ارزیابی تهدیدهای تجهیزات شبکه غیر بومی در دفاع سایبری

امیر حسین پورشمس[۱]، علی فانیان[۲]

[۱] مهندسی کامپیوتر- نرم‌افزار، دانشگاه صنعتی اصفهان
اصفهان- ایران

phz.ahp@gmail.com

[۲] استادیار دانشکده برق-کامپیوتر، دانشگاه صنعتی اصفهان
اصفهان- ایران

a.fanian@cc.iut.ac.ir

چکیده

در حال حاضر بخشی قابل ملاحظه‌ای از تجهیزات شبکه مورد استفاده در سازمان‌ها و نهادهای کشور غیر بومی هستند. هر کدام از این زیر ساخت‌های برقرار کننده ارتباط اطلاعات، قابلیت ایجاد حفره‌هایی از پیش تعریف شده‌ای را دارند که در صورت نیـاز، شرکت‌های سازنده می‌توانند با فراهم‌آوری فضای نفوذ، اختلال و یا سرقت اطلاعات، منافع شرکت‌های خود را تأمین نمایند، لـذا با توجه به استفاده روزافزون این تجهیزات در نهادهای راهبردی کشور، و اهمیت امنیت اطلاعات در این سازمان‌ها باید راه‌کاری اندیشیده شود تا آسیب‌پذیری به سازمان مورد نظر از این بابت کاهش یابد. در این مقاله ابتدا تعدادی از حملات امنیتـی کـه از این ناحیه وجود دارند مورد بررسی قرار می‌گیرند و سپس راه‌کارهای مقابله با این تهدیدات ارائه خواهد شد.

کلمات کلیدی:

امنیت شبکه، تجهیزات غیر بومی، شنود اطلاعات، اختلال سرویس، درب‌های پشتی

۱- مقدمه

اگر فضای سایبری را به همراه زیر ساخت‌های سخت‌افزاری و نرم‌افزاری‌اش به عنوان غیرقابل پیش‌بینی‌ترین حوزه‌های امنیتی کشور بدانیم گفته‌ای دور از حقیقت نیست چرا که استفاده از شبکه‌های کامپیوتری توسط نهادها و سازمان‌ها از چندین سال قبل آغاز، و در سالیان اخیر روند تصاعدی پیدا کرده است.

زیر ساخت‌های سایبری بستر مناسب فعالیت‌های سازمان‌ها را برای استفاده از فناوری و عرضه اطلاعات فراهم می‌نمایند، عرضه این اطلاعات می‌تواند در وسعت محلی[۱] و یا جهانی[۲] همچنین بصورت عمومی و یا محرمانه باشد، لذا هرچه اطلاعات محرمانه‌تر باشد تعریف نواحی امنیتی حساس‌تر و بیشتر معنا پیدا می‌کند. در یک شبکه مدرن و پیشرفته، منابع بسیاری برای حفاظت وجود دارند، تجهیزات شبکه مانند سوئیچ‌ها، مسیریاب‌ها، اطلاعات عملیات شبکه مانند جداول مسیریابی و پیکربندی لیست دسترسی، منابع نامحسوس مانند پهنای باند شبکه، پایگاه‌های داده و اطلاعات در حال تبادل در هر لحظه زمانی، از جمله مهمترین منابعی هستند که به نسبت ناحیه حساسیت سیستم باید مورد توجه بیشتر قرار بگیرند[۱].

به طور کلی حملات فضای مجازی در لایه پیوند داده[۳] و شبکه[۴] را به سه دسته عمده می‌توان تقسیم‌بندی نمود که عبارتند از دسترسی غیر مجاز به اطلاعات در حال تبادل شبکه[۵]، دستکاری و تغییر در منابع[۶] و حملات اختلال سرویس[۷]، حال اگر هر کدام از تجهیزات به کار رفته در شبکه خود به عنوان فراهم کننده بستر نفوذ و یا سرقت اطلاعات توسط درب‌های پشتی[۸] به کمک نفوذگر بروند، انجام هرکدام از این حملات ممکن و یا حداقل ساده‌تر خواهد شد [۷، ۲، ۱].

یک بسته داده[۹]با الگوی خاص اما قابل پذیرش برای لایه‌های امنیتی، پس از ورود به شبکه می‌تواند با ایجاد یک درب پشتی، فعالیت دیوارهای آتش برنامه‌ریزی شده با استانداردهای متعارف همچنین سیستم‌های تشخیص نفوذ را تحت تاثیر قرار داده و روند پیمایش شبکه را برای تشخیص آسیب‌پذیری و نفوذ نا تمام بگذارد.

لذا نفوذ به سخت‌افزارها و ارتباط با کامپایلر فرمان جهت اعمال دستور مورد نظری که نفوذگر دنبال آن است از راه‌های مختلفی در زیر ساخت‌های شبکه امکان‌پذیر می‌باشد، راه ذکر شده در این مقاله تلاش می‌کند تمامیت موضوع را با هدف اثبات این مسئله عنوان نماید که سازندگان و صاحبان منافع و قدرت برای اجرای اهداف خود در زمان نیاز و موقعیت‌های حساس خطر، به یقین راه‌های ویژه‌ای را در نظر می‌گیرند که تنها با آزمایش‌ها پی در پی و سیستمی قابل تشخیص خواهند بود.

پیش از طرح این موضوع به عنوان مقاله، بارها با اساتید و صاحب‌نظران دانشگاهی در این زمینه به گفت و گو پرداختم، صاحب نظران وجود چنین تهدیدی را در تمام سخت‌افزارها و نرم‌افزارهای تولیدی اثبات شده، اما تا حدودی غیرقابل کشف می‌دانند.

در این نوشتار تلاش خواهیم کرد به اثبات وجود این حفره‌های امنیتی در مهمترین ابزارهای غیربومی شبکه، که در بسیاری از زیر ساخت‌ها و تأسیسات زیربنایی در حال استفاده هستند بپردازیم.

۲- خطر وجود درب‌های پشتی

درب‌های پشتی و یا اعمال هدف از راه دور، به هر نوع معبر باز در یک سخت‌افزار و یا نرم‌افزار گفته می‌شود که حمله کننده بدون اطلاع یافتن مدیر سیستم و یا دیگر کاربران، به داخل سیستم نفوذ کرده و تمامی سیستم‌های امنیتی را دور بزند، به عبارت دیگر درب پشتی راهی ساده برای ورود و اعمال فعالیت بدون پیش نیازهای امنیتی می‌باشد[۲].

درب‌های پشتی انواع متفاوتی دارند که با هدف‌های گوناگون در سخت‌افزارها و نرم‌افزارها جاسازی می‌شوند. چندین درب پشتی فضایی را فراهم می‌کند که نفوذگر اهداف خود را ساده و بدون درگیری با سیستم‌های دیوار آتش و تشخیص نفوذ دنبال کند.

به طور معمول درب‌های پشتی مرتبط با نفوذگری در لایه دوم TCP/IPبه گونه‌ای طراحی می‌شوند که قالب خاصی از بسته‌های مخرب پنهان و در حال انتقال توسط پروتکل IP ، ICMP و TCP، بتوانند فرمان خود را توسط درب پشتی به سیستم هدف اعمال کنند، تا سیستم پس از مرور بسته و پردازش آن دستور مربوطه را اجرا کند[۷].

این درب‌ها که بر اساس نوع کامپایلر سیستم عامل سخت‌افزار ممکن است نوشته شده و بصورت نامحسوس در آن، جاسازی شده باشند، در تفکیک عملکرد به دو گروه عمده تک فرمان منفرد و اجرای فرمان از راه دور تقسیم‌بندی می‌شوند که به نسبت زمان نیاز امکان

[1] LAN
[2] WAN
[3] The Data-link Layer
[4] The Network Layer
[5] Interception
[6] Modification
[7] Interruption
[8] Backdoor
[9] Pocket

عمل و اعمال هدف نفوذگر را به سیستم جهت تخریب‌گری و یا سرقت اطلاعات فراهم می‌کنند[۷].

از آغاز ورود جهان به دنیای فن‌آوری اطلاعات بسیاری از این درب‌های پشتی که شرکت‌های سازنده برای زمان نیاز خود در سخت‌افزارها و نرم‌افزارها تعبیه کرده‌اند توسط نفوذگران کشف و مورد حمله قرار گرفته است اما آنها در برابر آن سکوت کرده‌اند.

نمونه‌ای تاریخی از وجود این باگ در سال ۱۹۸۲ میلادی بود که دولت شوروی در راستای برنامه کسب یا سرقت فناوری‌های حیاتی از ایالات متحده، کامپیوترهایی را برای کنترل خط لوله‌گاز ترانس، سیبری تهیه کرد. ماهیت پیچیده این خط لوله نیاز به سیستم‌های پیچیده‌ای را برای کنترل اقتضا می‌کرد. به همین دلیل،آن‌ها تصمیم گرفتند از فناوری‌های غربی استفاده کنند و سراغ کانادا رفتند CIA باعلم به این خرید، باگی را در این سیستم‌ها جاسازی کرد که در بررسی‌های اولیه روس‌ها خود را نشان نداد، اما بعد در عملیات باعث انفجار خطوط گاز شد[۳].

نمونه‌ای دیگر از باگ کشف شده در سال گذشته براساس تحقیق Secunia که مایکروسافت در برابر آن سکوت کرد آسیب‌پذیری در بخش Microsoft WMI Administrative Tools بود، مشکلی که در دو متد AddContextRef و ReleaseContext موجود در WMIObjectViewerControl با نام WBEM Single View Ctrl.1، وجود داشت و باعث نفوذ بدافزارها بر سیستم قربانی می‌شد و همچنین به واسطه آن هکرها می‌توانستند کدهای مورد نظر خود را بر سیستم هدف اعمال کنند[۱۱].

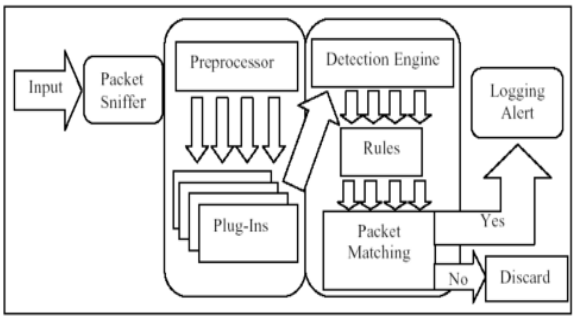
۲-۱- اثبات وجود درب‌های پشتی در سخت‌افزارها

در پروتکل TCP/IP هر ماشین ارتباط با کامپیوترهای درون شبکه را از طریق پورت‌های TCP و UDP انجام می‌دهد. تعداد این پورت‌های برای هر کدام ۶۵۵۳۵ پورت است. یک ماشین بدون عملکرد تبادل داده در شبکه معنایی نخواهد داشت پس اگر بخواهیم محدودترین حالت یک ماشین را در نظر بگیریم برای ارتباط با بیرون و تبادل داده حداقل نیاز به باز بودن و اتصال توسط یکی از این پورت‌ها دارد.

به یقین دیوارهای آتش بسته‌های غیر متعارف را شناسایی و از ادامه حرکت آنها در شبکه ممانعت به عمل خواهند آورد [۵]، سیستم‌های تشخیص نفوذ نیز یک رویداد خاص را نسبت به بسته‌های نامتعارف تولید می‌کنند اما خطر اصلی زمانی آغاز می‌شود که تمامی الگوهای غیر متعارف موجود در سیستم‌های تشخیص دهنده توسط سازمان‌های سازنده سخت‌افزار و تامین کننده منافع آنها تعریف شده باشد، علاوه بر اینکه یک بسته می‌تواند حاوی یک دستور خاص نفوذ با شکل متعارف نیز باشد.

اکنون یک سیستم نسل سوم تشخیص نفوذ [۱۰] را در نظر بگیرید، این سیستم به صورت فرآیندی نرم‌افزاری روی سخت‌افزار مورد نظر نصب و آن را به حالت بی قید و شرط می‌برد، به این معنی که تمام ترافیک شبکه در آن (دقیقاً همانند استراق سمع) مورد بررسی قرار می‌گیرد تا بر اساس قواعد تعریف شده یک رویداد یا Event تولید کند [۸].

نرم‌افزار Snort نمونه‌ای از عملکرد این سیستم است که از موتور IDS بهره گرفته، ترافیک شبکه را ربوده و آن را غربال می‌کند، سپس بر اساس مدل درونی که برای آن تعریف شده اقدام به انجام رخداد مورد نظر می‌نماید. در شکل (۱) مدل فعالیت این سیستم نشان داده شده است [۹،۸].



شکل(۱) : مدل ساختاری Snort

همانگونه که گفته شد سیستم به نسبت قواعد تعریف شده رخداد مورد نظر را تولید می‌نماید [۹،۸]. حال قواعد تعریف شده را بجای تشخیص بسته‌ها نامتعارف، با مدل متعارف الگوی خاص تعریف می‌کنیم، به وضوح مشخص است که سیستم خواهد توانست رویداد خاص را تولید کند.

این نوع حمله همچنین از مدل دیوارهای آتش نیز قابل اثبات است، لایه سوم دیوار آتش توسط فیلترهای هوشمند[۱۱] این توانایی را خواهد داشت تا نسبت به اعمال هدف مورد نظر اقدام کند، کافی است درون بسته در حال عبور از دیوار آتش برنامه‌ریزی شده، کلمه‌ای کلیدی جهت اعمال هدف مورد نظر باشد، دیوار آتش اقدام مورد نظر را انجام داده و بسته را به مقصد خواهد فرستاد [۷].

توزیع ناخواسته یک بسته در Backbone شبکه می‌تواند کل زیرساخت‌ها را مورد هجوم قرار دهد.

[10] Intrusion detection system
[11] State full

۲-۲- مدل تک فرمان منفرد و انتقالی

ازمیان انواع درب‌های پشتی که ممکن است سازمان‌های سازنده وابسته به اجرا کننده حمله در سخت‌افزارها استفاده کرده باشند مدل تک فرمان منفرد انتقالی است، این نوع درب پشتی به گونه‌ای است که نفوذگر با ارسال یک تک فرمان با الگوی خاص از طریق لایه انتقال[۱۲] به دستگاه هدف، در همان لحظه یک هدف را در ماشین مورد نظر انجام داده و ماشین همزمان با اجرای دستور یک نسخه تکرار از فرمان را به دیگر ماشین‌های متصل ارسال می‌کند [۲].

تزریق این فرمان اگرچه ممکن است از خارج شبکه و یا حتی در داخل شبکه و ناخواسته توسط فردی قربانی باشد، اما می‌تواند در قالب بسته‌ای قابل قبول برای دیوارهای آتش[۱۳] و سیستم تشخیص نفوذ در یک بستر شبکه حساس و مورد اهمیت در حوزه امنیتی تکثیر و در کوتاه‌ترین زمان پس از فراگرفتن بستر اصلی[۱۴] شبکه فعالیت آن را تحت تاثیر فرمان مورد نظر خود قرار دهد.

۲-۳- دسترسی به خط فرمان از راه دور (Remote Shell)

دسترسی از راه دور یکی دیگر از ابزارهای شناخته شده و پر توان اما قابل کنترل و حفاظت نسبت به مدل‌های منفرد است که می‌تواند در سخت‌افزارها برای اعمال تنظیمات مورد نیاز قرار گرفته باشد. ابزار یاد شده این امکان را به نفوذگر و یا کاربر می‌دهد تا با اتصال توسط یکی از راه‌های ارتباطی با سیستم عامل، فرمان‌های خود را بصورت موازی در آن اعمال نماید [۱۰].

سیستم عامل می‌تواند با یک رویداد خاص که توسط ترافیک گذرنده بر آن اعمال شده یکی از پروتکل‌های دسترسی از راه دور را بصورت هوشمند برای مهاجم باز کند تا وی بتواند دستورات لازم خود را توسط آن اجرا نماید [۲].

۳- مهم‌ترین حملات از طریق درب‌های پشتی

به طور معمول یک نفوذگر برای اجرای حمله‌هایی از جمله اختلال سرویس[۱۵] و یا شنود اطلاعات با این شرط که ماشین‌های هدف بصورت دقیق و بر اساس استانداردهای تعریف شده در لایه‌های شبکه پیکربندی شده باشد، نیازمند آن است تا از لایه‌های مختلف امنیتی عبور کرده و یا شاید حتی برای عبور از آنها نیز نا توان بماند، اما زمانی که درب‌های پشتی از پیش در سیستم نصب شده در اختیار وی قرار بگیرند، سختی‌های نفوذ ساده‌تر خواهند شد [۲].

به طور کلی براساس اهمیت زیرساخت‌های شبکه نصب و استفاده شده در حوزه‌های مختلف پیش‌بینی می‌شود دو حمله زیر برای دشمن در زمان نیاز مورد استفاده قرار گیرد.

۳-۱- اختلال سرویس

در تعریف حمله اختلال سرویس عبارت است از هر نوع اقدامی که موجب از کار افتادن یک ماشین و عدم فعالیت صحیح باشد. البته در بسیاری از مواقع حمله اختلال سرویس به عنوان پایه انجام حملات گسترده‌تر و فراهم کننده بستر لازم آن معنا می‌یابد [۱].

به طور معمول پیش‌بینی می‌شود حمله کننده برای اختلال در سرویس، سخت‌افزارهای اصلی شبکه از جمله مسیریاب‌ها، سوئیچ‌ها و هاب‌ها را به عنوان زیرساخت‌های اصلی مورد هجوم قرار بدهد [۷،۲].

۳-۱-۱- اختلال سرویس در مسیریاب‌ها

مسیریاب را به عنوان متصل کننده دو شبکه و سازنده یک شبکه می‌توان دانست که دو پروتکل متفاوت در لایه پیوند داده را به یکدیگر متصل می‌کند، لذا اختلال سرویس در یک مسیریاب می‌تواند بنیان فعالیت یک شبکه را به خطر اندازد [۷،۱].

یک مسیریاب، آدرس موجود در سرآیند[۱۶] پروتکل لایه شبکه که مشخص کننده مقصد نهایی بسته دریافت شده است را می‌خواند و آن را به مقصد یا به مسیریاب بعدی که در بسته مشخص شده تحویل می‌دهد.

یک بسته تخریبی که به دلیل پیروی از الگوهای معمول از دیوار آتش گذشته و در حال ورود به مسیریاب است، در صورت داشتن مدل خاص در سرآیند بسته IP می‌تواند تا لایه کاربرد بالا رفته و پس از خواندن بسته، دستور موجود آن را اجرا کند.

یکی از مهمترین دستورهای تخریبی که ممکن است در یک مسیریاب رخ دهد، حذف جدول مسیریابی می‌باشد، این هدف ممکن است با پاک کردن مستقیم و یا پاک کردن برنامه‌ریزی[۱۷] از پیش تعریف شده برای ماشین انجام شود، یک روتر ممکن است خود با

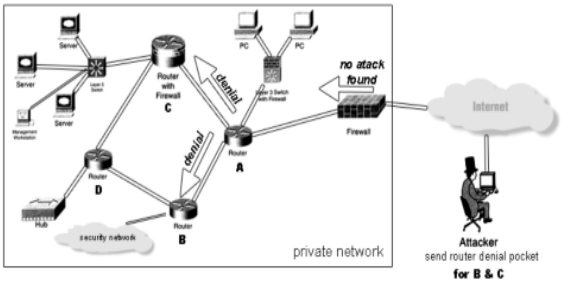
[12] Transport
[13] Firewall
[14] Backbone
[15] Denial of service
[16] Header
[17] Configure

دیگر دیوارهای امنیتی ایجاد شده در مقابل نفوذ اتصال سری داشته و با از کار افتادن آن، کل سیستم امنیتی دچار اختلال شده و فضا برای حمله اصلی باز شود [۷،۵].

وارد شدن بسته به یک روتر نسبت به اتصالات آن ممکن است بصورت ناخواسته توسط یکی از ماشین‌های متصل به شبکه داخلی در شبکه‌های خصوصی، و یا توسط یک حمله کننده از بیرون در شبکه‌های گسترده و عمومی باشد.

مدل حرکت یک بسته اختلال سرویس که در حال عبور از سخت‌افزارها برای رسیدن به مقصد مورد نظر و اعمال رخداد خود است، در شکل (۲) قابل مشاهده است.

یک بسته همچنین می‌تواند یک پورت در لایه کاربرد را برای حمله کننده باز کند تا اقدامات خود را توسط سیستم‌های کنترل از راه دور انجام دهد.



شکل (۲) : اختلال سرویس در مسیریاب

۳-۱-۲- اختلال سرویس در سوئیچ و هاب

اگرچه مدل‌های قدیمی سوئیچ و هاب در لایه دوم فعالیت کرده و به همین دلیل دارای پردازنده‌های ضعیف و توان انجام فعالیت‌های سطح بالا را ندارند، اما امروزه سوئیچ‌ها با قابلیت فعالیت در لایه‌های بالاتر نیز روانه بازار شده‌اند، لذا با توجه به تولید بدافزارهای[18] دارای کدنویسی سطح بالا، پیش‌بینی می‌شود این ماشین‌ها نیز تحت حمله اختلال سرویس قرار بگیرند.

اختلال سرویس در سوئیچ و هاب بیشتر با هدف اعمال خراب کارانه انجام می‌گردد. البته زمانی حساسیت حمله نا محسوس به یک سوئیچ مشخص می‌شود که دستگاه‌های متصل به آن قسمت‌های حیاتی یک تاسیسات زیربنایی را تشکیل می‌دهند و یا به عنوان رابط‌های شبکه در یک مجموعه ماشین صنعتی مورد استفاده قرار گرفته باشند.

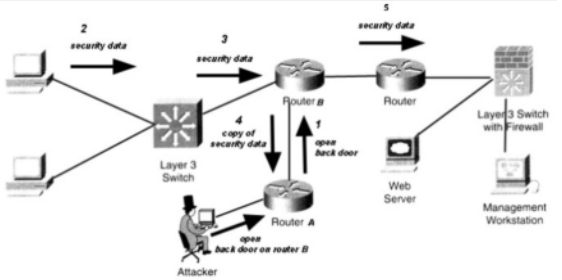
یک بسته همچنین می‌تواند با اعمال دستور در سوئیچ، درگاه کاوشگر حمله را نیز برای لحظاتی متوقف کند تا نفوذگر بتواند اقدامات بعدی خود را نسبت به سیستم اعمال کند [۵].

۳-۲- شنود و اسراق سمع

به طور کلی حمله استراق سمع عبارت است از تلاش به گوش دادن اطلاعات در حال تبادل در سطح شبکه که در لایه پیوند داده انجام می‌شود که نفوذگر بدون انجام اقدام محسوس در سطح شبکه، این اطلاعات در حال تبادل را زیر نظر گرفته و بر اساس نیاز خود، اطلاعات مورد نیاز را از جمله شناسه‌های کاربری و کلمه‌های عبور ارسال شده، پرس و جوها، پاسخ‌های DNS پیغام‌های پست الکترونیک حساس و دیگر اطلاعات مربوطه را جمع‌آوری می‌کند [۲].

۳-۲-۱- استراق سمع از مسیریاب‌ها

یک مسیریاب به عنوان سازنده شبکه پل اصلی عبور داده‌هاست، یک تحلیل کننده دیتا در لایه‌های بالایی همانگونه که می‌تواند بسته‌های در حال عبور را تحلیل و سپس بر اساس دستور تعیین شده اقدام لازم را انجام دهد، همانگونه نیز می‌تواند در صورت مطابقت با الگوی تعریف شده یک نسخه آن را به مقصدی دیگر ارسال کند. مدل ارسال یک بسته فرمان شنود در شکل (۳) رسم شده است.



شکل (۳) : مدل ارسال یک بسته داده

اطلاعاتی که برای یک حمله کننده مهم است، می‌تواند نام‌های کاربری یا کلمه‌های عبور در حال عبور از یک مسیریاب برای اتصال به شبکه‌های دیگر باشد [۲]. این دیتاها زمانی اهمیت ویژه پیدا خواهند کرد که مربوط به یک شبکه زیر بنایی در حال فعالیت درون تاسیسات مهم باشند. البته روش دیگری نیز برای استراق سمع[19] وجود دارد، بسته دارای الگو، رخدادی را برای باز کردن یکی از پورت‌ها در لایه کاربرد به ماشین مورد نظر ارایه تا آن را اجرا نماید،

[18] malware

[19] Sniffer

سپس درگاه باز شده در لایه کاربرد[20] می‌تواند بستری را برای شنود اطلاعات در اختیار حمله کننده قرار دهد [۷].

۳-۲-۲- استراق سمع از سوئیچ و هاب

استراق سمع از سوئیچ و هاب نیز دقیقاً همانند شنود اطلاعات از مسیریاب‌ها است، با این تفاوت که احتمال وجود ابزار کمک کننده برای استراق سمع با توجه به پردازشگر ضعیف آنها اگرچه غیر ممکن نیست اما با احتمال ضعیف فرض می‌شود.

با این وجود یک سوئیچ پس از دریافت بسته الگو می‌تواند بر اساس دستور موجود کپی از بسته‌های تعریف شده که وارد آن می‌شود را به یکی دیگر از درگاه[21]های متصل و یا اینترفیس‌های تعریف شده ارسال نماید.

۴- راه کارهای مقابله

از دیدگاه صاحب‌نظران، موضوعات مطرح شده در این مقاله اثبات شده اما از طرفی دیگر اگر نگوییم غیر قابل کشف، یافتن آنها بسیار دشوار خواهد بود. چرا که به عنوان یک برگ برنده در اختیار شرکت‌های قدرتمند سازنده‌ای است که می‌توانند در زمان مورد نیاز از آن استفاده نمایند.

ضرورت آمادگی در دفاع سایبری باید به گونه‌ای باشد که حتی آخرین برگ و یا تنها برگ برنده نیز از جدول نفوذگران برای اعمال هدف خود حذف گردد.

از طرف دیگر استفاده از تجهیزات غیر بومی شبکه در حوزه‌های مختلف از جمله صنعت، تجارت، سازمان‌ها و نهادها و ... ضرورتی اجتناب‌ناپذیر است، از این رو لزوم مقابله با تهدیدات احتمالی ذکر شده پررنگ و بیشتر احساس می‌شود.

راهکارهای زیر جهت مقابله با تهدید عنوان شده پیشنهاد می‌گردد.

۴-۱- مانیتورینگ همزمان، مقایسه و اسکن شبکه

یکی از اقداماتی که به گروه‌های مقابله با هجوم سایبری کمک می‌کند تا حمله‌های نفوذگران را ناکام بگذارند، مانیتورینگ همزمان، مقایسه و اسکن شبکه در تمام قسمت‌های گسترده آن است [۵،۲،۱].

متاسفانه این مهم در بسیاری از شبکه‌های حساس مورد توجه قرار نگرفته و معمولا بصورت جزئی انجام می‌گیرد.

در مدل پیشنهادی، برای مقابله با تهدید ذکر شده به نسبت حساسیت یک شبکه و جایگاه استفاده، باید ترافیک مورد تبادل تمام اینترفیس‌ها و درگاه‌های شبکه در مسیریاب‌ها و سوئیچ‌ها مورد کنترل همزمان در سیستم‌های مقایسه‌گر قرار بگیرد.

با فرض فعالیت دقیق دیوار آتش برای مقابله با بسته‌های نامتعارف و با توجه به اینکه سخت‌افزارهای شبکه گیرنده و فرستنده اطلاعات هستند (غیر از زمان برنامه‌ریزی خود ماشین[22]) تمام ترافیک صحیح ورودی باید به مقصد دیگری منتقل شود.

هر نوع ناهماهنگی در ورودی و خروجی اینترفیس‌ها و یا درگاه‌های مبادله می‌تواند نشانی از حمله نا محسوس و یا بسته هجومی عبور کرده از دیوارهای آتش باشد.

همچنین باید ماشین‌ها در سطح لایه کاربرد مرتبا در حال اسکن و گزارش‌گیری باشند چرا که باز شدن یک پورت در این لایه می‌تواند نشان نفوذ و یا عملکرد درب پشتی برای اعمال اهداف نفوذگر باشد.

۴-۲- رمزنگاری تمام داده‌های در حال تبادل

یکی از اساسی‌ترین راه‌ها و مدل‌های پیشنهادی برای مقابله با حفره‌های مخفی شده در زیر ساخت‌های شبکه، رمز نگاری تمامی داده‌های در حال مبادله بین ماشین‌های آن است.

رمز نگاری داده‌ها فرمی از کد کردن داده‌های بین سیستم ارسال کننده بسته درون شبکه و دریافت کننده آن است، به طوری که غیر از گیرنده و فرستنده، فرد دیگری در میانه راه توان بررسی اطلاعات را نداشته باشد [۱].

تغییر و رمز شدن داده‌های در حال ورود و خروج از شبکه و مقابله با ورود هر نوع داده رمز نشده به سیستم همان رخدادی است که تا حدودی خواهد توانست از انجام فعالیت هر نوع بسته ساخته شده برای فعالیت‌های تخریبی جلوگیری کند.

با توجه به اینکه سخت‌افزارهای شبکه تولید شده تاکنون از پردازشگرهای بسیار قدرتمندی برخوردار نیستند، رمزگشایی و تحلیل داده‌های کد شده برای آنها بسیار دشوار خواهد بود، از طرفی داده‌های تغییر یافته نیز امکان اعمال فرمان مورد نظر را نخواهند داشت.

[20] Application
[21] Port
[22] Configure

البته این سیستم اغلب در شبکه‌های خصوصی و غیر مرتبط با شبکه‌های گسترده مانند اینترنت کاربرد خواهد داشت. رمزنگاری کلید عمومی مدل مناسبی است تا داده‌های در حال مبادله بین شبکه تنها توسط مبدا و مقصد ارسال کننده پیام قابل دسترسی باشند.

۴-۳- آزمایش‌های نفوذپذیری

آزمایش نفوذپذیری فرآیندی است که جهت ارزیابی امنیت ماشین‌ها و سیستم‌های متصل به شبکه انجام می‌شود، به این صورت که تیم امنیتی با سناریو و شبیه‌سازی حمله به یافتن حفره‌هایی می‌پردازد که سیستم را در زمان حمله نفوذگر، در سطح آسیب‌پذیری قرار می‌دهد.

نیاز به یک آزمایشگاه تست نفوذپذیری سخت‌افزارها در شبکه‌هایی که قرار است داده‌های حساس و امنیتی را مبادله کنند ضروری است، با توجه به حمله عنوان شده مهم‌ترین مواردی که در این آزمایشگاه‌ها باید مورد بررسی قرار بگیرد سیستم عامل مسیریاب‌ها و سوئیچ‌های بکار رفته در شبکه می‌باشد.

تحلیل مدل و ساختار سیستم عامل سخت‌افزار، نحوه هماهنگی سیستم عامل با کامپایلر و پردازنده، آزمایشژهایی هستند که می‌تواند در تشخیص حفره امنیتی موجود در ماشین مورد نظر ما، را یاری دهد.

پردازش بسته‌های گوناگون به نسبت پیچیدگی آنها جهت تحلیل توسط موتور IDS حجم متفاوت از پردازنده را در اختیار می‌گیرد [۹]. لذا می‌توان در آزمایش‌های متوالی، بسته‌های متفاوت را به سیستم وارد و واکنش پردازنده را نسبت به آن بسته تحلیل کرد.

۴-۴- رسم مدل ساختاری شبکه بصورت پویا همراه با مقایسه‌گر

ساختار آنالیز شبکه بصورت پویا[23] باید در اختیار مدیران امنیتی باشد و لحظه به لحظه با مدل‌های رسم شده توسط پویشگرها و اسکنرها همچنین گراف ترافیک شبکه[24] مقایسه گردد [۵].

هر نوع اختلاف در مدل ساختاری تعیین شده و گزارش دریافت شده توسط دیگر سیستم‌های کنترل امنیت می‌تواند نشانی از تلاش نفوذگر به سیستم و یا ورود یکی از بسته‌های بیان شده به سیستم برای تخریب یا شنود اطلاعات باشد.

۴-۵- ایجاد شبکه‌های معادل موازی و پنهان

با فرض اینکه راه‌های مقابله با حمله موفق عمل نکرد و نفوذگر توانست بسته خود را وارد شبکه کرده و در آن اختلال ایجاد کند، شبکه‌های معادل و موازی که از دید نفوذگر و بررسی کننده شبکه پنهان شده‌اند با شبکه اصلی به عنوان پشتیبان عمل کرده و موجب ادامه فعالیت شبکه بدون اختلال تا زمان رفع مشکل و بازگردانی به حالت معمول خواهند شد [۵].

همچنین این شبکه‌ها را می‌توان به گونه‌ای در مدل ساختاری شبکه اصلی در نظر گرفت که نفوذگر دچار خطا شده و بجای شبکه اصلی معادل‌ها را مورد حمله اختلال و یا شنود قرار دهد [۵].

۴-۶- حرکت به سمت بومی‌سازی

در کنار تمام راه‌کارهای مقابله امنیتی که عنوان شد، یکی از ضرورت‌ها و موضوعاتی که طی سال‌های اخیر بارها مورد تاکید رهبر معظم انقلاب قرار گرفته بومی‌سازی فن‌آوری‌های راهبردی می‌باشد، که در حوزه زیرساخت‌های شبکه و ابزارهای مربوطه با توجه به روند افزایش تهدیدات سایبری و لزوم مقابله با آن کمتر مورد توجه قرار گرفته است.

ایشان در سیاست‌های کلی نظام که در بهمن ماه سال ۸۹ ابلاغ شد، ارتقاء سطح دانش و ظرفیت‌های علمی، پژوهشی، آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت فضای اطلاعاتی و ارتباطی (افتا) و همچنین تکیه بر فناوری بومی و توانمندی‌های تخصصی داخلی در توسعه زیرساخت‌های علمی و فنی، امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی را مورد توجه قرار داده‌اند[۴].

لذا حرکت به سمت بومی‌سازی این فضا در چهار حوزه مهم و اساسی بومی‌سازی سخت‌افزارها، ایجاد رمزنگاری بومی در انتقال داده‌ها، بومی‌سازی دیوارهای آتش و سیستم‌های تشخیص نفوذ با توجه به روند افزایش تهدیدات سایبری برای جلوگیری از سه نوع حمله امنیتی و خطرساز شنود اطلاعات، تخریب اطلاعات و حملات اختلال سرویس قابل توجه ارزیابی می‌شود.

امروز در روند رسیدن به امنیت پایدار در حوزه سایبری، این مهم احساس می‌شود که متخصصان حوزه‌های سخت‌افزاری و امنیت حرکت پر سرعت‌تر و جدی‌تری را برای تحقق این فرمان معظم له بردارند.

[23] Dynamic Network Analysis
[24] Bandwidth monitoring

۵- نتیجه‌گیری

سرعت توسعه سخت‌افزارها و زیرساخت‌های شبکه نیاز به فراهم کردن امنیت سایبری لازم دارد که باید توسط نهادهای متخصص و علمی تعیین شود. در این میان زیرساخت‌های شبکه غیر بومی که بیشتر آنها توسط شرکت‌های تامین کننده منافع قدرت‌های استکباری تولید و توزیع می‌شود خود می‌توانند به عنوان تهدیدی درون شبکه باشند. یکی از حفره‌های اثبات شده اما به سختی قابل کشف در این سخت‌افزارها درب‌های پشتی هستند، این درب‌ها فضایی را فراهم می‌کنند تا نفوذگر بدون نیاز به عبور از در دیوارهای امنیتی خواسته خود را بر روی سیستم اجرا کند.

خواسته‌های نفوذگر ممکن است ایجاد اختلال سرویس و یا سرقت اطلاعات حساس بر اساس الگوهای تعریف شده باشد که به طور معمول مسیریاب‌ها و سوئیچ‌ها به عنوان اصلی‌ترین زیرساخت‌های شبکه تحت هجوم قرار خواهند گرفت. اگرچه این حفره‌های امنیتی به سختی قابل تشخیص هستند اما راه کارهای ارایه شده در این مقاله تا حدی خواهد توانست فضای انجام فعالیت نفوذگر را محدودتر سازد. بکارگیری اقدامات بیان شده در شبکه‌های حساس و مرتبط با فعالیت‌های زیربنایی و امنیتی ضروری است.

مراجع:

[۱] ملکیان، احسان، نفوذگری در شبکه و روش‌های مقابله، تهران، نص، ۱۳۸۸

[۲] داوری دولت‌آبادی، مجید، مرجع کامل حملات هکری و روش‌های مقابله، تهران، پندار پارس، ۱۳۸۷

[۳]ماهنامه شبکه - خرداد ۱۳۹۰ شماره ۱۲۲

[۴] پایگاه اطلاع‌رسانی دفتر حفظ و نشر آثار مقام معظم رهبری http://farsi.khamenei.ir

[5] Convery Sean, *network security architectures* , cisco press, 2004

[6] Joe Grand, Ryan Russell, *hardware hacking*,syngress, 2004

[7] Jason Andress, Steve Winterfeld, *Cyber warfare*, elsevier, 2011

[8] FaeizAlserhani, MonisAkhlaq, IrfanAwan, Andrea Cullen, John Mellor and, PravinMirchandani, *Evaluating Intrusion Detection Systems in High SpeedNetworks*,In Press, Fifth International Conference of Information Assurance and,Security (IAS), IEEE Computer Society,2009

[9] Dihua Liu, Hui Li, *Research on Intelligent Intrusion Prevention System Based on Snort*, International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE),2010

[10] AniruddhaBohra, IulianNeamtiu, Pascal Gallard, Florin Sultan, and LiviuIftode, *Remote Repair of Operating System State Using Backdoors*, Autonomic Computing. Proceedings. International Conference, 2004

[11] *http://secunia.com*