CN414
Computer Network Security

Week 10:- Intrusion Detection System & Intrusion Protection System

By

Dr. Piya Techateerawat

IDS & IPS

- **Intrusion Detection System**
- Intrusion Prevention System

IDS & IPS

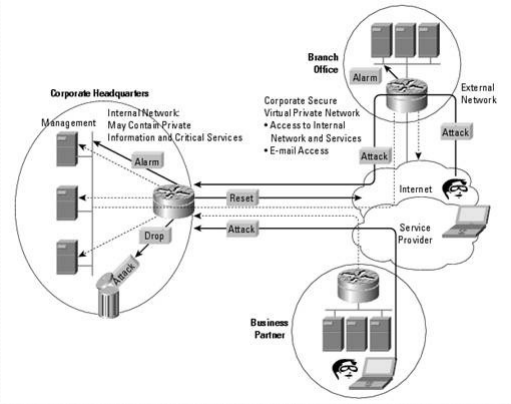
- Intrusion Detection System
  - To detect several types of malicious behaviors that can compromise the security and trust of a computer system.
    - network attacks
    - data driven attacks on applications
    - host based attacks such as privilege escalation
    - unauthorized logins
    - access to sensitive files
    - malware (viruses, Trojan horses, and worms)

IDS & IPS

- Intrusion Detection System
  - An IDS can be composed of several components:
    - **Sensors** which generate security events,
    - **Console** to monitor events and alerts and control the sensors, and a
    - **Central Engine** that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.

IDS & IPS

- **Intrusion Detection System**



IDS & IPS

- Intrusion Detection System
  - Term

  - **False positive**- An alert or alarm that is triggered when no actual attack has taken place.
  - **False negative**- A failure of an IDS to detect an actual attack.

IDS & IPS

- **Intrusion Detection System**
  - **Types:-**
    - **Network**
    - **Host Base**
    - **(Protocol, Application, …)**

IDS & IPS

- **Intrusion Detection System**
  - **Decision**
    - **Anomaly Detection**
      - **based on normal network traffic evaluations**
    - **Rule Based Detection**
      - **based on preconfigured pattern or signature**

IDS & IPS

- Intrusion Detection System
- **Intrusion Prevention System**

IDS & IPS

- **Intrusion Prevention System**
  - **monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.**
  - **For example, Network-based IPS, will operate in-line to monitor all network traffic for malicious code or attacks . When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass. Intrusion prevention technology is considered by some to be an extension of intrusion detection (IDS)**

IDS & IPS

- **Intrusion Prevention System**
  - **Types:-**
    - **Host**
    - **Network**
    - **(Contents, Protocol, …)**

IDS & IPS

- **Intrusion Prevention System**

- **Host-based vs. network**
- **HIPS can handle encrypted and unencrypted traffic equally, because it can analyze the data after it has been decrypted on the host.**
- **NIPS does not use processor and memory on computer hosts but uses its own CPU and memory.**

IDS & IPS

- **Host-based vs. network**
- **NIPS is a single point of failure, which is considered a disadvantage; however, this property also makes it simpler to maintain. However, this attribute applies to all network devices like routers and switches and can be overcome by implementing the network accordingly (failover path, etc.). A Bypass Switch from a vendor like Net Optics can be deployed to alleviate the single point of failure disadvantage though. Multi-segment Bypass Switches have recently become more popular as IPS vendors have rolled out high density solutions. This also allows the NIPS appliance to be moved and be taken off-line for maintenance when needed.**

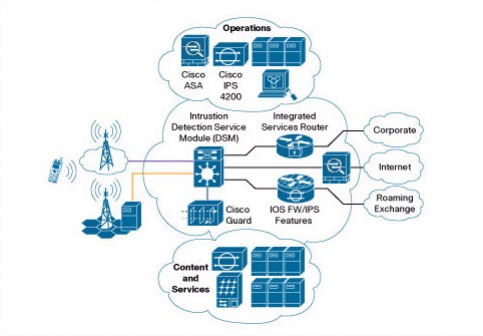
IDS & IPS

Host-based vs. network

- **NIPS can detect events scattered over the network (e.g. low level event targeting many different hosts, like hostscan, worm) and can react, whereas with a HIPS, only the hosts data itself is available to take a decision, respectively it would take too much time to report it to a central decision making engine and report back to block.**

IDS & IPS

- **Intrusion Prevention System**



IDS & IPS

- **Intrusion Prevention System**

Cisco IPS

IDS & IPS

- **Academic Perspective View**

IDS_Paper.pdf

References

- http://en.wikipedia.org/wiki/Intrusion-detection_system
- http://www.javvin.com/pics/ids.jpg
- http://en.wikipedia.org/wiki/Intrusion-prevention_system
- http://www.cisco.com/en/US/netsol/ns731/networking_solutions_solution.html
- Lippmann, R.P.; Fried, D.J.; Graf, I.; Haines, J.W.; Kendall, K.R.; McClung, D.; Weber, D.; Webster, S.E.; Wyschogrod, D.; Cunningham, R.K.; Zissman, M.A., "Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation," *DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings* , vol.2, no., pp.12-26 vol.2, 2000
  URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=821506&isnumber=17794


Q & A