Institute of Public Administration
Communication and Network Security
Group 1
Homework (6) Solution

Question (1)

What is the Intrusion Detection?

Solution:

Intrusion detection wants to detect intrusion activities as quickly as possible so that appropriate actions can be taken to minimize damages caused by the intrusions. It also wants to trace intruders and collect evidence to indict the criminals. A common approach to detecting intrusions is to find ways to identify abnormal events, such as finding behavior discrepancies between the intruder and the legitimate user impersonated by the intruder.

Question (2)

What is the goal of Intrusion Detection?

Solution:

The goal of intrusion detection is to identify intrusion activities that already occurred or are currently occurring inside an internal network.

Question (3)

What is the basic methodology of detecting intrusions?

Solution:

The basic methodology of detecting intrusions is to log system events and analyze them using appropriate methods. For example, one may build a simple IDS as follows: log all the packets passing through a router (or a firewall) using a packet sniffer/logger, and analyze the log to identify suspicious events on the basis of a given set of rules that specify what events are unacceptable.

Question (4)

What are the types of Intrusion Detection?

Solution:

The first type of intrusion detection is referred to as network-based detection (NBD), the second type as host-based detection, and the third type as hybrid detection (HBD).

Question (5)

List the three Intrusion Detection System components and describe each one.

Solution:

1. Assessment: the assessment component evaluates security needs of a system and produces a security profile for the target system.
2. Detecyion: the detection component collects system usage events and analyzes these events to detect intrusion activities, where each record in the event log should contain information useful for detecting intrusions.
3. Alarm: when an attacker impersonates a legitimate user to log on to the user’s account, the attacker’s behaviors would likely be different from the true user’s behaviors, which would be considered unacceptable and will therefore trigger the IDS to alarm the user or the system administrator.

Question (6)

Describe the Intrusion Detection Policies.

Solution:

Intrusion detection policies (IDP) are used to identify intrusion activities. They specify what data must be protected and how well they should be protected. They also specify what kinds of activities are considered intrusions and how to respond when suspicious activities are identified.

Question (7)

What is the Unacceptable Behavior?

Solution:

An unacceptable behavior is a sequence of events that violate the system security policy.

Question (8)
Describe the Network-Based Detections and Host-Based Detections.

Solution:
Network-based detections analyze network packets. Host-based detections analyze system events and user behaviors. A hybrid IDS supports both NBDs and HBDs.

Question (9)
Describe the Outsider Behaviors and Insider Misuses.

Solution:
People who have authenticated access to a computer system are referred to as insiders of the system. People who do not have authenticated access to the system are referred to outsiders of the system.

Question (10)
What is the Behavioral Data Forensics?

Solution:
Behavioral data forensics studies how to use data mining techniques to analyze event logs and search for useful information.

Question (11)
What are the Honeypots?

Solution:
Any device, system, directory, or file used as a decoy to lure attackers away from important assets and to collect intrusion behaviors is referred to as a honeypot.

Question (12)
List the types of Honeypots and describe each one.

Solution:

1. Physical Systems: Early honeypots, developed in 1990, were physical systems. They were simply host computers connected to unprotected LANs with real IP addresses.
2. Software Techniques: Since the late 1990s, researchers have developed new software techniques to construct virtual honeypots by emulating operating systems or network services. They are easy to deploy and require low-level interactions between the honeypot daemon and the local hard disk.