**ASSIGNMENT FRONT SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | **Unit 5: Security** | | |
| **Submission date** |  | **Date Received 1st submission** |  |
| **Re-submission Date** |  | **Date Received 2nd submission** |  |
| **Student Name** |  | **Student ID** |  |
| **Class** |  | **Assessor name** |  |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice. | | | |
|  |  | **Student’s signature** |  |

**Grading grid**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| P1 | P2 | P3 | P4 | M1 | M2 | D1 |
|  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **❒ Summative Feedback: ❒ Resubmission Feedback:** | | |
| **Grade:** | **Assessor Signature:** | **Date:** |
| **Signature & Date:** | | |

**Assessment Brief**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number** | Unit 5: Security | | |
| **Assignment title** | Security Presentation | | |
| **Academic Year** | 2020 | | |
| **Unit Tutor** |  | | |
| **Issue date** |  | **Submission date** |  |
| **IV name and date** | Khoa Canh Nguyen, Michael Omar, Nhung 9th/01/2020 | | |

|  |
| --- |
| **Submission Format** |
| The submission is in the form of two documents/files:   1. A ten-minute Microsoft® PowerPoint® style presentation to be presented to your colleagues. The presentation can include links to performance data with additional **speaker notes** and a **bibliography using the Harvard referencing system.** The presentation slides for the findings should be submitted with speaker notes as one copy. 2. A detailed report that provides more thorough, evaluated or critically reviewed technical information on all of the topics.   You are required to make use of the font **Calibri,** **Font size 12,** **Line spacing 1.5, Headings,** P**aragraphs**, S**ubsections and illustrations** as appropriate, and all work must be **supported with research and referenced** using the **Harvard referencing system.** |

|  |
| --- |
| **Unit Learning Outcomes** |
| **LO1** Assess risks to IT security. **LO2** Describe IT security solutions. |
| **Assignment Brief and Guidance** |
| You work as a trainee IT Security Specialist for a leading Security consultancy in Vietnam called FPT Information security FIS.  FIS works with medium sized companies in Vietnam, advising and implementing technical solutions to potential IT security risks. Most customers have outsourced their security concerns due to lacking the technical expertise in house. As part of your role, your manager Jonson has asked you to create an engaging presentation to help train junior staff members on the tools and techniques associated with identifying and assessing IT security risks together with the organizational policies to protect business critical data and equipment.  In addition to your presentation you should also provide a detailed report containing a technical review of the topics covered in the presentation.  Your presentation should:   1. **Identify** the security threats FIS secure may face if they have a security breach. Give an example of a recently publicized security breach and discuss its consequences 2. **Describe** a variety of organizational procedures an organization can set up to reduce the effects to the business of a security breach. 3. **Propose** a method that FIS can use to prioritize the management of different types of risk 4. **Discuss** three benefits to FIS of implementing network monitoring system giving suitable reasons. 5. Investigate network security, **identifying** issues with firewalls and **IDS** incorrect configuration and **show** through examples how different techniques can be implemented to improve network security. 6. **Investigate** a ‘trusted network’ and through an analysis of positive and negative issues determine how it can be part of a security system used by FIS.   Your detailed report should include a summary of your presentation as well as additional, evaluated or critically reviewed technical notes on all of the expected topics. |

|  |  |  |
| --- | --- | --- |
| Learning Outcomes and Assessment Criteria | | |
| Pass | Merit | Distinction |
| **LO1** Assess risks to IT security | | **LO1 & 2 D1** Investigate how a ‘trusted network’ may be part of an IT security solution. |
| **P1** Identify types of security threat to organisations.  Give an example of a recently publicized security breach and discuss its consequences.  **P2** Describe at least 3 organisational security procedures. | **M1** Propose a method to assess and treat IT security risks. |
| **LO2** Describe IT security solutions | |
| **P3** Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS.  **P4** Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security. | **M2** Discuss three benefits to implement network monitoring systems with supporting reasons. |

**P1 Identify types of security threat to organisations. Give an example of a recently publicized security breach and discuss its consequences.**

Some businesses in Vietnam are currently worried about the possibility of secret information technology protection that business customers should be concerned about.

**Digital Security Risks:**

* **MALWARE**

- Malware is software that enters a computer system without the user’s knowledge or consent and then performs an unwanted and usually harmful action.

- Strictly speaking, the malware uses a threat vector to deliver a malicious “payload” that performs a harmful function once it is invoked.

**More specifically, there is the following malware:**

- Oligomorphic malware: Once it is executed, this malware switches its internal code to one of a given number of predefined mutations. However, as there are only a small number of mutations in oligomorphic malware, it will inevitably transform back into a previous form that can then be identified by a scanner.

- Polymorphic malware: Malware code that completely changes from its original form whenever it is executed is known as polymorphic malware. This is usually accomplished by the malware containing “scrambled” code that, when the malware is activated, is “unscrambled” before it is executed.

- Metamorphic malware can actually rewrite its own code and thus appears different each time it is executed. It does this by creating a logical equivalent of its code whenever it is run.

**There are many types of malware that can invade a user's computer:**

* Most common types: Circulation/Infection.

1. Viruses:

+ Programs that secretly attach to another document or program and execute when that document or program is opened.

+ It could contain instructions that trigger problems ranging from showing an irritating message to removing files from a hard drive or constantly crashing a device.

+ Antivirus software defends against viruses is.

+ Drawback of antivirus software is that it must be updated to recognize new viruses.

+ Updates (definition files or signature files) can be downloaded automatically from the Internet to a user’s computer.

1. Worms:

* Although similar in nature, worms are different from viruses in two regards:

+ A virus attaches itself to a computer document, such as an e-mail message, and is spread by traveling along with the document.

+ A virus requires the user to perform some sort of action to start the infection, such as starting a program or reading an e-mail message.

+ Worms are usually distributed via e-mail attachments as separate executable programs.

+ In many instances, reading the e-mail message starts the worm.

+ If the worm does not start automatically, the user can be fooled by attackers to start the program and start the worm.

1. Trojan horses:

+ Programs that conceal their true purpose and then when triggered, show themselves.

+ May be disguised as free calendar programs or other useful applications.

* Common strategies:

+ Giving a malicious program the name of a file associated with a benign program.

+ Combining two or more executable programs into a single filename.

* Defend against Trojan horses with the following products:

+ Antivirus tools, which are one of the best defenses against combination programs.

+ Special software that alerts you to the existence of a Trojan horse program.

+ Anti-Trojan horse software that disinfects a computer containing a Trojan horse.