Summative Security Coursework

Dr Chris G. Willcocks

Last Modified: January 21, 2021

1 Introduction

In this coursework you will be reviewing the security of a server belonging to a new startup company. The server hosts the company's successful shop "durhamazon.com" (not a real website) that sells a range of products. It also contains a suite of proprietary tools, a database, and several employee user accounts. Some of the employees have been acting strangely recently. You've been hired to evaluate the security of the machine. It is important to make sure that the server is fully secured, including all services that are running, and ensure that no sensitive or confidential information can be leaked. You will be given a virtual machine image of the company server. Your job is to i) **identify** security vulnerabilities that are present, ii) explain how the vulnerabilities may be **exploited**, and iii) explain how to **remove** the vulnerability.

The report

This table is how you should structure your report, and the example will also help you gain access to the server:

Vulnerability	**Exploit / Problem**	**Mitigation**
1) There is a user account called 'user' which has a weak password which is 'password'.	Someone could guess the password 'password' and gain access to the server.	The vulnerability can be secured by selecting an appropriately secured password, for example random mixed case letters, numbers, and symbols.

Formatting

You should submit a single **PDF** document with a table consisting of a **maximum of 3 pages**. This will therefore need to include short concise discussions for each vulnerability. If you wish, although not required, you may submit up to 3 additional pages of numbered screenshots or diagrams (with no detailed text) that may be referenced in the table. Do not submit any modified virtual machine image as this is not required.

2 Marking

There are over 25 vulnerabilities present on the machine. Most of the vulnerabilities are worth **up to 5 marks** each but there are a small number of very easy vulnerabilities that are only worth **3 marks**. Duplicate vulnerabilities in the table won't be awarded any extra marks. Each vulnerability is marked as follows:

1. Identify the vulnerability: **1 mark**
2. Concisely explain or write a step-by-step guide to exploit the vulnerability: **1-2 marks**
3. Concisely explain or write a step-by-step guide to remove the vulnerability: **1-2 marks**

Solve the Mystery

Some of the employees have been acting strangely recently. In a maximum of six sentences, explain what is going on. Can you prevent a crime? Can you offer any relationship advice, or information to Durham Constabulary? You don't need to explain how you arrived at your conclusions. Solving this correctly is worth **8 marks**.

In summary, you can receive **up to a maximum of 90 marks** for correctly identifying and handling the vulnerabilities, where a further **2 marks** are available for the conciseness, clarity and unambiguity of the writing in your table (short and direct answers are best, don't try to write too much per table cell, if it's correct and not ambiguous you get 2 marks), and lastly **8 marks** are available for solving the mystery (you will be deducted marks if you write more than 6 sentences for this part).

3 Setup

You will be provided with a VirtualBox machine image. You should download and install VirtualBox on your computer. There are lots of guides for installing VirtualBox, just search online for how to install for your operating system. The machine image contains a Linux server that runs a number of services. To install the image provided, double click on it once you've installed VirtualBox, or you can click 'File > Import Appliance' from inside VirtualBox. You'll probably want to keep this image file as you may need to re-install later if you break the installed image.

Due to the file size, you may have a problem with a corrupted download. If you think you might have a corrupted download check the MD5 hash which should be: 0f20c9b26d5869929c2eb0befd340b68 If you have a slow internet connection, download the image to a USB stick from the university network. The virtual machine image is lightweight (on purpose) and may be out of date. You will not be awarded marks for stating that you can update the system to mitigate a vulnerability.

Common issues: (1) If you experience a 'kernel panic' or crash at startup, you likely don't have 'hardware virtualization' enabled. Reboot your computer/laptop, enter the BIOS, and find the hardware virtualization setting and enable it, then restart. (2) If the Durhamazon shop doesn't work, it probably means your host machine isn't connected to the internet. (3) You do not need to use Kali Linux (or equivilent) to get 100% and mitigate every vulnerability. If you want to transfer files to-and-from the server easily, without the hassle of setting up the network adapters correctly, consider simply using: www.file.io or uguu.se. (4) If the display is too large or too small, right click the VM in VirtualBox then go to 'Display' and change the 'Scale Factor' accordingly.

4 Anti-collusion

This assignment is to be worked on independently. All reports will be checked for collusion using a custom-built Python script, in addition to Turnitin. The collusion detection script runs through each PDF extracting features with a deep language model, then it creates a large tensor of these features between all pairs of students. This is carefully embedded giving a distance matrix. Students who work together in pairs or in groups light up like a Christmas tree in this matrix, even if they have swapped synonyms/rephrased and reordered the table. Pairs or groups of students with significant similarities will be carefully investigated. In the past few years, these scripts have caught out several students who have been working together. In all cases, evidence highlighted from the scripts and by manual investigation has been provided to a departmental panel and the offending students have been found guilty and marked 0. So please don't consider collision here, it's not worth the risk.

5 Remarks

There are a number of files placed around the system that are hints for identifying a vulnerability. Use whatever third-party tools you like. Every vulnerability in the server has been/will be discussed at some point during one of the lectures. I hope you enjoy the coursework.