**PART 2**

**IDS LIMITATIONS**

**IDSs have many limitations. These are the major ones:**

* They aren’t scalable to large or distributed enterprise networks.
* They can be difficult to manage, with awkward user control and alarm display interfaces.
* Different commercial IDSs rarely interoperate with each other, so you may not be able to consolidate your IDSs across your enterprise if you use more than one vendor’s IDS.
* Commercial IDSs rarely interoperate with other security or network management packages.
* There are significant error rates, especially false positives, in IDS results. These can take up a great deal of a security staff’s time and resource.
* They cannot compensate for significant deficiencies in your organizations security strategy, policy, or security architecture.
* They cannot compensate for security weaknesses in network protocols.
* They cannot substitute for other types of security mechanisms (such as Identification and Authentication, encryption, single sign on, firewalls, or access control)
* They cannot, by themselves, completely protect a system from all security threats.

REFERENCES

<https://csrc.nist.rip/library/NIST%20SP%20800-031%20Intrusion%20Detection%20Systems%20(IDS),%202001-11.pdf>