**Security Technology Tools II**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**Case 03**

INTRODUCTION

Compare the **functions**, **features** and **components** of **commercial IDPS systems**. In writing your paper, use the classifications and descriptions you have learned from the reading materials as well as your own research in IDPS systems.

Your paper should include the following:

1. **Types** of IDPS systems
2. **Methodology** each system uses
3. **Main functions** of each system

BODY

An IDS specifically looks for suspicious activity and events that might be the result of a [virus](http://www.webopedia.com/TERM/V/virus.html), [worm](http://www.webopedia.com/TERM/W/worm.html) or [hacker](http://www.webopedia.com/TERM/H/hacker.html). This is done by looking for known [intrusion signatures](http://www.webopedia.com/TERM/I/intrusion_signature.html) or attack signatures that characterize different worms or viruses and by tracking general variances which differ from regular system activity. The IDS is able to provide notification of only known attacks.

PASSIVE INTRUSIOIN DETECTION SYSTEM

A passive intrusion detection system (passive IDS) is configured to monitor and analyze network traffic activity. These systems will alert operators when, potential vulnerabilities, or attacks, or both, take place, but are limited in capability; as such, they cannot perform protective or corrective measures on their own. This, along with making them easier and more rapidly deployable, makes them not impervious, but less susceptible to attacks (Beal, 2005).

Figure 1 is an example of a Passive Network-Based intrusion detection and prevention system (IDPS) Sensor Architecture.

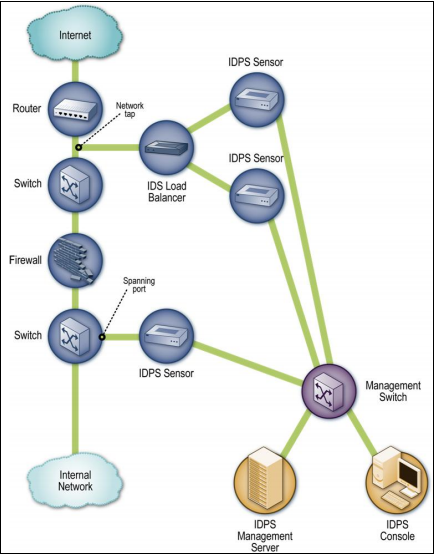


Figure 1: Passive Network-Based Intrusion Detection System. Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 3 December 2015.

ACTIVE INTRUSION DETECTION SYSTEM

An active intrusion detection system (active IDS) is configured to monitor and analyze network traffic activity. These systems will alert operators when, potential vulnerabilities, or attacks, or both, take place, and they attempt to perform protective or corrective measures on their own. They are also known as, intrusion detection and prevention systems (IDPS) (Beal, 2005).

NETWORK INTRUSION DETECTION AND PREVENTION SYSTEM

Network-based IDS systems (NIDS) are often standalone hardware devices. These devices, typically, include network intrusion detection capabilities consisting of hardware, software sensors. Hardware sensors are located at various different places along the network. Software sensors are installed to system computers connected to the network. These sensors analyze data packets entering and leaving the network (Beal, 2005).

Figure 2 is an example of an Inline Network-Based Sensor Architecture.

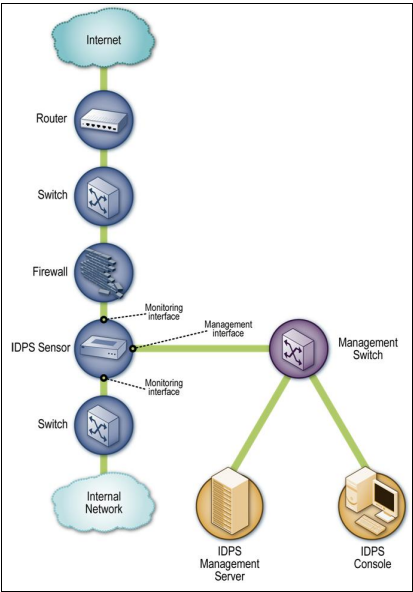


Figure 2: Inline Network-Based Intrusion Detection System. Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 3 December 2015.

WIRELESS INTRUSION DETECTIONAND PREVENTION SYSTEM

“A wireless IDPS monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves” (Scarfone et al., 2007).

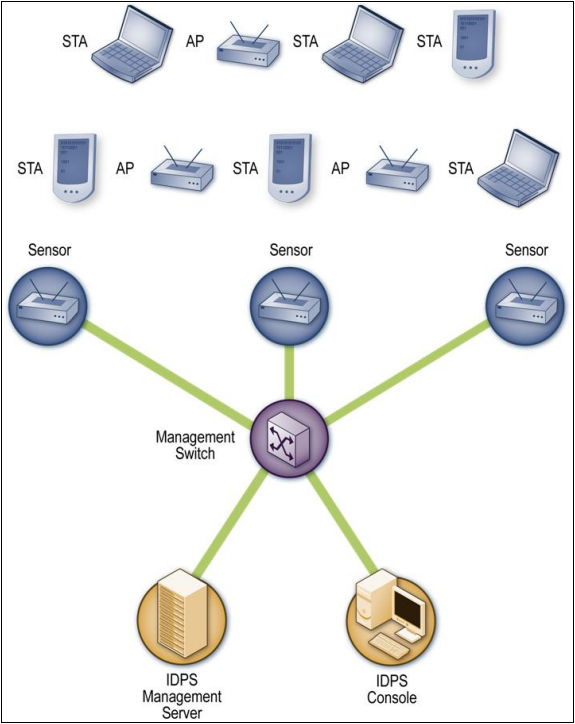


Figure 3: Wireless IDPS Architecture. Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 3 December 2015.

NETWORK BEHAVIOR ANALYSIS (NBA)

HOST INTRUSION DETECTION AND PREVENTION SYSTEM

Host-based IDS systems (HIDS) are comprised of software agents that are installed on the individual computers within the system. Traffic to and from the specific machine within the system is analyzed and there are three specific intrusion events that HIDS can monitor and stop that NIDS cannot.

HIDS, above and beyond NIDS, is capable of monitoring changes to key system files and any attempt to overwrite them. HIDS are also able to monitor such activities that only an administrator would have the authority to implement. Any attempt to install Trojan software or to use methods that bypass normal authentication or secure unauthorized access, remotely, or obtain access to plaintext while trying to avoid detection, or any combination of these malicious activities can be monitored and stopped by HIDS.

Figure 3 is an example of a Host-Based IDPS Agent Deployment Architecture.

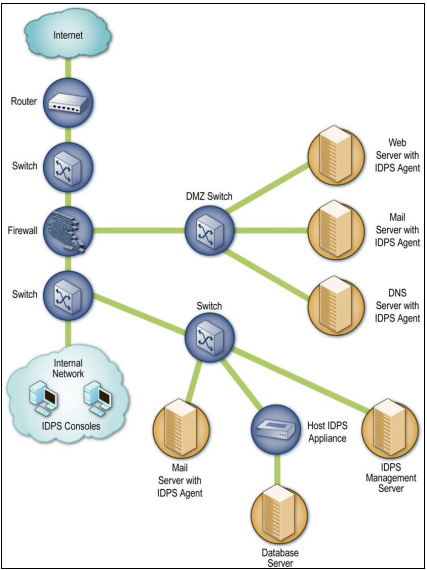


Figure 4: Host-Based IDPS Agent Deployment Architecture. Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 3 December 2015.

CONCLUSION

REFERENCES

Beal, V. (2005, July 15). Intrusion Detection (IDS) and Prevention (IPS) Systems. Retrieved December 3, 2015, from [http://www.webopedia.com/DidYouKnow/Computer\_Science/intrusion\_detection\_preve ntion.asp](http://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_preve%09ntion.asp)

Examining Different Types of Intrusion Detection Systems. (2015). Retrieved November 30, 2015, from <http://www.dummies.com/how-to/content/examining-different-types-of-> intrusion-detection-s.html

Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 3 December 2015.