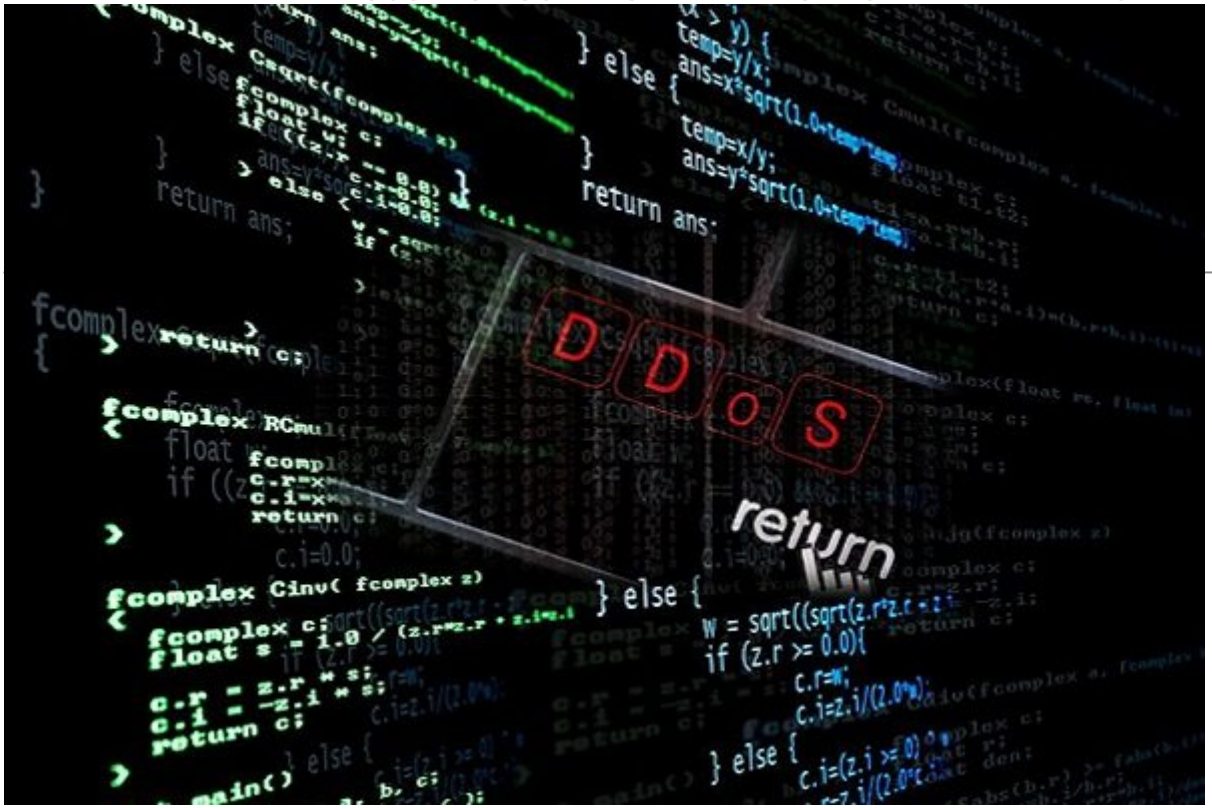
دفاع در برابر حمله منع سرویس انکار شده

راهکارهایی برای شناسایی و دفع حمله منع سرویس توزیع شده (DDoS)



پرسشی که اغلب از سوی مدیران امنیتی و وب‌مسترها مطرح می‌شود این است که ما چه زمانی می‌توانیم متوجه شویم زیرساخت‌های شبکه یا سایت تحت سرپرستی ما گرفتار یک حمله منع سرویس توزیع شده قرار گرفته است؟ برخی از سازمان‌ها سعی می‌کنند برای مقابله با این حمله از نیروی انسانی کمک گرفته و به شکل روزانه یا حتی ساعتی زیرساخت‌های خود را تحت نظارت قرار دهند. با وجود این کارآیی این تکنیک خیلی زیاد نیست. راهکار موثرتر دیگری که در این زمینه پیش روی شما قرار دارد به‌کارگیری سرویس‌های نظارتی قدرتمند است. سرویس‌هایی که به شکل خودکار و البته هوشمندانه منابع را مورد بررسی قرار دهند.

نظارت خودکار روی منابع به منظور شناسایی حملات منع سرویس توزیع شده به تیم امنیتی سازمان شما اجازه می‌دهد روی وظایف مهم‌تری متمرکز شده و اعلان‌های درست را در زمان مناسبی دریافت کنند. همچنین فراموش نکنید ابزارها و سرویس‌های نظارتی در اغلب موارد قادر هستند با ارائه راه‌حل‌هایی به مقابله با این حملات بپردازند. Arbor Networks که تقریبا 50درصد سهام بازار را در زمینه ارائه راهکارهای محافظت در برابر حملات منع سرویس توزیع شده در اختیار دارد، Radware که یک مکانیزم حفاظتی در برابر انواع مختلفی از حملات DDoS را ارائه می‌کند و Fortinet که محصولات متنوعی در ارتباط با ایمن‌سازی زیرساخت‌های فناوری اطلاعات ارائه می‌کنند، از جمله این موارد هستند.

حمله منع سرویس توزیع شده چیست؟

به‌طور خلاصه، یک حمله منع سرویس توزیع شده یک حمله سیل‌آسا بوده که ترافیک افسارگسیخته‌ای را به سمت هاست یا سرور روانه می‌کند. یک هکر می‌تواند ترافیک سنگینی را ارسال کند تا به سرعت پهنای باند و منابع سرور از دسترس خارج شوند. در این حالت سرور دیگر قادر نیست به درخواست‌ها رسیدگی کند. در این حالت ممکن است سرور دچار مشکل شده یا پهنای باند برای پاسخ‌گویی به درخواست‌های معتبر مشتریان وب‌سرویس شما در دسترس نباشد. همان‌طور که ممکن است حدس زده باشید تا زمانی که حمله ادامه پیدا کند خدمات‌رسانی متوقف می‌شود که این حرف به معنای از دست دادن درآمدهای مالی شما از سرویسی است که آن‌را ارائه کرده‌اید. حملات منع سرویس توزیع شده برای هر کسب‌وکار آنلاینی ویرانگر بوده و در هر ساعت از شبانه‌روز ممکن است رخ دهند. در نتیجه مهم است که بدانید این حمله چگونه عمل می‌کند و چطور باید آن‌را در کوتاه‌ترین زمان متوقف کنید. در مدت زمان بروز چنین حملاتی شما با یک منبع حمله‌کننده واحد سروکار ندارید تا با فیلتر کردن آدرس آی‌پی هکر حمله را متوقف کنید. هکرهایی که حملات منع سرویس توزیع شده را پیاده‌سازی می‌کنند در ابتدا سامانه‌های کاربران را آلوده می‌کنند. این سامانه‌ها می‌توانند کامپیوترهای شخصی، سامانه‌های توکار یا دستگاه‌های اینترنت اشیا باشند. در ارتباط با دستگاه‌های توکار و اینترنت اشیا هکرها به‌طور مستقیم به میان‌افزاری که وظیفه کنترل دستگاه را عهده‌دار است حمله می‌کنند. در ادامه هکرها از یک سامانه متمرکز که وظیفه ارسال دستورات را بر عهده دارد استفاده می‌کنند.

سامانه‌ای که به ماشین‌های آلوده به بدافزار اعلام می‌دارد ترافیک را به سمت یک سایت ارسال کنند. شدت یک حمله به تعداد ماشین‌هایی که یک هکر موفق شده است آن‌ها را آلوده کند بستگی دارد. به‌طور معمول، تعداد این کامپیوترها ممکن است 1000 عدد یا حتی فراتر از 10 هزار دستگاه برود. مکانیزم به‌کار گرفته شده در حملات منع سرویس توزیع شده در اغلب موارد پیچیده است. به‌طور مثال هکرها می‌توانند درخواست‌های اتصال ناقص را ارسال کرده که این مکانیزم باعث به وجود آمدن حالت انتظار می‌شود. در این تکنیک به‌طور مرتب درخواست‌های جدیدی ارسال می‌شود. شما در حالت عادی می‌توانید میزان ترافیکی را که از بابت یک حمله قادر به دفع آن هستید، محاسبه کنید. به‌طور مثال، اگر ترافیک عادی شما برابر با 100 ارتباط ورودی در یک لحظه بوده و سرور در این وضعیت قادر است به فعالیت‌های خود ادامه دهد، به معنای آن است که به احتمال زیاد ارتباط 100 ماشین روی ترافیک شما تاثیرگذار نخواهد بود. با این حال در یک حمله منع سرویس توزیع شده هزاران اتصال مبتنی بر آدرس‌های آی‌پی مختلف در یک زمان به سرور حمله می‌کنند. اگر سرور نتواند در یک لحظه 10 هزار ارتباط را مدیریت کند، به معنای آن است که شما در برابر یک حمله منع سرویس توزیع شده آسیب‌پذیر خواهید بود. (شکل یک) به عبارت دقیق‌تر در یک لحظه ممکن است صدها یا هزاران ماشین (سرور، کامپیوترهای شخصی یا حتی دستگاه‌های موبایل) ترافیک خود را به سمت شما گسیل کنند. در عرض چند دقیقه عملکرد سایت کاهش پیدا کرده و منابع هدر می‌روند. در این حالت کاربران عادی موفق نخواهند شد به سایت شما دسترسی پیدا کنند.

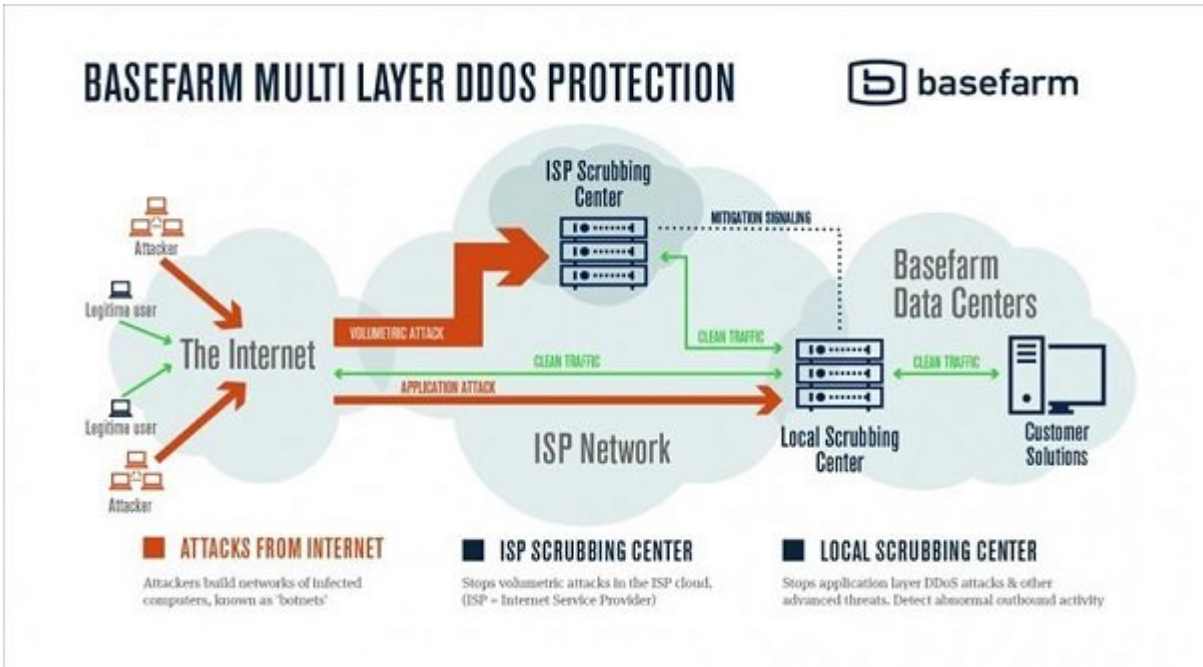
چگونه می‌توانیم اطلاع پیدا کنیم یک حمله منع سرویس توزیع شده رخ داده است؟

حملات منع سرویس توزیع شده از آن جهت بدترین نوع حملات به شمار می‌روند که بدون هیچ‌گونه هشداری از راه می‌رسند. در حالی که برخی از گروه‌های بزرگ هکری پیش از حمله هشدارهایی را ارسال می‌کنند، اما در اغلب موارد مهاجمان بدون هیچ‌گونه هشداری به سایت شما حمله می‌کنند. در این حالت شما تنها زمانی از این موضوع مطلع خواهید شد که مشتریان شکایت می‌کنند که مشکلی رخ داده و قادر نیستند به سایت شما دسترسی پیدا کنند. در ابتدا تصور نمی‌کنید یک حمله منع سرویس توزیع شده رخ داده است، در نتیجه فکر می‌کنید سرور یا هاست دچار مشکل شده‌اند. در ادامه سرور را بررسی کرده و یکسری آزمایش‌های اولیه انجام می‌دهید، اما فقط حجم بالایی از ترافیک را مشاهده می‌کنید که باعث شده به‌کارگیری منابع به حداکثر ظرفیت ممکن برسد. در ادامه به سراغ بررسی این موضوع می‌روید که آیا برنامه‌هایی در پس‌زمینه در حال اجرا هستند، اما بازهم هیچ نشانه‌ای از یک مشکل را پیدا نمی‌کنید. مدت زمانی که صرف درک این موضوع می‌کنید که یک حمله منع سرویس توزیع شده رخ داده و مدت زمانی که صرف کم کردن آسیب‌ها می‌کنید حداقل چند ساعت زمان خواهد برد. در این چند ساعت ارزشمند شما ممکن است ضرر مالی زیادی را متحمل شوید. در نتیجه هر چه سریع‌تر این حمله را تشخیص دهید میزان خسارت به بار آمده به حداقل می‌رسد.

راهنمای تشخیص حمله منع سرویس توزیع شده

موثرترین راهکار برای مقابله با یک حمله منع سرویس توزیع شده درست همان زمانی است که حمله آغاز شده است. در این‌جا چند سرنخ وجود دارد که نشان می‌دهند یک حمله منع سرویس توزیع شده رخ داده است.
یک آدرس آی‌پی x درخواست را در مدت زمان y ثانیه ایجاد کرده است.
سرور پیغام خطای 503 به معنای غیر قابل دسترس بودن سرور به دلیل ترافیک زیاد را نشان می‌دهد.
زمان زندگی (TTL) سرنام time to live روی یک درخواست پینگ به اتمام رسیده است.
کارمندان از کندی سرعت گلایه دارند.
و در نهایت گزارش‌های تحلیلی خبر از یک ترافیک بزرگ می‌دهند.
بیشتر این نشانه‌ها می‌توانند از سوی یک سامانه هشداردهنده جمع‌آوری شده و از طریق یک ایمیل یا پیام برای مدیران ارسال شوند. سامانه هشداردهنده طراحی شده از سوی loggly از جمله راهکارهایی است که در این زمینه پیش روی سازمان‌ها قرار دارد. (شکل یک)

شکل 1

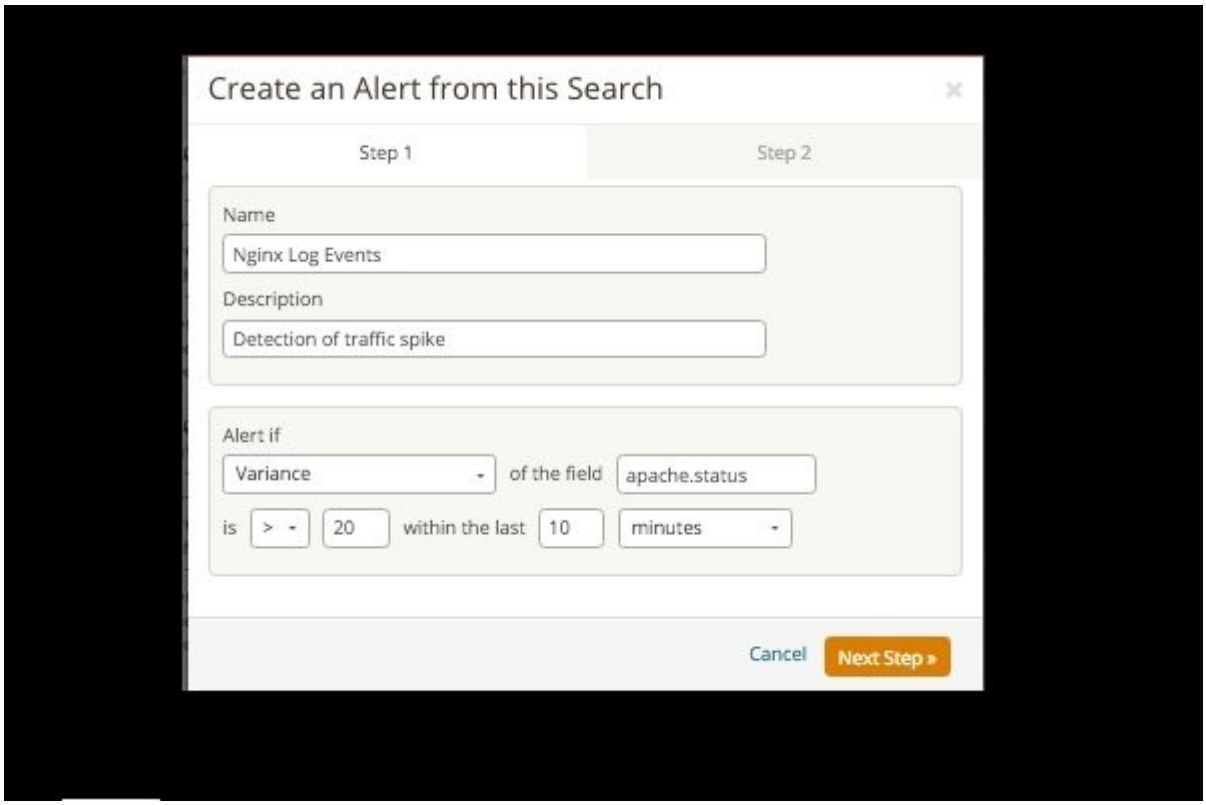


ارسال درخواست‌های زیاد از طریق یک آدرس آی‌پی

شما به شکل موقت می‌توانید روتر را به گونه‌ای تنظیم کنید تا ترافیک مبتنی بر یکسری آدرس‌های آی‌پی خاص را به سمت مسیرهایی هدایت کند که وجود ندارند. این تکنیک در حقیقت آدرس‌های آی‌پی حمله کننده را به یک مسیر خالی که وجود ندارد هدایت کرده و اجازه نمی‌دهد روی عملکرد سرور تاثیرگذار باشند. راهکار ساده‌تری که پیش روی شما قرار دارد، این است که آدرس‌های آی‌پی غیرقانونی را مسدود کرده و به این شکل حمله را متوقف کنید. اما این روش مشکلی دارد. آدرس‌های آی‌پی منبع حمله‌کننده ممکن است گمراه‌کننده باشند.
تنظیم هشدارها از طریق دیوارهای آتش یا سامانه‌های تشخیص نفوذ نیز ممکن است پیچیده باشد. هکرها ممکن است از روبات‌هایی که عملکرد عادی دارند برای فریب این سامانه‌ها استفاده کنند. به‌طور کلی، شما باید سامانه یا مکانیزم هشداردهنده را به گونه‌ای تنظیم کنید که هر زمان تعداد زیادی درخواست را از آدرس‌های آی‌پی دریافت کرد که همگی در یک محدوده قرار دارند و از قبل مشخص شده‌اند و درون یک پنجره یکسان دریافت می‌شوند را تشخیص داده و این موضوع را به شما اطلاع دهد. به احتمال زیاد به یک فهرست سفید از آدرس‌های متعبر نیاز دارید. به واسطه آنکه ربات گوگل موسوم به Googlebot با سرعت و نرخ بالایی فرآیند خزیدن را انجام می‌دهد. در نتیجه اگر این فهرست را در اختیار نداشته باشید آنگاه بات‌ها و اسکریپت‌های معتبری همچون ربات گوگل ممکن است به عنوان یک تهدید شناخته شده و سامانه هشدار دهنده یک پیغام هشدار کاذب را تولید کند.

سرور با کد 503 پاسخ می‌دهد

در ویندوز شما می‌توانید هشدارها را به گونه‌ای تنظیم کنید که اگر یک رویداد خاص در Event Viewer اجرا شد از آن مطلع شوید. شما می‌توانید هر موضوعی همچون خطاها، هشدارها یا هر نوع رویدادی را به یک وظیفه الصاق سنجاق کنید. این‌کار باعث می‌شود تا پیش از آنکه یک موقعیت بحرانی شکل بگیرید موضوع را بررسی کنید. برای الصاق یک رویداد 503 ابتدا باید رویداد موردنظر خود را در Event Viewer پیدا کنید. برای این منظور Event Viewer را باز کرده و روی رویداد موردنظر کلیک راست کنید. (شکل دو) این‌کار باعث می‌شود تا صفحه پیکربندی، مکانی که در نظر دارید یک رویداد را برای ارسال یک ایمیل به مدیر یا تیمی از پژوهشگران پیکربندی کنید، در اختیارتان قرار گیرد.



شکل 2

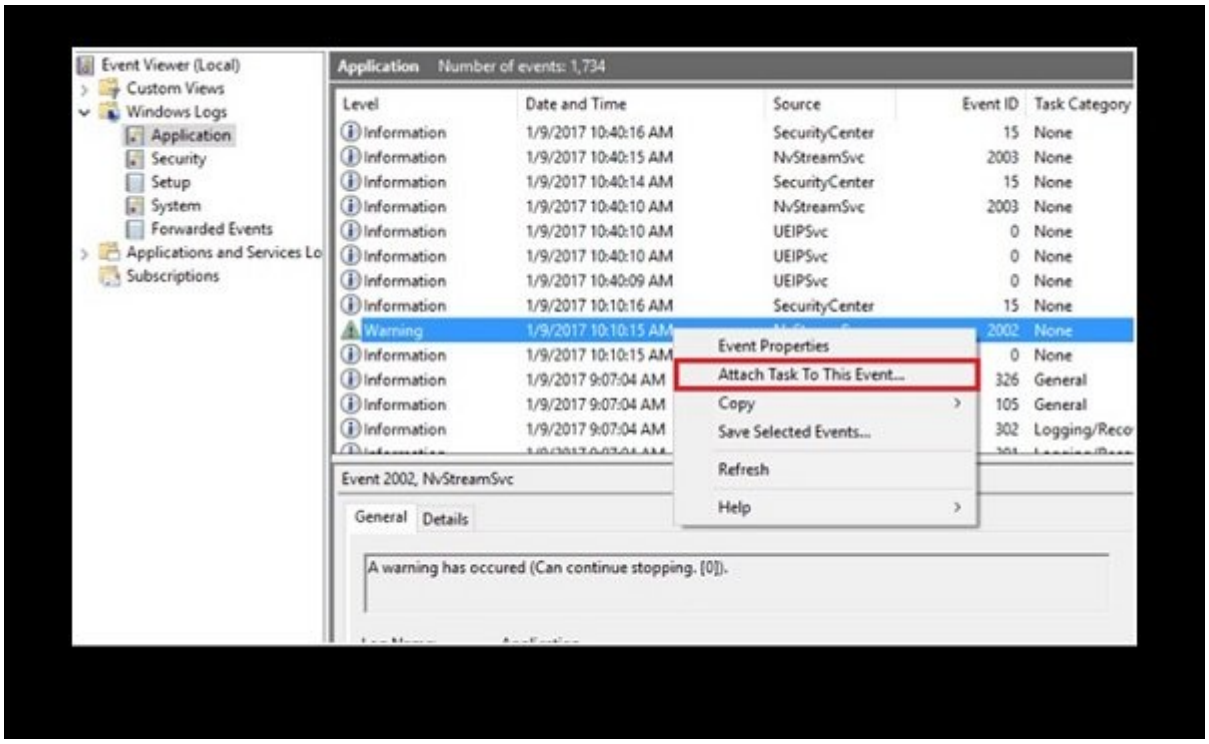
TTL Time Out

شما به‌طور معمول می‌توانید سرور را برای آزمایش پهنای باند و ارتباطات پینگ کنید، اگر در نظر دارید فرآیند هشداردهی را خودکارسازی کرده به‌طوری که پیش از وقوع یک حمله به شما اطلاع‌رسانی کند، این راهکار کمک چندانی به شما نمی‌کند. البته بعضی مواقع پینگ کردن سرور با اشتباهاتی نیز همراه است. برای آنکه بتوانید هشداردهی مبتنی بر پینگ را خودکارسازی کنید، چند سرویس روی وب وجود دارند که اجازه می‌دهند از هر نقطه در جهان سایت خود را پینگ کنید. این سرویس‌ها را می‌توانید به شکل منطقه‌ای پیکربندی کرده تا فرآیند پینگ کردن را انجام دهند. از طریق این سرویس‌ها، سایت شما در 24 ساعت شبانه‌روز و هفت روز کاری تحت نظارت قرار می‌گیرد. در نتیجه تیم فناوری اطلاعات می‌تواند در صورت بروز مشکل روی سرور به سرعت موضوع را بررسی کند. به واسطه آنکه حمله منع سرویس انکار شده به سرعت پهنای باند شما را مصرف می‌کند، زمان پینگ ممکن است بیش از اندازه طولانی شود. در این حالت سرویس‌های فوق قادر هستند هشداری را برای تیم شما ارسال کرده تا به سرعت تدابیر امنیتی فنی را برای حل مشکل اعمال کنند.

چگونه می‌توانیم از طریق فرمان netstat یک حمله منع سرویس توزیع شده را شناسایی کنیم؟

راهکارهای مختلفی برای شناسایی یک حمله منع سرویس انکار شده وجود دارد. به‌طور مثال می‌توانید از Wireshark استفاده کرده و بسته‌های SYN را مورد بررسی قرار دهید. اما از طریق فرمان netstat که روی پلتفرم‌های مختلف قابل استفاده است می‌توانید به شناسایی این موضوع بپردازید.

شکل 3



(شکل سه) در ادامه با چند کاربرد این فرمان آشنا می‌شوید:

1. فرمان netstat –na همه ارتباطات اینترنتی فعال به سرور و فقط ارتباطات در حالت انتظار را نشان می‌دهد.

2. فرمان netstat -an | grep :80 | sort ارتباطات اینترنتی فعال به سرور از طریق پورت 80 را نشان می‌دهد. با توجه به اینکه فرمان فوق پورت مرتبط با پروتکل http را بررسی می‌کند، زمانی که یک وب‌سرور دارید این دستور کمک کننده است. خروجی این فرمان به صورت فهرست شده نشان داده می‌شود. از این فرمان برای شناسایی یک حمله single flood و به منظور تشخیص اینکه چه تعداد ارتباط وارد شونده از یک آدرس آی‌پی وارد شده است، استفاده کنید.

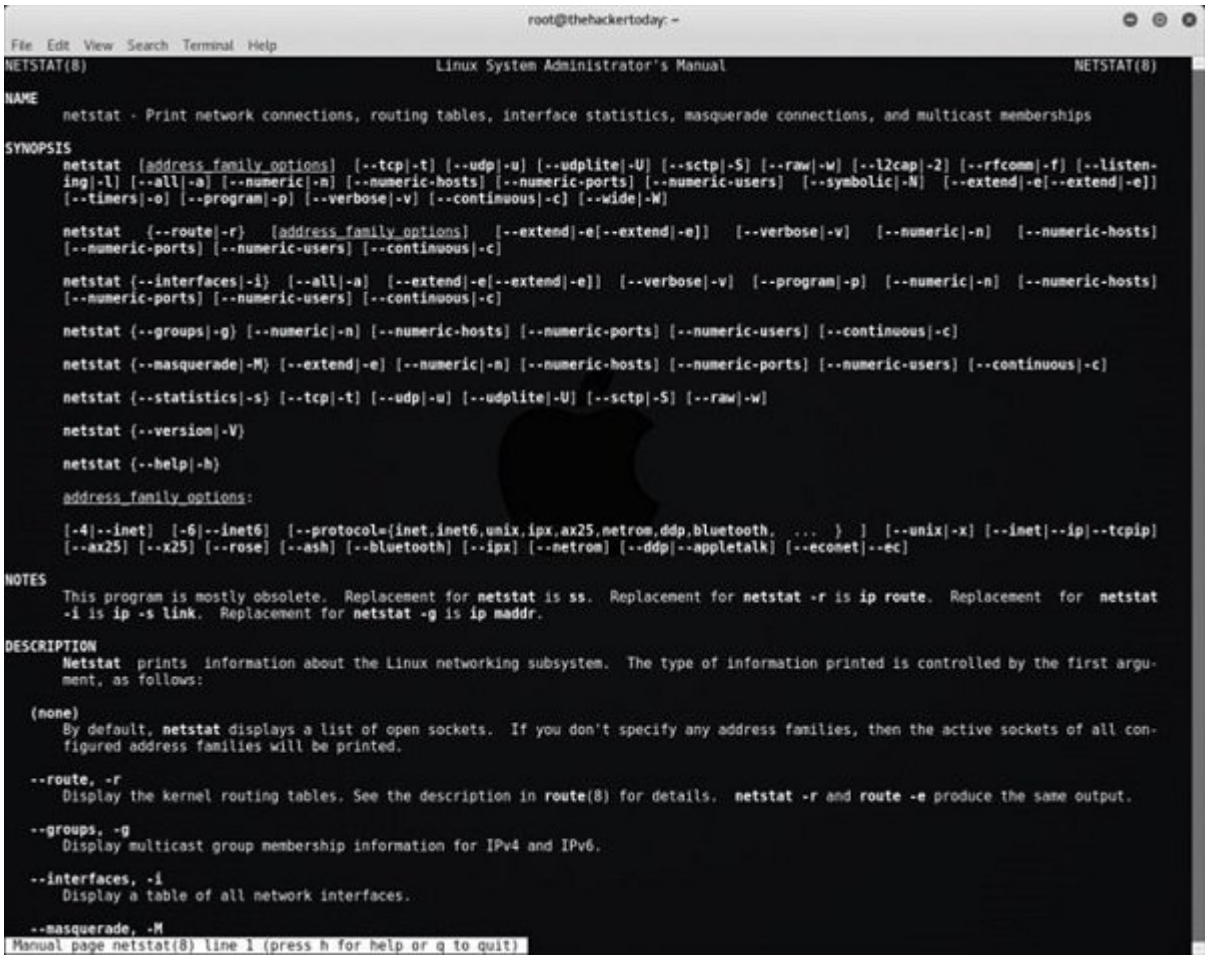
3. فرمان netstat -n -p|grep SYN_REC | wc –l اجازه می‌دهد تعداد SYN_REC فعال در حال اجرا روی سرور را محاسبه کنید. این تعداد باید نسبتا کم باشد. در اغلب موارد باید کمتر از 5 باشد. در یک حمله DoS یا mail bombs این تعداد رشد چشم‌گیری دارد. البته فراموش نکنید که این مقدار به سامانه شما نیز بستگی دارد. در نتیجه یک مقدار بالا ممکن است برای سرور دیگری حکم میانگین را داشته باشد.

4. فرمان netstat -n -p | grep SYN_REC | sort –u به جای آنکه تنها تعداد آدرس‌های آی‌پی را نشان دهد همه آدرس‌های آی‌پی را فهرست می‌کند.

5. فرمان netstat -n -p | grep SYN_REC | awk ‘{print $5}’ | awk -F: ‘{print $1}’ همه آدرس‌های آی‌پی منحصر به فرد مربوط به یک گره را که در حال ارسال SYN_REC هستند، نشان می‌دهد.

6. فرمان netstat -ntu | awk ‘{print $5}’ | cut -d: -f1 | sort | uniq -c | sort –n برای محاسبه و شمارش تعداد ارتباطاتی که هر آدرس آی پی روی سرور ایجاد کرده به کار برده می‌شود. (شکل چهار)

شکل 4



7. فرمان netstat -anp |grep ‘tcp|udp’ | awk ‘{print $5}’ | cut -d: -f1 | sort | uniq -c | sort –n تعداد ارتباطات مرتبط با آدرس‌های آی‌پی را که از طریق پروتکل‌های TCP یا UDP به سرور متصل شده‌اند، شمارش کرده و نشان می‌دهد.

8. فرمان netstat -ntu | grep ESTAB | awk ‘{print $5}’ | cut -d: -f1 | sort | uniq -c | sort –nr به جای آنکه همه ارتباطات را مورد بررسی قرار دهد ارتباطات ایجاد شده (ESTABLISHED) را بررسی کرده و تعداد ارتباطات مرتبط با هر آدرس آی‌پی را نشان می‌دهد.

9. فرمان netstat -plan|grep :80|awk {‘print $5’}|cut -d: -f 1|sort|uniq -c|sort -nk 1 آدرس آی‌پی و ارتباط مرتبط با آن را نشان داده و فهرست می‌کند. ارتباطاتی که از طریق پورت 80 انجام شده‌اند. پورت 80 در اصل در ارتباط با درخواست‌های مرتبط با یک صفحه وب مبتنی بر پروتکل HTTP مورد استفاده قرار می‌گیرد.
از طریق به‌کارگیری فرمان‌های فوق موفق خواهید شد یک آدرس آی‌پی را که آماده است برای اجرای یک حمله DDoS مورد استفاده قرار گیرد، شناسایی کنید.

منبع:
thehacktoday

loggly
tutorialspoint
tomsitpro
iplocation
dzone

تاریخ انتشار:
28 تیر 1397

نشانی منبع:
https://www.shabakeh-mag.com/tricks/security-tricks/13061/%D8%B1%D8%A7%D9%87%DA%A9%D8%A7%D8%B1%D9%87%D8%A7%DB%8C%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%B4%D9%86%D8%A7%D8%B3%D8%A7%DB%8C%DB%8C-%D9%88-%D8%AF%D9%81%D8%B9-%D8%AD%D9%85%D9%84%D9%87-%D9%85%D9%86%D8%B9-%D8%B3%D8%B1%D9%88%DB%8C%D8%B3-%D8%AA%D9%88%D8%B2%DB%8C%D8%B9-%D8%B4%D8%AF%D9%87-ddos