

IDS

Author: Satanic Soulful



©All Rights Reserved For Satanic Team

©All Rights Reserved For Persian Hacher 2005-2006



Satanic Hell

جهنم شیطانی

IϥS

مباحثی پیرامون ای دی اس

نویسنده: Satanic Souful

تاریخ: 14/1/1384

Contact:

Satanic.souful@GMail.Com

Satanic_Souful@Yahoo.Com

Special TNX2:

Hell Hacker – **B0rn2h4k** – Phacker_Ir – McT – X Hulk
& Dr. Hoshmand

ملاحظات:

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 شیطنانی هیچ گونه مسوولیتی نسبت به استفاده نادرست از این مقاله را بر عهده نمی گیرند!

استفاده از مطالب این مقاله با ذکر نام نویسنده و همچنین گروه های 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 پیچ 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 حفاظت 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 چیست؟

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 پورتهها ، 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 غيرمعارف 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 وقايع 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.

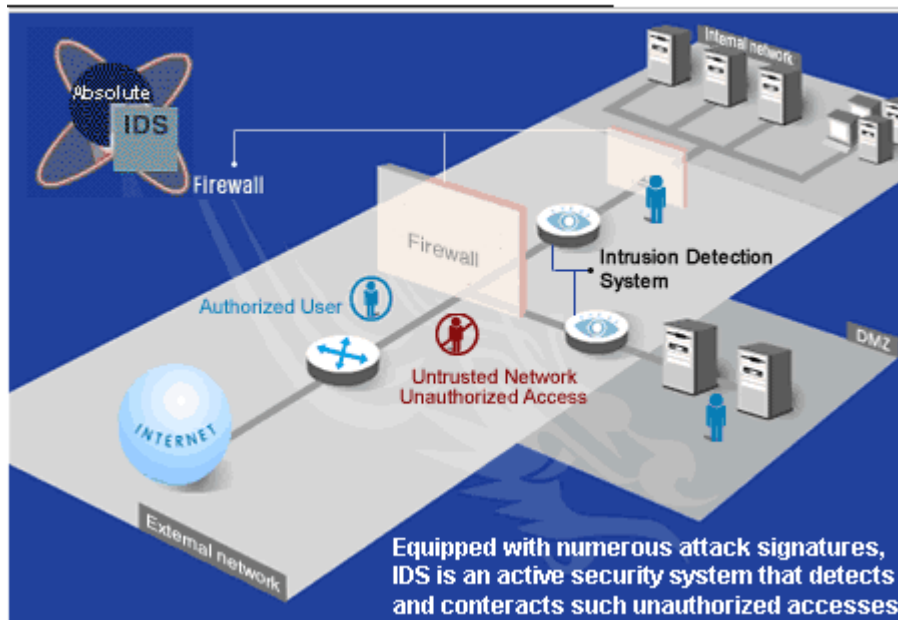
4- ديواره آتش (Firewall)

5- مكانيزمهاي امنيتي مانند SSL ، VPN و Radius و

تکنولوژی IDS

- 1 Plain Hand Work
- 2 Network Based
- 3 Host Based
- 4 Honey pot

Absolute IDS (Intrusion Detection System)



(Network Base) NIDS

گوش دادن به شبکه و جمع آوری اطلاعات از طریق 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.

(Host Base) HIDS

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 عملاً طوری تنظیم شده است که در معرض حمله قرار بگیرد. اگر یک پوششگری از NIDS ، HIDS و دیوار 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 خرابکاری ها برای امن کردن شبکه استفاده کرد. (در رابطه با ظرف عمل مقاله کاملی نوشته شود دانلود این مقاله از [اینجا](#))

چرا دیوار آتش به تنهایی کافی نیست ؟

به دلایل زیر دیوار آتش نمی تواند امنیت شبکه را به طور کامل تامین کند :

1. چون تمام دسترسی ها به اینترنت فقط از طریق دیوار آتش نیست.
2. تمام تهدیدات خارج از دیوار آتش نیستند.

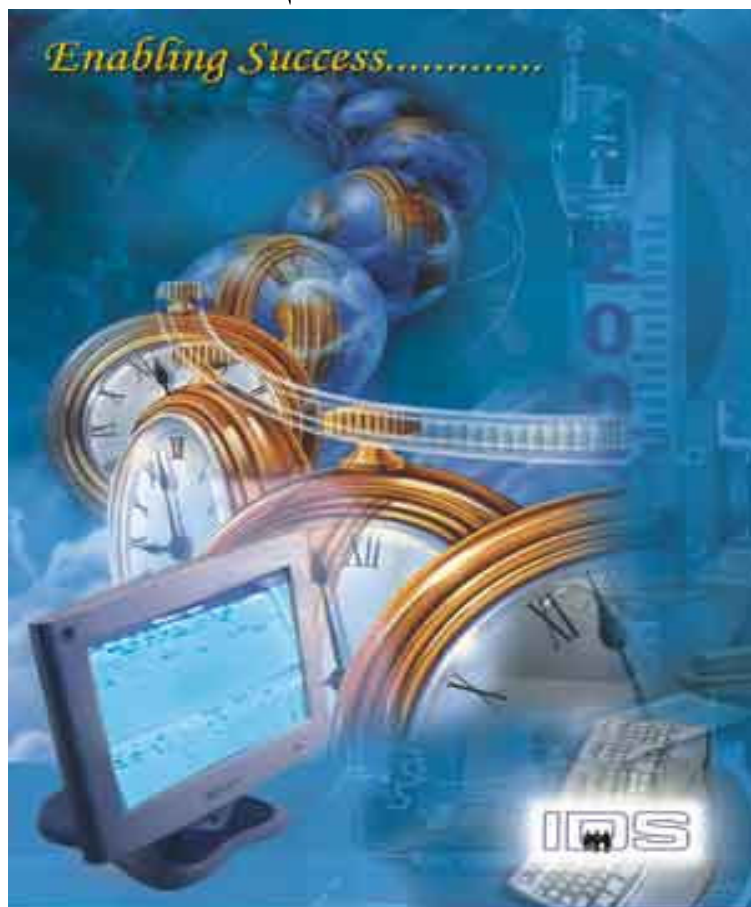
3. امنیت کمتر در برابر حملاتی که توسط نرم افزارها مختلف به اطلاعات و داده های سازمان می شود ، مانند Active ، Java ، Virus Programs ، Applet .

برای تامین امنیت يك شبکه، Firewall اولین چیزی است که بایستی پیاده سازی شود. نکته حائز اهمیت آنکه، نصب يك Firewall در شبکه به تنهایی امنیت آن شبکه را تامین نخواهد کرد!!!

فایروال معمولاً سیستمی است که با تعریف يك سری قوانین مشخص روی آن از ورود و یا خروج بسته های خاص جلوگیری می کند اما IDS بسته هایی را که از نظر فایروال اجازه عبور را دارند نیز کنترل نموده و در صورت تشخیص امکان نفوذ آنها را مسدود می نمایند برای توضیح بیشتر در نظر بگیرید که ما در برنامه فایروال خود قوانین را تعریف کرده ایم که امکان دسترسی کاربران اینترنت به پورت 80 رایانه سرور وب خود را داده و به کاربران شبکه محلی خودمان نیز امکان اتصال به پورت 80 رایانه های موجود در شبکه اینترنت را داده ایم . از نظر فایروال هر بسته خروجی که به مقصد پورت 80 سایر رایانه ها باشد مجوز عبور دارد در حالی که برای مثال ویروس code red از رایانه میزبان وب ما اتصالات زیادی به پورت 80 سایر رایانه ها برقرار ساخته و با اشغال کردن مسیر ارتباط باعث از کار افتادن سرور وب ما می گردد که این از نظر يك فایروال بدون اشکال می باشد اما سیستم IDS با بررسی بسته های ارتباطی و اطلاع از نوع عملکرد این تروجان پی می برد که این يك ویروس Red code بوده و عملیات آنرا متوقف می نماید IDS دارای يك بانک اطلاعاتی کامل راجع به تروجانها ، نوع عملکرد آنها ، ساختار بسته های آنها و پورتهای که معمولاً جهت اتصال استفاده می کنند می باشند که به سیستم این امکان را می دهد که از نفوذ به داخل سیستم جلوگیری نماید ضمناً معمولاً يك نفوذگر قبل از شروع به نفوذ جهت کسب اطلاعات از وضعیت امنیتی

سیستم ما اقدام به عملیاتی خاص می نماید که این از دید یک فایروال مخفی می ماند برای مثال اولین کاری که معمولاً نفوذگران انجام می دهند عملیات بررسی پورتها (Port scan) می باشد که جهت کسب اطلاعات راجع به پورتهای باز و بسته سیستم و اینکه اگر یک پورت باز است چه سرویسی روی سرور فعال شده می باشد از نظر فایروال یک سری اتصال به پورت های مختلف اتفاق افتاده که نسبت به قوانین تعریف شده در فایروال (باز بودن یا بسته بودن پورت) با آنها برخورد می شود اما از دید یک IDS اگر یک شخصی تعداد زیادی اتصال در مدتی کوتاه به پورتهای سیستم داشته باشد به عنوان یک نفوذگر که عملیات Port scan را انجام می دهد شناخته می شود و گزارش از عملکرد و همچنین موقعیت او و شناسه (IP) او به کار می دهد

مدیران شبکه با بررسی وضعیت گزارشهای نفوذ می توانند تدابیر خاص خود را در نظر گرفته و در صورت مشخص بودن موقعیت شخص نفوذگر نسبت به طی مراحل قانونی جهت جلوگیری از نفوذ های بعدی و احیاناً جبران خسارت اقدام کنند.



برای تشخیص خطرات و حملات احتمالی می بایست سیستم خود را در برابر تقاضاهایی که سرویس های نامناسب درخواست می کنند مورد بررسی قرار دهید. این بررسی ها در تشخیص حملات واقعی به ما کمک می کند. با توجه به انواع راه هایی که نفوذگران برای دسترسی به سیستمها استفاده می کنند نگاهی اجمالی به روشهای آسیب رسانی و نفوذ می اندازیم.

استفاده از آسیب پذیری های معروف:

در اکثر موارد حمله به معنی تلاش برای استفاده از نقص یا ایجاد آن در سیستم امنیتی يك سازمان اطلاق می شود و این یکی از راههای نفوذگری در شبکه می باشد.

اغلب خود سازمان ممکن است از ابزاری برای امن کردن شبکه استفاده کند که کار حمله کننده را آسان می سازد به بیان واضح تر اینکه ابزارهای امنیتی نیز خود دارای نواقص و حفره های امنیتی می باشد که اختیارات بیشتری را به نفوذگر می دهد. این نرم افزارها اغلب مانند شمشیر دو لبه عمل می کنند و مورد استفاده هردو گروه کاربران و حمله کنندگان قرار می گیرد مانند نرم افزارهای کنترل صحت و یکپارچگی فایل یا نرم افزارهایی که جهت تست آسیب پذیری شبکه مورد استفاده قرار می گیرند.

چک کردن یکپارچگی فایلها با استفاده از روش های سیستمی و با قابلیت ادغام روشهای مختلف با یکدیگر و با ابزارهایی نظیر anti-SATAN یا Courtney امکان پذیر می باشد.

ترافیک خروجی غیر معمول:

يك نفوذگر با استفاده از تعداد زیادی Exploit و حتی نفوذ های ناموفق سعی در به دست آوردن کنترل کامپیوتر مقصد دارد. این عملیات نفوذگرانه، ترافیک معمول شبکه را افزایش می دهد و نشانه

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

حد تکرار برای کمک به تشخيص فعاليتهاي واقعي و مشكوك :

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

زمان بين تکرار فعاليتها:

پارامترها براي تشخيص زمان سپري شده بين دو واقعه متوالي. مثلاً" وقتي بخواهيد با نام کاربري 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 که در يك Session ايجاد مي شود. پروتکل ها وسرويس هاي شبکه به صورت کاملاً" دقيقي مستند شده اند و از ابزارهاي نرم افزاري خاص استفاده مي کنند. هرگونه ناهماهنگي با قالب شناخته شده(مثل اشتباه در تايپ يك دستور) ممکن است اطلاعاتي براي شناسايي سرويسهاي که مي توانند مورد حمله يك نفوذگر قرار بگيرند باشد.

اگر امکان Audit در سیستم فعال شده باشد، مثل Send Mail Relaying، توالی ارتباط Log بصورت معمولی و قابل پیش بینی اتفاق می افتد. هرچند که اگر در Log دریافت شده دستورات غیر مجاز دیده شود ممکن است نتیجه موارد اشتباه غیر عمدی و یا سعی در Spoofing باشد. (Spoofing به این معنی است که نفوذگر آدرس خود را به آدرسی که برای سیستم شناخته شده است تغییر داده و به این ترتیب به سیستم نفوذ می کند.)

تست تلاشهای مخرب ممکن است شامل موارد زیر باشد:

- شناسایی تلاشهای متعدد برای جبران خطاهای تایپی و تکرار دستورات
- تشخیص خطاهای مکرر برای یافتن پروتکل ها که بدنبال يك تلاش موفق انجام می شود.
- تشخیص خطا و یادگیری در جهت شناسایی نرم افزارهای و یا سیستم عامل های موجود در سایت مقصد.

ناهماهنگی در جهت ارسال و دریافت اطلاعات

هرگونه ناهماهنگی ترافیکی در Packet ها یا يك Session نشانه ای از يك حمله پنهانی است. بررسی آدرس مبدا و مقصد (به صورت ورودی یا خروجی) میتواند جهت Packet را تشخیص بدهد. روند برقراری يك session با تشخیص اولین پیام ارسال شده شناسایی می شود. يك درخواست برای دریافت يك سرویس از شبکه محلی به صورت يك session ورودی است و پروسه فعال کردن يك سرویس بر پایه Web از يك شبکه محلی يك session خروجی است.

موارد زیر می تواند به عنوان حمله محسوب شود:

- Packet هایی که منشاء آنها اینترنت است بدون اینکه در خواستی از سمت شبکه محلی داشته باشد و وارد شبکه شود.

این حالت ممکن است نشان دهنده يك حمله IP Spoofing از خارج باشد. این مشکلات می توانند در Router هایی که قابلیت مقایسه آدرس مبدا و مقصد را دارند بر طرف شوند. در عمل تعداد اندکی از Router ها در شبکه می توانند به عنوان فایروال عمل کنند.

- بر عکس حالت قبل Packet هایی که به صورت خروجی در يك شبکه محلی ایجاد می شوند و به يك شبکه خارجی فرستاده می شوند

- Packet ها با پورت های مبدا و مقصد غیر مشخص. اگر منبع پورت در مورد يك درخواست ورود یا خروج اطلاعات با نوع سرویس یکسان نباشد ممکن است به عنوان يك تلاش برای نفوذ یا پوشش سیستم تلقی شود. بطور مثال در خواست Telnet از روی پورت 100 در محیطی که انتظار چنین پشتیبانی برای سرویس وجود ندارد. (در رابطه با تلنت نیز مقاله جامعی موجود میباشد متوانید از [اینجا](#) دریافت کنید)

ترافیک غیر معمول بیشتر توسط فایروال شناسایی شده و Packet های مشکوک را از بین می برد. با توجه به اینکه فایروالها همیشه با سیستم های تشخیص نفوذ ادغام نمی شوند ، بنابراین ممکن است که سیستمهای تشخیص نفوذ راه حلی برای این مشکل باشد.

علائم نفوذ

معمولا با اجرای برنامه های خاص در سیستم انتظار مواجهه با رفتارهای خاص و مشابه وجود دارد

بعضی از موارد مانند موارد زیر :

مشخصات تاریخ و زمان :

در بعضی محیط های خاص بطور معمول بعضی رفتارها در زمان خاصی در شبکه اتفاق می افتد. مثلاً فرض کنید بطور معمول شنبه صبح یکسری اطلاعات به بخش مرکزی شرکت ارسال می شود که مربوط به اطلاعات مالی است. چنین ترافیکی در شنبه صبح همیشه اتفاق می افتد و عادی است در صورتیکه چنین ترافیکی روز جمعه اتفاق بیفتد و ثبت شود ، غیر معمول است و باید به عنوان یک رفتار غیر معمول یا نفوذ به سیستم مورد بررسی دقیق قرار گیرد.

مشخصات منابع سیستم:

بعضی نفوذ های خاص باعث خرابی بعضی پارامترهای خاص سیستم میشود مثلاً یک حمله Brute Force برای شکستن حرف رمز باعث در گیر کردن CPU میشود در حالیکه یک حمله DoS همین کار را با سرویس های سیستم انجام میدهد. استفاده سنگین از منابع سیستم (پروسور، حافظه، دیسک سخت ، سرویسها و اتصالات شبکه) که در زمانهای غیر معمول اتفاق می افتد برای شناسایی حمله بسیار مفید هستند و باید به آنها بسیار توجه کرد.

Packet هایی با تایید های TCP غیر معمول :

اگر در یک Packet نشانه مربوط به ACK فعال باشد و قبل از آن هیچ SYN-Packet ارسال نشده باشد، ممکن است نتیجه یک حمله در سیستم باشد همچنین این حالت ممکن است اثر یک Packet خراب هم باشد که در یک شبکه با نرم افزار های خراب ایجاد می شود و واقعا " حمله نفوذی نباشد.

سرویس های مختلف با علایم مختلف :

ممکن است در بعضی موارد انتظار ایجاد ترافیک خاص از یک کاربر مشخص داشته باشیم مثلاً کاربری که در یک ماموریت اداری

بسر مي برد معمولاً " فقط نامه هاي خود را چك مي كند و يا 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 افزار سيستم مثل خاموش شدن بدون علت سرور ، عدم كار كرد بعضي برنامه هاي نرم افزاري مانند IIS ، موارد غير معمول restart شدن سيستم ها ، تغييرات در تنظيم clock سيستم

2- بروز اشكالات 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 مثلاً " در Router ها يا سرويس هاي سيستم مثل كند شدن سرور

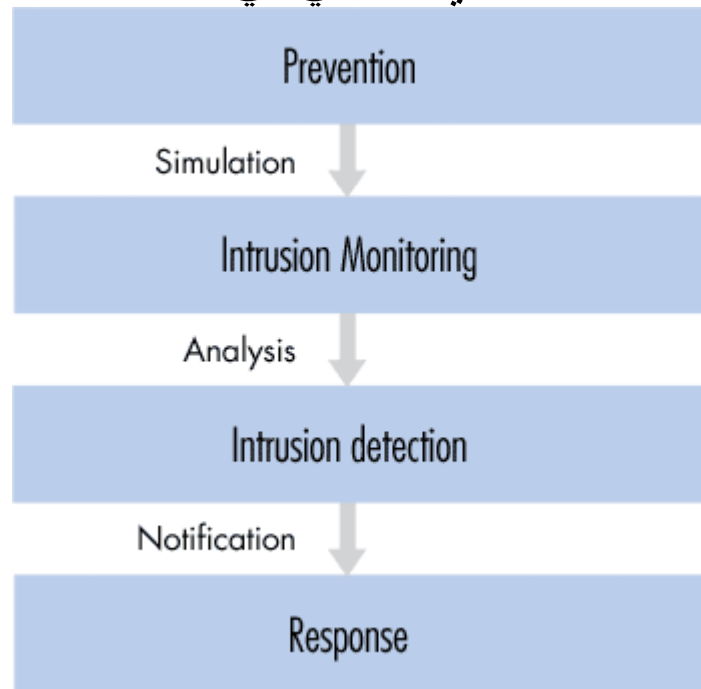
5- بروز رفتارهاي مشكوك در اجراي برنامه هاي كاربر مثل اشكال در دسترسي به بعضي منابع شبكه

6- عملکرد مشکوک در فایل‌های ثبت وقایع (Log ها) بررسی این فایل ها از نظر سایز برای اینکه حجم فایل از اندازه متعارف خیلی بیشتر یا کمتر نباشد. مگر اینکه مدیر شبکه خود چنین تغییری ایجاد کرده باشد.



مهمترین کار يك سیستم کشف نفوذگر، دفاع از کامپیوتر بوسیله شناسایی حمله و جلوگیری از آن است. شناسایی حمله هکر بستگی به نوع و تعداد عکس العمل مورد نظر دارد. (شکل 1)
مقابله با نفوذ، نیاز به يك سیستم ترکیبی دام گذاری و تله اندازی دارد که هر دو این پروسه ها باید با بررسی و دقت انجام شود. از کارهای دیگری که باید انجام داد ، تغییر دادن جهت توجه هکر است.

هر دو سیستم واقعی و مجازی (Honey-pot) به دام اندازی هکر به طور دائمی دیده بانی (Monitor) می شوند و داده های تولید شده توسط سیستم شناسایی نفوذگر (IDS) برای شناسایی نحوه عملکرد حمله به دقت بررسی می شود که این مهمترین وظیفه یک IDS جهت شناسایی حملات و یا نفوذهای احتمالی می باشد.



(شکل 1)



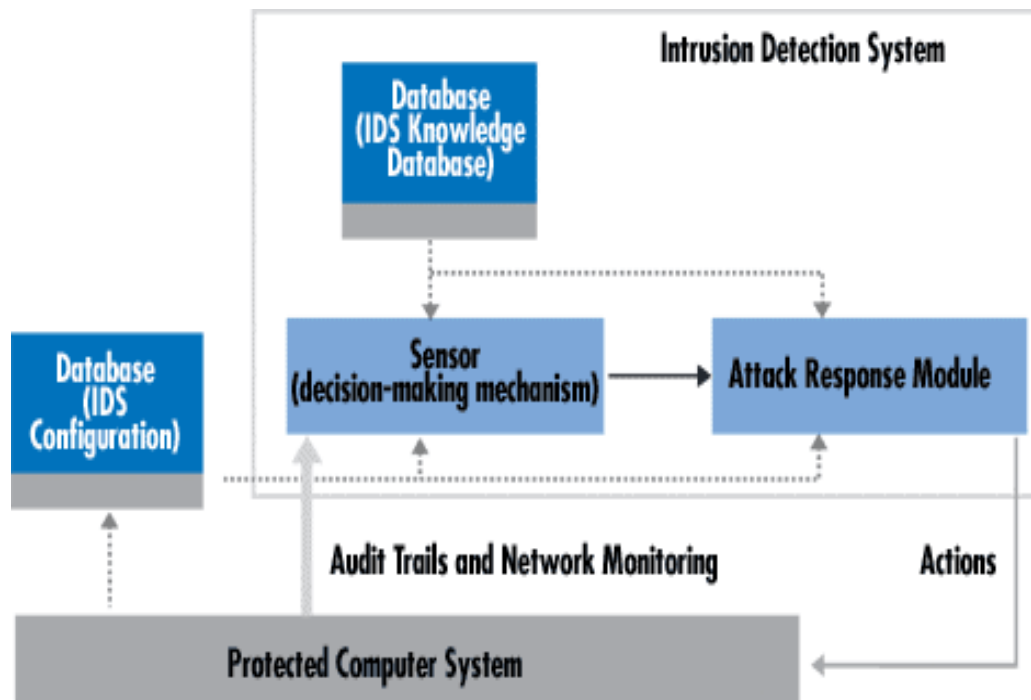
(شکل 2)

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

در بين وظائف 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 و يا يك منبع شبکه جلوگیری كرد. شناسايي نفوذ ممكن است گاهي اوقات زنگ خطر اشتباهي را به صدا در آورد. براي مثال نتيجه خراب كار كردن يك كارت شبکه و يا ارسال شرح يك حمله و يا اثر يك نفوذ از طريق Email.

ساختار و معماری سیستم تشخیص نفوذ:

سیستم تشخیص نفوذ يك هسته مركزي دارد و يك تشخیص دهنده (موتور تشخیص) است كه مسئولیت تشخیص نفوذ را دارد. اين سنسور يك مكانيزم تصميم گيري بر اساس نوع نفوذ دارد.



(شکل 3)

این سنسور اطلاعات خام را از سه منبع دریافت می کند.

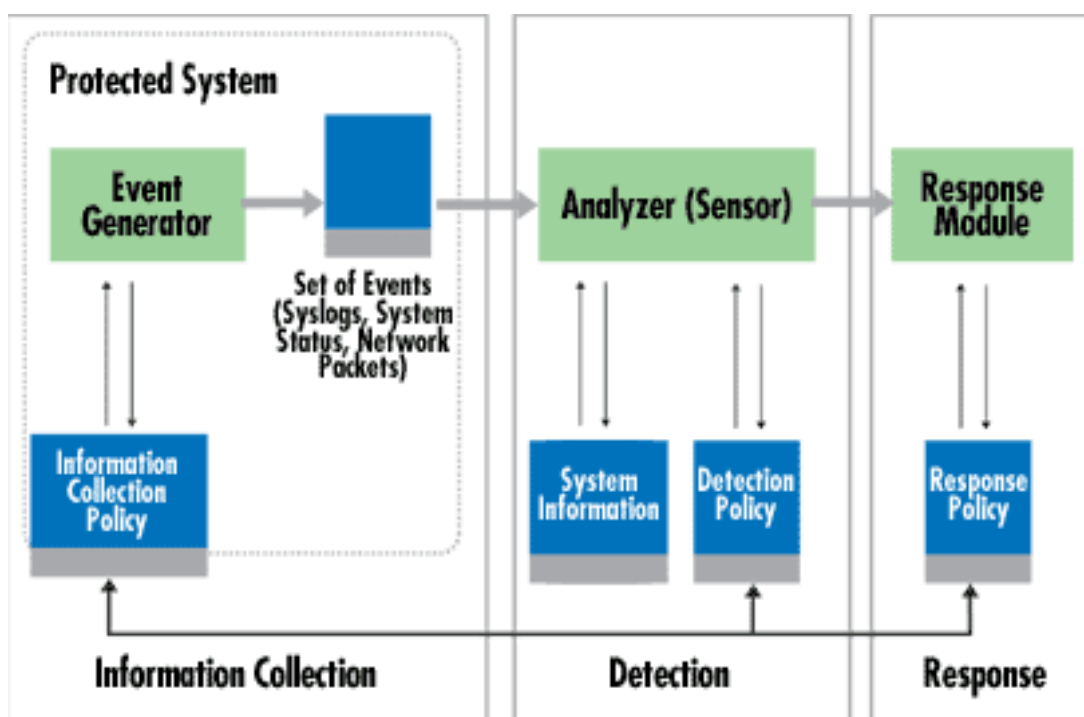
- 1- از اطلاعات موجود در بانک اطلاعاتی خود IDS .
- 2- فایل ثبت وقایع سیستم (syslog).
- 3- آثار ترافیک عبوری و دیده بانی شبکه .

فایل ثبت وقایع سیستم (syslog) ممکن است به طور مثال اطلاعات پیکربندی سیستم و دسترسی های کاربران باشد. این اطلاعات اساس تصمیم گیری های بعدی مکانیزم سنسور خواهد بود.

این سنسور با یک Event Generator که مسئول جمع آوری اطلاعات است با هم کار می کنند. (شکل 4) . قوانین جمع آوری اطلاعات که بوسیله سیاست های Event generator مشخص می شود ، تعیین کننده نوع فیلترینگ از روی حوادث و اطلاعات ثبت شده است.

Event Generator ، مثل سیستم عامل یا شبکه یا یک برنامه اجرایی ، تولید کننده Policy هایی هستند که ممکن است یک واقعه

ایجاد شده در سیستم عامل یا Packet های شبکه را ثبت کنند. این مجموعه به همراه اطلاعات Policy می تواند در یک سیستم محافظت شده یا خارج از شبکه قرار داده شود. در بعضی شرایط خاص هیچ محل مشخصی به عنوان محل حفظ اطلاعات ایجاد نمی شود مثل وقتی که اطلاعات جمع آوری شده از وقایع مستقیماً به یک سیستم آنالیز ارسال می شود.



(شکل 4)

وظیفه سنسور فیلتر کردن اطلاعات است و حذف کردن هر داده غیر مرتبط که از طرف منابع دریافت اطلاعات می رسد. تحلیل کننده برای دستیابی به این هدف از Policy های موجود استفاده می کند. تحلیل گر نکاتی مانند اثر و نتیجه حمله ، پرو فایل رفتارهای نرمال و صحیح و پارامترهای مورد نیاز مثل Threshold ها را بررسی می کند. علاوه بر همه اینها بانک اطلاعاتی که پارامترهای پیکربندی IDS را در خود نگه می دارد، روشهای مختلف ارتباطی

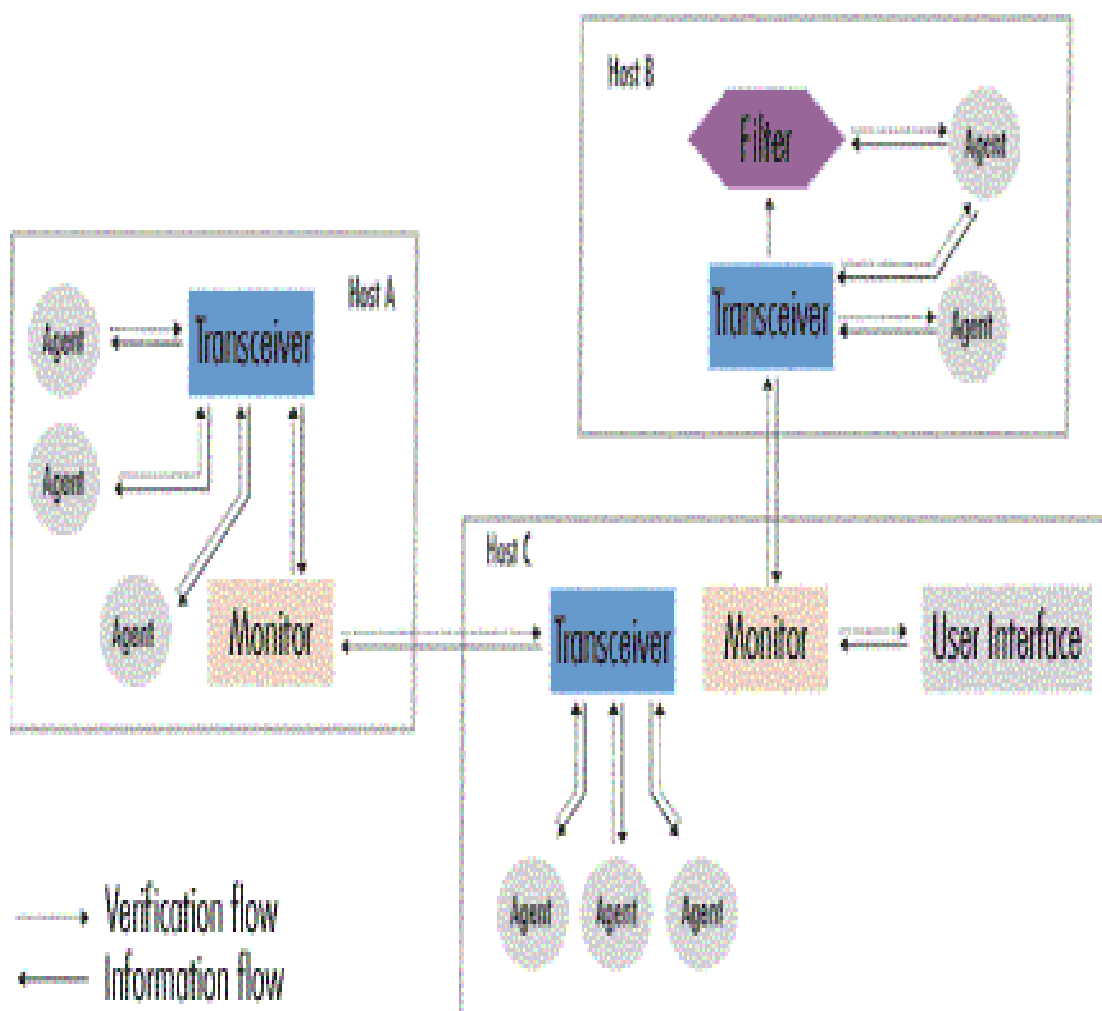
را ایجاد می کنند. سنسور یا گیرنده هم بانک اطلاعاتی خاص خود را دارد، که شامل تاریخچه پویایی از نفوذهای پیچیده بوده یا با توجه به تعداد حمله مورد تحلیل قرار گرفته است.

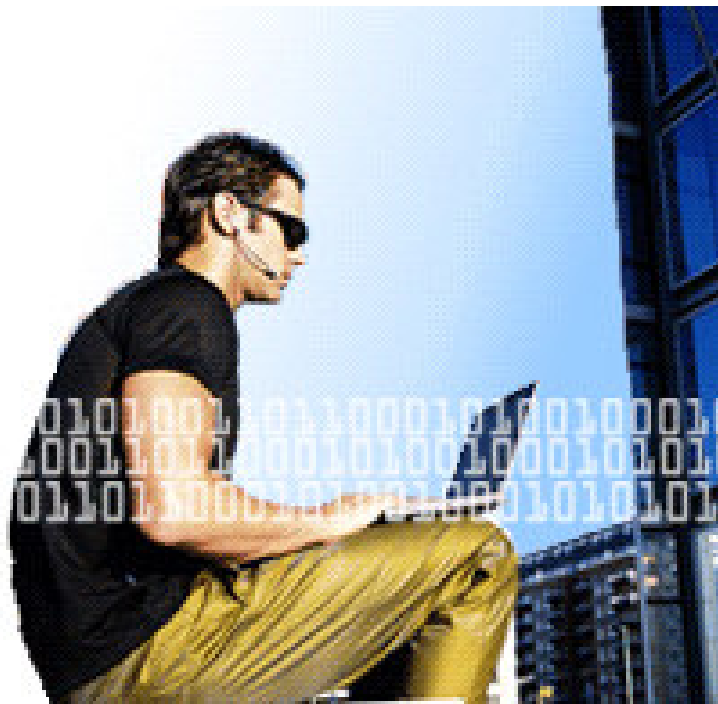
سیستم تشخیص نفوذ می تواند به صورت متمرکز مثل برقراری یک فایروال فیزیکی یا به صورت غیر متمرکز انجام شود. یک IDS غیر متمرکز شامل تعداد زیادی سیستم تشخیص نفوذ در یک شبکه بزرگ است که هر کدام از آنها با هم در ارتباط هستند. سیستم های پیچیده تر از ساختاری پیرو می کنند که مازول های مشابه برنامه های خود اجرایی دارند که روی هر کامپیوتر اجرا می شوند. عملکرد این سیستم جایگزین، مونیتر و فیلتر کردن تمام فعالیت های مرتبط با یک بخش محافظت شده است که بتواند یک آنالیز دقیق و پاسخ متناسب از شبکه دریافت کند.

یکی از قسمت های بسیار مهم IDS برنامه ای است که به سرور آنالیز کننده گزارش می دهد، (DIDS(Database IDS) و دارای ابزار آنالیز پیچیده تری است که حملات غیر متمرکز را نیز شناسایی می کند. دلیل دیگری که وجود دارد مربوط به قابلیت حمل و انتقال در چند منطقه فیزیکی است. علاوه بر این عامل جایگزین مشخص برای تشخیص و شناسایی اثر حمله های شناخته شده می باشد.

یک راه حل ساختاری چند برنامه ای که در سال 1994 ایجاد شد AAFID یا Autonomous Agent for Intrusion Detection است. (شکل 5). این ساختار از یک جایگزین استفاده می کند که بخش به خصوصی از رفتار سیستم را در زمان خاص دیده بانی می کند. بطور مثال یک جایگزین می تواند تعداد دفعاتی را که به سیستم Telnet شده تشخیص داده و در صورتی که این عدد منطقی به نظر نرسد آنرا گزارش کند. یک جایگزین همچنین قابلیت ایجاد زنگ خطر در زمان وقوع یک حادثه مشکوک را دارد. جایگزین ها می

توانند مشابه سازی شوند و به سیستم دیگر منتقل گردند. به غیر از جایگزین ها ، سیستم می تواند رابط هایی برای دیده بانی کل فعالیت های یک کامپیوتر بخصوص داشته باشد. این رابط ها همیشه نتایج عملیات خود را به یک مانیتور مشخص ارسال می کنند. سیستم های مانیتور اطلاعات را از نقاط مختلف و مشخص شبکه دریافت می کنند و این بدین معنی است که می توانند اطلاعات غیر متمرکز را بهم ارتباط دهند و نتیجه گیری نهایی را انجام دهند. به انضمام اینکه ممکن است فیلتر هایی گذاشته شود تا داده های تولید شده را بصورت انتخابی دریافت نماید.





یک مثال یک واقعیت !

دانشگاه ایالتی آرکانزاس برای مشکلی تقاضای یاری می‌کند. دانشگاه در نیمه کار ارتقا شبکه اصلی خود با ظرفیت چند گیگابیت جهت ارائه خدمات شبکه‌ای به هر اتاق خوابگاه و دفتر دانشکده می‌باشد. از نظر Grey Williamson مسئول روابط سرویسهای اطلاع‌رسانی و تکنولوژی دانشگاه Ark در Jonesboro ساختن چنین شبکه‌ای مثل يك زمین‌بازی فریبنده برای هر هکر خواهد بود که تبدیل به جولانگاهی برای آنها خواهد شد.

شبکه IDS - سیستم آشکارکننده متجاوز

- (Intrusion Detection System) شرکت Cisco Systems مشکل Williamson را حل خواهد کرد. زمانیکه شبکه با ویروسی مواجه می‌شود و یا مورد حمله يك هکر قرار می‌گیرد، IDS مدیریت مرکزی را از آن مطلع می‌سازد. اگر عملیات خراب‌سازی خیلی جدی باشد، سیستم بصورت اتوماتیک کاربران IT را چک کرده و

دست‌رسی کسی را که احتمال می‌دهد از جانب آن، این مشکلات پدید آمده باشد قطع می‌نماید و حتی توانایی شناسایی اتاقي را که هکر در خوابگاه از آنجا وارد شبکه شده است را نیز دارد و سپس سیستم امنیتی دانشکده را از این خرابکاری مطلع می‌سازد.

بسیاری از سازمانها، شبیه دانشگاه ایالتی آرکانزاس به دنبال چنین سیستم‌هایی می‌گردند. چرا که سیاست‌های شناسایی و تعیین هویت کاربران و نرم‌افزارهای ضدویروس برای امنیت شبکه کافی نمی‌باشند.

فعالیت شرکت‌هایی چون Cisco Systems، EnteraSys، Networks، Internet Security Systems در این زمینه نشان از رشد بازار تکنولوژی آشکارسازی متجاوز دارد. شرکت‌های جدیدی که در این زمینه شروع به فعالیت کرده‌اند عبارتند از IntruVert، One Secure و Resource Technologies (Resource) به تازگی توسط شرکت Symantec خریداری شده است) و حتی IDS‌هایی از طرف منابع آزاد چون Snort نیز معرفی شده‌اند.

در ساده‌ترین حالت سیستم آشکارکننده متجاوز، وضعیت امنیتی کار کاربران را شناسایی نموده و آن را ثبت می‌کند. مثلاً اگر کسی در حال اسکن کردن پورت‌های سرور و یا تلاش برای log in شدن به شبکه با استفاده از اسم رمزی تصادفی باشد، را شناسایی می‌کند. البته آن جایگزین کلیه موارد امنیتی شبکه نمی‌باشد. به گفته Stuart McClure مدیر آموزشی و مشاوره امنیتی Foundstone در کالیفرنیا و Misson Viejo، IDS مشابه یک دوربین ویدیویی که در بانک و یا یک فروشگاه بکار گرفته می‌شود، می‌باشد.

چنین دوربین ویدیویی جایگزین سیستم امنیتی و یا قفل درها نمی‌باشد، اما اگر کسی کار خلافی انجام دهد و به نحوی از سیستم امنیتی بکار گرفته شده عبور نماید، دوربین از آن یک رکورد تهیه کرده که در شناسایی مجرم و یا رفع اشکال سیستم امنیتی بکار رفته

می تواند موثر باشد.

سیستمهای آشکار کننده متجاوز به چند روش کار می کنند.

IDS مبتنی بر شبکه شامل سنسورهایی می باشد که پکتها (Packet) را ضمن عبور از شبکه نظارت می کند. بطور نمونه يك IDS مبتنی بر شبکه سنسورهایی را در نقاط ورود به شبکه (برای مثال در کنار فایروالها) یا در مرز بین زیر شبکه ها با سطوح امنیتی مختلف (مثلا بین شبکه LAN و مرکز دیتا) قرار می دهد.

IDS مبتنی بر میزبان (Host-based) با شفافیت و وضوح فعالیت بر روی سرورهای خاص را بررسی می کند. میزبانهای main frame به دنبال فایل های بحرانی می گردند و حتی سیستم عامل های خاصی را بررسی می کنند (مثلا به دنبال پیام های خطای مشکوک و یا پردازش های غیر متعارف سرور می گردند).

IDS مبتنی بر میزبان و شبکه (Network & host Based) مشابه اسکنر ویروس به اسکن کردن امضاها پرداخته و به دنبال نشانه هایی که حاکی از انواع حمله ها می باشند می گردد. ضعف چنین سیستم هایی آن است که امضاها باید مرتبا و با توجه به پیشرفت تکنیک هایی که هکرها بکار می برند، به هنگام شوند. برای پیدا کردن این خرابکاری ها، بعضی از سیستم های آشکار کننده متجاوز به دنبال هرگونه فعالیت شبکه ای خارج از حیطه تعریف شده فعالیت های مجاز می گردند. این نوع عملکرد به عنوان آشکارسازی چیزهای غیر معمول شناخته شده است.

مشکل تمام سیستم های آشکار کننده متجاوز آن است که Plug & Play نبوده و احتمالا در آینده نیز نخواهند بود. برخلاف فایروالها، اغلب سیستم های آشکار کننده متجاوز، برای نصب و راه اندازی به افراد متخصص و وارد به کار نیاز دارند. مسئله مهمتر سیستم آلام آنها جهت کنترل و مدیریت شبکه می باشد. هر IDS زمانیکه به فعالیت مشکوکی برخورد می کند، هشداري را تولید می نماید. از آنجائیکه شبکه ها یکسان نمی باشند. کامپیوترها در بیان این شبکه ها

نمی‌توانند به خوبی عمل نمایند. مثلاً کامپیوتر نمی‌تواند بین یک فایل ویروسی با عنوان "I Love You" و یک پیام email با همین موضوع تفاوت قائل شود. به عنوان نتیجه می‌توان گفت که اغلب سیستم‌های آشکار کننده متجاوز مرتباً پیام هشدار می‌فرستند و در نتیجه پیام‌های خطای زیادی، شاید بیش از هزاران پیام خطا در روز و در زمینه‌های مختلف تولید می‌شوند.

Lloyd Hession سرپرست بخش امنیتی Radianz، در شهر نیویورک که فراهم کننده سرویس‌های شبکه IP برای صنایع مالی است می‌گوید: "هر فروشندگانی برای نمایش کار محصولات خود روشی دارد". به گفته Hession: "مدیران موفق IT با توده انبوهی از اضافه بار اطلاعاتی مواجه شده‌اند. هر کدام از این هشدارها با ارزش می‌باشند و مسئول امنیتی شبکه مجبور به ارزیابی آن به منظور تعیین اینکه آیا استفاده از آن قانونی و یا یک حمله غیرقانونی می‌باشد، است.

به علاوه مسئول رسیدگی و کنترل IDS باید نحوه تشخیص حمله‌های واقعی از هشدارهای خطا را بیاموزند و آنها باید نحوه تنظیم IDS به منظور کاهش هشدارهای خطا را نیز یاد بگیرند.

Williamson از دانشگاه ایالتی آرکانزاس می‌گوید: "کارمندان در روز 30 الی 40 پیام خطا را که توسط IDS شبکه تولید می‌شد، دریافت می‌کردند. بعد از اینکه سیستم برای چند ماهی استفاده شد تعداد پیام‌های خطا به 2 الی 3 اشتباه در روز رسید.

Michael Rusmussen مدیر پژوهشی امنیت اطلاعات در Mass Based Giga کمبریج می‌گوید: "شاید شش ماه طول بکشد تا تمام پیام‌های خطایی را که IDS تولید می‌نماید، برطرف کنید.

اهداف فروشندگان ای دی اس

فروشندگان IDS بیکار ننشسته‌اند. شرکت‌های IDS جدید همچون One Secure و Intruvert به منظور افزایش هوشیاری

سیستم‌هایشان از تکنیک‌های آشکار کننده متجاوز بر پایه امضا و حالت‌های غیر عادی با هم استفاده می‌کنند و حتی زمانیکه حمله‌ای اتفاق می‌افتد، به جای اینکه از سیستم ساده هشدار دهنده استفاده نمایند آن را مسدود می‌کنند. سایر فروشندگان مانند ForeScout از آنالیزهای آماری ترافیک عادی شبکه خود برای شناسایی اتوماتیک پاکت‌های غیر عادی که در واقع یک نوع IDS خود تنظیم می‌باشد، استفاده می‌کنند.

بعضی دیگر از فروشندگان، مانند Tipping Point Technologies و Source Fire به کمک استفاده از سخت‌افزار به رفع این مشکل پرداخته‌اند. آنها اقدام به ساخت تجهیزات IDS بهینه شده بسیار سریع کرده‌اند که می‌توانند ترافیک شبکه را در سرعت‌های بالاتر از سرورهای متعارفی که نرم‌افزار IDS را اجرا می‌کنند، آنالیز نمایند. (این سیستم‌ها از الگوریتم‌های آشکارسازی امضا بسیار پیچیده‌تری استفاده می‌کنند). در نهایت گردانندگان بازار، چون ISS و سیسکو امید به ارائه محصولات بهتر یا ارتقا مدیریت و هوشیاری سنسورهای شبکه‌شان دارند.

یک عضو فنی برجسته در CERT Coordination Center در دانشگاه Carnegie Mellon در Pittsburgh می‌گوید: "من فکر نمی‌کنم سازمان‌ها خواهان یک ریسک باشند و تنها به داشتن وسایل و ابزار اکتفا نمایند". "همیشه نقص دیدگاه‌های انسانی و تجزیه و تحلیل افراد متخصص در این پروسه وجود دارد".

Bruce Larson طراح معماری سیستم‌های امنیتی شبکه برای SAIC Clients در چندین سازمان و شرکت دولتی – نائب رئیس سیستم و مدیرعامل اجرایی شبکه‌های اختصاصی برای SAIC Internatinal می‌گوید: "آشکارسازی متجاوز واقعا کاری هزینه‌بر می‌باشد". او برآورد می‌کند که شما حداقل به یک مهندس شبکه تمام وقت برای مونی‌تور کردن و تنظیم IDS با حقوق مکفی نیاز دارید.

يك راه چاره

مدیریت اطلاعات خروجیهای IDS به منظور ارائه سرویسهای مدیریت شده می‌باشد، در این رابطه شرکت Counterpane Internet Security کارمندانی دارد که تنها آلارم‌های IDS را چک کرده و هشدارهای مهم را به مسئول IT خود می‌فرستند.

IDS چگونه کار می‌کند؟ (طبق گفته خودشان)

طبق اظهارات Jeff Wilson مدیر اجرایی Infonetics و Sum Jose مشاور و پژوهشگر بازاریابی، چه با مدیریت اطلاعات خروجی و چه بدون آن سیستم‌های آشکارکننده متجاوزگران می‌باشند، با داشتن تجهیزاتی در حدود 15000 دلار یا کمی بیشتر می‌توان یک سیستم مناسب داشت ولی یک سیستم بسیار کامل ممکن است در حدود 100000 دلار یا بیشتر درآید. به علاوه باید هزینه خدمات و پشتیبانی فنی و نصب و راه‌اندازی سیستم را هم اضافه کرد. این یکی از دلایلی است که هنوز بازار IDS نسبت به فایروالها بسیار کوچک می‌باشد. دلیل دیگر مدیریت بسیار مشکل آنها می‌باشد.

Jeff Wilson در این زمینه می‌گوید: "هنوز بازار IDS چندان رونقی ندارد و باید از اطلاعات مختلفی بهره جست تا پی به ارزش آن بطور کامل برد".

از سویی دیگر اگر شما چیز با ارزشی برای حفاظت داشته باشید، چاره‌ای جز استفاده از IDS نخواهید داشت. شرکتها اغلب به تکنولوژی IDS برای معرفی شبکه خود، به عنوان یک شبکه مطمئن نیاز دارند به ویژه در صنایع قانونمند که تابع مقررات و ضوابط خاصی می‌باشند. مثل سرویس‌های مالی و مراقبت‌های بهداشتی. GERT'S Allen می‌گوید: "شما مجبور هستید به کل عرضه و تقاضای خود نگاه کنید و ببینید از چه چیزی می‌خواهید حفاظت کنید، به چه چیزی نیاز دارید و چه کار می‌توانید با آن انجام دهید."

اما بکارگیری IDS راحت نیست. طبق اظهارات Rasmussen اغلب شرکتهایی که IDS را بکار گرفته‌اند از شروع کار خود مطمئن هستند اما فقط يك چهارم آنها شانس موفقیت دارند و شاید يك دهم واقعا موفق می‌شوند.

به عبارت دیگر IDS شما یکی از ابزارهای امنیتی شبکه می‌باشد. بکارگیری سطوح مختلف امنیتی در يك سیستم بسیار مفید می‌باشد که توسط بسیاری از ارگان‌های امنیتی توصیه می‌گردد. Allen پیشنهاد می‌دهد که برای يك IT اجرایی از تکنیکهای امنیتی زیر باید استفاده کرد: "سنسورهای آشکارکننده متجاوز برپایه شبکه، آشکارکننده، متجاوز برپایه Host، گزارش‌گیری مرکزی، کنسول مونیטورینگ برای هشدارهای IDS و سایر پیام‌های شبکه، فایروالها و فایل‌های ثبت وقایع و روشهای متداول در به رسمیت شناختن کاربر.

هدف، پردازش مناسب بر اساس داده تولید شده توسط IDS به منظور مدیریت و کنترل شبکه می‌باشد. Foundstone's McClure می‌گوید: "IDS تنها از دید مردم عادی که به آن نگاه می‌کنند، خوب می‌باشد". اگر شما قصد مونیטورینگ آن را ندارید می‌توانید يك doorstep 50000 دلاری بخرید. Rasmussen توصیه می‌کند که پیاده‌سازی IDS باید با پردازش‌های واضح برای پاسخ به آلارمها، خط‌مشی‌های نگهداری شبکه (مثل به هنگام کردن امضا و اصلاحیه‌های سیستم عامل) و آموزشهای پیوسته کارمندان بخش امنیت شبکه همراه باشد.

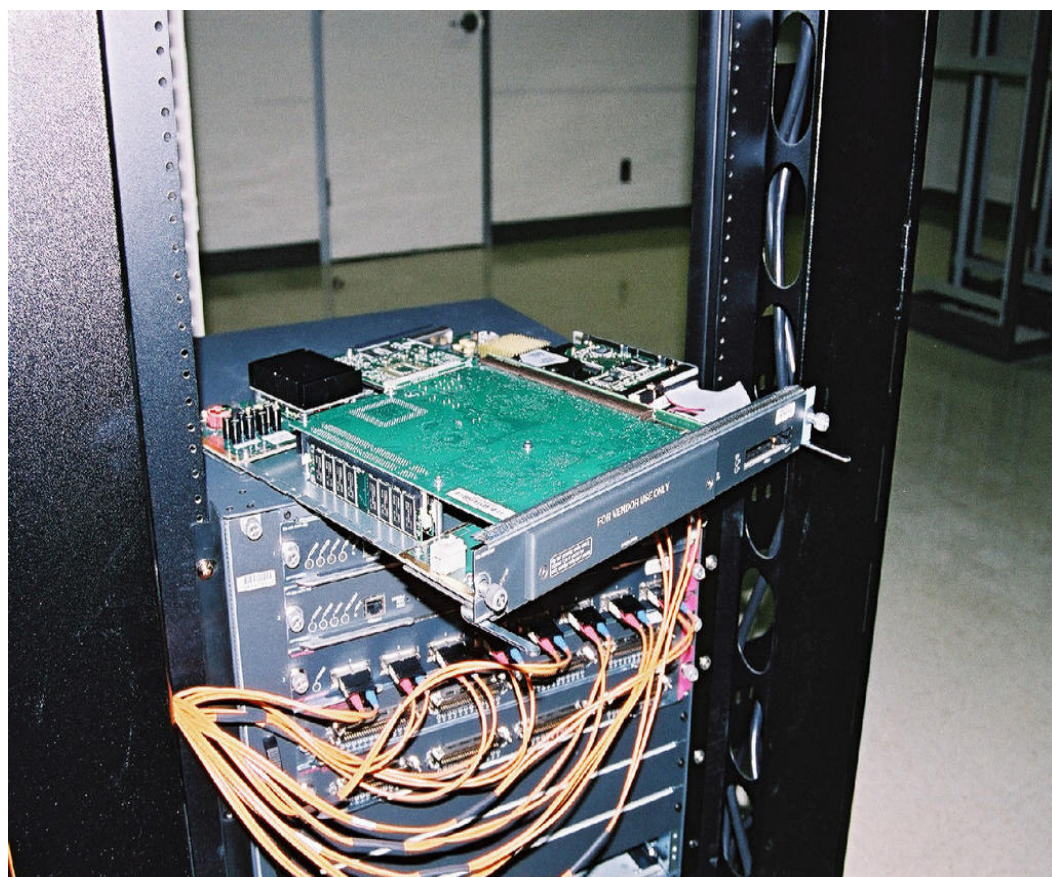
همچنین Rasmussen به شروع با حجم کوچک، با يك یا دو سنسور IDS در نقاط حساس شبکه توصیه می‌کند. باید به حدي کوچک باشد که بتوان آن را کنترل نموده و مهندسین شبکه زمان کافی برای یاد گرفتن سیستم و تنظیم آن بدون مواجه شدن با هزاران آلارم را داشته باشند.

Williamson زمان تست IDS در دانشگاه ایالتی آرکانزاس را در نیمه بهار زمانی که ترافیک شبکه پایین می‌باشد انتخاب کرده 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 تقريباً هر نوع استفاده غيرمجاز از شبكه مثل نرم‌افزار مبادله فايل‌هاي ممنوعه تنظيم نمود.

اگر شما بخواهيد مي‌توانيد تقريباً 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 (10BaseT/100BaseT/1000BaseT w/RJ-45)	IDS-4235-K9 200Mbps Sensor (10/100/1000BaseT w/RJ-45)	IDS-4250-SX-K9 500Mbps Sensor i 1000BaseSX w/SC connector j IDS-4250-TX-K9 500Mbps Sensor i 10/100/1000BaseT w/RJ-45 j

IDS-4235



©®

تمام حقوق مقاله مربوط به تیم های پرشین هکرز و جهنم شیطانی میباشد.



۲۰ قانون از کتاب ...

۱. از افسوس و ترحم 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 در صلح .
۴. از یک استراحت کوتاه بیشتر از یک خواب درازمدت لذت ببرید.
۵. یک "دروگر" باشید ، بدین سان دانه خواهید کاشت.
۶. هرگز به چیزی آن مقدار عشق نورزید که نتوانید شاهد مرگش باشید.
۷. بر روی ماسه چیزی نسازید ، بلکه بر بلندای 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 در همه حال پیروز خواهید بود.

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

۱۲. آن کس که بر بلندای " مرتفع ترین هرم ساخته شده از جمجمه ها " ایستاده ، می تواند دورترین نقطه را ببیند.

۱۳. از عشق دوری نکنید ولی با آن ، آنگونه رفتار کنید که با یک شیاد رفتار می کنید - همواره منصف باشید.

۱۴. هر آن چیز که عظیم است بر فراز اندوه بنا شده

۱۵. تنها بسمت جلو مبارزه نکنید ، در جهت ترقی نیز بجنگید - از برای آنکه عظمت در آسمان ها بیار آمد.

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

۱۷. بگذارید عشق زندگی یک هدف باشد اما اجازه دهید بالاترین هدفتان " بزرگی و سربلندی " باشد.

۱۸. هیچ چیز زیبا نیست ، بجز انسان : ولی زن زیباترین در جهان است.

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

۲۰. آن چیز که نمی کشد ، قویتر میسازد.

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
©® Copyright For : Satanic Team 2005-2006
For More Information Go to [Http://Hack-er.cjb.net/](http://Hack-er.cjb.net/)



SATANIC
DIGITAL NETWORK SECURITY
www.Hack-er.cjb.Net

©®All Right Reserved For Persian Hacker's™
Mr.PHacker_Ir
2005-2006 For More Information
Visit: [Http://PersianHacker.Net/](http://PersianHacker.Net/)



Life & Girl Are Not Matter's
The End.