

ITBU 313, Introduction to Cybersecurity

Sample Examination

December 27, 2022

1 Instructions

The Honor Code applies to this examination. You may not use your textbook, your notes, or any other written or electronic material, including the internet. You may not give or receive aid from another person. Violations of the Honor Code will result in the failure of this examination and dismissal from the course. Submission of your answers to this examination constitutes an acknowledgment of the Honor Code and your compliance therewith.

Please answer the following questions. Please answer in complete sentences. Please answer all questions briefly and succinctly — no long essays permitted. Do not use short answers unless the question specifically calls for short answers. You must exhibit understanding of the material covered by the question.

Submit your answers in accordance with the instructions given orally in class. Late submissions will result in failure of this examination.

2 Questions

1. List the four approaches to identifying and mitigating risks to an organization's IT infrastructure.
2. List the four threat categories of human caused threats.
3. Explain the difference between an audit review and an audit analysis.
4. What is the X.509 standard?
5. Give an example of *role based access*, describing in your example how RBAC works.
6. What is the difference between *phishing* and *spear-phishing*? What is *whaling*?
7. How does a NIDS differ from an HIDS?
8. What is meant by *least privilege*? Give an example of this concept.
9. What are some issues organizations face with respect to abuse of email by employees?
10. What are the four general means of establishing a user's identity? Give one example of each.