DEPARTMENT OF COMPUTER SCIENCE

SUMMATIVE COURSEWORK ASSIGNMENT BRIEF

KEY INFORMATION

- Module title: Databases & Information Security
- Module code: CS2DI17
- Lecturer responsible: Dr Martin Lester
- Type of assignment (coursework/online test): Coursework — Penetration testing exercise
- Individual/group assignment: Individual
- Weighting of the assignment: 25%
- Page limit/word count: 4 pages A4 (excluding cover sheet)
- Expected hours spent on this assignment: 5 hours in practicals + 5 hours independently
- Items to be submitted: PDF written report
- Work to be submitted on-line via Blackboard Learn by: 12:00 midday on Fri 28th Oct 2022
- Work will be marked and returned by: Fri 18th Nov 2022

PLAGIARISM

By submitting this assignment, you are certifying that it is all your own work. Any sentences, figures, tables, equations, code snippets, artworks and illustrations in this report must be original and must not have not been taken from any other person's work, except where explicitly acknowledged, quoted, and referenced. You understand that failing to follow this requirement will be considered plagiarism. Plagiarism is a form of academic misconduct and will be penalised accordingly. The University's Statement of Academic Misconduct is available on the University web pages.

LATE SUBMISSION

If your work is submitted after the deadline, 10% of the maximum possible mark will be deducted for each working day (or part thereof) it is late. A mark of zero will be awarded if your work is submitted more than 5 working days late. It is strongly recommended that you hand work in by the deadline as a late submission of one piece of work can have an impact on other work.

If you believe that you have a valid reason for failing to meet a deadline, then you should complete an Exceptional Circumstances Form and submit it to the Student Support Centre before the deadline, or as soon as is practicable afterwards, explaining why.

1. ASSIGNMENT DESCRIPTION

SUMMARY

You will be supplied with disk images for two virtual machines, called **club** and **tester**. **club** is configured to host a simple Web application and some other network services. Some basic network scanning and vulnerability testing tools have been installed on **tester**. Connect the two virtual machines using a virtual network. Use the tools installed on **tester** to perform penetration testing on **club**. Write a report describing what you did, what you found and any changes you would recommend being made to **club**.

In your PDF report, you must answer each subtask on a separate page and use at most one page for each subtask.

You must not connect tester to the University network or the public Internet. If you scan the University network for vulnerabilities, you may be subject to disciplinary procedures.

TASK DESCRIPTION

Scenario

Earley Birds Badminton Club is a sports club that hosts competitions between its members. The club has decided to make information about its members available online, so that they can contact each other and arrange matches. Mr Shuttleworth, a retired stock trader who helps run the club, has written a simple Web application that enables this. Club members will enter their name and a password into a form on a website, which will display a list of contact details of other members in the same competitions.

Mr Shuttleworth is quite enthusiastic about his new system, but does not know much about computer security and has asked you for your opinion. You have decided to penetration test the server running the application.

Setup

Download the disk images for the club's server **club** and the penetration testing machine **tester**. Unzip them; each should be about 1 GB in size uncompressed. Create a new virtual machine from each disk image. The operating system type/version in VirtualBox should be set to Linux/Debian (32-bit).

Important: Before you start either virtual machine, ensure they are both connected to the same internal virtual network. For each machine, go to Settings, select Network and look at the Adapter 1 tab. Change "Attached to:" from "NAT" to "Internal Network" and enter a network name, such as "infosec". You must use the same network name for both virtual machines.

Start both virtual machines. Login to **tester** using the username *tester* and the password *pentester*. The *root* password is also *pentester*. When you have finished working, you can shut down both virtual machines cleanly using the VirtualBox menu option *Machine > ACPI Shutdown*.

In this coursework, you are simulating attacking **club** over the network. Therefore you should not type anything into the window for the **club** virtual machine.

Subtask 1. Information gathering (20%)

Use **tester** to gather information about the network services running on **club**, including the versions of any software providing the services. In your report:

1. Show output (screenshots or logs) from the tool or tools you used. (10%)
2. Explain what you have discovered. (10%)

Subtask 2. Penetration testing: remote login (20%)

Gain access to a user account on **club** using tools installed on **tester**.

For this task, you should target one of the remote login services you found in the previous task, using the password cracking tools supplied. (There may be other ways to gain access to a user account, but please use this method.) You will gain more credit if you can find a way of gaining access to the administrator account (`root`).

If you are unable to find or exploit a vulnerability, explain what you tried and give evidence of your attempt. You will still gain some credit for this.

In your report:

1. Show evidence (screenshots or logs) of exploiting the vulnerability. (10%)
2. Explain briefly what caused the vulnerability and how the tool or process you used exploited it. (10%)

Subtask 3. Penetration testing: Web application (20%)

Gain access to the database on **club** using the Web application from **tester**. Show the output from the tools you used. Explain briefly how the attack works.

For this task, you could attempt an SQL injection on the Web application running on **club**. Or you could attempt to exploit the Shellshock vulnerability.

You should not use any password cracking tools in this task. Nor may you use any information, such as usernames or passwords, that you discovered through the previous task.

In your report:

1. Show evidence (screenshots or logs) of exploiting the vulnerability. (10%)
2. Explain briefly what caused the vulnerability and how the tool or process you used exploited it. (10%)

Subtask 4. Recommendations (20%)

What recommendations would you make to Mr Shuttleworth to secure his system?

In your report:

1. Explain how you would protect the system from the 1st vulnerability you exploited (remote login). (5%)
2. Explain how you would protect the system from the 2nd vulnerability you exploited (Web application). (5%)
3. Make at least 2 other recommendations. You may consider both technical and procedural issues. (10%)

Writing and presentation (20%)

This assignment is partly an exercise in technical report writing. Marks will be awarded for writing clear, correct English. Marks will also be awarded for structuring your report clearly with consistent use of style, but not for fancy formatting.

Hints

The machine **tester** has no GUI, so you will need basic familiarity with the Linux command line. Here are some programs that are available, many of which will be useful:

```
ls          less        nano        ifconfig
nmap        links       ssh         ftp
telnet      ncrack      john        nc
sqlite3     man         wget        su
mv          cp          rm
```

Remember that `man` can be used to display a brief manual for any program. Remember that `cd` is used to change the current working directory.

You should begin your exploration of **club** by opening a Web browser on **tester** and attempting to view a student's marks through the Web application.

ADDITIONAL INFORMATION

Resources supplied or required

You can download the disk images `club.vdi` and `tester.vdi` from Blackboard.

For this coursework, you can either work on your own computer, or on the workstations in the computer rooms in the Polly Vacher Building (available through a remote access service).

If you use your own computer, you will first need to install Oracle VM VirtualBox, which you can download from www.virtualbox.org or (for Linux users) through your distribution's package manager (for example, `sudo apt-get install virtualbox`).

The lecture slides on Blackboard provide an overview of penetration testing. You may find the chapters on "Attacking the network" and "Web security" particularly useful.

Practicals

There are 5 x 1-hour practicals timetabled for completing this coursework. There are 2 groups; please attend the practical for the group to which you have been assigned, although you may attend the practicals for other groups if there is space. You are advised to attend these practicals, as this will be the easiest way to obtain support. A lecturer and a student demonstrator will be available to help. Please ask us if you are stuck. We will not tell you exactly what to do, but we will try to provide you with guidance.

You may also wish to discuss the coursework with other students in practicals. This is both permitted and encouraged, but please remember that this is individual coursework. Any output or screenshots from the virtual machine must be generated by you. Every sentence in your report must be your own work.

To stay on target to submit by the deadline, you are advised to follow this schedule:

- Week 1: Set up virtual machine in practical. Test web application.
- Week 2: Information gathering in practical. Write up information gathering afterwards.
- Week 3: Find vulnerability 1 in practical. Write up afterwards, including recommendation.
- Week 4: Find vulnerability 2 in practical. Write up afterwards, including recommendation.
- Week 5: Tidy report and write other recommendations.

Please ask questions about coursework in practicals if you can, but you are also welcome to ask questions during the lecturer's drop-in office hours. **Support will not be available after the end of week 5.**

2. ASSIGNMENT SUBMISSION REQUIREMENTS

FRONT PAGE

The first page of your submission should include the following information:

- Module code: CS2DI17
- Assignment report title: Penetration testing
- Student Number (for example, 25098635):
- Date of completion:
- Actual time spent on the assignment (hours):

We will use information about how long you spent on the assignment when we review and balance coursework between modules for later years. An exact answer is not necessary, but please try to give a reasonable approximation.

ASSIGNMENT CONTENT

You should submit your report as a PDF through Blackboard, following the instructions at the submission point.

Answer each subtask on a separate page and use at most one page for each subtask. If you fail to do so, you will lose marks for presentation. Furthermore, if your answer for a subtask is significantly longer than one page, you will gain credit only for the first page of your answer. The minimum permissible font size for the body text of your report is 10 pt; 12 pt is recommended.

You are not required to include any references in your report. However, you may choose to do so if it helps to support a claim you make, provided you stay within the page limits. If you do so, use any reasonable, consistent referencing style.

3. ASSESSMENT CLASSIFICATIONS

This coursework assesses your ability to perform penetration testing over a network, to assess and explain vulnerabilities, and to make recommendations to secure a system.

You will gain credit for:

- making correct technical claims about the system being tested;
- describing how you obtained information about the system;
- providing evidence (such as screenshots or logs) to support your claims;
- explaining how tools or attacks work and how to protect against them;
- linking to references to support your claims and explanations;
- using clear, correct English and structuring your report clearly.

Your assignment will be marked according to the mark scheme outlined in Section 4. The mark scheme is designed so that the mark obtained in this way will correspond to the following qualitative degree classification descriptions:

Degree Classification	Description
First Class (>= 70%)	Excellent
Upper Second Class (60-69%)	Good
Lower Second Class (50-59%)	Satisfactory
Third Class (40-49%)	Poor
Pass (35-39%)	Very Poor
Fail (0-34%)	Inadequate

4. MARKING SCHEME

Marks will be awarded for each part of the assignment as follows:

1. Page 1: Information gathering. (20%)
    1. Network scanning tool output. (10%)
    2. Explanation of output. (10%)
2. Page 2: Penetration testing: vulnerability 1. (20%)
    1. Evidence of vulnerability. (10%)
    2. Explanation of exploit. (10%)
3. Page 3: Penetration testing: vulnerability 2. (20%)
    1. Evidence of vulnerability. (10%)
    2. Explanation of exploit. (10%)
4. Page 4: Recommendations. (20%)
    1. Mitigation of vulnerability 1. (5%)
    2. Mitigation of vulnerability 2. (5%)
    3. Other technical or procedural recommendations. (10%)
5. Writing and presentation. (20%)
    1. Layout and formatting of report. (10%)
    2. Correctness and clarity of English. (10%)

A reasonably complete, clear and correct answer for a component of the assignment will be awarded full marks. Incomplete, unclear or incorrect answers may be awarded partial marks.