ITBU 443, Threats and Counter Measures

Examination 01

February 3, 2023

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 and briefly describe the three objectives of computer security.
2. What is the X.509 standard?
3. Describe five methods of attacking passwords.
4. What different concerns do authentication, authorization, and audit entail?
5. List some of the defenses against SQL injection attacks.
6. What are the differences between a virus, a worm, and a trojan horse?
7. What is the difference between kernel mode and user mode?
8. Describe the TCP *three way handshake*. Why does TCP use this method?
9. Name some tasks (behaviors) that intruders may perform.
10. Briefly discuss the ramifications of the two default firewall policies. Be specific.
11. Buffer overflows typically attack targets in three locations. Describe these locations.
12. How can an attacker exploit unvalidated data sent from one process to another process?