مدل لايه بندی شده امنيت شبکه

سيد رضا کامل طباخ فريضي
دانشگاه آزاد- واحد تهران جنوب
Rezakamel@toosashena.com
مريم شاه پسند
موسسه آموزش عالي سجاد
E_sh_1983@yahoo.com

چکيده : با پيشرفت و گسترش روزافزون استفاده از کامپيوتر و شبکه ها در زمينه هاي مختلف علمي و تجاري و همچنين فراگير شدن استفاده از اينترنت . دنياي شبکه اطلاعات, مبدل به محيطي شده است که نياز به وجود چهارچوب، قوانين، محدوديت ها و اعمال سياستهاي امنيتي براي آن بيشتر احساس مي شود.از کاربران اماتور,نفوذگران شبکه ,افرادي که از اينترنت براي پرشدن وقت خود استفاده مي کنند،تا شرکت هاي بزرگ که نقل و انتقالات مالي يا تجاري خود را در مقياس وسيع بر روي اين شبکه انجام مي دهند همه و همه مشترکين تکنولوژي عصر حاضر مي باشند . در چنين دنياي مجازي مي توان گفت که امنيت يک ضرورت است نه يک انتخاب براي هر مقياس .

کلمات کليدي : security , firewall , sniffing , spoofing .

۱- مقدمه

آنچه در اين مقاله ارائه داده مي شود يک مدل پيشنهادي لايه بندي شده در خصوص امنيت شبکه مي باشد و سعي شده تا در ساختار ارائه شده حتي الامکان مستقل از توپولوژي شبکه يا سازمان مربوطه باشد. در واقع اين مدل به صورت کلي براي کوچکترين شبکه ها تا بزرگترين شرکتها و شبکه هاي آنها قابل استفاده مي باشد. فقط نياز به اضافه يا کم کردن اهميت هر يک از سطوح هرم مي باشد که مسلماً با هزينه رابطه مستقيم دارد.

۲- امنيت در يک نگاه

بيشتر گفتيم که امنيت يک ضرورت است نه يک انتخاب و اين اهميت مستقل از مقياس شبکه مي باشد . اکنون مي توان اضافه نمود که تدابير امنيتي در يک شبکه هيچگاه يک آرايش صد درصد را براي شبکه ايجاد نخواهند نمود زيرا امنيت شبکه به فاکتورهاي بسيار متنوعي وابسته است. در واقع امنيت براي يک شبکه حکم ديوار را دارد, با اعمال تدابير مختلف امنيتي ما فقط مي توانيم ديوار را بالاتر ببريم اما هيچگاه نمي توانيم سقف ايجاد کنيم. با اضافه کردن اين مطالب که اگر کسي کليد داشته باشد و از در وارد شود طول ديوار کمکي نمي تواند بکند. به هر حال فقط کليد يا کلمات عبور و ساير ورودیهاي امن شبکه جزئي از هرم امنيتي به شمار مي آيد. پياده سازي هرم از بالا به پايين از دو بعد قابل اهميت است اول اينکه تعداد از افراد يا برنامه هايي که مي تواند اين سطوح امنيتي را پشت سر بگذارند کاهش

مي يابد (كاهش شانس نفوذ) و دوم اينكه زحمت اين گروه افراد يا برنامه بيشتر مي شود. (فاكتورها كاري يا كارهاي كه بايد انجام بدهند.)در واقع ديوار بلندتر به نردبان و افراد ماهرتري نياز دارد. شايد فقط اطلاع از بلندي ديوار نفوذگر را از شروع به كار مأيوس نمايد. در واقع سرفصل امنيت يک سرفصل پررنگ و قابل توجه در هزينه هاي سازمان بايد باشد.[3]

۳- Protocol analyzer

تحليلگرهاي پروتكل اولين سد امنيت و نوك اوليه هرم امنيت را در سايتها تشكيل مي دهند با استفاده از اين ابزراها كوچكترين حركات مشكوك قابل شناسايي بوده و مي توان خلآهاي امنيتي و محلهاي قابل نفوذ و آسيب پذير را در سايت مشخص نمود. استفاده از اينگونه ابزراها امكان بررسي و تحليل داده هاي مختلف مربوط به پروتكلهاي گوناگون، بررسي ترافيک شبكه، تشخيص برخي مشكلات و گردآوري اطلاعات آماري در مورد شبكه ها را فراهم مي كند. از ديگر موارد كاربرد اينگونه ابزارها مي توان به تشخيص عدم ارتباط يک ايستگاه كاري يا شبكه و بررسي دليل آن تشخيص خرابي تجهيزات و كشف تداخل آدرسها, كنترل شبكه براي پورتهاي باز و تلاشها و دسترس هاي مشكوک و ... اشاره كرد. ظاهراً به نظر مي رسد كه تحليلگرهاي پروتكل بيشتر ابزار مانيتورينگ شبكه باشند تا ابزار صنعتي اما از آنجايي كه در برخي شرايط تفاوت دستاورد يک حمله بالابردن ترافيک شبكه يا سرريز كردن يا سرويس خاص مي باشد, تحليلگرهاي پروتكل مي توانند با اعلان به موقع قبل از حاد شدن هر مشكل آن اطلاع دهند.در واقع مستقل از وجود يا عدم وجود ديوارهاي امنيتي شبكه نياز به نگهباني آگاه دارند كه شبانه روز از صحت شبكه و رفت و آمدهاي مشكوک اطمينان حاصل نمايند و در صورت وجود هر فرايند مشكوک آن را اطلاع دهد.[4]

۴- **Routing :**

استفاده از تكنيكهاي مسيريابي مي تواند يكي از قدرتمندترين لايه هاي امنيتي را در شبكه به وجود آورد [4] با پيكربندي صحيح مسيريابي در شبكه مي توان به صورت خودكار, از دسترسي هاي غيرمجاز جلوگيري كرد. همچنين با كمک اين تكنيكها مي توان برخي از پروتكل ها، دستورات و سرويسهاي شبكه را براي يک سري از بسته هاي مشخص (از لحاظ مبدأ و مقصد) غير فعال و يا دسترسي به برخي منابع را براي يک گروه كاري خاص كه داراي يک پورت ورودي يا آدرس خاص هستند محدود كرد.[5]

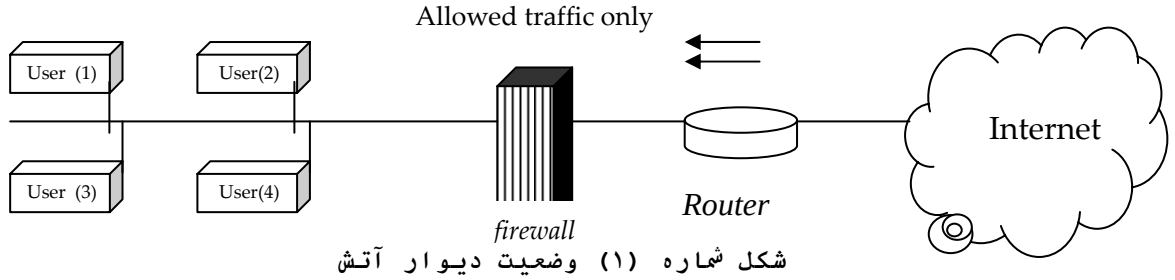
در واقع مسيريابي صحيح در شبكه مانند ايجاد بزرگي راههاي بدون فرعي و تقاطع ها غير همسطح مي باشد كه به خودي خود سدي در برابر دسترسيهاي غير مجاز مي باشد اما بايد در نظر داشت كه ايجاد محدوديتهاي سرويس يا تنظيم قوانين در مسيريابها سربار قابل ملاحظه اي بر روي تجهيزات قرار مي دهد كه مسلماً نياز به استفاده از مسير يابهاي قدرتمندتري را در شبكه به وجود مي آورد (افزايش هزينه) از طرف ديگر هر چه با كاري مسيريابها به حد مرز خود نزديک تر باشد, نفوذگران نياز به زحمت كمتري جهت افزايش باركاري سرريز كردن پشته ها و ميسيريابها يا سوئيچهاي لايه۳ دارند كه خود يک راه نفوذ را براي آنها باز مي گذارند. در اكثر مسيريابها با افزايش بار كاري از حد نرمال باعث مي شود مسيريابي از برخي از قواعدي كه باركاري زيادي بر روي مسيرياب مي گذارند صرف نظر كند (مانند acl ها) و اين دقيقاً همان چيزي است كه نفوذگر مي خواهد . در برخي از سوئيچ ها نيز سرريز شدن جدول مسيريابي سوئيچ باعث مي شود تا سوئيچ مشكي هاب عمل كرده و اطلاعات در شبكه broad cast شوند به عنوان مثال براي يک

سيستم نفوذ رساندن باركاري زير ۱۰% به بالاي ۹۰% بسيار دشوار تر از رساندن باركاري ۸۰% به بالاي ۹۰% مي باشد كه باعث باز شدن برخي از راهها نفوذ و يا سرريز شدن مسيريابها مي شود

لازم به ذكر است ايجاد چنين پيكربندي نياز به افراد مجرب و مهندسان خبره دارد كه داراي تسلط كافي بر ساختار سايت و اهداف آن باشند. همچنين قدرت امنيتي سيستم عاملهاي موجود بر روي مسيريابهاي مورد استفاده نيز در امنيت ايجاد شده نقش مهمي را ايفا مي كند.[3]

: firewall -۵

با استفاده از ديواره هاي آتشين مي توان تمام نقاط اتصال يك شبكه داخلي با خارج را به يك يا چند نقطه تبديل و به اين شكل كليه ارتباطات با دنياي خارج را مورد بررسي و كنترل قرار داد[۳] و از آنها گزارش تهيه كرد.در واقع firewall يك چتر امنيتي است كه بر روي كل شبكه كشيده مي شود. معمولا هدف عمده ديواره هاي آتش كنترل و محدود كردن ترافيك و ترجمه آدرسها مي باشد.تونلها و ارتباطات UDN به firewall ختم مي شود. برخي از ديواره هاي آتش در لايه ۳ كار مي كنند و اطلاعات را فقط از لحاظ منبع ومقصد مورد بررسي قرار مي دهد.اما در برخي ديگر از ديواره هاي آتش حتي مي توان بسته ها را از لحاظ معني و محتوي مورد بررسي قرار داد . ديواره هاي آتش كه عمل ترجمه آدرسهاي داخلي به آدرسهاي اينترنتي را انجام مي دهند (مانند proxy ها) باعث مي شوندپي بردن به ساختار داخلي شبكه از روي اينترنت تقريبا كاري غير ممكن مي باشد. از جمله مواردي ه ديوارهاي آتشين در مقابل آنها قادر به انجام هيچ كاري نيستند مي توان به حملات داخلي و يا نفوذگرائي كه كلمه عبور از ديوار آتشين را مي دانند اشاره كرد. بهر حال ديوارهاي آتشين يكي از تجهيزات خروجي جهت استقرار امنيت در يك سايت يا شبكه مي باشد.



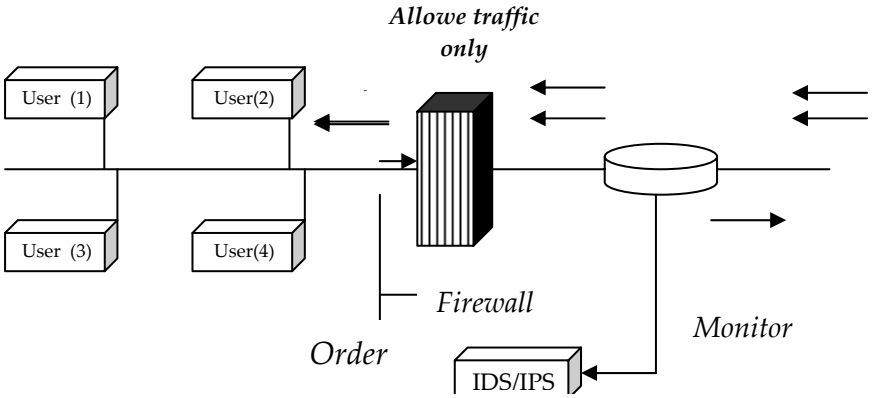
شكل شماره (۱) وضعيت ديوار آتش

اطمينان حاصل نمود . اول اينكه اطلاعات رسيده از مبدا مورد نظر (trustedhost) واقعا مربوط به آن ماشين بوده و آدرس جعلي مي باشد .دوم اينكه در خارج از ديواره آتش و بر روي اينترنت اين اطلاعات در دسترسي ديگران قرار گرفت ، قابل مفهوم و يا قابل استفاده نباشد.بنابراين استفاده از پروتكل هايhttp يا ssl ها جهت استفاده از سايتهاي مورد اطمينان يا بكاربردن فايلهاي UDP و كليدهاي خاص رمز گذاري جهت برقراري ارتباط شعبات شبكه بر روي اينترنت يا كامپيوترهاي قابل حمل (labtops) از ضروريات مي باشد.در واقع اطلاعات در ديوارخارجي ديواره هاي آتش از مبدا تا مقصد بايد رمزگذاري و كد شده باشند (network level encryption) تا اگر احتمالا اطلاعات در دسترس ديگران قرار گرفت ،باز هم قابل استفاده نباشد .[1]

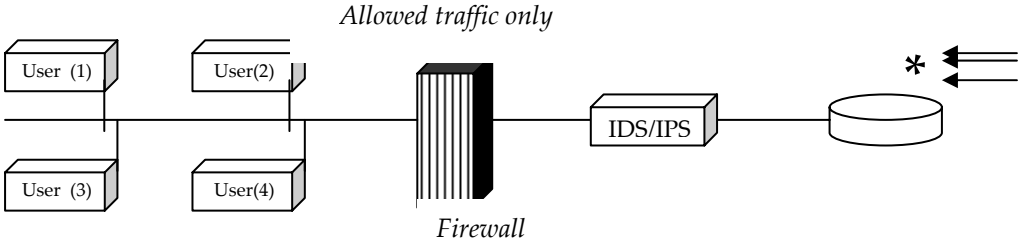
۶- سيستم تشخيص نفوذ يا در كمين مهاجمان نشستن IDS

سيستم تشخيص يا پيشگيري نفوذ اطلاعات , ورودي و خروجي شبكه را با هوشمندي بيشتري نسبت به ديواره هاي آتش مورد بررسي قرار مي دهند . از ديد يك ديواره آتش يك ارتباط يا مطمئن است و يا ناامن ، اما با توالي از عمليات مجاز نيز مي توان راه نفوذ را به يك سيستم باز نمود . در اين شرايط IDS ها مجموعه سوابق ترافيك را با بانك اطلاعاتي خود مقايسه كرده و در خصوص يك مجموعه عمليات ناامن

به مدير سيستم هشدار مي دهد و IDS ها ترافيک مشکوک را block مي نمايد . معمولاً گزارشات فراوان و هشدارهاي اشتباه يا بلاک کردن پي در پي سرويس هاي مجاز باعث مي شود تا توجه راهبران شبکه (Admin) به اين سيستم ها کم شده يا جهت آزاد سازي يک سرويس مجاز بسياري از قوانين و امکانات دست و پا گير اينگونه را غير فعال نمايند. بنابراين تنظيم صحيح و تغيير و متناسب کردن تنظيمات در طول نمودار با توجه به شبکه و خصوصيات آن که مسلماً به هزينه و پرسنل متخصص نياز دارد باعث مي شود تا از زمان اين تجهيزات کم شده و هوشياري آنها به موقع بوده و به واقعيت بيشتر نزديک باشد.



Out – of Band IDS/IPS ***شکل شماره (۲)***



In- line IDS/IPS *شکل شماره (۳)*

۷- Antisniffing :

Antisniffing ها نيز ابزارهايي هستندکه به محکم کردن سد امنيتي شبکه کمک ميکنند . اين ابزارها معمولا بصورت نرمافزارهايي بر روي يکي از ماشينهاي شبکه نصب مي شوند . از لحاظ نوع فعاليت sniffer و Antisniffe ها به سه دسته کلي زير تقسيم مي شوند :

دسته اول نرم افزاريي که با استفاده از روشها و اطلاعات جامع به بررسي شبکه مي پردازند يا در واقع سعي مي کنندبا حملات را شبيه سازي کنند. گزارشات از سيستمهاي آسيب پذير شبکه تهيه کرده آنها را اعلام مي نمايند. (VA tools)

دسته دوم نرم افزاريي که با بررسي لحظه اي يا دوره اي شبکه دسترسي به منابع را کنترل کرده و در واقع ترافيکهاي مشکوک را گزارش مي دهد.اينگونه Antisniffe ها مشابه IDS ها مي باشند با اين تفاوت که IDS ها معمولا در DMZ قرار مي گيرند، اما Antisniffe ها برروي ماشين در داخل شبکه نصب شده و ترافيکهاي داخلي را کنترل مي نمايند.

دسته سوم Antisniffe هايي هستند که در هنگام مواجه شدن با sniffer ها در شبکه که به جمع آوري اطلاعات براي نفوذگر مي پردازد ، وارد عمل

شده و با ارسال اطلاعات اشتباه و يا ايجاد ترافيكهاي مجازي سعي در گمراهي sniffer مي نمايد.
بايد توجه داشت كه نرم افزارهاي sniffer منابع زيادي را به خود اختصاص داده و اجراي آنها بر روي سرويس دهنده ها يا شبكه بار كاري را افزايش داده كارايي شبكه يا سرويس دهنده را به شدت كاهش مي آورند.همچنين اين ابزارها قادرند با پروتكل هاي ارتباطي مختلف بر روي محيطهاي مختلف فعاليت نمايند .[6]

۸- Operation System

امنيت , قابليت اطمينان, استحكام و قدرت سيستم عامل نقش مهمي در ساختار و كارايي شبكه ايفا مي كند. سيستم عاملهاي اصلي شبكه كه بر روي سرويس دهنده ها نصب مي شوند بايستي داراي سپرهاي امنيتي خاص خود باشند, زيرا وجود كوچكترين بخش قابل نفوذ در سيستم عامل, ميزان آسيب پذيري سايت و كل شبكه را بالا خواهد برد. از جمله مواردي كه مهاجمان از آن براي نفوذ به يك سيستم استفاده مي كنند استفاده از فايلهاي اشتراكي سيستم عامل بين دو يا چند كامپيوتر و يا استفاده از فايلهاي سابقه سيستم است. در اين راستا استفاده از ديوارهاي آتشين داخلي و فيلتر نمودن بسته ها و نيز كنترل شبكه محلي مي تواند نقش مهمي را در حفاظت از سيستم عامل ايفا كند. همچنين مي توان با روشهايي, دسترسي به فايلهاي سابقه سيستم عامل را نيز براي سايرين غير ممكن ساخت.
همچنين در اين راستا مي توان از قابليت انحصاري كردن سيستم عاملها استفاده كرد كه اين كار با استفاده از تكنولوژي Digital Watermark امكانپذير است به گونه اي كه واترمارك را در قالب يك Component به يك سيستم عامل اضافه كرده و سيستم عامل بصورت منحصر به فرد در آمده و در نتيجه نفوذگر نمي تواند نوع آنرا تشخيص و نهايتا نقاط آسيب پذير را شناسايي كند.[8]

۹-Anti spoofing

Spoofing به معناي گمراه كردن و كلاهبرداري مي‌باشد. روش هايي براي ورود و نفوذ به شبكه وجود دارند كه به اين نام ناميده ميشوند و اساس كار آنها گمراه كردن ميزبانها يا سيستم هاي امنيتي شبكه مي‌باشد. در اين خصوص نيز سياستهاي امنيتي شبكه بايد به صورتي باشد كه بتواند در مقابل اين گونه حملات مقاوم باشد. ابزارهايي كه به مقابله با Spoofing مي‌پردازند، نرم افزارهايي هستند كه با چك كردن پروتكل ها و اطلاعات رد و بدل شده در شبكه اين گونه تهاجم ها را تشخيص داده، اطلاع مي دهند يا اينگونه ترافيك ها را بلاك مي نمايند.در برخي شرايط Anti-Spoofing مي تواند به صورت قوانين خاصي در IDS يا IPSها بدون سربار هزينه اي براي سازمان پياده سازي شود و همچنين از Spoofing ها نيز مي توان در شبكه براي گمراه كردن مهاجمين و تحويل دادن اطلاعات اشتباه به آنها استفاده نمود. سه محيط مناسب براي به كار بردن Spoofing ها از طرف مهاجمين وجود دارد: اول محيط هايي كه سيستم امنيتي فقط آدرس هاي مبداء و مقصد را جهت تائيد ميزبان قابل اطمينان استفاده نموده و اطلاعات در هنگام انتقال بر روي شبكه با كليد خاصي رمز گذاري نمي شوند.
دوم در شرايطي كه ماشين منبع يك روش قابل پيش بيني براي توليد شماره هاي افزايش تناوبي به كار مي برد. سوم شبكه هايي كه داراي ميزبانهاي قابل اطمينان(پاورقي) TrustedHostدر خارج از شبكه مي باشند

كه مهاجم مي تواند به راحتي شرايط آن ميزبان را در غياب آن سيستم تقليد نمايد. با استفاده از
Network Level Secunting مي توان راه اكثر انواع Spoofing را سد نمود.
بستر مناسب ديگر براي Spoofing پست الكترونيك مي باشد. ارسال نامه ها با فرستنده هاي جعلي يا نامه‌هايي كه از فرستنده واقعي به صورت غير ارادي و به صورت يك ويروس منتشر شونده براي كليه مقاصدي كه آدرس آنها در صندوق پشت فرستنده است، ارسال مي‌شوند. معمول ترين روش هاي Mail-Spoofing است. استفاده از Antivirus ها براي Mail Server ها و استفاده از كليدهاي عمومي و خصوصي يا امضاء ديجيتالي براي نامه ها، راههاي مقابله با اينكه Spoofing مي‌باشد.[6]

APP&Services -١٠

اين مرحله از امنيت مرتبط با ميزبانها، برنامه هاي كاربردي و سرويسهاي در حال اجرا برروي آنها مي باشد. به دليل تنوع ميزبانها يا سرويس دهنده هاي شبكه از لحاظ سخت افزاري و نرم افزاري اين قسمت به توجه خاصي نياز دارد. زيرا هر سرويس و يا برنامه كاربردي بايد به صورت مستقل مورد بررسي قرار گيرد (كه البته داراي هزينه است و نيروي مديريتي زيادي را نياز دارد)تنوع تكنيكها يا نرم افزارهاي مورد نياز از خصوصيات اين لايه مي‌باشد. اگر به اين قسمت اهميت داده نشود، به راحتي اطلاعات و ركوردهاي بانكهاي اطلاعاتي قابل دسترس مهاجمان مي‌باشد. واقعيت اين است كه اكثر برنامه هاي كاربردي بدون در نظر گرفتن مسائل امنيتي كد مي‌شوند. به خصوص بسته هاي نرم افزاري WebBase كه در واقع تنها راه دسترسي بانكهاي اطلاعاتي از خارج از ديواره هاي امن شبكه مي باشند. اين قسمت جايگاه بسيار مناسبي براي نفوذ و استخراج ديتا از بانك هاي اطلاعاتي مي باشد. بنابراين انتخاب نرم افزارها، سيستم عاملهاي سرويس وب و همچنين پست الكترونيك نقش حياتي در امنيت و محدود كردن دسترسي به داده ها را ايفا مي‌كنند.
ابزارهايي وجود دارند كه در نقش FireWallبرروي ميزبانها نصب شده و به صورتي تنظيم مي شود كه هيچ سرويس يا برنامه كاربردي نتواند عملياتي را انجام دهد كه مجاز به اجراي آن نيست. اجراي كدهاي اجرايي مربوط به نامه هاي ويروس يا اجراي كدهاي درج اطلاعات توسط صفحاتي كه به صورت پيش فرض حالت خواندني دارند و ارسال اطلاعات شبكه از داخل به سمت اينترنت كه از سطوح امنيتي Firwall ها و IDS ها به راحتي مي‌گذرند(به دليل اينكه اين سيستم ها معمولاً ترافيك ورودي را چك مي‌نمايند) مشكلات اين لايه است. اين مشكلات بايد توسط Firewall هاي حساس به فرايند يا محدود كننده نامه ها كاربردي ، محدود مي‌شوند.
مرحله بعد فراهم آوردن امكان authentic براي ارتباط كاربر با برنامه هاي كاربردي و همچنين براي ارتباط هر برنامه با بانك اطلاعات مي باشد.(ضرورتEncrypt مربوط به ارسال اطلاعات در لايه ٣ مطرح شده است.) چك كردن اعتبار ورودي ها و اطمينان از اينكه به خصوص اطلاعات وارد شده در صفحات وب توسط كاربران باعث سرريز شدن يا اعمال كدهاي غير قابل كنترل بر روي داده ها نمي‌شود. تدابيري است كه در اين لايه بايد انديشيده شود.
كلاً قسمت بالا به سه دسته كلي زير بايد تقسيم شود :
- استفاده از سرويس دهنده هاي مطمئن (Mail Server،Webo.s)
- استفاده از Firwell هاي خاص ميزبان جهت كنترل فرايندها
- چك كردن اعتبار ورودي ها

به عنوان مثال نبايد به كاربر اجازه دادكه از داده هاي طولاني يا كلمات كليديSQL در جعبه هاي متن استفاده كند.

ارائه اين سرويس در هر سيستم عامل عموماً به صورت قسمتي از آن سيستم عامل و يا يك بسته نرم افزاري بر روي آن است. از آنجا كه نفوذ به شبكه و دسترسي به اطلاعات و يا تغيير آنها از طريق سرويس وب بسيار آسان است، امنيت در سيستم عامل ارائه كننده اين سرويس بسيار حائز اهميت است و لذا اين سرويس دهنده ها بايد تا حد امكان قابل اطمينان باشند، بخصوص در سايتهايي كه نقل و انتقالات مالي از طريق اين سرويس صورت مي‌گيرد. از اين رو بهتر است علاوه بر تدابيري كه در سيستم عامل انديشه شده است، سايت مجهز به يك سري ابزارهاي رديابي و مقابله با مهاجمان باشد. همچنين استفاده از رمز گذاري و سيستم هاي كدگذاري در ساختار نيز از اهميت بالايي برخوردار است.[10]

۱۱- Encryption :

استفاده از روشهاي كد گذاري يكي از موثرترين روشها در بالا بردن سطح امنيت ارتباطات اينترنتي است كه آخرين لايه امنيتي سايت را تشكيل مي دهد. استفاده از يك روش خاص كدگذاري در ارتباطات و يا استفاده از امضاهاي الكترونيكي و غيره مي تواند داده ها را از دسترسي هاي غير مجاز حفظ نموده و امنيت را بالا ببرد. اين كدگذاري در چند سطح مختلف قابل استفاده مي باشد كه پياده سازي آن در كليه سطوح, امنيت سايت را به حالت ايده آل نزديكتر مي سازد. كد گذاري را مي توان در ارائه اطلاعات به كاربر و دريافت اطلاعات, ثبت اطلاعات در بانكهاي اطلاعاتي, ارتباطات بين نرم افزارهاي خاص منظوره و بانكهاي اطلاعاتي سايت و تهيه پشتيبان مورد استفاده قرار دارد.

۱۲- تاثير روال اداري بر امنيت سايت [1] :

يكي از مهمترين عوامل موثر در امنيت سايت كه جايگاه آن در سطوح امنيتي سايت نيست اما مي‌توان به عنوان يكي از عوامل امنيتي به آن اشاره كرد، روال اداري مي‌باشد. زيرا با در نظر نگرفتن اين مورد، حتي محكمترين سطوح امنيتي قابل نفوذ مي‌باشد. به عبارت ساده مي‌توان نفوذ گري را در نظر گرفت كه كليد دارد. در اين صورت ارتفاع ديوار يا نوع سيستم امنيتي و به هيچ وجه در نفوذ فرد تاثير نخواهد داشت.

در صورت وجود نقايضي در سيستم اداري يك سايت يا شبكه و خروج ناآگاهانه اطلاعات، كلمات عبور، كليدهاو روشهاي كدگذاري از اين سيستم يا نفوذ افراد يا ابزارهايي در ساختار سايت، ديگرهيچ سيستم امنيتي نمي‌تواند به مقابله به اينگونه نفوذها يا سرقت و خرابكاري اطلاعات بپردازد. نمونه هايي از اين نوع نفوذها عبارت است از اسبهاي تراوا (Trojan Horses) يا نرم افزارهاي Back door كه امكان دسترسي نامحدود به سيستم را در اختيار مهاجمين قرار مي دهد واضح است كه نصب نرم افزارهاي مشكوك يا رسيده توسط پست الكترونيك توسط مسئولين يا كارمندان بي اطلاع و بي احتياط باعث راه اندازي اينگونه نرم افزارها مي‌شود از ديگر موارد نفوذ عدم تغيير كلمات عبور پيش فرض نرم افزارها، سيستم عامل يا برنامه هاي كاربردي، سهل انگاري كاربران يا مسئولين در انتخاب اسم رمزي كه به راحتي قابل پيش بيني است و عدم تعويض دوره اي كلمات عبور،مي‌باشد.

اين موارد به قدرت امنيتي شبكه وابسته نيستند، بلكه ارتباط مستقيم با هوشياري و آگاهي افراد مسئول و كاربران شبكه دارد. همچنين روال و ساختار محكم و مرتب اداري سايت و يا سازمان مستند سازي و تعويض دوره اي كلمات عبور، در جلوگيري از بروز مشكلات فوق نقش بسيار مؤثري دارد.

۱۳- نتيجه گيری :

با توجه به ضرورت امنيت دنياي امروز و اهميت آن در نقل و انتقال داد ها روشهايي پيشنهاد شد كه تركيب آن سر محكم در برابر نفوذ كاربران غير مجاز است اما بايد به دو نكته توجه داشت : اولا بكار بردن هر كدام از روشها فقط ديوار دفاعي را بلندتر مي كند و هيچگاه سقف ايجاد نمي كند. ثانيا بكار بردن روشها نيازمند هزينه هاي مربوط به آن لايه مي باشد كه سازمانهاي خواستار اين لايه بايد

[1] . Operatinal Procedures

اين نكته را در نظر گرفته و با توجه به فاكتورهاي مهم كه ممكن است زمان, امنيت داده ها , قابليت نفوذ و هزينه لايه ها را اولويت بندي و از آنها استفاده كنند .

١٤- مراجع :

1) Managing a Network with a Protocol Analyzer openxtra.co.uk

2) Ef_ cient Security Mechanisms For Routing Protocols , Yih – Chun Hu and Adrian Perrig and David B. Johnson.

3) CORBA Firewall Security: Increasing the Security of CORBA Applications, Hbatamu Abie and Janury 2000.

4) tracing data diffusion in industrial research with robust watermarking, christoph busch and Stephen D.wolthsen

5) securing cisco routers,steven kieffer,November 2002

6) the business case for high avaibility(HA),a cybergoard corporation,august2002

7) network security assessment white paper,will Spence,20 april 2000