آموزش كلي Ids و روشهاي 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 سایی نفوذگر داره و اگه تشخیص بده که عادی نیست به نحو مناسب مسیول شبکه رو در جریان میذاره.

''''''''''''

بخش اول: پيش درآمد

IDSها به نام اصلي Intrusion Detection System يا سيستم كشف و ردياپي نفوذگري هم اكنون به يكي از مهمترين اجزاي ساختار امنيتي شبكه ها تبديل شدند كه ديدم خيلي حيفه اينجا راجبش صحبت نشه .
شايد اسم شون رو شنيده باشيد يا چيزهايي در بارش بدونيد اونوقت با خودتون بگيد شبكه ما از چند فايروال خيلي مطمئن و قوي استفاده ميكنه پس احتياجي به اين سيستم نبايد داشته باشيم
در يك كلام IDS همينطور كه از اسمشون پيداست كار يك سري نفوذگري ها و اخلال گري ها در شبكه رو ردگيري و كشف ميكنند .
اگر بخوام واضح تر بگم اين سيستم ها سعي ميكنند حملات و يا سو استفاده هاي انجام شده از شبكه يا كامپيوتر ها رو شناسايي ميكنند و به مسئولان اطلاع ميدهند.
اما اين سيستم ها چه فرقي با فايروال ها دارند ؟؟
اگرچه ميشه اين دو ابزار رو كنار هم استفاده كرد ولي نبايد با هم يكسان فرضشون كرد خب ميگين چرا ؟ اگر فايروال رو نگهبان درخونتون فرض كنيد حتما بهش گفتين كه چه كساني رو راه بده و چه كساني رو راه نده.....
يا اگر ممكنه كيف و جيب مراجعين رو هم بگرد و اگر كسي چيز خطرناكي داشت راهش نده. حالا اگه يه مامور پست كه توي كيفش ۲ كيلو مواد منفجره يا چه ميدونم اسلحه داشته باشه چي ؟؟ نگهبان ممكنه كيف يه پستچي رو اصلا نگاه نكنه.....
يا نه اگر يه دزد بخواد از روي نرده , ديوار يا هر چيز ديگه يا كلا كاري كه من علاقه دارم يعني تونل زدن !! رو امتحان كنه چي ؟؟
درسته كه فايروال ها درجه هاي هوشمند زيادي دارند اما در عمل در نحوه انجام عملياتي خود انعطاف زيادي ندارند.....
همچنين اگر با ارائه يك دسته گزارش و ثبت تلاش هاي نفوذگري در فايل هاي لاگ شما رو آگاه ميكنند ولي معمولا اين گزارش ها واضح و دقيق نيستند بحث IDS ها از اينجا شروع ميشه.....

IDS ها , لزوم و كليات

Computer Security يعني شناسايي و جلوگيري از هرگونه دسترسي و استفاده غير مجاز از يك كامپيوتر. تعريفي كه بر دو مفهوم اساسي جلوگيري و ممانعت Prevention و كشف و شناسايي Detection بنا شده است! اگر چه هم فايروال ها و هم IDS ها در هردو جنبه اي كه گفتم كاربرد مشتركي پيدا ميكنند اما بايد توجه داشته باشيد كه وظيفه اصلي فايروال جلوگيري و وظيفه يك IDS در شناسايي هست براي همين از اينها دو مكمل هم نام ميبرند و در عين حال با توجه به افزايش نفوذگري ها در عصر اينترنت و پيدايش روشهاي جديد و پيچيده نفوذگري نياز به IDS ها كم كم غير قابل اجتناب ميشود چون كه IDSها مي توانند انواع متنوع و پيچيده تري از نفوذها و اخلال هارو شناسايي كنند و در صورت امكان خودشون از ين اقدامات جلوگيري كنند
شايد براتون جالب باشه كه بدونيد در آمريكا تقريبا تمامي شركت ها و سازمان هاي كوچيك و بزرگ از IDS ها استفاده مي كنند و اينم بدونيد كه IDS ها خيلي گرون تر از فايروال ها هستند !!

IDS ها تا اين لحظه بهترين وموثرترين انتخاب براي شناسايي و پاسخگويي به حملات دروني و بيروني يك شبكه به حساب ميان.

توجه:
هيچ ابزار امنيتي و از جمله سيستم هاي IDS هرگز امنيت كامل شبكه شما رو تضمين نميكنه ! اما وقتي در كنار اعمالي مثل تعيين خط مشي هاي امنيتي Security Policy , ارزيابي نقاط ضعف سيستم ها Vulnerability Assessment , رمز كردن ديتا ها و اطلاعات Data Encryption , اعتبار سنجي ومجوز دهي Authentication و Authorization و فايروال و سپس استفاده از يك IDS ميشه گفت به ميزان قابل توجهي امنيت شبكه رو بالا برديد.....

انواع IDS ها

IDS هاي موجود در دو نوع Host Based و Network Based موجودند گر چه بعضي از انواع جديدشون تركيبي از اين دو مدل هستند هركدوم از اين دو نوع متد هاي خودشون رو براي نظارت و حفاظت از اطلاعات دارند و هر كدوم هم مزايا و معايب خاص خودشون رو دارند به طور خلاصه Host Based ها داده هاي موجود روي هر كامپيوتر را به طورجداگانه برسي ميكنند در حالي كه Network Based ها اطلاعات رد بدل شده بين كامپيوتر هاي شبكه رو بازرسي ميكنند

IDS هاي مبتني بر ميزبان (Host Based IDS)

IDS هاي مبتني بر ميزبان يا HIDS ها معمولا بسته هايي هستند كه روي كامپيوتري كه قراره ازش محافظت كنند قرار ميگيرند.
بيشتر اين HIDS از System Log ها و Audit Log و Event Log هاي سيستم عامل و برنامه هاي كاربردي مختلف براي ارائه گزارش يا ارسال هشداري مبتني بر عملكرد پردازش هاي سيستم/كربر هستند, استفاده ميكنند.
HIDS ها اعمال مختلفي براي براي كشف يك حمله به يك ميزبان انجام ميدهند يكي از معمولي ترين كارهايي كه اين نوع IDS برلي شنا انجام ميدهد , بررسي و حصول اطمينان از درستي و سالم بودن فايل هاي سيستم ميباشد (File Integrity)
HIDS ها در امور مربوط به امنيت فايل ها عملكرد خوبي دارند , مواردي همچون تشخيص اين كه آيا فايل هاي مهم و حساس يك سيستم مورد دستكاري قرار گرفته يا نه و يا رديابي دستيابي غير مجاز يك كاربر كه خارج از حيطه مجاز و سطح دسترسي داده شده به كاربر ميباشد
يك HIDS بري اينكار يك بار فايلهاي سيستم رو بازرسي و يك Signature يا نشانه رمز شده براي هر يك از فايل ها ايجاد مي كنه (Cryptographic Signature) پس از اين كار IDS هر چند وقت يك بار فايل هارو با ين نشانه مقايسه و بررسي مي كنه و اگر تغيير و تفاوتي رو پيدا كنه سريعا گزارش ميده

از مزايا و ويژگي هاي IDS هاي Host-Based مي توان به موارد زير اشاره كرد :

١- اطلاعات صريحي درمورد انكه چه كسي در چه زماني چه كاري را به چه مقصدي انجم داده ارائه مي كنند!! يعني معمولا مبدا , مقصد , زمان و نوع عمل انجام شده را مشخص مي كنند , در چنين شرايطي نياز به محاسبه و مقايسه و ارزيابي براي فهميدن يك هشدار يا گزارش نخواهيد داشت و مي توانيد براحتي درباره فرد يا برنامه اي كه مسبب انجام عملي هست تصميم بگيريد.

٢- HIDS ها معمولا كمتر ممكن است به اشتباه اعلام خطر كنند , چرا كه همان طور كه گفته شد اطلاعاتشان مستقيما به افراد و برنامه هاي مشخص مربوط ميشود

٣- ترافيك شبكه اي كمتري نسبت به IDS هاي مبتني بر شبكه ايجاد مي كنند

در عين حال اين نوع IDS ها تقاط ضعفي هم دارند از جمله اين كه قابليت انتقال خوبي بر روي سيستم عامل هاي مختلف ندارند.
معمولا براي هر نوع سيستم عامل بابد يك نرم افزار IDS مبتني برميزبان نوشته شود همچنين از آنجايي كه در يك شبكه بزگ با تعداد زيادي ميزبان يا گره (Node) مواجه هستيم , جمع آوري انبوهي از اطلاعات جداگانه و خاص براي هر يك از كامپيوتر ها ميتواند كاري سخت و ناكارامد باشد و نهايتا اين كه چنانچه يك مهاجم و نفوذگري به نحوي عمل جمع آوري اطلاعات روي يكي از كامپيوتر ها را غير فعال سازد برنامه IDS موجود روي آن كامپيوتر عملا به هيچ كاري نمي اید.

چند نمونه از منبع پكيج هاي HIDS عبارتند از :

١- Intruder Alert از شركت Axent Technologies به آدرس www.axent.com
٢- Tripwire از شركت Trip Security Systems به آدرس www.Tripwiresecurity.com
٣- POLYCENTER Security Intrusion Detecto

IDS**هاي مبتني بر شبكه** (Network Based IDS)

بسته هاي نرم افزاري كه ارائه كننده اين نوع IDS مي باشند معمولا سيستم هايي اختصاصي هستند كه تمامي يك بخش يا Segmentاز شبكه را از بيرون و گاهي از درون يك فايروال مورد نظارت و بررسي قرار ميدهند .
اين سيستم ها معمولا از دو بخش ناظر Monitoring) يا Sniffering يا (Sensor و عامل (Agent) تشكيل شده اند.
ناظر Monitor يك دستگاه و يا يك پكيج نرم افزاري است كه شبكه را به منظور يافتن بسته هاي اطلاعاتي مشكوك مورد بررسي قرار ميدهد .

عامل (Agent) كه ترجمه درستش مامور يا جاسوس هست نرم افزاري است كه معمولا به طور جداگانه روي هريك از كامپيوترهاي مورد نياز قرار مي گيرد و نقش ارسال اطلاعات را بصورت بازخورد به ناظر بر عهده دارد.

همچنين ممكن است بخش ديگري به نام كنسول مديريت (Management Console) هم وجود داشته باشد كه به شكلي مطمئن با

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

در بيشتر موارد كار اصلي IDS هاي مبتني بر شبكه جمع آوري بسته هاي اطلاعاتي ورودي به شبكه و بررسي آن ها بر پايه دسته اي از عوامل است تا از اين طريق بفهمند آيا اين بسته ها ممكن است علت يكي از انواع حملات شناخته شده يا فعاليت هاي مشكوك باشند يا نه.
در حقيقت بر خلاف IDS هاي مبتني بر ميزبان و به جاي بررسي اطلاعاتي كه بر روي يك كامپيوتر قرار دارند و يا از آنجا سرچشمه ميگيرند اين نوع IDS ها با استفاده از تكنيك هايي مانند Packet Sniffing يا كالبد شكافي بسته ها ديتا ها را از درون بسته هاي اطلاعاتي (TCP/IP و يا ساير پروتكل ها) كه در حال رفت و آمد در شبكه مي باشند استخراج مي كنند .
اين مراقبت و نظارت بر ارتباط ميان كامپيوتر ها باعث مي شود كه NIDS ها در كشف و تشخيص نفوذگري هاي انجام شده از محيط بيروني شبكه مورد حفاظت عنصر موثر و كارامدي به حساب بيايند.

از مزايا و ويژگي هاي NIDS ها مي توان به موارد زير اشاره كرد:

-1كارايي 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 شبكه صورت ميگيرند. بسته هايي كه حاوي يا ايجاد كننده اين نوع حملات هستند به خوبي توسط IDS هاي Network based شناسايي مي شوند.

-2كارايي خوب در برابر دستيابي هاي غير مجاز خارجي. هنگامي كه يك كاربر غير مجاز به يك كامپيوتر Login مي كند و يا در اين راستا تلاش مي كند اين IDS هاي مبتني بر ميزبان هستند كه بهتر از هر عنصر امنيتي ديگري چنين رويدادي را تشخيص ميدهند اما تشخيص كاربران غير مجاز پيش از اقدام به ورود به سيستم بهتر از هر ابزار ديگري از عهدهIDS هاي مبتني بر شبكه بر مي ايد.

-3به نوع سيستم عامل يا يك برنامه كاربردي خاص وابسته نيستند چرا كه درسطح بسته ها عمل مي كنند همچنين براي اجرا و گرفتن نتيجه از آن ها نيازي به داشتن مجوزها كلمات عبور سيستم عامل و همچنبن برنامه هاي كاربردي نداريد.

نقاط ضعف :

اين نوع IDS ها نيز البته دراي نقاط ضعفي هم هستند . مهمترين نقطه ضعف اينIDS ها به هنگام كار در شبكه هاي سريع (۱۰۰۰ Mbpsو 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 چنانه ترافيك شبكه رمز شده باشد IDS نشانه هاي يك حمله را نمي تواند نمي تواند تشخيص بدهد) قابل توجه هكرهاي حرفه اي(
در ضمنNIDS ها در شبكه هاي سوئيچ شده نيز دچار مشكل مي شوند.

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

-1از شركت Cisco Systems به آدرس www.cisco.com Netranger
-2به آدرسwww.iss.net ISS Real Secure
-3از Network Associates به آدرسwww.nai.com CyberCop Monitor

Shadow , Snort! , Dragon , NFR -و NetProwler چند نام تجاري و معروف ديگر از اين دسته هستندr از شركت Digital به آدرس www.digital.com

چگونگي قرار گرفتن IDS در شبكه

هر IDS مبتني بر ميزبان بر روي يك كامپيوتر سرويس دهنده در شبكه نصب و اجرا ميشود.
IDSمبتني بر شبكه , درون شبكه و بلافاصله پشت فايروال قرار دارد. البته بايد توجه داشت كه اين راه حل تنها روش ممكن نيست مثلا ميتوان يك IDS مبتني بر شبكه را به گونه اي نصب كرد كه بخش ناظر يا Sensor آن به ناحيه) DMZ شبكه متصل به هر دو شبكه داخلي و خارجي) و ديگر بخش هاي آن به شبكه داخلي متصل باشد .خيلي وقت ها يك IDS مبتني بر شبكه را درون DMZ قرار مي دهيم در اين حالت فرض كرده ايم كه يك فايروال داريم و يك DMZ نيز ايجاد كرده ايم . اگر IDS را پشت فايروال قرار دهيم آنگاه مي توان حملات پروتكل ها و منابعي كه از فايروال عبور مي كنند و همچنين حملات كاربران داخلي شبكه را نيز شناسليي و آشكار كرد.
اكنون IDS مبتني بر شبكه مي تواند براي آشكار سازي يا واكنش به يك حمله يا دسترسي غير مجاز يكي از كارهاي زير را انجام دهد:
-1يك , E-Mail فراخوان (Page) يا SNMP Trap ارسال كند
-2يك ارتباط مبتني بر TCP را بلوكه كند يا به كلي از بين ببرد
-3يك اسكريپت تعريف شده توسط كاربر يا برنامه خاصي را اجرا كند (مثلا برخي سريس هاي شبكه اي را به ترتيب اولويت)ShutDownكند

تكنيك هاي IDS

هر يك از دو نوع IDS ها Host-Based و Network-Based از ۴ تكنيك اصلي براي كشف و رديابي نفوذگران استفاده مي كنند:

1- Anomaly Detectionيا نمونه هاي غير متعارف
2- Signature (Misuse) Detectionيا كشف از روي نشانه يا سو استفاده
3- Target Monitoringيا نظارت بر هدف
4- Stealth Probesيا كاوش هاي نهايي.

و حالا يكي يكي توضيح ميدم

1-تشخيص نمونه هاي غير متعارف (Anomaly Detection)

IDSيك مرز نرمال از الگوهاي متعارف استفاده از سيستم براي خود ترسيم و تعريف ميكند. هر رفتار يا روايدي كه به ميزان زيادي از اين الگوها دور باشد , به عنوان يك اخلالگري محتمل بر شبكه در نظر گرفته مي شود.
آن چه خلاف قاعده و غير متعارف فرض مي شود مي تواند متغيير باشد اما معمولا رويدادي كه با تناوبي بيشتر يا كمتر از دو مرتبه انحراف از آمار نرمال به وقوع بپيوندد غير متعارف فرض ميشود.

چند مثال براي اين شرايط عبارتند از:
كاربري كه به جاي يك يا دو بار ورود و خروج نرمال از سيستم در طول يك روز ۲۰ بار اين اين كار را انجام داده است
كامپيوتري كه در ساعت ۲ بعد از نيمه شب مورد استفاده قرار گرفته در صورتي كه قرار نبوده پس از ساعت اداري روشن باشد
در يك سطح ديگر اين تكنيك مي تواند الگوهايي در مورد كاربران از جمله برنامه هايي كه به اجرا در مي آورند را مورد بررسي قرار دهند مثلا اگر كاربري از بخش گرافيك يك سازمان ناگهان شروع به دست يابي به برنامه هاي حسابداري يا كامپايل كردن كد بنمايد سيستم مي تواند يك هشدار به Administrator يا مسئول امنيتي شبكه ارسال كند

2-كشف از روي نشانه يا سو استفاده (Signature Or Misuse Detection)
اين روش از دسته اي از الگوهاي شناخته شده از رفتارهاي غير مجاز به منظور پيش بيني و كشف تلاش هاي مشابه بعدي استفاده مي نمايد. اين الگوهاي خاص Signature ناميده ميشوند. براي IDS هاي مبتني بر ميزبان ۳بار تلاش نا موفق براي Login ميتواند يك Signatureباشد. براي IDS هاي مبتني بر شبكه Signature ميتواند يك الگوي خاص باشد كه با بخشي از يك بسته همخواني داشته باشد. به عنوان مثال نشانه هاي مربوط به سربرگ يك بسته اطلاعاتي مي تواند نشانه يك عمل غير مجاز مثلا اجراي يك FTP غير عادي باشد. بسته به ميزان اهميت و جدي بودن نشانه يا Signature ممكن است يك عكس العمل يا Response به عمل انجام شده و يا روس قبلي تكنيك هاي اول و دوم رو شرح دادم و حالا ادامه بحث

3-نظارت بر هدف(Target Monitoring)
در اين روش به جاي جستجو براي يافتن يك مورد غير متعارف يا يك نشانه, تغيير و دستكاري احتمالي بعضي فايل ها مورد بررسي قرار ميگيرد .اين تكنيك بيشتر يك شيوه كنترلي تصحيح كننده است يعني براي آشكار سازي يك عمل غير مجاز پس از به وقوع پيوستن آن و به منظور انجام عمل معكوس طراحي شده است
يكي از راه هاي كشف دستكاري شدن پنهاني فايل ها اين است كه كد هاي رمز شده اي براي آن ها ايجاد شود (Cryptographic Hash)و در فواصل زماني معيني باHash هاي جديد هر فايل مقايسه شود. پياه سازي چنين سيستمي آسان است زيرا به نطارت مستمر Administrator نيازي ندارد.
فواصل زماني بررسي سالم بودن و جامعيت فايل ها و نيز اينكه آيا تمامي آن ها و يا صرفا برخي فايل هاي مهم سيستمي مورد بررسي قرار بگيرند به راحتي قابل تتظبم و كنترل مي باشد

4-كاوش نهايي(Stealth Probes)
اين تكنيك براي رديابي نفوذگراني كه سعي مي كنند عملياتشان را در دوره هاي زماني طولاي به انجام برسانند به كار مي رود. مثلا يك نفوذگر در يك دوره زماني دو ماهه به بررسي ضعف هاي امنيتي و پورت هاي باز يك سيستم مي پردازد سپس دو ماه ديگر صبر مي كند تا حمله اش را واقعا عملي كند. تكنيك كاوش هاي نهايي مجموعه متنوع و زيادي از داده ها را از سيستم جمع آوري مي كند و بر پايه آن به دنبال آثار يك حمله ساخت يافته و اسلوب مند در يك زمان طولاني مي گردد. در اين روش نمونه گيري هاي زيادي از سيستم جهت كشف حملات مرتبط با اين شواهد و نمونه ها صورت مي پذيرد.
اين روش از دو تكنيك رفتار غير متعارف و سو استفاده براي آشكار سازي رفتارهاي مشكوك استفاده مي كند

چند نكته پاياني

بي شك وجود سيستم هاي امنيتي يك سطح امنيتي بهبه شبكه شما مي افزايد بخصوص اگر دلايلي داريد مبني بر اين كه پيش از پيش هدف تهاجم هكرها قرار مي گيرد , مثلا اگر نمونه هاي Port Scan بي شماري در لاگ فايل هاي فايروال مشاهده مي كنيد و يا اينكه مورد تهاجم واقعي قرار گرفته ايد استفاده از IDS ضروري مي نمايد

در عين حال فراموش نكنيد كه اين ابزارهاي امنيتي مانند هر وسيله ديگري مي تواند معايبي نيز داشته باشد علاوه بر نقاط ضعفي كه قبلا در مورد دو نوع مختلف IDS توضيح دادم به طور كلي همه آن ها مي توانند داراي دو عيب زير باشند:

1- False Positivesيا اعلام خطر هاي اشتباه
اگرچه ممكن است ترجيح بدهيد كه IDS شما بيشتر حساس باشد تا اين كه اصلا بعضي موارد نفوذگري را تشخيص ندهد, اما يك Connection يا False Positivesگاه ممكن است برايتان گران تمام بشود , مثلا اگر IDS را طوري تنظيم كرده ايد كه هرگونه ارتباط مشكوك را قطع كند چنين اشتباهي ميتواند منجر به قطع ارتباط كاربر مشروع از سيستم شما شود اگر عامل زمان براي سرويسي كه ارائه مي كنيد مهم باشد (مثلا يك سايت ويژه تجارت الكترونيك) اين اشتباه مصيبت بار خواهد بود

2-كاهش كارايي سيستم

با پيدايش سيستم هاي جديدتر و سريع تر اين عامل از اهميت كمتري برخوردار است البته فكر نمي كنم در ايران كم اهميت باشه , اما به هر حال بايد توجه داشت كه آناليز كردن بسته هاي شبكه و Audit Log هاي سيستم يك عمل زمان بر و به طور بالقوه مصرف كننده توان پردازنده مي باشد بخصوص اگر ترافيك شبكه اي زياد و يا سرويس دهنده اي كه اطلاعات فراواني براي آناليز توليد مي كنند داشته باشيد ممكن است كه متوجه شويد كه سرويس هاي شبكه اي يا سرويس هاي موجود روي ميزبان ها به شكل غير قابل قبولي كند شده است.
بهتر است در صورت امكان پيش از تهيه IDS اطلاع يابيد كه چه ميزان فعاليت براي IDS مورد نظر زياد محسوب مي شود و يا اينكه ابتدا يك نسخه نمونه آزمايشي از محصول را روي شبكه خود امتحان كنيد

-چنان چه سيستم ها و شبكه شما به درستي پيكربندي و تنظيم شده باشد IDS با ساير اجزا و ادوات امنيتي شبكه از جمله فايروال تداخل وظيفه پيدا نخواهد كرد , در عين حال يك فايروال نبايد به گونه اي تنظيم شده باشد كه از عملكرد عادي IDS جلوگيري نمايد چرا كه IDS يك ابزار كشف و رديابي است كه انتظار مي رود كليه نفوذگري ها و اقدامات انجام شده در شبكه از جمله آن هايي كه از ساير محصولات امنيتي موجود در شبكه سر چشمه مي گيرند جمع آوري , بررسي و در صورت لزوم آشكار نمايند

اميدوارم كه مورد توجه هكرهاي عزيز قرار گرفته باشه , اين IDS ها ممكنه كه برامون گرون تموم بشن .....يك تذكر يا هشدار به افراد مسئول ارسال شود

"""""""""""""""""""""

اين هم توضيح هاي ساده تر و خلاصه تر من :
تو اين مقاله بعد از بررسی آی دی اس روشهای فرار از چنگ ای دی اس رو هم ميگم.
كلا ما در دو سطح ids داريم
۱)در سطح لايه شبكه
۲)در سطح لايه كاربرد

در سطح لايه شبكه:

آی دی اس در اين سطح تمام بسته های ip رو دريافت و جمع آوری ميكنه و اونا رو تحليل ميكنه و بسته های مربوط به نفوذگر رو تشخيص ميده.
Ids بايد انبوه بسته ها رو منظورم ip رو چه tcp چه udp را مرتب ميكنه و تشخيص ميده.
كلا اينا يه بانک اطلا عاتی دارن كه الگو های مختلف حمله توش هست اسمش هم هست(attack signature&future) يعنی ويژگی ها و امضای حمله.
يعنی ids خودشو با اين بانک تطبيق ميدهو اگه اون ترافيک هايی كه واستون گفتم با اين بانک تطابق داشت آره ديگه يارو لو ميره؟
وقتی هم فهميد كه حمله ای شده واسه ادمين ميل ميزنه و يه جوری خبر ميده ديگه و به تعقيب طرف هم ادامه ميده كه ديگه يارو سر و كارش با ۱۱۰ ديگه؟؟
مثلا ممكنه يارو پورت تلنتش ۲۳ باز باشه وببينه كه يه هكر ميخواد نفوذ كنه انوقته كه ...

خوب حالا چطوری از ids لايه شبكه فرار كنيم:

۱)ترافيک ارسالی به شبكه هدف بايد با الگوی هيچ حمله ای مطابقت نداشته باشه و اونم يه راه داره و اينه كه هكر خودش يه برنامه واسه نفوذ بنويسه (هكر ها برنامه نويسيشون خوبه و محتاج نرم افزار نيست)
عزيز برو يه كتاب سی بخر بخون من هم برنا مه نويسی سوكت رو يادت ميدم تو شروع كن يا علی رو بگو منم هستم؟؟؟
خلاصه چون اين نرم افزار هكره الگوی از قبل تعريف شده ای نداره اون ids هم استاد ميشه.
۲)بسته های ارسالی به يک شبكه يه جوری باشه كه عملكرد نهايی اوون تو host استاد بشه
خوب اينجا چی گفتم من خوب دقت كن:
همونطور كه تو tcp/ip بلدی يه بسته ip ميتونه يه سلسله از قطعات كوچيک باشه (fragment) و هر بسته شكسته شده سر آيند بسته ip رو همراه خودشون دارن
ما اين قطعات رو می فرستيم واسه اون طرف و اين بسته ها هيچ چيزی نشدن فقط ريز ريز شدن و ميرن تو host طرف و بهم ميچسبن و باز سازی ميشن
خوب آی دی اس با بسته های ريز ريز شده مواجه شده بايد مثل host اونا رو دريافت كنه ديگه درسته؟
و بعد هم سر همشون كنه ببينه جريان چيه؟؟
شما ميتونيد بسته های ip رو در قطعه های كوچيک بذاريد مثلا(۸بايتی) و بفرستيدشون .
در ضمن اگه شما بسته های ip علكی بسيار زياد و رد گم كنی ديگه ای رو وسطای بسته های اصليتون بفرستيد ids فلج ميشه.
می دونيد چرا چون ids بايد بافر زيادی در اختيار داشته باشه تا همه رو جفت و جور كنه و اونا رو بهم بچسبونه . فهميديد كه چی شد.

----------><----------روش حمله:

۱+++)فرض كنيد يه بسته ip محتوی يک بسته tcp(در فيلد Pay load) باشد : چون بخش pay loadاز هربسته ip می تواند قطعه قطعه شود لذا بصورت عمدی قطعه اول به قدری كوچک در نظر گرفته ميشه كه فقط دو بايت اول از بسته tcp/ip رو شامل ميشه بنابراين دو بايت دوم از بسته tcp را شامل شود كه شماره پورت مقصد (destination Port) را در بر ميگيرد در بسته دوم ارسال می شود .
معمولا سيستم های Ids برای تشخيص حمله به سر آيند بسته tcp احتياج دارن تا مثلا تلاش برای برقراری ارتباط با پورت ۲۳ رو تشخيص بدن .
چون بسته اول سر آيند كامل بسته tcp و شما ره پورت مقصد رو ندارن معمولا ids ان را معمولی در نظر ميگيرن واز آن ميگذرن بدين صورت هكر hds رو دور ميزنه.(برو حالشو ببر)
+++۲)يه نوع ديگه حمله بر عليه ids استفلده از قطعات همپوشان هستش(Fragment Overlap)كه با دستكاری در فيلد fragment Ofsset از بسته ip انجام ميشود . به گونه ای كه در ip ميدونيد اين فيلد برای باز سازی قطعات بسته ip تنظيم می شوند و در حقيقت اين شماره محل فرار گرفتن قطعه جاری را در ديتا گرام اصلی مشخص ميكند
----------><----------خوب حالا ميريم سراغ مكانيزم ارسال:
۱)اولين قطعه بسته ip كه شامل سرآيند بسته tcp هست رو و دارای شماره پورت مجازه (مثل HTTP-TCP 80)
۲)دومين قطعه بگونه ای تنظيم ميشه كه بعد از بازسازی روی قطعه های قبل اضافه ميشه پس حالا شما ره پورت واقعی در قطعه دوم مشخص ميشه شماره پورتی كه در قطعه اول اومده بود پوچ بود و سركاری چون وقتی دومی ميياد اون شماره پرته بازنويسیOVERWRITE ميشه
فهميديد كه چی شد ابسته هر كدوم همديگرو كامل ميكنن و با هر كدوم اطلاعات كمكم كاملتر ميشه/
۳)چون احتمالا فقط قطعه اول از هر ip توسط Ids بررسی ميشه لذا قطعه دوم كه اولی رو باز نويسی ميكنه توسطش تشخيص داده نمی شه!

۴)قطعات همپوشان پس از با زسازی در ماشین هدف بسته tcp اصلی رو با شماره پورت واقعی تشکیل خواهند داد.

FRAG ROUTER هم یه ابزار واسه این مرحله از حمله است البته شرمنده که تحت یونیکسه.
این ابزار حدود ۳۵ روش مختلف رو در قطعه قطعه کردن IP یا TCP در نظر میگیره.
یه جوری مسیر یاب نرم افزاریه نفوذگر اونو روی ماشینی نصب میکنه و با تکنیکهای قطعه سازی مختلف هر ابزاری که واسه حمله نیاز داره اسفاده میکنه .
و یه جور MANAGER واسه ابزارهای دیگه است و بسته های شما قبل از خروج رو به روشهای ۳۵ گانه که الان افزایش هم پیدا کرده به بیرون میفرسته و ids هم .....؟؟؟؟
اینم سایتش: توسط گروه DUG SONG همون گروهی که من خیلی دوستش دارم؟؟؟
/http://www.anzen.com/research/nidsbench

سیستم IDS (کشف مزاحمت) در لایه کاربرد :

سیستم کشف مزاحمت در لایه کاربرد تمام تقا ضاهای ارسالی هر برنامه رو بررسی میکنه و اگه دید غیر طبیعی هستش و خطرناکه هشدار میده همونطور که میدونید شبکه پروتکل های مختلفی داره از جمله HTTP/SMPT/... و هر پروتکل نیاز داره به یه IDS مجزا .
یه مثال حالا به کار میاد:
فرض کنید یه تقاضای HTTP از نوع GET با قالب زیر صادر شده باشه
GET /cgi-bin/broken.cgi HTTP/1.0
این تقاضا باعث می شه تا یه برنامه آسیب پذیر از نوع CGI بر روی سرویس دهنده هدف اجرا بشه
Ids میتونه این تقاضا رو کشف کنه و به صاحابش بگه!!!
تو این سطح هم ids یه سری قانونها از پیش تعریف شده داره.

------->حمله بر علیه IDS جهت کشف برنامه ها ی cgi اسیب پذیر:

دیگه داریم میرسیم آخراش اکثر برنامه های تحت وب با اسکریپتهای cgi نوشته میشن .
اسکریپت های cgi کدهای اجرایی خاصی هستن که روی سرویس دهنده وب اجرا میشن .
مثلا یه اسکریپت cgi میتونه داده های ارسالی کاربر رو بگیره و توی یه بانک اطلاعاتی ذخیره کنه.
امیدوارم با مفهوم سی جی آی آشنا شده باشین.
اگه کمی فکر کنین میبینین همه CGI های معمولی این کار ها رو انجام میدن:
۱)جستجو در بانک اطلا عاتی به دنبال یه آیتم خاص و مورد نظر کاربر
۲)ذخیره اطلا عات ارسالی توسط کاربر در یک بانک اطلاعاتی
۳)انجام یه محا سبه فوری و سریع
اکثر برنامه های مبتنی بر وب بر اساس اسکریپتهای CGI یا روشهای مشابه مثل asp (active srver page) یا perl نوشته می شن php
خیلی از سرویس دهنده های وب مثل apache یا iis (مایکروسافت) روشهای اسکریپت نویسی رو با مثالهایی شروع میکنن که برنامه نویسا از یه نقطه خوب شرو ع کنن .
اما خوشبختانه و یا متا سفانه بخش خیلی زیادی از این اسکریپت ها ناقص و ضعیف نوشته میشن.
حالا مطلب رو یه کم تخصصی تر میکنیم:

برخی از برنامه های cgi اونقدر ضعیف هستن که داده های کاربر رو که ارسال کرده مستقیما میگیره و روی سرویس دهنده اصلی اجرا میکنه.
مثلا یه اسکریپت رو در نظر بگیرین که یک فرمان پرس و جو رو (query) رو از صفحه وب کاربر میگیره و اوون رو مستقیما به sql server میفرسته .
ادمای عادی این چیزا رو متوجه نمی شن و اون اسکریپت رو مستقیما از صفحه وب راه اندازی میکنن ولی یه هکر نه از طریق صفحه وب بلکه از طریق برنا مه نویسی با پورت ۸۰سرویس دهنده ارتباط برقرار میکنه و تقا ضای راه اندازی یه اسکریپت را از طریق صفحه وب راه میندازه البته با متود GET اسکریپتهای ضعیفCGI این رو یعنی هر چی که طرف بفرسته اجرا میکنن دیگه بعد هم؟؟
پس یه هکر برای پیدا کردن این نقطه ضعفها باید اسکریپت های آسیب پذیر رو چک کنه برای جستجوی این نقاط ابزارهای زیادی هست که به نظر می رسه قویترین اونها ویسکر whisker هستش
چون این یه چیز دیگست و علاوه بر جستجو یه کار دیگه هم میکنه واون گول زدن ids هستش.
این ابزار رو می تونید در سایت RAINFOREST puppy s که یه بار پکت ستورم PACKET STORM همون سایت خفنی که همه میشناسنش رو با روش sql piggy backing هک کرد .
/http://www.wiretrip.net/rfp
در دستزس هست و به زبان پرل هست (nessus هم این کار رو انجام میده ولی در سطح tcp/ip قویه ولی whisker در سطح لایه کاربرد و وب) براتون ازش بگم که بیش از ۸۰۰ نوع اسکریپت cgi و asp رو میشناسه و امتحان میکنه.
میتونه با سرویس دهنده های وب مجازی vitural Web server که روی یک ماشین واحد اجرا میشوند ارتباط برقرار کند. در ضمن (آقا قابلیت زیاد داره.....) روشی برای حدس زدن userid و کلمه عبور در هنگام احراز هویت (Web Authentication) درخواست می شود پیاده سازی کرده .
بزرگترین ویژگیش هم که تا حالا ۱۰۰ بار گفتم گول زدن ids هستش.
خیلی از سیستمهایی که ids لایه کاربرد دارن تمام تقا ضاها رو کهget/put/post/delete دارن بازرسی میکنه(اینایی که گفتم متودهای پروتکل http) میشه
و Whisker هم کارش Web Ids گول زدنه.
دیگه شیوه هاشو براتون نمیگم که چه مکانیزمهایی واسه این کار داره که اونوقت باید MIME هم براتون بگم.ایشالله در مقالات دیگر کاملش میکنم.
اگه مکا نیزم هاشو خواستید بگید تا وقت کردم براتون بگم /زیاده ولی چند تا باشه.

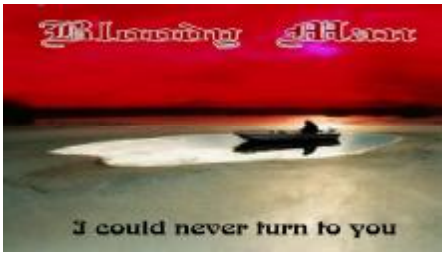
اینم مقاله من در مورد Ids امیدوارم این چند ساعت و نیم وقتی که گذاشتم سودی داشته باشه.!!

می دونید هک و امنیت یه علمه دیدید چه روشهایی داره من دوست دارم همه بهش به دید یه علم نگاه کنن نه تفریح و اوون رو اصولی یاد بگیرن روشها خیلی زیبا هستن وکلاسیک باید رووشون تمرکز کرد ویادشون گرفت.

اگه کاری با من داشتید با آی دی من تماس داشته باشید:diablo_7_diablo@yahoo.com

قربان همه شما عزیزان

> > > حسام.ح دانشجوی سال سوم کامپیوتر نرم افزار



منابع: ۱) مقاله از مهدي هگز(mahdi_hexboy)و ايمان (توضيحات كلي در مورد آي دي اس)
۲) كتابهاي شبكه و سايت www.Astalavista.box.sk