The IDS component responsible for collecting data is the user interface. **False**

**RFC 4767** is a document that describes the application level protocol for exchanging data between intrusion detection entities.

Snort can perform intrusion prevention but not intrusion detection. **False**

Anomaly detection is effective against misfeasors. **False**

**Insider attacks** are among the most difficult to detect and prevent.

A **Markov proces**s model is used to establish transition probabilities among various states.

A packet filtering firewall is typically configured to filter packets in both directions. **True**

The **tiny fragment** attack is designed to circumvent filtering rules that depend on TCP header information.

The primary role of the personal firewall is to deny unauthorized remote access to the computer. **True**

A **circuit-level** gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.

One disadvantage of a packet filtering firewall is its simplicity. **False**

The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function. **True**

Typically the systems in the **DMZ** require or foster external connectivity such as a corporate Web site, an email server or a DNS server.

DKIM is designed to provide an email authentication technique that is transparent to the end user. **True**

Most browsers come equipped with SSL and most web servers have implemented the protocol. **True**

IPsec can assure that **a router advertisement comes authorized, update isn’t forged and a redirect message comes from the original router.**

As and alternative the RSA public-key encryption algorithm can be used with either the SHA-1 or the MD5 message digest algorithm for forming signatures. **True**

The **protocol identifier** field in the outer IP header indicates whether the association is an AH or ESP security association.

DKIM has been widely adopted by a range of email providers and many Internet service providers. **True**

A benefit of IPsec is **below the transport layer, no need to revoke keying material, and can provide security for individual users.**