SIT182- Real World Practices for Cybersecurity T1 2019

Assessment Task 1 Teamwork Report
Due: Sunday April 14th at 11.59pm (end of week 6).
Total Available Marks: 50, Weighting 30%
(Teamwork Report Marks: 40, Weighting 20%
Individual Contribution Marks: 10, Weighting 10%)

General Requirements

The 'Teamwork Report' TEMPLATE and 'Individual Contribution' TEMPLATE provided in the assessments folder on the Unit Site MUST be used to complete this assessment.

- NO EXTENSIONS allowed without medical or other certification.
- LATE ASSIGNMENTS will automatically lose 5% per day up to a maximum of five days, including weekends and holidays. Assignments submitted 6 or more days late will not be marked and are given zero.
- You **MUST** use the ***SIT182 Assessment*** Pod to perform the tasks required for the Team Work Report. This is available from the VMLab system: https://vmlab.it.deakin.edu.au/
- As with the practicals there are a limited number of pods available for this assessment. It is critical that you organise a schedule for using the pods and begin the work required early to ensure you can complete on time.
- NO work is saved or backed up on the pod – if your pod reservation expires, and you make a new reservation, where you were previously will not be saved and you will need to perform the steps again.
- Ensure you take screenshots of your work for evidence and that these are legible in your report.
- To complete this assessment you will need to do research, review the class material and complete the practicals for weeks 1-4.
- Your submission must be in a form readable by Microsoft Word.
- **EACH GROUP IS ONLY REQUIRED TO SUBMIT 1 TEAMWORK REPORT**. The report must not be more than 22 pages (including cover page and table of contents), each page must have margins no less than 2cm, and font size no less than 11 point. Oversized assignments will be penalised.
- Each student **MUST SUBMIT AN INDIVIDUAL CONTRIBUTION** with the same formatting guidelines as the teamwork report.
- Ensure you keep a backup copy of your work.
- Plagiarism is not tolerated. For information on Plagiarism and Collusion including penalties please refer to the link: http://www.deakin.edu.au/students/clouddeakin/help-guides/assessment/plagiarism
- The APA Referencing Style is to be used for this assignment where appropriate. https://www.deakin.edu.au/students/studying/study-support/referencing/apa-6

Help with the assessment

It is important to understand this is a challenge and will require you to work in a team and apply your knowledge and skills learned to a real world scenario. Also make sure you don't share your progress or solutions with other groups.

If you require assistance please ask your instructors (Burwood students ask your practical demonstrator; Geelong and Cloud students ask Damien Hutchinson). We will **NOT** answer questions that are requesting answers or solutions. A question MUST be substantiated with evidence that work has been attempted relating to the question being asked.

Objectives of the assessment

The learning objectives of this assessment task are to:
ULO 2 Work as a team to assess the impact of social engineering attacks in various organisations and analyse the effectiveness of its countermeasures.
ULO 3 Improve the level of security of systems with remote control by using proper access control, authentication, privilege management and encryption methods.
ULO4 Apply the appropriate use of tools to facilitate network security to prevent various types of computer and network attacks, and malicious software that exists

Cybersecurity Scenario

A network security solutions company called 'NETsec' provides security solutions for their clients. They want to ensure that their web system is appropriately secured and protected from potential cybersecurity attacks. This is of upmost importance for maintaining an exemplary reputation and business relationships with their clients. Given NETsec is in the business of providing security services, a successful breach could result in the collapse of their company.

To ensure this does not happen NETsec has requested the services of your team to apply the necessary knowledge and skills to identify any security vulnerabilities, attempt to infiltrate their system by performing attacks and providing appropriate recommendations so countermeasures can be applied.

Teamwork report

Each group is to work as a team and submit a report of approximately 2000 words and exhibits following the Teamwork Rubric provided. In order to be eligible to be awarded maximum marks for each rubric criterion the report MUST include *descriptions and evidence of results of the steps performed*. The difference between a HD and P grade will be the cohesiveness between sections of the report and tasks performed, and not just parts of the work being completed by different members and 'glued' together.

Your team is required to perform the following cybersecurity attacks in an attempt to subvert the security of the NETsec Web system and ultimately gain access to the restricted administration page of the website:

- Perform a bruteforce password attack;
- Perform a privilege escalation attack;
- Perform a social engineering attack.

Individual contribution

A major component of this assessment task is teamwork. As outlined in the Unit Guide, teamwork is Deakin's GLO7 (Graduate Learning Outcome number 7) and requires demonstration of working and learning with others from different disciplines and backgrounds.

In week 2 we had a guest speaker during the class present on the importance of teamwork and the tools to be used for the individual contribution component of this assessment task. If you did not make it to class, ensure you review the recording.

Each student is to submit a reflection of their individual contribution to team work.
Your reflection will be developed by completing the following tasks:

1. Create your Self-Evaluation of Teamwork Behaviours – BEFORE document
2. Create your Self-Evaluation of Teamwork Behaviours – AFTER document
3. List one of the statements including its BEFORE and AFTER rating where the rating changed because of your contribution to the team project. Briefly describe (approx. 100 words) how you think your contribution facilitated the change.
4. Provide a reflection (approx. 100 words) on the output of your SPARKPLUS self and peer assessment and feedback. Include your RPF (Relative Performance Factor) and choose a criterion e.g. DISCUSSION from one of the categories e.g. CONTRIBUTION TO TEAM TASK to describe the difference/similarity between your self-assessment and peer assessment feedback.

Assessment Rubric

TEAMWORK RUBRIC TOTAL AVAILABLE MARKS 40			
Executive Summary	**0 marks**	**3 marks**	**6 marks**
Identification of cybersecurity problems and recommendations	Missing	Missing description of 3 major security problems or recommendations	List and description of 3 major security problems and recommendations provided
Report Structure	**0 marks**	**0.5 marks**	**1 mark (each)**
Table of contents	Missing	Incomplete TOC or poor report layout or poor report cohesion	Complete TOC and good report layout and good report cohesion
Introduction	Missing	Overview of scenario and objective(s) lacking in detail	A comprehensive overview of the scenario and objective(s) provided
Conclusion	Missing	Missing description of cybersecurity information related to the case or analysis and presentation of solutions	Description of cybersecurity information related to the case and analysis and presentation of solutions provided
System Environment	**0 marks**	**0.5 marks**	**1 mark (each)**

Overview of networked IT infrastructure	Missing/incorrect	Missing Topology Image, or description or how the machines are linked together	Topology Image and description including how the machines are linked together provided
Description of machines	Missing/incorrect	Missing description or screenshots of machines	Description and screenshots of Machines provided
Access to Website on client machine	Missing/incorrect	Missing description or screenshot of access to Website on client machine	Description and screenshot of access to Website on client machine provided
Locate and analyse system information	**0 marks**	**0.5 marks**	**1 mark (each)**
Website description	Missing/incorrect	Missing description of the website or what you can/cannot get access to or screenshots	Describe the website and what you can/cannot get access to with screenshots
Access and analyse network logs	Missing/incorrect	Missing Description of process used to analyse logs or distinguishing between protocols and traffic	Describe process used to analyse logs Distinguish between protocols and traffic
Identify access credentials	Missing/incorrect	Missing identification of access credentials or description or screenshot	Access credentials identified, described and screenshot provided
Identify the attack vector and target	Missing/incorrect	Missing identification of attack vector or target of attack	Identification of attack vector and target of attack provided
Establish Remote Access	**0 marks**	**3 marks**	**7 marks**
Perform attack to access Web server remotely using tool(s) located on the attack machine	Missing/incorrect	Missing description and demonstration of the tool(s) used or less than 4 screenshots or the attack procedure or separate screenshot confirming remote access	Description and demonstration of the tool(s) used and at least 4 screenshots of the attack procedure and separate screenshot confirming remote access provided.
Privilege escalation attack	**0 marks**	**0.5 marks**	**1 mark (each)**

Identification of path to Web folders and files on server	Missing/incorrect	Missing description or screenshot of Web folder and path	Description and screenshot of Web folder and path provided
File listing	Missing/incorrect	Missing file listing or screenshot with permissions or description of 3 files	File listing including screenshot with permissions and description of 3 files provided
Identify file vulnerability	Missing/incorrect	Missing identification of file vulnerability or explanation in terms of access control or screenshot	File vulnerability identified and explained in terms of access control and screenshot provided
File transfer procedure	Missing/incorrect	Missing description of file transfer procedure or screenshot	Description of file transfer procedure and screenshot provided
Modification of file to escalate privileges	Missing/incorrect	Missing description of modification procedure or screenshot	Description of modification procedure and screenshot of successful file modification provided
Execute script	Missing/incorrect	Missing description of how script was executed and result or screenshot	Description of how script was executed and result including screenshot provided
Login to Website interface	Missing/incorrect	Missing description of credentials used to login to interface or screenshot	Description of credentials used to login to interface and screenshot provided
Social Engineering attack Design	**0 marks**	**3 marks**	**7 marks**
Spear-phishing email design	Missing/incorrect	Missing design of phishing email to convince CTO to provide credentials to gain access to administration account or screenshot to clearly identify at least 5 elements of the attack	Design of phishing email to convince CTO to provide credentials to gain access to administration account Screenshot to clearly identify at least 5 elements of the attack provided

Perform Social Engineering attack	**0 marks**	**0.5 marks**	**1 mark (each)**
Execute attack on CTO	Missing/incorrect	Missing sending email using client outside of VMlab or screenshot	Email using client outside of VMlab sent and screenshot provided
Demonstration of attack success	Missing/incorrect	Missing reply from CTO or screenshot	Reply received from CTO including screenshot
Access to administration login	Missing/incorrect	Missing demonstration of successful login as administrator or screenshot	Demonstration of successful login as administrator including screenshot provided
END OF RUBRIC			

INDIVIDUAL CONTRIBUTION RUBRIC TOTAL AVAILABLE MARKS 10		
Teamwork Behaviours	**0 marks**	**1 mark**
Create your Self-Evaluation of Teamwork Behaviours – BEFORE document	Missing	Completed
Create your Self-Evaluation of Teamwork Behaviours – AFTER document	Missing	Completed
Reflection on Teamwork Contribution **MUST INCLUDE ALL 3 ELEMENTS LISTED TO RECEIVE A MARK ELSE 0 MARKS WILL BE AWARDED**	**0 marks**	**3 marks**
1. Statement listed 2. BEFORE and AFTER rating 2. Description of how you think your contribution facilitated the change	Missing	Completed
1. SPARKPLUS RPF is stated. 2. Criterion from one of the categories included. 3. Description of the difference/similarity between your self-assessment and peer assessment feedback.	Missing	Completed
END OF RUBRIC		