtual machine provided for the SEED labs. `https://www.virtualbox.org/wiki/Downloads`
2. Get the Seed Ubuntu 20.04 image[2] from `https://seedsecuritylabs.org/labsetup.html`

To create a new virtual machine from the image you have downloaded, follow these instructions:

`https://github.com/seed-labs/seed-labs/blob/master/manuals/vm/seedvm-manual.md`

If you encounter any errors when running VirtualBox on macOS, try this:

`https://medium.com/@Aenon/mac-virtualbox-kernel-driver-error-df39e7e10cd8`

The very first time, login as `seed`, with password `dees`. When the login procedure is completed you should see the GUI, and be able to select programs from the menus and run them. It is not too different from operating Windows systems, although it is common on UNIX systems to use a terminal window to type in commands. You can open up a terminal window by clicking on the icon. You can use the `passwd` command to change the login password to something else if you wish. If you later forget this login password, you may have issues :) Make sure you type it correctly (it asks you twice).

[1] Please check your email for the password and usercode

[2] There should be a copy of this up at Zhejiang University, but I cannot seem to find it. Perhaps you can! :)

Assuming you can log in OK, you can do the following short task, to get a mark for this part (part 2) of laboratory 1:

- Use the `md5sum` (File Checksum Integrity Verifier) program to find the MD5 checksum of the file `/usr/bin/wireshark`. You will use this checksum as a security code when you get your mark.
- Access the DOTA grading website, and enter your username, password, and the MD5 checksum, along with whatever you want to give yourself as a mark:
  `https://hugh.comp.nus.edu.sg/DOTA/introlab1/gradesintrolab1-2.php`
  You can give yourself whatever mark you believe you deserve.

3 Lab 1, part 3: WSE

Today we have a case study of the Windows Scripting Encoder. Even simple encryption schemes still find use today! In particular, we will investigate a slightly simplified version of the Windows Scripting Encoder, provided by Microsoft a few years ago to "encrypt" the program code of programs running on webservers. The scripting engine itself could decode and execute the program code, but it looks encrypted to anyone else. The motivation behind the Scripting Encoder was to prevent an attacker who illegally downloaded these programs from gaining any information about how the program works. Quite often programs written from the web also contain passwords for database servers hidden among the program code. The Scripting Encoder's aim was to hide these from an attacker. In this part of the laboratory, your goal is to investigate how it works and to recover a password!

Firstly, open a terminal window in Unix on the SEED virtual machine. Now download the wse encryption program - you can get it by using wget, a useful tool for retreiving files:

```
seed@VM:~$ wget https://www.comp.nus.edu.sg/~hugh/DOTA2022/Labs/introlab1/wse
seed@VM:~$ chmod +x wse                  # now make it executable
seed@VM:~$ ls -l wse                     # look at the attributes of the file
seed@VM:~$ file wse                      # and it's type
```

The `chmod` tells the system that this is a program (an executable file). Create some test data files to be encrypted. Each file can have a small amount of text in it (sample passwords in, say, `sample1.txt`, `sample2.txt`...). Use `wse` to encrypt them:

```
seed@VM:~$ wse < sample1.txt
```

Alternatively, you can just enter in strings directly from the console window "`wse`". The password for the DOTA grading administrator has been found by harriet-the-hacker in a wse-encrypted file at:

```
https://www.comp.nus.edu.sg/~hugh/DOTA2022/Labs/introlab1/DOTA2022Password.encrypted
```

Use `wget` to get the file, and then look at it by typing "`cat DOTA2022Password.encrypted`". It is a wse-encrypted version of the administrator's password. Really. If you can discover the original administrator password, you can input your grade through the web page, as before. Your goal is to figure out how the encoding works so you can learn the password!

During the lecture, we discussed a few possible attacks against encryption systems. Think about the chosen ciphertext and chosen plaintext attacks. Perhaps one of them would be helpful to you here. Now it's time to investigate! You can try to encrypt as many messages as you want by running the "`wse`" program.

Once you find the administrator password - please do not share it with others in the class. Access the DOTA grading website, and enter your username, password, and the administrator's password, along with whatever you want to give yourself as a mark:

`https://hugh.comp.nus.edu.sg/DOTA/introlab1/gradesintrolab1-3.php`

You can give yourself whatever mark you believe you will in the future deserve.