امنیت در محاسبات ابر،حملات داس و تکنیک های مقابله با آن

مریم کمالیان برازجانی[1]
۱- کارشناسی ارشد، کامپیوتر،نرم افزار ، ایران،
maryamkamalian@yahoo.com

چکیده
همزمان با ارائه خدمات رایانشی قابل دسترس و به موقع از طریق رایانش ابری، روز به روز شرکت های بیشتری شروع به پذیرش تغییرات از طریق بردن اساس داده ها و نرم افزارهایشان به سمت ابر می کنند.همزمان مفهوم مهم دیگری از ساختار کامپیوتری اینترنت در پیش روی ما قرار می گیرد که همان شبکه ارتباطی نرم افزار است[1].در حالیکه رایانش ابری، مدیریت رایانشی و منابع ذخیره ای را تسهیل می کند،شبکه ارتباطی نرم افزار تغییرات تدریجی و تکاملی دیگری از قبیل مدیریت پیچیده شبکه ارتباطی و همچنین حفظ امنیت را بیان می کند [1]. در این مقاله به بیان امنیت در ابر،حملات داس و تکنیک های مقابله با تهدیدهای امنیتی پرداخته می شود.

کلمات کلیدی: امنیت،حمله،داس،مقابله،تهدید

۱– مقدمه
علی رغم این حقیقت که شبکه ارتباطی به عنوان کاندید ساختار اینترنتی نسل آینده است، شرکت هایی مثل گوگل شبکه ارتباطی نرم افزار را در مراکز داده های اینترنتی شان به کار گرفته اند. بنابراین با شروع این عصر رایانش ابری و شبکه ارتباطی نرم افزار دست در دست هم خدمات فناوری اطلاعات را به شرکت ها ارائه می کنند. در کنار تمام مزایایی که به وضوح قابل رویت است، همکاری این دو ممکن است خطرات احتمالی بر روی امنیت شبکه ارتباطی داشته باشد[1].گرچه متخصصان امنیتی شبکه ارتباطی تلاش های زیادی برای حل این مشکل کرده اند، حملات داس همچنان رو به افزونی است. به نظر می رسد راه حل های دفاعی خطرات داس موجود به وسیله مدیران شبکه ها می توانند قطعات سخت افزار مطمعنی برای پیدا کردن یا کم کردن حملات داس شبکه های ارتباطی قرار دهند[2].محققان دیگر بر روی مزایای اس دی ان و رایانش ابری برای دفاع در برابر حملات داس تمرکز دارند.از مهم ترین تهدیدهای امنیتی در محاسبات ابری حملات داس می باشد که در ادامه به بیان آن می پردازیم.

۲– حملات DoS(Denial-of-Service)
حمله DoS مخفف عبارت Denial- Of - Service یا عدم پذیرش سرویس است . این نوع حمله باعث از کارافتان 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 تصیب آخرین وصله های امنیتی از حمله جلوگیری خواهند کرد .شایان ذکر 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 داس جلوگیری از استفاده صحیح از منابع کامپیوتری و شبکه ای و از بین بردن این منابع است [3].علیرغم تلاش و صنایعی که برای ایمن سازی علیه خرابکاری معروف گشته است ، سیستم

های متصل به اینترنت با تهدیدی واقعی و مداوم به نام حملات داس مواجه هستند این امر بدلیل دو مشخصه اساسی اینترنت است :منابع تشکیل دهنده اینترنت به نوعی محدود و مصرف شدنی هستند، امنیت اینترنت تا حد زیادی وابسته به تمام عوامل است[3].

۱-۲- دسته بندی انواع حملات داس :

حملات داس به پنج سطح اصلی تقسیم میشوند

۱-۱-۲- حمله های سطح NETWORK DEVICE

این حمله ها از ضعف های موجود در ساخت سخت افزار مورد استفاده در شبکه سواستفاده می کنند .برای مثال بعضی از روترها مشکل سرریز شدن بافر دارند که می تواند توسط حمله کننده برای از کار انداختن روتر استفاده شود[3].

۲-۱-۲- حمله سطح سیستم عامل

دسته دوم ، حمله سطح سیستم عامل است که در آن از بعضی جنبه های موجود در پیاده استری پروتکل وهمچنین خود سیستم عامل ماشین مورد نظر بهره جویی می شود[4].

۳-۱-۲- حمله سطحAPPLICATION

در این حمله از حفره های موجود در برنامه های کاربردی سو استفاده می کند .برای مثال این نوع حمله می تواند از کاستی های موجود در ساختار داده ای الگوریتم های استفاده شده در برخی برنامه های متداول بهره گیرد[4] .

۴-۱-۲- حمله های DATA FLOOD

در این نوع حمله با فرستادن سیل آسای بسته هایی با آدرس مبدا جعلی وبا نرخ بالا ، به هدفش که گرفتن منابع سیستم و پهنای باند است، می رسد . این کار، سیستم را مشغول رسیدگی به این بسته های جعلی کرده و از بررسی داده های مفید و اصلی باز می دارد[4] .

۵-۱-۲- حمله نوعPROTOCOL FEATURE

برای مثال SYN FLOOD در این نوع حمله از طراحی غیر ایمن بعضی پروتکل های استاندارد بهره می گیرنداز فرآیند دست تکانی سه مرحله ای در پروتکل تی سی پی واین حقیقت که در پروسه مسیریابی صحیح بودن آدرس آی پی مبدا چک نمی شود ، سو استفاده می کند[4] .

۴- راهکارهایی برای محافظت شبکه در حملات DOS

در این بخش روش های کلی که لازم است یک شبکه در خصوص جلوگیری از قرارگرفتن در برابر این حملات به آن توجه کند، مطرح می کنیم[7] .

۱-۴- طراحی استوار ودارای افزونگی

هر چقدر که در طراحی از سایت از جایگزین و افزونگی بیشتری استفاده کنیم احتمال به خطر افتادن آن کمتر می شود . اگرسایت یک شرکت برای اتصال به اینترنت دارای یک اتصال از طریق یک مسیریاب باشد و سرور تنها بر روی یک ماشین درحال اجرا باشد ، این سایت از طراحی استواری بهره مند نخواهد بود .در چنین حالتی حمله کننده می تواند حمله داس را علیه سرور راه اندازی کند وسایت را در حالت خارج از سرویس دهی قرار دهد .در حالت ایده آل یک سایت نه تنها باید اتصالات چندگانه ای به اینترنت داشته باشد بلکه باید این اتصالات ازمناطق جغرافیایی مختلف باشند[7].

۲-۴- ایجاد محدودیت پهنای باند

ازطریق حمله داس که علیه پروتکل خاص صورت می گیرد ، حمله کننده می تواند کل پهنای باند شبکه هدف را بگیرد . برای مثال اگر حمله کننده به شبکه ما از طریق پورت شماره ۲۵ حمله داس را راه اندازی کند، درصورت موفقیت آمیز بودن حمله پس از گذشت مدت زمان کوتاهی کل پهنای باند شبکه اشغال خواهد شد .در این زمان اگر یک کاربر عادی بخواهد از طریق پورت شماره ۸۰ به سرورما متصل شود، تقاضای اتصال اورد خواهدشد .یک راه برای جلوگیری از بروز این مشکل قرار دادن محدودیت برای پهنای باند بر مبنای پروتکل است .برای مثال پورت ۲۵ حداکثر می تواند ۲۰ درصد از کل پهنای باند را به خود اختصاص دهد وپورت ۸۰ حداکثر ۵۰ درصد را .نکته کلیدی که درمورد اینگونه راه حل ها باید به آن توجه داشت این است که این روش ها ایده آل نیستند و می توانند به وسیله حمله کننده ها خنثی شوند .برای مثال برای خنثی کردن مورد ذکرشده ، حمله کننده می توانند دوحمله داس یکی بر روی پورت ۲۵ و دیگری بر پورت ۸۰ راه اندازی کند . کاری که ابزارهای پیش رفته حمله به صورت اتوماتیک انجام می دهند [8] .

۳-۴- نصب به موقع وصله های امنیتی موجود برای سیستم ها

وقتی یک حمله علیه ماشینی اتفاق می افتد، معمولا انجمن های مربوطه شروع به بررسی علت و پیدا کردن راهی برای مقابله می پردازند و در صورت پیدا کردن راه حل ، آنها را به صورت وصله های نرم افزاری توزیع می کند .پس سایتی که بخواهد امنیت نسبی درمقابل حملات شناخته شده داشته باشد ، باید همیشه به روز باشد و از وصله های آماده شده استفاده نماید نکته دوم درمورد وصله های امنیتی این است که حتما باید قبل از استفاده، تست شود تا اطمینان حاصل شود که در کنار حل کردن مشکل قبلی، مشکل جدیدی به وجود نمی آیند[9] .

۴-۴- راه اندازی کمترین تعداد سرویس ها

وقتی تعداد کمتر سرویس در حال اجرا باشد مدیریت و مراقبت از امنیت آنها برای مدیر شبکه آسان تر خواهد بود .بنابراین همواره باید قاعده کمترین امتیاز را درنظرگرفت و کمترین تعداد سرویس هایی را که یک ماشین می تواند با آن به عملکرد عادی خود ادامه دهد، بر روی ماشین اجرا کرد[9] .

۵- نتیجه گیری

ابرها برای مقابله با حمالات باید حمالات را شناخته و از فایروالها و شیوه های رمزنگاری قوی استفاده کنند و حفره های موجود در برنامه ها و پروتکل ها را به موقع ترمیم کنند.

۶- مراجع

[۱]. حامد نیشابوری، "محاسبات ابر"، دانشگاه سبزه وار، ۱۳۹۱.

[۲]. محسن صدر، محمد کارگر، " چالش ها و راه حل آنها درمحاسبات ابری "، هشتمین کنفرانس پیشبرد علم و تکنولوژی، ۱۳۹۲.

[3]. Sisalem, Dorgham, Jiri Kuthan, and Sven Ehlert. "Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms." IEEE Network 20, no. 5 (2006): 26-31.

[4]. Ormazabal, Gaston S., Henning G. Schulzrinne, Eilon Yardeni, and Somdutt B. Patnaik. "Prevention of denial of service
(DoS) attacks on session initiation protocol (SIP)-based systems using return routability check filtering." U.S. Patent 8,966,619, issued February 24, 2015.

[5].Thing, Vrizlynn LL, Morris Sloman, and Naranker Dulay. "Adaptive response system for distributed denial-of-service attacks." In 2009 IFIP/IEEE International Symposium on Integrated Network Management, pp. 809-814. IEEE, 2009.

[6].Wang, Bing, Yao Zheng, Wenjing Lou, and Y. Thomas Hou. "DDoS attack protection in the era of cloud computing and software-defined networking." Computer Networks 81 (2015): 308-319.

[7].Chonka, Ashley, Yang Xiang, Wanlei Zhou, and Alessio Bonti. "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks." Journal of Network and Computer Applications 34, no. 4 (2011): 1097-1107.

[8].Krutz, Ronald L., and Russell Dean Vines. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing, 2010.

[9.]Krutz, Ronald L., and Russell Dean Vines. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing, 2010.