باسمه تعالی

حملات DDoS با سوءاستفاده از پیکربندی نامناسب SNMP

مقدمه

امروزه شبکه اینترنت به عنوان بزرگ‌ترین شبکه جهانی شناخته می‌شود و اگر شخصی بخواهد به سرویس‌ها یا منابع یک سرور مشخص دسترسی پیدا کند، باید درخواست‌های خود را از طریق لینکی مشخص به سمت سرور موردنظر ارسال نماید. اما پهنای باند هر سروری که در شبکه قرار دارد محدود بوده و هر کدام از بسته‌هایی که به سمت آنها فرستاده می‌شود، مقداری از پهنای باند را به هدر می‌دهند. اگر تعداد این بسته‌ها از یک حد مشخص بیشتر شود، ازدحام در شبکه به وجود آمده و در بهترین حالت، پاسخ‌دهی به این درخواست‌ها با تاخیر صورت خواهد گرفت. حملات منع سرویس توزیع شده (DDOS) که عمدتاً به دنبال اتلاف پهنای باند در شبکه هستند، پهنای موجود برای سیستم هدف را از طریق ارسال تعداد زیادی از بسته‌ها به سمت سیستم هدف هدر می‌دهند. از طرف دیگر از آنجا که سیستم هدف باید به این درخواست‌ها پاسخ دهد، ناگزیر منابع خود را به اشتراک گذاشته و به نوعی مورد حمله DDOS قرار می‌گیرد. یکی از انواع این حملات از پروتکل SNMP سوءاستفاده می‌نمایدکه برای کنترل و مانیتورینگ دستگاه‌های موجود در شبکه مورد استفاده قرار می‌گیرد.

مشاهدات نشان می‌دهد که اخیراً سوءاستفاده از این آسیب‌پذیری گسترش یافته است. به‌همین دلیل متن حاضر در معرفی روش حمله تهیه شده است.

قبل از اینکه به معرفی حمله منع سرویس توزیع‌شده با استفاده از پروتکل SNMP بپردازیم، نیاز است تا ابتدا به‌طور مختصر با مفاهیم اولیه و پایه این پروتکل آشنا شویم.

پروتکل SNMP

SNMP سرویسی است که بر روی سیستم‌های میزبان اجرا شده و به مدیران شبکه کمک می‌نماید تا از این سرویس برای نظارت بر وضعیت سلامت میزبان و نحوه عملکرد و پایداری شبکه به صورت لحظه‌ای استفاده نمایند. سیستم‌های میزبان شامل مجموعه بزرگی از تجهیزات از جمله روترها، دیواره‌های آتش، load balancer ها، سرورهای وب یا سایر نرم‌افزارها، کامپیوترهای شخصی، دستگاه‌های موبایل، دوربین‌های اینترنتی و بسیاری دیگر می‌باشند.

هنگامی که سرویس SNMP در یک دستگاه پیکربندی می‌شود، دستگاه مورد در نظر در حالت listening برای دریافت درخواست‌های SNMP قرار می‌گیرد. البته برای این که به query هایی که به سمت دستگاه ارسال می‌شوند پاسخ دهد، نیاز است که بسته‌های دریافتی community string های صحیح داشته باشند. در واقع می‌توان Community String را رمز عبور SNMP محسوب نمود و از آن به عنوان Preshared Key استفاده نمود.

سرویس SNMP به طور پیش‌فرض تنها روی برخی از دستگاه‌ها فعال است و به عنوان یک قابلیت درون بسیاری از دستگاه‌ها در نظر گرفته می‌شود. مسئولین شبکه و به طور دقیق‌تر سیستم‌های مانیتورینگ خودکار، درخواست‌هایی به دستگاه‌هایی که SNMP روی آنها فعال است، ارسال می‌نمایند. SNMP این قابلیت را در اختیار مدیران شبکه می‌گذارد تا از این طریق مشخصه‌هایی از شبکه مثل حرارت دستگاه‌ها، وضعیت عملکرد اینترفیس‌های درون شبکه، وضعیت پردازشگر، نرخ تبادل داده روی این اینترفیس‌ها و پارامترهایی از این قبیل را دنبال نمایند.

به طور کلی، پروتکلSNMP این قابلیت را در اختیار مدیران شبکه قرار می‌دهد تا با استفاده از این پروتکل از سلامت فعلی و وضعیت هر کدام از دستگاه‌ها و یا سیستم‌ها مطلع گردند. هم‌چنین از این پروتکل می‌توان برای هشداردهی به ادمین‌ها هنگامی که مشکلی در شبکه به وجود می‌آید، استفاده نمود.

دستگاه‌ها چگونه برای استفاده از این پروتکل پیاده‌سازی می‌گردند؟

هنگامی که پروتکل SNMP روی یک دستگاه یا سیستم اجرا می‌گردد، حداقل کاری که باید صورت بگیرد این است که پروتکل به گونه‌ای پیکربندی گردد تا در حالت listening برای یک community string مشخص قرار گرفته باشد. هنگامی که SNMP فعال می‌گردد، اگر هیچ community string مشخصی تنظیم نشده باشد، از مقادیر پیش‌فرض استفاده می‌شود. معمولاً community string هایی که به صورت پیش‌فرض برای خواندن و نوشتن مورد استفاده قرار می‌گیرند، "public" و "private" می‌باشند.

معمولاً پروتکل SNMP در شبکه‌های عمومی که نا امن بوده و در دسترس همه قرار دارند (مانند شبکه اینترنت) مورد استفاده قرار نمی‌گیرد، مگر در شرایطی که تدابیر امنیتی برای شبکه مثل تعریف سطح دسترسی مختلف برای آدرس‌های IP مختلف در نظر گرفته شده باشد.

پروتکل‌های SNMP نسخه ۱ و ۲ از community string های رمز نشده استفاده می‌نمایند. این مشکل امنیتی در نسخه ۳ این پروتکل از طریق رمزنگاری، احراز اصالت و سایر مکانیزم‌های امنیتی برطرف گردیده است.

متاسفانه بسیاری از مکانیزم‌های امنیتی که برای این پروتکل در نظر گرفته شده است، به درستی پیکربندی نمی‌شوند. به‌طور مثال، در پروتکل‌های SNMP نسخه ۱ و ۲ اگر هیچ community string ای در نظر گرفته نشود، به صورت پیش‌فرض یک رشته انتخاب می‌گردد که حدس زدن این رشته کار دشواری نمی‌باشد. رشته‌های public و private به صورت پیش‌فرض به عنوان community string برای read و write مورد استفاده قرار می‌گیرند. از طرف دیگر در پروتکل SNMPv3 اگر مرحله امنیتی به صورت noAuth انتخاب شود، پروتکل هیچ تفاوتی با ورژن‌های قبلی نخواهد داشت.

SNMP DDOS Attack

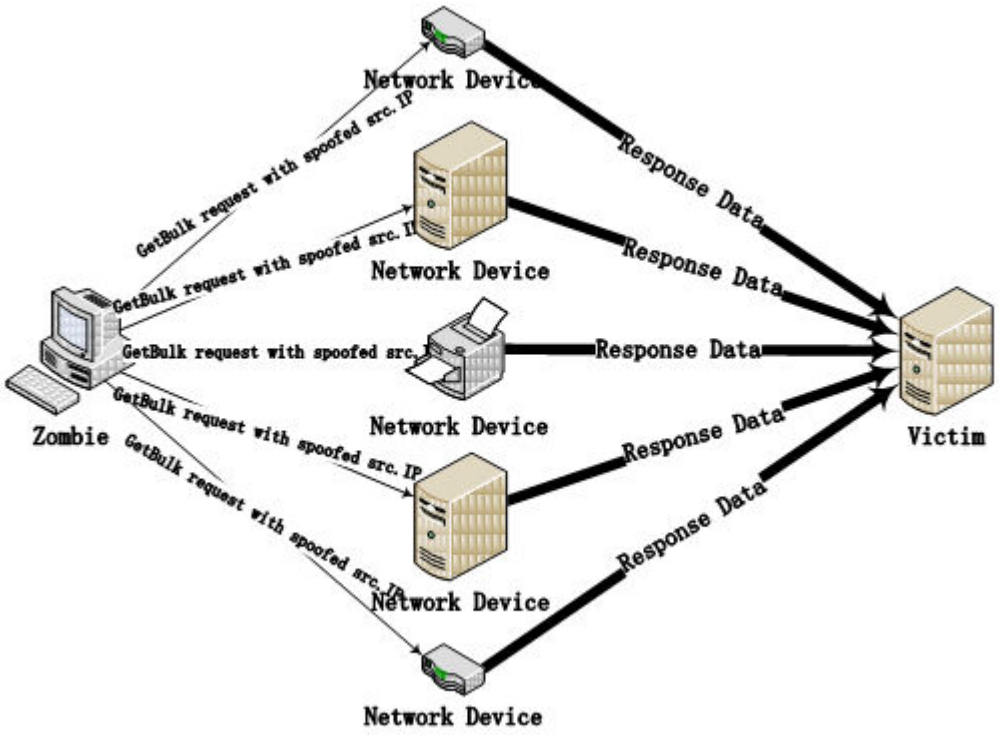
حمله SNMP Reflected Amplification DDoS از دستگاه‌هایی که SNMP روی آنها فعال است برای هدایت مقدار زیادی از ترافیک به سمت هدف (که دارای آدرس IP مشابه با آدرس جعل‌شده درون درخواست SNMP است) استفاده می‌نماید. خطر این حملات زمانی احساس می‌شود که دستگاه‌هایی که در خانه‌ها استفاده می‌شوند دارای SNMP فعال باشند. در این حالت این‌گونه دستگاه‌ها به هر SNMP query که از هر کاربری در شبکه اینترنت به سمت آنها با community string پیش‌فرض ارسال میگردد، پاسخ خواهند داد. بنابراین اگر یک community string شناخته شده و یا پیش‌فرض در این دستگاه‌ها استفاده شود، که حمله کننده بتواند آن را تشخیص دهد، احتمال اینکه یک کاربر ناشناس به کاربر هدف یک درخواست موفقیت آمیز ارسال نماید، افزایش می‌یابد.

از طرف دیگر SNMP از پروتکل UDP و پورت ۱۶۱ برای ارسال بسته‌های خود استفاده می‌نماید که این پروتکل برخلاف TCP پروتکلی از نوع بدون اتصال است. استفاده از این پروتکل سبب می‌گردد تا جعل نمودن آدرس مبدا یک درخواست SNMP راحت‌تر انجام گیرد، چرا که دیگر نیازی به دریافت پاسخ از طرف کاربر هدف نیست.

در متداول‌ترین نوع حمله از این دسته، حمله‌گر به جای استفاده از queryهایی مثل GET، از بسته‌های درخواست "SNMP "GetBulkRequest استفاده می‌نماید. چرا که این درخواست از سیستم مورد نظر حجم زیادی از داده‌ها را درخواست نموده و حمله‌ای قوی‌تر شکل خواهد گرفت (زیرا اندازه پاسخی که در جواب این query ارسال می‌گردد، خیلی بیشتر از اندازه query فرستاده شده است). حال این SNMP query به مجموعه عظیمی از دستگاه‌های قابل دسترسی که از یک community string پیش‌فرض مثل public و یا هر رشته شناخته شده دیگر استفاده می‌نمایند، ارسال می‌گردد. هنگامی که این بسته ارسال می‌شود، فرد حمله‌گر آدرس مبدا بسته‌ها را جعل نموده و آدرس IP مربوط به کاربر قربانی را قرار می‌دهد.

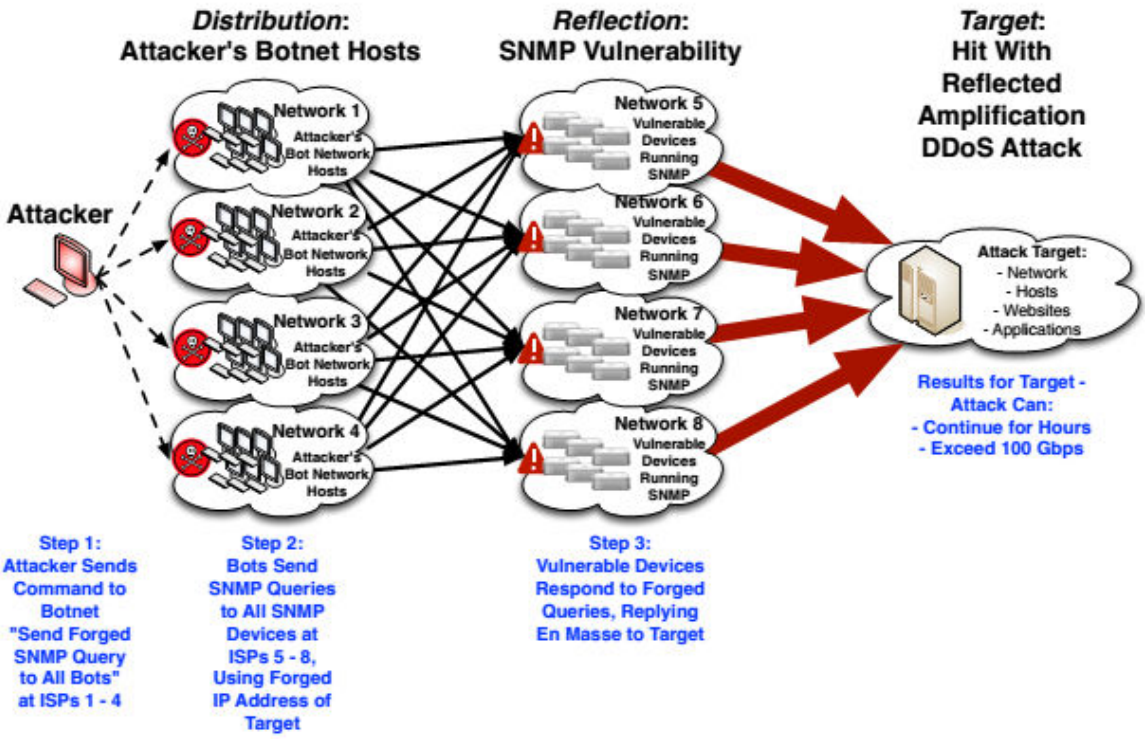
تمامی دستگاه‌هایی که در حال گوش‌دادن به درخواست‌های SNMP بوده و از همین community string استفاده می‌نمایند، بلافاصله پاسخ خود را ارسال می‌نمایند. به طور مثال در حالت استفاده از بسته GetBulkRequest، درخواست‌های معمولی در بازه ۶۰ الی ۱۰۲ بایت بوده ولی بسته‌ای به طول ۴۲۳ الی ۱۵۶۰ بایت در جواب به این درخواست‌ها ارسال می‌گردد. درنتیجه مشاهده می‌گردد که پاسخی که دریافت می‌شود، خیلی بیشتر از اندازه درخواست فرستاده شده است.

شکل زیر سناریوی این حمله هنگامی که حمله‌گر بسته‌های درخواست خود را به سمت کاربران مختلف ارسال می‌نماید، نشان می‌دهد. همانطور که در شکل نیز مشاهده می‌شود، کاربر بسته‌های GetBulk خود را به سمت دستگاه‌های مختلف موجود ارسال نموده و برای آدرس مقصد، IP سیستم هدف را قرار می‌دهد. اگر این دستگاه‌ها دارای community string مشابه باشند، پاسخ خود را به سمت آدرس مبدا که همان IP سیستم هدف است، ارسال می‌نمایند.



برای اینکه تاثیر حمله بیشتر شود، فرد حمله‌گر می‌تواند از یک شبکه توزیع شده از کاربرانی که به یک بدافزار آلوده شده و به عنوان بخشی از شبکه بات هستند، استفاده نماید. استفاده از شبکه بات، به حمله‌کننده این قابلیت را می‌دهد تا حمله را با قدرت بیشتری انجام دهد.

شکل زیر سناریوی کلی این حمله را نشان می‌دهد. همانطور که می‌بینید با استفاده از شبکه‌های بات، فرد حمله‌گر می‌تواند روند حمله خود را به چند مرحله تقسیم نماید. به دلیل اینکه فرد حمله‌گر داده‌هایی با حجم بسیار پایین را از طریق شبکه بات متشکل از مجموعه‌ای از کاربران ارسال می‌نماید، شناسایی مبدا حمله کار دشواری است. زیرا از طرف مبدا حمله، ترافیک مشکوک و زیادی ایجاد نمی‌گردد. هم‌چنین برای کاربران نهایی که شبکه بات را تشکیل می‌دهند، تشخیص اینکه سیستم آنها به عنوان یک بات مورد استفاده قرار گرفته است یا نه، کار دشواری است چرا که اندازه بسته‌هایی که از سیستم آنها خارج می‌شوند، کم است.



در نتیجه توصیه می‌گردد که درصورت عدم نیاز به استفاده از پروتکل SNMP، این سرویس غیرفعال گردد. اما درصورت استفاده از این پروتکل، با استفاده از کنترل سطوح دسترسی و قوانین مناسب دیواره آتش و تغییر مقادیر پیش‌فرض، جلوی سوءاستفاده از آن گرفته شود.