School of Computing, Southern Illinois University Carbondale

CS 531 – Fall 2020

SECURITY IN CYBER-PHYSICAL SYSTEMS

QUIZ #2

09/01/2020

If there are more than one answer, please select both. Hint: Some questions may have multiple answers.

Please write justification for each answer for partial credits.

1) Which of the following is an active attack? (15 points)
    a. DoS
    b. MiTM
    c. Phishing
    d. Impersonation
    e. Replay
    f. Interception

2) What is packet encapsulation? Give one simple example how it works. (10 points)

3) Which of the following are an example of Confidentiality attacks? (15 points)
    a. Packet capture
    b. Port scan
    c. Dumpster diving
    d. Wireless interception
    e. Wiretapping
    f. Social Engineering

4) What is the target of DDoS attack, considering CIA Triad? (10 points)

5) What are three different malware attack examples? Please provide real world attack examples for each three malware you picked. (30 points)

6) Please select which attacks suitable for Signature detection and which attacks suitable for Anomaly detection. (20 points)

- Application layer reconnaissance and attacks
- Transport layer reconnaissance and attacks
- Network layer reconnaissance and attacks
- Unexpected application services
- Policy violations
- Denial-of-service (DoS) attacks
- Scanning
- Worms