مرکز اطلاعات و مدارك علمي ايران
مجله الکترونیکی
شماره دوم دوره چهارم

ارائه يک الگوي امنيتي براي شبکه هاي کامپيوتري

نويسنده : محمدمهران لسان صدق
دانشجوي کارشناسي ارشد کامپيوتر - نرم افزار
دانشگاه آزاد اسلامي واحد نجف آباد

چکيده
رايج ترين مدل شبکه هاي کامپيوتري، مدل چهار لايه TCP/IP است که با بهره گيري از پشته پروتکل TCP/IP به تبادل داده و نظارت بر مبادلات داده مي پردازد ولي عليرغم محبوبيت، داراي نقاط ضعف و اشکالات امنيتي است و نحوه رفع اين اشکالات و مقابله با نفوذگران کامپيوتري، همواره بعنوان مهمترين هدف امنيتي هر شبکه تلقي مي گردد.
در اين مقاله پس از بررسي انواع رايج تهديدات امنيتي عليه شبکه هاي کامپيوتري و راهکارهاي مقابله با آنها، با توجه به تنوع شبکه هاي کامپيوتري از نظر ساختار، معماري، منابع، خدمات، کاربران و همچنين اهداف امنيتي خود، با دنبال کردن الگوي امنيتي ارائه شده به راهکارهاي امنيتي مناسب دست يابد.

کليد واژه ها: امنيت- حمله- تهديد- شبکه- نفوذ- مقابله

۱- مقدمه:

در شبکه کامپيوتري براي کاهش پيچيدگي هاي پياده سازي، آن را مدل سازي ميکنند که از جمله ميتوان به مدل هفت لايه OSI و مدل چهار لايه TCP/IP اشاره نمود. در اين مدلها، شبکه لايه بندي شده و هر لايه با استفاده از پروتکلهاي خاصي به ارائه خدمات مشخصي ميپردازد. مدل چهار لايه TCP/IP نسبت به OSI محبوبيت بيشتري پيدا کرده است ولي عليرغم اين محبوبيت داراي نقاط ضعف و اشکالات امنيتي است که بايد راهکارهاي مناسبي براي آنها ارائه شود تا نفوذگران نتوانند به منابع شبکه دسترسي پيدا کرده و يا اينکه اطلاعات را بربايند. [۱]
شناسائي لايه هاي مدل TCP/IP، وظايف، پروتکلها و نقاط ضعف و راهکارهاي امنيتي لايه ها در تعيين سياست امنيتي مفيد است اما نکته اي که مطرح است اينست که تنوع شبکه هاي کامپيوتري از نظر معماري، منابع، خدمات، کاربران و مواردي از اين دست، ايجاد سياست امنيتي واحدي را براي شبکه ها غيرممکن ساخته و پيشرفت فناوري نيز به اين موضوع دامن ميزند و با تغيير داده ها و تجهيزات نفوذگري، راهکارها و تجهيزات مقابله با نفوذ نيز بايد تغيير کند.

۲- مروري بر مدل TCP/IP:

اين مدل مستقل از سخت افزار است و از ٤ لايه زير تشکيل شده است [۲]:

۱- لايه ميزبان به شبکه:

دراين لايه رشته اي از بيتها بر روي کانال هاي انتقال رد و بدل مي شوند و از تجهيزاتي مانند HUB,MAU,Bridge و Switch براي انتقال داده در سطح شبکه استفاده ميشود.

۲- لايه اينترنت يا شبکه (IP):

وظيفه اين لايه هدايت بسته هاي اطلاعاتي (IP-Packet) روي شبکه از مبدا به مقصد است. مسيريابي و تحويل بسته ها توسط چند پروتکل صورت مي گيرد که مهمترين آنها پروتکل IP است. از پروتکلهاي ديگر اين لايه ميتوان ARP,RIP,ICMP,IGMP را نام برد. مسيرياب (ROUTER) در اين لايه استفاده ميشود.

۳- لايه انتقال (TCP):

برقراري ارتباط بين ماشينها بعهده اين لايه است که ميتواند مبتني بر ارتباط اتصال گراي TCP يا ارتباط غير متصل UDP باشد. داده هايي که به اين لايه تحويل داده مي شوند توسط برنامه کاربردي با صدازدن توابع سيستمي تعريف شده در واسط برنامه هاي کاربردي (API) ارسال و دريافت ميشوند. دروازه هاي انتقال در اين لايه کار ميکنند.

۴- لايه کاربرد:

اين لايه شامل پروتکل هاي سطح بالائي مانند HTTP,SMTP,TFTP,FTP,Telnet است.در اين لايه دروازه کاربرد ديده ميشود.

۳- تهدیدات علیه امنیت شبکه:

تهدیدات و حملات علیه امنیت شبکه از جنبه هاي مختلف قابل بررسي هستند. از یک دیدگاه حملات به دو دسته فعال و غیر فعال تقسیم مي شوند و از دیدگاه دیگر مخرب و غیر مخرب و از جنبه دیگر میتوان براساس عامل این حملات آنهارا تقسیم بندي نمود. بهرحال حملات رایج در شبکه ها بصورت ذیل میباشند [۱۱]:

۱- حمله جلوگیري از سرویس (DOS):

در این نوع حمله، کاربر دیگر نمیتواند از منابع و اطلاعات و ارتباطات استفاده کند. این حمله از نوع فعال است و میتواند توسط کاربر داخلي و یا خارجي صورت گیرد.

۲- استراق سمع:

در این نوع حمله، مهاجم بدون اطلاع طرفین تبادل داده، اطلاعات و پیامها را شنود مي کند. این حمله غیرفعال است و میتواند توسط کاربر داخلي و یا خارجي صورت گیرد.

۳- تحلیل ترافیک:

در این نوع حمله مهاجم براساس یکسري بسته هاي اطلاعاتي ترافیک شبکه را تحلیل کرده و اطلاعات ارزشمندي را کسب میکند. این حمله یک نوع حمله غیر فعال است و اکثرا توسط کاربران خارجي صورت مي گیرد.

۴- دستکاري پیامها و داده ها:

این حمله یک حمله فعال است که در آن مهاجم جامعیت و صحت اطلاعات را با تغییرات غیر مجاز بهم مي زند و معمولا توسط کاربر خارجي صورت مي گیرد.

۵- جعل هویت:

یک نوع حمله فعال است که در آن مهاجم هویت یک فرد مجاز شبکه را جعل مي کند و توسط کاربران خارجي صورت میگیرد.

۴- راهکارهاي امنیتي:

در این بخش سرویس ها، مکانیزم ها و تجهیزات امنیتي نام برده میشود.

سرویس هاي امنیتي عبارتند از [۳]:

۱- حفظ محرمانگي: یعني کاربران خاصي از داده بتوانند استفاده کنند.

۲- حفظ جامعیت داده: یعني داده ها بدرستي در مقصد دریافت شوند.

۳- احراز هویت: یعني گیرنده از هویت فرستنده آگاه شود.

۴- کنترل دستیابي مجاز: یعني فقط کاربران مجاز بتوانند به داده ها دستیابي داشته باشند.

۵- عدم انکار: یعني فرستنده نتواند ارسال پیام توسط خودش را انکار کند.

مکانیزم هاي امنیتي عبارتند از :

۱- رمز نگاري که در آن با استفاده از کلید خصوصي یا عمومي و با استفاده از الگوریتم هاي پیچیده پیام بصورت رمز درآمده و در مقصد رمزگشایي مي شود.

۲- امضاء دیجیتال که براي احراز هویت بکار مي رود.

تجهیزات امنیتي عبارتند از [۱۰]:

۱ - فایروال: امکاناتي است که میتواند بصورت سخت افزاري یا نرم افزاري در لبه هاي شبکه قرار گیرد و سرویس هاي کنترل دستیابي ، ثبت رویداد ، احراز هویت و ... را انجام دهد.

۲- VPN بهره مندي از شبکه عمومي براي اتصال دو یا چند شبکه خصوصي است .

۳- IDS : سیستم تشخیص نفوذ است که در لایه بعد از فایروال مي تواند امنیت را تقویت کند و نفوذ مهاجمین رابر اساس تحلیل هاي خاص تشخیص مي دهد.

۴- IPS : سیستم جلوگیري از نفوذ است که پس از تشخیص نفوذ مي تواند به ارتباطات غیرمجاز ومشکوک بصورت یکطرفه پایان دهد.

۵- AntiVirus : که مي تواند با تشخیص محتواي فایل، فایل هاي آلوده را بلوکه کند.

۶- Vulnerability Scan : امکانات نرم افزاري است براي تشخیص آسیب پذیري شبکه.

۷- Logserver & Analysis: امکاناتي است که براي ثبت و کنترل رویدادها مورد استفاده قرار مي گیرد.

۸- سرورهاي AAA: براي احراز هویت، کنترل و نظارت بر دسترسي کاربران داخلي و خارجي استفاده مي شوند.

البته بغیر از تجهیزات فوق الذکر،با استفاده از مسیریابها و سوئیچ هاي مدیریت پذیر مي توان امنیت در مسیر تبادل را نیز تا حد زیادي تامین نمود.

در ادامه حملات، سرویس ها و مکانیزم ها و تجهیزات امنیتي در لایه هاي مختلف در قالب جداول ۱-۲-۳-٤ با یکدیگر

مقايسه مي شوند و همانطور كه در جداول مذكور نشان داده شده است مي توان نتيجه گرفت كه بيشترين حملات به ترتيب در لايه IP,TCP ، كاربرد و ميزبان به شبكه است و سرويس ها و مكانيزم ها بيشتر در لايه IP به چشم مي خورد و تجهيزات امنيتي با بهره گيري از مكانيزم هاي مختلف بيشتر در لايه IP , TCP و كاربرد ، كاربري دارند .
در جدول ٥تجهيزات امنيتي از نظر پارامترهاي مختلف با يكديگر مقايسه مي شوند و مورد ارزيابي قرار مي گيرند، استفاده از تجهيزات سخت افزاري نظير فايروال، سوئيچ ها و مسيريابهاي مديريت پذير، گران است و هزينه پشتيباني آنها نيز بالاست و از پيچيدگي نسبتا بالايي برخوردارند. در تجهيزات نرم افزاري نيز هزينه پشتيباني بدليل لزوم Update مرتب ، بالا است ولي هزينه استقرار و پيچيدگي پائين است.

جدول ١. مقايسه تهديدات امنيتي در لايه هاي چهارگانه TCP/IP

لايه تهديد	Host to Network	IP	TCP	Application
Trojan,Virus,Worm				✓
SQL-Injection				✓
TCP/IP Spoofing		✓	✓	
Session Hijacking			✓	✓
Port Scan			✓	✓
Physical Attacks	✓			
Phishing			✓	✓
Password Attacks				✓
Packet Sniffing		✓	✓	
Dos/DDos Attacks		✓	✓	✓
Network Layer Attacks		✓		
Application Layer Attacks				✓
Buffer Over Flow Attacks		✓	✓	✓
Replay	✓	✓	✓	✓
Traffic Analysis	✓	✓	✓	
Message Modification	✓	✓	✓	

جدول ٢. اهراف امنيتي در منابع شبكه

منابع اهداف	شبكه				كاربران شبكه
	سخت افزارها	نرم افزارها	اطلاعات	ارتباطات	
محرمانگي			✓	✓	
صحت	✓	✓	✓	✓	
قابليت دسترسي	✓	✓	✓	✓	
محافظت فيزيكي	✓				
تشخيص هويت					✓
صدور اختيارات					✓
حريم خصوصي					✓
آگاهي رساني امنيتي					

جدول ٣. سرويس هاي امنيتي در لايه هاي مختلف TCP/IP

لايه سرويس	Host to Network	IP	TCP	Application
محرمانگي	✓	✓	✓	✓
تاييد هويت	✓	✓	✓	✓
رد انكار				✓
كنترل جامعيت و صحت		✓	✓	

جدول ٤. مكانيزم هاي امنيتي مربوط به لايه هاي مختلف TCP/IP

لايه	Host to Network	IP	TCP	Application

مكانيزم				
رمزنگاري	✓	✓	✓	✓
امضاء ديجيتال		✓	✓	✓
كنترل دستيابي		✓	✓	✓
درستي و صحت داده		✓	✓	✓
كنترل مسيريابي			✓	
رد انكار (سنديت)			✓	✓

جدول ٥. مقايسه تجهيزات امنيتي در لايه هاي چهارگانه TCP/IP

لايه **تجهيزات امنيتي**	**Host to Network**	**IP**	**TCP**	**Application**
حفاظت فيزيكي	✓			
رمزنگاري	✓	✓	✓	✓
IP Sec		✓		
SSL			✓	
Firewall		✓	✓	✓
AntiVirus				✓
AAA Server	✓	✓	✓	✓
VPN	✓	✓	✓	✓
PGP				✓
IDS/IPS		✓	✓	✓

٥ - الگوي امنيتي

٦-١ : معماري امنيتي

با توجه به ساختار هر شبكه، معماري امنيتي شبكه بصورت نهفته در لايه هاي شبكه در نظر گرفته مي شود و لايه بندي با توجه به محدوده هاي داخلي ، خارجي ، ارتباط از راه دور و غيره بصورت يک معماري امنيتي ٤ لايه تعيين مي گردد كه عبارتند از[٤]:

١ - امنيت زيرساخت كه شامل پيكربندي دقيق تجهيزات شبكه است.

٢ - امنيت ارتباطات كه در آن با استفاده از فايروال ها، سيستمهاي IDS,IPS ، ضد ويروسها ، سرورهاي AAA، نرم افزارهاي مانيتورينگ، ثبت و تحليل رويدادها مي توان به تشخيص هويت و كنترل كاربران پرداخت.

٣- امنيت سيستم ها كه در آن با بهره گيري از پويشگرها ي امنيتي، آنتي ويروسها، IDS و IPS به ثبت و كنترل دسترسي كاربران به منابع پرداخته مي شود.

٤- امنيت كاربردها كه با بهره گيري از سيستمهاي IDS ، آنتي ويروس، پويشگر امنيتي و فيلترهاي محتوا بر دسترسي كاربران نظارت مي شود.

٦-٢ : الگوريتم جهت تهيه الگوي امنيتي شبكه

با توجه به تنوع شبكه ها استفاده از الگوريتم ذيل در طرح الگوي امنيتي شبكه مفيد است.

الگوريتم از مراحل ذيل تشكيل مي گردد:

١ - شروع

٢ - در صورتي كه شبكه موجود است به مرحله ١٠ برويد.

٣ - نيازمنديهاي امنيتي را تعيين كنيد.

٤- منابع راشناسايي كنيد.

٥- مخاطرات مربوط به شبكه را تحليل كنيد.

٦- راهكارهاي مقابله با مخاطرات را ارائه كنيد.

٧- تجهيزات و امكانات امنيتي مناسب را تعيين نماييد.

٨- سياستها و رويه هاي امنيتي را تدوين كنيد.

٩ - سياستها و رويه هاي امنيتي اجرا كنيد.

١٠ - وضعيت موجود را بررسي كنيد.

١١ - در صورتي كه نيازمنديهاي سازمان تامين نشده است، به مرحله ٣ برويد.

١٢ - در صورتي كه نيازمنديهاي امنيتي شبكه تامين نشده است به مرحله ٤ برويد.

۱۳ - به مرحله ۱۰ برويد.
همانطور كه ملاحظه مي شود اين الگوريتم يک الگوريتم گردشي است كه به طور مداوم بايد براي شبكه هاي كامپيوتري اجرا گردد.

۶- نتيجه گيري :

از يک شبكه كامپيوتري، عوامل مهمي مانند نوع سيستم عامل، موجوديتها، منابع، برنامه هاي كاربردي، نوع خدمات و كاربران نقش مهم ومستقيمي در امنيت شبكه دارند. برقراري امنيت بصورت ۱۰۰% امكان پذير نيست چرا كه بعضي از عوامل از حيطه قوانين سيستمي خارج هستند، بعنوان نمونه كانالهاي مخابراتي هدايت ناپذير (مثل امواج مخابراتي و ارتباط ماهواره اي) يا كاربران شبكه (كه هميشه از آموزشهاي امنيتي داده شده استفاده نمي كنند.).
بنابراين الگوي امنيتي شبكه يک طرح امنيتي چند لايه و توزيع شده را پيشنهاد مي كند]۳[به نحوي كه كليه بخشهاي شبكه اعم از تجهيزات، ارتباطات، اطلاعات و كاربران را در برمي گيرد. در الگوي امنيتي ضمن مشخص كردن سيا ست امنيتي شبكه كه در اصل در مورد اهداف امنيتي بحث مي كند، راهكارهاي مهندسي و پياده سازي امنيت نيز ارئه مي گردد و با آموزشهاي مختلف امنيتي و نظارت مداوم ، امنيت شبكه بطور مداوم ارزيابي مي گردد.

قدرداني

از زحمات كليه كساني كه در انجام اين پژوهش مرا ياري نموده اند خصوصا از آقاي دكتر فضل ... اديب نيا كه بدون شك انجام اين كار بدون رهنمودهاي ايشان ممكن نبود، تشكر مي‌نمايم.

منابع

۱- تنن بام . شبكه هاي كامپيوتري. ترجمه دكتر پدرام و مهندس ملكيان (۱۳۸۲)
۲- مهندس احسان ملكيان (۱۳۸۱). نفوذگري در شبكه ها و روشهاي مقابله
۳- اريك ميلوالد(۱۳۸۳). امنيت شبكه
۴- محمود خالقي (۱۳۸۳). سيستم مديريت امنيت اطلاعات
۵- MCSE-TCP/IP . ترجمه مهندس كيادي مقدم (۱۳۸۰).
۶- Network+. ترجمه مهندس شهرام سبحاني (۱۳۸۲).

7- Hacker beware, by: eric Cole(2001)
8- Cisco Security, by: Cisco Press(2000)
9-The protocols,by: Richard Stivens(1999)
10-Network Security fundamentals,by: Peter Norton (SAMS)1999
11-Mastering Network Security,by: Chris Brenton (Sybex)1998