# IDS

# Satanic Hell

## جهنم شیطانی

# IDS

## مباحثی پیرامون ای دی ا س

نویسنده: Satanic Soulful
تاریخ: **14/1/1384**

Contact:
Satanic.soulful@GMail.Com
Satanic_Soulful@Yahoo.Com
Special TNX2:
Hell Hacker – **B0rn2h4k –** Phacker_Ir – McT – X Hulk & Dr. Hoshmand

ملاحضات:
لازم به تذکر است کلیه مطالب گفته شده تنها جنبه آموزشی دارد و هر گونه استفاده غیر آموزشی به عهده خود کاربر می باشد و نویسنده این مقاله و مدیریت سایت پرشین هکرز و جهنم شیطانی هیچ گونه مسولیتی نسبت به استفاده نادرست از این مقاله را برعهده نمی گیرند!

استفاده از مطالب این مقاله با ذکر نام نویسنده و همچنین گروهای مربوط بلامانع است.

منابع:

ژورنال سیاه – گروه مشورت
Cisco IDS- B2net-Hucom Security-FounderNet
و راهنمای دکتر هوشمند

به نام خدای عشق

مقدمه:

هر روز که میگذرد بر علم گسترده و بزرگ کامپیوتر و نت ورک اطلاعات بیشتری اضافه میشود.

هر روز حفره ها گوناگون کشف میشود پچ های جدید ساخته میشود و ...

در دنیای امروز دیگر هکر ها فکرو ذهن خودشان را به هک کردن کلاینت ها و چند سایت نمگذارند.

هدف امروز هکرها سرور ها و شبکه های گسترده می باشد با هک کردن یک سرور میزبان صدها و شاید هزاران سایت هک و دیفیس میشود.

وقتی یک شبکه مثلا شبکه لن یک دانشگاه هک میشود میشه با استفاده از ابزار گوناگون به هزار کامپیوتر نفوذ کرد!

با توجه به این موارد میشود برای حفاضت از سرور خود کارهای انجام داد یکی از این کارها قرار دادن ای دی اس هست.

اگر هکری در حال نفوذ باشد ای دی اس آن را شناسایی میکند!

پس میشود از هک شدن شبکه یا سرور جلوگیری کرد

یکی دیگر از مزیت های ای دی اس اینست که مشخص میکند نفوذ کننده در داخل شبکه هست یا در خارج از شبکه...

## IDS چيست؟

IDS يك سيستم محافظتي است كه خرابكاريهاي در حال وقوع روي شبكه را شناسايي مي كند.

روش كار به اين صورت است كه با استفاده از تشخيص نفوذ كه شامل مراحل جمع آوري اطلاعات ، پويش پورتها ، به دست آوري كنترل كامپيوترها و نهايتا هك كردن مي باشد ، مي تواند نفوذ خرابكاريها را گزارش و كنترل كند.

از قابليتهاي ديگر IDS ، امكان تشخيص ترافيك غيرمتعارف از بيرون به داخل شبكه و اعلام آن به مدير شبكه و يا بستن ارتباطهاي مشكوك و مظنون مي باشد.

ابزار IDS قابليت تشخيص حملات از طرف كاربران داخلي و كاربران خارجي را دارد.

بر خلاف نظر عمومي كه معتقدند هر نرم افزاري را مي توان به جاي IDS استفاده كرد، دستگاههاي امنيتي زير نمي توانند به عنوان IDS مورد استفاده قرار گيرند:

1- سيستم هايي كه براي ثبت وقابع شبكه مورد استفاده قرار مي گيرند مانند : دستگاههايي كه براي تشخيص آسيب پذيري در جهت از كار انداختن سرويس و يا حملات مورد استفاده قرار مي گيرند.

2- ابزارهاي ارزيابي آسيب پذيري كه خطاها و يا ضعف در تنظيمات را گزارش مي دهند.

3- نرم افزارهاي ضدويروس كه براي تشخيص انواع كرمها، ويروسها و به طوركلي نرم افزارهاي خطرناك تهيه شده اند.

4- ديواره آتش (Firewall )

5- مكانيزمهاي امنيتي مانند SSL ، VPN و Radius و ... .

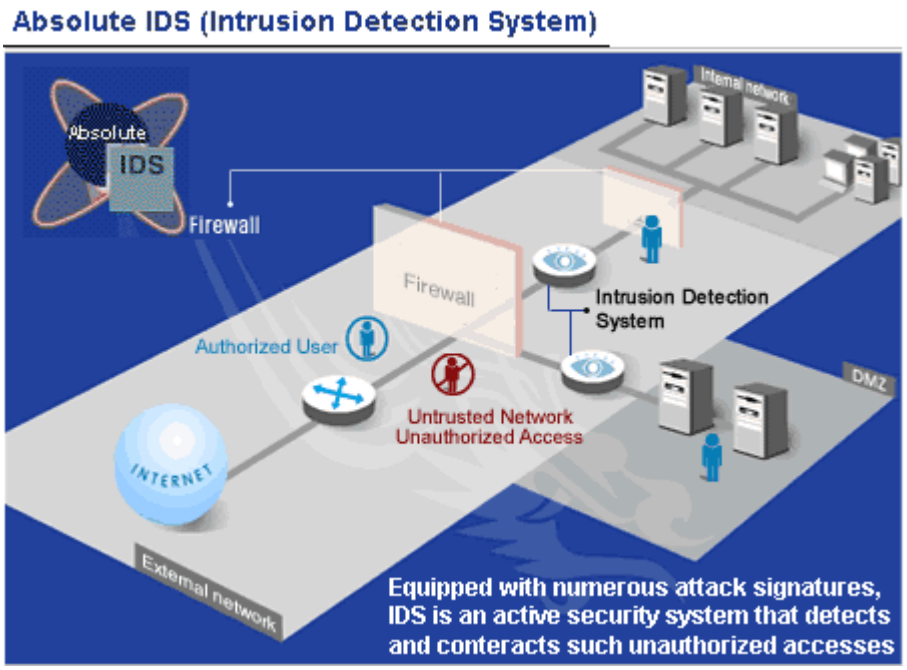
# تكنولوژي IDS

1- Plain Hand Work

2- Network Based

3- Host Based

4- Honey pot




## (Network Base) NIDS

گوش دادن به شبكه و جمع آوري اطلاعات ازطريق كارت شبكه اي كه در آن شبكه وجود دارد .

به تمامي ترافيك هاي موجود گوش داده و در تمام مدت در شبكه مقصد فعال باشد.

## (Host Base) HIDS

تعداد زيادي از شركتها در زمينه توليد اين نوع IDS فعاليت مي كنند.

روي PC نصب مي شود و از CPU و هارد سيستم استفاده مي كنند.

داراي اعلان خطر در لحظه مي باشد.

## جمع آوري اطلاعات در لايه Application

مثال اين نوع IDS ، نرم افزارهاي مديريتي مي باشند كه ثبت وقايع را توليد و كنترل مي كنند.

## Honey pot

سيستمي مي باشد كه عملا طوري تنظيم شده است كه در معرض حمله قرار بگيرد. اگر يك پويشگري از NIDS ، HIDS و ديواره آتش با موفقيت رد شود متوجه نخواهد شد كه گرفتار يك Honey pot شده است. و خرابكاري هاي خود را روي آن سيستم انجام مي دهد و مي توان از روشهاي اين خرابكاريي ها براي امن كردن شبكه استفاده كرد.(در رابطه با ظرف عسل مقاله كاملی نوشته شود دانلود اين مقاله از اينجا)

## چرا ديواره آتش به تنهايي كافي نيست ؟

به دلايل زير ديواره هاي آتش نمي توانند امنيت شبكه را به طور كامل تامين كنند :

1. چون تمام دسترسي ها به اينترنت فقط از طريق ديواره آتش نيست.
2. تمام تهديدات خارج از ديواره آتش نيستند.

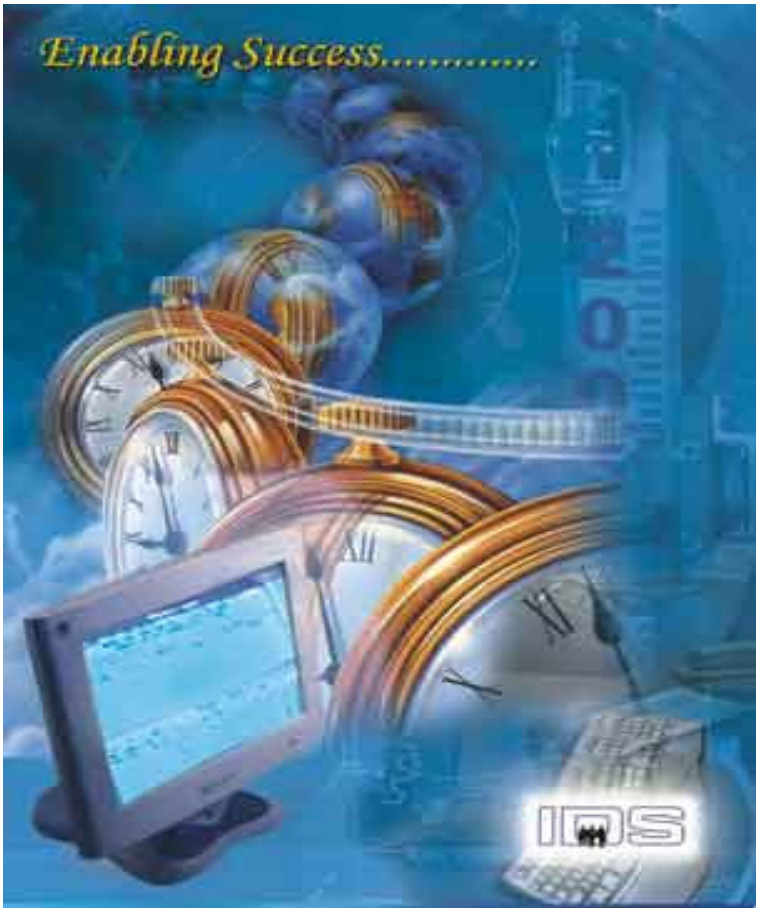
3. امنيت كمتر در برابر حملاتي كه توسط نرم افزارها مختلف به اطلاعات و داده هاي سازمان مي شود ، مانند Active ، Java Applet، Virus Programs.

برای تامین امنیت یك شبكه، Firewall اولین چیزی است كه بایستی پیاده سازی شود. نكته حائز اهمیت آنكه، نصب یك Firewall در شبكه به تنهایی امنیت آن شبكه را تامین نخواهد كرد!!!

فايروال معمولا سيستمي است كه با تعريف يك سري قوانين مشخص روي آن از ورود و يا خروج بسته هاي خاص جلوگيري مي كند اما IDS بسته هايي را كه از نظر فايروال اجازه عبور را دارند نيز كنترل نموده و در صورت تشخيص امكان نفوذ آنها را مسدود مي نمايند براي توضيح بيشتر درنظر بگيريد كه ما در برنامه فايروال خود قوانين را تعريف كرده ايم كه امكان دسترسي كاربران اينترنت به پورت 80 رايانه سرور وب خود را داده و به كاربران شبكه محلي خودمان نيز امكان اتصال به پورت 80 رايانه هاي موجود در شبكه اينترنت را داده ايم . از نظر فايروال هر بسته خروجي كه به مقصد پورت 80 ساير رايانه ها باشد مجوز عبور دارد در حالي كه براي مثال ويروس code red از رايانه ميزبان وب ما اتصالات زيادي به پورت 80 ساير رايانه ها بر قرار ساخته و با اشغال كردن مسير ارتباط باعث از كار افتادن سرويس وب ما مي گردد كه اين از نظر يك فايروال بدون اشكال مي باشد اما سيستم IDS با بررسي بسته هاي ارتباطي و اطلاع از نوع عملكرد اين تروجان پي مي برد كه اين يك ويروس Red code بوده و عمليات آنرا متوقف مي نمايد IDS داراي يك بانك اطلاعاتي كامل راجع به تروجانها ، نوع عملكرد آنها ، ساختار بسته هاي آنها و پورتي كه معمولا جهت اتصال استفاده مي كنند مي باشند كه به سيستم اين امكان را مي دهد كه از نفوذ به داخل سيستم جلوگيري نمايد ضمنا معمولا يك نفوذ گر قبل از شروع به نفوذ جهت كسب اطلاعات از وضعيت امنيتي

سيستم ما اقدام به عملياتي خاص مي نمايد كه اين از ديد يك فايروال مخفي مي ماند براي مثال اولين كاري كه معمولا نفوذ گران انجام مي دهند عمليات بررسي پورتها (Port scan) مي باشد كه جهت كسب اطلاعات راجع به پورتهاي باز و بسته سيستم و اينكه اگر يك پورت باز است چه سرويسي روي سرور فعال شده مي باشد از نظر فايروال يك سري اتصال به پورت هاي مختلف اتفاق افتاده كه نسبت به قوانين تعريف شده در فايروال (باز بودن يا بسته بودن پورت) با آنها برخورد مي شود اما از ديد يك IDS اگر يك شخصي تعداد زيادي اتصال در مدتي كوتاه به پورتهاي سيستم داشته باشد به عنوان يك نفوذ گر كه عمليات Port scan را انجام مي دهد شناخته مي شود و گزارش از عملكرد و همچنين موقعيت او و شناسه (IP) او به كار ميدهد

مديران شبكه با بررسي وضعيت گزارشهاي نفوذ مي توانند تدابير خاص خود را در نظر گرفته و در صورت مشخص بودن موقعيت شخص نفوذگر نسبت به طي مراحل قانوني جهت جلوگيري از نفوذ هاي بعدي و احيانا جبران خسارت اقدام كنند.



براي تشخيص خطرات وحملات احتمالي مي بايست سيستم خود را در برابر تقاضاهايي كه سرويس هاي نامناسب درخواست مي كنند مورد بررسي قرار دهيد.اين بررسي ها در تشخيص حملات واقعي به ما كمك مي كند. با توجه به انواع راه هايي كه نفوذ گران براي دسترسي به سيستمها استفده مي كنند نگاهي اجمالي به روشهاي آسيب رساني و نفوذ مي اندازيم.

### استفاده از آسيب پذيري هاي معروف:

دراكثر موارد حمله به معني تلاش براي استفاده از نقص يا ايجاد آن در سيستم امنيتي يك سازمان اطلاق مي شود و اين يكي از راههاي نفوذگري در شبكه مي باشد.

اغلب خود سازمان ممكن است از ابزاري براي امن كردن شبكه استفاده كند كه كار حمله كننده را آسان مي سازد به بيان واضح تر اينكه ابزارهاي امنيتي نيز خود داراي نواقص و حفره هاي امنيتي مي باشد كه اختيارات بيشتري را به نفوذگر مي دهد. اين نرم افزارها اغلب مانند شمشير دو لبه عمل مي كنند و مورد استفاده هردو گروه كاربران وحمله كنندگان قرارمي گيرد مانند نرم افزارهاي كنترل صحت و يكپارچگي فايل يا نرم افزارهايي كه جهت تست آسيب پذيري شبكه مورد استفاده قرارمي گيرند.

چك كردن يكپارچگي فايلها با استفاده از روش هاي سيستمي و با قابليت ادغام روشهاي مختلف با يكديگر و با ابزارهايي نظير anti-SATAN يا Courtney امكان پذير مي باشد.

### ترافيك خروجي غير معمول:

يك نفوذگر با استفاده از تعداد زيادي Exploit و حتي نفوذ هاي ناموفق سعي در به دست آوردن كنترل كامپيوتر مقصد دارد. اين عمليات نفوذگرانه، ترافيك معمول شبكه را افزايش مي دهد و نشانه

وقوع يك حمله درآينده مي باشد. هر ابزار تست آسيب پذيري مي بايست قابليت تشخيص فعاليت هاي مشكوك و غير متعارف را داشته باشد و با ارائه گزارش ، اعلام خطر لازم را به مدير شبكه بدهد.

حد تكرار براي كمك به تشخيص فعاليتهاي واقعي و مشكوك :

فعاليتهاي شبكه بوسيله دريافت و كنترل بعضي پارامترها قابل شناسايي است مانند User Profile يا از Session State .

زمان بين تكرار فعاليتها:

پارامتري براي تشخيص زمان سپري شده بين دو واقعه متوالي. مثلا" وقتي بخواهيد با نام كاربري اشتباه وارد سيستم شويد، سه تلاش براي ورود با نام غلط بين فاصله زماني 2 دقيقه يك فعاليت مشكوك به نظر مي رسد.

اشتباه در تايپ ويا جوابهايي كه در يك Session ايجاد مي شود.

پروتكل ها وسرويس هاي شبكه به صورت كاملا" دقيقي مستند شده اند و از ابزارهاي نرم افزاري خاص استفاده مي كنند. هرگونه ناهماهنگي با قالب شناخته شده( مثل اشتباه در تايپ يك دستور ) ممكن است اطلاعاتي براي شناسايي سرويسهاي كه مي توانند مورد حمله يك نفوذگر قراربگيرند باشد.

اگر امكان Audit در سيستم فعال شده باشد ،مثل Send Mail Relaying، توالي ارتباط Log بصورت معمولي و قابل پيش بيني اتفاق مي افتد.هرچند كه اگر در Log دريافت شده دستورات غير مجاز ديده شود ممكن است نتيجه موارد اشتباه غير عمدي ويا سعي در Spoofing باشد.( Spoofing به اين معني است كه نفوذگر آدرس خود را به آدرسي كه براي سيستم شناخته شده است تغيير داده و به اين ترتيب به سيستم نفوذ مي كند.)

تست تلاشهاي مخرب ممكن است شامل موارد زير باشد:

- شناسايي تلاشهاي متعدد براي جبران خطاهاي تايپي و تكرار دستورات
- تشخيص خطاهاي مكرر براي يافتن پروتكل ها كه بدنبال يك تلاش موفق انجام مي شود.
- تشخيص خطا و يادگيري در جهت شناسايي نرم افزارهاي و يا سيستم عامل هاي موجود در سايت مقصد.

## ناهماهنگي در جهت ارسال و دريافت اطلاعات

هرگونه ناهماهنگي ترافيكي در Packetها يا يك Session نشانه اي از يك حمله پنهاني است. بررسي آدرس مبداء و مقصد ( به صورت ورودي يا خروجي) ميتواند جهت Packet را تشخيص بدهد. روند برقراري يك session با تشخيص اولين پيام ارسال شده شناسايي مي شود. يك درخواست براي دريافت يك سرويس از شبكه محلي به صورت يك session ورودي است و پروسه فعال كردن يك سرويس بر پايهWeb از يك شبكه محلي يك session خروجي است.

موارد زير مي تواند به عنوان حمله محسوب شود:

- Packet هايي كه منشاء آنها اينترنت است بدون اينكه در خواستي از سمت شبكه محلي داشته باشد و وارد شبكه شود.

اين حالت ممكن است نشان دهنده يك حمله IP Spoofing از خارج باشد. اين مشكلات مي توانند در-Router هايي كه قابليت مقايسه آدرس مبداء و مقصد را دارند بر طرف شوند .در عمل تعداد اندكي از Router ها در شبكه مي توانند به عنوان فايروال عمل كنند.

- بر عكس حالت قبل Packet هايي كه به صورت خروجي در يك شبكه محلي ايجاد مي شوند و به يك شبكه خارجي فرستاده مي شوند

- Packet ها با پورت هاي مبداء و مقصد غير مشخص. اگر منبع پورت در مورد يك درخواست ورود يا خروج اطلاعات با نوع سرويس يكسان نباشد ممكن است به عنوان يك تلاش براي نفوذ يا پويش سيستم تلقي شود. بطور مثال در خواست Telnet از روي پورت 100 در محيطي كه انتظار چنين پشتيباني براي سرويس وجود ندارد.(در رابطه با تلنت نيز مقاله جامعی موجود ميباشد متوانيد از **اينجا** دريافت كنيد)

ترافيك غير معمول بيشتر توسط فايروال شناسايي شده و Packet هاي مشكوك را ازبين مي برد. با توجه به اينكه فايروالها هميشه با سيستم هاي تشخيص نفوذ ادغام نمي شوند ، بنابراين ممكن است كه سيستمهاي تشخيص نفوذ راه حلي براي اين مشكل باشد.

## علايم نفوذ

معمولا با اجراي برنامه هاي خاص در سيستم انتظار مواجهه با رفتارهاي خاص و مشابه وجود دارد

بعضي از موارد مانند موارد زير :

## مشخصات تاريخ و زمان :

در بعضي محيط هاي خاص بطور معمول بعضي رفتارها در زمان خاصي در شبكه اتفاق مي افتد. مثلا فرض كنيد بطور معمول شنبه صبح يكسري اطلاعات به بخش مركزي شركت ارسال مي شود كه مربوط به اطلاعات مالي است. چنين ترافيكي در شنبه صبح هميشه اتفاق مي افتد و عادي است در صورتيكه چنين ترافيكي روز جمعه اتفاق بيفتد و ثبت شود ، غير معمول است و بايد به عنوان يك رفتار غير معمول يا نفوذ به سيستم مورد بررسي دقيق قرارگيرد.

## مشخصات منابع سيستم:

بعضي نفوذ هاي خاص باعث خرابي بعضي پارامترهاي خاص سيستم ميشود مثلا يك حمله Brute Force براي شكستن حرف رمز باعث در گير كردن CPU ميشود در حاليكه يك حمله DoS همين كاررا با سرويس هاي سيستم انجام ميدهد. استفاده سنگين از منابع سيستم ( پروسسور، حافظه، ديسك سخت ، سرويسها و اتصالات شبكه ) كه در زمانهاي غير معمول اتفاق مي افتد براي شناسايي حمله بسيار مفيد هستند و بايد به آنها بسيار توجه كرد.

## **Packet** هايي با تاييد هاي **TCP** غير معمول :

اگر در يك Packet نشانه مربوط به ACK فعال باشد و قبل از آن هيچ SYN-Packet ارسال نشده باشد، ممكن است نتيجه يك حمله در سيستم باشدهمچنين اين حالت ممكن است اثر يك Packet خراب هم باشد كه در يك شبكه با نرم افزار هاي خراب ايجاد مي شود و واقعا" حمله نفوذي نباشد.

## سرويس هاي مختلف با علايم مختلف :

ممكن است در بعضي موارد انتظار ايجاد ترافيك خاص از يك كاربر مشخص داشته باشيم مثلا كاربري كه در يك ماموريت اداري

بسر مي برد معمولا" فقط نامه هاي خود را چك مي كند ويا فايلي را انتقال مي دهد . در صورتيكه دسترسي اين كاربر به پورت هاي مختلف از طريق Tel net، دليلي بر امكان نفوذ يا حمله است .

## علامت نفوذ

## موارد غير معمول

يك نفوذ كننده بالقوه ممكن است عمليات نفوذ خود را به گونه اي طراحي كند كه اثر جانبي آن باعث رفتارهاي غير معمول در سيستم باشد. مانيتورينگ اثرات جانبي بسيار سخت است چون پيدا كردن محل آنها به سادگي امكان پذير نيست از موارد غير منتظره سيستم به موارد زير مي توان اشاره كرد:

1- مشكلات تعريف نشده در سخت افزار يا نرم افزارسيستم مثل خاموش شدن بدون علت سرور، عدم كاركرد بعضي برنامه هاي نرم افزاري مانند IIS ، موارد غير معمول restart شدن سيستم ها ، تغييرات در تنظيم clock سيستم

2- بروزاشكالات نامشخص در منابع سيستم مثل File System Overflow يا مشغول بودن بيش از حد CPU

3- دريافت پيام هاي غير متعارف از بعضي برنامه هاي خود اجرا ، مثل پيغامهايي كه نشان دهنده عدم اجرا و يا خطا در هنگام اجراي يك برنامه ايجاد شده باشد.بخصوص برنامه هايي كه براي مانيتور كردن سيستم طراحي شده اند مثل Syslog .

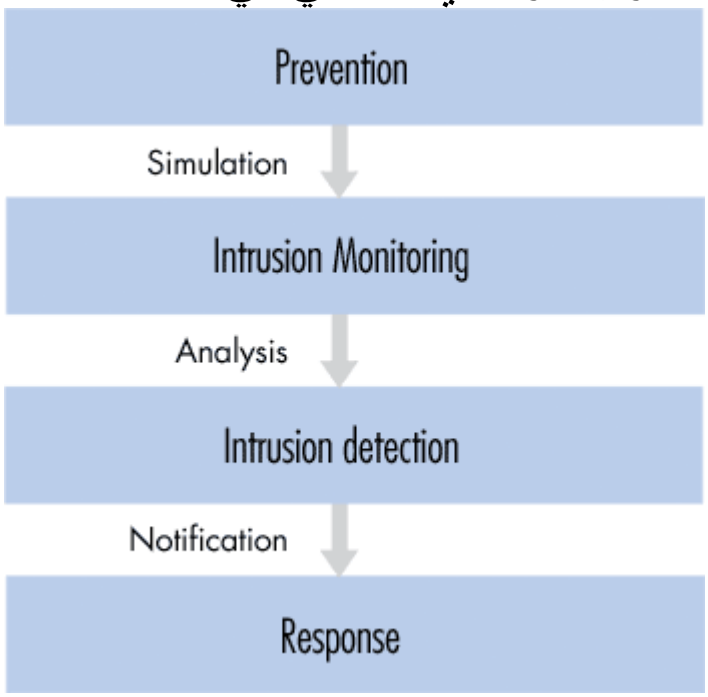
4- بروز اشكالات نامشخص در كارايي سيستم مثلا" در Router ها يا سرويس هاي سيستم مثل كند شدن سرور

5- بروز رفتارهاي مشكوك در اجراي برنامه هاي كاربرمثل اشكال در دسترسي به بعضي منابع شبكه

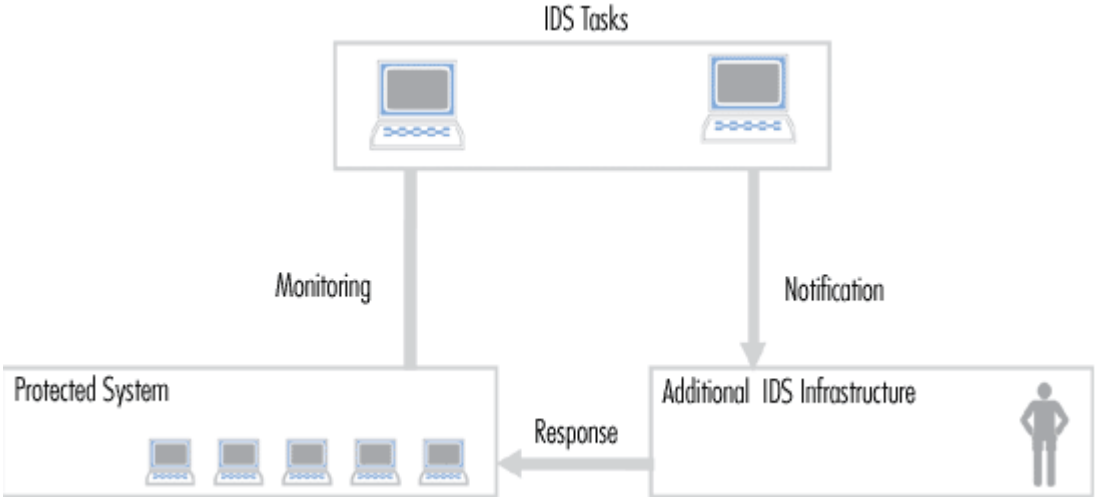
6- عملكرد مشكوك در فايلهاي ثبت وقايع ( Log ها)بررسي اين فايل ها از نظر سايز براي اينكه حجم فايل از اندازه متعارف خيلي بيشتر يا كمتر نباشد. مگر اينكه مدير شبكه خود چنين تغييري ايجاد كرده باشد.


مهمترين كار يك سيستم كشف نفوذگر،دفاع از كامپيوتر بوسيله شناسايي حمله و جلوگيري از آن است. شناسايي حمله هكر بستگي به نوع و تعداد عكس العمل مورد نظر دارد. ( شكل 1)
مقابله با نفوذ، نياز به يك سيستم تركيبي دام گذاري و تله اندازي دارد كه هردو اين پروسه ها بايد با بررسي و دقت انجام شود. از كارهاي ديگري كه بايد انجام داد ، تغيير دادن جهت توجه هكر است.

هر دوسيستم واقعي و مجازي(Honeypot) به دام اندازي هكر به طور دائمي ديده باني (Monitor ) مي شوند و داده هاي توليد شده توسط سيستم شناسايي نفوذ گر (IDS) براي شناسايي نحوه عملكرد حمله به دقت بررسي مي شود كه اين مهمترين وظيفه يك IDS جهت شناسايي حملات و يا نفوذهاي احتمالي مي باشد.




( شكل 1 )



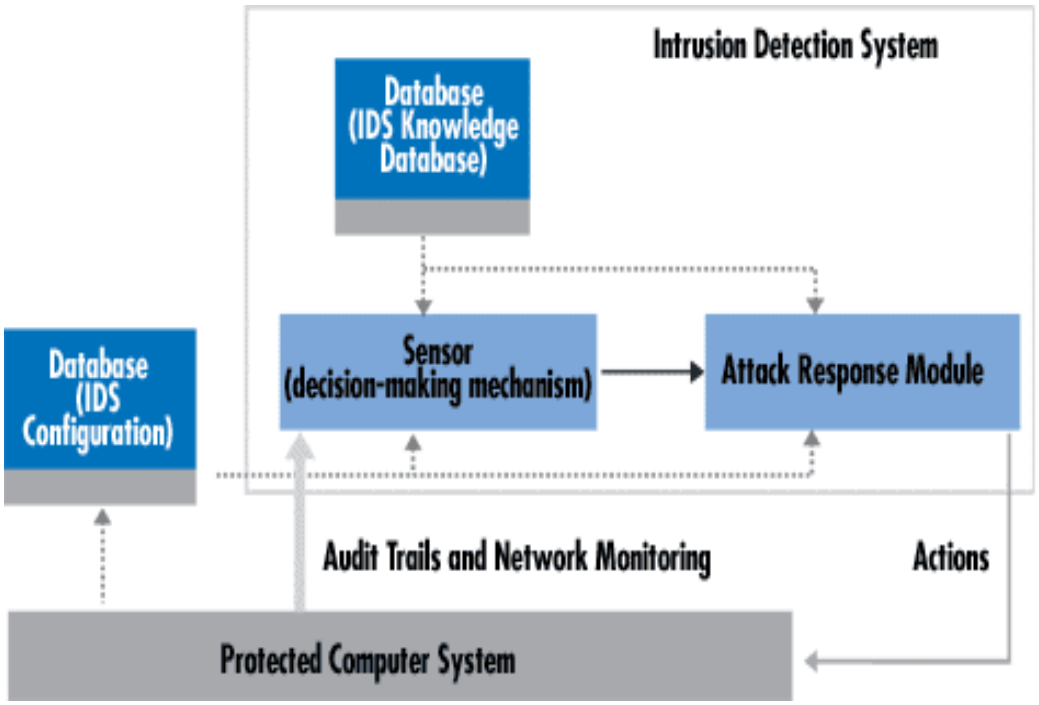

( شكل 2 )

وقتي كه يك حمله يا نفوذ شناسايي شد، IDS سرپرست شبكه را مطلع مي سازد. مرحله بعدي كار مي تواند بر عهده سرپرست شبكه يا خود IDS باشد كه از بررسيهاي به عمل آمده نتيجه گيري كرده و اقدام متقابل را انجام دهد.(مانند جلوگيري از عملكرد يك قسمت بخصوص براي پايان بخشيدن به Session هاي مشكوك يا تهيه نسخه پشتيبان از سيستم براي حفاظت از اطلاعات ، و يا انتقال ارتباط به يك سيستم گمراه كننده مانند Honeypot و چيزهاي ديگر كه بر اساس سياستهاي ( Policy ) شبكه قابل اجرا باشد . در حقيقت IDS يك از عناصر سياستهاي امنيتي شبكه است .

در بين وظايف مختلف IDS ، شناسايي نفوذگر از اساسي ترين آنهاست .حتي ممكن است در مراجع قانوني از نتايج و گزارشات حوادثي كه IDS اعلام مي كند استفاده نمود، و از حملاتي كه در آينده اتفاق خواهد افتاد با اعمال وصله هاي امنيتي مناسب از حمله به يك كامپيوتر بخصوص ويا يك منبع شبكه جلوگيري كرد.
شناسايي نفوذ ممكن است گاهي اوقات زنگ خطر اشتباهي را به صدا در آورد. براي مثال نتيجه خراب كاركردن يك كارت شبكه و يا ارسال شرح يك حمله و يا اثر يك نفوذ ازطريق Email .

## ساختار و معماري سيستم تشخيص نفوذ:

سيستم تشخيص نفوذ يك هسته مركزي دارد و يك تشخيص دهنده(موتور تشخيص) است كه مسئوليت تشخيص نفوذ را دارد. اين سنسور يك مكانيزم تصميم گيري بر اساس نوع نفوذ دارد.




( شكل 3)

اين سنسور اطلاعات خام را از سه منبع دريافت مي كند.

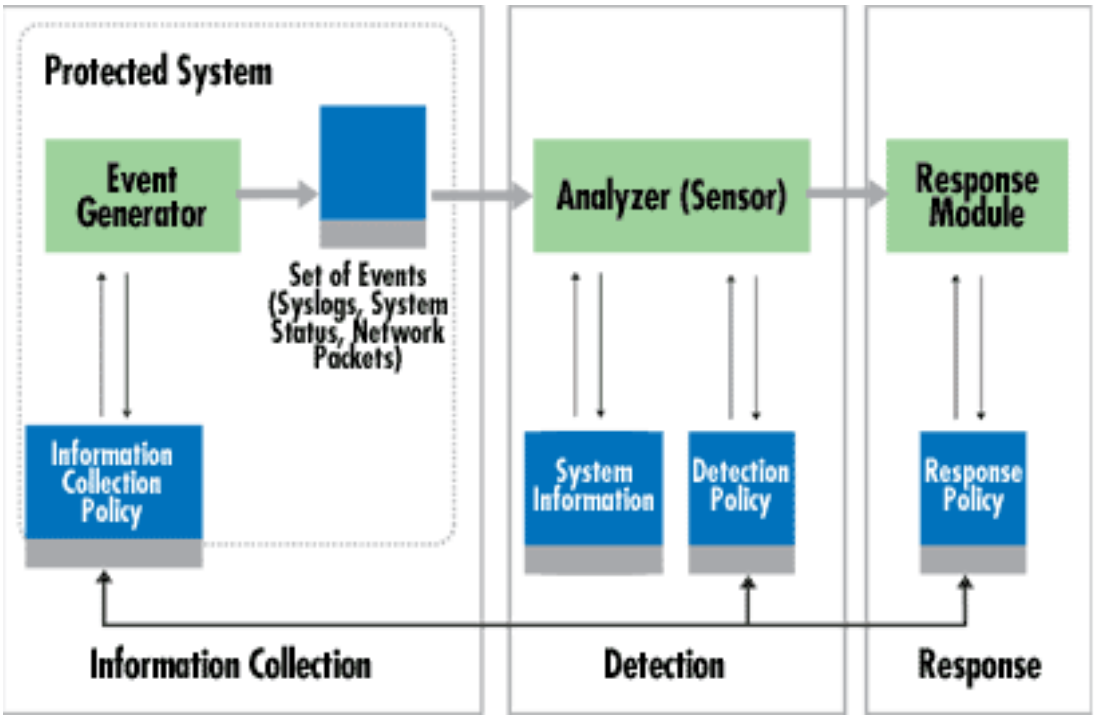
1- از اطلاعات موجود در بانك اطلاعلتي خود IDS .
2- فايل ثبت وقايع سيستم (syslog).
3- آثار ترافيك عبوري و ديده باني شبكه .

فايل ثبت وقايع سيستم (syslog) ممكن است به طور مثال اطلاعات پيكربندي سيستم و دسترسي هاي كاربران باشد. اين اطلاعات اساس تصميم گيري هاي بعدي مكانيزم سنسور خواهد بود.

اين سنسور با يك Event Generator كه مسئول جمع آوري اطلاعات است با هم كار مي كنند. ( شكل 4) . قوانين جمع آوري اطلاعات كه بوسيله سياست هاي Event generator مشخص مي شود ، تعيين كننده نوع فيلترينگ از روي حوادث و اطلاعات ثبت شده است.

Event Generator ، مثل سيستم عامل يا شبكه يا يك برنامه اجرايي ، توليد كنندهPolicy هايي هستند كه ممكن است يك واقعه

ايجاد شده در سيستم عامل يا Packet هاي شبكه را ثبت كنند. اين مجموعه به همراه اطلاعات Policy مي تواند در يك سيستم محافظت شده يا خارج از شبكه قرار داده شود. در بعضي شرايط خاص هيچ محل مشخصي به عنوان محل حفظ اطلاعات ايجاد نمي شود مثل وقتي كه اطلاعات جمع آوري شده از وقايع مستقيما" به يك سيستم آناليز ارسال مي شود.



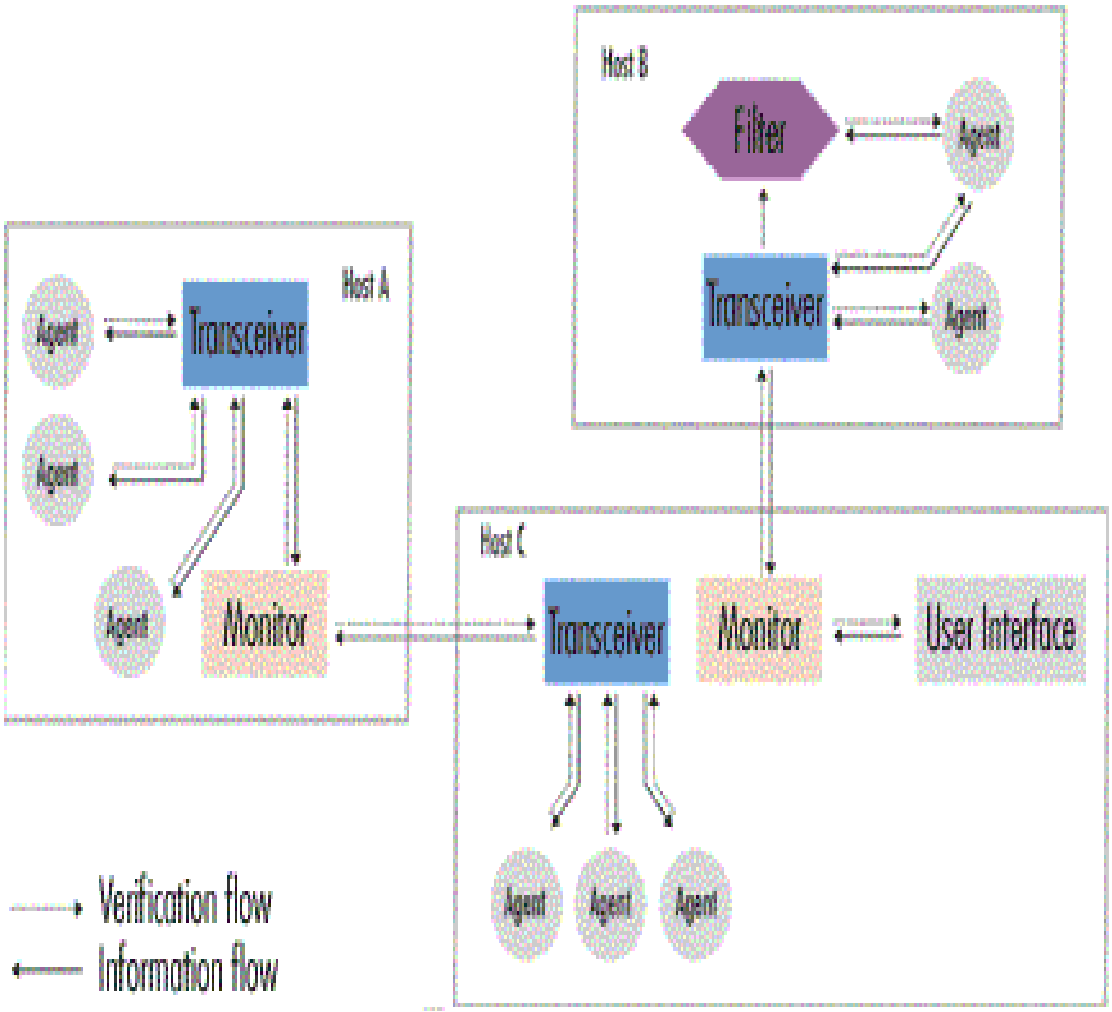

( شكل 4 )

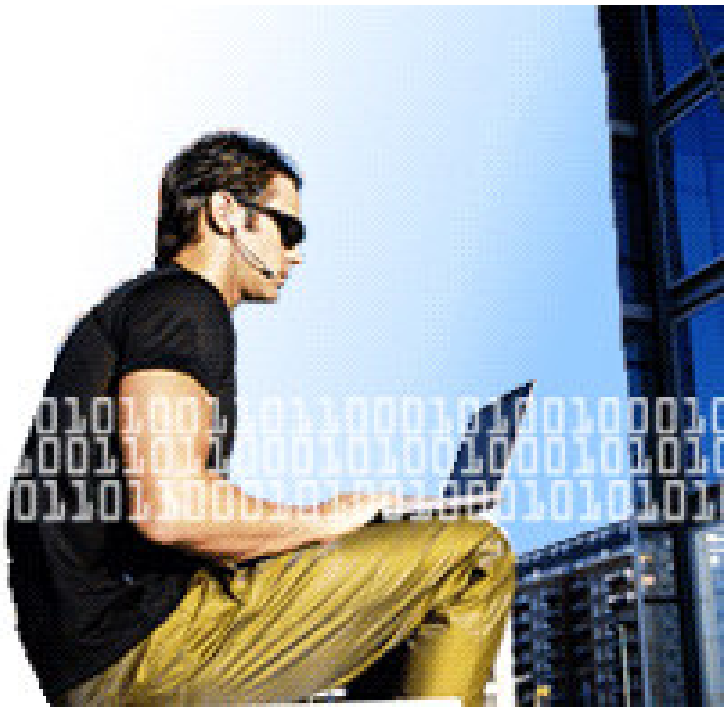
وظيفه سنسور فيلتر كردن اطلاعات است و حذف كردن هر داده غير مرتبط كه از طرف منابع دريافت اطلاعات مي رسد. تحليل كننده براي دستيابي به اين هدف از Policy هاي موجود استفاده مي كند.تحليل گر نكاتي مانند اثر و نتيجه حمله ، پرو فايل رفتارهاي نرمال و صحيح و پارامترهاي مورد نياز مثل Threshold ها را بررسي مي كند .علاوه بر همه اينها بانك اطلاعاتي كه پارامترهاي پيكربندي IDS را در خود نگه مي دارد، روشهاي مختلف ارتباطي

را ايجاد مي كنند.سنسور يا گيرنده هم بانك اطلاعاتي خاص خود را دارد، كه شامل تاريخچه پويايي از نفوذهاي پيچيده بوده يا با توجه به تعدد حمله مورد تحليل قرارگرفته است.
سيستم تشخيص نفوذ مي تواند به صورت متمركز مثل برقراري يك فايروال فيزيكي يا به صورت غير متمركز انجام شود.يك IDS غير متمركز شامل تعداد زيادي سيستم تشخيص نفوذ در يك شبكه بزرگ است كه هركدام از آنها با هم در ارتباط هستند.سيستم هاي پيچيده تر از ساختاري پيروي مي كنند كه ماژول هاي مشابه برنامه هاي خود اجرايي دارند كه روي هر كامپيوتر اجرا مي شوند. عملكرد اين سيستم جايگزين ، مونيتور و فيلتر كردن تمام فعاليتهاي مرتبط با يك بخش محافظت شده است كه بتواند يك آناليز دقيق و پاسخ متناسب از شبكه دريافت كند.
يكي از قسمت هاي بسيار مهم IDS برنامه اي است كه به سرور آناليز كننده گزارش مي دهد ، DIDS(Database IDS) و داراي ابزار آناليز پيچيده تري است كه حملات غير متمركز را نيز شناسايي مي كند. دليل ديگري كه وجود دارد مربوط به قابليت حمل و انتقال درچند منطقه فيزيكي است .علاوه بر اين عامل جايگزين مشخص براي تشخيص و شناسايي اثر حمله هاي شناخته شده مي باشد .

يك راه حل ساختاري چند برنامه اي كه در سال 1994 ايجاد شد AAFIDيا Autonomous Agent for Intrusion Detection است. (شكل 5). اين ساختار از يك جايگزين استفاده مي كند كه بخش به خصوصي از رفتار سيستم را در زمان خاص ديده باني مي كند . بطور مثال يك جايگزين مي تواند تعداد دفعاتي را كه به سيستم Telnet شده تشخيص داده و در صورتي كه اين عدد منطقي به نظر نرسد آنرا گزارش كند. يك جايگزين همچنين قابليت ايجاد زنگ خطر در زمان وقوع يك حادثه مشكوك را دارد . جايگزين ها مي

توانند مشابه سازي شوند و به سيستم ديگر منتقل گردند. به غير از جايگزين ها ، سيستم مي تواند رابط هايي براي ديده باني كل فعاليتهاي يك كامپيوتر بخصوص داشته باشد. اين رابط ها هميشه نتايج عمليات خود را به يك مونيتور مشخص ارسال مي كنند. سيستم هاي مانيتور اطلاعات را از نقاط مختلف و مشخص شبكه دريافت مي كنند و اين بدين معني است كه مي توانند اطلاعات غير متمركز را بهم ارتباط دهند و نتيجه گيري نهايي را انجام دهند.به انضمام اينكه ممكن است فيلتر هايي گذاشته شود تا داده هاي توليد شده را بصورت انتخابي در يافت نمايد.





یک مثال یک واقعیت !

دانشگاه ايالتي آركانزاس براي مشكلي تقاضاي ياري مي‌كند. دانشگاه در نيمه كار ارتقا شبكه اصلي خود با ظرفيت چند گيگابيت جهت ارائه خدمات شبكه‌اي به هر اتاق خوابگاه و دفتر دانشكده مي‌باشد. از نظر Grey Williamson مسئول روابط سرويسهاي اطلاع‌رساني و تكنولوژي دانشگاه Ark در Jonesboro ساختن چنين شبكه‌اي مثل يك زمين‌بازي فريبنده براي هر هكر خواهد بود كه تبديل به جولانگاهي براي آنها خواهد شد.

شبکه IDS - سیستم آشکارکننده متجاوز

(Intrusion Detection System) - شركت Cisco Systems مشكل Williamson را حل خواهد كرد. زمانيكه شبكه با ويروسي مواجه مي‌شود و يا مورد حمله يك هكر قرار مي‌گيرد، IDS مديريت مركزي را از آن مطلع مي‌سازد. اگر عمليات خراب‌سازي خيلي جدي باشد، سيستم بصورت اتوماتيك كاربران IT را چك كرده و

دسترسي كسي را كه احتمال مي‌دهد از جانب آن، اين مشكلات پديد آمده باشد قطع مي‌نمايد و حتي توانايي شناسايي اتاقي را كه هكر در خوابگاه از آنجا وارد شبكه شده است را نيز دارد و سپس سيستم امنيتي دانشكده را از اين خرابكاري مطلع مي‌سازد.

بسياري از سازمانها، شبيه دانشگاه ايالتي آركانزاس به دنبال چنين سيستمهايي مي‌گردند. چرا كه سياستهاي شناسايي و تعيين هويت كاربران و نرم‌افزارهاي ضدويروس براي امنيت شبكه كافي نمي‌باشند.
فعاليت شركتهايي چون Cisco Systems، EnteraSys Networks، Internet Security Systems در اين زمينه نشان از رشد بازار تكنولوژي آشكارسازي متجاوز دارد. شركتهاي جديدي كه در اين زمينه شروع به فعاليت كرده‌اند عبارتند از IntruVert، One Secure و Resource Technologies (Resource به تازگي توسط شركت Symantec خريداري شده است) و حتي IDSهايي از طرف منابع آزاد چون Snort نيز معرفي شده‌اند.
در ساده‌ترين حالت سيستم آشكاركننده متجاوز، وضعيت امنيتي كار كاربران را شناسايي نموده و آن را ثبت مي‌كند. مثلا اگر كسي در حال اسكن كردن پورت‌هاي سرور و يا تلاش براي log in شدن به شبكه با استفاده از اسم رمزي تصادفي باشد، را شناسايي مي‌كند. البته آن جايگزين كليه موارد امنيتي شبكه نمي‌باشد. به گفته Stuart McClure مدير آموزشي و مشاوره امنيتي Foundstone در كاليفرنيا و Misson Viejo، IDS مشابه يك دوربين ويديويي كه در بانك و يا يك فروشگاه بكار گرفته مي‌شود، مي‌باشد.
چنين دوربين ويديويي جايگزين سيستم امنيتي و يا قفل درها نمي‌باشد، اما اگر كسي كار خلافي انجام دهد و به نحوي از سيستم امنيتي بكار گرفته شده عبور نمايد، دوربين از آن يك ركورد تهيه كرده كه در شناسايي مجرم و يا رفع اشكال سيستم امنيتي بكار رفته

مي‌تواند موثر باشد.
سيستمهاي آشكار كننده متجاوز به چند روش كار مي‌كنند.
IDS مبتني بر شبكه شامل سنسورهايي مي‌باشد كه پكتها (Packet) را ضمن عبور از شبكه نظارت مي‌كند. بطور نمونه يك IDS مبتني بر شبكه سنسورهايي را در نقاط ورود به شبكه (براي مثال در كنار فايروالها) يا در مرز بين زير شبكه‌ها با سطوح امنيتي مختلف (مثلا بين شبكه LAN و مركز ديتا) قرار مي‌دهد.
IDS مبتني بر ميزبان (Host-based) با شفافيت و وضوح فعاليت بر روي سرورهاي خاص را بررسي مي‌كند. ميزبانهاي main frame به دنبال فايلهاي بحراني مي‌گردند و حتي سيستم عاملهاي خاصي را بررسي مي‌كنند (مثلا به دنبال پيامهاي خطاي مشكوك و يا پردازشهاي غيرمتعارف سرور مي‌گردند.)
IDS مبتني بر ميزبان و شبكه (Network & host Based) مشابه اسكنر ويروس به اسكن كردن امضاها پرداخته و به دنبال نشانه‌هايي كه حاكي از انواع حمله‌ها مي‌باشند مي‌گردد. ضعف چنين سيستم‌هايي آن است كه امضاها بايد مرتبا و با توجه به پيشرفت تكنيك‌هايي كه هكرها بكار مي‌برند، به هنگام شوند. براي پيدا كردن اين خرابكاري‌ها، بعضي از سيستم‌هاي آشكار كننده متجاوز به دنبال هرگونه فعاليت شبكه‌اي خارج از حيطه تعريف شده فعاليتهاي مجاز مي‌گردند. اين نوع عملكرد به عنوان آشكارسازي چيزهاي غيرمعمول شناخته شده است.
مشكل تمام سيستمهاي آشكار كننده متجاوز آن است كه Plug & Play نبوده و احتمالا در آينده نيز نخواهند بود. برخلاف فايروالها، اغلب سيستمهاي آشكار كننده متجاوز، براي نصب و راه‌اندازي به افراد متخصص و وارد به كار نياز دارند. مسئله مهمتر سيستم آلارم آنها جهت كنترل و مديريت شبكه مي‌باشد. هر IDS زمانيكه به فعاليت مشكوكي برخورد مي‌كند، هشداري را توليد مي‌نمايد. از آنجائيكه شبكه‌ها يكسان نمي‌باشند. كامپيوترها در بيان اين شبكه‌ها

نمي‌توانند به خوبي عمل نمايند. مثلا كامپيوتر نمي‌تواند بين يك فايل ويروسي با عنوان "I Love You" و يك پيام email با همين موضوع تفاوت قائل شود. به عنوان نتيجه مي‌توان گفت كه اغلب سيستمهاي آشكار كننده متجاوز مرتبا پيام هشدار مي‌فرستند و در نتيجه پيامهاي خطاي زيادي، شايد بيش از هزاران پيام خطا در روز و در زمينه‌هاي مختلف توليد مي‌شوند.

Lioyd Hession سرپرست بخش امنيتي Radianz، در شهر نيويورك كه فراهم كننده سرويسهاي شبكه IP براي صنايع مالي است مي‌گويد: "هر فروشنده‌اي براي نمايش كار محصولات خود روشي دارد". به گفته Hession: "مديران موفق IT با توده انبوهي از اضافه بار اطلاعاتي مواجه شده‌اند. هر كدام از اين هشدارها با ارزش مي‌باشند و مسئول امنيتي شبكه مجبور به ارزيابي آن به منظور تعيين اينكه آيا استفاده از آن قانوني و يا يك حمله غيرقانوني مي‌باشد، است.

به علاوه مسئول رسيدگي و كنترل IDS بايد نحوه تشخيص حمله‌هاي واقعي از هشدارهاي خطا را بياموزند و آنها بايد نحوه تنظيم IDS به منظور كاهش هشدارهاي خطا را نيز ياد بگيرند.

Williamson از دانشگاه ايالتي آركانزاس مي‌گويد: "كارمندانش در روز 30 الي 40 پيام خطا را كه توسط IDS شبكه توليد مي‌شد، دريافت مي‌كردند. بعد از اينكه سيستم براي چند ماهي استفاده شد تعداد پيامهاي خطا به 2 الي 3 اشتباه در روز رسيد.

Michael Rusmussen مدير پژوهشي امنيت اطلاعات در Mass Based Giga كمبريج مي‌گويد: "شايد شش ماه طول بكشد تا تمام پيامهاي خطايي را كه IDS توليد مي‌نمايد، برطرف كنيد.

## اهداف فروشندگان ای دی اس

فروشندگان IDS بيكار ننشسته‌اند. شركتهاي IDS جديد همچون One Secure و Intruvert به منظور افزايش هوشياري

سيستمهايشان از تكنيكهاي آشكار كننده متجاوز بر پايه امضا و حالتهاي غيرعادي با هم استفاده مي‌كنند و حتي زمانيكه حمله‌اي اتفاق مي‌افتد، به جاي اينكه از سيستم ساده هشداردهنده استفاده نمايند آن را مسدود مي‌كنند. ساير فروشندگان مانند ForeScout از آناليزهاي آماري ترافيك عادي شبكه خود براي شناسايي اتوماتيك پاكتهاي غيرعادي كه در واقع يك نوع IDS خود تنظيم مي‌باشد، استفاده مي‌كنند.

بعضي ديگر از فروشندگان، مانند Tipping Point Technologies و Source Fire به كمك استفاده از سخت‌افزار به رفع اين مشكل پرداخته‌اند. آنها اقدام به ساخت تجهيزات IDS بهينه شده بسيار سريع كرده‌اند كه مي‌توانند ترافيك شبكه را در سرعتهاي بالاتر از سرورهاي متعارفي كه نرم‌افزار IDS را اجرا مي‌كنند، آناليز نمايند. (اين سيستمها از الگوريتم‌هاي آشكارسازي امضا بسيار پيچيده‌تري استفاده مي‌كنند). در نهايت گردانندگان بازار، چون ISS و سيسكو اميد به ارائه محصولات بهتر يا ارتقا مديريت و هوشياري سنسورهاي شبكه‌شان دارند.

يك عضو فني برجسته در CERT Coordination Center در دانشگاه Carnegie Meelon در Pittsburgh مي‌گويد: "من فكر نمي‌كنم سازمانها خواهان يك ريسك باشند و تنها به داشتن وسايل و ابزار اكتفا نمايند". "هميشه نقص ديدگاه‌هاي انساني و تجزيه و تحليل افراد متخصص در اين پروسه وجود دارد".

Bruce Larson طراح معماري سيستمهاي امنيتي شبكه براي SAIC Clients در چندين سازمان و شركت دولتي – نائب رئيس سيستم و مديرعامل اجرايي شبكه‌هاي اختصاصي براي SAIC Internatinal مي‌گويد: "آشكارسازي متجاوز واقعا كاري هزينه‌بر مي‌باشد". او برآورد مي‌كند كه شما حداقل به يك مهندس شبكه تمام وقت براي مونيتور كردن و تنظيم IDS با حقوق مكفي نياز داريد.

## يك راه چاره

مديريت اطلاعات خروجيهاي IDS به منظور ارائه سرويسهاي مديريت شده مي‌باشد، در اين رابطه شركت Counterpane Internet Security كارمنداني دارد كه تنها آلارم‌هاي IDS را چك كرده و هشدارهاي مهم را به مسئول IT خود مي‌فرستند.

## IDS چگونه كار مي‌كند؟(طبق گفته خودشان)

طبق اظهارات Jeff Wilson مدير اجرايي Infonetics و Sum Jose مشاور و پژوهشگر بازاريابي، چه با مديريت اطلاعات خروجي و چه بدون آن سيستمهاي آشكاركننده متجاوزگران مي‌باشند، با داشتن تجهيزاتي در حدود 15000 دلار يا كمي بيشتر مي‌توان يك سيستم مناسب داشت ولي يك سيستم بسيار كامل ممكن است در حدود 100000 دلار يا بيشتر درآيد. به علاوه بايد هزينه خدمات و پشتيباني فني و نصب و راه‌اندازي سيستم را هم اضافه كرد. اين يكي از دلايلي است كه هنوز بازار IDS نسبت به فايروالها بسيار كوچك مي‌باشد. دليل ديگر مديريت بسيار مشكل آنها مي‌باشد.

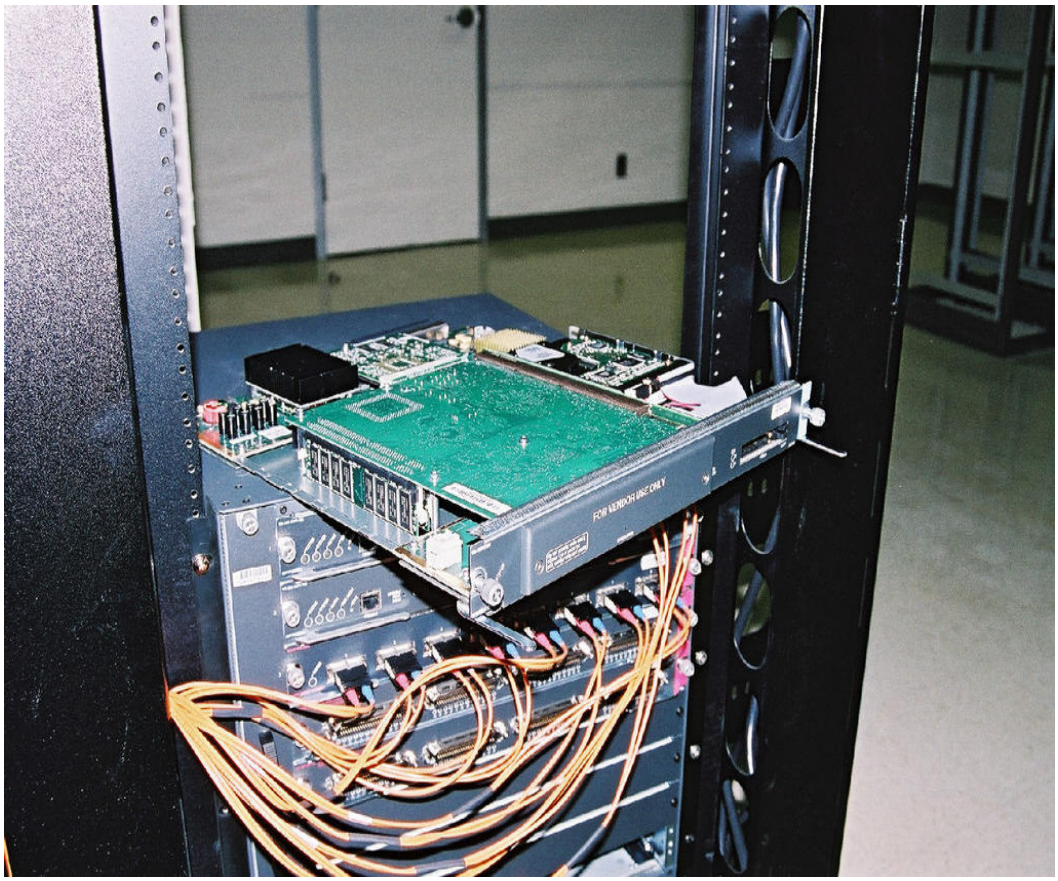
Jeff Wilson در اين زمينه مي‌گويد: "هنوز بازار IDS چندان رونقي ندارد و بايد از اطلاعات مختلفي بهره جست تا پي به ارزش آن بطور كامل برد".

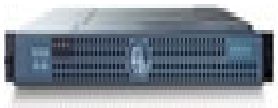
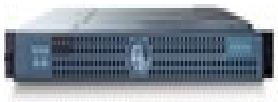
از سوي ديگر اگر شما چيز با ارزشي براي حفاظت داشته باشيد، چاره‌اي جز استفاده از IDS نخواهيد داشت. شركتها اغلب به تكنولوژي IDS براي معرفي شبكه خود، به عنوان يك شبكه مطمئن نياز دارند به ويژه در صنايع قانونمند كه تابع مقررات و ضوابط خاصي مي‌باشند. مثل سرويس‌هاي مالي و مراقبتهاي بهداشتي. GERT'S Allen مي‌گويد: "شما مجبور هستيد به كل عرضه و تقاضاي خود نگاه كنيد و ببينيد از چه چيزي مي‌خواهيد حفاظت كنيد، به چه چيزي نياز داريد و چه كار مي‌توانيد با آن انجام دهيد."

اما بكارگيري IDS راحت نيست. طبق اظهارات Rasmussen اغلب شركتهايي كه IDS را بكار گرفته‌اند از شروع كار خود مطمئن هستند اما فقط يك چهارم آنها شانس موفقيت دارند و شايد يك دهم واقعا موفق مي‌شوند.
به عبارت ديگر IDS شما يكي از ابزارهاي امنيتي شبكه مي‌باشد. بكارگيري سطوح مختلف امنيتي در يك سيستم بسيار مفيد مي‌باشد كه توسط بسياري از ارگان‌هاي امنيتي توصيه مي‌گردد. Allen پيشنهاد مي‌دهد كه براي يك IT اجرايي از تكنيكهاي امنيتي زير بايد استفاده كرد: "سنسورهاي آشكاركننده متجاوز برپايه شبكه، آشكاركننده، متجاوز برپايه Host، گزارش‌گيري مركزي، كنسول مونيتورينگ براي هشدارهاي IDS و ساير پيام‌هاي شبكه، فايروالها و فايلهاي ثبت وقايع و روشهاي متداول در به رسميت شناختن كاربر.
هدف، پردازش مناسب براساس داده توليد شده توسط IDS به منظور مديريت و كنترل شبكه مي‌باشد. Foundstone’s McClure مي‌گويد: "IDS تنها از ديد مردم عادي كه به آن نگاه مي‌كنند، خوب مي‌باشد". اگر شما قصد مونيتورينگ آن را نداريد مي‌توانيد يك doorstop 50000 دلاري بخريد. Rasmussen توصيه مي‌كند كه پيادەسازي IDS بايد با پردازش‌هاي واضح براي پاسخ به آلارمها، خطمشي‌هاي نگەداري شبكه (مثل به هنگام كردن امضا و اصلاحيه‌هاي سيستم عامل) و آموزشهاي پيوسته كارمندان بخش امنيت شبكه همراه باشد.
همچنين Rasmussen به شروع با حجم كوچك، با يك يا دو سنسور IDS در نقاط حساس شبكه توصيه مي‌كند. بايد به حدي كوچك باشد كه بتوان آن را كنترل نموده و مهندسين شبكه زمان كافي براي ياد گرفتن سيستم و تنظيم آن بدون مواجه شدن با هزاران آلارم را داشته باشند.
Williamson زمان تست IDS در دانشگاه ايالتي آركانزاس را در نيمه بهار زمانيكه ترافيك شبكه پايين مي‌باشد انتخاب كرده است تا

مهندسين بتوانند در يك فرصت چند ماهه تا بازگشايي كلاس‌ها در پاييز كاملا كار با سيستم را بياموزند. مي‌توان آن را براي جستجوي تقريبا هر نوع استفاده غيرمجاز از شبكه مثل نرم‌افزار مبادله فايلهاي ممنوعه تنظيم نمود.
اگر شما بخواهيد مي‌توانيد تقريبا هر چيزي را ببنديد. در واقع IDS مانند لنز قويي است كه از شبكه مواظبت كرده و مشكلات آن را پيدا مي‌كند.

در اینجا شما را با چند ای دس اس آشنا میکنیم

| IDS-4210 | IDS-4235 | IDS-4250 |
| --- | --- | --- |
|   |   |   |
| **IDS-4210-K9** 45Mbps Sensor<br>( 10Base*f*l*f*b*f*g*f*  [*f*N—p )<br> | **IDS-4235-K9** 200Mbps Sensor<br>( 10/100/1000BaseT w/RJ-45 )<br> | **IDS-4250-SX-K9** 500Mbps Sensor<br> i 1000BaseSX w/SC connector <br> j<br>**IDS-4250-TX-K9** 500Mbps Sensor<br> i 10/100/1000BaseT w/RJ-45<br> j |

## IDS-4235

## ۲۰ قانون از کتاب ...

1.از افسوس و ترحّم بگریزید زیرا اینانند که " نیرومند " را از پای در می آورند.

۲.همواره توانایی خود را بیازمایید ، از آن بابت که دروغها موفق اند.

۳.شادی را در پیروزی بجویید - نه درصلح .

۴.ازیک استراحت کوتاه بیشتر ازیک خواب درازمدت لذت ببرید.

۵.یک " دروگر" باشید ، بدین سان دانه خواهید کاشت.

۶.هرگز به چیزی آن مقدارعشق نورزید که نتوانید شاهد مرگش باشید.

۷.بر روی ماسه چیزی نسازید ، بلکه بربلندای صخره - و برای امروز یا دیروز نسازید ، بلکه برای تمام زمان ها .

۸.همواره برای بیشتر تلاش کنید ، پیروزی پایانی ندارد .

۹.بمیرید بجای آنکه تسلیم شوید .

۱۰.یاد بگیرید روی پای خود بایستید ، پس درهمه حال پیروز خواهید بود.

۱۱.خون یک جاندار بهترین است از برای آبیاری دانه های یک زندگی جدید .

۱۲.آن کس که بربلندای " مرتفع ترین هرم ساخته شده ازجمجمه ها " ایستاده ، می تواند دورترین نقطه را ببیند.

۱۳.ازعشق دوری نکنید ولی با آن ، آنگونه رفتار کنید که با یک شیّاد رفتار می کنید - همواره منصف باشید.

۱۴.هرآن چیز که عظیم است برفرازاندوه بنا شده

۱۵.تنها بسمت جلو مبارزه نکنید ، درجهت ترقّی نیز بجنگید - ازبرای آنکه عظمت درآسمان ها بیارامد.

۱۶.مانند باد خنک نیرومندی باشید که آفرینش ها را درهم می شکند.

۱۷.بگذارید عشق زندگی یک هدف باشد امّا اجازه دهید بالاترین هدفتان " بزرگی وسربلندی " باشد.

۱۸.هیچ چیز زیبا نیست ، بجزانسان : ولی زن زیباترین درجهان است.

۱۹.دروغ ها و نیرنگ ها را از خود برانید این دو، مانع اند از برای انسانِ قدرتمند.

۲۰.آن چیز که نمی کشد ، قویترمیسازد.

**Author: Satanic Soulful**
**E-Mail: Satanic.Soulful@GMail.Com**
**Satanic_Soulful@Yahoo.Com**
**Developed In:Satanic Digital Network Security ™**
**Special TNX 2 :Hell Hacker – Mr.P Hacker – I loveu Mct Collector & X Hulk**
**Research By:5/-\t4N1C**

**For More Information Go to Http://Hack-er.cjb.net/**





Life & Girl Are Not Matter's

The End.