IDS چیست ؟

IDS یک سیستم محافظتی است که خرابکاریهای در حال وقوع روی شبکه را شناسایی می کند.

روش کار به این صورت است که با استفاده از تشخیص نفوذ که شامل مراحل جمع آوری اطلاعات ، پویش پورتها ، به دست آوری کنترل کامپیوترها و نهایتا هک کردن می باشد ، می تواند نفوذ خرابکاریها را گزارش و کنترل کند.

از قابلیتهای دیگر IDS ، امکان تشخیص ترافیک غیرمتعارف از بیرون به داخل شبکه و اعلام آن به مدیر شبکه و یا بستن ارتباطهای مشکوک و مظنون می باشد.

ابزار IDS قابلیت تشخیص حملات از طرف کاربران داخلی و کاربران خارجی را دارد

بر خلاف نظر عمومی که معتقدند هر نرم افزاری را می توان به جای IDS استفاده کرد، دستگاههای امنیتی زیر نمی توانند به عنوان IDS مورد استفاده قرار گیرند:

1- سیستم هایی که برای ثبت وقابع شبکه مورد استفاده قرار می گیرند مانند : دستگاههایی که برای تشخیص آسیب پذیری در جهت از کار انداختن سرویس و یا حملات مورد استفاده قرار می گیرند.

2- ابزارهای ارزیابی آسیب پذیری که خطاها و یا ضعف در تنظیمات را گزارش می دهند.

3- نرم افزارهای ضدویروس که برای تشخیص انواع کرمها، ویروسها و به طورکلی نرم افزارهای خطرناک تهیه شده اند.

4- دیواره آتش (Firewall)

5- مکانیزمهای امنیتی مانند SSL ، VPN و Radius و ... .

چرا دیواره آتش به تنهایی کافی نیست ؟

به دلایل زیر دیواره های آتش نمی توانند امنیت شبکه را به طور کامل تامین کنند :

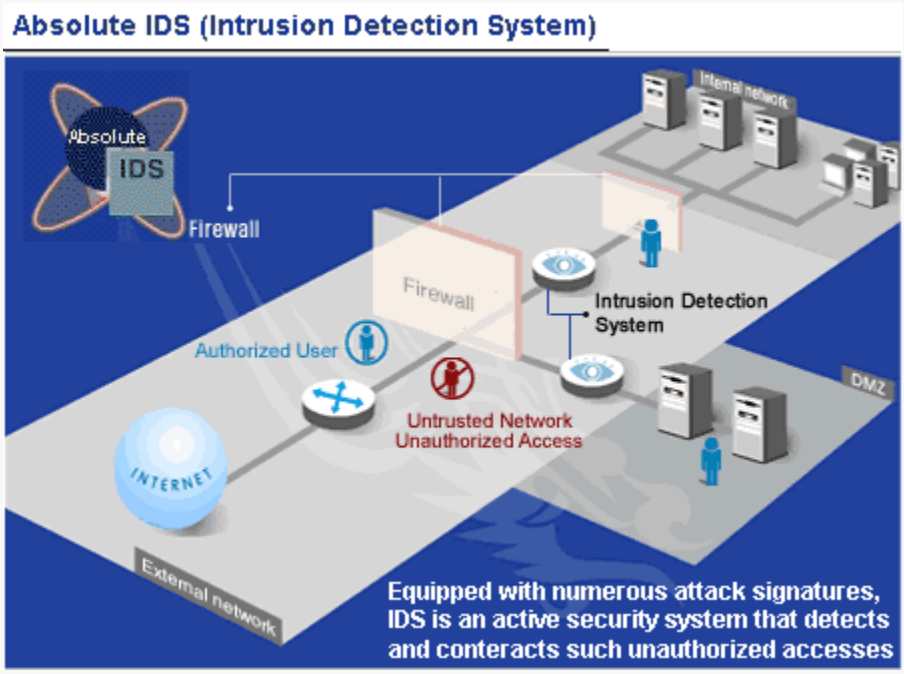
1. چون تمام دسترسی ها به اینترنت فقط از طریق دیواره آتش نیست.
2. تمام تهدیدات خارج از دیواره آتش نیستند.
3. امنیت کمتر در برابر حملاتی که توسط نرم افزارها مختلف به اطلاعات و داده های س ازمان می شود ، مانند Active ، Java Applet، Virus Programs.

تکنولوژی IDS

1- Plain Hand Work

2- Network Based

3- Host Based



NIDS (Network Base)

گوش دادن به شبکه و جمع آوری اطلاعات ازطریق کارت شبکه ای که در آن شبکه وجود دارد .

به تمامی ترافیک های موجود گوش داده و در تمام مدت در شبکه مقصد فعال باشد

HIDS (Host Base)

تعداد زیادی از شرکتها در زمینه تولید این نوع IDS فعالیت می کنند.

روی PC نصب می شود و از CPU و هارد سیستم استفاده می کنند.

دارای اعلان خطر در لحظه می باشد.

جمع آوری اطلاعات در لایه Application

مثال این نوع IDS ، نرم افزارهای مدیریتی می باشند که ثبت وقایع را تولید و کنترل می کنند.

Honey pot

سیستمی می باشد که عملا طوری تنظیم شد ه است که در معرض حمله قرار بگیرد . اگر یک پویشگری از NIDS ، HIDS و دیواره آتش با موفقیت رد شود متوجه نخواهد شد که گرفتار یک Honey pot شده است. و خرابکاری های خود را روی آن سیستم انجام می دهد و می توان از روشهای این خرابکاریی ها برای امن کردن شبکه استفاده کرد.

محل قرارگیری IDS

محل قراگیری IDS ها کجاست ؟

بیرون دیواره آتش ؟

داخل دیواره آتش (داخل DMZ یا شبکه داخلی)؟

چه ترافیکی را می بایست کنترل کند؟

چه چیزهایی را می بایست کنترل کند؟

کارآیی یک IDS خوب وقتی مشخص می شود که :

بتوان کنترل و مدیریت آن را به صورت 24 ساعته و 7 روز در هفته انجام داد.

توسط یک مدیر با دانش بالا مدیریت شود تا بتواند از وقایع بدست آمده کنترل های جدیدی را روی دیوار آتش پیاده سازی کند.

مرتب کنترل وبا توجه به حوادث روزانه (ویروس ها و ورم ها و روش های هک جدید) به روزرسانی شود.

حملات به طور کلی به دو بخش تقسیم می شوند:

1- **غیرفعال** : فکر دسترسی به سیستم های آسیب پذیر بدون دستیابی به اطلاعات

2- **فعال** : دستیابی بدون اجازه به همراه تغییر در منابع و اطلاعات یک سازمان

از نظر شخص نفوذگر حملات به گروههای زیر تقسیم می شوند:

1- **داخلی** : یعنی اینکه حملات از طریق کارکنان و یا شرکای تجاری و یا حتی مشتریانی که به شبکه شما متصل می باشند.

2- **خارجی** : حملاتی که از خارج سازمان و معمولا از طریق اینترنت انجام می گیرد.