Computer Security
Tutorial 1
VM Setup, Wireshark, and Firewalls

Margus Lind

The primary goal of this tutorial is to make sure you have all the necessary coursework 1 VMs setup and can run some of the necessary software. If you get done quickly, or if setup is taking a while, you should skip to section 4 and try out some of the security games.

This tutorial sheet intentionally provides limited guidance on using some of the tools mentioned. It is up to you to search for tutorials, examples, articles, or read the manpages. You will be expected to be able to look up the usage of new tools in the coursework.

1 Setting up the Virtual Lab

Your first task is to set up the Virtual Lab used in the first Coursework. To do so, obtain the coursework handout from the course website and complete *Section 1 - Setup*.

The following is a quotation from the most pertinent part of the coursework:

> For your convenience we have provided the following script which sets up the VMs for you. The TA cobbled it together from bits and pieces of code examples from the Internet when working late. Its probably fine....
>
> `/group/teaching/cs/cw1/setup.sh`
>
> Running the script will create VMs in VirtualBox under your account. These VMs use the disk images stored in the class group directory and only store your changes to your home directory. Consequently, the VMs themselves will not consume your disk quota, but if you add big files to the VMs those will use your disk quota.

1.1 Frequently Asked Questions

Passwords *alice* has the user name "alice" and password "alice". *bob* has the user name "bob" and the password "bob". *charlie* is a black box, you cannot log into *charlie*.

"mallory" == "Kali" These are the same, we know it is confusing, sorry. Kali's user is "root" and password is "toor".

My mouse is trapped and can't exit the VM. Press the right control key. This is a "feature" of VirtualBox.

How do I edit a file We recommend the `nano` text editor for beginners. If you don't know what that is, we recommend first completing the "Introduction to Unix" primer linked off the course website.

1.2 Getting Familiar with the VMs

1. Log onto **alice** directly through the alice VM

2. Create a file in her home directory. It doesn't matter what is in the file, just create one.
3. Log out of **alice**
4. Start **mallory**
5. Open a terminal and type: `ping alice`
6. Log into alice through ssh by typing: `ssh alice@alice`
7. Verify the file is still there and unchanged
8. Shutdown **alice** by typing the following into the alice terminal: `shutdown now` or by turning off the VM under the "machine" menue at the top of the alice VM.
9. Start the **alice** VM again.
10. Log onto **alice** and verify the file you created is missing.
11. Learn the lesson: coursework VMs do not have persistent changes - do not keep any work on there.

Congratulations! The VMs are now all setup and working.

2 Wireshark

Wireshark is a great tool for monitoring and analysing network traffic. You will also need to use Wireshark in the coursework!

1. Make sure you have **alice**, **bob**, and **mallory** running.
2. Open Wireshark on **mallory**. An error will likely pop up saying something like: "Error during loading", you can safely ignore it.
3. Click on the eth0 interface to start capturing traffic.
4. Open a web browser on **mallory** and try and visit: `https://alice/proxy`

Now answer the following questions:

- What host does the browser on **mallory** request the website from?
- What details can you see on Wireshark about this request?
- How does the browser know what IP **alice** is at?
- How would it know what IP **inf.ed.ac.uk** has?
- Is the final connection using HTTPS or HTTP?
- Who is the Certificate Authority that signed the SSL/TLS certificate for **alice**? Why is this trusted by the browser?
- **alice** does not host the content served back to the request. Instead, this is queried from **bob** in the background. What details are you able to see on Wireshark about the background request?
- How would you improve the security of this system?

3 Advanced Wireshark

Wireshark is great for filtering and observing packets on a network. However, it can do so much more.

alice is hosting a File Transfer Protocol (FTP) server. Without additional layers of protection, FTP operates on plaintext. A script on **bob** requests a file from **alice** once every minute. You need to recover the transmitted file using Wireshark.

You should ensure that **alice** and **bob** are both up and running. Now, open Wireshark on **mallory**, and wait until you have captured the file transfer. An appropriate filter in Wireshark may be helpful. From here, you can use Wireshark's built-in modules to extract the file transmitted.

If you get stuck try an online search for "how to extract ftp file from wireshark".

4 Firewall Games

Firewalls are often the first line of defence against the unknown dangers that come in over networks. At their core, a firewall is a very simple concept. You create a set of rules stating what is allowed into a network and what is not. The firewall then enforces those rules on all traffic flowing across it. Simple.

In this part of the tutorial you will be playing several Firewall-themed games created by past students in internships or as part of thesis projects. These games are explicitly intended to help students just like you learn about the principles of Firewalls in a fun and structured way.

Go play a firewall related game:
`https://groups.inf.ed.ac.uk/tulips/security_games.html`.

Note that some of the games have small bugs in them. The bugs are normally described at teh bottom of each game screen, so please look there first.