

Lecture 28: June 2, 2021

Reading: *text*, §23.10, 26.1–26.3

Assignments: Homework 5, due June 2

Lab 4, due June 3

1. Defenses
 - (a) Scanning
 - (b) Distinguishing between data and instructions
 - (c) Containment
 - (d) Specifications as restrictions
 - (e) Limiting sharing
 - (f) Statistical analysis
 - (g) Trust
2. Basic intrusion detection
 - (a) Basis
 - (b) Anomaly detection (“what is unexpected is bad”)
 - (c) Misuse (signature-based, rule-based) detection (“what is bad is known; everything else is good”)
 - (d) Specification-based detection (“what is good is known; everything else is bad”)
 - (e) Host-based intrusion detection
 - (f) Network-based intrusion detection
 - (g) Combined intrusion detection