Murdoch University

ICT287 Computer Security

Due Dates:
Topic proposal: Sunday 25th Feb 2024, 23:55
Description report: Sunday 3rd Mar 2024, 23:55
Demo report: Sunday 7th Apr 2024, 23:55

Assignment Information

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

You must do this assignment as an individual student.

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

You should submit each part of your assignment as ONE word-processed document containing **all** the required parts and/or question answers. The documents, except the initial proposal, 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 reported to the University's academic misconduct investigators.** 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

You have been recruited as a full-time security administrator. In addition to your regular 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 the vulnerability, and provide a demonstration and presentation to educate your team members about the significance of this vulnerability and how it can be mitigated.

The aim of this project is to put your skills to 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 reports will contain details on the vulnerability, the setup and demonstration 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 three phases: (1) topic proposal, (2) vulnerability description and (3) vulnerability demonstration and vulnerability exploitation final report.

Topic Proposal

You must pick a vulnerability you want to tackle. It is not your teacher's responsible to suggest vulnerabilities to you. **Each vulnerability must be approved by your tutor/teacher, so make sure you get the approval prior to the submission.**

To get approval for this vulnerability, you must contact your tutor/teacher via email. Your email must contain:

1. Your name and student number
2. Vulnerability (CVE number and name)
3. One or two paragraph description of the vulnerability which must be written by you and not be copied from other sources.
4. One paragraph description of the software you will use for the exploitation. This must include both the exploit code and the vulnerable software of the target and must also include links that demonstrate where you will obtain the software from.

A vulnerability is only approved, after your tutor/teacher has approved your proposal in writing via email. **You must contact your tutor/teacher no later than 1 week prior to the vulnerability description report deadline to obtain approval before submitting the vulnerability description report. Submitting a vulnerability description report for an unapproved vulnerability will result in 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 deadline of the first report.

The following requirements apply. Any choices that do not fulfil the requirements are automatically rejected (or if submitted will result in 0 marks) unless an exception has been granted by the unit coordinator in writing.

1. **In each lab/workshop one vulnerability can only be picked by one student.** 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.**
2. The selected vulnerability must have a significant impact (5.0 or higher 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.
3. The vulnerability must be from **the year 2021 or newer** (as per CVE).
4. 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 interests you and for which you can set up a demonstration (choosing open-source OS and applications can be easier to deal with).

Vulnerability Description

The activities that you will undertake are as follows:

1. Describe and explain the vulnerability **with a 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. 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 enough, but you should provide detailed information, such as a patch number or a version number of the software that fixes the problem.
3. Describe how to demo the exploit of the vulnerability. This plan should list the required software, operating systems, code etc. that is required and provide an overview on how an exploitation demonstration will work.

Vulnerability Exploitation

The main activities that you will undertake are as follows:

1. 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 unless you have obtained permission from the unit coordinator to do so.

You should use the following credentials for your test environment:

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

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

You may choose different credentials but, in this case, you must document the chosen credentials very explicitly in your report.

If you submit a VM that we cannot access, due to wrong credentials or any other reasons then you will get a penalty of 20% of the total marks for this report.

You are not permitted to demonstrate a vulnerability by simply running Metasploit (msfconsole), any tool based on Metasploit (msfconsole) or any similar tool that provides a range of vulnerabilities with an easy-to-use interface. 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. **If you are in doubt, discuss it with your teacher first.**

In the report you need to be able to explain the code (even if you haven't written it). The idea is that you 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.

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

3. 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 and a reader of the report will understand what happens in each step. The outcome of the exploit must be described in detail as well.

4. Prepare and give a live demonstration of the exploitation and prepare to be asked questions after the demonstration. Demonstrations must be presented live either face-to-face (on-campus students) or via video conferencing tool (off-campus students). Screen capture videos of parts of the demo are permissible in extenuating circumstances, e.g. if the vulnerability needs a long time to pull it off, and only if approved by the unit coordinator.

Assessment Items

The following items need to be submitted for assessment:

1. Topic proposal (proposal and approval via email).
   This is a mandatory unmarked component of the assignment.

2. Vulnerability description written report:
   a. Introduction (1-2 paragraphs) providing an overview of the report.
   b. Explanation and documentation of vulnerability. This should explain all the technical details, the outcome of exploitation and affected systems.
   c. Mitigation and prevention strategies for the exploit. This should be more than "patch the software". You should refer to your explanation of the vulnerability and explain how and why the mitigations are suitable (no more than 1 page).
   d. Plan for exploiting vulnerability (no more than 1 page).

   This is a mandatory marked component of the assignment.

3. Vulnerability exploitation written report:
   a. Introduction (1-2 paragraphs) providing an overview of the report.
   b. Explanation and documentation of vulnerability. This can be taken from the previous report but should be improved as required.
   c. Documentation for setting up the test environment. Screenshots are very useful here. All steps specific for the vulnerability must be explained.
   d. Demonstration of the exploit in action. You must explain all steps and the outcome. You must use screenshots to illustrate the different steps and the outcome.

   This is a mandatory marked component of the assignment.

4. Demonstration of 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. You don't have to create any slides, but it is highly recommended to have a few slides for the vulnerability explanation and mitigation parts. The demonstration will conclude with a short question and answer section.
   This is a mandatory marked component and will be done in the last teaching or exam prep week face-to-face (internal students) or in an online session (external students). Details will be announced in the middle of the teaching period.

5. Test environment (VMs). Due to the size of the test environment, it cannot be submitted via LMS and you need to submit it to your teacher via MS OneDrive using **your student account** (as a Murdoch University student you automatically get free space on OneDrive). A link to your uploaded VMs must be included in the report and you should also send your tutor an email with the link and instructions on how to access the VMs.
   This is a mandatory unmarked 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.

Assessment

The overall mark allocation out of 40 marks is as follows:

Vulnerability Description Description (8 marks) will be marked on the level of detail provided, correctness of description and structure and clarity of the description. Mitigation (3 marks) will be marked based on correctness, completeness, clarity, level of detail and how well it refers back to the mechanics of the vulnerability and exploit. The plan (3 marks) will be assessed on whether it is sound, realistic, fulfills the goals of demonstrating the important aspects of the vulnerability succinctly and completeness of the description. **Approval from your tutor/teacher for the vulnerability must have been obtained in writing before you submit this. A report for an unapproved vulnerability will be marked with 0.** **The maximum length for this report is 6 pages (excluding title page, ToC, references, and appendices with supplementary material). Documents longer than the allowed limit may receive a penalty of 10% for each page over the limit.**	14 (35%)
Vulnerability Exploitation Vulnerability description (2 marks) will be marked on level of detail provided, correctness of description, completeness, and clarity of the description. Description of setup and exploitation (12 marks) will be marked based on completeness, quality of explanation, sensible chosen structure, appropriate details for each part and step, how well it links to the workings of the exploit, how well the setup and demo could be reproduced and how well it demonstrates the exploit. **The maximum length for this report is 12 pages (excluding title page, ToC, references, and appendices with supplementary material). Documents longer than the allowed limit may receive a penalty of 10% for each page over the limit.**	14 (35%)
Demonstration of the exploit and Q&A will be marked based on successful demonstration of exploit, sensible structure of demo, correctness, completeness, quality of explanations and appropriate level of detail for each part, presentation skills and ability to answer questions during Q&A. **The demonstration must not take longer than 10 minutes followed by 2-3 minutes of Q&A. More details will be provided later.**	12 (30%)