THE UNIVERSITY OF DODOMA

COLLEGE OF INFORMATICS AND VIRTUAL EDUCATION



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

IA 313: OPERATING SYSTEMS SECURITY

Tutorial 1

1. What is the purpose of an intrusion detection system (IDS)?
2. What is the difference between host-based and network-based intrusion detection?
3. In the context of an IDS, what is an anomaly?
4. In the context of an IDS, what is a signature and what is it used for?
5. Explain the strengths and weaknesses of Network based IDS
6. Describe the strengths and drawbacks of the host-based IDS
7. What is an intrusion prevention system?
8. How do intrusion prevention systems work?
9. What are the advantages and disadvantages of intrusion prevention systems?