Detection and prevention systems, and other security tools

* An intrusion occurs when an attack e attempts to gain entry into or disrupt the normal operations of an information system, almost always with the intent to do harm.
* Intrusion prevention activities are writing and implementing good enterprise information security policy, planning and executing effective information security programs, installing and testing technology-based information security countermeasures and conducing measuring the effectiveness of employee training and awareness activities.
* Intrusion detection systems work like burglar alarms, in that it detects a violation and actives an alarm. Alarm can be configured to just about any way admins want.
* Intrusion prevention systems can detect an intrusion and also prevent that intrusion from successfully attacking the organization by means of an active response.
* Intrusion detection and prevention systems (IDPS) are current anti-intrusion technologies.
* IDPS terminology:
  + Alarm – indication that a system has been attacked or is under attack.
  + Evasion – Process by which attackers change the format and/or timing to avoid detection.
  + False attack stimulus – Event that triggers an alarm when no actual attack is in progress. Often occurs during testing.
  + False negative – Failure of an IDPS to react to an actual attack event.
  + False positive – An alarm that occurs in the absence of an actual attack. Happens when normal system activity is mistaken for an attack.
  + Noise – Alarm events that are accurate and noteworthy but that do not pose significant threats to info security.
  + Site policy – Rules and config guidelines governing the implementation and operation of IDPSs within the organization.
  + Site policy awareness – IDPSs ability to dynamically modify its config in response to environmental activity. “Smart” IDPS can adapt its reactions in response to administrator guidance over time and circumstances of the current local environment.
  + True attack stimulus – An event that triggers alarms and causes and IDPS to react as if a real attack is in progress, whether it’s a drill or actual attack.
  + Tuning – The process of adjusting an IDPS to maximize its efficiency in detecting true positives.
  + Confidence value – The measure of an IDPS’s ability to correctly detect and identify certain types of attacks. Value that the organization places on the IDPS is based on experience and past performance.
  + Alarm filtering – The process of classifying IDPS alerts so that they can be more effectively managed. Set up by admin who lets the system run for a while to track what types of false positives it generates and then adjusting the alarm classifications.
  + Alarm clustering and compaction – A process of grouping almost identical alarms that happen at close to the same time into a single higher-level alarm.
* Why use an IDPS?
  + Prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system.
  + To detect attacks and other security violations that are not prevented by other security measures.
  + To detect and deal with the preambles to attacks.
  + To document the existing threat to an organization.
  + To act as quality control for security design and administration, especially in large and complex enterprises.
  + To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.
* They increase fear of detection among would-be hackers. Should be installed when network can’t protect itself.
* Hacker’s initial estimation of systems through probing is called doorknob rattling.
* Footprinting are activities that gather information about eh organization and its network activities and assets.
* Fingerprinting are activities that scan network locales for active systems and then identify the network services offered by the host systems.
* Types of IDPS
  + IDPSs operate as network- or host-based systems.
  + Network Based IDPS (NIDPS) resides on a computer or appliance connected to a segment or an organization’s network and monitors network traffic on that network segment, looking for indications of ongoing or successful attacks.
  + When examining incoming packets, an NIDPS look for patterns within network traffic such as large collections of related items of a certain type (DoS attack), or the exchange of a series of related packets in a certain pattern (port scan in progress).
  + When placed next to a hub, switch, or other key networking device, the NIDPS may use that device’s monitoring port.
  + Monitoring port AKA switched port analysis (SPAN) port or mirror port, is specially configured connection on a network device that is capable or viewing all of the traffic that moves through the entire device.
  + Hubs receive traffic from one node and retransmit it to all other nodes. Any device connected to the hub can monitor all traffic passing through the hub. Security risk because anyone connected to the hub can monitor all the traffic that moves through that network segment.
  + Switches, on the other hand, create dedicated point-to-point links between their ports.
  + Protocol stack verification looks for invalid data packets—that is, packets that are malformed under the rules of TCP/IP protocol. DoS requires malformed packets.
  + In application protocol verification, the higher order protocols (HTTP, FTP and Telnet) are examined for unexpected packet behavior or improper use. Sometimes an attack uses valid packets but in not normal large quantities. This focuses on the packets use.
  + It might be beneficial to have two NIDPSs installed one focusing on app protocol and the other protocol stack to reduce the effectiveness of cache poisoning.
  + Advantages of NIPDS:
    - Good network design and placement of NIDPS devices can enable an organization to use a few devices to monitor a large network.
    - NIDPSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations.
    - NIDPSs are not usually susceptible to direct attack and, in fact, may not be detectable by hackers.
  + Disadvantages:
    - Can become overwhelmed by network volume and fail to recognize attacks it might otherwise have detected.
    - NIDPSs require access to all traffic be monitored. Since switches mostly have limited or no monitoring port capability, some networks aren’t capable or providing aggregate data for the NIDPS.
    - NIDPSs cannot analyze encrypted packets.
    - NIDPSs cannot reliably ascertain if an attack was successful or not.
    - Some forms of attack are not easily discerned by NIDPSs, specifically those involving fragmented packets.
  + Wireless NIDPS monitor and analyze wireless network traffic, looking for potential problems with the wireless protocols.
  + Issues with wireless:
    - Physical security – they’re placed in public places.
    - Wireless sensor range can be affected.
    - Access point and switch locations – must be aware of a hacker connecting to a wireless access point from a range far beyond the minimum.
    - Wired network connections without one it may be impossible to implement a senor.
    - Cost.
  + Wireless IDPSs can detect:
    - Poorly secured WLAN or unauthorized WLANs and WLAN devices.
    - Unusual usage patterns
    - Use of wireless network scanners
    - DoS attacks
    - Man-in-the-middle attacks
  + Network Behavior analysis system (NBA) systems examine network traffic in order to identify problems related to the flow of traffic. They use a version of the anomaly detection method to identify excessive packet flows such as might occurred in the case of equip malfunctions of dos attacks.
  + Typical flow and data particularly relevant to intrusion detection and prevent includes:
    - Source and destination IP address
    - Source and destination
    - TCP or UDP ports of ICMP types and codes
    - Number of packets and bytes transmitted in the session.