**Student Name:** **Weight: 40%**

**Student ID:** **Marks: /170**

Project: Penetration Testing

# Instructions

The purpose of this project is for you to understand both the offensive and defensive perspectives of social engineering. You will first take the offensive position and plan an attack based on organizational vulnerabilities. Then you’ll take the defensive position and plan a mitigation strategy for the organization.

In Assignment 2, you have already done preliminary research on a target organization for exploitable information and demonstrated some infiltration techniques based on principles of human psychology. For this Project, you will take that research a step further. You will need to get approval from the instructor of the organization you wish to target.

In this Project, you will go beyond the first steps and proceed to evaluate an entire organization’s vulnerabilities to defend it against potential threats. You will also create a plan to mitigate vulnerabilities caused by the human factors that can undermine security protocols.

**Provide a detailed report that includes:**

* title page with the list of group members
* table of contents
* references in APA7 or IEEE format (if any)

**The report must outline:**

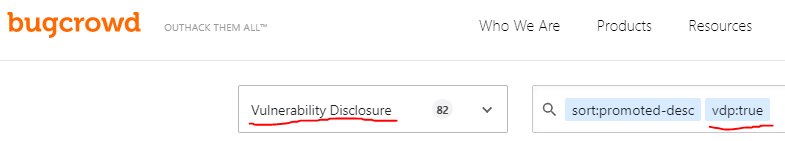
1. The organization that you plan to penetrate and why
2. The organization’s vulnerabilities
3. A mitigation strategy for the organization

You will work in a group of up to five members. This assignment will be completed outside of class. The marks referred to in the Marking Guide below are to provide guidance as to the relative weight to be placed on the various criteria.

**Choosing the organization**

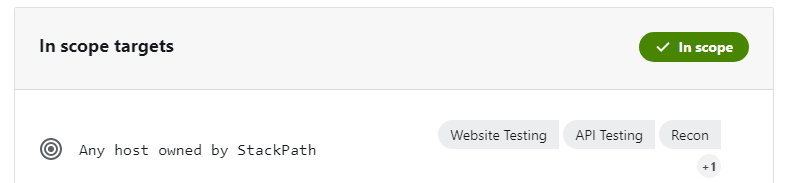
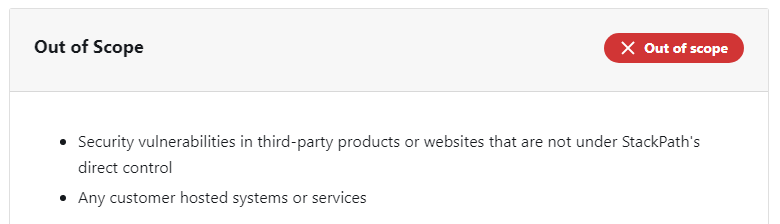
You must choose an organization that appears on the **Bugcrowd’s Vulnerability Disclosure Program (VDP)** list. To find the list of organizations, navigate to <https://bugcrowd.com/programs>

and filter the organizations by “Vulnerability Disclosure”.



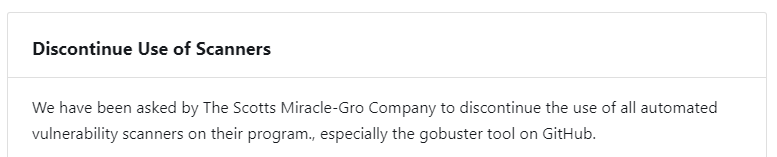
Once you choose the organization, confirm that **you understand in scope** and **out of scope** requirements.

Example:

Check the **Announcements** for your chosen organization to confirm that there are no new restrictions.

Example:



Once you select organization, you will need to get approval from the instructor before continuing.

**Follow the steps below using your chosen organization:**

**Part A (10%)**: **Overview of the target organization and why you chose it**

* What are the potential criminal threats that the specific organization is subject to?
* What are the common vulnerabilities for organizations in this industry?
* What motivated you to choose this specific organization?

**Part B (20%)**: **Information gathering and report**

* Conduct online target research on your chosen organization and provide a detailed report of what you what you found, where you found it and how it opens the organization up to social engineering attempts.
* Conduct any additional research and provide a detailed discussion of the information you find. **This research must be within the scope of the Bugcrowd’s VDP. If you are unsure, discuss any additional details with your instructor first to ensure legality.**
* Provide a detailed report for the organization that outlines its vulnerabilities based on your research. (Some of your earlier research may be used for this section.)
* Provide a detailed example of how this information could be used by a social engineer (i.e., how you would penetrate the company). This section should provide a step-by-step account of how the attack would take place. For example, is there a particular employee or department that a social engineer would contact in order to get further information? What kind of information could you obtain? How would this information be used?

**Part C (10%): Mitigation strategies.**

* Suggest practical mitigation strategies which could be implemented to address the vulnerabilities which you have identified.
* Be specific, and conscious of the cost, both in money, time and efficiency for any measures which you suggest.

Marking Criteria

|  |  |
| --- | --- |
| **Introduction (Part A)**   * Introduce the organization. * Provide your audience with enough detail that they will understand *who* the organization is, *what* they do, the industry the organization is part of, and your motivation for choosing this particular organization. | /15 |
| **Common vulnerabilities and criminal threats (Part A)**   * Discuss vulnerabilities common to this industry and provide specific examples of previous cases. Be sure to address the following questions: * Are there vulnerabilities specific only to this organization? Why? * Why do these vulnerabilities exist? * What are potential criminal threats that the organization is subject to? (Provide examples of previous cases.) * What are the typical motivations of social engineers who target these types of organizations? | /30 |
| **Overall**   * The information is presented clearly and concisely. * There is a logical flow to the information. * Terminology is relevant to the fields of social engineering and is defined where necessary. * The language and structure of the report is professional and appropriate. * Part A should not be longer than 4 pages. | /5 |
| **TOTAL** | **/50** |

|  |  |
| --- | --- |
| **Online target research (Part B)**   * Conduct a thorough online investigation of potential organizational vulnerabilities. * Present the information that you find in a detailed manner and discuss the significance of each piece of information (i.e., how it could be used by a social engineer). | /25 |
| **Additional target research**   * Conduct additional research (to be discussed with instructor first) on the target organization. * Present a detailed discussion of the information obtained and the significance of each piece of information. | /20 |
| **Examples**   * Use examples of previous cases that show how similar information has been used in a social engineering attempts in the past. | /10 |
| **Identify Specific Organizational Vulnerabilities**   * Present a detailed list of the vulnerabilities discovered. * Include potential motivations and rationales of hacking, as well as potential employees or departments that pose greater vulnerability. | /15 |
| **Discussion**   * Provide a discussion of how easy or difficult it was to find certain pieces of information. | /10 |
| **Overall**   * The information is presented in a clear and concise manner. * There is a logical flow to the information. * Terminology is relevant to the fields of social engineering and is defined where necessary. * The report is written for the intended audience (executives of the organization).The language and structure of the report is appropriate. | /5 |
| **TOTAL** | **/85** |

|  |  |
| --- | --- |
| **Mitigation strategies (Part C)**   * Provide a detailed discussion of how the organization could mitigate some of the risks discussed in part A. * Connect information from your target research to the mitigation strategy. | /20 |
| **Conclusion**   * Present an overall conclusion that connects parts A, B and C. * Present a compelling discussion of how organizations can become more aware through the use of penetration testing. | /10 |
| **Overall**   * The information is presented clearly and concisely. * There is a logical flow to the information. * Terminology is relevant to the fields of social engineering and is defined where necessary. * The report is written for the intended audience (executives of the organization). The language and structure of the report is appropriate. | /5 |
| **Total** | **/35** |