ECM2426: Network and Computer Security

Continuous Assessment

University of Exeter

Academic year: Term 1, 2023/24
Hand-in date: See ELE Submission Page

Abstract

This continuous assessment covers topic taught in the module ECM2426 "Computer and Network Security". The continuous assessment focuses on your understanding of the practical aspects of security that you acquired during the labs, lecture, and practical exercises in the lecture notes.

This continuous assessment requires you work a virtual machine that is assigned to you individually, and to submit your solution in a very specific format. Read the instructions carefully, it is your responsibility to ensure that your submission adheres to the specified format. Please ensure you read the entire document before you begin the assessment.

Changelog:

- Version 4:
  - Exercise 6: The path specified in the first line of the description has been corrected.
- Version 3:
  - Exercise 4: Updated instructions to mitigate a bug affecting some VMs.
- Version 2:
  - Exercise 2: Updated instructions for E.2.3 and E.2.4.

General Instructions

System Access

For completing this course work, you need to use a VM that is provided to you a hosted on Azure Labs, i.e., the same system that we are also using for the workshop:

- Name of the VM: `2023-ecm2426-ca`
- User: `lh`
- Password: `Initial1`

Invitation emails for this VM will be sent out on the 24th of October 2023 and latest arrive in your inbox early morning on the 25th of October 2023.

Note that sometimes the Azure dashboard **seems to hang in a "starting" state.** This is a known bug of the user interface of Azure Labs: you can already connect to the virtual machine while the user interface shows "starting." For this, access the RDP connection details in the dashboard by clicking menu with the three dots. Copy this information in your RDP client ("Remote Desktop Application").

System Resources

Note that access to the cloud system is expensive and billed "by the minute". Thus, please always switch VMs off, after you finished your work. To mitigate the risk of "cost explosion", the VM has a maximum amount of hours assigned. This is not a maximum allowed time. The consumption will be monitored and whenever VMs have only a few hours left, more time will be added.

Moreover, you can ask for more time by sending am email (body can be empty) with the subject "`ECM2426 CA: Please check VM time`" to `a.brucker@exeter.ac.uk`. The deadline for such requests is the last Tuesday before the submission deadline, precisely:

2023-12-05T17:59:59 GMT

After this deadline, request will be processed on a "best effort"-basis, but there is no guarantee that they are processed before the submission deadline.

Referencing and Academic Conduct

This is an individual assessment. Hence, you are not allowed to discuss solutions of this course work, or concrete instructions how to obtain solutions, with others. This includes discussions on WhatsApp groups or posting questions on Stack Overflow. The university requires you to cite the work of others used in your solution and to include a list of references. You must avoid plagiarism, collusion and any academic misconduct behaviours. For further information and guidance, please take the self-learning "Academic Honesty and Plagiarism".

Furthermore, **you need to work on the VM assigned to you**. Not following this rule, will also consider as academic misconduct.

Marking Scheme

The marks for the individual questions are denoted for each (sub)-question. In addition, please note:

- You need to work on the VM assigned to you and only to you. Some tasks result in solutions that are unique to your VM. Hence, **solutions obtained on a different VM will result in zero marks.**
- Your submission needs to follow a specific format, detailed in the next section. **Not following this format will result in zero marks**. As part of the VM, a script is supplied that does provide a basic check of the required format. You are encouraged to make use of this script. If this script cannot recognise your solution/submission, it will likely result in zero marks.

Submission

The submission consists only out of one spreadsheet in OpenDocument format (`.ods`). This file format is, for example, supported by LibreOffice (`https://www.libreoffice.org/`), which is installed on the provided VM. The VM also provides a template of the

spreadsheet, named `2023-ecm2426-ca-<uuid>.ods` (the `<uuid>` part will be replaced by a unique identifier) in the home directory of the user `lh` in a folder `coursework`, i.e., `/home/lh/coursework`.

For each sub-question, you will need to fill out a clearly marked field in the **column B** of the provided spreadsheet. If you want to declare the use of specific references, you can do this in **column D**. Please do not change the UUID in the last row of the spreadsheet.

The VM contains a tool `check-submission` that you can use to check the validity of your created zip file. **It is strongly recommended** that you use this tool to check the compliance of your spreadsheet to the required submission format, before submitting your solutions:

```
lh@ML-RefVm-326614:~$ check-submission 2023-ecm2426-ca-<uuid>.ods
```
Bash

This script will check the syntactic compliance of your submission, i.e., there is a solution for each question. It does not check for the correctness of your submission. Note that a successful run of the `check-submission` script does neither guarantee that your submission is complete nor that it follows the guidelines. *Checking that the submission is complete and that the individual entries comply to the specified format is your responsibility!*

You can copy the spreadsheet to your local machine using `scp` or `sftp`. Note that also for scp (and sftp), you need to configure the correct port. Assuming that you can connect to the VM using the following command:

```
achim@logicalhacking:~$ ssh -p 65042 lh@host.azure.com
```
Bash

You can use (note the scp using an uppercase P for specifying the remote port):

```
achim@logicalhacking:~$ scp -P 65042 lh@host.azure.com:coursework/2023-
    ecm2426-ca-<uuid>.ods .
```
Bash

to copy the spreadsheet to your local machine. Of course, you can also use a graphical front-end, as, e.g., provided by putty or winscp.

Some question might refer to files provided on the VM in a folder `/home/lh/coursework`. If you accidentally delete or modify a file, there is a read-only backup available in the hidden directory `/home/lh/.coursework` (note that the directory starts with a '.' and, therefore is only shown when doing an `ls -a`).

1 Foundations & Access Control

Exercise 1 **(20 marks)**

The virtual machine `2023-ecm2426-ca` has several regular user accounts configured. In this exercise, you should explore these accounts and their access rights.

E.1.1. (5 marks): List all logins (not the full usernames) that both have numerical user id larger or equal than 2000 **and** that are a member of the group `staff`.
Submit your answer in cell B2, separate the logins with a comma, e.g., "`joe, jane, root`".

E.1.2. (5 marks): Analyse the VM to obtain the password of the user with the numerical user id `2000`. Note that **you should obtain the password using reconnaissance**, not by running a computational expensive password cracking tool.
Submit your answer in cell B3 of the spreadsheet.

E.1.3. (5 marks): The user with the numerical user id `2001` has a file `flag` in their home directory. What is the content of this file?
Submit your answer in cell B4 of the spreadsheet.

E.1.4. (5 marks): List *all* users with their login that can access the content of the file `flag` in the home directory of the user with the numerical id `2001`.
Submit your answer in cell B5 of the spreadsheet, separate the logins with a comma, e.g., "`joe, jane, root`".

2 Cryptography, Signatures & PKIs

Exercise 2 **(15 marks)**

In the home directory of the user `lh` there is an X.509 certificate stored in a file called `/home/lh/coursework/exercise02/cert.pem`. This certificate should be used for securing a web server. The directory also contains an asymmetric key pair, stored in the file `key.pem` and an encrypted file `secret.txt.enc`. There is no password set on this key pair.

For this excercise, you might want to use the `openssl` command line tool, which is provided on the virtual machine.

E.2.1. (2 marks): Name the signature algorithm that has been used for signing the certificate.
Submit your answer in cell B6 of the spreadsheet.

E.2.2. (2 marks): Name key length used by the signature algorithm that has been used for signing the certificate.
Submit your answer in cell B7 of the spreadsheet.

E.2.3. (3 marks): Is the certificate valid for the domain `www1.exeter.ac.uk`?
Submit your answer in cell B8 of the spreadsheet.

E.2.4. (3 marks): Is the certificate valid for the domain `www3.exeter.ac.uk`?
Submit your answer in cell B9 of the spreadsheet.

E.2.5. (5 marks): Decrypt the file `secret.txt.enc`. What it is content?
Submit your answer in cell B10 of the spreadsheet.

3 Security Protocols

Exercise 3 **(15 marks)**

The provided VM allows you to access a network that uses the IP range `172.17.0.*` and your virtual machine is connected to this network via the network interface `docker0`. This network contains a number of computers that might have insecure services installed.

As user `lh`, analyse the network traffic on the `172.17.0.*` (e.g., using Wireshark) and answer the following questions related to the http session:

E.3.1. (5 marks): Give the full URI of the password protected web area accessed in this session.
Submit your answer in cell B11 of the spreadsheet.

E.3.2. (5 marks): Give the username of the user who is successfully accessing the protected web area successfully.
Submit your answer in cell B12 of the spreadsheet.

E.3.3. (5 marks): Give the (cleartext) password of the user accessing the protected area. Note that no computational expensive techniques (e.g., a brute-force attack on a password hash) are required.
Submit your answer in cell B13 of the spreadsheet.

4 Formal Analysis of Security Protocols

Exercise 4 **(15 marks)**

The file `/home/lh/coursework/exercise04/ecm2426.AnB` contains a (incomplete) security protocol specification in Alice&Bob notation. The specification is incomplete, as it lacks one fact of the initial knowledge (denoted by `<fact>`). Moreover, the last protocol step, that is required to complete the protocol securely, is missing. Answer the following questions with the help of `ofmc`.

E.4.1 (5 marks): One role has an incomplete initial knowledge, denoted by `<fact>` in the provided specification. Replace `<fact>` with the minimal fact that is required so that the protocol is executable.
Submit your answer in cell B14 of the spreadsheet.

E.4.2 (2 marks): Who needs to send the last message required to complete the protocol securely?
Submit your answer in cell B15 of the spreadsheet.

E.4.3 (3 marks): Who receives the last message required to complete the protocol securely?
Submit your answer in cell B16 of the spreadsheet.

E.4.4 (5 marks): What message needs to be exchanged in the last protocol step that is required to complete the protocol securely?
Submit your answer in cell B17 of the spreadsheet.

Important Note: Due to a bug in the setup script for the VMs, in some instances the initial knowledge of the roles specified in `/home/lh/coursework/exercise04/ecm2426.AnB` lacks the roles themselves. If this is the case, please add them in addition to the denoted missing `<fact>`. For example, if your protocol specification includes

A&B
```
Knowledge:
    A: pk(A), g;
    B: pk(C), <fact>, h
```

then please change it to:

A&B
```
Knowledge:
    A: A, B, pk(A), g;
    B: A, B, pk(C), <fact>, h
```

5 (Manual) Dynamic Security Testing

Exercise 5 **(20 marks)**

The VM has a small Message Board application installed that allows people to post (encrypted) messages. It can be accessed at `http://127.0.0.1:5000`, using a web browser that runs on the VM.

The user `lh` can use `sudo` to start/stop the application:

Bash
```
lh@ML-RefVm-326614:~$ sudo systemctl start message-board
lh@ML-RefVm-326614:~$ sudo systemctl stop message-board
```

During the start of the application, the database is reset to an empty state. Note that also during a system restart, the database state is reset.

Assume you are a penetration tester tasked to analyse this application. You should test the application for Cross-Site Scripting (XSS) and SQL Injection (SQLi) vulnerabilities. In particular, you should find:

- One SQL Injection (SQLi) vulnerability that allows you to access a post that otherwise is not accessible.

  E5.1. (5 marks): What is the full URL used for exploiting the vulnerability? *Submit your answer in cell B18 of the spreadsheet.*

  E5.2. (5 marks): What is the content of this "secret" message? *Submit your answer in cell B19 of the spreadsheet.*

- One XSS vulnerability that allows you to access a session cookie.

  E5.3. (5 marks): What is the full URL used for exploiting the vulnerability? *Submit your answer in cell B20 of the spreadsheet.*

  E5.4. (5 marks): What is the content of the session cookie? *Submit your answer in cell B21 of the spreadsheet.*

6 Static Security Testing

Exercise 6 ***Static Analysis*** **(15 marks)**

In the directory `/home/lh/coursework/exercise06/` there is copy of a version (not necessarily the one that you analysed in the last exercise) of a message board application. Analyse the application using the static security scanner "bandit" (`https://github.com/PyCQA/bandit`). The bandit tool is part of the provided VM and the version installed on the VM will be used as a reference for assessing your solution.

You can run bandit as follows, and it should report three potential security issues:

```
achim@logicalhacking:~/coursework/exercise06/$ pipenv run bandit -r .
Test results:
>> Issue: [Bxxx]
>> Issue: [Bxxx]
>> Issue: [Bxxx]
```

Bash

The actual output will provide more details. Not all of these findings are real vulnerabilities, and neither are all findings of bandit real vulnerabilities. Moreover, we limit the scope of our analysis: We only

- focus on software vulnerabilities in the application itself, the Python source code or templates used for generating html pages. We do not consider configuration issues (for example, using http instead of https or the fact that the application is configured to run in development mode, are out of scope for this exercise).
- classify an issue as a vulnerability, if it can actually be exploited by an attacker.

E6.1. (1 marks): What is the identifier (e.g., "B105") and line number/position (e.g, 42:17) of the first reported vulnerability? Separate both by a comma (e.g., B105, 42:17). *Submit your answer in cell B22 of the spreadsheet.*

E6.2. (4 marks): Can the first reported vulnerability be exploited by an attacker? *Submit your answer in cell B23 of the spreadsheet.*

E6.3. (1 marks): What is the identifier (e.g., B105) and line number/position (e.g, 42:17) of the second reported vulnerability? Separate both by a comma (e.g., B105, 42:17). *Submit your answer in cell B24 of the spreadsheet.*

E6.4. (4 marks): Can the second reported vulnerability be exploited by an attacker? *Submit your answer in cell B25 of the spreadsheet.*

E6.5. (1 marks): What is the identifier (e.g., B105) and line number/position (e.g, 42:17) of the third reported vulnerability? Separate both by a comma (e.g., B105, 42:17). *Submit your answer in cell B26 of the spreadsheet.*

E6.6. (4 marks): Can the third reported vulnerability be exploited by an attacker? *Submit your answer in cell B27 of the spreadsheet.*