# IDS (سیستم‌های تشخیص و جلوگیری از نفوذ)

## NIDS (سیستم‌های تشخیص و جلوگیری از نفوذ شبکه)

NIDS (Network Intrusion Detection System) یک سیستم تشخیص و جلوگیری از نفوذ در سطح شبکه است. این سیستم‌ها با بررسی ترافیک شبکه و تشخیص الگوهای مشکوک و خطرناک، سعی در شناسایی فعالیت‌های نفوذی دارند. NIDS به عنوان یک سنسور نفوذ در شبکه عمل می‌کند و به صورت پس‌زمینه ترافیک شبکه را مورد نظر قرار می‌دهد. زمانی که الگوها و امضاهای مشکوک تشخیص داده شوند، اقدام به هشدار و گزارش آن‌ها می‌کند. اما نمی‌تواند به صورت مستقیم در مسیر ترافیک شبکه تغییری ایجاد کند.

## HIDS (سیستم‌های تشخیص و جلوگیری از نفوذ مبتنی بر میزبان)

HIDS (Host-based Intrusion Detection System) یک سیستم تشخیص و جلوگیری از نفوذ مبتنی بر میزبان است. این سیستم‌ها در داخل سرورها و سیستم‌های کاربردی نصب می‌شوند و فعالیت‌های نفوذی را در سطح میزبان تشخیص می‌دهند. HIDS به صورت مداوم فعالیت‌های سیستم و تغییراتی که در آن‌ها رخ می‌دهد را مشاهده می‌کند و در صورت شناسایی عملکردهای مشکوک یا خطرناک، هشدار می‌دهد. این سیستم‌ها معمولاً با استفاده از مقایسه الگوها و آمارهای مرتبط، به دنبال علایم فعالیت‌های نفوذی هستند.

# IPS (سیستم‌های جلوگیری و جلوگیری از نفوذ)

## NIPS (سیستم‌های جلوگیری و جلوگیری از نفوذ شبکه)

NIPS (Network Intrusion Prevention System) یک سیستم جلوگیری و جلوگیری از نفوذ در سطح شبکه است. این سیستم‌ها به عنوان یک سنسور نفوذ در شبکه فعالیت می‌کنند و به صورت مستقیم در مسیر ترافیک شبکه قرار می‌گیرند. آن‌ها ترافیک را تحلیل کرده و در صورت شناسایی الگوهای نفوذی، اقدام به جلوگیری از ادامه آن‌ها می‌کنند. اقدامات جلوگیری شامل مسدود کردن ترافیک مشکوک، ایجاد قوانین فایروال، ایجاد اعلان‌ها و گزارش‌ها و غیره است.

## HIPS (سیستم‌های جلوگیری و جلوگیری از نفوذ مبتنی بر میزبان)

HIPS (Host-based Intrusion Prevention System) یک سیستم جلوگیری و جلوگیری از نفوذ مبتنی بر میزبان است. این سیستم‌ها در داخل سرورها و سیستم‌های کاربردی نصب می‌شوند و فعالیت‌های نفوذی را در سطح میزبان شناسایی کرده و جلوگیری می‌کنند. HIPS به صورت مداوم فعالیت‌های سیستم را مشاهده می‌کند و در صورت شناسایی عملکردهای مشکوک یا خطرناک، اقداماتی مانند مسدود کردن، قطع ارتباط و یا جلوگیری از عملکرد آن‌ها را انجام می‌دهد.

این سیستم‌های IDS و IPS جهت محافظت و جلوگیری از نفوذ به سیستم‌های شبکه و میزبان در استفاده‌های مختلف امنیتی بکار می‌روند. هر کدام از آن‌ها وظایف و قابلیت‌های خود را دارند و با ترکیب آن‌ها، می‌توان سطح امنیت سیستم را بهبود بخشید.