Cybersecurity Guided Notes Lesson 2.4.6 - Logic Bomb & Rootkits

Name: ______ Class: _____ Date: _____

1. Define a logic bomb and provide examples of triggers that can activate it.

2. Explain what distinguishes a time bomb from other types of logic bombs.

3. Describe how insider threats can utilize logic bombs and provide an example of a real-world case.

4. What are some defense strategies against logic bombs?





5. Explain how system backups played a crucial role in identifying and prosecuting the perpetrator in the UBS Paine Webber case.

6. What is a rootkit, and what purpose does it serve for attackers?

7. Explain why rootkits are difficult to detect.

8. Describe the different types of rootkits based on their loading phases during startup.



9. Provide examples of well-known rootkits targeting different operating systems.

10. Discuss the main components and impact of the Stuxnet rootkit.

11. What defense measures can be implemented against rootkits?

