### 

### **3413ICT Network Security**

### **Workshop – 11A**

|  |
| --- |
| **Review Questions:**   1. Discuss the different types of Intrusion Detection systems and explain how each of them operates.   The different types of intrusion detection systems include:  **Signature-based intrusion detection**: Signature techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious. In very general terms, we can characterize all approaches as focusing on either anomaly detection or penetration identification, although there is some overlap in these approaches.  **Network-based intrusion detection**: A network-based IDS (NIDS) monitors traffic at selected points on a network or interconnected set of networks. The NIDS examines the traffic packet by packet in real time, or close to real time, to attempt to detect intrusion patterns. The NIDS may examine network-, transport-, and/or application-level protocol activity. Note the contrast with a host-based IDS; a NIDS examines packet traffic directed toward potentially vulnerable computer systems on a network. A host-based system exam- ines user and software activity on a host.  **Host-based intrusion detection**: Specialized layer of security software added to vulnerable or sensitive systems; examples include database servers and administrative systems. The host-based IDS monitors activity on the system in a variety of ways to detect suspicious behavior. In some cases, an IDS can halt an attack before any damage is done, but its primary purpose is to detect intrusions, log suspicious events, and send alerts.  The primary benefit of a host-based IDS is that it can detect both external and internal intrusions, something that is not possible either with network-based IDSs or firewalls.  **Anomaly detection**: Pattern of behaviour that do not conform to the expected pattern or behaviour. Also known as outliers, exceptions, etc.   1. Explain the advantages of contextual anomaly detection compared with point-anomaly detection. Discuss the challenges of contextual anomaly detection.   **Point anomaly detection**: An individual data record is viewed as anomalous with respect to the data, without considering other conditions  **Contextual anomaly detection:**  An individual data instance is anomalous within a context.  The challenge faced during contextual anomaly detection concerns the data may be skewed for a set of data that would cause a false positive to be detected.   1. What are the challenges in enhancing the performance of network anomaly detection systems?   -Normal data behaviour keeps evolving  -Very small amount of anomaly in a huge amount of data  -Data may contain noise -Need very efficient algorithms   1. What performance metrics are commonly used to quantify the performance of an anomaly detection technique? Explain each of them briefly.   **Label**: - Each test instance is given a normal or anomaly label  - This approach is used in classification-based techniques of anomaly detection  **Score (Fuzzy Logic)**:  Each test instance is assigned an anomaly score  Allows the output to be ranked  Requires an additional threshold parameter     1. List the different types of anomaly detection techniques and briefly explain each of them.   **Classification-based techniques: Build a classification model for normal and anomalous events, based on labelled training data; then use it to classify each new event.**  **Nearest neighbour based techniques:** **Normal points have close neighbours while anomalies are located far from other points**    **i. Distance based methods:** **Anomalies are data points most distant from other points**    **ii. Density based methods: Anomalies are data points in low density regions**    **Clustering based techniques:**     1. The Hamming distance between two points, and,is defined as:     that is, the number of coordinate positions where anddiffer.Given the following data items which are points of the 4-dimensional space, for each pair of data items, calculate the Hamming distance between them: |
|  |
|  |

**Hands-on Exercises:**

Complete the 5th lab on VPN.