

# آموزش کلی IDS و روشهای عبور از آن



بنام خدا

IDS:

کلا به اینا میگن سیستمهای کشف مزاحمت مثل کالر آی دی تلفن می مونه. این برنامه ها با تحلیل ترافیک جاری شبکه یا تحلیل تقاضاها سعی در شنا سازی نفوذگر داره و اگه تشخیص بده که عادی نیست به نحو مناسب مسیول شبکه رو در جریان میذاره.

.....

## بخش اول: پیش درآمد

IDSها به نام اصلی **Intrusion Detection System** یا **سیستم کشف و ردیابی نفوذگری** هم اکنون به یکی از مهمترین اجزای ساختار امنیتی شبکه ها تبدیل شدند که دیدم خیلی حیفه اینجا راجیش صحبت نشه . شاید اسم شون رو شنیده باشید یا چیزهایی در بارش بدوینید اونوقت با خودتون بگید شبکه ما از چند فایروال خیلی مطمئن و قوی استفاده میکنه پس احتیاجی به این سیستم نباید داشته باشیم .  
در يك کلام IDS همینطور که از اسمشون پیداست کار يك سري نفوذگري ها و اخلال گري ها در شبکه رو ردگيري و کشف میکند . اگر بخوام واضح تر بگم این سیستم ها سعی میکنند حملات و یا سو استفاده هاي انجام شده از شبکه یا کامپیوتر ها رو شناسایی میکنند و به مسئولان اطلاع میدهند.

### اما این سیستم ها چه فرقی با فایروال ها دارند؟؟

اگرچه همیشه این دو ابزار رو کنار هم استفاده کرد ولي نباید با هم یکسان فرضشون کرد خب میگین چرا ؟ اگر فایروال رو نگاهیان درخونتون فرض کنید حتما بهش گفتین که چه کسانی رو راه بده و چه کسانی رو راه نده.....  
یا اگر ممکنه کیف و جیب مراجعین رو هم بگرد و اگر کسی چیز خطرناکی داشت راهش نده. حالا اگه به مامور پست که توی کیفش ۲ کیلو مواد منفجره یا چه میدونم اسلحه داشته باشه چي؟؟ نگاهیان ممکنه کیف به پستچی رو اصلا نگاه نکنه.....  
یا نه اگر به دزد بخواد از روی نرده ، دیوار یا هر چیز دیگه یا کلا کاری که من علاقه دارم یعنی **تونل زدن !!** رو امتحان کنه چي؟؟ درسته که فایروال ها درجه های هوشمند زیادی دارند اما در عمل در نحوه انجام عملیاتی خود انعطاف زیادی ندارند.....  
همچنین اگر با ارائه يك دسته گزارش و ثبت تلاش هاي نفوذگري در فایل هاي لاگ شما رو آگاه میکنند ولي معمولا این گزارش ها واضح و دقیق نیستند بحث IDS ها از اینجا شروع میشه.....

## IDS ها ، لزوم و کلیات

Computer Security یعنی شناسایی و جلوگیری از هرگونه دسترسی و استفاده غیر مجاز از يك کامپیوتر. تعریفی که بر دو مفهوم اساسی جلوگیری و ممانعت Prevention و کشف و شناسایی Detection بنا شده است! اگر چه هم فایروال ها و هم IDS ها در هر دو جنبه ای که گفتم کاربرد مشترکی پیدا میکنند اما باید توجه داشته باشید که وظیفه اصلی فایروال جلوگیری و وظیفه يك IDS در شناسایی هست برای همین از اینها دو مکمل هم نام میبرند و در عین حال با توجه به افزایش نفوذگري ها در عصر اینترنت و پیدایش روشهای جدید و پیچیده نفوذگري نیاز به IDS ها کم کم غیر قابل اجتناب میشود چون که IDSها می توانند انواع متنوع و پیچیده تري از نفودها و اخلال هارو شناسایی کنند و در صورت امکان خودشون از این اقدامات جلوگیری کنند  
شاید براتون جالب باشه که بدوینید در آمریکا تقریباً تمامی شرکت ها و سازمان هاي کوچک و بزرگ از IDS ها استفاده مي کنند و اینم بدوینید که IDS ها خیلی گرون تر از فایروال ها هستند !!

IDS ها تا این لحظه بهترین و موثرترین انتخاب برای شناسایی و پاسخگویی به حملات درونی و بیرونی یک شبکه به حساب میان.

### توجه:

هیچ ابزار امنیتی و از جمله سیستم های IDS هرگز امنیت کامل شبکه شما رو تضمین نمیکند ! اما وقتی در کنار اعمالی مثل تعیین خط مشی های امنیتی Security Policy , ارزیابی نقاط ضعف سیستم ها Vulnerability Assessment , رمز کردن دیتا ها و اطلاعات Data Encryption , اعتبار سنجی و مجوز دهی Authentication و Authorization و فایروال و سپس استفاده از یک IDS همیشه گفت به میزان قابل توجهی امنیت شبکه رو بالا بردید.....

### انواع IDS ها

IDS های موجود در دو نوع Host Based و Network Based موجودند گر چه بعضی از انواع جدیدشون ترکیبی از این دو مدل هستند هرکدوم از این دو نوع متد های خودشون رو برای نظارت و حفاظت از اطلاعات دارند و هر کدوم هم مزایا و معایب خاص خودشون رو دارند به طور خلاصه Host Based ها داده های موجود روی هر کامپیوتر را به طور جداگانه بررسی میکنند در حالی که Network Based ها اطلاعات رد بدل شده بین کامپیوتر های شبکه رو بازرسی میکنند

### IDS های مبتنی بر میزبان ( Host Based IDS )

IDS های مبتنی بر میزبان یا HIDS ها معمولا بسته هایی هستند که روی کامپیوتری که قراره ازش محافظت کنند قرار میگیرند. بیشتر این HIDS از System Log ها و Audit Log و Event Log های سیستم عامل و برنامه های کاربردی مختلف برای ارائه گزارش یا ارسال هشدار مبتنی بر عملکرد پردازش های سیستم/کریر هستند, استفاده میکنند. HIDS ها اعمال مختلفی برای کشف یک حمله به یک میزبان انجام میدهند یکی از معمولی ترین کارهایی که این نوع IDS برلی شنا انجام میدهد , بررسی و حصول اطمینان از درستی و سالم بودن فایل های سیستم میباشد ( File Integrity ) HIDS ها در امور مربوط به امنیت فایل ها عملکرد خوبی دارند , مواردی همچون تشخیص این که آیا فایل های مهم و حساس یک سیستم مورد دستکاری قرار گرفته یا نه و یا ردیابی دستیابی غیر مجاز یک کاربر که خارج از حیطه مجاز و سطح دسترسی داده شده به کاربر میباشد یک HIDS بری اینکار یک بار فایل های سیستم رو بازرسی و یک Signature یا نشانه رمز شده برای هر یک از فایل ها ایجاد می کنه ( Cryptographic Signature ) پس از این کار IDS هر چند وقت یک بار فایل هارو با این نشانه مقایسه و بررسی می کنه و اگر تغییر و تفاوتی رو پیدا کنه سریعاً گزارش میده

### از مزایا و ویژگی های IDS های Host-Based می توان به موارد زیر اشاره کرد :

۱- اطلاعات صریحی درمورد آنکه چه کسی در چه زمانی چه کاری را به چه مقصدی انجام داده ارائه می کنند!! یعنی معمولا مبدا , مقصد , زمان و نوع عمل انجام شده را مشخص می کنند , در چنین شرایطی نیاز به محاسبه و مقایسه و ارزیابی برای فهمیدن یک هشدار یا گزارش نخواهید داشت و می توانید براحتی درباره فرد یا برنامه ای که مسبب انجام عملی هست تصمیم بگیرید.

۲- HIDS ها معمولا کمتر ممکن است به اشتباه اعلام خطر کنند , چرا که همان طور که گفته شد اطلاعاتشان مستقیماً به افراد و برنامه های مشخص مربوط میشود

۳- ترافیک شبکه ای کمتری نسبت به IDS های مبتنی بر شبکه ایجاد می کنند

در عین حال این نوع IDS ها نقاط ضعفی هم دارند از جمله این که قابلیت انتقال خوبی بر روی سیستم عامل های مختلف ندارند. معمولا برای هر نوع سیستم عامل باید یک نرم افزار IDS مبتنی بر میزبان نوشته شود همچنین از آنجایی که در یک شبکه بزرگ با تعداد زیادی میزبان یا گره ( Node ) مواجه هستیم , جمع آوری انبوهی از اطلاعات جداگانه و خاص برای هر یک از کامپیوتر ها میتواند کاری سخت و ناکارآمد باشد و نهایتاً این که چنانچه یک مهاجم و نفوذگر به نحوی عمل جمع آوری اطلاعات روی یکی از کامپیوتر ها را غیر فعال سازد برنامه IDS موجود روی آن کامپیوتر عملاً به هیچ کاری نمی آید.

### چند نمونه از منبع پکیج های HIDS عبارتند از :

- ۱- Intruder Alert از شرکت Axent Technologies به آدرس [www.axent.com](http://www.axent.com)
  - ۲- Tripwire از شرکت Trip Security Systems به آدرس [www.Tripwiresecurity.com](http://www.Tripwiresecurity.com)
  - ۳- POLYCENTER Security Intrusion Detecto
- ### IDS های مبتنی بر شبکه ( Network Based IDS )

بسته های نرم افزاری که ارائه کننده این نوع IDS می باشند معمولا سیستم هایی اختصاصی هستند که تمامی یک بخش یا Segment از شبکه را از بیرون و گاهی از درون یک فایروال مورد نظارت و بررسی قرار میدهند . این سیستم ها معمولا از دو بخش ناظر ( Monitoring ) یا Sniffing یا ( Sensor و عامل ( Agent ) تشکیل شده اند. ناظر Monitor یک دستگاه و یا یک پکیج نرم افزاری است که شبکه را به منظور یافتن بسته های اطلاعاتی مشکوک مورد بررسی قرار میدهد .

عامل ( Agent ) که ترجمه درستش مامور یا جاسوس هست نرم افزاری است که معمولا به طور جداگانه روی هر یک از کامپیوترهای مورد نیاز قرار می گیرد و نقش ارسال اطلاعات را بصورت بازخورد به ناظر بر عهده دارد.

همچنین ممکن است بخش دیگری به نام کنسول مدیریت ( Management Console ) هم وجود داشته باشد که به شکلی مطمئن با

اعتبار سنجي و رمزنگاري به ناظر متصل مي شود و از آن گزارش دريافت مي کند و نيز به تبادل اطلاعات مربوط به تنظيم و پيکر بندي سيستم مي پردازد.

در بيشتر موارد کار اصلي IDS هاي مبتني بر شبکه جمع آوري بسته هاي اطلاعاتي ورودي به شبکه و بررسي آن ها بر پایه دسته اي از عوامل است تا از اين طريق بفهمند آیا اين بسته ها ممکن است علت يکي از انواع حملات شناخته شده يا فعاليت هاي مشکوک باشند يا نه.

در حقيقت بر خلاف IDS هاي مبتني بر ميزبان و به جاي بررسي اطلاعاتي که بر روي يك کامپيوتر قرار دارند و يا از آنجا سرچشمه ميگيرند اين نوع IDS ها با استفاده از تکنیک هايي مانند **Packet Sniffing** يا کالبد شکافي بسته ها ديته ها را از درون بسته هاي اطلاعاتي ( TCP/IP و يا ساير پروتکل ها ) که در حال رفت و آمد در شبکه مي باشند استخراج مي کنند .  
اين مراقبت و نظارت بر ارتباط ميان کامپيوتر ها باعث مي شود که NIDS ها در کشف و تشخيص نفوذگري هاي انجام شده از محيط بيروني شبکه مورد حفاظت عنصر موثر و کارامدي به حساب بيايند.

از مزايای و ویژگی هاي NIDS ها مي توان به موارد زير اشاره کرد:

1- کارايي خوب در برابر حملات مبتني بر DOS و ربودن پهناي باند. اين نوع حملات خارجي با هدف سو استفاده و يا استفاده بيش از حد ( Overload ) از منابع شبکه صورت ميگيرند. بسته هايي که حاوي يا ايجاد کننده اين نوع حملات هستند به خوبي توسط IDS هاي Network based شناسايي مي شوند.

2- کارايي خوب در برابر دستيابي هاي غير مجاز خارجي. هنگامی که يك کاربر غير مجاز به يك کامپيوتر Login مي کند و يا در اين راستا تلاش مي کند اين IDS هاي مبتني بر ميزبان هستند که بهتر از هر عنصر امنيتي ديگري چنين رويدادي را تشخيص ميدهند اما تشخيص کاربران غير مجاز پيش از اقدام به ورود به سيستم بهتر از هر ابزار ديگري از عهده IDS هاي مبتني بر شبکه بر مي آيد.

3- نوع سيستم عامل يا يك برنامه کاربردي خاص وابسته نيستند چرا که در سطح بسته ها عمل مي کنند همچنين براي اجرا و گرفتن نتيجه از آن ها نيازي به داشتن مجوزها کلمات عبور سيستم عامل و همچنين برنامه هاي کاربردي ندارند.

### نقاط ضعف :

اين نوع IDS ها نيز البته دراي نقاط ضعفي هم هستند . مهمترين نقطه ضعف اين IDS ها به هنگام کار در شبکه هاي سريع ( 1000 Mbps و بالاتر ) و نيز مواجهه با بسته هاي رمز شده مي باشد .  
در مورد اول چنانچه NIDS برخي بسته ها و اطلاعات را به دليل سرعت بالاي انتقال شان از دست بدهد آن گاه از جمع آوري و تجزيه تحليل صحيح آن ها باز مي ماند و در مورد دوم چنانچه ترافیک شبکه رمز شده باشد IDS نشانه هاي يك حمله را نمي تواند تشخيص بدهد ( قابل توجه هکرهاي حرفه اي )  
در ضمن NIDS ها در شبکه هاي سوئيچ شده نيز دچار مشکل مي شوند.

برخي از منابع بسته هاي نرم افزاري NIDS ها عبارتند از:

1- Netranger از شرکت Cisco Systems به آدرس [www.cisco.com](http://www.cisco.com)

2- ISS Real Secure به آدرس [www.iss.net](http://www.iss.net)

3- CyberCop Monitor از Network Associates به آدرس [www.nai.com](http://www.nai.com)

Shadow , Snort! , Dragon , NFR و NetProwler چند نام تجاري و معروف ديگر از اين دسته هستند از شرکت Digital به آدرس [www.digital.com](http://www.digital.com)

### چگونگي قرار گرفتن IDS در شبکه

هر IDS مبتني بر ميزبان بر روي يك کامپيوتر سرويس دهنده در شبکه نصب و اجرا ميشود.  
IDS مبتني بر شبکه , درون شبکه و بلافاصله پشت فایروال قرار دارد. البته بايد توجه داشت که اين راه حل تنها روش ممکن نيست مثلا ميتوان يك IDS مبتني بر شبکه را به گونه اي نصب کرد که بخش ناظر يا Sensor آن به ناحيه ( DMZ شبکه متصل به هر دو شبکه داخلي و خارجي ) و ديگر بخش هاي آن به شبکه داخلي متصل باشد. خيلي وقت ها يك IDS مبتني بر شبکه را درون DMZ قرار مي دهيم در اين حالت فرض کرده ايم که يك فایروال داريم و يك DMZ نيز ايجاد کرده ايم . اگر IDS را پشت فایروال قرار دهيم آنگاه مي توان حملات پروتکل ها و منابعي که از فایروال عبور مي کنند و همچنين حملات کاربران داخلي شبکه را نيز شناسايي و آشکار کرد.

اکنون IDS مبتني بر شبکه مي تواند براي آشکار سازي يا واکنش به يك حمله يا دسترسي غير مجاز يکي از کارهاي زير را انجام دهد:

1- E-Mail فراخوان ( Page ) يا SNMP ارسال کند

2- يك ارتباط مبتني بر TCP را بلوکه کند يا به کلي از بين ببرد

3- يك اسکرپت تعريف شده توسط کاربر يا برنامه خاصي را اجرا کند (مثلا برخي سرپس هاي شبکه اي را به ترتيب اولويت ShutDown کند)

### تکنیک هاي IDS

هر يك از دو نوع IDS ها Host-Based و Network-Based از 4 تکنیک اصلي براي کشف و ردیابی نفوذگران استفاده مي کنند:

- 1- Anomaly Detection یا نمونه های غیر متعارف
- 2- Signature (Misuse) Detection یا کشف از روی نشانه یا سو استفاده
- 3- Target Monitoring یا نظارت بر هدف
- 4- Stealth Probes یا کاوش های نهایی.

و حالا یکی یکی توضیح میدم

### 1- تشخیص نمونه های غیر متعارف (Anomaly Detection)

IDS يك مرز نرمال از الگوهای متعارف استفاده از سیستم برای خود ترسیم و تعریف میکند. هر رفتار یا رویدادی که به میزان زیادی از این الگوها دور باشد، به عنوان يك اختلالگري محتمل بر شبکه در نظر گرفته می شود. آن چه خلاف قاعده و غیر متعارف فرض می شود می تواند متغییر باشد اما معمولاً رویدادی که با تناوبی بیشتر یا کمتر از دو مرتبه انحراف از آمار نرمال به وقوع بپیوندد غیر متعارف فرض میشود.

چند مثال برای این شرایط عبارتند از:

کاربري که به جای يك یا دو بار ورود و خروج نرمال از سیستم در طول يك روز ۲۰ بار این کار را انجام داده است  
 کامپیوتری که در ساعت ۲ بعد از نیمه شب مورد استفاده قرار گرفته در صورتی که قرار نبوده پس از ساعت اداری روشن باشد  
 در يك سطح دیگر این تکنیک می تواند الگوهای در مورد کاربران از جمله برنامه هایی که به اجرا در می آورند را مورد بررسی قرار دهند مثلاً اگر کاربری از بخش گرافیک يك سازمان ناگهان شروع به دست یابی به برنامه های حسابداری یا کامپایل کردن کد نماید سیستم می تواند يك هشدار به Administrator یا مسئول امنیتی شبکه ارسال کند

### 2- کشف از روی نشانه یا سو استفاده (Signature Or Misuse Detection)

این روش از دسته ای از الگوهای شناخته شده از رفتارهای غیر مجاز به منظور پیش بینی و کشف تلاش های مشابه بعدی استفاده می نماید. این الگوهای خاص Signature نامیده میشوند. برای IDS های مبتنی بر میزبان ۳ بار تلاش نا موفق برای Login میتواند يك Signature باشد. برای IDS های مبتنی بر شبکه Signature میتواند يك الگوی خاص باشد که با بخشی از يك بسته همخوانی داشته باشد. به عنوان مثال نشانه های مربوط به سربرگ يك بسته اطلاعاتی می تواند نشانه يك عمل غیر مجاز مثلاً اجرای يك FTP غیر عادی باشد. بسته به میزان اهمیت و جدي بودن نشانه یا Signature ممکن است يك عکس العمل یا Response به عمل انجام شده و یا روس قبلی تکنیک های اول و دوم رو شرح دادم و حالا ادامه بحث

### 3- نظارت بر هدف (Target Monitoring)

در این روش به جای جستجو برای یافتن يك مورد غیر متعارف یا يك نشانه، تغییر و دستکاری احتمالی بعضی فایل ها مورد بررسی قرار میگردد. این تکنیک بیشتر يك شیوه کنترلی تصحیح کننده است یعنی برای آشکار سازی يك عمل غیر مجاز پس از به وقوع پیوستن آن و به منظور انجام عمل معکوس طراحی شده است  
 یکی از راه های کشف دستکاری شدن پنهانی فایل ها این است که کد های رمز شده ای برای آن ها ایجاد شود (Cryptographic Hash) و در فواصل زمانی معینی Hash های جدید هر فایل مقایسه شود. پناه سازی چنین سیستمی آسان است زیرا به نظارت مستمر Administrator نیازی ندارد.  
 فواصل زمانی بررسی سالم بودن و جامعیت فایل ها و نیز اینکه آیا تمامی آن ها و یا صرفاً برخی فایل های مهم سیستمی مورد بررسی قرار بگیرند به راحتی قابل تنظیم و کنترل می باشد

### 4- کاوش نهایی (Stealth Probes)

این تکنیک برای ردیابی نفوذگرانی که سعی می کنند عملیاتشان را در دوره های زمانی طولانی به انجام برسانند به کار می رود. مثلاً يك نفوذگر در يك دوره زمانی دو ماهه به بررسی ضعف های امنیتی و پورت های باز يك سیستم می پردازد سپس دو ماه دیگر صبر می کند تا حمله اش را واقعاً عملی کند. تکنیک کاوش های نهایی مجموعه متنوع و زیادی از داده ها را از سیستم جمع آوری می کند و بر پایه آن به دنبال آثار يك حمله ساخت یافته و اسلوب مند در يك زمان طولانی می گردد. در این روش نمونه گیری های زیادی از سیستم جهت کشف حملات مرتبط با این شواهد و نمونه ها صورت می پذیرد.  
 این روش از دو تکنیک رفتار غیر متعارف و سو استفاده برای آشکار سازی رفتارهای مشکوک استفاده می کند

### چند نکته پایانی

بی شك وجود سیستم های امنیتی يك سطح امنیتی بهیچ شبکه شما می افزاید بخصوص اگر دلایلی دارید مبنی بر این که بیش از پیش هدف تهاجم هکرها قرار می گیرد، مثلاً اگر نمونه های Port Scan بی شماری در لاگ فایل های فایروال مشاهده می کنید و یا اینکه مورد تهاجم واقعی قرار گرفته اید استفاده از IDS ضروری می نماید

در عین حال فراموش نکنید که این ابزارهای امنیتی مانند هر وسیله دیگری می تواند معایبی نیز داشته باشد علاوه بر نقاط ضعفی که قبلاً در مورد دو نوع مختلف IDS توضیح دادم به طور کلی همه آن ها می توانند دارای دو عیب زیر باشند:

### 1- False Positives یا اعلام خطر های اشتباه

اگرچه ممکن است ترجیح بدهید که IDS شما بیشتر حساس باشد تا این که اصلاً بعضی موارد نفوذگری را تشخیص ندهد، اما يك False Positives گاه ممکن است برایتان گران تمام بشود، مثلاً اگر IDS را طوری تنظیم کرده اید که هرگونه ارتباط یا Connection مشکوک را قطع کند چنین اشتباهی میتواند منجر به قطع ارتباط کاربر مشروع از سیستم شما شود اگر عامل زمان برای سرویسی که ارائه می کنید مهم باشد (مثلاً يك سایت ویژه تجارت الکترونیک) این اشتباه مصیبت بار خواهد بود

### 2- کاهش کارایی سیستم

با پیدایش سیستم های جدیدتر و سریع تر این عامل از اهمیت کمتری برخوردار است البته فکر نمی کنم در ایران کم اهمیت باشه ، اما به هر حال باید توجه داشت که آنالیز کردن بسته های شبکه و Audit Log های سیستم يك عمل زمان بر و به طور بالقوه مصرف کننده توان پردازنده مي باشد بخصوص اگر ترافیک شبکه اي زياد و يا سرویس دهنده اي که اطلاعات فراواني براي آنالیز تولید مي کنند داشته باشید ممکن است که متوجه شوید که سرویس های شبکه اي یا سرویس های موجود روي ميزبان ها به شکل غير قابل قبولي کند شده است.

بهتر است در صورت امکان پیش از تهیه IDS اطلاع یابید که چه میزان فعالیت برای IDS مورد نظر زیاد محسوب مي شود و یا اینکه ابتدا يك نسخه نمونه آزمایشي از محصول را روي شبکه خود امتحان کنید

-چنان چه سیستم ها و شبکه شما به درستي پیکربندی و تنظیم شده باشد IDS با سایر اجزا و ادوات امنیتی شبکه از جمله فایروال تداخل وظیفه پیدا نخواهد کرد ، در عین حال يك فایروال نباید به گونه اي تنظیم شده باشد که از عملکرد عادي IDS جلوگیری نماید چرا که IDS يك ابزار کشف و ردیابی است که انتظار مي رود کلیه نفوذگري ها و اقدامات انجام شده در شبکه از جمله آن هایی که از سایر محصولات امنیتی موجود در شبکه سر چشمه مي گیرند جمع آوري ، بررسی و در صورت لزوم آشکار نمایند

**امیدوارم که مورد توجه هکرهاي عزیز قرار گرفته باشه ، این IDS ها ممکنه که برامون گرون تموم بشن .....يك تذکر یا هشدار به افراد مسئول ارسال شود**

.....

این هم توضیح های ساده تر و خلاصه تر من :  
تو این مقاله بعد از بررسی آی دی اس روشهای فرار از چنگ ای دی اس رو هم میگویم.  
کلا ما در دو سطح ids داریم  
۱) در سطح لایه شبکه  
۲) در سطح لایه کاربرد

### در سطح لایه شبکه:

آی دی اس در این سطح تمام بسته های ip رو دریافت و جمع آوری میکنه و اونا رو تحلیل میکنه و بسته های مربوط به نفوذگر رو تشخیص میده. Ids باید انبوه بسته ها رو منظورم ip رو چه tcp چه udp را مرتب میکنه و تشخیص میده.  
کلا اینا به بانک اطلاعاتی دارن که الگوهای مختلف حمله توش هست اسمش هم هست(attack signature&future) یعنی ویژگی ها و امضای حمله.  
یعنی ids خودشو با این بانک تطبیق میدهو اگه اون ترافیک هایی که واستون گفتم با این بانک تطابق داشت آره دیگه یارو لو میره؟  
وقتی هم فهمید که حمله ای شده واسه ادمین میل میزنه و به جوری خبر میده دیگه و به تعقیب طرف هم ادامه میده که دیگه یارو سر و کارش با ۱۱۰ دیگه؟؟  
مثلا ممکنه یارو پورت تلنتش ۲۳ باز باشه وبینه که یه هکر میخواد نفوذ کنه اونوقته که ...

### خوب حالا چطوری از ids لایه شبکه فرار کنیم:

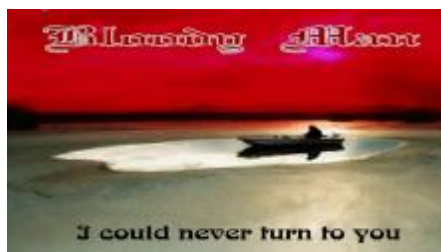
۱) ترافیک ارسالی به شبکه هدف باید با الگوی هیچ حمله ای مطابقت نداشته باشه و اونم به راه داره و اینه که هکر خودش یه برنامه واسه نفوذ بنویسه (هکر ها برنامه نویسیخون خوبه و محتاج نرم افزار نیست)  
عزیز برو یه کتاب سی بخر بخون من هم برنا مه نویسی سوکت رو یادت میدم تو شروع کن یا علی رو بگو منم هستم؟؟؟  
خلاصه چون این نرم افزار هکره الگوی از قبل تعریف شده ای نداره اون ids هم استناد میشه.  
۲) بسته های ارسالی به یک شبکه به جوری باشه که عملکرد نهایی اوون تو host استاد بشه  
خوب اینجا چی گفتم من خوب دقت کن:  
همونطور که تو tcp/ip بلدی یه بسته ip میتونه یه سلسله از قطعات کوچیک باشه (fragment) و هر بسته شکسته شده سر آیند بسته ip رو همراه خودشون دارن  
ما این قطعات رو می فرستیم واسه اون طرف و این بسته ها هیچ چیزی نشدن فقط ریز ریز شدن و میرن تو host طرف و بهم میچسبن و باز سازی میشن  
خوب آی دی اس با بسته های ریز ریز شده مواجه شده باید مثل host اونا رو دریافت کنه دیگه درستته؟  
و بعد هم سر همشون کنه ببینه جریان چیه؟؟  
شما میتونید بسته های ip رو در قطعه های کوچیک بذارید مثلا(۸بایتی) و بفرستیدشون .  
در ضمن اگه شما بسته های ip علکی بسیار زیاد و رد کم کنی دیگه ای رو وسطای بسته های اصلیتون بفرستید ids فلج میشه.  
می دونید چرا چون ids باید بافر زیادی در اختیار داشته باشه تا همه رو جفت و جور کنه و اونا رو بهم بچسبونه . فهمیدید که چی شد.  
-----<روش حمله:

+++)) فرض کنید یه بسته ip محتوی یک بسته tcp(در فیلد Pay load) باشد : چون بخش pay load از هر بسته ip می تواند قطعه قطعه شود لذا بصورت عمدی قطعه اول به قدری کوچک در نظر گرفته میشه که فقط دو بایت اول از بسته tcp/ip رو شامل میشه بنابراین دو بایت دوم از بسته tcp را شامل شود که شماره پورت مقصد (destination Port) را در بر میگيرد در بسته دوم ارسال می شود .  
معمولا سیستم های Ids برای تشخیص حمله به سر آیند بسته tcp احتیاج دارن تا مثلا تلاش برای برقراری ارتباط با پورت ۲۳ رو تشخیص بدن . چون بسته اول سر آیند کامل بسته tcp و شما ره پورت مقصد رو ندارن معمولا ids ان را معمولی در نظر میگيرن واز آن میگذرن بدین صورت هکر hds رو دور میزنه.(برو خالشو ببر)  
++++)) یه نوع دیگه حمله بر علیه ids استفاده از قطعات همپوشان هستش(Fragment Overlap) که با دستکاری در فیلد Offset از بسته ip انجام میشود . به گونه ای که در ip میدونید این فیلد برای باز سازی قطعات بسته ip تنظیم می شوند و در حقیقت این شماره محل فرار گرفتن قطعه جاری را در دیتا گرام اصلی مشخص میکند  
-----<خوب حالا میریم سراغ مکانیزم ارسال:

۱) اولین قطعه بسته ip که شامل سرآیند بسته tcp هست رو و دارای شماره پورت مجازه (مثل HTTP-TCP 80)

۲) دومین قطعه بگونه ای تنظیم میشه که بعد از بازسازی روی قطعه های قبل اضافه میشه پس حالا شما ره پورت واقعی در قطعه دوم مشخص میشه شماره پورتهی که در قطعه اول اومده بود پوچ بود و سرکاری چون وقتی دومی میاد اون شماره پرته بازنویسی OVERWRITE میشه فهمیدید که چی شد بسته هر کدوم همدیگرو کامل میکنن و با هر کدوم اطلاعات کمکم کاملتر میشه/  
۳) چون احتمالا فقط قطعه اول از هر ip توسط Ids بررسی میشه لذا قطعه دوم که اولی رو باز نویسی میکنه توسطش تشخیص داده نمی شه!





منابع: (۱) مقاله از مهدی هگز (mahdi\_hexboy) و ایمان (توضیحات کلی در مورد آی دی اس)  
(۲) کتابهای شبکه و سایت [www.Astalavista.box.sk](http://www.Astalavista.box.sk)

کلیه حقوق این مقاله مربوط به سایت [www.4shir.com](http://www.4shir.com) و نویسنده میباشد.