این مقاله طبق مجوز شماره ۹۳/۱۷/۸۰۵ مرکز منطقه ای اطلاع رسانی علوم و فناوری RICeST زیر نظر وزارت علوم، تحقیقات و فناوری در آن مرکز نمایه و منتشر شده است.

بررسی حملات تحت وب،روش تشخیص و مقابله با آنها و امنیت در سرورهای ابری

پریسا هاشمی نیا[1]، ناصر نعمت بخش[2]

[1] گروه کامپیوتر،دانشگاه غیر انتفاعی شهید اشرفی اصفهانی،اصفهان،ایران

[2] استادیار،گروه کامپیوتر،دانشگاه غیر انتفاعی شهید اشرفی اصفهانی،اصفهان،ایران Nemat@ashrafi.ac.ir

چکیده

یکی دیگر از مسایلی که دنیای سرورهای تحت وب اهمیت دارد ، حملات وب می باشد که میتواند بسیار خطرناک باشند و سطح دسترسی کاربر را از یک سطح دسترسی پایین به سطح دسترسی root برسانند.امروزه بسیاری از کاربران مایلند که دادها و طلاعات خود را به صورت آنلاین به صورت همیشگی دسترسی داشته باشند.سیستم ها از حالت سنتی خار ج شده و جریان فن آوری اطلاعات به سمت یک پارچه نمودن سیستم ها و استفاده ی بهینه از آن ها به صورت آنلاین پیش می رود. این موضوع باعث ظهور سیستم هایی همچون سیست هاس ابری شده است.با توجه به گستردگی فعالیت سیستم های ابری،همچنین فراگیر بودن و دسترسی آنلاین با این سیستم ها، بررسی بحث امنیت امری ضروری و حیاتی است که سال ها مورد مطالعه قرار گرفته است.برای بررسی امنیت سیستم های ابری ابتدا بایست حمله به سیستم و شبکه را مطالعه نموده تا شناسایی وبررسی ضعف های موجود یا احتمالی،نکات امنیتی را حفظ نمود.

واژه های کلیدی:

وب ،Root ، سیستم های ابری ،امنیت ،روش های حمله در سیستم های ابری

مقدمه

امروزه با رشد و توسعه ی شبکه های کامپیوتری، بهبود وارتقای این شبکه ها از اهمیت بسیار بالایی برخوردار است.معیارهای مختلفی در ارتباط با سنجش عملکرد شبکه های کامپیوتری وجود دارد. اما در این بین مسئله ی امنیت از اهمیت بسار بالایی برخوردار می شوند که بسیار حا ئز اهمیت است که این حملات و نفوذ واقع شده بر روی شبکه به درستی و به سرعت شناسایی شود.در این بین روش های مختلفی جهت شناساییی حملات به شبکه ها وجود دارد که اساس این روش ها بر مبنای شناسایی و تشخیص بخش های غیرخودی از بخش های خودی قرار دارد.بخش های غیر خودی همان ویروس ها و حملات واقع شده در شبکه هستند.با ظهور خدمات ابری ،به دلیل اینکه نمیتوان مکان دقیق دادهای ذخیره شده را تشخیص داد، موضوع امنیت از حالت سنتی خارج شده است.در خدمات ابری،ارتباط با نرم افزارها و داده ها معمولا از طریق مرورگر وب صورت می گیرد و بستر پیاده سازی آن بر روی اینترنت است.یکی از چالش ها یا شاید بتوان گفت محدودیت های خدمات ابری، آنلاین بودن آن است.نکته مهم این است که برای حفظ محرمانگی و امنیت دادها باید مکانیزم های خاصی فراهم شود.امنیت باید به صورتی باشد که حتی اگر سیستم کاربر آلوده به بدافزار خاصی بود، تاثیربر سرویس دهنده ی ابر نداشته باشد و این سیستم ها فعالیت این بد افزارها را قبل از اجرا تشخیص داده و از بروز اتفاق های نا خواسته جلوگیری نمایند.

مانیتورینگ حملات و برنامه های سیستمی

در این بخش که معمولا وظیفه یک برنامه مانند آنتی ویروس می باشد، حملاتی از قبیل Buffer overflow ویا Format string را باید به دقت مانیتور کرد. از این رو با فرض بر اینکه تمامی موانع امنیتی ایجاد شده توسط هکر یکی پس از دیگری کنار گذاشته شود و می توان در این مرحله نبز رخ دادن چنین حملاتی را تشخیص داد.ضد ویروس اصطلاخی است که به برنامه یا مجموعه ای از برنامه ها اطلاق می شود که برای محافظت از کامپیوتر ها در برابر ویروس ها استفاده می شوند.مهم ترین قسمت هر برنامه ضد ویروس موتور اسکن آن است.جزئیات عملکرد هر موتور متفاوت است ولی همه آنها وظیفه اصلی شناسایی فایل های آلودهبه ویروس را با استفاده از امضای ویروس ها بر عهده دارند.بعضی از برنامه های ضد ویروس برای شناسایی ویروس های جریری که هنوز فایل امضای آنها ارائه نشده از رئش های جستجوی ابتکاری استفاده می کنند.

قابلیت های نرم افزار های ضد ویروس

سطح محافظت نرم افزار بسته به جریر و بروز بودن آن متغیر است. محصولات جدیدتر قابلیت هایی مانند بروز رسانی خودکار ، اسکن های زمان بندی شده، محافظت از سیستم به صورت ماندگار در حافظه و همچنین امکان یکپارچه شدن با برنامه های کاربردی اینترنتی مانند مرورگرهای وب ر ا دارند. نسخه های قدیمی ت نرم افزارهای ضد ویروس تنها یک اسکنر بودند که باید به صورت دستی راه اندازی می شدند.حداقل توقعی که می توان از یک برنامه ضد ویروس خوب داشت این است که در برابر ویروس های ماکرو ،اسب تروا و فایل های اجرایی آلوده به ویروس و کرم اقدامات محافظتی لازم را به عمل آورد.

آنتی ویروس

نرم افزار آنتی ویروس سه وظیفه ی عمده را انجام می دهد:

۱- بازرسی یا کشف[1]*

۲- تعیین هویت یا شناسایی[2]*

[1] Detection