# University of Westminster
## School of Computer Science and Engineering

| 6COSC019C Cyber Security<br>Assignment Specification (2022/23) | |
|---|---|
| Module leader | Saman Hettiarachchi |
| Unit | Coursework |
| Weighting: | 50% |
| Qualifying mark | 30% |
| Description | Scenario-based lab report: Answers are based on all labs. |
| Learning Outcomes Covered in this Assignment: | LO3 Evaluate security architecture and design and provide the means to enhance operation security;<br><br>LO4 Examine cryptography protocols and vulnerabilities and identify attack vectors to exploit them;<br><br>LO5 Synthesise emerging trends through engagement and analysis with current research. |
| Handed Out: | Wednesday 08 February 2023 |
| Due Date | Tuesday 09 May 2023 at 01:00 pm |
| Expected deliverables | Single Report |
| Method of Submission: | Electronic submission on tunrnitin (in PDF format) name your file with your student number and the module code. i.e.: W000000000_7BUIS022W |
| Type of Feedback and Due Date: | Written feedback and marks will be given 15 working day (3 Weeks) after the submission deadline. **All marks will remain provisional until formally agreed by an Assessment Board.** |

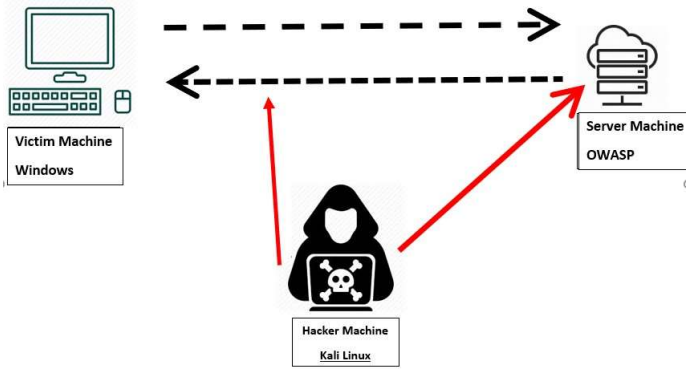
**Assessment regulations**

Refer to section 4 of the "Framework for undergraduate course" guide for undergraduate students for a clarification of how you are assessed, penalties and late submissions, what constitutes plagiarism etc.
https://www.westminster.ac.uk/sites/default/public-files/general-documents/Section-17-Framework-forundergraduate-taught-courses-2022.pdf

**Penalty for Late Submission**

If you submit your coursework late but within 24 hours or one working day of the specified deadline, 10 marks will be deducted from the final mark, as a penalty for late submission, except for work which obtains a mark in the range 40 – 49%, in which case the mark will be capped at the pass mark (40%). If you submit your coursework more than 24 hours or more than one working day after the specified deadline, you will be given a mark of zero for the work in question unless a claim of Mitigating Circumstances has been submitted and accepted as valid. For more detailed information regarding University Assessment Regulations, please refer to the following website:[http://www.westminster.ac.uk/study/current-students/resources/academic-regulations](http://www.westminster.ac.uk/study/current-students/resources/academic-regulations)

# Coursework description




To be able to complete your assessment use the lab exercises and activities to map to your allocated scenario. You will have three VMs, the Victim machine (**Windows**), the server machine (**OWASP**) and the hacker machine (**Kali Linux**).

# Building your scenario [3 marks]

- **Each of you will need to build their own scenario for a company.**
- Your scenario must have the following requirements:
  - Your scenario public website is https://cwscenario.site/
  - A database and web services
  - Users
- Your should defne the following assumptions for your scenario:
  1. **Type and size of business:**
     - it could be any type of business as long as you defne it.
     - This is important as it will also defne the type of users and data for your information system environment.
     - For example: A school, an estate agent, an engineering company, etc..
     - The size of the organisation is important as it will dictate how many users there are, where do they access, etc..
     - For example a business can be a startup with 10 users working in one ofce, a small school with 20 teachers and 200 students or a multi national company with thousands of users.
  2. **Type of data:**
     - The type of data is relevant to the business type you chose.

- For example, a school will hold information about the students. This could be financial information, personal information or marks and progress records.
- The type of data the organization holds will dictate the type of controls you put to protect your data.

3. **Type of users:**
   - The type of users is relevant to the business type you chose.
   - For example a school can have teachers and parents as users.
   - The type of users the organization have will dictate how complex accessing your system is.
   - it could be any type of business as long as you define it.
   - This is important as it will also define the type of users for your information system environment.
   - For example: A school, an estate agent, an engineering company, etc.

‹ **Below is a scenario example with all the assumptions and requirements defined.**

My company was hired to conduct a penetration test for a **medium sized estate agent company** with **many branches** across the UK. Their web application allows their potential customers to search for properties and book appointments. The website does not hold any financial data for the properties owners but stores **personal information** for **potential customers** who are interested in the property. **Staff** can access the web application to **manage properties on the web application**. Staff receive potential customers enquiries by email. **Staff credentials** are stored on the database.

‹ **You must not use the same example for your assignment.**

## Requirements and Deliverables

**You have completed your penetration testing assessment on the scenario application and identified their vulnerabilities and weaknesses.**

**You are now expected to document your findings in a penetration testing report.**

**Your report should contain all the information below that are required by the company that hired you.**

**You should assume that the person reading the document does not have a technical background**

**You should show that you were able to identify or exploit vulnerabilities and explain them.**

**You should explain the impact of those vulnerabilities and exploits on the system.**

**Report requirements for your client**

A- Information Gathering

(1) OSINT Activities

- Show three examples of your Open-Source Intelligence (OSINT) investigation activities you have carried out on your scenario example. [3 marks]
- Research and evaluate how OSINT can be effective and explain why it is one of the first activities that penetration testers carry out. [3 marks]
- *Scenario assessment:* In your opinion, how dangerous are the information you were able to obtain for your allocated scenario [2 marks]

(2) Reconnaissance

- Show some of the information you were able to obtain by testing web applications in the lab. [3 marks]
- *Scenario assessment:* Explain how the information obtained by testing the web applications can be used at a later stage to exploit company's web services? Give an example of information that can be relevant to your scenario. [3 marks]

(3) Port Scanning and Enumeration

- Show that you have identified the ports you found in the lab running on the server machine. [3 marks]
- Research and explain what an open port means and identify threats an open port can potentially causes? [3 marks]
- *Scenario assessment:* Explain the threats of the open ports you have identified when carrying the port scanning and how dangerous they are for your scenario and the data your scenario company holds. [3 marks]

B- Server-side exploits

(1) Data tampering

- Identify if the application is vulnerable to data tampering and exploit it if possible. [3 marks]
- Briefly research and explain data tampering vulnerability. Which Cyber Security tenet this vulnerability violates? [2 marks].
- *Scenario assessment:* What is the vulnerable information for data tampering that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [2 marks]

(2) SQL injection

- Identify if the application is vulnerable to SQL injection and exploit it if possible. [3 marks]

- Briefly research and explain SQL injection vulnerability. Which Cyber Security tenet this vulnerability violates? [2 marks].
- *Scenario assessment:* What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [2 marks]

(3) XSS Scripting

- Identify if the application is vulnerable to XSS vulnerability and exploit it if possible. [3 marks]
- Briefly explain XSS scripting vulnerability. Which Cyber Security Tenet this vulnerability violates? [2 marks].
- *Scenario assessment:* What are the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [2 marks]

(4) OWASP vulnerable machine contains several other vulnerabilities that can be exploited.

- Identify two other vulnerabilities you were able to identify in the vulnerable machine. [2 marks]
- *Scenario assessment:* Research and investigate their threats for your scenario and identify which Cyber Security tenet these vulnerabilities violate? [2 marks]

C- Client-side exploits

(1) Man in the Middle Attack (MiTM)

- Show how the attacker can capture traffic from a session between a genuine user and the server side of the application. [3 marks]
- *Scenario assessment:* What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [4 marks]

(2) Social engineering attack

- Show how an attacker can lure a normal user of the server to your computer instead of the server machine. [3 marks]
- *Scenario assessment:* What is the information that attackers can obtain when this activity is carried out and how dangerous they are for your scenario? [4 marks]

D- Denial of Service attacks

(1) DoS the web server

- Show how an attacker can carry on a denial-of-service attack on the web server. [2 marks]

- Which Cyber Security Tenet this vulnerability violates? [1 mark]
- *Scenario assessment:* What is the impact of this attack on your scenario company? [2 marks]

E- Recommendations to protect the scenario company server.

(1) Briefly research what you can do to minimize the threats to the findings in the reconnaissance phase when you tested the web application in section A.2. [2 marks]

(2) Briefly research what port knocking is and explain how it can protect against threats you have identified in section A.3. [2 marks]

(3) Briefly research and explain how to protect your database against SQL injection exploited in section B.2. [3 marks]

(4) Briefly research and explain how to protect your web application against cross site Scripting attacks exploited in section B.3. [3 marks]

(5) Investigate what activities a security analyst can carry out to protect, or at least minimize the impact of Man in the Middle attack carried out in section C.1 [3 marks]

(6) Research the work that companies should do to ensure that their users do not fall victims to social engineering attacks similar to the attack you carried out in section C.2. [3 marks]

(7) Research and explain what companies do to protect their web services against a DoS attack similar to the one you have carried out in section D.1. [2 marks]

(8) Intrusion Detection and Prevention systems

- Show some examples of firewall and iptables rules that can protect your scenario company against attacks you identified in the assessment you carried out before. [3 marks]
- Evaluate the effectiveness of the following tools and specify which is more suitable for your scenario and justify you answers. [3 marks]
  - Firewall (ufw)
  - iptables
- Explain the differences between Intrusion Detection System IDS and Intrusion prevention System IPS. [3 marks]
- *Scenario assessment:* Suggest a recommendation for the scenario you have in hand and justify your answer. [3 marks]

# Learning Outcomes

The following Learning outcomes will be addressed in this assignment:

- **LO3** Evaluate security architecture and design and provide the means to enhance operation security.

- **LO4** Examine cryptography protocols and vulnerabilities and identify attack vectors to exploit them.
- **LO5** Synthesize emerging trends through engagement and analysis with current research.

## Instructions

- You should not exceed **5000 words** in total excluding references page and any appendix you can include.
- References should follow Harvard referencing.

## marking Scheme

| Section | Subsection | Question | Max Points | Marking scheme - rubric (points) | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 0 | 1 | 2 | 3 | 4 |
| Building you Scenario | | | 3 | Student did not define their scenario | Student has defined the scenario including the type of business and size but did not define the type of data or the type of users. | Student has defined the scenario including the type of business and size. The student did not define. either the type of data they hold (Personal, sensitive, etc.) or what type of users access the system and what level of privilege they have (can they edit, delete or only read) | Student has defined the scenario including the type of business and size and the type of data they hold. (Personal, sensitive, etc.). The student also clearly explain the users type and what access privilege they hold (can they edit, delete or only read) . | |
| A- Information Gathering | A1- OSINT Activities | 1 | 3 | Student did not show any evidence that OSINT acticties were conducted or has shown activites that are not related to OSINT. | Student has shown one correct activity example with a screneshot | Student has shown two correct activites with relevant screenshots. | Student has shown three correct activites with relevant screenshots. | |
| | | 2 | 3 | Not attempted or the student did not demonstrate how OSINT can be effective and why it is the first activity a penetration tester would do. | Student has explained briefly how effective is OSINT or Student did not explain why it is the first activity carried out by penetration tester. No references to external sources | Student has explained how effective is OSINT why it is the first activity carried out by penetration tester. No references to external sources | Student has provided a clear explanation of how effective OSINT is and why it is the first activity carried out by penetration tester with references to external sources | |
| | | 3 | 2 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | Student has provided a brief explaination of how dangerous OSINT would be for their scenario. | Student has provided a very good explaination with clear justification on why they believe the information obtained from the OSINT activities are/ are not dangerous to their sceanario | | |
| | 2- Reconnaissance | 1 | 3 | Student did not show any evidence that reconnaissance activities were conducted or has shown activites that are not related to reconnaissance. | Student has shown only one correct activity example with a screneshot such as example of version of wordpress or other web applications available by browing the OWASP page. Student did not put any statement to explain what it is | Student has shown few activity examples screneshots but did not provide any explaination what they represent. | Student has shown few activity examples screneshots and briefly explained what what they represent. | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2 | 3 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | You have discussed some of the results in relation to your scenario.Scenario relevance is not justified. | You have discussed your findings to a great extent in relation to your scenario. A correct exanple was given | You have discussed your findings to a great extent in relation to your scenario. A good example was given | Excellent discussion of your findings in relation to your scenario. An excellent example is provided |
| | 3- Port Scanning and Enumeration | 1 | 3 | Student did not show any evidence that port scanning and enumeration activities were conducted or has shown activites that are not related to port scanning and enumeration . | Log confirms a limited port scanning and enumeration activities undertaken | Port scanning and enumeration Logs are organised and has some structure. You have discussed some of the result | Port scanning and enumeration Log of practical work is organised and professionally presented. Excellent discussion is presented | |
| | | 2 | 3 | No real attempt. Submission is devoid of any meaningful material. Work submitted does not demonstrate that port scanning and enumeration techniques are fully understood.There is no reference to expernal sources. You did not identify threats to open ports. | Work presented does not demonstrate that port scanning and enumeration techniques are fully understood. Threats are not identified and no example given | Work presented demonstrates more than a basic understanding of port scanning and enumeration techniques are fully understood. You briefly identified threats to open ports. An example is given without explaination | Work presented shows very good understanding of port scanning and enumeration techniques are fully understood. You briefly identified threats to open ports. Good example is presented | |
| | | 3 | 3 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | You have discussed your findings to a great extent in relation to your scenario. Good justification is presented | Excellent discussion of your findings in relation to your scenario. Excellent justification is presented | |
| | 1- Data Tampering | 1 | 3 | No real attempt. Submission is devoid of any meaningful material. You did not identify if the application is vulnerable to data tampering. You did not also show any evidence that Data tampering was exploited. | Work presented fails to convey correct use of tools to identify if application is vulnerable to data tampering. You have shown some examples that it was exploiited but they are unstructured and inconclusive | Work presented shows more than a basic correct use of tools to demonstrate how data tampering can be exploited You have shown some examples that it was exploiited. | Work presented shows very clear understanding of how the tools were used and an explanation is provided for each. You have identified that the application is vulnerable to data tampering. You have shown excellent examples of how it was exploiited | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2 | 2 | No real attempt. Submission is devoid of any meaningful material. No research to data tampering. You did not identify the correct security tenet data tampering violates (Integrity) | Some research is provided on Data Tampering but more needed to show a clear understanding and no refernece to external sources. You identified the correct security tenet data tampering violates (Integrity) | Excellent research is also provided on data tampering with very good resources. You identified the correct security tenet data tampering violates (Integrity) | | |
| | | 3 | 2 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | You have discussed your findings to a great extent in relation to your scenario. brief justification is presented | Excellent discussion of your findings in relation to your scenario. Excellent justification is presented | | |
| B- Server Side Exploits | 2- SQL Injection | 1 | 3 | No real attempt. Submission is devoid of any meaningful material. You did not identify if the application is vulnerable to SQL Injjection. You did not also show any evidence that SQL injection was exploited. | Work presented fails to convey correct use of tools to identify if application is vulnerable to SQL Injection. You have shown some examples that it was exploiited but they are unstructured and inconclusive | Work presented shows more than a basic correct use of tools to demonstrate how SQL Injection can be exploited You have shown some examples that it was exploiited. | Work presented shows very clear understanding of how the tools were used and an explanation is provided for each. You have identified that the application is vulnerable to SQL Injection. You have shown excellent examples of how it was exploiited | |
| | | 2 | 2 | No real attempt. Submission is devoid of any meaningful material. No research to dSQL Injection. You did not identify the correct security tenet SQL Injection violates (Confidentiality) | Some research is provided on SQL Injection but more needed to show a clear understanding and no refernece to external sources. You identified the correct security SQL Injection violates (Confidentiality) | Excellent research is also provided on SQL Injection with very good resources. You identified the correct security tenet SQL Injection violates (Confidentiality) | | |
| | | 3 | 2 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | You have discussed your findings to a great extent in relation to your scenario. brief justification is presented | Excellent discussion of your findings in relation to your scenario. Excellent justification is presented | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 3- XSS Scripting | 1 | 3 | No real attempt. Submission is devoid of any meaningful material. You did not identify if the application is vulnerable to data tampering. You did not also show any evidence that Data tampering was exploited. | Work presented fails to convey correct use of tools to identify if application is vulnerable to XSS Scripting. You have shown some examples that it was exploiited but they are unstructured and inconclusive | Work presented shows more than a basic correct use of tools to demonstrate how XSS scripting can be exploited You have shown some examples that it was exploiited | The work presented shows a very clear understanding of how the tools were used and an explanation is provided for each. You have identified that the application is vulnerable to XSS scripting. You have shown excellent examples of how it was exploited | |
| | | 2 | 2 | No real attempt. Submission is devoid of any meaningful material. No research to XSS Scripting. You have did not identify the correct security tenet data tampering violates (Integrity, condeitiality, availaility) | Some research is provided on XSS Scripting. You have but more needed to show a clear understanding and no refernece to external sources. You identified the correct security tenet data tampering violates (Integrity, condeitiality, availaility) | Excellent research is also provided on XSS Scripting. You have very good resources. You identified the correct security tenet data tampering violates (Integrity, confidentiality, availability) | | |
| | | 3 | 2 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | You have discussed your findings to a great extent in relation to your scenario. brief justification is presented | Excellent discussion of your findings in relation to your scenario. Excellent justification is presented | | |
| | 3- Other exploits | 1 | 2 | No real attempt. Submission is devoid of any meaningful material. You did not identify two vulnrabilities. | You have identified one vulnerability and briefly explained it or you have identified two vulerabilities with no explaination | You have identified the two vulnerabilities and provided excellent explaiantion to both. | | |
| | | 2 | 2 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | You have discussed your findings to a great extent in relation to your scenario. brief justification is presented | Excellent discussion of your findings in relation to your scenario. Excellent justification is presented | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| C- Client Side Exploits | 1- Man in the Middle Attacks | 1 | 3 | No real attempt. Submission is devoid of any meaningful material. You did not identify how MiTM can be carried out between user and server. You did not also show any evidence that MiTM was exploited. | Work presented fails to convey correct use of tools to identify how MiTM can be carried out between user and server. You have shown some examples that it was exploiited but they are unstructured and inconclusive | Work presented shows more than a basic correct use of tools to demonstrate how MiTM can be carried out between user and server. You have shown some examples that it was exploiited | Work presented shows very clear understanding of how the tools were used and an explanation is provided for each. You have shown how MiTM can be carried out between user and server. You have shown excellent examples of how it was exploiited | |
| | | 2 | 4 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | Work presented shows a very basic understanding,of MiTM attack in relation to your scenario.You have identified briefly some information the attacked can obtain and how dangerous they are for your scenario. No justifications are provided. | Work presented shows more than a basic understanding,of MiTM attack in relation to your scenario.You have identified and explained briefly what are the information the attacked can obtain and how dangerous they are for your scenario. No justifications are provided. | Work presented shows very good understanding in relation to your scenario and MiTM attack.You have identified and explained briefly what are the information the attacked can obtain and how dangerous they are for your scenario. You have provided some good justifications. | Excellent discussion of your findings in MiTM attack in relation to your scenario.You have identified and explained what are the information the attacked can obtain and how dangerous they are for your scenario. You have provided some excellent justifications. |
| | 2- Social Engineering Attacks | 1 | 3 | No real attempt. Submission is devoid of any meaningful material. You did not identify how social engineering can be carried out between user and server. You did not also show any evidence that social engineering attack was exploited. | Work presented fails to convey correct use of tools to identify how social engineering attack. You have shown some examples that it was exploiited but they are unstructured and inconclusive | Work presented shows more than a basic correct use of tools to demonstrate how social engineering attack can be exploited You have shown some examples that it was exploiited | Work presented shows very clear understanding of how the tools were used and an explanation is provided for each. You have identified how social engineering attack can be carried out between user and server. You have shown excellent examples of how it was exploiited | |
| | | 2 | 4 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | Work presented shows a very basic understanding of social engineering attack in relation to your scenario.You have identified briefly some information the attacked can obtain and how dangerous they are for your scenario. No justifications are provided. | Work presented shows more than a basic understanding,of social engineering attack in relation to your scenario.You have identified and explained briefly what are the information the attacked can obtain and how dangerous they are for your scenario. No justifications are provided. | Work presented shows very good understanding of the relation between your scenario and social engineering attack.You have identified and explained briefly what are the information the attacked can obtain and how dangerous they are for your scenario. You have provided some good justifications. | Excellent discussion of your findings in social engineering attack in relation to your scenario.You have identified and explained what are the information the attacked can obtain and how dangerous they are for your scenario. You have provided some excellent justifications. |
| D- Denial of Service Attacks | Dos The web server | 1 | 2 | No real attempt. Submission is devoid of any meaningful material. You did not show how DoS or DDoS can be carried out on your server. You did not show any evidence that this activity was carried out. | Work presented shows a basic understanding DoS or DDoS can be carried out on your server. You have shown some evidence that this activity was carried out. | Work presented shows very clear understanding DoS or DDoS can be carried out on your server. You have excellent evidence that this activity was carried out. | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2 | 1 | No real attempt. Submission is devoid of any meaningful material such as incorrect identification of the availability security tenet | You have identified availability security tenet as the correct cyber security tenet that DoS or DDoS viollates. | | | |
| | | 3 | 2 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | Work presented shows a very basic understanding,of the impact of DoS and DDoS on your scenario. No justifications are provided or not correct. | Excellent discussion on how DoS and DDos attacks impact the availability on your scenario. You have provided some excellent justifications. | | |
| | 1 | | 2 | No real attempt. Submission is devoid of any meaningful material. No research evidence is presented | Work presented shows basic understanding of methodds to minimize threats to the findings in the reconnaisance phase. No references to external sources | Work presented shows very good understanding of methodds to minimize threats to the findings in the reconnaisance phase.Good references to external sources | | |
| | 2 | | 2 | No real attempt. Submission is devoid of any meaningful material. No research evidence is presented | Work presented shows basic understanding of port knocking and how it can protect against threats identifing in infomration gathering section. No references to external sources | Work presented shows very good understanding of port knocking and how it can protect against threats identifing in infomration gathering section. Good references to external sources | | |
| | 3 | | 3 | No real attempt. Submission is devoid of any meaningful material. No research evidence is presented | Work presented shows basic understanding of how you can protect your applications against SQL injection No references to external sources | Work presented shows very good understanding of how you can protect your applications against SQL injection. Good references to external sources | Work presented shows excellent understanding of how you can protect your applications against SQL injection. Excellent references to external sources | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| E- Recommendations | 4 | | 3 | No real attempt. Submission is devoid of any meaningful material. No research evidence is presented | Work presented shows basic understanding of how you can protect your applications against XSS scripting No references to external sources | Work presented shows very good understanding of how you can protect your applications against XSS scripting. Good references to external sources | Work presented shows excellent understanding of how you can protect your applications against XSS scripting. Excellent references to external sources | |
| | 5 | | 3 | No real attempt. Submission is devoid of any meaningful material. No research evidence is presented | Work presented shows basic understanding of how you can protect or minimize the impact of MiTM attacks. No references to external sources | Work presented shows very good understanding of how you can protect or minimize the impact of MiTM attacks. Good references to external sources | Work presented shows excellent understanding of how you can protect or minimize the impact of MiTM attacks. Excellent references to external sources | |
| | 6 | | 3 | No real attempt. Submission is devoid of any meaningful material. No research evidence is presented | Work presented shows basic understanding of what companies should do ensure their users do not fall to social engineering attacks. No references to external sources | Work presented shows very good understanding of what companies should do ensure their users do not fall to social engineering attacks. Good references to external sources | Work presented shows excellent understanding of what companies should do ensure their users do not fall to social engineering attacks. Excellent references to external sources | |
| | 7 | | 2 | No real attempt. Submission is devoid of any meaningful material. No research evidence is presented | Work presented shows basic understanding of what companies should do to protect their services against DoS or DDoS attacks. No references to external sources | Work presented shows very good understanding of what companies should do to protect their services against DoS or DDoS attacks.. Good references to external sources | | |
| | | 1 | 3 | No real attempt. Submission is devoid of any meaningful material. You did not show examples of firewalls and iptables rules and how they can protect your scenario against some attacks exploited previously. | Work presented fails to convey correct examples of firewalls and iptables rules and how they can protect your scenario against some attacks exploited previously. You have shown examples of those rules that are unstructured and inconclusive. | Work presented shows more than a basic examples of firewalls and iptables rules and how they can protect your scenario against some attacks exploited previously. You have shown good examples of those rules. | Work presented shows very clear understanding of how the firewalls and iptables rules can be used to protect yor scenario examples. You have shown excellent examples of those rules. | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2 | 3 | No real attempt. Submission is devoid of any meaningful material. No research evidence of the evaluation is presented | Student presented a very brief evaluation of the effectiveness of ufwfirewall and iptables tools and identified which is more suitable for your scenario. No justification is presented. No refernces to external sources | Work presented shows very good understanding of the effectiveness of ufwfirewall and iptables tools and identified which is more suitable for your scenario. A good justification is presented. Good refernces to external sources | Student has shown an Excellent knowledge of the effectiveness of ufwfirewall and iptables tools and identified which is more suitable for your scenario. An excellent justification is presented. Very good refernces to external sources | |
| | 8- Intrusion Detection and Prevention | 8- Intrusion Detection and Prevention | | | | | | |
| | | 3 | 3 | No real attempt. Submission is devoid of any meaningful material. No research evidence of the comparison is presented | Student presented a very brief comparison between IDS and IPS systemts No refernces to external sources | Work presented shows very good understanding of the differences between IDS and IPS systems. Good refernces to external sources | Student has shown an Excellent knowledge of the differences between IDS and IPS systems. Very good refernces to external sources | |
| | | 4 | 3 | No real attempt. Submission is devoid of any meaningful material. You did not refer to your scenario in this section | Work presented shows a very basic understanding,of the security needs for your scenario and your recommendations are either not relevant or not correct. No justifications are provided. | Work presented shows very good understanding of security needs for your scenario and you have provided some very good recommendation You have provided some good justifications. | Excellent discussion of your findings and you have shown a very good understanding of security needs for your scenario and you have provided some very good recommendationYou have provided some excellent justifications. | |
| | | **Total** | 100 | | | | | Mark |