پردیس بین الملل

پایان نامه کارشناسی ارشد

طراحی و پیاده سازی یک مدل امنیتی برای مقابله با حملات DDoS بر روی سرورهای وب

از:

ابوصالح محمد شریفی

استاد راهنما:

دکتر رضا ابراهیمی آتانی

شهریور ۱۳۹۰


بسم الله الرحمن الرحيم

مهندسی فناوری اطلاعات (تجارت الکترونیک)

طراحی و پیاده سازی یک مدل امنیتی برای مقابله با حملات DDoS بر روی سرورهای وب

از

ابوصالح محمد شریفی

استاد راهنما

دکتر رضا ابراهیمی آتانی

استاد مشاور

دکتر اسدالله شاه بهرامی

شهریورماه ۱۳۹۰

فهرست مطالب

فهرست جداول

فهرست اشکال

چکیده

طراحی و پیاده سازی یک مدل امنیتی برای مقابله با حملات DDoS بر روی سرورهای وب

ابوصالح محمد شریفی

بدون تردید، اینترنت باعث وقوع انقلاب فراگیر در کل سیستم ارتباطی دنیا شده است. به جرات می توان گفت که جهان هیچگاه شاهد چنین شتابی برای استفاده از یک پدیده علمی نبوده است. امروزه تصور زندگی بدون بسیاری از خدمات مبتنی بر اینترنت امکان پذیر نمی باشد. یکی از تهدیدات بزرگ برای ارائه خدمات ،حملات انکار سرویس توزیع شده می باشد،با وجود تحقیقات بسیار بر روی این موضوع، هنوز هم این حملات به عنوان یکی از بزرگترین نگرانی های ارائه خدمات مبتنی بر اینترنت باقی مانده است. تعداد زیادی از خدمات داده توسط بانکها، بیمارستان ها، دانشگاه ها و نظایر آنها نیازمند یک اتصال امن در اینترنت است. حفظ یکپارچگی، محرمانگی و در دسترس بودن خدمات نیز وابستگی بالایی به یک اتصال امن در شبکه دارد. سامانه های دانشگاهی یکی از این خدمات می باشند،این سامانه ها توسط کاربران زیادی مورد استفاده قرار می گیرند، لذا هرگونه اختلالی در ارائه خدمات توسط آنها موجب نارضایتی کاربران خواهد شد.

دراین پایان نامه با بحث در مورد جنبه های مختلف حملات انکار سرویس توزیع شده و مکانیسم های دفاعی ارائه شده در برابر آنها، مدلی برای مقابله با این حملات بر روی سرور طراحی و پیاده سازی می شود. برای درک بهتر حملات و ارائه راهکار مناسب، با راه اندازی این حملات بر روی یک سامانه دانشگاهی، نتایج حاصله ارزیابی شده و راهکار هایی برای دفاع در برابر آنها پیشنهاد می گردد.

کلمات کلیدی: حملات انکار سرویس توزیع شده، وب سرور، سناریو های حمله، تاثیر حملات، مکانیسم های دفاعی.

Abstract

Design and Implementation of a Security Model to Prevent DDoS Attacks on Web Servers
Aboosaleh Mohammad Sharifi

Undoubtedly, the Internet cause pervasive revolution in the hole world's communication system. Dare to say that the world never witnessed for used scientific phenomenon hastily. Now imagine living without many of the Internet-based services is not possible. One major threat to such services is Distributed Denial of Service (DDoS) attacks.

Despite of the plethora of research on the topic, yet, DDoS attacks still remains as one of the largest concerns for Internet based services. Several web services offered by banks, hospitals, universities, etc, require a secure connection over the internet. Protecting the integrity, confidentiality and availability in transit is of the objectives of a secure connection.

University systems have one of these services. These systems are used by many users;therefore, any disruption in services offered by them will lead to dissatisfaction among users.

The purpose of this thesis is to discuss the various aspects of Distributed Denial-of-Service (DDoS) attacks and defense mechanism against them, on web servers in the Internet. To better understand the attacks and provide appropriate solutions, launch attacks on one of the university system and evaluation results, then solutions for defense against them is recommended.

Keywords: Distributed Denial of Service attack, Web Server, Attack Scenario, Defenses Against Attacks

فصل۱ :

مقدمه

۱-۱- مقدمه

در ابتدا اینترنت به عنوان یک شبکه پژوهشی برای به اشتراک گذاری منابع تحقیقاتی شروع به فعالیت نمود، ازآنجاییکه گسترش و رشد اینترنت اولویت اول مطرح شده برای آن بوده است لذا مسائل امنیتی در آن بدرستی بررسی و پیاده سازی نشده است.امروزه اینترنت فقط به عنوان یک ابزار تحقیقاتی شناخته نمی شود بلکه به یک زیر ساخت اطلاعاتی برای جامعه جهانی تبدیل شده است. سازمانها، نهادها، دولتها و نظایر آنها با استفاده از اینترنت خدمات و اطلاعات خود را به شهروندان ارائه می دهند.

اینترنت با حذف محدودیت های جغرافیایی این توانایی را در اختیار یک کامپیوتر قرار می دهد که بتواند از راه دور به میلیونها کاربر در جهان خدمات ارائه نماید. با استفاده از این امکان، اینترنت بصورت گسترده ای بعنوان یک اصل در جامعه مورد قبول واقع شده و بطور فزاینده ای بعنوان یک بخش جداناپذیر از زندگی بشر تبدیل شده است.

افراد از امکانات چنین محیطی نظیر تجارت الکترونیک، دولت الکترونیک، آموزش الکترونیک، بانکداری الکترونیک و نظایر آن منتفع شده و تا حد زیادی منتفع می شوند. این امکانات عموماً با استفاده از وب سرو هایی که مختص این کار راه اندازی شده اند در دسترس کاربران قرار می گیرند، از این رو چگونگی تامین چنین خدماتی و قابلیت اعتماد و اطمینان کاربران به استفاده از آنها و خصوصاً امنیت بکارگیری چنین محیطی ازنگرانی مهندسین و پژوهشگران در این رابطه می باشد.

یکی از این حملات که قادر است دسترسی به اطلاعات را از کاربر سلب نماید، حملات انکار سرویس می باشد. یکی از بزرگترین نگرانی های امنیتی در راه اندازی وب سرور های ارائه دهنده خدمات در اینترنت، ناتوانی ذاتی اینترنت در مقابله با حملات انکار سرویس است. این حملات براحتی اجرا شده و بصورت محلی یا از راه دور قابل کنترل می باشند. اکثر این حملات در

رسیدن به اهداف اصلی حمله موفق بوده و مهاجم را به خواسته های خود می رساند. علت این امر دراین است که مکانیسم های زیادی برای راه اندازی این حملات بر اساس مشخصات سرور قربانی وجود دارد، همین امر خود موجب می شود که نتوان یک راه حل دفاعی جامع در برابر حملات ارائه نمود.

حملات انکار سرویس توزیع شده نوعی از حملات انکار سرویس می باشند که باعث بروز اختلالات شدیدتری خواهد شد. این قدرت تخریب ناشی از ماهیت ذاتی این حملات است. مهاجمان با استفاده از نقاط ضعف متعدد موجود بر روی سرور های هدف، حملاتی مخرب را راه اندازی می نمایند. ناتوانی اینترنت در مدیریت پهنای باند مصرفی موجب می گردد تا مهاجمان با خیال آسوده و با سرعت و حجم دلخواه، ترافیک حمله را بر روی هدف ارسال نمایند.

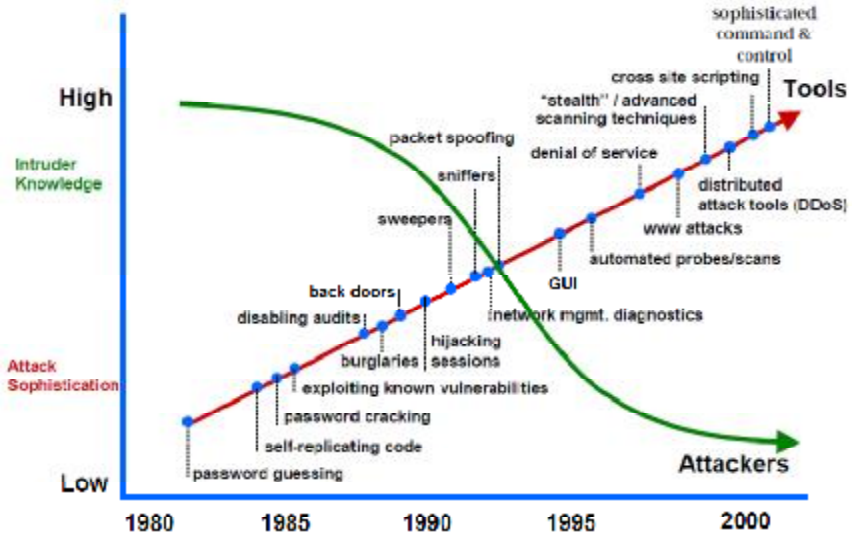
ماهیت غیر قابل تشخیص بودن مهاجم، در این نوع حملات خود مزید بر سایر دلایل است، مهاجم با راه اندازی یک حمله توسط بسیاری از سیستم های نا آگاه، خود از مسیر حمله خارج شده و منتظر نتیجه می ماند.

اگرچه بروز حملات انکار سرویس از دیر باز در اینترنت مطرح است اما تا زمانی که سایتهای معروفی چون Yahoo، Amazon، CNN و EBay در سال ۲۰۰۰ مورد حمله گسترده قرار نگرفته بودند[۱]، تحقیقات خاصی در ارتباط با این حملات صورت نگرفته بود. از آن زمان به بعد تحقیقات روند رو به گسترشی یافته و راهکارهای و مدل های امنیتی متفاوتی ارائه گردید. البته لازم به ذکر است که هیچ یک از این مدل ها نمی تواند یک تضمین مناسب و کاملی را در برابر این حملات ارائه نمایند.

اخیراً این حملات با بدافزار های متفاوتی نظیر ویروس ها، کرم های اینترنتی و... ترکیب شده و قدرت مخرب تری را از خود نشان داده اند، با این وجود هنوز هیچگونه پاسخی بجهت دفاع صد در صد در برابر آنها یافت نشده است.

گرچه بر پیچیدگی های فنی و تکنیکی این حملات روز بروز افزوده شده، اما برای راه اندازی این حملات، مهاجم نیاز به دانش بالا درباره سیستم قربانی و تکنیک های راه اندازی حملات ندارد.

برای درک بهتر این موضوع شکل زیر ارتباط دانش مهاجمان را در راه اندازی انواع حملات نشان می دهد.



شکل (۱-۱) رابطه دانش مهاجمان در برابر پیچیدگی حملات-گزارش موسسه CERT [۲].

همانطور که در شکل مشخص است، هرچه قدرت و پیچیدگی حملات بالاتر می رود دانش مهاجمین پایین ترمی آید.بعنوان مثال برای راه اندازی حملات تشخیص و یا شکستن رمز عبور مهاجم باید به دانش رمزنگاری و زبان اسمبلی آشنایی داشته باشد، اما برای حمله ای مانند انکار سرویس کافیست سیستمی با پهنای باند مناسب در اختیار گرفته و از ابزار رایگان موجود در اینترنت برای راه اندازی حمله استفاده نماید. بر این اساس مهاجمان بیشتر به سمت حملات مخرب تر علاقه مند شده و این امر موجب خطر بسیار بالاتری برای خدمات تحت وب خواهد بود.

تاثیر این حملات معمولاً بر اساس هدف حمله متفاوت می باشد اما می توانند ضربات مهلک اقتصادی، سیاسی و یا سازمانی را در پی داشته باشند. لذا ضروری است ضمن شناسایی این حملات، برای جلوگیری از آنها و یا به حداقل رساندن آسیب پذیری اقدامات مناسبی صورت یابد. برای مبارزه و دفاع در برابر این حملات مسائل تکنیکی نظیر پیشگیری، تشخیص، واکنش و مقاومت مطرح می شود. هدف از پیشگیری، رفع حفره های امنیتی مانند پروتکل های ناامن، طرح

های تصدیق هویت ضعیف و آسیب پذیرو نظایر آنها، که می توانند سنگ بنای راه اندازی حملات انکار سرویس شوند، می باشد.

هدف از این رویکرد، بهبود سطوح امنیتی جهانی است و بهترین راه برای مبارزه با حملات انکار سرویس در سطح تئوریک محسوب می شود. با این حال نقطه ضعف آن در عدم همکاری جهانی بدلیل گستردگی تجهیزات و کاربران می باشد. این امر موجب می شود چنین مکانیسمی در واقعیت عملی نگردد.

تشخیص حمله روش دیگری است که در برابر این حملات پیشنهاد می گردد. اغلب این روشها در تشخیص ترافیک غیر قانونی بجای قانونی دچار خطا می شوند، لذا تمرکز تنها بر روی این روشها قابل استناد نمی باشد.

هدف از واکنش در برابر حملات در واقع محدود کردن خسارات وارده می باشد، بطوریکه علاوه بر مبارزه با حمله بتوان به کاربران قانونی همچنان سرویس دهی نمود. البته برای این کار لازم است روشهای مقاومت در برابر حملات بمحض شناسایی فعال شوند.

۱-۲- اهداف پایان نامه

هدف اصلی این پایان نامه طراحی و پیاده سازی یک مدل امنیتی برای مقابله با حملات انکار سرویس توزیع شده بر روی سرور های وب می باشد. این مطالعه با هدف بررسی این حملات بر روی وب سرورها سعی دارد تا با فراهم آوردن یک درک کلی از حملات و روشهای راه اندازی آنها بهمراه مکانیسم های دفاعی بتواند راه مناسبی را در برابر سایر محققین قرار دهد. برای شناخت بهتر این حملات لازم است ابتدا وب سرور ها و مفاهیم آنها بیان شده، سپس نقاط ضعف آنها در برابر حملات انکار سرویس توزیع شده تشریح گردد.

در این مطالعه، با تمرکز بر روی حملات انکار سرویس توزیع شده، ابتدا ابزار های متداول راه اندازی این حملات را بیان شده و سپس طبقه بندی مناسبی را بر اساس تکنیک های عملکرد،

انتشار و همچنین شبکه های حمله ارائه می شود. در ادامه و برای شناخت مکانیسم های دفاعی در برابر این حملات، طبقه بندی کاملی از آنها به همراه نقاط ضعف هر یک ارائه می شود.

همانطور که قبلاً اشاره شد، سازمانهای زیادی خدمات خود را مبتنی بر اینترنت و وب سرور ها ارائه می نمایند، یکی ار مهمترین این سازمانها، دانشگاه ها و موسسات آموزش عالی می باشد.دانشگاه ها با راه اندازی سرور ها، البته تقریباً بدون تجهیزات مناسب امنیتی خدمات آموزشی و دانشجویی خود را در اختیار کاربران قرار می دهند. با توجه به اینکه تعداد کاربر استفاده کننده از این سرور ها بسیار زیاد می باشد، لذا هر گونه اختلال در دسترسی کاربران به این خدمات می تواند ضربات مهلکی را به چهره سازمانی دانشگاه ها وارد نماید.

البته لازم به ذکر است که اکثر مهاجمان احتمالی به این سرور ها دانشجویان بوده، که برای سرگرمی و شهرت در بین هم دانشگاهی های خود اقدام به راه اندازی این حملات می نمایند.این امر موجب می شود که در اکثر مواقع این سامانه ها تحت تاثیر حملات بوده و از دسترس سایر کابران خارج باشد. بنابراین بررسی امکان راه اندازی این حملات بر روی سامانه های دانشگاهی و ارزیابی نتایج حاصل از این حملات می تواند موجب شناخت بهتر حملات و ارائه راه کار های مناسب برای دفاع در برابر آنها گردد.

این سامانه ها معمولاً بدلیل ارائه خدمات مختلف در زمانهای خاص نظیر زمانهای انتخاب واحد، دریافت نمرات و...، بیشتر در معرض حملات انکار سرویس قرار دارند.حال در نظر بگیرید اگر مهاجمان در چنین زمانهایی حملات گسترده انکار سرویس را بر روی این سامانه ها راه اندازی نمایند و این حملات در زمانهای طولانی ادامه دهند، آنگاه این سامانه ها در مدت زمان زیادی از دسترس خارج خواهند شد، در این صورت نمی توان عکس العمل کاربران قانونی را پیش بینی نمود.

طبق بررسی های انجام شده اکثر این سامانه ها دارای نقاط ضعف و آسیب پذیری بالایی بوده که براحتی مهاجمان را به سمت خود ترغیب می نمایند، این آسیب پذیری های شامل موارد متعددی بوده که در فصول بعدی به تفصیل شرح داده می شود.

در این مطالعه ضمن بررسی سناریو های مختلف حملات انکار سرویس توزیع شده بر روی یکی از سامانه های مطرح دانشگاهی در کشور، نتایج حاصله بررسی شده و مدل امنیتی مناسبی بر پایه مکانیسم تشخیص حمله و واکنش مناسب در برابر آن برای این سامانه ها پیشنهاد می شود.

۱-۳- ساختار پایان نامه

مطالب موجود در پایان نامه بر اساس ساختاری که در ادامه می آید ارائه خواهد شد:

در فصل دوم، با بیان حملات رایج برروی وب سرور ها به بررسی اجمالی آسیب پذیری های آنها در برابر حملات انکار سرویس توزیع شده پرداخته می شود. این حملات بر اساس موارد متفاوتی نظیر پروتکل ها، ویژگی ها و خدمات ارائه شده بر روی آنها دسته بندی می شوند.

در فصل سوم بطور خاص حملات انکار سرویس توزیع شده مورد بررسی قرار گرفته و فرآیند های راه اندازی آنها عنوان شده، ابزار های متداول راه اندازی حملات با شیوه های مختلف توصیف می شود. این حملات با تکنیک های متعددی راه اندازی می شوند لذا در ادامه این حملات بر اساس تکنیک های انتشار، عملکرد و همچنین بستر شبکه راه اندازی، دسته بندی و ارائه می شود.

در فصل چهارم چالش های و مکانیسم های دفاعی در برابر حملات انکار سرویس توزیع شده بهمراه مشکلات و نقاط ضعف آنها بیان می گردد.از آنجاییکه اصول مدل های امنیتی دفاع در برابر حملات همیشه دارای چالش های متعددی می باشد، لذا بر اساس این چالش ها، مکانیسم های دفاعی دسته بندی و توصیف می شود. از آنجاییکه مکانیسم های دفاعی با استراتژی های مختلفی پیاده سازی می شوند، در ادامه این طبقه بندی براساس مکانیسم های پیشگیری، تشخیص، واکنش و مقاومت در برابر حمله ارائه می گردند.

در فصل پنجم برای ارائه یک مدل امنیتی مناسب به جهت مقابله با حملات بر روی سامانه های دانشگاهی، یک حمله با سناریو ها و تجهیزات مختلف پیاده سازی شده و نتایج آن ثبت می گردد.