DOS ATT4CK

Author: Satanic Soulful

Shabgard

SatanicHell

©®All Right Reserved For SatanicHell

©®All Right Reserved For Shabgard Security 2005-2006

Satanic Hell

جهنم شیطانی

DOS ATTACK

مباحثی پیرامون حملات عدم پذیرش سرویس

نویسنده: Satanic Soulful
تاریخ:28/6/1384

Contact:
Satanic.soulful@GMail.Com
Satanic_Soulful@Yahoo.Com
Special TNX♥2:
Hell Hacker – **C0llecT0r –** S hahro Z – XshabgardX – Rap Game - Black Eye Girl

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 شبگرد 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:

, IDS Journal, Cert, Microsfot, Network Security Essential by William Stallings
Washington.Edu , Denial info , Black hat Hacker's Journal Of Attack In Network

به نامه خدای خوبی ها و پاکی ها

مقدمه:

در سالهای قبل در دنیای مجازی ما هکر ها که حملات کامپیوتری اکثرا از یک نوع بود و مانند هم اکنون بسیار پیچیده و از نوع های مختلف نبود و اکثرا هکرهای برجسته و صاحب نوع از یک نوع حملات استفاده می کردنند!

اما امروز دیگر حملات مانند قدیم نمیباشد و اکثرا تشکیل شده از چند نوع حمله می باشند.

مثلا وقتی شما در یک سایت خبرگزاری مطلع میشود که یک گروه توانسته است شمار زیادی سایت را هک و دیفیس (تغییر دادن شکل ظاهری یک سایت)کند با استفاده باگه کرنل وقتی در نگاه اول شما این خبر میبنید فکر میکنید یک حمله ساده با استفاده از باگه کرنل بوده ولی در واقع تشکیل شده از چند نوع حمله میشود. تلنت،نتکت،دزدی هویت،در های پشتی و ... هر کدام از اینها یک نوع حمله می باشد و هر کدام دارای الگوریتم خاصی برای خود می باشند.یکی از این نوع حملات حمله از نوعهDOS(عدم پذیرش_ سرویس)می باشد!

شاید تاکنون شنیده باشید که یک وب سایت مورد تهاجمی از نوع DoSقرار گرفته است . این نوع از حملات صرفا" متوجه وب سایت ها نبوده و ممکن است شما قربانی بعدی باشید .تشخیص حملات DoSاز طریق عملیات متداول شبکه امری مشکل است ولی با مشاهده برخی علائم در یک شبکه و یا کامپیوتر می توان فهمید که مورد حمله قرار گرفتید یا که نه...

مدير امنيتي شبكه براي برطرف كردن نيازهاي امنيتي نياز به شناخت نقصهاي امنيتي و انتخاب سياست ها و محصولات امنيتي متفاوت دارد.

يكي از راه هاي برطرف سازي نيازها در نظرگرفتن سه وجه امنيت اطلاعات است.

حملات امنيتي:

هر فعاليتي كه طي آن اطلاعات امنيتي كه متعلق به هر سازماني مي باشد ، افشا شود يا دستخوش تغييرات گردد.

مكانيسم امنيتي:

مكانيسمي كه براي بررسي، ممانعت و يا رفع نقص ايجاد شده از طرف حملات امنيتي طراحي شده است.

سرويس هاي امنيتي:

هر سرويسي كه امنيت پردازش ديتا و اطلاعات انتقالي به سازمان را افزايش مي دهد.اين سرويس ها حملات امنيتي را شمارش كرده و مكانيسم امنيتي بيشتري را فراهم مي كند.

همانطور كه ميدانيم ، امنيت اطلاعات درباره چگونگي ممانعت از تقلب يا اختلال مي باشد و همچنين در مورد شناسايي تقلب ها در اطلاعات پايه اي سيستم كه در آن جا اطلاعات تنها معني حضور فيزيكي نمي دهد.

جدول زير تعدادي از بيشترين مثال هاي تقلب يا جعل را نشان ميدهد. هركدام از آنها برخاسته از مثال هاي دنياي زير زمينی هكرها ميباشد:

1.دستيابي غير مجاز به اطلاعات
2.وارد شدن به جاي كاربر ديگري، خواه براي دستيابي به مسئوليت ديگران خواه براي استفاده از گواهي ديگران براي اهداف زير:

a.بدست آوردت اطلاعات

b.ایجاد اطلاعات تقلبی و کاربرهای جدید

c.استفاده از هويت هاي تقلبي براي دست يافتن به امكانات غيرمجاز

d.انتقالات تقلبي به ظاهر مجاز و شناسايي آن ها

3.رد مسئولیت یا اعتماد به اطلاعات ریشه یابي شده توسط متقلب.

4.تأييدي كه از سوي ديگر كاربران ايجادشده كه متقلبان آن را ايجاد كرده اند (مسئولیت ها و اعتمادهاي تقلبي , مثال:شما امضای الکترونیکی شرکتی را بدست اورده باشید)

5.تأييدي كه بايد در زمان مشخصي به شخصي فرستاده شود اما فرستاده نشود يا در زمان متفاوتي فرستاده شود.

6.رد دريافت اطلاعاتي كه در واقع دريافت شده است يا تأييد در زمان اشتباه

7.بزرگنمايي گواهي مجاز متقلب (براي دسترسي، ريشه يابي) و بخش و غيره....

8.اصلاح اطلاعات ديگران بدون مجوز مجاز (متقلب) نقش ديگران را بازي كرده و محدوديت هاي گواهي ها را كم يا زياد مي كند.

9.عوض کردن اطلاعات

10.خود را در لینک ها ارتباطي ميان ديگر كاربران به عنوان نقطه قابل اعتماد فعال جا زدن.

11.پیگیری اطلاعات رد و بدل شده در شبکه

12.عيب جويي از اطلاعات كامل پروتكل با آشكارسازي اطلاعاتي كه متقلب توسط پروتكل ها مخفي نگه داشته(آناليز ديتا ها)

13.منحرف كردن عملكرد نرم افزار نوعاً توسط ديگر عملكردهاي اضافي

14.مسبب مختل سازي پروتكل ها توسط معرفي اطلاعات غلط از طريق ديگران

15.پايين آوردن سطح اعتماد در پرووتكل از طريق ايجاد شكست هاي آشكار در سيستم

16.ممانعت از برقراري ارتباط در پروتكل ميان كاربران علي الخصوص تداخل هايي كه سبب ارتباط هاي به ظاهر صحيح مي شوند. مانند ارتباطات غيرقابل اعتماد كه رد مي شوند.

بهترين روش براي مشاهده حملات دقت روي عملكرد سيستم كامپيوتر يا شبكه در طول آماده سازي اطلاعات است.

چهار دسته از حملات

وقفه: زمانيكه سيستم از بين مي رود يا غيرقابل دسترسي مي شود، حمله روي دسترسي انجام شده. مثال ها شامل از بين رفتن قسمتي از سخت افزار مثل هارد، حذف خط ارتباط يا غيرفعالسازي فايل مديريت سيستم مي شوند.

بريدگي: دسترسي غيرمجاز است كه حمله بحرمانگي سيستم صورت گرفته. گروه غيرمجاز ميتواند يک شخص، يک برنامه يا يک كامپيوتر باشد. مي توان به دست آوردن سيم ها براي جمع آوري اطلاعات در يک شبكه يا كپي غيرمجاز يک فايل يا يک برنامه در اين زمينه اشاره كرد.

دستكاري: دسترسي غيرمجاز در اين مرحله همراه با مداخله صورت مي گيرد. اين حمله ايست كه روي تماميت سيستم صورت مي گيرد. مثال ها شامل تغيير ارزش در يک فايل اطلاعات، تغيير

برنامه به نحوي كه به صورت ديگري عمل كند و تغييرات در محتوي پيام در حال انتقال در شبكه است.

تقليد و جعل: افراد غيرمجاز چيزهاي جعلي را وارد سيستم مي كنند. اين حمله روس صحت و سندیت صورت مي گيرد، مانند وارد كردن پيام هاي جعلي در شبكه يا اضافه كردن ركوردهايي به فايل.

(البته به زبان عاميانه اينطور بيان ميشوند ! ولی در اصطلاح به حالت اول Down شدن سيستم , به حالت دوم ايجاد يک کاربر جديد , حالت سوم ويرايش اطلاعات و دزدی هويت)

حمله هاي فعال و غيرفعال

حملات کامپيوتری بسيار زياد هستند ولی کل حمله ها زير مجومه اين دو نوع ميباشند!

حمله هاي غيرفعال (Passive) كه براي به دست آوردن اطلاعات انتقالي صورت مي گيرد، به نوعي استراق سمع يا مشاهده انتقال اطلاعات به حساب مي آيد انواع مختلفی دارد:

1. آشكارسازي محتوای پيام:

به آساني قابل تشخيص است. يک مكالمه تلفني، يک پيام الكترونيكي، و يا يک فايل انتقالي هركدام مي توانند شامل اطلاعات مهمي باشند كه ما خواهان جلوگيري از فاش شدن محتوي آن در طول انتقال براي حريف هستيم.

2. آناليز ترافيک شبكه:

بسيار ماهرانه تر انجام مي شود. اگر ما بتوانيم به طريقي اطلاعات و محتوي پيام را پنهان كنيم؛ حتي اگر پيام توسط حريف كسب

شود، قابليت نشان دادن اطلاعات و محتوي پيام به او را ندارد.
معمول ترين راه مقابله رمزنگاري است که در اين صورت نيز حريف مي تواندااطلاعاتي از قبيل مبدأ، مقصد، اندازه پيام و بعضي اطلاعات ديگر را که ممکن است براي او مفيد باشد را به دست آورد.
نتيجه: حمله هاي غيرفعال به جهت آن که هيچگونه تغييراتي در اطلاعات انجام نمي دهد، به راحتي قابل تشخيص نيستند و در اين حالت ممانعت از حمله واجب تر از تشخيص حمله است.

حمله های فعال (Active)

شامل تغييرات در اطلاعات و ايجاد اطلاعات غلط مي باشد که چهار گروه وانمودکردن، تکرار، تغيير پيام ، و انکار سرويس و خدمات مي باشد.

1. وانمود کردن به حمله:

زماني صورت مي گيرد که چيزي تظاهر به چيز ديگري بودن مي کند. اين حمله معمولاً همراه با فرم ديگري از حمله صورت مي گيرد. براي مثال سکانس سنديت پس آن که عمليات معتبري روي آن صورت گرفت به دست آورده شده و تکرار مي شود؛ دادن امتياز مجاز باعث مي شود که وي امتياز بالاتري کسب کند.

2. تکرار:

اطلاعات غيرفعال را به دست مي آورد و متعاقب آن اطلاعات بعدي را کسب مي کند تا تأثير و تغيير غيرمجاز را حاصل کند.

3. تغيير پيام:

كسري از پيام مجاز تغيير داده مي شود تا تأثيرات غيرمجاز صورت پذيرد. مثلاً پيامي كه به معني " اجازه دهيد John Smith فايل حساب ها را بخواند" مي باشد، به "اجازه دهيد Joe Deb فايل جساب ها را بخواند" تغيير پيدا مي كند.

4. انكار سرويس:

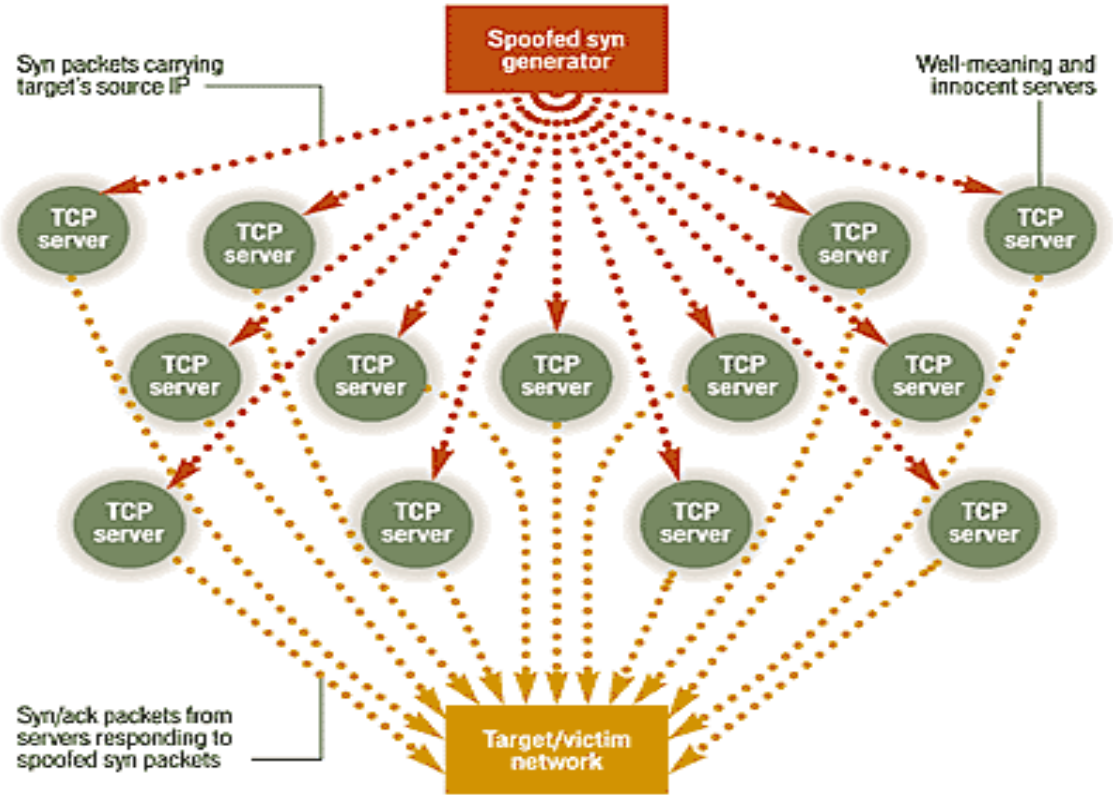
از كاربردهاي معمول يا مديريت ارتباطات وامكانات جلوگيري مي كند.ممكن است هدف خاصي در بر داشته باشد؛ مثلاً شخصي تمام پيام هاي فرستاده شده به مقصد معيني را پنهان مي كند(سرويس بازرسي امنيتي). فرم ديگري از انكار سرويس قطع تمام شبكه است كه مي تواند با غيرفعال سازي شبكه يا لبريز شدن آن با پيام ها به نحوي كه عملكرد آن را پايين آورد، صورت گيرد.

حملات فعال متفاوت با حملات غيرفعال رفتار مي كنند.

اگرچه حمله هاي غيرفعال به سختي قابل تشخيص هستند، معيارهايي براي جلوگيري از موفقيت آنها وجود دارد.حمله هاي فعال كاملاً به سختي قابل جلوگيري هستند. زيرا نياز به محافظت كامل از تمام امكانات و راه هاي ارتباطي در تمام زمان ها دارد. در مقابل هدف تشخيص و بازيابي تمام خسارت ها و تغييرات ايجاد شده توسط حمله ها است. تشخيص تأثيري مانع شونده دارد و از حمله جلوگيري مي كند.

حملات عدم پذیرش سرویس(DOS)

در یک تهاجم از نوع DoS ، یک مهاجم باعث ممانعت دستیابی کاربران تائید شده به اطلاعات و یا سرویس های خاصی می نماید یک مهاجم با هدف قرار دادن کامپیوتر شما و اتصال شبکه ای آن و یا کامپیوترها و شبکه ای از سایت هائی که شما قصد استفاده از آنان را دارید ، باعث سلب دستیابی شما به سایت های Email ، وب سایت ها ، accountهای online و سایر سرویس های ارائه شده بر روی کامپیوترهای سرویس دهنده می گردد .
تهاجم از نوع DoS حملاتي مي‌باشند که در آن مهاجم با ارسال درخواست‌های گسترده به یک کارگزار، آن را مشغول کرده و از انجام فعالیت‌های عادی و رسیدگی به درخواست‌های واقعی باز می‌دارد و در نتیجه باعث ازکارافتادگی و به اصطلاح خوابیدن سرویس می‌شود. این حملات انواع مختلف دارند و بر علیه سرویس‌هاي مختلفی مانند وب, سرویس‌هاي اشتراکي و DNS صورت مي‌گیرند.



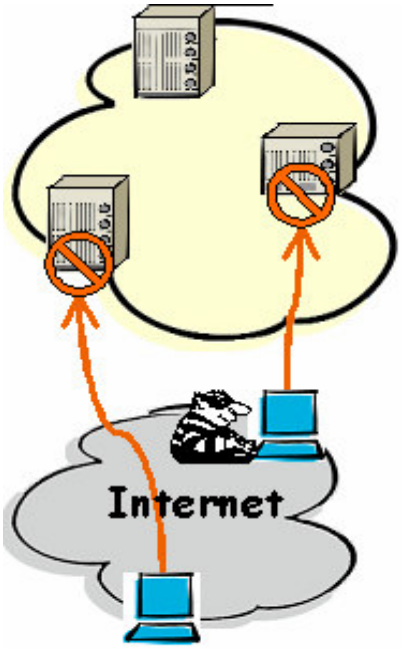
اين نوع حمله مي‌تواند به صورت توزيع شده نيز صورت گيرد. در اين حالت يك شبكه حمله ايجاد شده و حمله توسط تمام اعضاي اين شبكه صورت مي‌گيرد. اين شبكه به اين صورت ايجاد مي‌گردد كه مهاجم اقدام به كشف كامپيوترهايي كه از نظر امنيتي ضعيف مي‌باشند مي‌نمايد و بر روي آن‌ها برنامه‌هايي نصب مي‌كند كه مي‌توان آن‌ها را از طريق شبكه كنترل نمود و براي حمله مورد استفاده قرار داد. هدف از این پروژه، ابداع و طراحی یک حمله‌ی DoSجدید و پیاده‌سازی آن است.
هدف از حمله هاي DoS ايجاد اختلال در منابع يا سرويس هايي است كه كاربران قصد دستيابي و استفاده از آنها را دارند(از كار انداختن سرويس ها)
مهمترين هدف اين نوع حمله ها جلوگيري از دسترسي به يک منبع خاص است. در اين نوع حمله مهاجمان با به كارگيري روش هاي متعدد تلاش مي كند كه كاربران مجاز به دستيابي و استفاده از يک سرويس خاص را دچار مشكل نمايند.

- تلاش در جهت ايجاد ترافيک كاذب در شبكه
- اختلال در ارتباط ميان 2 ماشين
- ممانعت از دستيابي كاربرمجاز به سرويس
-ايجاد اختلال در سرويس

متداولترین و مشهودترین نوع حملات DoS ، زمانی محقق می گردد که یک مهاجم اقدام به ایجاد یک سیلاب اطلاعاتی(وقتی که دیتای زیادی در شبکه در حاله انتقال باشد در یک شبکه نماید. زمانی که شما آدرس URL یک وب سایت خاص را از طریق مرورگر خود تایپ می نمائید ، درخواست شما برای سرویس دهنده ارسال می گردد . سرویس دهنده در هر لحظه قادر به پاسخگوئی به حجم محدودی از درخواست ها می باشد، بنابراین اگر یک مهاجم

با ارسال درخواست های متعدد و سیلاب گونه باعث افزایش حجم عملیات سرویس دهند گردد ، قطعا" امکان پردازش درخواست شما برای سرویس دهنده وجود نخواهد داشت. حملات فوق از نوع DoS می باشند، چراکه امکان دستیابی شما به سایت مورد نظر سلب شده است .

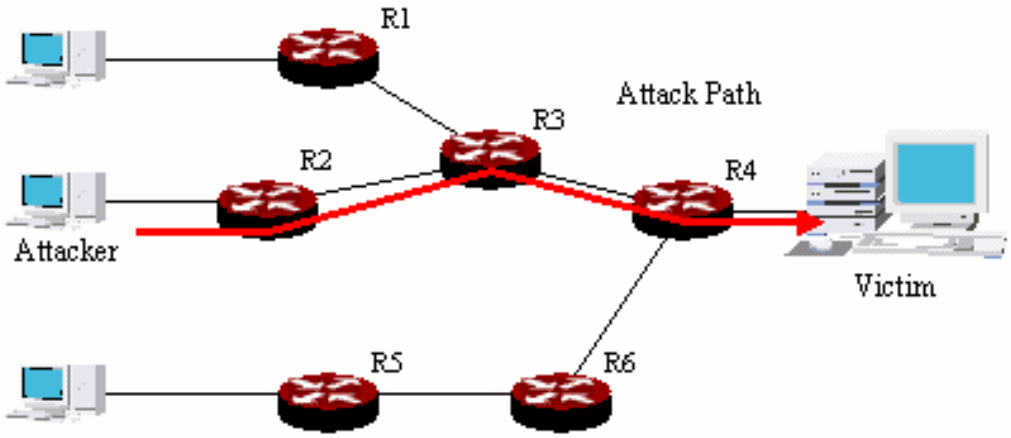
یک مهاجم می تواند با ارسال پیام های الکترونیکی ناخواسته که از آنان با نام Spam یاد می شود ، حملات مشابهی را متوجه سرویس دهنده پست الکترونیکی نماید . هر account پست الکترونیکی (صرفنظر از منبعی که آن را در اختیار شما قرار می دهد ، نظیر سازمان مربوطه و یا سرویس های رایگانی نظیر یاهو دارای ظرفیت محدودی می باشند.) پس از تکمیل ظرفیت فوق ، عملا" امکان ارسال Email دیگری به account فوق وجود نخواهد داشت . مهاجمان با ارسال نامه های الکترونیکی ناخواسته سعی می نمایند که ظرفیت account مورد نظر را تکمیل و عملا" امکان دریافت email های معتبر را از account فوق سلب نمایند.



DOS Attacks

این نوع حمله(DOS) باعث از کارافتادن یا مشغول شدن بیش از اندازه کامپیوتر می شود تا حدی که غیرقابل استفاده می شود. در بیشتر موارد، حفره های امنیتی محل انجام این حملات است و لذا نصب آخرین وصله های امنیتی از حمله جلوگیری خواهند کرد.
شایان گفتن است که علاوه بر اینکه کامپیوتر شما هدف یک حمله DoS قرار می گیرد، ممکن است که در حمله DoS علیه یک سیستم دیگر نیز شرکت داده شود.
نفوذگران با ایجاد ترافیک بی مورد و بی استفاده باعث می شوند که حجم زیادی از منابع سرویس دهنده و پهنای باند شبکه مصرف یا به نوعی درگیر رسیدگی به این تقاضاهای بی مورد شود و این تقاضا تا جایی که دستگاه سرویس دهنده را به زانو در آورد ادامه پیدا می کند. نیت اولیه و تأثیر حملات DoS جلوگیری از استفاده صحیح از منابع کامپیوتری و شبکه ای و از بین بردن این منابع است. علیرغم تلاش و منابعی که برای ایمن سازی علیه نفوذ و خرابکاری مصروف گشته است، سیستم های متصل به اینترنت با تهدیدی واقعی و مداوم به نام حملات DoS مواجه هستند.

DoS Attack



این امر بدلیل دو مشخصه اساسی اینترنت است:

1. منابع تشکیل دهنده اینترنت به نوعی محدود و مصرف شدنی هستند.

زیرساختار سیستم ها و شبکه های بهم متصل که اینترنت را می سازند، کاملاً از منابع محدود تشکیل شده است. پهنای باند، قدرت پردازش و ظرفیت های ذخیره سازی، همگی محدود و هدف های معمول حملات DoS هستند. مهاجمان با انجام این حملات سعی می کنند با مصرف کردن مقدار قابل توجهی از منابع در دسترس، باعث قطع میزانی از سرویس ها شوند. وفور منابعی که بدرستی طراحی و استفاده شده اند ممکن است عاملی برای کاهش میزان تاثیر یک حمله DoS باشد، اما شیوه ها و ابزار امروزی حمله حتی در کارکرد فراوان ترین منابع نیز اختلال ایجاد می کند.

2. امنیت اینترنت تا حد زیادی وابسته به تمام عوامل است.

حملات DoS معمولاً از یک یا چند نقطه که از دید سیستم یا شبکه قربانی عامل بیرونی هستند، صورت می گیرند. در بسیاری موارد، نقطه آغاز حمله شامل یک یا چند سیستم است که از طریق سوءاستفاده های امنیتی در اختیار یک نفوذگر قرار گرفته اند و لذا حملات از سیستم یا سیستم های خود نفوذگر صورت نمی گیرد. بنابراین، دفاع برعلیه نفوذ نه تنها به حفاظت از اموال مرتبط با اینترنت کمک می کند، بلکه به جلوگیری از استفاده از این اموال برای حمله به سایر شبکه ها و سیستم ها نیز کمک می کند.

پس بدون توجه به اینکه سیستم هایتان به چه میزان محافظت می شوند، قرار گرفتن در معرض بسیاری از انواع حمله و مشخصاً

DoS ، به وضعیت امنیتی در سایر قسمت های اینترنت بستگی زیادی دارد.

هدف بسیاری از حملات، ایجاد اخلال و وقفه در سرویس‌دهی یک ماشین در شبکه است. هدف مهاجم از این حملات وارد کردن ضربات اقتصادی یا سیاسی یا خدشه‌دار کردن اعتبار یک گروه، سازمان یا یک شبکه اطلاع‌رسانی است. از نظر نتیجه‌ي حمله، حملات DoS بُعد دسترس‌پذیریِ امنیت را خدشه‌دار می‌سازند. ولی از نظر آسیب‌پذیری مورد استفاده، ممکن است از آسیب‌پذیری‌های گوناگونی استفاده نمایند .

حملات DoS از نظر فنی به دو دسته تقسیم می‌شوند:

1. منع خدمت از طریق ارسال داده‌های مخرب و فرآیند[3] .این دسته از حملات از نقطه ضعف‌های موجود در نرم‌افزار بهره می‌گیرند .
2. اشباع منابع سیستم :در این روش مهاجم به گونه‌ای منابع سیستم را تلف می‌کند و سیستم دیگر نمی‌تواند به کاربران مجاز سرویس دهد. برای مثال حمله‌ی (SYN Flood) نمونه‌ای از این نوع حملات است.

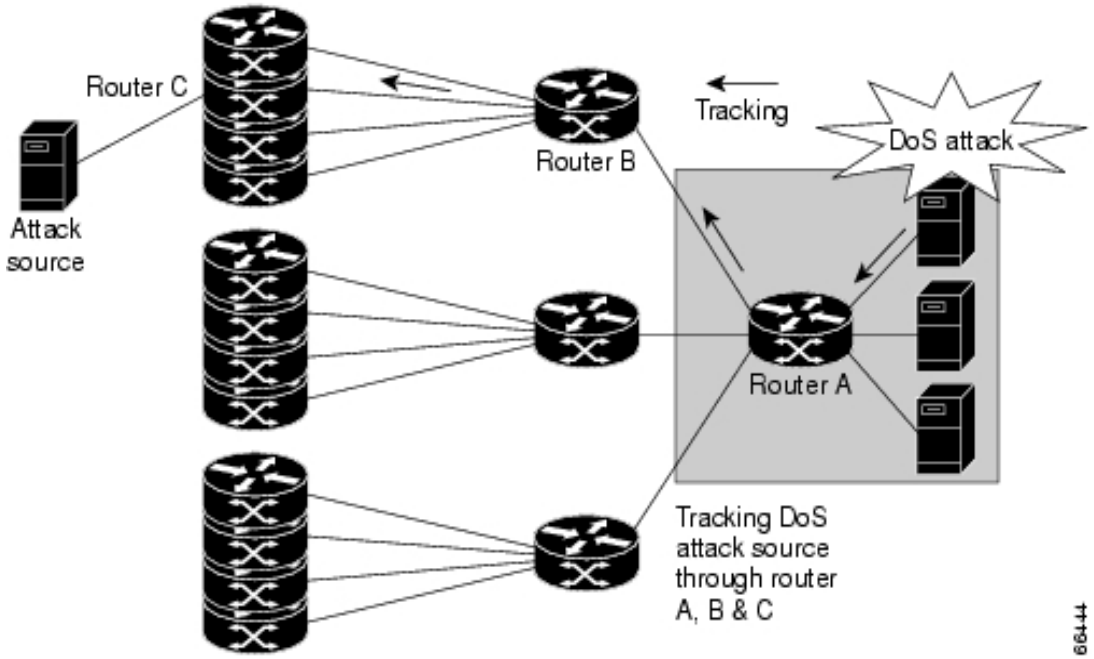
تاکنون راه‌حل‌های جامعی برای حملات DoS ارائه نشده است ولی می‌توان با به روز رسانی نرم‌افزارها، فیلتر کردن ترافیک ناخواسته و محدود کردن منابع کاربران تا حد زیادی با این حملات مقابله کرد .

مقابله با حملات DoS تنها یک بحث عملی نیست. محدودکردن میزان تقاضا، فیلترکردن بسته ها و دستکاری پارامترهای نرم افزاری در بعضی موارد می تواند به محدودکردن اثر حملات DoS کمک کند، اما بشرطی که حمله DoS در حال مصرف کردن تمام منابع موجود نباشد.

در بسیاری موارد، تنها می توان یک دفاع واکنشی داشت و این در صورتی است که منبع یا منابع حمله مشخص شوند. استفاده از جعل آدرس IP در طول حمله و ظهور روش های حمله توزیع شده و ابزارهای موجود یک چالش همیشگی را در مقابل کسانی که باید به حملات DoS پاسخ دهند، قرار داده است.

تکنولوژی حملات DoS اولیه شامل ابزار ساده ای بود که بسته ها را تولید و از «یک منبع به یک مقصد» ارسال می کرد. با گذشت زمان، ابزارها تا حد اجرای حملات از «یک منبع به چندین هدف»، «از چندین منبع به هدف های تنها» و «چندین منبع به چندین هدف»، پیشرفت کرده اند.

امروزه بیشترین حملات گزارش شده به CERT/CC مبنی بر ارسال تعداد بسیار زیادی بسته به یک مقصد است که باعث ایجاد نقاط انتهایی بسیار زیاد و مصرف پهنای باند شبکه می شود. از چنین حملاتی معمولاً به عنوان حملات طغیان بسته (Packet flooding) یاد می شود. اما در مورد «حمله به چندین هدف» گزارش کمتری دریافت شده است.



انواع بسته ها (Packets) مورد استفاده برای حملات طغیان بسته ، در طول زمان تغییر کرده است، اما چندین نوع بسته معمول وجود دارند که هنوز توسط ابزار حمله DoS استفاده می شوند.

1. طغیان های TCP: رشته ای از بسته های TCP با پرچم های (flag) متفاوت به آدرس IP قربانی فرستاده می شوند. پرچم های SYN، ACK و RST بیشتر استفاده می شوند.

2. طغیان های تقاضا\پاسخ ICMP (مانند طغیان های ping): رشته ای از بسته های ICMP به آدرس IP قربانی فرستاده می شود.
3. طغیان های UDP: رشته ای از بسته های UDP به آدرس IP قربانی ارسال می شوند.

از آنجا که حملات طغیان بسته های دیتا معمولاً تلاش می کنند منابع پهنای باند و پردازش را خلع سلاح کنند، میزان بسته ها و حجم دیتای متناظر با رشته بسته ها عوامل مهمی در تعیین درجه موفقیت حمله هستند.
بعضی از ابزارهای حمله خواص بسته ها را در رشته بسته ها بدلایلی تغییر می دهند:

1. **آدرس IP منبع :**

در بعضی موارد، یک آدرس IP منبع ناصحیح، (روشی که جعل IP نامیده می شود) برای پنهان کردن منبع واقعی یک رشته بسته استفاده می شود.
در موارد دیگر، جعل IP هنگامی استفاده می شود که رشته های بسته به یک یا تعداد بیشتری از سایت های واسطه

فرستاده می شوند تا باعث شود که پاسخ ها به سمت قربانی ارسال شود.
مثال بعدی در مورد حملات افزایش بسته است (مانند smurf و fraggle)

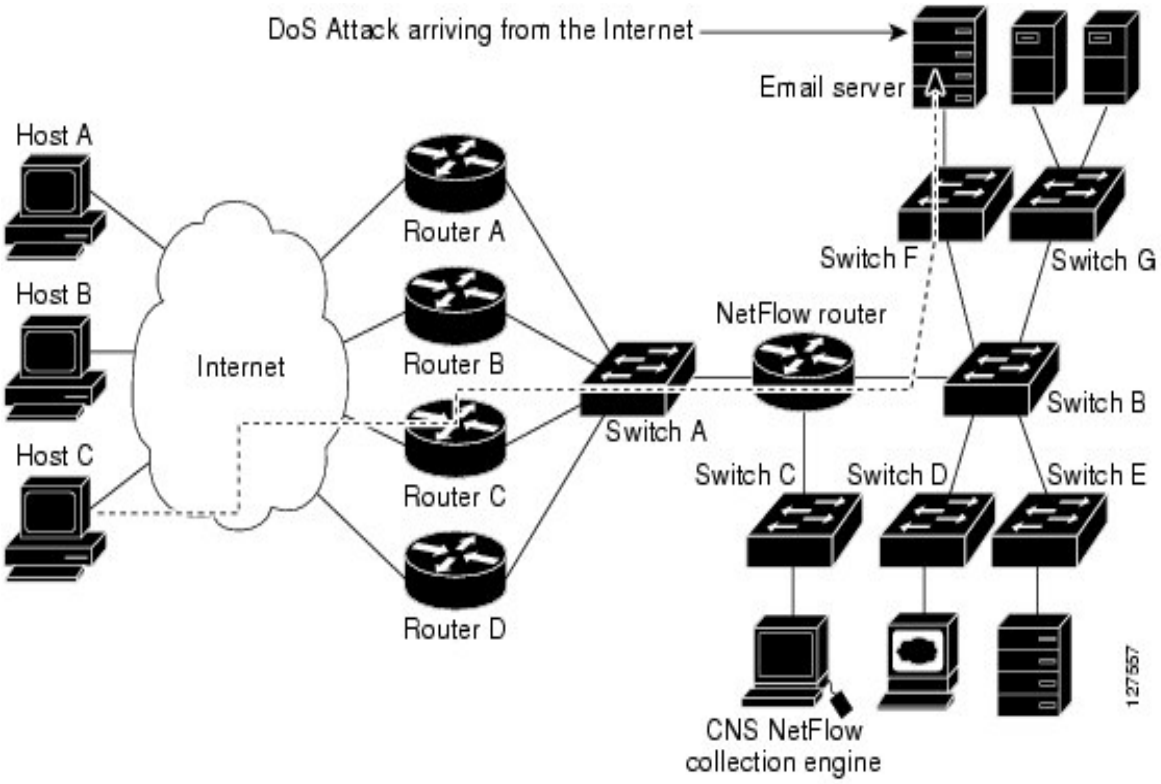
2. پورتهای منبع\مقصد:

ابزار حمله طغیان بسته بر اساس TCP و UDP ، گاهی اوقات پورت منبع و یا مقصد را تغییر می دهند تا واکنش توسط فیلتر کردن بسته را مشکل تر کنند.

3. مقادیر IP Header دیگر :

در نهایت در ابزار حمله DoS مشاهده کرده ایم که برای مقداردهی تصادفی، مقادیر Header هر بسته در رشته بسته ها طراحی شده اند که تنها آدرس IP مقصد است که بین بسته ها ثابت می ماند.

بسته ها با خواص ساختگی بسادگی در طول شبکه تولید و ارسال می شوند. پروتکل TCP/IP به آسانی مکانیزم هایی برای تضمین پیوستگی خواص بسته ها در هنگام تولید و یا ارسال نقطه به نقطه بسته ها ارائه نمی کند.
معمولاً، یک نفوذگر فقط به داشتن اختیار کافی روی یک سیستم برای بکارگیری ابزار و حملاتی که قادر به تولید و ارسال بسته های با خواص تغییریافته باشند، نیاز دارد.
ژوئن ۱۹۹۹، آغاز بکارگیری ابزار DoS با چندین منبع یا DDos (Distributed DoS) بود.



انواع حمله DoS

در این قسمت به یک تقسیم بندی کلی درباره انواع حملات DoS می پردازیم:

حملات عدم پذیرش سرویس به شش دسته تقسیم میشود:

Smurf.1
Fraggle.2
Syn Flood.3
Ping Of Death.4
DNS.5
Land.6

Smurf/Snurfing

حملات smurf یک از مخرب ترین حملات DoS هستند.

در حمله Smurf (حمله براساس ازدیاد بسته های ICMP)، نفوذگر یک تقاضای اکوی ICMP (ping) به یک آدرس ناحیه می فرستد.

آدرس منبع تقاضای اکو، آدرس IP قربانی است. (از آدرس IP قربانی بعنوان آدرس برگشت استفاده می شود). بعد از دریافت تقاضای اکو، تمام ماشین های ناحیه پاسخ های اکو را به آدرس IP قربانی می فرستند. در این حالت قربانی هنگام دریافت طغیان بسته های با اندازه بزرگ از تعداد زیادی ماشین، از کار خواهد افتاد.

حمله Smurf برای ازکار انداختن منابع شبکه سیستم قربانی از روش مصرف پهنای باند استفاده می کند. این حمله این عمل را با استفاده از تقویت پهنای باند نفوذگران انجام می دهد. اگر شبکه تقویت کننده ۱۰۰ ماشین دارد، سیگنال می تواند ۱۰۰ برابر شود، و بنابراین حمله کننده با پهنای باند پایین (مانند مودم ۵۶ کیلوبیتی) می تواند سیستم قربانی را با پهنای باند بیشتری (مانند اتصال T1) از کار بیندازد.

این نوع حمله ها بر تابع replay مربوط به پروتکل ICMP (Internet Control Message Protocol) بوده و بیشتر با تابع Ping شناخته شده اند.در این نوع حمله ها مهاجم اقدام به ارسال بسته هاي اطلاعاتي Ping به آدرس Broadcast شبکه نموده که در آن آدرس مبدأ هريک از بسته هاي اطلاعاتي Ping شده با آدرس کامپيوتر قرباني جايگزين مي شود.

بدين ترتيب يک ترافيک کاذب در شبکه ايجاد و امکان استفاده از منابع شبکه با اختلال مواجه مي شود.

Fraggle:

اين نوع حمله شباهت زيادي به حمله نوع Smurf دارد. تنها تفاوت موجود به استفاده ازUDP (User Datagram Protocol) بر مي گردد. در حمله فوق بسته اطلاعاتي UDP به مقصد پورت 7 (Echo) و يا پورت 19 (Charger) هدايت مي گردد.

حمله Fraggle (تقویت بسته UDP) در حقیقت شباهت هایی به حمله Smurf دارد. حمله Fraggle از بسته های اکوی UDP بر طبق همان روش بسته های اکوی ICMP در حمله Smurf استفاده می کند. Fraggle معمولاً به ضریب تقویت کمتری نسبت به Smurf می رسد، و در بیشتر شبکه ها اکوی UDP سرویسی با اهمیت کمتر نسبت به اکوی ICMP است، بنابراین Fraggle عمومیت Smurf را ندارد.

SYN Flood

در این نوع حمله از امتیاز Three-way handshake مربوط به TCP استفاده مي گردد. سيستم مبدأ بدون آن كه Ack(Acknowledge) نهايي آن ها را بفرستد، اقدام به ارسال مجموعه اي گسترده از درخواست هاي Syn مي نمايد.
حمله طغیان SYN قبل از کشف حمله Smurf بعنوان مخرب ترین شیوه حمله DoS بشمار می رفت. این روش برای ایجاد حمله DoS بر اساس قحطی منابع عمل می کند.
در طول برقراری یک ارتباط معمولی TCP، سرویس گیرنده یک تقاضای SYN به سرویس دهنده می فرستد، سپس سرور با یک ACK/SYN به کلاینت پاسخ می دهد، در نهایت کلاینت یک ACK نهایی را به سرور ارسال می کند و به این ترتیب ارتباط برقرار می شود.
اما در حمله طغیان SYN، حمله کننده چند تقاضای SYN به سرور قربانی با آدرس های منبع جعلی بعنوان آدرس برگشت، می فرستد. آدرس های جعلی روی شبکه وجود ندارند. سرور قربانی سپس با ACK/SYN به آدرس های ناموجود پاسخ می دهد. از آنجا که هیچ آدرسی این ACK/SYN را دریافت نمی کند، سرور قربانی منتظر ACK از طرف کلاینت می ماند.

ACK هرگز نمی رسد، و زمان انتظار سرور قربانی پس از مدتی به پایان می رسد. اگر حمله کننده به اندازه کافی و مرتب تقاضاهای SYN بفرستد، منابع موجود سرور قربانی برای برقراری یک اتصال و انتظار برای این ACKهای در حقیقت تقلبی مصرف خواهد شد.
این منابع معمولاً از نظر تعداد زیاد نیستند، بنابراین تقاضاهای SYN جعلی حتی با تعداد نسبتاً کم می توانند باعث وقوع یک حمله DoS شوند.

Ping Flood یا Ping of death:

در این نوع حمله با ارسال مستقیم درخواست Ping به کامپیوتر قرباني سعي مي گردد كه سرويس ها بلاک و یا فعالیت آن ها كاهش يابد. در اين نوع حمله اندازه بسته هاي اطلاعاتي به حدي زياد (بالاي 64K كه در Ping غير مجاز) مي شودكه كامپيوتر قرباني قادر به برخورد مناسب با آميختن بسته هاي اطلاعاتي نيست و مختل مي شود.

حملات DNS

در نسخه های اولیه BIND (Berkely Internet Name Domain)، حمله کنندگان می توانستند بطور مؤثری حافظه نهان یک سرور DNS را که در حال استفاده از عملیات بازگشت برای جستجوی یک ناحیه بود که توسط این سرور سرویس داده نمی شد، مسموم کنند. زمانی که حافظه نهان مسموم می شد، یک کاربر قانونی به سمت شبکه مورد نظر حمله کننده یا یک شبکه ناموجود هدایت می شد. این مشکل با نسخه های جدیدتر BIND برطرف شده است. در این روش حمله کننده اطلاعات DNS غلط که می تواند باعث تغییر مسیر درخواست ها شود، ارسال می کند.

Land:

در این حمله مهاجمان اقدام به ارسال بسته اطلاعاتي TCP- IP Synchronization که داراي آدرس و پورت هاي مبدأ و مقصد يكسان هستند؛ مي نمايد و بدين ترتيب با ايجاد يک لوپ که مبدا و مقصد یکسانی دارد قربانی را زیر بار مصنوعی مختل میکند.

ضعف ادوات سیسکو در مقابل حملات DoS

حملات DoS روترها و سایر ادوات IOS که از سرورهای Sequre SSH (Shell) برای مدیریت از راه دور استفاده می‌کنند را مورد حمله قرار می دهد.حمله کنندگان می توانند به شیوه های مختلف از این نقطه ضعف استفاده کنند که می‌تواند شامل نفوذ به حافظه و ارسال دستوراتی که باعث دو باره بار شدن روتر می شوند باشد.این مشکل ادوات IOS که نسخه 2 SSH را اجرا می کنند را تهدید می کند.

در مشکل دوم هکرها با ارسال بسته های اطلاعاتی خاصی به یک روتر که معروف به پیغامهای کلید تبادل اینترنت Internet Key (Exchange) IKE هستند و تحت عنوان سرور Easy VPN پیکربندی شده است، به منابع شبکه دسترسی می یابند.

این مشکل فقط ادواتی را که بر اساس IOS کار می‌کنند و در حال اجرایEasy VPN Servers Ios هستند را تحت تا ثیر قرار می دهد.

لازم به ذکر است که شرکت سیسکو نرم افزارهایی را به منظور برطرف کردن این دو مشکل منتشر ساخته است.

حملات از نوع DDoS (distributed denial-of-service)

حملات DDoS (Distributed Denial of Service) حمله گسترده ای از DoS است. در اصل DDos حمله هماهنگ شده ای برعلیه سرویس های موجود در اینترنت است. در این روش حملات DoS بطور غیرمستقیم از طریق تعداد زیادی از کامپیوترهای هک شده بر روی کامپیوتر قربانی انجام می گیرد. سرویس ها و منابع مورد حمله ، «قربانی های اولیه» و کامپیوترهای مورد استفاده در این حمله «قربانی های ثانویه» نامیده می شوند. حملات DDoS عموماً در از کار انداختن سایت های کمپانی های عظیم از حملات DoS مؤثرتر هستند.

در یک تهاجم از نوع DDoS ، یک مهاجم ممکن است از کامپیوتر شما برای تهاجم بر علیه کامپیوتر دیگری استفاده نماید . مهاجمان با استفاده از نقاط آسیب پذیر و یا ضعف امنتیی موجود بر روی سیستم شما می توانند کنترل کامپیوتر شما را بدست گرفته و در ادامه از آن به منظور انجام عملیات مخرب خود استفاده نمایند.

ارسال حجم بسیار بالائی داده از طریق کامپیوتر شما برای یک وب سایت و یا ارسال نامه های الکترونیکی ناخواسته برای آدرس های Emailخاصی ، نمونه هائی از همکاری کامپیوتر شما در بروز یک تهاجم DDOS می باشد .

حملات فوق ، "توزیع شده " می باشند ، چراکه مهاجم از چندین کامپیوتر به منظور اجرای یک تهاجم DoS استفاده می نماید.

انواع حملات DDoS

عموماً حملات DDoS به سه گروه Trinoo، TFN/TFN2K و Stecheldraht تقسیم می شوند.

Trinoo

Trinoo در اصل از برنامه های Master/Slave است که با یکدیگر برای یک حمله طغیان UDP بر علیه کامپیوتر قربانی هماهنگ می شوند. در یک روند عادی، مراحل زیر برای برقراری یک شبکه Trinoo DDoS واقع می شوند:

مرحله۱: حمله کننده، با استفاده از یک میزبان هک شده، لیستی از سیستم هایی را که می توانند هک شوند، گردآوری می کند. بیشتر این پروسه بصورت خودکار از طریق میزبان هک شده انجام می گیرد. این میزبان اطلاعاتی شامل نحوه یافتن سایر میزبان ها برای هک در خود نگهداری می کند.

مرحله۲: به محض اینکه این لیست آماده شد، اسکریپت ها برای هک کردن و تبدیل آنها به اربابان(Masters) یا شیاطین (Daemons) اجراء می شوند. یک ارباب می تواند چند شیطان را کنترل کند. شیاطین میزبانان هک شده ای هستند که طغیان UDP اصلی را روی ماشین قربانی انجام می دهند.

مرحله۳: حمله DDoS هنگامی که حمله کننده فرمانی به میزبانان Master ارسال می کند، انجام می گیرد. این اربابان به هر شیطانی دستور می دهند که حمله DoS را علیه آدرس IP مشخص شده در فرمان آغاز کنند و با انجام تعداد زیادی حمله DoS یک حمله DDoS شکل می گیرد.

TFN/TFN2K

TFN (Tribal Flood Network) یا شبکه طغیان قبیله ای، مانند Trinoo، در اصل یک حمله Master/Slave است که در آن برای

طغیان SYN علیه سیستم قربانی هماهنگی صورت می گیرد.
شیاطین TFN قادر به انجام حملات بسیار متنوع تری شامل طغیان ICMP، طغیان SYN و حملات Smurf هستند، بنابراین TFN از حمله Trinoo پیچیده تر است.
TFN2K نسبت به ابزار TFN اصلی چندین برتری و پیشرفت دارد. حملات TFN2K با استفاده از جعل آدرس های IP اجرا می شوند که باعث کشف مشکل تر منبع حمله می شود. حملات TFN2K فقط طغیان ساده مانند TFN نیستند.
آنها همچنین شامل حملاتی می شوند که از شکاف های امنیتی سیستم عامل ها برای بسته های نامعتبر و ناقص سوءاستفاده می کنند تا به این ترتیب باعث از کار افتادن سیستم های قربانی شوند. حمله کنندگان TFN2K دیگر نیازی به اجرای فرمان ها با وارد شدن به ماشین های مخدوم (Client) (به جای Master در TFN) ندارند و می توانند این فرمان ها را از راه دور اجراء کنند. ارتباط بین Clientها و Daemonها دیگر به پاسخ های اکوی ICMP محدود نمی شود و می تواند روی واسط های مختلفی مانند TCP و UDP صورت گیرد. بنابراین TFN2K خطرناک تر و همچنین برای کشف کردن مشکل تر است.

Stacheldraht

کد Stacheldraht بسیار شبیه به Trinoo و TFN است، اما Stacheldraht اجازه می دهد که ارتباط بین حمله کننده و Masterها (که در این حمله Handler نامیده می شوند) رمزنگاری شود؛ عامل ها می توانند کد خود را بصورت خودکار ارتقاء دهند، می توانند اقدام به انواع مختلفی از حملات مانند طغیان های ICMP، طغیان های UDP و طغیان های SYN کنند.

نحوه پیشگیری از حملات

متاسفانه روش موثری به منظور پیشگیری در مقابل یک تهاجم DoSو یا DDoS وجود ندارد . علیرغم موضوع فوق ، می توان با رعایت برخی نکات و انجام عملیات پیشگیری ، احتمال بروز چنین حملاتی (استفاده از کامپیوتر شما برای تهاجم بر علیه سایر کامپیوتر ها) را کاهش داد.

نصب و نگهداری نرم افزار آنتی ویروس (جایگاه نرم افزارهای ضدویروس. (نصب و پیکربندی یک فایروال)

چگونه از وقوع حملات آگاه شویم ؟

خرابی و یا بروز اشکال در یک سرویس شبکه ، همواره بدلیل بروز یک تهاجم DoS نمی باشد . در این رابطه ممکن است دلایل متعددی فنی وجود داشته و یا مدیر شبکه به منظور انجام عملیات نگهداری موقتا" برخی سرویس ها را غیر فعال کرده باشد . وجود و یا مشاهده علائم زیر می تواند نشاندهنده بروز یک تهاجم از نوع DoSو یا DDoS باشد :

کاهش سرعت و یا کارآئی شبکه بطرز غیر معمول (در زمان باز نمودن فایل ها و یا دستیابی به وب سایت ها.)
عدم در دسترس بودن یک سایت خاص (بدون وجود دلایل فنی)
عدم امکان دستیابی به هر سایتی (بدون وجود دلایل فنی)
افزایش محسوس حجم نامه های الکترونیکی ناخواسته دریافتی

در صورت بروز یک تهاجم ، چه عملیاتی را می بایست انجام داد ؟
حتی در صورتی که شما قادر به شناسائی حملات از نوع DoS و یا

DDoSباشید ، امکان شناسائی مقصد و یا منبع واقعی تهاجم ، وجود نخواهد داشت . در این رابطه لازم است با کارشناسان فنی ماهر ، تماس گرفته تا آنان موضوع را بررسی و برای آن راهکار مناسب را ارائه نمایند .

در صورتی که برای شما مسلم شده است که نمی توانید به برخی از فایل ها ی خود و یا هر وب سایتی خارج از شبکه خود دستیابی داشته باشید ، بلافاصله با مدیران شبکه تماس گرفته و موضوع را به اطلاع آنان برسانید . وضعیت فوق می تواند نشاندهنده بروز یک تهاجم بر علیه کامپیوتر و یا سازمان شما باشد.

دفاع علیه حملات Smurf و Fraggle

اگر در معرض حمله Smurf قرار گرفته باشید، کار چندانی از شما ساخته نیست. هرچند که این امکان وجود دارد که بسته های مهاجم را در روتر خارجی مسدود کنید، اما پهنای باند منشاء آن روتر مسدود خواهد شد. برای اینکه فراهم کننده شبکه بالاسری شما، حملات را در مبداء حمله مسدود کند، به هماهنگی نیاز است.
بمنظور جلوگیری از آغاز حمله از سایت خودتان، روتر خارجی را طوری پیکربندی کنید که تمام بسته های خارج شونده را که آدرس مبداء متناقض با زیرشبکه شما دارند، مسدود کند. اگر بسته جعل شده نتواند خارج شود، نمی تواند آسیب چندانی برساند.
برای جلوگیری از قرار گرفتن بعنوان یک واسطه و شرکت در حمله DoS شخص دیگر، روتر خود را طوری پیکربندی کنید که بسته هایی را که مقصدشان تمام آدرس های شبکه شماست، مسدود کند. یعنی، به بسته های ICMP منتشر شده به شبکه خود، اجازه عبور از روتر ندهید.

این عمل به شما اجازه می دهد که توانایی انجام ping به تمام سیستم های موجود در شبکه خود را حفظ کنید، در حالیکه اجازه این عمل را از یک سیستم بیرونی بگیرید.
اگر واقعاً نگران هستید، می توانید سیستم های میزبان خود را طوری پیکربندی کنید که از انتشارهای ICMP کاملاً جلوگیری کنند.

دفاع علیه حملات طغیان SYN

بلاک های کوچک

بجای تخصیص یک شیء از نوع ارتباط کامل (که باعث اشغال فضای زیاد و نهایتاً اشکال در حافظه می شود)، یک رکورد کوچک (micro-record) تخصیص دهید.
پیاده سازی های جدیدتر برای SYN های ورودی ، تنها ۱۶ بایت تخصیص می دهد.

کوکی های SYN

یک دفاع جدید علیه طغیان SYN «کوکی های SYN» است. در کوکی های SYN، هر طرف ارتباط، شماره توالی (Sequence Number) خودش را دارد.
در پاسخ به یک SYN، سیستم مورد حمله واقع شده، یک شماره توالی مخصوص از ارتباط ایجاد می کند که یک «کوکی» است و سپس همه چیز را فراموش می کند یا بعبارتی از حافظه خارج می کند (کوکی بعنوان مشخص کننده یکتای یک تبادل یا مذاکره استفاده می شود).
کوکی در مورد ارتباط اطلاعات لازم را در بردارد، بنابراین بعداً می تواند هنگامی که بسته ها از یک ارتباط سالم می آیند، مجدداً اطلاعات فراموش شده در مورد ارتباط را ایجاد کند.

کوکی های RST

جایگزینی برای کوکی های SYN است، اما ممکن است با سیستم عامل های ویندوز 95 که پشت فایروال قرار دارند، مشکل ایجاد کند. روش مذکور به این ترتیب است که سرور یک ACK/SYN اشتباه به کلاینت ارسال می کند.
کلاینت باید یک بسته RST تولید کند تا به سرور بگوید که چیزی اشتباه است.
در این هنگام، سرور می فهمد که کلاینت معتبر است و ارتباط ورودی از آن کلاینت را بطور طبیعی خواهد پذیرفت.
پشته های (stack) های TCP بمنظور کاستن از تأثیر طغیان های SYN می توانند دستکاری شوند.
معمول ترین مثال کاستن زمان انقضاء (timeout) قبل از این است که پشته، فضای تخصیص داده شده به یک ارتباط را آزاد کند.
تکنیک دیگر قطع بعضی از ارتباطات بصورت انتخابی است.

دفاع علیه حملات DNS

دفاع از سرور اصلی (root server)

پایگاه داده سرور اصلی کوچک است و بندرت تغییر می کند. یک کپی کامل از پایگاه داده اصلی تهیه کنید، روزی یک بار آپدیت ها را چک کنید و گاه و بیگاه بارگذاری های مجدد انجام دهید.
از سرورهای اصلی با استفاده از آدرس های anycast استفاده کنید (این عمل باعث می شود که سیستم ها در شبکه های با موقعیت های مختلف بعنوان یک سرور بنظر برسند.)

دفاع از خود در مقابل نفوذ ها

اگر سازمان شما یک اینترانت دارد، باید دسترسی های جداگانه ای از DNS برای کاربران داخلی و مشتریان خارجی خود فراهم کنید. این عمل DNS داخلی را از حملات خارجی در امان نگاه می

دارد. ناحیه اصلی را کپی کنید تا سازمان خود را از حملات DDoS آتی روی قسمت های اصلی محفوظ نگه دارید.
همچنین به کپی کردن نواحی DNS از شرکای تجاری خود که در خارج از شبکه شما قرار دارند، توجه کنید.
هنگامی که بروز رسان های DNS به روی اینترنت می روند، می توانند در هنگام انتقال مورد ربایش و دستکاری قرار گیرند.
از TSIGها (transaction signature) یا امضاهای معاملاتی برای امضای آن ها یا ارسال بروز رسان ها روی VPN (شبکه های خصوصی مجازی) یا سایر کانال ها استفاده کنید.

مقابله با حملات DDoS

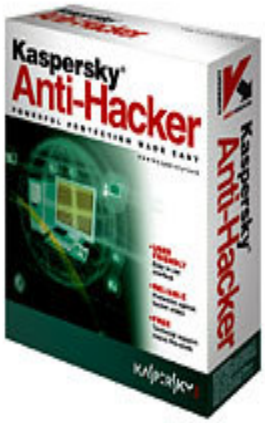
چگونه می توانید از سرورهای خود در مقابل یورش دیتاهای ارسالی از طرف کامپیوترهای آلوده موجود در اینترنت مراقبت کنید تا شبکه شرکت شما مختل نشود؟ در اینجا به چند روش بطور مختصر اشاره می شود:

سیاه چاله

این روش تمام ترافیک را مسدود می کند و به سمت سیاه چاله! یعنی جایی که بسته ها دور ریخته می شود هدایت می کند.
اشکال در این است که تمام ترافیک – چه خوب و چه بد- دور ریخته می شود و در حقیقت شبکه مورد نظر بصورت یک سیستم off-line قابل استفاده خواهد بود. در روش های اینچنین حتی اجازه دسترسی به کاربران قانونی نیز داده نمی شود.

مسیریاب ها و فایروال ها

روتر ها می توانند طوری پیکربندی شوند که از حملات ساده ping با فیلترکردن پروتکل های غیرضروری جلوگیری کنند و می توانند آدرس های IP نامعتبر را نیز متوقف کنند.
بهرحال، روترها معمولاً در مقابل حمله جعل شده پیچیده تر و حملات در سطح Application با استفاده از آدرس های IP معتبر، بی تأثیر هستند.



تامین امنیت سیستم با دیوار آتش قدرتمند Kaspersky :: Anti-Hacker 1.8.180

شرکت Kaspersky که با عرضه ي ویروس کش قدرتمند خود به یکي از برترین شرکت هاي تولید کننده ي نرم افزارهاي امنیتي تبدیل گشته است , علاوه بر ویروس کش دیوار آتش قدرتمند دیگري با نام **Kaspersky Anti-Hacker** را نیز داراست . این محصول امنیت سیستم شما را در مقابل حملات و خطرهاي اینترنتي که باعث پخش ویروس در سیستم و دزدیده شدن اطلاعات و بسیاري حملات دیگر تامین مي نماید و به گفته ي سایت سازنده به هکرها نه مي گوید ! این نرم افزار بسیاري از حملات DOS و Ping of Death و Land, Helkern, Lovesan attacks and SMBDie و ... را جلوگیري به عمل مي آورد . کنترل هر نرم افزار و فایلي که مي خواهد از سیستم شما به اینترنت متصل شود را به شما مي دهد . از ارسال و دریافت Packet ها جلوگیري به عمکل مي آورد و همچنین با مخفي نمودن سیستم شما در

اينترت احتمال شناسايي شدن آن را توسط هكرها به حد اقل مي رساند ! اين ديوار آتش قدرتمند با ويندوز هاي 98, , ME,NT 4.0 2000 و XP سازگاري كامل دارد .

سیستم های کشف نفوذ

روش های سیستم های کشف نفوذ (intrusion detection systems) توانایی هایی ایجاد می کند که باعث تشخیص استفاده از پروتکل های معتبر بعنوان ابزار حمله می شود. این سیستمها می توانند بهمراه فایروال ها بکار روند تا بتوانند بصورت خودکار در مواقع لزوم ترافیک را مسدود کنند. در بعضی مواقع سیستم تشخیص نفوذ نیاز به تنظیم توسط افراد خبره امنیتی دارد و البته گاهی در تشخیص نفوذ دچار اشتباه می شود.

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 ... .

(راجبه این سیستم ها مقاله کاملی نوشته شده است میتوانید با مراجعه به سایت Hack-er.cjb.net مقاله مورد نظر را دریافت کنید)

سرورها

پیکربندی مناسب applicationهای سرویس دهنده در به حداقل رساندن تأثیر حمله DDoS تأثیر بسیار مهمی دارند. یک سرپرست شبکه می تواند بوضوح مشخص کند که یک application از چه منابعی می تواند استفاده کند و چگونه به تقاضاهای کلاینت ها پاسخ دهد. سرورهای بهینه سازی شده، در ترکیب با ابزار تخفیف دهنده، می توانند هنوز شانس ادامه ارائه سرویس را در هنگامی که مورد حمله DDoS قرار می گیرند، داشته باشند.

ابزار حفاضت در مقابل حملات DDoS

چندین شرکت ابزارهایی تولید می کنند که برای ضدعفونی ! کردن ترافیک یا تخفیف حملات DDoS استفاده می شوند که این ابزار قبلاً بیشتر برای متعادل کردن بار شبکه یا فایروالینگ استفاده می شد. این ابزارها سطوح مختلفی از میزان تأثیر دارند.

هیچکدام کامل نیستند.

بعضی ترافیک قانونی را نیز متوقف می کنند و بعضی ترافیک غیرقانونی نیز اجازه ورود به سرور پیدا می کنند.

زیرساخت سرور هنوز باید مقاوم تر شود تا در تشخیص ترافیک درست از نادرست بهتر عمل کند.

پهنای باند زیاد

خرید یا تهیه پهنای باند زیاد یا شبکه های افزونه برای سروکار داشتن با مواقعی که ترافیک شدت می یابد، می تواند برای مقابله با DDoS مؤثر باشد.عموماً، شرکت ها از قبل نمی دانند که یک حمله DDoS بوقوع خواهد پیوست.

طبیعت یک حمله گاهی در میان کار تغییر می کند و به این نیاز دارد که شرکت بسرعت و بطور پیوسته در طی چند ساعت یا روز، واکنش نشان دهد. از آنجا که تأثیر اولیه بیشتر حملات، مصرف کردن پهنای باند شبکه شماست، یک ارائه کننده سرویس های میزبان روی اینترنت که بدرستی مدیریت و تجهیز شده باشد، هم پهنای باند مناسب و هم ابزار لازم را در اختیار دارد تا بتواند تأثیرات یک حمله را تخفیف دهد.

مقاله دیگر تمام شود امیدوارم شما را با حملات بسیار جالب ☺ عدم پذیرش سرویس آشنا کرده باشم♥

دوباره تنها یک چیز میگویم: من یک کلاه سیاه نیستم ولی کلاه سیاه ها را دوست دارم..
دوستان دنیای مجازی ما هکرها دنیای بسیار بزرگی است ما هر چقدر هم از نظر درک علمی بالا باشیم نمیتوانیم بگویم به انتهای سایبر رسیده ایم پس تنها سعی ما کوشش برای نزدیک شدن به انتها است!!!

یه نفر خوابش میاد برای خواب جا نداره
یکی یه لقمه نون برای فردا نداره
یه نفر میشنه و اسکناساشو میشماره
می خواد ببینه تا زنده است داره یا نداره
یه نفر از بس بزرگه خونشون توش گم میشه
اون یکی خونشون برای خواب جا نداره
یکی دفترش پر از نقاشی خط خطیه
اون یکی مداد برای آب و بابا نداره
یکی ویلای کنار دریاشون قصره ولی
اون یکی حتی تو فکرش آب برای دریاش نداره


LOCKER
ROOM

!


Acrobat

©CopyRight®

Author: Satanic Soulful
E-Mail: Satanic.Soulful@GMail.Com
Satanic_Soulful@Yahoo.Com
Developed In:Satanic Digital Network Security ™
Special TNX 2 :Hell Hacker – Collector – S_hahroo_Z
Research By:5/-\t4N1C
©®Copyright For : Satanic Team 2005-2006
For More Information Go to Http://Hack-er.cjb.net/

©®All Right Reserved For Shabgard Security ™
Mr.XShabgardX
2005-2006 For More Information
Visit:Http://Shabgard.Org

My Deram Is All Day For Girl Is Dark&Ominous♀