Intrusion Detection System (IDS)

L'Intrusion Detection System o IDS è un dispositivo software e hardware (a volte la combinazione di tutti e due) utilizzato per **identificare accessi non autorizzati ai computer o alle reti locali.** Le intrusioni rilevate possono essere quelle prodotte da cracker esperti, da tool automatici o da utenti inesperti che utilizzano programmi semiautomatici.

Gli IDS vengono utilizzati per **rilevare tutti gli attacchi alle reti informatiche e ai computer:** per esempio gli attacchi tramite lo sfruttamento di un servizio vulnerabile, attacchi attraverso l'invio di dati malformati e applicazioni malevole, tentativi di accesso agli host tramite innalzamento illecito dei privilegi degli utenti, accessi non autorizzati a computer e file, e i classici programmi malevoli come virus, trojan e worm.

Un IDS è composto da **diversi componenti:**

- uno o più sensori utilizzati per ricevere le informazioni dalla rete o dai computer;
- una console utilizzata per monitorare lo stato della rete e dei computer;
- un motore che analizza i dati prelevati dai sensori e provvede a individuare eventuali falle nella sicurezza informatica.

Il motore di analisi si appoggia a un database ove sono memorizzate una serie di regole utilizzate per identificare violazioni della sicurezza.

Esistono **diverse tipologie di IDS** che si differenziano a seconda del loro compito specifico e delle metodologie utilizzate per individuare violazioni della sicurezza. Il più semplice IDS è un dispositivo che integra tutte le componenti in un solo apparato.

Un IDS consiste quindi in un **insieme di tecniche e metodologie** realizzate ad-hoc per rilevare pacchetti sospetti a livello di rete, di trasporto o di applicazione.