Murdoch University

ICT287 Computer Security

Due Dates: LMS

Assignment Information

You must **submit your assignment online using the Assignment submission on LMS**.

This is a group assignment. Each group consists of 2 or 3 students. Smaller or larger groups will only be allowed in extreme circumstances and only if approved by the unit coordinator before the topic approval deadline.

Late submissions will be penalised at the rate of 10% of the total mark per day late or part thereof.

You should submit your assignment as ONE word-processed document containing **all** of the required question answers. The document must have a title page indicating the assignment, student name and number and the submission date. The document must be submitted in **PDF format**.

You **must** keep a copy of the final version of your assignment as submitted (PDF and source document) and be prepared to provide it on request.

The University treats plagiarism, collusion, theft of other students' work and other forms of academic misconduct in assessment seriously. **Any instances of academic misconduct in this assessment will be forwarded immediately to the Faculty Dean.** For guidelines on academic misconduct in assessment including avoiding plagiarism, see: http://our.murdoch.edu.au/Student-life/Study-successfully/Study-Skills/Referencing/

VULNERABILITY RESEARCH PROJECT

Following on from your successful analysis of *Planet of the Grapes* you have been recruited as a full time security administrator by an online partner organization *Paul's Wine Network (PWN).* In addition to your regular admin tasks, one of your roles is to provide training and education to the rest of the team. To do so, you will choose a security vulnerability, document it and provide a demonstration and presentation to educate others about the significance of this vulnerability.

The aim of this project is to put your skills to more practical use. In this project you will research and learn about a security vulnerability and then develop a test environment to demonstrate this vulnerability. You will demonstrate the vulnerability to other students in class. Your report will contain details on the vulnerability as well as on mitigation strategies.

It is anticipated that students will attempt a very diverse range of projects; specific details of the project may be discussed with your teacher in class to give you more guidance.

The project has two phases: (1) topic proposal and (2) actual project.

Topic Proposal

You must organise yourself into a group of 2 (or 3 students only in extraordinary cases) and pick a vulnerability you want to tackle. Your tutor/teacher can help you to find a group. However, it is not your teacher's responsible to suggest vulnerabilities to you.

You must submit a one-page document containing the list of group members (student names and numbers), the vulnerability (CVE number and name) and a 2-3 paragraph description of the vulnerability and how you plan to demonstrate it via LMS by the topic proposal deadline. The description must be written by you and not be copied from other sources. It should demonstrate that you actually understand the basic of the vulnerability is and how it could be demonstrated. The topic proposal submission is worth 5/100 for a proposal submitted on time. No extensions (including EQAL) will be given for the topic proposal and any late submissions will receive 0 marks.

Vulnerabilities without CVE identifier will only be accepted at the discretion of the unit coordinator and only if you can make a good case at least 1 week prior to the proposal deadline.

Each vulnerability must be approved by your tutor/teacher, so make sure you get the approval prior to the submission.

Please note that in each lab/workshop one CVE can only be picked by one group. This is so the final demonstrations are not just a repetition of the same vulnerability, but everybody will learn about several vulnerabilities. **Check with your teacher which vulnerabilities are still available before topic submission and submit the topic proposal early to get the vulnerability of your choice.**

The following requirements apply. The selected vulnerability must have a significant impact (as per the CVE rating) and must have the potential to be reasonably widespread as in it should be a vulnerability that affect(ed) reasonably popular OS/application/devices. You can only choose vulnerabilities that are from 2017 or newer. You cannot choose vulnerabilities that are trivial to exploit, for example a vulnerability where in some version of some application authentication was disabled accidentally and there is no real exploit needed at all is not a valid choice.

Pick a vulnerability that really interests you and for which you can actually set up a demonstration (choosing open source OS and applications can be easier to deal with).

Absolutely no extensions will be given for the topic proposal. Any late submissions will receive 0 marks for the topic proposal component.

Project

The main activities that you will undertake are as follows:

1. Describe and explain the vulnerability **with a reasonable high level of technical detail** in your own words. **A copy of a CVE report is not acceptable and a superficial description will attract low marks.** The description must include outcomes of the vulnerability, i.e. what it can be used for, what level of access it provides, and which systems are affected by the vulnerability.

2. Identify a system or systems where the vulnerability exists "in the wild". You can use operating system or application statistics to proof your point or find vulnerable systems via search engines, such as Shodan. You can also take into consideration previous studies on the vulnerability, but make sure you properly reference these.

3. Describe and explain mitigation and prevention strategies that can be used to protect against the vulnerability. These should be specific strategies for the chosen vulnerability and you must provide sufficient detail. For example, simply saying "there is a patch" is not sufficient, but you should provide detailed information, such as a patch number or a version number of the software that fixes the problem.

4. Build a test environment that allows to demonstrate the vulnerability. The test environment should be saved as one or more Virtual Box VM image(s) that are self-contained and need to be submitted. You are not allowed to reuse any of the provided lab VMs. Credentials for the test environment must be:

Account Type	Username	Password
Administrator Account*	admin	admin
Regular user	user	user

*Under Unix the username/password can be root/root.

If you submit a VM that we cannot access, due to wrong credentials or any other reasons then you will get 0 marks for the VM submission component.

You are not permitted to demonstrate a vulnerability by simply running metasploit. However, you can use existing code (including code from metasploit). For pretty much every existing vulnerability you will find code. There are no limits to programming languages, you can choose whatever you like. In the report you need to be able to explain the code (even if you haven't written it). The idea is that you actually fully understand your vulnerability and how it works, something you will not learn from just running a tool like metasploit. You are permitted to use msfvenom to build payloads.

You need to document the setup of the test environment. This does not need to include trivial steps, like how to install Windows/Linux, but any configuration/installation for the vulnerability must be documented in detail.

You also need to write a step-by-step explanation of the vulnerability demonstration. The level of detail must be such that the teacher can use your VM(s) and test the vulnerability. The outcome of the exploit must be described as well.

Assessment Items

The following items need to be submitted for assessment:

1. Submit the topic proposal on LMS (before you submit, discuss it with your teacher first!). **This is a mandatory component of the assignment.**

2. Submit a written report on LMS discussing the
    a. Explanation and documentation of vulnerability (approximately 2-3 pages);
    a. Existence of the vulnerability in production systems (roughly 1 page);
    b. Documentation for setting up the test environment (the length of this depends on the vulnerability. Screenshots are very useful here.);
    c. Demonstration of the exploit in action (again the length varies, but you must use screenshots to illustrate the different steps and the outcome);
    d. Mitigation and prevention strategies for the exploit (this should be more than simply "patch the software". You should refer to your explanation of the vulnerability to explain how and why the mitigations are suitable (roughly 1-2 pages).

    This is a mandatory component of the assignment.

3. Demonstrate the test environment and exploit to your fellow students in class. This is meant to be a practical demonstration rather than a slide presentation. However, you should think about how to demonstrate it best, so that other people can understand what you are talking about. Your demonstration should have a clear structure, such as introduction, vulnerability explanation, demonstration, mitigation techniques, but you don't need to create any slides. The demonstration will conclude with a short question and answer section. **This is a mandatory component of the assignment and will be done in the last lab/workshop time slot (internal students) or with a screen capture video with audio commentary (external students).**

4. Submit the test environment (VMs). Due to the size of the test environment, it can usually not be submitted via LMS and you need to submit it directly to your teacher, for example via USB stick. **This is a mandatory component of the assignment.**

Note that NOT submitting one of the mandatory components will result in a fail in this assessment, i.e. your mark for this assessment will be capped at a maximum of 49.

The overall mark allocation is as follows:

Topic approval submitted by deadline with 2-3 paragraph self-written description of vulnerability	5
Written report as described above containing vulnerability description (20), description of possible impact (10), description of setup (VM, tools etc.) and how to exploit the vulnerability (20) and mitigation strategies (10). Presentation (5) is also marked.	65
Submission of VM	0
Demonstration of exploit and Q&A	30