國立成功大學

114學年度碩士班招生考試試題

編　號：143

系　所：智慧資訊安全碩士學位學程

科　目：資訊安全概論

日　期：0210

節　次：第 1 節

注　意：1.不可使用計算機
2.請於答案卷(卡)作答，於試題上作答，不予計分。

1. Please explain what "**Phishing**" **(7%)** and "**Spear Phishing**" **(7%)** are and how they differ **(6%)**.
2. Please explain what the "**Cyber Kill Chain**" is **(10%)**, and describe its main standardized stages, providing an explanation for each stage **(10%)**.
3. There are many types of malware, please try to define "**WORM**" **(10%)** and "**Trojan horse**" **(10%)** among them.
4. Please try to translate the following into Mandarin **(11%)** and try to answer related questions.
   Various approaches for modeling cybersecurity attacks and defenses have been developed over time. Among them are methodologies based on tree structures, as well as frameworks introduced by organizations such as Lockheed Martin's Cyber Kill Chain, Microsoft's STRIDE, and the MITRE ATT&CK framework. These models describe the steps involved in either executing an attack or defending against one, and they provide different levels of detail depending on the context. This paper expands upon previous work that employed the Blackboard Architecture for cyber warfare and introduces a more generalized framework for modeling attacks based on frameworks or paradigms. This approach goes beyond the typical focus on exploiting a single vulnerability targeting a specific asset. The proposed system, known as the Blackboard Architecture Cyber Command Entity Attack Route (BACCER), integrates a set of rules and factual information to determine the type of attack and guide decision-making. It also incorporates actions that support reconnaissance activities and both offensive and defensive measures. The paper illustrates how BACCER can effectively model tree-structured attacks and other complex models. (from IEEE SmartCloud 2020)
   (1) Which manufacturer or organization proposed the STRIDE model? **(3%)**
   (2) What is the name of the model proposed by Lockheed Martin? **(3%)**
   (3) What is the name of the system or framework proposed in this abstract? Please write the full text and abbreviations. **(3%)**
5. Please try to translate the following into Mandarin **(11%)** and try to answer related questions.
   The Diamond model uses a diamond-shaped structure to highlight the relationships and characteristics of an attack, based on its four essential components: adversary, infrastructure, capability, and victim. This model illustrates how an adversary leverages a capability over an infrastructure to target a victim. The four key components of an attack form the vertices of the diamond, which is the origin of the model's name. Additionally, the model defines supplementary meta-features to support higher-level constructs, applying measurement, testability, and repeatability to establish a more thorough scientific method of analysis. Released by the US Department of Defense in 2013, the Diamond model serves as both a cognitive framework and a set of mathematical techniques. The cognitive model helps security professionals organize complex, interrelated logic, while the mathematical techniques aid in refining strategic decision-making and analytical workflows in the face of adversarial threats. (from IEEE ISSE 2022)
   (1) What elements does the core component of the diamond model consist of? **(3%)**
   (2) When and who proposed the diamond model? **(3%)**
   (3) From the information, which journal or conference do you think the above article was published in? Please specify the journal or conference and provide its name. **(3%)**