Intrusion detection systems

In this video, we'll introduce you to intrusion detection and intrusion prevention systems.

Imagine that you've just installed a home intrusion security system.
You've installed intruder sensors for each entry and exit point in your home, including doors and windows.
Those sensors work by sending out sound waves, and when an object touches a sound wave, the waves bounce back to your sensor and trigger an alert to your phone, notifying you that an intrusion was detected.

An intrusion detection system, or IDS, works in a very similar way to home intrusion sensors.
An intrusion detection system is an application that monitors system and network activity, and produces alerts on possible intrusions.
Like the home intrusion sensor, IDS collects and analyzes system information for abnormal activities.
If something unusual is detected, the IDS sends out an alert to appropriate channels and personnel.

Now, imagine a jewelry storefront with a window sensor.
When the sensor detects that the window's glass has been shattered, it triggers a steel roll-up door to automatically replace the shattered window and prevent unauthorized entry into the store.

This is what an intrusion prevention system does.
Intrusion prevention systems, or IPS, have all the same capabilities as an IDS, but they can do more.
They monitor system activity for intrusions and take action to stop it.

Many tools have the ability to perform the function of both IDS and IPS.
Some popular tools are Snort, Zeek, Kismet, Sagan, and Suricata.
We will be exploring Suricata in upcoming lessons.

You might be wondering, where do these alert notifications go?
Well, coming up, we'll discuss how to manage alerts using security information and event management tools.

Revision #1
Created 6 September 2023 11:04:05 by naruzkurai
Updated 1 November 2023 01:10:46 by naruzkurai