عنوان مقاله : بررسی و روش های جلوگیری از حملات عدم پذیرش سرویس (DOS&DDOS) در سرور های لینوکس

چکیده

در سال های قبل با به وجود آمدن کامپیوتر ها ، نحوه دستیابی به صورت غیر مجاز به آن ها هر روز بیشتر می شد و با پیدایش سایت ها و سرور ها گسترش حملات به صورت قابل توجه ای افزایش یافت. با پیشرفته شدن کامپیوتر ها و افزایش پهنای باند در دنیای امروزی ، هکر ها از روش های مختلفی جهت حمله استفاده می کنند . شاید برای شما پیش آمده باشد هنگامی که وارد سایتی شده اید ، در صفحه اول سایت درج شده باشد که این سایت توسط افرادی هک شده است ، یا شاید وارد سایتی شده اید که سرعت سایت به شدت پایین بوده و اکثر اوقات سایت بالا نیامده و نمی تواند به شما سرویس دهد . در بیشتر مواقع این علائم نشان دهنده این است که شخص خاصی در حال حمله به سایت است و سرور را زیر نظر حمله قرار داده است. یکی از مخرب ترین نوع حملات ، حملات DoS (Denial of Service) که به آن حملات تکذیب سرویس نیز می گویند می باشد . این نوع حملات با استفاده از الگوریتم های خاص به صورت نرم افزاری در آمده و هکر از آن جهت حمله به سرویس مورد نظر استفاده میکند. به عنوان مثال شما میخواهید وارد یه خیابان شوید که در داخل آن ماشین هایی در حال رفت آمد می باشند. اگر عرض خیابان را منابع و پهنای باند در نظر بگیریم ، حال تصور کنید ماشین های زیادی به صورت عمدی وارد خیابان شوند ، در این صورت ماشین های عادی نمی توانند خیابان را طی نموده و به مقصد برسند و ترافیک بالا رخ می دهد . حملات DoS هم به همین صورت است. ترافیک بالا توسط هکر به سرور ارسال می شود و باعث می شود کاربران عادی نتوانند از منابع سایت استفاده کنند و سرعت سایت به شدت افت میکند و بعضی مواقع باعث از کار انداختن سرویس در نتیجه قطعی سایت به طور کامل خواهند شد. تشخیص ای نوع حملات روش های زیادی را شامل می شود و میتوان از هرکدام برای بهبود بخشید به امنیت سرور از آن استفاده کرد.

کلمات کلیدی: DoS،DDoS، حملات ، امنیت ، سایت ، شبکه

مقدمه :

قصد داریم تا در طی این مقاله به معرفی حملات DoS یا DDoS بپردازیم و شما را با این نوع حملات آشنا و روش های شناسایی و پیشگیری را در سرور های لینوکس معرفی و بررسی نماییم . این نوع حملات در عین سادگی بسیار مخرب هستند. به گونه ای که می توان با استفاده از ارسال ترافیک بالا و بی مورد به سرور کاری کرد که سرویس مورد نظر را به طور کامل قطع کرد. حملات DoS به این صورت است که با ارسال ترافیک بالا و بی مورد ، توسط یک سرور یا چندین سرور به سرور مورد نظر ، کل منابع سرور مورد نظر را مصرف کرده که این کار باعث از کار افتادن سرور مورد نظر می شود و کاربران نمی توانند وارد سایت شوند و از منابع سرور استفاده نمایند . پس با روش های شناسایی و پیشگیری می توان ترافیک های واقعی را از ترافیک های مخرب تشخیص داد و کاری کرد که ترافیک های واقعی و سالم به سرور هدایت شوند. شایان گفتن است حملات DoS مخصوص به وب سایت ها نمی باشند و می توان از آن ها جهت حمله به سرور های گیمینگ ، سرور های سازمانی با شبکه های داخلی و هر نوع سروری که در معرض دید هکر ها است استفاده نمود.

حمله DoS چیست؟

حملات DoS (Denial of Service) به حملاتی گفته می شود که هدف حمله کننده یا حمله کنندگان به دست آوردن اطلاعات شخصی کاربر نمی باشد بلکه هدف استفاده بیش از حد از منابع (پردازنده، پایگاه داده، پهنای باند، حافظه و...) می باشد به طوری که سرویس دهی عادی آن به کاربران دچار اختلال شده یا آن سرویس از دسترس خارج شود. این نوع حملات از سمت یک سرور حمله کننده به سمت سرور مورد نظر می باشد و در سرویس های مونیتورینگ معمولا فقط یک IP را نشان میدهد و آن IP ، IP سروری است که حمله را انجام داده است.

حمله DDoS چیست؟

حملات DDoS (Distributed Denial of Service) به حملاتی گفته می شوند که به صورت گسترده و به صورت هماهنگ از نقاط مختلف صورت می گیرد تا گروه حمله کننده تاثیر مخرب تری بر روی سرویس مورد نظر داشته باشند. این نوع حملات از سمت چندین سرور حمله کننده به صورت توزیع شده و همزمان به سمت سرور مورد نظر می باشد و در سرویس های مونیتورینگ معمولا چندید IP را نشان میدهد و آن IP ها ، IP های چندین سروی است که حمله را انجام داده است.

عمده حملات DDoS برای از کار انداختن سرویس های وب می باشد و بیشترین قربانی این گونه حملات بانک ها ، سرورهای میزبانی وب ، DNS Root Server ها و ... می باشند.

اهداف حمله

به طور کلی انجام این حمله برای اهداف زیر صورت می‌گیرد:

- ✓ پایین آوردن سرعت و کیفیت سرویس‌دهی شبکه (دسترسی به سایت یا انتقال فایل)
- ✓ از دسترس خارج کردن وب‌سایت مورد نظر
- ✓ قطع دسترسی تمام وب‌سایت‌ها (با حمله به name server ها)
- ✓ افزایش تعداد هرزنامه‌ها (که به بمب ایمیلی نیز معروف است)

لازم به ذکر است که این حمله فقط مختص به سرورها نیست و ممکن است یک شبکه و یا حتی روتر نیز مورد حمله قرار گیرد و ممکن است کار بخش عمده‌ای از اینترنت را مختل کند (همانطور که در طول تاریخ ۲بار اینترنت کل دنیا با این حمله مختل شده‌است).

انواع روش های حملات DDoS :

Buffer Overflow Attack

حمله سر ریز بافر هنگامی رخ می دهد که میزان اطلاعات نوشته شده در بافر بیش از میزان پیش بینی شده برای آن باشد. حمله کننده می تواند دیتای کنترل کننده مسیر اجرای برنامه را بازنویسی کرده و با سرقت و در دست گرفتن کنترل برنامه کدهای برنامه دلخواه خود را به جای پروسه های سرور به اجرا در آورد.

Ping of Death Attack

این شیوه که یکی از مشهورترین حملات دی داس قرن بیستم بوده است به طور کلی بلوکه شده و جلوی آن گرفته شده است. حمله کننده به عمد یک پاکت یا بسته IP بزرگتر از ۶۵۵۳۶ بایت را که توسط پروتکل IP مجاز شناخته می شود را ارسال می کند. در این پروتکل فایل در مبدا به بسته های اطلاعاتی خرد شده و پس از ارسال به کامپیوتر مقصد، بسته های اطلاعاتی در مقصد سر هم شده و بر روی کامپیوتر مقصد فایل دوباره ساخته می شود. اما سیستم عامل مقصد از عهده سر هم کردن پاکت های اطلاعاتی با اندازه بزرگتر از استاندارد که حمله کننده به صورت عمدی ساخته و ارسال کرده بود، بر نمی آمد و ری استارت می شد یا حتی به سادگی کرش می کرد.

Smurf Attack

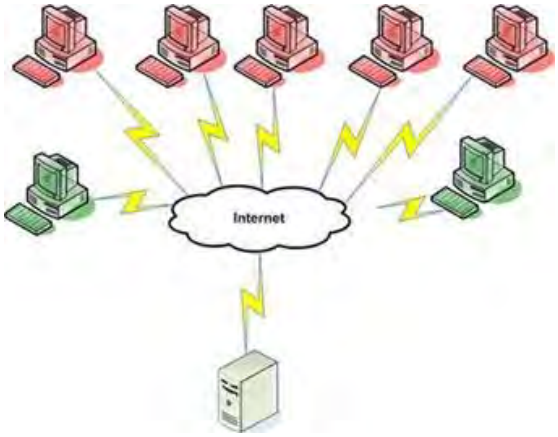
این روش حمله دی داس شیوه ای برای ایجاد یک ترافیک معنی دار و آزار دهنده بر روی شبکه کامپیوتری قربانی است. در این شیوه حمله کننده سیستم قربانی را با ارسال پیام های Ping قلابی غرق می کند . در این روش، حمله کننده تعداد بسیار زیادی ترافیک ICMP echo یا همان پینگ تولید می کند و آنها را از منابع ناشناس و قلابی به سمت هاست قربانی ارسال می کند. نتیجه هم تعداد فراوانی پاسخ پینگ است که باعث کند شدن و هنگ کردن سیستم قربانی می شود.

SYN Flood

حمله ی SYN Flood از مزایای پروتکل TCP در فرایند سه طرفه ی Handshake استفاده میکند . این روش به دو صورت مجزا انجام میشود . در هر دو روش مهاجم سعی میکند تا یک فرایند سه طرفه ی Handshake را اغاز کند ولی ان را به اتمام نرساند .

در روش اول مهاجم یک در خواست Synchronize یا هماهنگ سازی با یک IP جعلی ارسال میکند. وقتی که سرور سعی میکند که به درخواست پاسخ دهد و تاییده یا SYN-ACK را ارسال کند هیچ پاسخی دریافت نمیکند . در این صورت سرور هیچ وقت در خواست Acknowledge را دریافت نمیکند و آنSession ایجاد شده به صورت نیمه باز میماند وباعث هدر رفتن منابع سرور میشود .

در روش دوم مهاجم عمدا درخواست ACK را ارسال نمیکند . در هر دو روش، با منتظر گذاشتن سرور و سرگرداندن ان باعث از بین رفتن منابع ان میشوند . خوشبختانه این ضعف امنیتی مانند روش Ping of Death سال هاست در سخت افزار های جدید برطرف شده است .



Tear Drop

این حمله شامل ارسال قطعات پاکت های اطلاعاتی روی هم افتاده ای است که بزرگ تر از اندازه معمول هستند اما کاملا انباشته نشده اند. این بسته ها در سیستم عامل های مختلف به دلیل باگ های موجود در کد های دوباره سازی بسته های اطلاعاتی مرتبط با پروتکل TCP/IP، باعث کرش کردن سیستم می شوند.

Application Attack

این حملات طراحی شده اند برای هدف قرار دادن سرویس های خاصی مانند HTTP ، DNS و SIP Device ها و با ارسال ترافیک با حجم زیاد به سمت این سرور ها ، سرویس دهی آنها را دچار اخلال می نمایند. به این صورت ممکن چند ساعت یا چندین روز سرویس DNS از کار بیفتد ، با از کار افتدان سرویس DNS سایت به صورت کامل Down می شود و علاوه بر لود نشدن سایت ، ممکن است در سئوی سایت و میزان رتبه بندی آن در الکسا و پیج رنک پایین بیاید.

چه کسانی حمله DDoS را انجام می دهند؟

اصولا حمله های DDoS با انگیزه های متفاوت ممکن است توسط یک یا چند نفر و یا حتی گروهی از افراد صورت گیرد، اما آماری که تا به امروز به ثبت رسیده، حکایت از انگیزه های بیشتر فردی یا چند نفره داشته است، به طور مثال ممکن است افرادی برای از سر راه برداشتن ناجوانمردانه رقیبشان در وب، دست به این نوع اعمال بزنند تا مخاطبان آن سایت یا سرور دچار دلسردی شده و از آن فاصله بگیرند یا برعکس عده ای هکر، خیرخواهانه به سایتی ضد اجتماعی یا به فرض جنگ طلب حمله DDoS می کنند، لذا گستره افراد و انگیزه ها، بسته به نوع مورد، متفاوت خواهد بود، اما آنچه مسلم است معمولا انسان ها پشت این حملات هستند یا ترکیبی از اندیشه انسان و به کارگیری سیستم، سرور و ابزارهای خاص (DDoS tools) دست به دست هم می دهند تا یک حمله DDoS شکل بگیرد.

علائم حمله DDoS چیست؟

خوشبختانه یکی از موارد مثبت این نوع حملات این است که به سرعت می توان به نحوه عملکرد سرویس مشکوک شد و جلوی اختلال بیشتر را گرفت، پس از اینکه سروری مورد حمله DDoS قرار می گیرد ممکن است با توجه به اهداف و شیوه به کار رفته یک قسمت از منابع یا همه ی قسمت های آن دچار اختلال شود، در زیر لیستی از این علائم را ذکر می کنیم. کندی در پاسخگویی به درخواست هاسروری که مود حمله قرار گرفته باشد، معمولا خیلی کند و با وقفه به درخواست بارگذاری صفحات پاسخ می دهد، البته این نشانه همیشه دلیل حمله DDoS نیست، چرا که این اتفاق به طور طبیعی نیز برای سرورها و سایتهای با بازدید بالا ممکن است رخ دهد یا کنترل این امر بستگی زیادی به قدرت سخت افزاری سرور و تنظیمات آن دارد.عدم اتصال به پایگاه دادهگاهی ممکن است صفحات استاتیک که نیازی به اتصال پایگاه داده ندارند به راحتی بارگذاری شوند، ولی اتصال به پایگاه داده برای صفحات داینامیک برقرار نشود، در چنین مواقعی معمولا پیام تکمیل ظرفیت اتصال به پایگاه داده یا too many connection ظاهر خواهد شد، بهترین کار در چنین حالتی این است که با تنظیم یک دستور هِدر HTTP۵۰۰ ، به ربات های جستجوگر بگوییم که سایت ما فعلا دچار مشکلی است و بعدا مراجعه نمائید!، چرا که در غیر اینصورت با وجود down بودن دیتابیس سرور، ربات ها با دریافت وضعیتHTTP 200 ، صفحه خالی را ایندکس می کنند که این حالت اصلا مناسب نیست، در php این کار را با دستورات header می توان انجام داد.

```
header('HTTP/1.0 500 Internal Server Error');
```

مصرف بیش از حد منابع سروریکی دیگر از نشانه های حمله DDoS می تواند مصرف بیش از حد و غیر طبیعی منابع سرور مثل حافظه و یا پهنای باند در یک بازه زمانی کوتاه باشد.افزایش انفجاری درخواست هایکی دیگر از نشانه های حمله DDoS ، وجود شمار زیادی درخواست http به سرور است که با مشاهده فایل log و قسمت آمار، می توان به این موضوع پی

برد.اختلالات در سرویس های جانبی نظیر ایمیلگاهی مواقع حملات DDoS سرویس های جانبی یک سرور نظیر سرویس ایمیل را هدف می گیرند، در این مواقع ارسال و دریافت ایمیل ممکن است به کندی صورت گیرد یا دچار وقفه شود، البته همانطور که گفتیم، هر وقفه و اختلالی به معنی حمله DDoS نیست، تنها به عنوان یک نشانه می توان آن را محسوب کرد.

به طور خلاصه برخی از علائم حملات DDoS :

کند شدن وب سایت

عدم اتصال به پایگاه داده

مصرف بیش از حد منابع سرور

اختلال در سرویس Email

حمله DDoS چقدر طول می کشد؟

یکی از سوال های همیشگی در چنین موقعیت هایی این است که یک حمله DDoS چقدر طول می کشد و ظرف چه مدتی به پایان می رسد، پاسخ این سوال نیز می تواند یک جمله باشد: تا زمانی که به پایان رسد! این موضع بستگی به میزان سماجت مهاجم و ضعف مدافع دارد، یعنی اگر مهاجم بر ادامه حملات خود اصرار داشته باشد و در مقابل مدافع که همان مدیران سرور هستند نتوانند از عهده کنترل اوضاع بر آیند، ممکن است حمله DDoS ساعت ها یا روزها به طول انجامد، در خوش بینانه ترین حالت ظرف چند دقیقه و در بدترین حالت چندین و چند روز و به دفعات ممکن است طول بکشد.

حملات DDoS به چه صورتی انجام می شود :

همانطور که گفته شد حملات می توانند به صورت تکی یا گروهی انجام شوند. هیچ گاه هکر از اینترنت خود جهت حمله استفاده نمی کند ، زیرا لازم به سرعت بالای پهنای باند ، سرعت بالای سیستم و ترافیک خیلی بالای خطوط می باشد. پس هکر آن را از طریق یک سرور مجازی یا از طریق چندین سرور مجازی ، که سرعت بالایی دارند جهت حمله استفاده کرده و حمله خود را اغاز میکند و سرور تا زمانی که این حمله توسط فرد قربانی مورد نظر تشخیص و جلوگیری نشود ادامه خواهد داشت و ممکن است حتی چندین روز طول بکشد

روش های جلوگیری (به صورت کلی)

به طور کلی هیچ راه تضمین کننده‌ای برای جلوگیری از این حمله وجود ندارد و تنها راه‌هایی برای جلوگیری از برخی روش‌های متداول و کم کردن اثرات سایر روش‌ها موجوداست، چرا که بسیاری از روش‌ها به هیچ‌عنوان قابل پیشگیری نیست، به عنوان مثال اگر شبکه botnet با صدهزار zombie صفحه‌ای از سایت را باز کنند، این درخواست یک درخواست عادی بوده و نمی‌توان تشخیص داد که درخواست دهنده سیستم معمولی است یا zombie و به همین جهت نمی‌توان جلوی آن‌را گرفت. برای پاسخگویی به این حملات از SYN cookie استفاده می‌گردد. سرور با دریافت SYN Segmant به جای ایجاد یک connection نیمه باز یک TCP قرارداد هدایت انتقال و با ارسال SYN ACK آن را ارسال می‌کند. سپس تنها در صورت دریافت ACK به ایجاد connection و اختصاص منابع روی می‌آورد.استفاده از دیواره‌های آتش یکی از راه‌های متداول و بهترین راه جلوگیری است، البته استفاده از هر دیواره‌آتشی توصیه نمی‌شودو تنها دیواره‌های آتشی مناسبند که به هدف جلوگیری از DoS طراحی شده‌اند.استفاده از سوییچ و مسیریاب‌های مناسب که برخی دارای دیواره آتش و سیستم‌های تشخیص‌دهنده هستند نیز راه مناسبی است. همچنین درست تنظیم کردن سوییچ‌ها و مسیریاب‌ها (روترها) امری ضروری برای جلوگیری از بسیاری از انواع حمله‌است.استفاده از سیستم‌های تشخیص دهنده (IPS) سیستم‌های تشخیص براساس سرعت بسته‌ها (RBIPS) و اینگونه سیستم‌ها نیز روش مناسبی برای جلوگیری از این حملات است.بسته‌های نرم‌افزاری نیز موجودند که شامل تمام این سیستم‌ها هستند، استفاده از این بسته‌ها علاوه بر حملات DDoS بسیاری دیگر از حملات را شناسایی می‌کنند، بسته نرم‌افزاری SSP (Sun Security Package) از جمله این بسته‌ها است که کار شناسایی و جلوگیری را به صورت خودکار انجام می‌دهد.

اصلی ترین روش های جلوگیری حملات DoS/DDoS در سرور های لینوکس :

روش هایی که در زیر توضیح داده ایم اصلی ترین روش هایی است که هر مدیر سرور ضروری است به ترتیب الویت ها و میزان برقراری امنیت آن ها که در جدول مقایسه آمده است ، را در سرور های خود پیاده سازی کند.

۱- استفاده از سرویس های ابری incapsula و Defense.net وCloudFlare :

اساس کار این سرویس ها به این صورت است که با آنالیز کردن ترافیک ورودی به سایت و سرور ، باعث جلوگیری از ترافیک مخرب می شود و ترافیک سالم را به سایت و سرور هدایت می کند.

از میان این سرویس ها ما به سرویس CloudFlare اشاره میکنیم :

اساس کار این سرویس به این صورت است که با ثبت نام در سایت cloudflare و ثبت سایت خود ، DNS هایی که کلود فلر به ما ارائه میدهد را جایگزین DNS های دامنه خود می کنیم و تا ۲۴ ساعت صبر کنیم تا DNS های کلود فلر بر روی دامنه ما فعال شود. به این ترتیب هر بازدید کننده ای که وارد سایت ما می شود ابتدا به سرور های کلود فلر وصل شده و توسط کلود چک می شود که این کاربر چه نوع کاربری بوده و هدف او از آمدن به وب سایت چیست و سپس آن کاربر به سایت ما متصل می شود پس اگر هر گونه حمله ای از طرف کاربر رخ دهد توسط کلود فلر بلاک خواهد شد.

به طور کلی کلود فلر باعث جلوگیری و بلاک نمودن ترافیک مخرب میگردد و ترافیک سالم را به سایت ما هدایت میکند.

این سرویس در ۴ پلن عرضه می شود :

۱- Free

۲- Pro
۳- Business
۴- Enterprise

در پنل Free تا مقداری را میتوان جلوی حملات DDoS را گرفت ، اما در پنل Business و پرداخت ماهیانه ۲۰۰$ میتوان به صورت خیلی پیشرفته جلوی حملات DDoS گرفت.

آدرس سرویس کاود فلر : https://www.cloudflare.com

۲- استفاده از فایروال csf و iptables :

برای استفاده از فایروال csf حتما باید فایروال iptables بر روی سرور فعال باشد تا csf با استفاده از رول های iptables به درستی کار کند. اساس کار این فایروال ها به این صورت است که میتوان برای هر IP تعداد کانکشن را تعریف نمود و اگر تعداد کانکشن برای هر IP از حد مجاز بیشتر بود یعنی حمله DDoS رخ داده است و توسط فایروال ها بلاک خواهد شد. با استفاده از این از فایروال ها میتوان تا حد خیلی بالایی را جلوی حملات ddosرا گرفت.
نکته : اگر این فایروال ها به صورت خیلی خوب کانفیگ شوند می توان ۸۰٪ جلوی حملات DDoS را گرفت.

۳- استفاده از فایروال comodo waf یا owasp :

اساس کار این دو فایروال جلوگیری از حملاتی که مربوط به وب اپلیکیشن هستند می باشند. برای استفاده از آن ها فقط باید یکی از فایروال ها را در نظر گرفت و نمیتوان از هر دوی آنها استفاده نمود. با استفاده از این فایروال ها می توان تا حد بسیار معمولی را جلوی حملات ddos را گرفت.

۴- استفاده از سیستم‌هایی مانند Captcha برای دسترسی به نقاط مختلف سایت :

با استفاده از Captcha ، میتوان برای فرم های ورود یا هر نوع فرمی که به سرور و دیتابیس درخواستی رو ارسال می کند استفاده کرد. این روش تا حد خیلی کمی ، جلوی حملات ddos را میگیرد و نمی توان از انتظار چشم گیری داشته باشیم و حتی اگر این سیستم را در سایت به کار نبریم می توانیم با روش های دیگر جلوی حملات را بگیریم.

۵- فایروال سخت افزاری :

این روش بسیار پر هزینه بوده و بر عهده دیتاسنتر نیز می باشد و می بابیست فایروال را در کنار سرور نصب و به صورت کانفیگ شده پیاده سازی شود. اساس کار این فایروال شبیه به فایروال های نرم افزاری می باشد و مهمترین ویژگی این فایروال ها امنیت بالای آن می باشد که نمی توان به سادگی آن ها را غیر فعال نمود. این

نوع فایروال جلوگیری میکند از ترافیک های مخرب که وارد سرور شده و ترافیک های سالم را به سرور هدایت میکند.

۶- استفاده از سرویس های IDS/IPS :

تعریف IDS : سیستمی که بتواند حمله هایی که در لایه شبکه انجام می شود را شناسایی کند .
تعریف IPS : سیستمی که بتواند در هنگام کشف حملات ، جلوی آن را گرفت و حملات را بلاک کرد.
این دو سیستم بهتر است که در کنار هم پیاده سازی شوند زیرا هر کدام کار خاصی را انجام می دهند و به تنهایی هیچ کدام ، نمی توانند با حملات مقابله کنند.
این دو سیستم باید در دیتاسنتر مربوطه به صورت سخت افزاری و نرم افزاری در سطح لایه شبکه و کاربرد پیاده سازی شوند.

۷- نصب نرم افزار DDoS Deflate بر روی سرور :

روشی دیگر برای جلوگیری از حملات DDoS نصب و استفاده از نرم افزار DDoS Deflate می باشد. با کانفیگ صحیح این نرم افزار می توان به طور چشمگیری جلوی حملات DDoS را گرفت و ترافیک سالم به سایت و سرور هدایت نمود.

دستورات مفید :

نحوه نصب نرم افزار DDoS Deflate :

```
wget http://www.inetbase.com/scripts/ddos/install.sh
chmod 0700 install.sh
./install.sh
```

نحوه پاک کردن نرم افزار DDoS Deflate :

```
wget http://www.inetbase.com/scripts/ddos/uninstall.ddos
chmod 0700 uninstall.ddos
./uninstall.ddos
```

ویرایش فایل کانفیگ (برای انجام تنظیمات) :

```
nano /usr/local/ddos/ddos.conf
```

مشاهده تعداد اتصالات مربوط به هر کانکشن :

```
sh /usr/local/ddos/ddos.sh
```

نحوه ریستارت کردن نرم افزار :

```
sh /usr/local/ddos/ddos.sh -c
```

جدول مقایسه انواع روش ها از نظر جلوگیری از حملات DDoS :

نام روش	برقراری امنیت	پیاده سازی	هزینه	الویت	معایب
CloudFlare(free)	خوب	آسان	ندارد	خیلی بالا	کندی سرعت سایت در اولین اتصال
CloudFlare(bussiness)	خیلی عالی	آسان	ماهیانه ۲۰۰$	متوسط	کندی سرعت سایت در اولین اتصال
csf و iptables	عالی	سخت	ندارد	خیلی بالا	نیاز به دانش بالا جهت مدیریت و آشنایی با رول ها، در صورتی که به خوبی کانفیگ نشود باعث افت سرعت می شود
comodo waf وowasp	متوسط	آسان	ندارد	بالا	نداشتن پنل مونیتورینگ حملات DDoS
Captcha	کم	سخت	ندارد	خیلی کم	پیاده سازی سخت،کاربر پسند نیست، درجاهایی که واقعا نیاز بود باید پیاده سازی شود مثل (فرم ثبت نام)

Firewall Hardware	عالی	سخت	پر هزینه	کم	هزینه خیلی بالا، نیاز به برقراری امنیت فیزیکی، مدیریت بسیار سخت ، نیاز به آشنایی ، پیاده سازی سخت، در صورتی که به خوبی کانفیگ نشود باعث افت سرعت می شود
DDoS Deflate	خوب	متوسط	ندارد	بالا	نیاز به آشنایی ، مدیریت سخت ، نداشتن پنل مونتیورینگ کاربر پسند، در صورتی که به خوبی کانفیگ نشود باعث افت سرعت می شود
IDS/IPS	خوب	سخت	پر هزینه	کم	نیاز به آشنایی، مدیریت سخت ، پیاده سازی در دیتاسنتر، هزینه بالا، نیاز به برقرای امنیت فیزیکی

ادامه :

نام روش	مزایا
CloudFlare(free)	کش کردن سایت و بالا رفتن سرعت سایت بعد از اولین اتصال
CloudFlare(bussiness)	کش کردن سایت و بالا رفتن سرعت سایت بعد از اولین اتصال، قابلیت های پیشرفته برای حملات ddos ، دارابودن پنل مونیتورینگ کاربران،بلاک کردن آی پی ها در رنج یک کشور، بهینه سازی نسخه موبایل برای وب سایت
csf و iptables	کارایی بسیار بالا در عین رایگان بودن ، در سرعت لود شودن سرور و سایت تاثیری ندارد، عملکرد خوب روی تمامی توزیع های لینوکس، دارا بودن تنظیمات خیلی پیشرفته
comodo waf وowasp	محیط کاربر پسند و به صورت خیلی آسان تنها با کلیک کردن
Captcha	علاوه بر حملات DDoS ، جلوی حملات اسپم را به صورت خیلی عالی میگیرد، جلوگیری از ارسال bot ها
Firewall hardware	دارا بودن پنل مدیریت خیلی پیشرفته جهت آنلایز کل ترافیک ورودی
DDoS Deflate	کارایی بسیار بالا در عین رایگان بودن ، عملکرد خوب روی تمامی توزیع های لینوکس ، دارا بودن تنظیمات خیلی پیشرفته
IDS/IPS	امنیت بالا، دارا بودن پنل مدیریت خیلی پیشرفته جهت آنالیز کل ترافیک ورودی به سرور و تشخیص حمله و مقابله با آن، دارا بودن ویژگی های بسیار بالا

روش هایی که ذکر شد جلوی بسیاری از حملات ddos را گرفته و ترافیک سالم را به سایت ما هدایت میکنند ولی همانطور که مستلزم هستید امنیت هیچ وقت ۱۰۰٪ نیست و امکان دارد هکر از روش هایی استفاده کند که با

هیچ کدوم از این روش ها نتوان جلوی آن را گرفت که با در نظر گرفتن این روش ها ، باید در نظر داشته باشیم که هر هکری نمی تواند به سرور حمله کند .

روش های شناسایی حملات DDoS :

علاوه بر روش هایی که می توان با سرویس های نظیر کلود فلر یا فایروال ها و لاگ فایل های آن ها و یا حتی پنل مدیریت فایروال های سخت افزاری و ... ، روش هایی نیز وجود دارد که اساسی ترین روش برای شناسایی حملات DDoS می باشد.یکی از پرکاربردترین دستورات برای شناسایی حملات DDoS فرمان netstats میباشد.این فرمان اطلاعاتی در رابطه با وضعیت تعداد کانکشن های شبکه دراختیارتان میگذارد .

اطاعاتی در رابطه با اینکه چه سرویسی برروی چه پورتی درحال Listening میباشد.

کد:

```
netstat -nlp
```

اطلاعات مربوط به مجموع اتصالات شبکه بر اساس وضعیت اتصال

کد:

```
netstat -nat | awk '{print $6}' | sort | uniq -c | sort -n
```

خروجی مانند زیر خواهد بود :

کد:

```
  CLOSE_WAIT 1
      1 CLOSING
      1 established
      1 Foreign
      4 LAST_ACK
      6 FIN_WAIT1
      6 SYN_RECV
      7 FIN_WAIT2
     29 ESTABLISHED
     44 LISTEN
     86 TIME_WAIT
```

اطلاعاتی در مورد وضعیت اتصالات یک ادرس IP خاص،خروجی مانند دستور قبلی خواهد بود،اما تنها مربوط به اتصالات یک ادرس IP

کد:

```
netstat -nat |grep {IP-address} | awk '{print $6}' | sort | uniq -c | sort -n
```

لیستی از آدرسهای IP متصل به سرور

کد:

```
netstat -nat | awk '{ print $5}' | cut -d: -f1 | sed -e '/^$/d' | uniq
```

مجموع آدرسهای IP متصل به سرور

کد:

```
netstat -nat | awk '{ print $5}' | cut -d: -f1 | sed -e '/^$/d' | uniq | wc -l
```

مشاهده ی تعداد اتصالات هر آدرس IP

کد:

```
netstat -atun | awk '{print $5}' | cut -d: -f1 | sed -e '/^$/d' |sort | uniq -c
| sort -n
```

مشاهده ی IP هایی که در حالت SYN_REC هستند.

کد:

```
netstat -n -p | grep SYN_REC | awk '{print $5}' | awk -F: '{print $1}'
```

هنگامی که مشاهده کردید که IP خاصی در حال حمله است ، میتوانید آن را به آسانی در فایروال Csf خود طبق کد زیر برای همیشه بلاک کنید :

```
Csf -d IP

Example : csf -d 127.0.0.1
```

و برای رفع بلاک کردن آی پی مورد نظر کد زیر را وارد کنید :

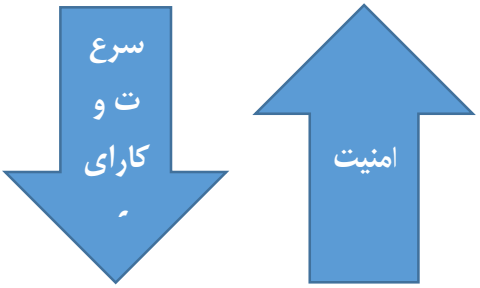
```
Csf -dr IP

Example : csf -dr 127.0.0.1
```

یا حتی میتوانید توسط سرویس های ابری نظیر کلود فلر آی پی یا رنج آپی مربوط به آن کشور را برای همیشه بلاک کنید.

به طور کلی میتوان به این صورت در نظر گرفت :

با افزایش امنیت به همان میزان ما افت سرعت و کارایی در وب سایت ها را خواهیم داشت ، پس باید همیشه به میزانی که واقعا نیاز است امنیت را در مقابل حملات DDoS بالا ببریم و در کنار آن با استفاده از سرویس های مونیتورینگ از صحت کاربران واقعی اطمینان حاصل نماییم و در صورتی که حمله ای رخ داد خیلی سریع جلوی آن را گرفته و آی پی های مربوطه را بلاک کنیم.



نتیجه گیری :

ما در این مقاله انواع روش های حملات ، روش های جلوگیری وشناسایی حملات را بررسی کردیم . به طور کلی میتوان در نظر گرفت که امنیت هیچ وقت ۱۰۰٪ نیست و هیچ وقت هم نباید به صورت ۱۰۰٪ در نظر بگیریم زیرا با افزایش امنیت کیفیت و کارایی سرور و سایت افت میکند . پس همیشه باید به یه میزان متوسط و تحلیل نیاز هایی که در پیش رو داریم امنیت را افزایش دهیم و در کنار به صورت ۲۴ ساعت سرور و سایت را مونیتورینگ کنیم و از هر نوع حمله آگاهی پیدا کنیم و در صورت رخ دادن هر نوع حمله ای جلوی آن را بگیریم . باید در نظر داشته باشیم ، همیشه حمله رخ می دهد و سپس روش های مقابله با آن منتشر خواهند شد . پس همیشه هکر ها از تیم امنیتی یک قدم جلوتر هستند . با مطالعه روز افزون مقالات و مشاهده باگ های نرم افزاری که در اینترنت منتشر خواهند شد می توان از انواع حملات آگاهی پیدا کرد و روش های مقابل با آن را تا قبل از اینکه حمله ای به سمت ما رخ دهد را بر روی سرور وسایت خود پیاده سازی کنیم .

منابع فارسی :

[1] http://blog.iranhost.com/10795/

[2]http://www.douran.com/DesktopModules/News/NewsView.aspx?TabID=1&Site=douranportal&Lang=fa-IR&ItemID=1865&mid=15223&wVersion=Staging

[3] http://centralvps.ir/articles/dos-ddos

منابع خارجی :

[1] https://www.cloudflare.com/ddos/

[2] https://panel.bullten.net/knowledgebase/4/Installing-DDoS-Deflate-To-Mitigate-DDoS-Attack.html

[3] http://www.hostdime.com/resources/csf-ssh-command-line-commands/

[4] https://en.wikipedia.org/wiki/Denial-of-service_attack

[5] Vrizlynn Thing Ling Ling , "Adaptive Response System for Distributed Denial-of-Service Attacks" , Ph.D. Thesis, College London, Aug 2008.

[6] B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE, "Distributed Denial of Service Prevention Techniques", April 2010.

[7] Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms",

funded by DARPA, University of Delaware and University of California, 2004.