Bezpečnost počítačových sítí

Jan Závorka

Firewall

Typy firevallů

- Paketové filtry
- Aplikační brány
- Stavové paketové filtry
- Stavové paketové filtry s kontrolou protokolů a IDS

IDS (Intrusion Detection System)

Systém pro detekci narušení

Pro analýzu paketů využívá dvě technologie

- Vyhledává známé signatury
- Dekóduje jednotlivé protokoly

SNORT

- Snort je jednoduchý a volně šířitelný program, který využívá metodu identifikace signatur. Je k dispozici pro celou řadu operačních systémů.
- Snort pracuje jako síťový sniffer (analyzátor paketů), který však navíc obsah přenášených dat srovná s databází pravidel definujících známé útoky, a pokud najde shodu, provede patřičnou akci (obvykle oznámí poplach).

IDS

Dobrým příkladem využití IDS je analýza síťového provozu detekce a zabránění DoS útokům (SYN Flood, Ping of Death, Teardrop, …).
Většina těchto útoků má své typické chování, které lze detekovat a útoku zabránit