# Module 3 - Case

## Security Technology Tools II

### Case Assignment

Compare the functions, features, and components of commercial IDPS systems. Your paper should include the following:

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

### Assignment Expectations 2 pages dbl spaced.

Your paper should provide a summary of your findings from the assigned materials and any quality resources you can find. Cite all sources and provide a reference list at the end of your paper. The following items will be assessed in particular:

1. Demonstration of your understanding of IDPS
2. Clear presentation of your findings

**Use at least 2 of below references:**

**Intrusion detection and prevention systems (IDPS's)**

Two types of IDPS systems (network-based and host based)

* [Network-based](http://www.ehow.com/about_6661697_network-intrusion-detection-prevention.html%22%20%5Ct%20%22_blank) (Wireless IDPS and Network behavior analysis): monitor network, analysis network activities
* [How to compare wireless IDPS systems](http://www.csoonline.com/article/502268/how-to-compare-and-use-wireless-intrusion-detection-and-prevention-systems%22%20%5Ct%20%22_blank)
* Intrusion detection and prevention - [Network behavior analysis IDPS](http://www.scribd.com/doc/2096981/Intrusion-Detection-and-Prevention-Systems%22%20%5Ct%20%22_blank)
* [More on network behavior analysis IDPS](http://www.isca.in/IJES/Archive/v1i1/9.ISCA-JEngS-2012-032.pdf%22%20%5Ct%20%22_blank)
* [Host based](http://www.windowsecurity.com/articles/hids_vs_nids_part1.html%22%20%5Ct%20%22_blank): resides on a particular machine, monitor activity only on that system.
* [Host based IDPS](http://www.centos.org/docs/4/html/rhel-sg-en-4/s1-ids-host.html%22%20%5Ct%20%22_blank)
* [More on Host based IDPS](http://www.cs.ucsb.edu/~chris/research/doc/infsec05_hids.pdf%22%20%5Ct%20%22_blank)

IDPS systems use mainly three kinds of methods to monitor and evaluate network traffic: signature-based, statistical-based, and stateful packet inspection approach.

* [Signature-based IDPS system](http://www.omnisecu.com/security/infrastructure-and-email-security/types-of-intrusion-detection-systems.htm%22%20%5Ct%20%22_blank)
* [Statistical-based (Anomaly based) IDPS](http://www.omnisecu.com/security/infrastructure-and-email-security/types-of-intrusion-detection-systems.htm%22%20%5Ct%20%22_blank)
* [Stateful packet inspection approach](http://kb.netgear.com/app/answers/detail/a_id/1178/~/denial-of-service-attacks-and-stateful-packet-inspection%22%20%5Ct%20%22_blank)

Companies that provide intrusion detection and prevention systems

* [http://www.enterasys.com](http://www.enterasys.com" \t "_blank) (network-based IPS)
* [http://www.cisco.com](http://www.cisco.com" \t "_blank) (network-based IPS)
* [http://www.ca.com](http://www.ca.com" \t "_blank) (Network-based and host-based IPSs)
* [http://www.ibm.com](http://www.ibm.com" \t "_blank) (network-based)
* [http://www.snort.org](http://www.snort.org" \t "_blank) (network-based)
* [http://www.symantec.com](http://www.symantec.com" \t "_blank) (host-based, network-based)

[An Overview of Issues in Testing Intrusion Detection Systems](http://csrc.nist.gov/publications/nistir/nistir-7007.pdf%22%20%5Ct%20%22_blank)

**Trap and trace technologies - Security defense to offense**

* [Honeypots and Honeynets - Security via deception](http://www.sans.org/reading_room/whitepapers/attacking/honey-pots-honey-nets-security-deception_41%22%20%5Ct%20%22_blank)
* [Padded cell](http://www.idc-online.com/technical_references/pdfs/data_communications/Honey_Pots_Honey_Nets_Padded_Cell_system.pdf%22%20%5Ct%20%22_blank)

Honeypots products

* [http://www.keyfocus.net/kfsensor](http://www.keyfocus.net/kfsensor%22%20%5Ct%20%22_blank) (detects nature of the attacks)
* [http://www2.netbaitinc.com](http://www2.netbaitinc.com" \t "_blank) (simulate fake services and distracts attackers away from the network, also able to track the trace of the hackers)
* [http://labrea.sourceforge.net/](http://labrea.sourceforge.net/%22%20%5Ct%20%22_blank) (honeypot that answers attacker machines’ connection requests, then make them get stuck)
* [http://www.honeyd.org](http://www.honeyd.org" \t "_blank) (monitor millions of unused IP addresses).

**Scanning and analysis tools**

* [Active and passive vulnerability scanners](http://www.itsecurity.com/interviews/amer-deeba-interview-qualsys-040507/%22%20%5Ct%20%22_blank)
* [Packet sniffers - packet analyzer](http://netsecurity.about.com/cs/hackertools/a/aa121403.htm%22%20%5Ct%20%22_blank)
* [More on packet sniffers](http://www.wisegeek.com/what-is-a-packet-sniffer.htm%22%20%5Ct%20%22_blank)

**Access control**

* [ID and Password security](http://www.plus.net/support/security/usernames_and_passwords/username_and_password_security.shtml%22%20%5Ct%20%22_blank)
* [Facial recognition](http://www.wired.com/gadgetlab/2012/05/apple-3d-facial-recognition/%22%20%5Ct%20%22_blank)
* [Smart card security](http://www.smartcardbasics.com/smart-card-security.html%22%20%5Ct%20%22_blank)