Secure Computer Systems I: Introductory lab

October 29, 2015

Due on **Monday, November 2, 2015 at 13:15h**

The purpose of this introductory lab is to check that you have sufficient background knowledge to complete the remaining labs (and get you up to speed if you don't). You will get to do some practical exercises, install software we will be using later in the course, and submit a lab report. The lab report will not count towards your grade, but you will get feedback that will help you perform better on the remaining labs.

The introductory lab is *individual*, but you may discuss it with other students.

If you have any questions, contact Charalampos Orfanidis (office ngstrm #72111 or `charalampos.orfanidis@it.uu.se`) Amendra Shrestha (office ITC #1457 or `amendra.shrestha@it.uu.se`).

Task 1: SQL

Read about SQL, for example at `http://www.w3schools.com/sql/default.asp`. When you have finished, take the quiz test on that same page to make sure you have understood. (Or start by taking the quiz to see what you need to read more about!)
Click the 'Try it yourself' button and try some SQL statements in the online editor.

Exercises:

(a) Give two SQL statements that are accepted by the editor. At least one of the statements should contain a `WHERE` clause. In the lab report, give the statements and their output. Explain carefully what the statements do and why they work.

(b) Give two SQL statements that are *not* accepted by the editor. At least one of the statements should contain a `WHERE` clause. In the lab report, give the statements and their error output. Explain carefully what the statements are trying (but failing) to do, and why they don't work.

Task 2: Get started with BackBox Linux and MyStore

Read about *penetration testing*, for example on Wikipedia [1]. Pen testing will be part of all labs in this course. We recommend that you use *BackBox* [2], a version of Ubuntu Linux specialized for the purposes of pen testing. We've provided a minimal BackBox system for you (on a USB stick) as a virtual machine that you can run under VirtualBox. You can use BackBox to safely connect to the course pen test lab via VPN (and we will show you how).

Another important part of the course is *web security*. For this, we'll be using a web store that is full of security holes. The web store named MyStore is also included in the provided file.

Note: It is **very important** that you get BackBox (or an equivalent system) as well as MyStore up and running, either on your own computer or in the PC lab, so if you have any problems with this, try to solve them as early as possible! We will try to help you during the scheduled lab hours or by email or appointment. If you want to use some other configuration, e.g., your own Linux/Windows/Mac system, we may not be able to provide support.

Running BackBox from USB

1. VirtualBox is already installed on the PC lab computers. If you don't have VirtualBox installed, go to `http://www.virtualbox.org`, download VirtualBox, and install it on your computer. **Please make sure you're running version $\geq$ 4.3!**
2. Open VirtualBox. Click 'New', give the machine a name, and select Linux/Ubuntu as your operating system. Click 'Next'. Set memory size to 1024K. Click 'Next' again and select 'Use an existing hard drive'. Navigate to the USB stick and select the file `BB-disk1.vmdk`.
3. Click 'Preferences' from the VirtualBox 'File' menu (or just from the VirtualBox menu, on Mac). Go to 'Network' and create a new NAT network. Give it a name and check 'Active'. Click 'OK'
4. Click 'Settings' for the machine you just created.
   (a) Go to 'Network' and click on the 'Adapter 1' tab. Enable Network Adapter if it is disabled. Select 'NAT Network' under 'Attached to'. Under 'Name', select the NAT network you created in the previous step. Set 'Promiscuous mode' to 'Allow all'.
   (b) Again select 'Adapter 2' tab and select 'Host-only Adapter' in 'Attached to' field. Under 'Name', select 'vboxnet0' (in Mac) and VirtualBox Host-Only Ethernet Adapter (in Windows). Set 'Promiscuous mode' to 'Allow all'. Click 'OK'.
5. Start the system. You should now have a version of BackBox and MyStore up and running from your USB stick. **DO NOT install updates** when the systems prompts you to, since there may not be enough space on the USB stick to do that.

Accessing MyStore from your local machine or BackBox

1. Open VirtualBox. Start your new BackBox VM machine and open a terminal. Type in `ifconfig`, you should see 2 Ethernet interface (i.e. ethX). The Network interface starting with 192.168.56.x is the IP address of your MyStore instance.
2. Open a web browser on your local machine (or in BackBox VM) and enter the IP address (192.168.56.x) from the previous step. If you see the MyStore webpage, you have succeeded.

Exercises:

There are three exercises at `http://www.danscourses.com/Network-Penetration-Testing/bash-line-commands-a-shell-scripting.html` to help you get started with pen testing. They are labeled Exercises 1, 2, and 3, and you will do all of them.

(a) Do *Exercise 1* twice, as follows:

I. Go to your BackBox VM and open a terminal. Follow *Exercise 1* as stated on the webpage, substituting 192.168.56.x for the 'test network environment' (192.168.1.x).

II. Type in `cd /home/security/vpn-lab` in the terminal, then `sudo openvpn user.conf`. Enter your root password (hint: it is related to `security`). Enter your VPN username and password (provided during lab). Open a new terminal window. Follow *Exercise 1* again, substituting 10.0.1.x for the 'test network environment'.

In the lab report, give the output of your commands (as shown in the exercise instructions).

(b) Do *Exercise 2* as stated on the webpage. In the lab report, give the output of your commands (as shown in the exercise instructions).

(c) Do *Exercise 3* as stated on the webpage, and comment your shell script(s) to explain what each line does. You can either do this in the code directly, or by explaining each line in the lab report. In the lab report, give the scripts and the explanations, plus the output of your commands (as shown in the exercise instructions).

Task 3: Find out more

An *exploit* is a piece of code that takes advantage of a security hole (for example, in an email server software) in order to make something unintended happen. Exploits can be used by a hacker to gain root access to a system. In this part of the lab, you'll get to practice finding information and referencing it correctly.

The University of York has a helpful guide to references [3]. For the assignments in this course, you should use the IEEE referencing style. If you are writing your report using LaTeX, references are automatically formatted if you choose the appropriate bibliography style, `\bibliographystyle{ieeetran}`. (The references in these instructions are formatted according to the IEEE style).

Exercises:

(a) Use your search skills to find out what *Metasploit* is. Write a brief explanation and don't forget to properly reference your sources.

(b) What is `CVE-2015-3860`? Write a brief explanation and don't forget to properly reference your sources.

Handing in

Hand in your report as a PDF file in the Student Portal, "Introduction Lab". Before you hand in, check that the following evaluates to true:

- My name, the date, the course name, and the lab title are all on the first page of the report.
- I have clearly stated who I have collaborated or discussed with (if anyone).
- The headings in my lab report match the headings in the instructions marked 'Task x' for $x \in \{1, 2, \ldots\}$.
- I have done all the exercises and answered all the questions in the instructions. (If I didn't manage to complete an exercise, this is clearly stated in my report.)
- The text has been spell checked.
- I have used references properly, following the guide [3] and using the IEEE style.
- I have read through the entire report, understood it, and can explain it to someone else who has *not* read it.
- The descriptions of what I did are so clear that if someone else reads them, they can replicate the result by following my steps.

Please note that plagiarism (copying someone else's work, or using someone else's work without properly referencing it) will NOT be tolerated and may lead to disciplinary measures. All reports will be checked automatically for possible plagiarism.

References

[1] Wikipedia, "Penetration test — Wikipedia, The Free Encyclopedia," accessed 16 Jan 2014. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Penetration_test

[2] "Backbox Linux," accessed 16 Jan 2014. [Online]. Available: http://www.backbox.org

[3] The University of York, "Referencing styles," accessed 16 Jan 2014. [Online]. Available: http://www.york.ac.uk/integrity/referencing.html