|  |  |
| --- | --- |
| Qualification Code: | ICT60515 |
| Qualification Title: | ADVANCED DIPLOMA OF COMPUTER SYSTEMS TECHNOLOGY |
| Unit Code/s: | ICTNWK614 |
| Unit Title/s: | Manage IT Security |
| Assessment Due Date: |  |
| Assessment Name: | Assessment Task 1 |
| Student’s name: | Benjamen Calleja |
| Student’s number: | Cal14385330 |
| Student’s Signature |  |
| Teacher’s name: | Murad Quazi |
| Teacher’s email: | mquazi@kangan.edu.au |

|  |
| --- |
| 1. Task Instructions |

**The student will:**

Answer the following questions:

**Research the internet, book and journal and write down your answers. (include diagram, pictures where applicable).**

1. With respect to security threats briefly describe what is meant by the term “worm”

**A worm virus is a malicious, self-replicating program that can spread throughout a network without human assistance.**

1. With respect to Virus software, briefly explain what is meant by the term “Trojan”

**Trojan horse is a type of malware that is often disguised as a legit software. Trojans can be employed by hackers trying to gain access to user’s system**

1. Briefly explain what is meant by the term “adware” **Adware is the name given to programs that are designed to display advertisements on your computer, redirect your search type data**
2. Briefly explain what is meant by the term “malware” **software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.**
3. Briefly explain what is meant by the term “spam” **Spam refers to the use of electronic messaging systems to send out unrequested or unwanted messages in bulk.**
4. List and briefly explain four classes of Network Attack  
   ***Structured threats* are more focused by one or more individuals with higher-level skills actively working to compromise a system. The targeted system could have been detected through some random search process, or it might have been selected specifically. The attackers are typically knowledgeable about network designs, security, access procedures, and hacking tools, and they have the ability to create scripts or applications to further their objectives.  
     
   *Unstructured threats* often involve unfocused assaults on one or more network systems, often by individuals with limited or developing skills. The systems being attacked and infected are probably unknown to the perpetrator. These attacks are often the result of people with limited integrity and too much time on their hands. Malicious intent might or might not exist, but there is always indifference to the resulting damage caused to others.**

***Internal threats* originate from individuals who have or have had authorized access to the network. This could be a disgruntled employee, an opportunistic employee, or an unhappy past employee whose access is still active. In the case of a past network employee, even if their account is gone, they could be using a compromised account or one they set up before leaving for just this purpose.**

***External threats* are threats from individuals outside the organization, often using the Internet or dial-up access. These attackers don’t have authorized access to the systems.**

**Marking Criteria**

UNGRADED

|  |  |
| --- | --- |
| **Grade** |  |
| NN | * Assessment aims have not been met |
| CA | * Assessment aims have been met |

|  |
| --- |
| 1. Submission instructions |

Answer all the questions and submit to your facilitator on the due date given.

|  |  |  |  |
| --- | --- | --- | --- |
| Student Signature: |  | Submission Date: |  |

Comments:

|  |  |  |  |
| --- | --- | --- | --- |
| Teachers Signature: |  | Date: |  |