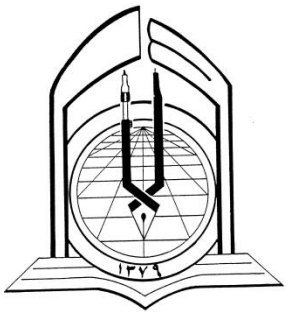

بسم الله الرحمن الرحیم



وزارت علوم،تحقیقات و فناوری

دانشگاه فنی حرفه ای

آموزشکده فنی پسران شهرضا(خوارزمی)

گروه :کامپیوتر

پایان نامه کاردانی رشته کامپیوتر(نرم افزار)

عنوان پروژه :

امنیت در سرور های وب

استاد راهنما:

محمد مهدی باغستانی

پژوهشگر:

ابوالفضل خلفی

تیر ماه ۱۴۰۰

صفحه سپاس گذاری : اختیاری

سپاس گذاری

سپاس خدایی را کـه توفیـق علـم جـویی ، خـدمت بـه جامعـه ی بشـری و دسـت گیـری از نیازمنـدان را به من اهدا کرد.

از مسـئولین دانشـکده فنـی حرفـه ای پسـران شهرضـا (خـوارزمی)بـه پـاس پیگیـری و زحمـات مکـرر و بی شائبه ی شان بسیار سپاس گزارم.

همچنـین مراتـب سـپاس و قـدر دانـی را از مـدیریت و پرسـنل و کـادر دفتـری دانشـگاه کـه همیشـه در همه ی مراحل همراه من بودند و از هیچ کمکی فروگذاری نکردند بجا می اورم.

و در اخـر وظیفـه ی خـود مـی دانـم کـه از اسـتاد بسـیار خـوب و دلسـوزم جنـاب اقـای محمـد مهـدی باغستانی کمال سپاس و تشکر را داشته باشم.

چرا که طی کردن این مسیر بدون داشتن راهنمایی دانا به سادگی امکان پذیر نبود.

با ارزوی توفیق روز افزون برای تمام مردم سرزمینم.

و من الله توفیق.

این صفحه: اختیاری

تقدیم به پدر و مادر عزیزم

سپاس و ستایش خدای را که آثار قدرت او بر چهره روز روشن، تابان است و نور حکمت او در دل شب تار، درفشان.

آفریدگاری که خویشتن را به ما شناساند و درهای علم را بر ما گشود و عمری و فرصتی عطا فرمود تا بدان، بنده ضعیف خویش را در طریق علم و معرفت بیازماید.

تقدیم به پدر بزرگوار و مادر مهربانم

آن دو فرشته ای که از خواسته هایشان گذشتند، سختی ها را به جان خریدند و خود را سپر بلای مشکلات و ناملایمات کردند تا من به جایگاهی که اکنون در آن ایستاده ام برسم .

تا اینجا بدون شماره صفحه

فهرست مطالب اتوماتیک
(با کلیک بر روی هر عنوان بتوان به مطالب آن بخش دسترسی داشت)

فهرست مطالب

عنوان صفحه

چکیده ۱

فصل اول : تعاریف ۲

۱-۱- مقدمه ۳

۱-۱-۱- تعریف وب سرور ۳

۱-۱-۲- ویژگی های مشترک ۳

۱-۲- سرور های اینترنتی ۳

۱-۲-۱- آپاچی : (**Apache**) ۳

۱-۲-۲- **IIS** ۴

۱-۲-۳- مقایسه عملکردهای امنیتی وب سرور های **Apache**و**IIS**... **Error! Bookmark not defined.**

۱-۳- ایجاد یک ارتباط ایمن در برنامه های وب ..... **Error! Bookmark not defined.**

۱-۳-۱- ضرورت ایجاد یک ارتباط ایمن بین سرویس گیرنده و سرویس دهنده.... **Error! Bookmark not defined.**

۱-۳-۲- رمز نگاری کلید عمومی و گواهینامه دیجیتالی ..... **Error! Bookmark not defined.**

۱-۳-۳- رمز نگاری کلید خصوصی (**Private key**) ..... **Error! Bookmark not defined.**

۱-۳-۴- رمز نگاری کلید عمومی (**public key**) ۶

۱-۳-۵- سیستم های مدرن رمز نگاری ۹

فصل دوم: امنیت وب سرور ها در شبکه ۱۱

۲-۱- مقدمه ۱۲

۲-۱-۱- به گزارش گروه ویژه امنیت ملی ۱۲

۲-۲- تعریف سرور ۱۳

۲-۳- انواع وب سرور ۱۴

۲-۳-۲- آپاچی (**Apache**) ۱۵

۲-۳-۳- **IIS** ۱۷

۲-۳-۴- عملیات قبل از نصب **IIS** ۱۸

۲-۳-۵- سرویس های **IIS** ۱۹
۲-۴- نحوه فعال کردن سرویس **www** ۲۱
۲-۴-۱- امنیت برنامه IIS ۲۱
۲-۵- به گزارش ویژه گروه امنیت ملی ۲۳
۲-۵-۱- مقایسه **IIS** و **Apache** ۲۳
۲-۶- مقایسه امنیتی Apache در مقابل IIS ۲۸
۲-۶-۱- آسیب پذیری ذاتی سرور ۲۸
۲-۶-۲- دانش و آگاهی از مدیریت وب موجود ۲۸
۲-۶-۳- انتخاب درست سیستم عامل(OS) توسط مدیران ۲۸
۲-۶-۴- مهارت های توسعه دهنده ۲۹
۲-۷- تامین امنیت سایت و سرور ۳۰
۲-۸- ۱۰ روش مفید برای بالا بردن ضریب امنیت در سرور های **Cpanel** ۳۱
فصل سوم : امنیت وب سایت ها ۳۲
۳-۱- مقدمه ۳۳
۳-۲- اقدامات پردیس برای حفظ امنیت سرور ها ..... **Error! Bookmark not defined.**
۳-۲-۱- عوامل رایج هک شدن سایت ها ..... **Error! Bookmark not defined.**
۳-۲-۲- راه حل های پیشنهادی ..... **Error! Bookmark not defined.**
۳-۳- قوانین حفظ حریم خصوصی ..... **Error! Bookmark not defined.**
۳-۴- جزئیات حفظ حریم خصوصی ..... **Error! Bookmark not defined.**
۳-۵- نگاهی به وضعیت آسیب پذیری وب سایت ها در برابر حملات سایبری ..... **Error! Bookmark not defined.**
۳-۶-**SSL**- راهنمایی برای امنیت وب سایت ها ..... **Error! Bookmark not defined.**
۳-۶-۱- **SSL**پایه و اساس امنیت فضایی مجازی ..... **Error! Bookmark not defined.**
۳-۶-۲- **SSL Authentication** ..... **Error! Bookmark not defined.**
۳-۶-۳- چگونگی عملکرد **SSL** ..... **Error! Bookmark not defined.**
۳-۶-۴- تجربیات کاربران از **SSL** ..... **Error! Bookmark not defined.**
۳-۶-۵- اهمیت انتخاب درست ارائه دهنده ی خدمات **SSL** ..... **Error! Bookmark not defined.**

۶-۶-۳- تجربه ی امنیت در سطحی بالاتر با بهره گیری از **EV SSL** .. **Error! Bookmark not defined.**
۱-۶-۶-۳- چگونگی عملکرد **EV SSL** ..... **Error! Bookmark not defined.**
۲-۶-۶-۳- چرایی اهمیت **EV SSL** ..... **Error! Bookmark not defined.**
۷-۳- سایت های تان را به **SSL** مجهز کنید! ..... **Error! Bookmark not defined.**
۸-۳- مزایایی بهره گیری از گواهی **SSL** ..... **Error! Bookmark not defined.**
۱-۸-۳- گواهی **SSL** در ایران ..... **Error! Bookmark not defined.**
۹-۳- چند نکته امنیتی برای مدیران سایت ها ..... **Error! Bookmark not defined.**
۱-۹-۳- تنظیمات سرور خود را چک کنید ..... **Error! Bookmark not defined.**
۲-۹-۳- به طور منظم فایل های **Log** خود را برسی کنید ..... **Error! Bookmark not defined.**
۳-۹-۳- نقاط آسیب پذیر معمول را بررسی کنید ..... **Error! Bookmark not defined.**
۴-۹-۳- مراقب محتویات تولید شده توسط افراد ثالث باشید ..... **Error! Bookmark not defined.**
۵-۹-۳- از جست جوی سایت (**SITE**)گوگل استفاده کنید ..... **Error! Bookmark not defined.**
۶-۹-۳- از **Webmaster Tools** گوگل استفاده کنید ..... **Error! Bookmark not defined.**
۷-۹-۳- از پروتوکل (قوانین) های امن استفاده کنید ..... **Error! Bookmark not defined.**
۸-۹-۳- وبلاگ امنیتی گوگل را مطالعه کنید ..... **Error! Bookmark not defined.**
۹-۹-۳- از هاستینگ خود پشتیبانی بخواهید ..... **Error! Bookmark not defined.**
۱۰-۳- لیستی از نقاط ضعف امنیتی وب سایت ها ..... **Error! Bookmark not defined.**
۱-۱۰-۳- کارت های اعتباری و بانکی ..... **Error! Bookmark not defined.**
۱۱-۳- امنیت در پایگاه های داده ای ..... **Error! Bookmark not defined.**
۱۲-۳- معماری امن شبکه با نگاه به پایگاه داده ..... **Error! Bookmark not defined.**
۱-۱۲-۳- ارائه امن اطلاعات ..... **Error! Bookmark not defined.**
۱۳-۳- تولید اطلاعات به صورت استاتیک و مسائل امنیتی آن ..... **Error! Bookmark not defined.**
۱۴-۳- تولید اطلاعات به صورت دینامیک ۳۳
فصل چهارم : نتیجه گیری ۳۵
۱-۴- چشم انداز آینده و نتیجه گیری ۳۶
منابع ..... Error! Bookmark not defined.

فهرست اشکال اتوماتیک

فهرست اشکال

عنوان **صفحه**

شکل ۱-۱ رمزنگاری کلید خصوصی ۵

شکل ۱-۲ رمزنگاری کلید عمومی (مرحله اول) ۷

شکل ۱-۳ رمزنگاری کلید عمومی (مرحله دوم) ۷

شکل ۱-۴ رمزنگاری کلید عمومی (مرحله سوم) ۸

شکل ۱-۵ رمزنگاری کلید عمومی (مرحله چهارم) ۸

شکل ۱-۶ رمزنگاری کلید عمومی (مرحله پنجم) ۹

شکل ۲-۱ شماتیکی از وب سرور ها ۱۲

شکل ۲-۲ تنظیمات سرور IIS ۲۰

شکل ۳-۱ شماتیکی از تجربیات کاربران از سرور SSL ..... **Error! Bookmark not defined.**

شکل ۳-۲ شماتیکی از چگونگی عملکرد EV SSL ..... **Error! Bookmark not defined.**

شکل ۳-۳ پایگاه داده و DMZ ..... **Error! Bookmark not defined.**

شکل ۳-۴ استفاده از دو کارت شبکه برای جدا سازی DMZ ..... **Error! Bookmark not defined.**

شکل ۳-۵ استفاده از SSH برای بر قراری تونل امن ..... **Error! Bookmark not defined.**

فهرست جداول اتوماتیک

فهرست جدول ها

عنوان صفحه

جدول ۲-۱ سهم استفاده بازار،از نرم افزار های وب سرور ۱۵

جدول ۲-۲ پشتیبانی های استاندارد توسط Apache و IIS ۲۷

جدول ۲-۳ مهم ترین تفاوت بین IIS و Apache در Perequisite ۲۸

فهرست علائم اختصاری

۱	IIS	Internet Information Services
۲	SSL	Secure Socket Layer
۳	LDAP	Lightweight Directory Access Protocol
۴	DNS	Domain Name System
۵	DHCP	Dynamic Host Control Protocol
۶	IP	Internet Protocol
۷	HTTP	Hyper Text Transfer Protocol
۸	HTTPS	HyperText Transfer Protocol Secure

چکیده

باگسترش استفاده از تکنولوژی وب و توسعه برنامه هایی که برای کارکرد درین بستر تولید میشوند مباحث مربوط به امنیت پایگاه های داده ای بعد جدیدتری پیدا کرده اند.

هر چند از آغاز پیداش پایگاه های داده همواره امنیت و تامین آن یک دغدغه مهم و پیاده سازی م کارای آن یک خصوصیت بنیادی در پایگاههای داده بوده است اما بهر روی بحث امنیت[۱] همواره مقولاتی همچون عملکرد مناسب[۲] ، کارایی[۳] و قابلیت اطمینان[٤] قرار میگرفت.

به عبارتی هنوز هم چندان عجیب نیست اگر ببینیم یک برنامه رده سازمانی (Enterprise Level زیادی Client بدون هیچگونه ملاحظه امنیتی تولید شده و مورد استفاده باشد.

حتی میتوان درین زمینه مثالهای جالبتری یافت. اغلب برنامه های Client-Server با نام کاربری sa (System Administrator) به پایگاه های داده متصل میشوند.

از دید امنیتی این مطلب یک فاجعه محسوب میشود. هیچ تغییر و یا خرابکاری ای قابل ردیابی نیست، همه کاربران به همه اطلاعات دسترسی دارند و الی آخر.

اجازه دهید یک فرض اساسی را مطرح کنیم. مدیران IT یک سازمان بر دو دسته اند: مدیران نوگرایی که به صورت داوطلبانه سازمان را به سمت ارائه خدمات عمومی و گسترده هدایت میکنند و به همین دلیل تکنولوژی وب را به عنوان تنها بستر موجود برای ارائه این خدمات می پذیرند و مدیران سنتی محافظه کاری که قابلیت اطمینان و کارایی سیستم جاری را تحت هیچ شرایطی حاضر نیستند در معرض خطر قرار دهند. وب از نظر این گروه دوم کماکان یک تکنولوژی مشکوک غیر قابل اطمینان است.

در واقع دلایل فنی این گروه دوم هنوز هم چشمگیر و قابل اعتناست، به خصوص گروهی که از mainframe ها صحبت میکنند.

قابلیت اطمینان ۰,۹۹۹۹۹ هنوز هم در دنیای غیر Mainframe یک رویاست و این پایان نامه به بررسی مسائل مربوط به امنیت وب سرور و وب سایت های در فضای مجازی اینترنت می پردازد.

واژه‌های کلیدی: امنیت وب سرور، امنیت وب سایت، فایروال ، سرور

در متن اصلی معادل فارسی کلمات لاتین نوشته میشود و کلیه اصطلاحات لاتین به صورت پاورقی نوشته شوند

۱- Security
۲- Functionality
۳- Performance
٤- Reliability

شماره صفحه (۱) از چکیده یا مقدمه شروع میشود

فصل اول : تعاریف

شماره گذاری بر اساس هر فصل و عناوین و زیر عناوین انجام میگیرد.

۱-۱- مقدمه

۱-۱-۱- تعریف وب سرور

یک برنامه کامپیوتری است که مسئول قبول کردن درخواستهای http از مشتریان است گرهای وب هستند و پاسخ ها را به همراه یک سری اطلاعات به آنها پست می‌کنند.

تو رفتگی ابتدای هر پاراگراف

این پاسخ ها همان صفحات Html هستند. بطور مثال اگر در صفحه مرور گرتان آدرس http://fa.wikipedia.org/index.php را وارد کنید ، یک درخواست به دامنه ای که نامش fa.wikipedia.org است ، فرستاده می‌شود.

یک کامپیوتراست که یک برنامه ی کامپیوتری را اجرا می‌کند و کارای اش همانند مطالبی است که دربالا گفته شد. هر کامپیوتری میتواند با نصب نرم افزار سرور به وب سرور تبدیل شود.

۱-۱-۲- ویژگی های مشترک

در عمل بسیاری از وب سرورها، ویژگیهای زیر را نیز پیاده سازی می‌کنند:

۱-شناسایی : درخواست شناسایی اختیاری قبل از اجازه دسترسی به انواع منابع

۲-نه تنها مفاهیم استاتیک (مفاهیم فایلی که بر روی سیستم فایلی وجود دارد) بلکه مفاهیم داینامیک را با یک یا چند ساختار نیز مانند SSI, CGI, SCGI, FastCGI, JSP, PHP, ASP, ASP.NET اداره می‌کند.

۳- پشتیبانی از HTTPS تا به کاربران اجازه دهد اتصالات مطمئنی به سرور را بر روی پورت ۴۴۳ به جای ۸۰ برقرار کنند.

۴-فشرده سازی مطالب تا بتوان از حجم پاسخ ها کم کرد. توسط کد سازی(GZIP)

۵-پشتیبانی از فایلهای بزرگ تا بتواند فایلهای بزرگ‌تر از ۲ گیگا بایت را سرویس دهی کند.

۶-کنترل کردن پهنای باند : تا سرعت پاسخها را محدود کند و شبکه را پر ازدحام نکند و قادر باشد تعداد بیشتری مشتری را سرویس دهی کند.[۲]

ارجاع متن به منبع استفاده شده در قسمت منابع (در تمام پایان نامه ، ملزم به رفرنسدهی میباشد)

۱-۲- سرور های اینترنتی

۱-۲-۱- آپاچی : (Apache)

این وب سرور در توسعه و همگانی شدن وب جهانی نقش بسیار مهمی داشته است .

متن : justify

این وب سرور که به زبان C نوشته شده است دارای قابلیت (cross- platform) بوده و بر روی ماشین های مختلف قابل اجرا میباشد .

دلیل انتخاب این اسم برای این وب سرور را نیز دو مورد ذکر کرده اند اول اینکه به یکی از قبایل قدیمی بومی آمریکا که به خاطر مقاومت و مهارت در ساخت ابزار آلات جنگی مشهور میباشند احترام گذاشته شود و ثانیا به این دلیل که (Root)ریشه پروژه به صورت یک سری پچ (Patch)میباشد . این وب سرور در یک گروه و به صورت کد باز (open source)گسترش یافت و از سال ۱۹۹۶ به عنوان محبوب ترین وب سرور برای HTTP در وب جهانی شناخته شده بود ولی در سال ۲۰۰۵ میدان مبارزه را به IIS مایکروسافت باخت و در حال حاضر نزدیک به ۴۹ ٪ بازار وب سرور های جهان را به خود اختصاص داده است همچنین MAC OS آن را به عنوان وب سرور اصلی در پشتیبانی از WEB OBJECT خود برگزیده است .

این وب سرور دارای ماژولهای امنیتی بسیار خوبی از جمله mod_access, mod_auth, mod_digest میباشد .

آپاچی برای میزبانی هر دو نوع وب ایستا و وب پویا مناسب است .

IIS -۱-۲-۲

وب سروری است که ارائه دهنده آن شرکت مایکروسافت میباشد و آخرین نسخه آن IIS۷,۰ است .

در واقع IIS مجموعه ای از سرویس های اینترنتی است که بصورت یکجا نمایش داده شده است .

طبق آخرین آماری که منتشر شد بعد از وب سرور آپاچی بیشترین محبوبیت را بین کاربران داشته است و هم اکنون نزدیک به ۳۶٪ بازار وب سرور های جهان را در اختیار دارد .

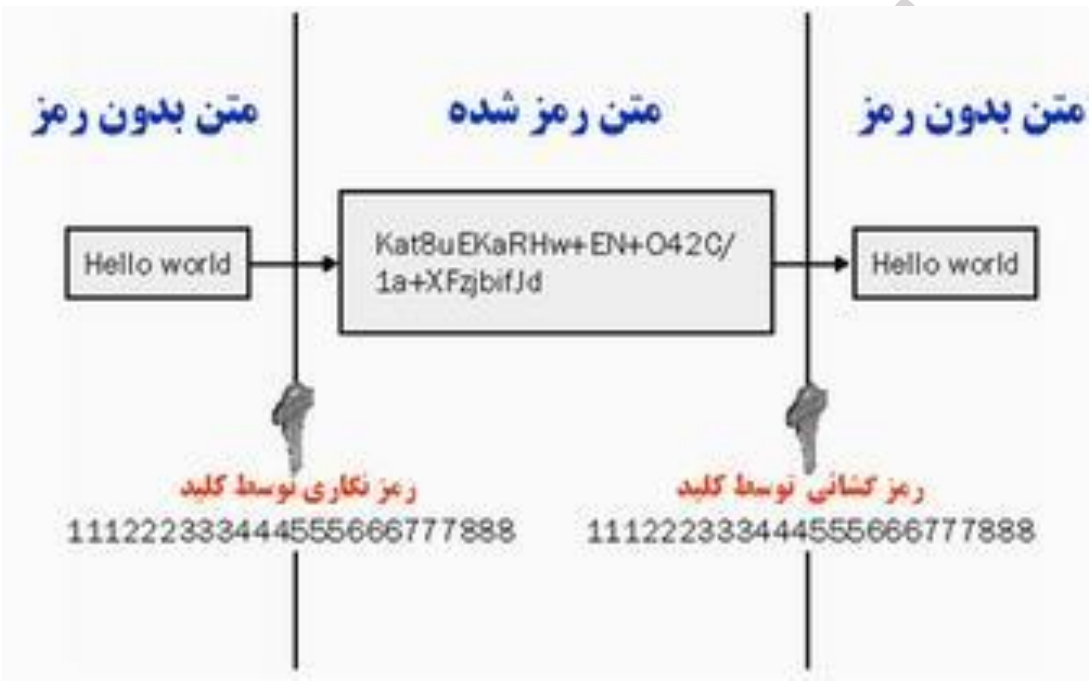
پلت فرمی که این وب سرور پشتیبانی میکند Microsoft Windows میباشد و در محیط های دیگر کار نمیکند .

برای اولین بار مایکروسافت آن را در یک پروژه آکادمیک در دانشگاه اسکاتلند به صورت مجانی عرضه کرد .

وسپس برای اولین بار از آن در Windows NT استفاده کرد که در آن قابلیت Active Server Page یا صفحه های فعال سرور را به آن افزود .

بعدها با تکامل نسخه های ویندوز ، IIS هم تکامل پیدا کرد و در نسخه شماره ۶,۰ آن مایکروسافت پشتیبانی از IPV ۶,۰ را نیز به آن اضافه کرد .

۳- مقایسه مشخصات امنیتی وب سرورهای آپاچی و IIS قبل از مقایسه باید به این نکته اشاره کنیم که به دلیل مجتمع بودن وب سرور IIS با سیستم عامل راه انداز آن ، و دارا بودن مسائل Integration مسائل امنیتی در این وب سرور بهتر رعایت شده است یعنی همان سیستمی که مسائل امنیتی را برای کابران سیستم اصلی فراهم میکند برای سیستم IIS هم کار میکند ولی آپاچی چون حالت Cross-platform دارد چنین قابلیتی را دارا نمی باشد .



شکل ۱-۱ رمزنگاری کلید خصوصی

شماره شکل بر اساس ترتیب عکس و شماره فصل نوشته میشود به همراه توضیحات مربوط به شکل

خصوصی دارای چندین نقطه ضعف می باشد. مبادله کلیدهای رمز در
ار و مشکل است .

دهای رمز ، مستلزم این واقعیت است که فرستندگان و گیرندگان می
بایست معتبر بوده و قبل از برقراری ارتباط ، آشنائی لازم را نسبت به یکدیگر داشته باشند(با تمام افرادیکه قصد ارتباط ایمن با آنان وجود داشته باشد) .

همچنین ، این نوع سیستم های رمزنگاری ، نیازمند استفاده از یک کانال ایمن به منظور توزیع کلیدهای " رمز" می باشند .

در صورتیکه چنین کانال ایمنی وجود داشته باشد ، چـرا از آن بـه منظـور ارسـال تمـامی پیـام رمـز استفاده نشود ؟ درسیستم های مبتنی بر وب که دارای تعاملات گذرا و کاربران متعددی مـی باشـند، به امکانات قدرتمندتری در ارتباط با رمزنگاری نیاز خواهد بود.

بنابراین ، رمزنگاری مبتنی بر کلید، عملا" به منظورایجاد یک ارتباط ایمن به تنهـائی کـافی نخواهـد بود. توزیع و عرضه کلید (یکی از مسائل مهم در ارتباط با مدیریت کلید) ، از جملـه مسـائل مهـم و درعین حال موثر به منظور شناخت سیستم های رمزنگاری جدید می باشد. رمزنگاری کلید خصوصـی دارای نقشی مهم در پروتکل SSL است(به همراه رمزنگاری کلید عمومی نامتقارن) .

۴-۳-۱- رمز نگاری کلید عمومی

رمزنگاری کلید عمومی که از آن با نام رمزنگاری نامتقارن نیز یاد می گردد ، دارای یک تفاوت مهم بـا رمزنگاری کلید خصوصی است . رمزنگاری کلید عمومی از دو کلید متفاوت استفاده مـی نمایـد : یـک کلید برای رمزنگاری و کلیدی دیگر برای رمزگشائی .

در رمزنگاری کلید خصوصی ، فرض بر این است که فرستنده و گیرنده دارای آگاهی لازم دررابطه بـا کلید استفاده شده در فرآیند رمزنگاری می باشند .

در رمزنگاری کلید عمومی ، با استفاده از یـک روش کـاملا" ایمـن یـک کلیـد بـرای ارسـال کننـده اطلاعات ایجاد و وی با استفاده از کلید فوق ، اقدام به رمزنگاری و ارسال پیام رمز شده بـرای گیرنـده می نماید . امکان رمزگشائی پیام رمز شده صرفا" توسط دریافت کننده ، امکان پذیر خواهد بود.

در رمزنگاری کلید عمومی ، سیستم یک زوج کلید خصوصی و عمومی ایجاد می نماید . کلید عمومی برای شخصی که از آن به منظور رمزنگاری یک پیام استفاده می نماید ، ارسال می گردد.

وی پس از رمزنگاری پیام با استفاده از کلید عمومی که دراختیار دارد ، پیام رمز شده را ارسـال مـی نماید .

دریافت کننده با استفاده از کلید خصوصی ، اقدام به رمزگشائی پیام می نماید .

(ماهیت کلید خصوصی استفاده شده در رمزنگاری کلید عمومی ، مشابه کلید خصوصی استفاده شده در رمزنگاری کلید خصوصی نمی باشد) .

حتی اگر یک فرد مزاحم ، به کلید عمومی دستیابی پیدا نماید وی نمی تواند با استفاده از آن اقدام به رمزگشائی پیام رمز شده نماید ، چراکه رمزگشائی پیام ، صرفا" با استفاده از کلید خصوصی امکان پذیر می باشد . برخلاف رمزنگاری کلید خصوصی ، کلید های استفاده شده در رمزنگاری کلید عمومی چیزی بمراتب بیشتر از رشته های ساده می باشند .

کلید در این نوع رمزنگاری دارای یک ساختار خاص با هشت فیلد اطلاعاتی است : از دو فیلد آن به منظور رمزنگاری با استفاده از کلید عمومی استفاده می گردد و شش فیلد دیگر به منظور رمزگشائی پیام با استفاده از کلید خصوصی مورد استفاده قرار می گیرد.

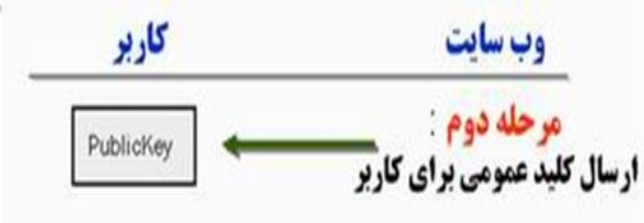
در سیستم رمزنگاری کلید عمومی با توجه به عدم ضرورت مبادله رمز مشترک ، اولین مسئله در مدیریت کلید برطرف می گردد.

رمزنگاری کلید عمومی ، شامل مراحل زیر است :

- مرحله اول : وب سایت مورد نظر ، یک زوج کلید عمومی و خصوصی را ایجاد می نماید .

شکل ۱-۲ رمزنگاری کلید عمومی (مرحله اول)

- مرحله دوم : وب سایت موردنظر ، کلید عمومی را برای کاربر ارسال می نماید .



شکل ۱-۳ رمزنگاری کلید عمومی (مرحله دوم)

• مرحله سوم : کاربر از کلید عمومی به منظور رمزنگاری داده مورد نظر خود استفاده می نماید (مثلا" شماره کارت اعتباری)

شکل ۱-۴ رمزنگاری کلید عمومی (مرحله سوم)

• مرحله چهارم : کاربر پیام رمز شده (در این مثال عدد رمز شده) را برای سرویس دهنده ارسال می نماید .

شکل ۱-۵ رمزنگاری کلید عمومی (مرحله چهارم)

•مرحله پنجم : سرویس دهنده با استفاده از کلید خصوصی ، پیام رمز شده دریافتی را رمزگشائی می نماید .

شکل ۱-۶ رمزنگاری کلید عمومی (مرحله پنجم)

۵-۳-۱- سیستم های مدرن رمز نگاری

یک رویکرد ترکیبی در سیستم های جدید رمزنگاری از ترکیب رمرنگاری مبتنی بر کلید عمومی و کلید خصوصی ، استفاده می گردد.

هر یک از روش های فوق دارای مزایای خاص خود بوده که با استفاده و ترکیب مزایای موجود در هر یک می توان یک مدل جدید رمزنگاری را ایجاد نمود.

حجم عملیات محاسباتی در مدل رمزنگاری کلید عمومی بالا می باشد (در مقایسه با مدل رمزنگاری کلید خصوصی) .

با توجه به سرعت مناسب مدل رمزنگاری کلید خصوصی (متقارن) در رابطه با حجم گسترده ای از اطلاعات ، در سیستم های رمزنگاری پیشرفته ، عموما" از مدل رمزنگاری کلید عمومی به منظور عرضه کلید استفاده شده و در ادامه از مدل رمزنگاری خصوصی به منظور رمزنگاری حجم بالائی از اطلاعات استفاده می گردد .

از سیستم های پیشرفته رمزنگاری در پروتکل SSL و به منظور ایمن سازی تراکنش های وب و یا ایمن سازی مدل نامه های الکترونیکی نظیر S/MIME که در محصولاتی نظیر مرورگر نت اسکیپ و IE پیش بینی شده است ، استفاده می گردد .

مسئله مدیریت کلید در هر سیستم رمزنگاری ،مجموعه ای از مسائل عملی و سوالات مختلف در رابطه با وجود امنیت لازم ، میزان اعتماد پذیری سیستم و رعایت حریم اطلاعات خصوصی ، مطرح می گردد. روش های رمزنگاری کلید عمومی و خصوصی که به آنان اشاره گردید، دارای امکانات لازم به منظور پاسخگوئی وارائه اطمینان لازم در خصوص امنیت اطلاعات می باشند .

مثلا" مرورگرهای وب از کلید عمومی یک وب سایت به منظور ارسال شماره کارت اعتباری برروی وب استفاده می نمایند .

با روشی مشابه ، شخصی که به فایل ها و یا اطلاعات حفاظت شده و رمز شده دستیابی پیدا می نماید ، می تواند با استفاده از یک کلید خصوصی ، اقدام به رمزگشائی آنان نماید .

در عمل ، هر یک از مسائل فوق ، نیازمند استفاده از یک کلید عمومی تضمین شده بوده که با استفاده از آن صحت عملیات رمزنگاری بین دو طرف درگیر در فرآیند رمزنگاری تضمین و امکان دخالت افراد غیر مجاز نیز سلب گردد .

رویکرد فوق ، سوالات متنوع دیگری را ذهن ایجاد می نماید :

• چگونه می توان اطمینان حاصل نمود که کلید عمومی استفاده شده توسط مرورگر به منظور ارسال اطلاعات کارت اعتباری ، همان کلید عمومی مورد نظر وب سایت دریافت کننده اطلاعات کارت اعتباری می باشد؟ (کلید عمومی تقلبی نباشد) .

• چگونه می توان با اطمینان اقدام به مبادله کلیدهای عمومی خود برای متقاضیان نمود تا آنان با استفاده از آن اقدام به رمزنگاری و ارسال اطلاعات نمایند ؟

فصل دوم: امنیت وب سرور ها در شبکه

عدم شماره گذاری صفحات اول هر فصل

۱-۲- مقدمه

با ورود اینترنت، مسئله امنیت مورد توجه بخش های مختلف آن قرار گرفت. یکی از این بخش ها و شاید مهم ترین بخش، قسمت سرورهای آن بود.

در این متن ضمن معرفی انواع سرور ها به طور خاص به مسئله امنیت در وب سرور ها پرداخته و سعی کرده ایم تا با معرفی و مشکلات امنیت آن ، کاربران و دانشجویان علاقمند را با اکثر این مشکلات آشنا سازیم. در ادامه به بحث در مورد چگونگی آشنایی با آسیب پذیری، مانند اسکنرهای آسیب پذیری و چگونگی برخورد با این مشکلات و حملات، مانند استفاده از فایروال ها پرداخته ایم.

شکل ۲-۱ شماتیکی از وب سرور ها

۱-۱-۲- به گزارش گروه ویژه امنیت ملی

استفاده از شبکه‌های کامپیوتری در سالیان اخیر روندی تصاعدی پیدا کرده است. شبکه‌های کامپیوتری، زیر ساخت مناسب برای سازمان‌ها و موسسات را در رابطه با تکنولوژی اطلاعات فراهم می‌نمایند.

مقوله تکنولوژی اطلاعات به همان اندازه که جذاب و موثر است، در صورت عدم رعایت اصول امنیت به همان میزان و یا شاید بیشتر، نگران کننده و مسئله آفرین خواهد بود.

اغلب سازمان‌های دولتی و خصوصی در کشور، دارای وب سایت اختصاصی خود در اینترنت می‌باشند. سازمان‌ها برای ارائه وب سایت، یا خود امکانات مربوطه را فراهم نموده و با نصب تجهیزات سخت افزاری و تهیه پهنای باند لازم، اقدام به عرضه سایت خود در اینترنت نموده اند یا از امکانات مربوط به شرکت‌های ارائه دهنده خدمات میزبانی استفاده می‌نمایند.

بدون تردید سرویس دهنده وب یکی از مهمترین نرم افزارهای موجود در دنیای اینترنت محسوب می‌گردد. کاربرانی که به سایت یک سازمان یا موسسه متصل و درخواست اطلاعاتی را می‌نمایند،

خواسته آنان در نهایت در اختیار سرویس دهنده وب گذاشته می‌شود. سرویس دهنده وب، اولین نقطه ورود اطلاعات و آخرین نقطه خروج اطلاعات از یک سایت است. نصب و پیکربندی مناسب چنین نرم افزار مهمی، بسیار حائز اهمیت بوده و تدابیر امنیتی خاصی را طلب می‌نماید.

۲-۲- تعریف سرور

به سرویس‌گیرنده‌ها و استفاده کنندگان از سرویس‌ها، میزبان و به سرویس دهنده‌ها و ارائه کنندگان سرویس، سرور گفته می‌شود. سرورها بسته به نوع خدماتی که ارائه می‌دهند دسته‌بندی‌های متفاوتی دارند. به عنوان مثال، به سرورهای زیر نگاهی بیاندازید:

Mail Server: سروری که به کاربران شبکه خدمات ایمیل را ارائه می‌دهد.

DHCP Server: سروری که به کاربران شبکه به طور خودکار آدرس IP می‌دهد.

DNS Server: سروری که امکان تبدیل درخواست کاربران شبکه، را برای دسترسی به سایت‌های اینترنت، با ارائه آدرس واقعی سایت مزبور می‌دهد، بدین ترتیب دیگر نیازی به حفظ بودن آدرس‌های IP سایت‌ها نخواهد بود.

Web Server: سروری که خدمات تحت وب را در قبیل میزبانی وب و ... را ارائه می‌دهد.

وب سرور در واقع به دو معنی است:

برنامه کامپیوتری که مسئول قبول کردن درخواستهای Http از مشتریان است که همان مرورگرهای وب هستند و پاسخ‌ها را به همراه یک سری اطلاعات به آنها ارسال می‌کند.

این پاسخ‌ها صفحات Html هستند.

بطور مثال اگر در صفحه مرورگر آدرس http//piau.ac.ir/index.php را وارد کنید، یک درخواست به دامنه‌ای که نامش piau.ac.ir است، فرستاده می‌شود تا نگاه سرور صفحه index.php را می‌فرستد.

کامپیوتری است که یک برنامه‌ی کامپیوتری را اجرا می‌کند و کارایی اش همانند مطالبی است که در بالا گفته شد. هر کامپیوتری می‌تواند با نصب نرم افزار سرور به وب سرور تبدیل شود.

در عمل بسیاری از وب سرورها، ویژگیهای زیر را نیز پیاده‌سازی می‌کنند:

شناسایی: درخواست شناسایی اختیاری قبل از اجازه دسترسی به انواع منابع

نه تنها مفاهیم استاتیک (مفاهیم فایلی که بر روی سیستم فایلی وجود دارد) بلکه مفاهیم دینامیک را با یک یا چند ساختار مانند ASP.NET, ASP, PHP, JSP ,FastCGI, SCGI ,SSI, CGI اداره می‌کند.

پشتیبانی از HTTPS تا به کاربران اجازه دهد اتصالات مطمئنی به سرور را بر روی پورت ۴۴۳ به جای ۸۰ برقرار کنند.

فشرده‌سازی مطالب تا بتوان از حجم پاسخها کم کرد (توسط کدسازیGZIP).

پشتیبانی از فایلهای بزرگ تا بتواند فایلهای بزرگ‌تر از ۲ گیگا بایت را سرویس‌دهی کند.

کنترل کردن پهنای باند تا سرعت پاسخها را محدود کند و شبکه را پر ازدحام نکند و قادر باشد تعداد بیشتری مشتری را سرویس دهی کند.

ترجمه مسیر : وب سرورها قادرند تا کامپوننت مسیر URL را به منابع فایل سیستم محلی (برای درخواستهای استاتیک) و برنامه داخلی یا خارجی (برای درخواستهای دینامیک) نگاشت کنند

برای مثال کاربر آدرس زیر را درخواست می‌کند:

http://www.example.com/path/file.html

مرورگر وب کاربر آنرا به یک اتصال به http://www.example.com با درخواست http ۱,۱ ترجمه می‌کند:

GET/path/file.html.php HTTP/۱,۱ HOST:http://www.example.com

۳-۲- انواع وب سرور

۱. وب سرور داخلی روی شبکه Intranet
۲. وب سرور خارجی روی شبکه Internet
۳. روی شبکه خصوصی قرار می‌گیرند.
۴. از اطلاعات مختص به شرکت نگهداری می‌کند.
۵. دسترسی به این سرور فقط از طریق کاربران داخلی است.
۶. روی شبکه عمومی قرار می‌گیرد.
۷. از اطلاعات کالاها، خدمات و تجارت شرکت نگهداری می‌کند.
۸. دسترسی به این سرور از طریق تمام کاربران امکان پذیر که ریسک بالایی دارد.
۹. وب سرور اینترانت

۱۰. وب سرور اینترنت

۱۱. سرورهای اینترنتی

سهم استفاده بازار، از نرم افزارهای وب سرور، در زیر نشان داده شده است که در برآورد Netcraft در ژانویه ۲۰۰۹ منتشر شده است.

فروشنده محصول	نام محصول	وب سایتهای میزبانی شده	درصد
بنیاد نرم افزار آپاچی	سرور آپاچی	۹۶،۵۳۱،۰۳۳	٪۵۲،۰۵
مایکروسافت	IIS	۴۷۴،۰۲۳،۶۱	٪۳۲,۹۰
گوگل	GWS	۹،۸۶۴،۳۰۳	٪۵,۳۲
Nginx	nginx	۳،۴۶۲،۵۵۱	٪۱,۸۷
Lighttpd	lighttpd	۲،۹۸۹،۴۱۶	٪۱,۶۱
Oversee	Oversee	۱،۸۴۷،۰۳۹	٪۱,۰۰
دیگر	-	۹،۷۵۶،۶۵۰	٪۵،۲۶
مجموع	-	۱۸۵،۴۷۴،۴۶۶	٪۱۰۰،۰۰

جدول ۲-۱ سهم استفاده بازار،از نرم افزارهای وب سرور

شماره جدول بر اساس ترتیب جدول و شماره فصل نوشته میشود به همراه توضیحات مربوط به جدول

HTTP Se در محیط کامپیوتری است، که به دلیل برخی از امکانات ل گسترش است.

می‌توان گفت که آپاچی برای برنامه نویسان حرفه‌ای برنامه‌ای فوق العاده است که به لحاظ امنیتی نیز به حفاظت سرورها و برنامه‌های موجود در آنها کمک می‌کند. متداولترین استفاده از ویژگیهای این برنامه htaccess است، که طراحان حرفه‌ای در محیط لینوکس از آن بهره می‌گیرند.

برای نمونه زمانی که بخواهند اولین صفحه در سایت صفحه بخصوصی باشد با یک دستور در آن پرونده (فایل) این امر ممکن می‌گردد یا زمانی که صاحب سایت مایل نیست که فایلهای موجود در سرور وی توسط دیگران دزدیده شود و بخواهد که مانع از پیوند مستقیم آنها شود آپاچی کمک می‌کند تا به خواستشان برسند.

زمانی که برنامه نویس بخواهد که محل واقعی صفحات دیده نشود نیز این برنامه مورد استفاده قرار می‌گیرد. این وب سرور در همگانی شدن وب نقش بسیار مهمی داشته است. این وب سرور که به زبان C نوشته شده، دارای قابلیت Cross- Platform بوده و بر روی ماشین‌های مختلف قابل اجرا می‌باشد. دلیل انتخاب این اسم برای این وب سرور را نیز دو مورد ذکر کرده‌اند.

اول اینکه به قبیله قدیمی بومی آمریکا که به خاطر مقاومت و مهارت در ساخت ابزار آلات جنگی مشهور می‌باشد احترام گذاشته شود و ثانیا به این دلیل که ریشه پروژه به صورت یک سری پچ می‌باشد.

این وب سرور در یک گروه و به صورت کد باز گسترش یافت و از سال ۱۹۹۶ به عنوان محبوب‌ترین وب سرور برای HTTP در وب جهانی شناخته شده بود ولی در سال ۲۰۰۵ میدان مبارزه را به IIS مایکروسافت باخت و در حال حاضر نزدیک به ۶۰٪ بازار وب سرورهای جهان را به خود اختصاص داده است. همچنین MAC OS آن را به عنوان وب سرور پیش‌فرض در پشتیبانی از WEB OBJECT خود برگزیده است.

این وب سرور دارای ماژولهای امنیتی خوبی از جمله mod_access, mod_auth, mod_digest می‌باشد.

آپاچی برای میزبانی هر دو نوع وب ایستا و وب پویا مناسب است.

یکی از کاربردی‌ترین موارد مربوط به آپاچی برای برنامه نویسان استفاده از پرونده (فایل) htaccess است. برنامه نویس می‌تواند با اعمال تغییراتی در این پرونده که بر هر شاخه‌ای قابل اضافه شدن است، دستورات ویژه آن شاخه را به سرور ارایه دهد.

برای نمونه اگر بخواهد که در صورت وارد کردن نشانی aa.html نام آن باقی بماند ولی در واقع پرونده main.php?page=bb اجرا شود به وسیله این پرونده قادر به اعمال دستورش خواهد بود.

امروزه عموماً می‌توانید آپاچی را در بسته‌های نرم‌افزاری لینوکسی که استفاده می‌کنید، بیابید.

تنها کافیست به برنامه‌ای که مربوط به نصب بسته‌های نرم‌افزاری است مراجعه کنید و بسته آپاچی را انتخاب کنید.

به عنوان مثال در لینوکس دبیان یا اوبونتو کافیست به داخل نرم‌افزار سیناپتیک بروید و بعد از انتخاب آپاچی آن را نصب کنید.

در لینوکس زوزه باید به YaST در قسمت اضافه و حذف نرم‌افزارها بروید و از آنجا آپاچی را نصب کنید.

پس از اجرای برنامه نصب خودکار، برنامه آماده استفاده است ولیکن هر فرد بنابر نیازهایی که دارد می‌تواند مشخصات سرور خود را تغییر دهد.

فایل httpd.conf حاوی اطلاعات سرور است که معمولاً با برنامه PHP همخوانی ندارد که با اضافه کردن چند دستور قابل اجرا است.

برای تعریف برنامه PHP دستورات زیر در پرونده مذکور اضافه می‌شود.

ScriptAlias /php/ “c:/php/”

AddType application/x-httpd-php.php

Action application/x-httpd-php “/php/php.exe”

IIS -۲-۳-۳

وب سروری است که ارائه دهنده آن شرکت مایکروسافت می‌باشد و آخرین نسخه آن IIS۷,۰ است. در واقع IIS مجموعه‌ای از سرویس‌های اینترنتی است که بصورت یکجا نمایش داده شده است.

طبق آخرین آماری که منتشر شد بعد از وب سرور آپاچی بیشترین محبوبیت را بین کاربران داشته است و هم اکنون نزدیک به ٪۳۶ بازار وب سرورهای جهان را در اختیار دارد.

پلتفرمی که این وب سرور پشتیبانی می‌کند Microsoft Windows می‌باشد و در محیط‌های دیگر کار نمی‌کند. ورژن‌های مختلف آن را در زیر می‌بینیم

IIS ۱,۰, Windows NT ۳,۵۱ available as a free add-on § IIS ۲,۰, Windows NT § ۴.۰ § IIS ۳,۰, Windows NT ۴,۰ Service Pack ۳ § IIS ۴,۰, Windows NT ۴,۰ Option Pack § IIS ۵,۰, Windows ۲۰۰۰ § IIS ۵,۱, Windows XP

Professional,Windows MCE § IIS ۶,۰, Windows Server ۲۰۰۳ and Windows XP Professional x۶۴ Edition § IIS ۷,۰, Windows Server ۲۰۰۸ and Windows Vista

برای اولین بار مایکروسافت آن را در یک پروژه آکادمیک در دانشگاه اسکاتلند به صورت مجانی عرضه کرد.

سپس برای اولین بار از آن در Windows NT استفاده کرد که در آن قابلیت Active Server Page یا صفحه‌های فعال سرور را به آن افزود.

بعدها با تکامل نسخه‌های ویندوز، IIS هم تکامل پیدا کرد و در نسخه شماره ۶،۰ آن مایکروسافت پشتیبانی از ASP.NET را نیز به آن اضافه کرد.

نسخه پنج IIS، صرفاً برای سیستم‌های مبتنی بر ویندوز ۲۰۰۰ قابل استفاده است.

نسخه‌های ویندوز ۲۰۰۰ Server و Advanced Server بمنظور نصب IIS، مناسب و بهینه می‌باشند.

نسخه پنج برای استفاده در نسخه‌های قدیمی ویندوز طراحی نشده است.

امکان نصبIIS نسخه پنج، بهمراه ویندوز Professional نیز وجود داشته ولی برخی از امکانات آن نظیر: میزبان نمودن چندین وب سایت، اتصال به یک بانک اطلاعاتی ODBC و یا محدودیت در دستیابی از طریق IP در آن لحاظ نشده است.

نسخه پنج IIS، سرویس‌های WWW، FTP، SMTP وNNTP را ارائه می‌نمایند.

سه نرم افزار و سرویس دیگر نیز با IIS در گیر می‌شوند: Index Server ،Certificate Server و Transaction Server.

۴-۳-۲- عملیات قبل از نصب IIS

در زمان نصب IIS، یک Account پیش فرض به منظور ورود کاربران گمنام به شبکه ایجاد می گردد.

نام پیش فرض برای Account فوق، IUSER_computername بوده که Computer Name نام کامپیوتری است که IIS بر روی آن نصب شده است.

Account فوق، می‌بایست دارای کمترین حقوق و مجوزهای مربوطه بوده و گزینه‌های User Cannot Change Password و Password Never Expires فعال شده باشد.

Account فوق همچنین می‌بایست از نوع Local Account بوده و domain-wide account را شامل نگردیده و دارای مجور ورود به شبکه بصورت محلی باشد (log on locally).

مجوزهای Access this computer from the network و یا log on as a batch job در رابطه با account فوق می‌بایست غیر فعال گردند.

در صورتیکه سیاست ارتباط با وب سایت، صرفاً برای کاربران مجاز باشد، پیشنهاد می‌گردد Account فوق، غیر فعال گردد.

بدین ترتیب تمام کاربران باید با استفاده از نام و رمز عبور مربوطه قادر به ورود به سایت خواهند بود.

۲-۳-۵- سرویس های IIS

در زمان نصب IIS، چهار سرویس بر روی سیستم نصب خواهد شد:

WWW: سرویس مذکور، بمنظور ایجاد یک سرویس دهنده وب و سرویس دهی لازم به درخواست سرویس گیرندگان برای صفحات وب استفاده می‌گردد.

FTP: سرویس مذکور، بمنظور ارائه خدمات لازم در خصوص ارسال و دریافت فایل بر روی سرویس دهنده برای کاربران استفاده می‌گردد.

SMTP: سرویس مذکور، امکان ارسال و دریافت نامه الکترونیکی برای سرویس گیرندگان را در پاسخ به فرم‌ها و برنامه‌های خاص دیگر فراهم می‌نماید.

NNTP: سرویس مذکور، بمنظور میزبانی یک سرویس دهنده خبری USENET استفاده می‌گردد.

در زمان نصب IIS، می‌توان تصمیم به نصب برخی از سرویس‌ها و یا همه آنها گرفت. بعد از نصب IIS، در صورتیکه به وجود برخی از سرویس‌ها نیاز نباشد، می‌توان آنها را غیر فعال نمود. بدین منظور می‌بایست مراحل زیر را دنبال کرد:

انتخاب گزینه Services از طریق مسیر زیر:

Programs => Administrative Tools => Services

انتخاب سرویسی که قصد غیر فعال کردن آن را داریم. در ادامه با فعال کردن کلید سمت راست ماوس، گزینه Stop را بمنظور توقف سرویس فعال نمائید.

بمنظور اطمینان از عدم اجرای سرویس غیر فعال شده در زمان راه اندازی مجدد سیستم، سرویس را مشخص و پس از فعال کردن کلید سمت راست ماوس، گزینه Properties را انتخاب و در بخش Startup type وضعیت اجرای سرویس را از حالت Automatic به Disable تغییر دهید.

شکل زیر نحوه غیر فعال نمودن سرویس WWW را نشان می‌دهد.

شکل ۲-۲ تنظیمات سرور IIS

۴-۲- نحوه فعال کردن سرویس www

۱-۴-۲- امنیت برنامه IIS

امنیت در IIS متاثر از سیستم عامل است.

مجوزهای فایل‌ها، تنظیمات ریجستری، استفاده از رمز عبور، حقوق کاربران و سایر موارد مربوطه، ارتباط مستقیم و نزدیکی با امنیت در IIS دارند.

قبل از پیکربندی مناسب IIS، لازم است که نحوه استفاده از سرویس دهنده دقیقاً مشخص گردد. پیکربندی دایرکتوری‌های IIS، فایل‌ها، پورت‌های TCP/IP وAccount کاربران نمونه‌هائی در این زمینه بوده که پاسخ مناسب به سوالات زیر در این رابطه راهگشا خواهد بود:

- آیا سرویس دهنده از طریق اینترنت قابل دستیابی است ؟
- آیا سرویس دهنده از طریق اکسترانت قابل دستیابی است ؟
- چه تعداد وب سایت بر روی سرویس دهنده میزبان خواهند شد ؟
- آیا وب سایت‌ها نیازمند استفاده از محتویات بصورت اشتراکی می‌باشند ؟
- آیا سرویس دهنده امکان دستیابی را برای افراد ناشناس (هر فرد) فراهم نموده و یا صرفاً افراد مجاز حق استفاده از سرویس دهنده را خواهد داشت؟ آیا هر دو؟
- آیا امکان استفاده و حمایت از SSL وجود دارد؟
- آیا سرویس دهنده صرفاً برای دستیابی به وب از طریق HTTP استفاده می‌گردد؟
- آیا سرویس دهنده، سرویس FTP را حمایت می‌نماید؟
- آیا کاربرانی وجود دارد که نیازمند عملیات خاصی نظیر کپی، فعال نمودن، حذف و یا ... فایل‌هائی بر روی سرویس دهنده باشند؟

موارد زیر در زمان نصب IIS پیشنهاد می‌گردد:

- کامپیوتری که IIS بر روی آن نصب شده است را در یک محل امن فیزیکی قرار داده و فقط افراد مجاز قادر به دستیابی فیزیکی به سرویس دهنده باشند.
- در صورت امکان، IIS را بر روی یک سرویس دهنده Standalone نصب نمائید.

در صورتیکه IIS بر روی یک سرویس دهنده از نوع Controller Domain نصب گردد و سرویس دهنده وب مورد حمله قرار گیرد، تمام سرویس دهنده به همراه اطلاعات موجود در معرض آسیب قرار خواهند گرفت.

علاوه بر مورد فوق، نصب IIS بر روی یک سرویس دهنده از نوع Domain controller، باعث افزایش حجم عملیات سرویس دهنده و متعاقباً کاهش کارآئی سیستم در ارائه سرویس‌های مربوط به وب خواهد شد.

- برنامه‌های کاربردی و یا ابزارهای پیاده‌سازی نمی‌بایست بر روی سرویس دهنده IIS نصب گردند.
- کامپیوتر مربوط به نصب IIS را بگونه‌ای مناسب پارتیشن نموده تا هر یک از سرویس‌ها نظیر www و یا FTP بر روی پارتیشن‌های مجزاء قرار گیرند.
- IIS امکان نصب برنامه‌ها را در مکانی دیگر بجز پارتیشن C فراهم نمی‌نماید (مگر اینکه یک نصب سفارشی داشته باشیم.) موضوع فوق به عملکرد سیستم عامل مرتبط می‌گردد.

مجوزهای پیش فرض در رابطه با %Systemdrive% اعمال می‌گردد (مثلاً درایو C). موضوع فوق می‌تواند باعث عدم صحت کارکرد مناسب برنامه‌های سرویس‌های IIS گردد.

می‌بایست مطمئن شد که مجوزهای سیستم عامل یا عملیات مربوط به سرویس‌های IIS، رابطه‌ای ندارند.

- تمام پروتکل‌های پشته‌ای (Stack) غیر از TCP/IP را از روی سیستم حذف نمائید.

(در مواردی که برخی از کاربران اینترانت نیازمند برخی از این نوع پروتکل‌ها می‌باشند می‌بایست با دقت اقدام به نصب و پیکربندی مناسب آن نمود.)

- روتینگ IP، بصورت پیش فرض غیرفعال است و می‌بایست به همان حالت باقی بماند.

در صورت فعال شدن روتینگ، این امکان وجود خواهد داشت که داده‌هائی از طریق کاربران اینترانت به اینترنت ارسال گردد.

- نصب Client for Microsoft networking، به منظور اجرای سرویس‌های HTTP,FTP,SMTP و NNTP ضروری خواهد بود.

در صورتیکه ماژول فوق نصب نگردد، امکان اجرای سرویس‌های فوق بصورت دستی یا اتوماتیک وجود نخواهد داشت.

- در صورتیکه تمایل به نصب سرویس‌های NNTP و SMTP، می‌بایست سرویس File and Print Sharing for Microsoft نیز نصب گردند.
- در رابطه با account IUSER_Computername، گزینه‌های User cannot change password و Password Never Expires را انتخاب و فعال نمائید.
- در صورتیکه تمایلی به ورود افراد گمنام به شبکه وجود نداشته باشد، می‌بایست Account مربوطه را غیر فعال نمود.
- برای هر وب سایت local admin groups ایجاد و Account مربوطه را مشخص نمائید.
- تمام مجوزهای NTFS مربوط به دایرکتوری Inetpub را حذف و صرفاً گروه‌ها و accountهای مجاز را به آن نسبت دهید.
- یک ساختار منطقی برای دایرکتوری ایجاد نمائید. مثلاً برای محتویات ایستا، فایل‌های asp، scripts و Html ، اسامی دایرکتوری دیگری ایجاد و با یک ساختار مناسب به یکدیگر مرتبط گردند.
- مجوزهای لازم NTFS بر روی ساختار دایرکتوری‌ها را در صورت نیاز اعمال نمائید.
- تمام دایرکتوری‌های نمونه و اسکریپت‌هائی که نمونه برنامه‌هائی را اجراء می‌نمایند، حذف نمائید.
- مجوز Log on locally را به کاربر اعتبار و ابزار as abatch service log on و Access this computer from the network از کاربر سلب گردد.

۵-۲- به گزارش ویژه گروه امنیت ملی

۱-۵-۲- مقایسه IIS و Apache

شما باید ابتدا نیازهای سیستم، محیط‌های عملیاتی، تدابیر یکپارچگی و ... را در پروژه خود شناخته و بعد تصمیم بگیرید.

اگر می خواهید یک وب سرور مطلق طراحی کنید هر دو مناسب هستند و می توانید هر کدام را که دوست دارید انتخاب کنید ولی بعضی مواقع فاکتورهای با ارزش، مسائل پشتیبانی، نگهداری و ملاحظات دیگر وجود دارند.

بنابراین فقط بعد از همه این واقعیتها و حقایق، متوجه می‌شوید که کدام محصول مناسبتر است و می‌تواند نیازهای شما را برآورده سازد.

از زمان ارائه سیستم عامل شبکه‌ای ویندوز NT ۴,۰، وب سرور IIS، یکی از اجزای سیستم عامل‌های سرور مایکروسافت بوده که نصب یا عدم نصب آن از طرف کاربر به صورت دلخواه و به راحتی در هر زمانی قابل انجام بوده است.

به عنوان مثال ویندوز NT۴,۰ همراه IIS۴، ویندوز ۲۰۰۰ همراه IIS۵ و ویندوز XP به همراه IIS۵,۱ به بازار ارائه شدند. تا قبل از ویندوز ۲۰۰۳، کلیه ویرایش‌ها و نسخه‌های مختلف IIS بسیار مشابه هم بودند و می‌شد آنها را جزء یک خانواده به حساب آورد، اما پس از آن و با به میان آمدن ویندوز ۲۰۰۳، که نسخه ششم IIS را بهمراه خود داشت، قضیه کاملاً متفاوت شد.

در این نسخه که می‌توان آن را یک بازنویسی کامل از وب سرور قدیمی دانست، بسیاری از مدلهای اجرای کد، تسهیلات مربوط به مدیریت و سرعت وکارایی آن، دچار تغییرات و بهبودهای قابل ملاحظه‌ای شده است.

از طرف دیگر آپاچی با سابقه‌ای بیشتر که بر اساس کدینگ Http کار می‌کرد، همواره بعنوان سمبل وب سرورهای دنیای یونیکس مطرح بود.

نسخه x۳,۱ آپاچی که تا سال ۲۰۰۲ مورد استفاده قرار می‌گرفت، با استفاده از ترفندهای تکنیکی خاصی بر روی سایر سیستم عامل‌ها و حتی ویندوز هم قابل نصب و اجرا بود.

اما با پیدایش آپاچی نسخه ۲، همه معادلات دچار تحولی بزرگ گردیده است. این نسخه که دارای محیطی کاملاً تغییر یافته بوده و توابع درون آن با ظرافت هرچه تمام‌تر استقلال خود را از سیستم عامل تثبیت کرده بودند، توانست بر روی کلیه سیستم عامل‌های ویندوز، یونیکس، لینوکس، مک OSX و حتی سیستم عامل‌های دیگری چون VMS و BE OS نصب و اجرا شود.

در مقام مقایسه IIS و APACHE، می‌توان گفت که هرکدام دارای مزایا و معایبی هستند.

IIS فقط برای اجرا در ویندوز ساخته شده است. به خصوص نسخه ششم آن، فقط در ویندوز ۲۰۰۳ قابل اجرا می‌باشد.

اگرچه بسیاری از کارشناسان، این مسئله را نوعی نقطه ضعف در ساختار IIS می‌دانند، برخی دیگر هماهنگی بسیار دقیق میان آن و ویندوز ۲۰۰۳ و سرویس‌های دیگر سیستم عامل را که باعث آسان‌تر شدن مدیریت IIS شده است را از نقاط برتری آن به حساب می‌آورند.

به خصوص در نسخه ششم جدا شدن ماژول مخصوص دریافت درخواستها (Request) از ماژول ویژه پردازش آن‌ها، سهم بسزایی در افزایش کارایی آن داشته است.

در این روش ماژول Listener که در کِرنل مستقر شده است (Http.sys)، درخواستهای ارسالی از طرف کلاینت‌ها را دریافت کرده و آنها را به ترتیب در داخل یک یا چند صف درخواست قرار می‌دهد. سپس IIS به این درخواست‌ها با اختصاص حداقل یک پروسه کاری (Worker Process) به هر درخواست، پاسخ می‌دهد.

این ویژگی باعث می‌شود حتی زمانی که IIS به شدت مشغول پاسخ دهی به درخواست‌های قبلی است، ماژول جداگانه‌ای که در کِرنل مستقر است، بتوانند درخواست‌های جدید را دریافت کرده و حداقل آنها را در انتظار پاسخ قرار دهند.

همچنین با این وضعیت، سیستم عامل می‌تواند کنترل بهتری را در اختصاص پروسه‌های لازم به IIS جهت پردازش درخواست‌ها انجام دهد. در آپاچی هم، جریان تا حدودی مشابه همین روال است.

در اینجا تعدادی ماژول با قابلیت انجام چند پردازش در واحد زمان وظیفه دریافت پاسخ به درخواست‌ها را برعهده دارند.

این ماژول‌ها که با استفاده از تکنولوژی APR بر روی بسیاری از سیستم عامل‌هایی که از کدهای کامپایل شده زبان C پشتیبانی می‌کنند، قابل اجرا هستند.

با استفاده از امکانات و قابلیت‌های Multi-Threading همان سیستم عامل میزبان به سرعت و به صورت همزمان در خواست‌های رسیده از طرف کلاینت‌ها را در صف پردازش می‌کنند.

Standards Support در بسیاری از قراردادها و خریدها مهم می‌باشد. جدول زیر خلاصه‌ای از پشتیبانی‌های استاندارد را توسط Apache و IIS نشان می‌دهد.

Comments	IIS	Apache	Feature
	Yes	Yes	HTTP ۱,۱
A commercial plug-in SNMP module is available for Apache from Covalent that provides real-time management information for Server	Yes	No	SNMP

access statistics, activity, load and utilization as well as on-the-fly configuration changes. Additional information is available at http://www.covalent.net/products/snmp/.			
	es	Yes	W۳C's extended log format
ISAPI extension modules are written by third parties and available as part of the Apache distribution.Apache supports ISAPI extensions but does not support ISAPI filters.	es	Yes	ISAPI
A module is available for Apache that provides strong cryptography for the Apache ۱,۳ Web Server SSL ۲/۳ and TLS ۱ (Transport Layer Security ۱) protocols.However, this module can be used only outside the United States for free.In the United States, you can use it for noncommercial purposes for free if you use RSAREF (because of various patents held by RSA).	es	Restricted	SSL ۲,۰/۳,۰
Part of Apache ۲,۰ functionality. WebDAV, which stands for Web	es	Yes	WebDAV

			Distributed Authoring and Versioning, is a standard under development by W۳C, for Web-based collaborative document development.

جدول ۲-۲ پشتیبانی های استاندارد توسط Apache و IIS

مهمترین تفاوت بین IIS و Apache در Prerequisite (شرایط لازم) می‌باشد که در جدول زیر خلاصه شده است.

Feature	Apache	IIS
OS dependency	یونیکس، لینوکس، ویندوز، OS/۲	ویندوز
Hardware platforms	Wide range of hardware supported by the different operating systems, including Intel and SPARC.	Those supported by Windows.

جدول ۲-۳ مهم ترین تفاوت بین IIS و Apache در Perequisite

۲-۶- مقایسه امنیتی Apache در مقابل IIS

چندی پیش مدیران وب، خیلی درگیر ورودیها به سازمان وب سرور خود نبودند، اگر با ویندوز کار می‌کردند IIS مایکروسافت را اجرا می‌کردند و اگر از Linux\Unix استفاده می‌کردند وب سرور Apache را انتخاب می‌کردند و این دو هرگز با هم برخورد نداشتند اما زمان تغییر کرده است و پروژه Apache Http Server محدودیت را از بین برده و دیوارها را خراب کرده است و کار مدیران ویندوز را آسان کرده است (انتظار نمی رود که مایکروسافت IIS را برای Linux به کار ببرد).

۴ فاکتور وجود دارد که می توانید تصمیم بگیرید که کدام امنیت بیشتری برای تشکیلات شما دارد.

۲-۶-۱- آسیب پذیری ذاتی سرور

Platformها در مقابل حملات آسیب پذیر هستند.

تحقیقات اخیر در CERT، پایگاه داده های آسیب پذیر را معرفی کرده است.

آسیب پذیری IIS را ۲۸ و آسیب پذیری Apache را ۲۵ اعلام کرده است.

۲-۶-۲- دانش و آگاهی از مدیریت وب سرور

اگر مدیران وب شما با یکی از Platformها آشنایی دارند، برای تنظیمات امنیتی مورد نظر بر روی آن راحت هستند.

Platform فاکتور بسیار مهمی می‌باشد.

تعداد زیادی از نفوذهای امنیتی به پیکربندی اشتباه به وسیله مدیران که مهارتهایشان کافی نمی باشد، مربوط می‌شود.

ساخت یک اشتباه موقعه ای که با یک platform جدید کار می‌کنید بسیار آسان است.

۲-۶-۳- انتخاب درست سیستم عامل(OS) توسط مدیران

امنیت یک وب سرور فقط به خوبی انتخاب یک سیستم عامل اصولی بستگی دارد.

اگر یک هکر بتواند به OS دسترسی پیدا کند، به خطر افتادن وب سرور کاری غیر قابل پیش بینی نیست.

بنابراین مهارتهای مدیران سیستم در تصمیم انتخاب OS مناسب مهم می باشد .

اگر با windows کار می کنید هر دو IIS و Apache قابل run شدن هستند.

اما اگر از Unix استفاده می کنید، باید از Apache استفاده کنید، به طوری که با switch کردن به IIS به باز آموزی مدیران به کار با محیط ویندوز نیاز پیدا خواهیدکرد.

۴-۶-۲- مهارت های توسعه دهنده

اگر صفحات وب Dynamic میسازید (CGI , PHP , Aspو ...)، به مهارتهای امنیتی توسعه دهنده باید توجه کنید.

مثلاً مدیران OS Developerها باید از بروز اشتباهات جلوگیری کنند و همچنین مواظب پورتهای بسیاری از سیستمهای توسعه وب مشترک برای Platformها برای آنچه که در اینترنت قابل دسترسی است بوده باشند.

یکی از مزایای IIS، ارتباط تنگاتنگ موجود بین آن و سیستم عامل است.

این عامل سبب می شود تا IIS با توجه به اینکه سیستم عامل، بسیاری از موارد امنیتی را قبل از رسیدن درخواست به وب سرور مورد بررسی قرار می دهد و هویت کاربران متصل را ارزیابی میکند، و با اطمینان بیشتری به کار خود ادامه دهد.

ضمن این که مدیر سیستم هم به دلیل اشتراک روشی که در تأمین امنیت بین سیستم عامل و وب سرور وجود دارد، مجبور به دوباره کاری نمی‌شود.

به عنوان مثال اگر در اکتیو دایرکتوری ویندوز ۲۰۰۳ دسترسی به یک یا چند فایل خاص را برای یک گروه از کاربران مجاز و برای گروهی دیگر غیر مجاز تعریف کرده باشید، این کاربران از هر روشی که بخواهند به آن فایلها دسترسی پیدا کنند (حتی از طریق وب سرور).

باید تابع قواعد تنظیم شده در اکتیو دایرکتوری باشند و این قوانین در IIS نیز حکمفرما است.

در مورد آپاچی نسخه دوم، مسئله به این سادگی و روانی نیست و قاعدتاً مدیریت امنیت در مورد آن پیچیده‌تر و وقت گیرتر از IIS است.

البته اکنون ماژول ها و آداپتورهای جدیدی در آپاچی تعبیه شده که امکان ارتباط بین آن و اکتیو دایرکتوری ویندوز یا Password یونیکس را به وجود می آورد، اما باز هم می توان گفت که اصولاً با وجود این ارتباط در آپاچی، سیستم عامل و وب سرور هر کدام ساز خود را می زنند و آپاچی چندان از قواعد امنیتی تعریف شده در سیستم عامل تبعیت نمی کند.

البته بسیاری از طرفداران آپاچی این مسئله را نوعی نقطه قوت آپاچی دانسته و با ذکر این نکته که اولاً هر درخواست از طرف خارج باید از دو سد محکم سیستم عامل و وب سرور عبور کند و ثانیاً حفره‌های امنیتی در سیستم عامل‌های یونیکس و آپاچی کمتر از ویندوز و IISاست.

استفاده از آپاچی را از لحاظ امنیتی دارای ریسک کمتری نسبت به IIS می‌دانند.

از لحاظ پروتکلهای امنیتی، هر دو وب سرور کلیه پروتکلها از جمله IPsec، SSL و مکانیسم‌های هویت سنجی Basic Digest LDAP را پشتیبانی می کنند.

۷-۲- تامین امنیت سایت و سرور

با توجه به پیشرفت دنیای مجازی حفظ امنیت این فضا در مقابل نفوذگران و افراد سود جو یکی از مهمترین و به روزترین مسائل می باشد .

با توجه به اهمیت حفظ اطلاعات در مقابل افرادی که حق دسترسی به این اطلاعات را ندارند نیاز به مشاوره با متخصصان امنیتی احساس می شود .

برقراری امنیت در تمامی حوزه ها از جمله سرورها ، برنامه های تحت وب ، شبکه های داخلی و ... امری بسیار پیچیده و تخصصی است که پرداختن این کار به هر شرکتی باید با تامل صورت گیرد .

در این حوزه بهترین متخصصانی که می توانند امنیت شما را برقرار کنند کسانی هستند که به تمامی شیوه های نفوذ نیز کاملا آگاه باشند .

برترین امتیاز این افراد در دست داشتن روش هایی است که مشاوران امنیتی از آن آگاه نیستند .

شرکت امنیتی میهن هک با کارشناسان متخصص و با بیش از ۶ سال تجربه فعالیت در زمینه امنیت شبکه اقدام به مشاوره و پیاده سازی تمامی طرح های امنیتی می کند .

با توجه به دسترسی کارشناسان شرکت امنیتی میهن هک به دنیای زیر زمینی نفوذگران و حفره گیری از این امر و در دست داشتن به روز ترین اطلاعات نفوذ و ضد نفوذ اقدام به پیاده سازی تدابیر امنیتی بر روی سرور های شما می کند .

با توجه به نیاز به ، بروزرسانی تمامی لایه های ایجاد شده ، کارشناسان شرکت امنیتی میهن هک به صورت تمام وقت نسبت به ارائه خدمات و پشتیبانی های لازم برای امن سازی سرویس دهنده های شما اقدام خواهند کرد.

۸-۲- ۱۰ روش مفید برای بالا بردن ضریب امنیت در سرور های Cpanel

توجه داشته باشید این توصیه ها فقط به صورت یک پیشنهاد هستند.

همان طور که می دانید امنیت یک سرور به مسائل بسیار پیچیده ای مرتبط هست و با چند مورد نمیشه اونها رو خلاصه کرد.

لذا موارد زیر رو می تونید درصورت تمایل روی سرور خودتون اعمال کنید.

۱- از کلمات عبور پیچیده استفاده کنید.

کلمات عبور ساده بزرگترین مشکل امینتی را برای سرور شما به وجود می آورند.

داشتن کلمات عبور امن و پیچیده (چه برای خود سرور و چه برای کاربرانی که روی سرور قرار دارند) بسیار با اهمیت است.

فصل سوم : امنیت وب سایت ها

فصل بندی با کمک اساتید محترم راهنما انجام میگیرد.

۳-۱- مقدمه

در مقدمه فصل از تلاش شرکت های میزبانی وب برای حفظ امنیت سرور های خود سخن گفته و اینکه امنیت موضوع تضمین شدنی نیست و هیچ شرکتی در دنیا نمی تواند ادعای تضمین ۱۰۰ درصدی سرورها و سرویس های خود را حتی با صرف هزینه های بالای امنیتی کند.

امنیت یک مقوله چند وجهی هست ، امنیت سایت ، امنیت سرور و امنیت حریم خصوصی کاربر.

یکی از مهم‌ترین عوامل افزایش امنیت یک وب‌سایت رعایت موارد امنیتی توسط مالک ، طراح و استفاده کننده سایت می‌باشد.

با توجه به اینکه شرکت ها تلاش می کنند تمامی موارد امنیتی را رعایت نماید در صورتی که مالکین ، طراحان و استفاده‌کننده سایت نیز موارد امنیتی را رعایت نمایند امنیت سایت های آنان به حدی افزایش خواهد یافت که احتمال نفوذ به آن ناچیز خواهد شد در همین راستا به تمامی کاربران توصیه می‌گردد تمامی موارد ذکرشده در ادامه این مقاله آموزشی را به دقت مطالعه نموده و اجرا نمایند تا امنیت وب سایت های آنان به میزان استاندارد افزایش یابد.

۳-۱۴- تولید اطلاعات به صورت دینامیک

این روش متداول ترین شیوه ایست که امروزه جهت ارائه خدمات بر بستر وب مورد استفاده قرار میگیرد.

درین روش صفحات موجود بر روی سرور وب عملا دارای هیچ اطلاعاتی نمیباشند یا دارای حداقل اطلاعات هستند.

تمامی اطلاعات در پایگاه داده است. به محض دریافت هر تقاضایی توسط سرور وب ، صفحات مورد درخواست او به صورت دینامیک از طریق جستجوی (Query) مناسب در پایگاه داده تولید میشود.

طی بخش گذشته عموما توجه ما معطوف به این مطلب بود که چگونه جلوی دستیابی افراد غیر مجاز به سیستم و اطلاعات گرفته شود.

اما هیچ گاه به این مطلب اشاره نکردیم که مجاز یا غیر مجاز بودن افراد را چگونه تشخیص میـدهیم. در واقع روش شناسایی افراد در یک سیستم امن چگونه میتواند باشد.

ابتدایی ترین روشی که درین زمینه میتوان در نظر گرفت تصدیق اعتبار ساده بر حسب نام کـاربری و کلمه عبور است. گرچه پیاده سازی این روش سنتی بسیار ساده است اما امنیتی هم که تامین میکند حداقل امنیت ممکن است.

درین روش کاربر یکبار در سیستم شناسایی میشود و پس ازان اطلاعـات بـه صـورت عـادی بـر روی شبکه جریان می یابد.

مشکلات این روش را میتوان به صورت زیر خلاصه کرد:

تمامی اطلاعات در بین راه قابل شنود هستند.

بند بالا به خصوص شامل خود نام کاربری و کلمه عبور هم میشود.

به عبارتی این دو هم به سادگی میتوانند توسط شخص ثـالثی در بـین راه شـنود شـده و بعـدا مـورد استفاده قرار گیرند.

در شرایطی که نام کاربری و کلمه عبور لو رود کل امنیت سیستم دچار اخلال خواهد شد.

در واقع این روش تنها تضمین کننده حداقل غیر قابل قبولی از امنیت در تصدیق اعتبـار افـراد اسـت. بنابراین باید به دنبال روشهای جایگزینی بود که معایب فوق را نداشته باشند.

فصل چهارم : نتیجه گیری

۱-۴- چشم انداز آینده و نتیجه گیری

به طور خلاصه می توان گفت که حملات هکرها به سایت های اینترنتی هر روز پیچیده و پیچیده تر می شود، بالاخره با پیشرفت مسائلامنیتی باید هم این طور باشد.

با افزایش پیچیدگی های امنیتی آنتی ویروس ها، فایروال ها ، و برنامه های مبتنی بر به روز رسانی دوره ای، هکرها هم که منبع درآمدشان را در خطر می بینند، نیاز به راه های خلاقانه و جدیدتری دارند.

در نتیجه آنها در پاسخ به افزایشامنیت با حملات فزاینده و پیچیده به جنگ صنعت امنیت رفته و فعالان این عرصه را به کار و تلاش دائمی برای مبارزه در این نبرد بی پایان وا می دارند.

اما چگونه هکرها همواره یک گام جلوتر از کارشناسان امنیتی قدم بر می دارند؟ یکی از این جواب ها آشکار است آنان مجبورند از ابتکار بیشتری برخوردار باشند در غیر این صورت باید این حرفه را کنار بگذارند.

یکی دیگر از جواب ها به ساختار تشکیلاتی هکرها بر می گردد یک هکر تنها که در زیرزمین خانه اش کار می کند خلاقانه تر و سریعتر اهداف خود را تامین می کند، تا یک شرکت نرم افزاری بزرگ و پر پیچ و خم .

بنابراین احتمال موفقیت هکر حرفه ای مطمئنا بیشتر است.

با این حال ، می توان گفت عاملی که بزرگترین نقش را در موفقیت مداوم هکرها دارد، فقدان آگاهی و هوشیاری لازم از سوی کاربران نرم افزار و صاحبان وب سایتها است.

با عرض پوزش از شما کاربر حرفه ای ، باید بگوییم افراد زیادی هستند که رمزعبور خود را همین کلمه «رمز عبور» یا معادل انگلیسی اش (password) قرار داده اند و برای همه رمزهای عبور خود از این کلمه استفاد میکنند.

کسانی هستند که از نرم افزار آنتی ویروسی آپدیت نشده ۲ ساله استفاده می کنند! اگر هر کسی متعهد به حافظت از داده های خود بود، هکرها مجبور به صرف زمان بسیار طولانی تر و شیوه های

پیچیده تری برای نفوذ بودند و خیلی از آنها هم از عهده چنین کارهایی بر نمی آمد. اما با وضعیت کنونی، به لطف اینکه بسیاری از مردم، غافل از آسیب پذیری خود هستند، برای هکرها نفوذ و حمله مانند بازی با اعداد آسان است.

در این پایان نامه ۱۰ روش موثر برای خنثی کردن تلاش هکرها شرح داده شده است که به طور خلاصه ذکر می گردد:

۱- نرم افزارها را به روز نگه دارید؛ همه نرم افزارها را

این یکی از ساده ترین راهها برای یکی دو گام جلوتر ایستادن از هکرها است.

با دانلود جدیدترین و به روز ترین بسته های آپدیت ویندوز، وردپرس و نسخه آنتی ویروس خود، می توانید سیستم یا وب سایت خود را در مقابل هر گونه حمله احتمالی به اندازه کافی سخت و نفوذ ناپذیر کنید. به این ترتیب ، هکرها هیچ وقت با حمله به چنین موردی خود را به زحمت نمی اندازند و ترجیح می دهند و به جای سایت شما به سایت های دیگر که مالک آن به هوشیاری شما نبوده است حمله کنند. در خط مقدم آن به روز کردن تمام وب اپلیکیشن ها ماژول ها و کامپوننت ها قرار دارد.

۲ -رمزهای عبور قوی و مطمئن انتخاب کنید

خب ، الان سال ۲۰۲۱ است. مدت ها از عمر وب می گذرد. الان دیگر زمانی نیست که شما رمز عبور خود را از نام همسر، اعداد تابلو ۱۲۳۴۵۶، یا کلمه مرگبار «password » انتخاب کنید. اگر چه ممکن است خیلی از ماها به این رمزهای عبور بخندیم و سری به نشانه تاسف تکان دهیم، اما این یک واقعیت شگفت آور است که مردم حتی زمانی مجبور به انتخاب کلمه عبور برای حساس ترین حساب های خود هم می شوند، تا حدودی سهل انگاری کرده و اسامی انتخاب می کنند که آسان کشف می شوند.

پس یادتان باشد رمزهای عبور قدرتمند(که به راحتی نشود کشفشان کرد) و متفاوتی، برای اطلاعات بانکی، ایمیل، CPanelسایت و کارت های اعتباری خود انتخاب کنید در غیر این صورت ، اطلاعات شما و سایت تان آسیب پذیر خواهد بود.

۳- permission -فایلهای سایت را محدود و قفل کنید

آیا می دانید پرمیشن دسترسی به فایل و پوشه ها روی چه عددی تنظیم شده؟ بعضی از برنامه برای نصب نیاز به تنظیم پرمیشن بر روی عدد «۷۷۷» دارند.

اما بیشتر ما فراموش می کنیم آنها را به عدد «۷۵۵» برای پوشه ها یا «۶۴۴» برای فایل های برگردانیم.

حتما یادتان باشد بررسی کنید تا اطمینان یابید که دسترسی ها برای برنامه هایی که ناشناس هستند قفل شده باشد.

۴ -به لینک ها دقت کنید

آیا واقعا می دانید به چه نوع سایت هایی لینک می دهید؟ برخی لینک ها به سایتی که به نظر می رسد ختم نمی شوند و کاربر را به آدرس دیگری می فرستند.

این یکی از دام های مهم هکرها برای حمله از طریق مرورگرهای مختلف به شمار می رود.

احتمالا می دانید زمانی که بر روی لینک خطرناک کلیک می کنید، چه اتفاقی می افتد. حالا تصور کنید زمانی که شما یک آدرس خطرناک را در سایت خود لینک می کنید، نتیجه چه خواهد بود .

بنابراین همیشه باید به هر سایتی که لینکی از ان را در سایت خود قرار می دهید اعتماد کامل داشته باشید.

۵ -برای ارسال ایمیل ها حتما از اس اس ال استفاده کنید

با توجه به وجود میلیون ها ایمیل غیر قابل اطمینان و خطرات مرتبط با آن، اگر مجبور هستید اطلاعات مهمی را از طریق ایمیل ارسال کنید، حداقل از این شیوه استفاده کنید.

۶ -از امنیت میزبان وب (Web Host) سایت خود با اجرای suPHP اطمینان حاصل کنید

در حال عادی زبان پی اچ پی ، اسکریپت ها معمولی اجرا می شوند و دسترسی به اسکریپت ها توسط «هر کسی» مجاز است، اما با استفاده ازsuPHP ، دسترسی به آنها محدود به کاربران مجاز خواهد بود .هنوز تمام میزبان ها از suPHP استفاده نمی کنند، بنابراین اطمینان یابید میزبان شما از ان استفاده کرده و سد بالقوه دیگری سر راه هکرها بگذارید!

۷ -در مورد میزبان ها (هاست ها)

زمانی که صحبت ازحصول اطمینان از امنیت وب سایت می شود، همه میزبان ها در این زمینه مانند هم نیستند و هر یک امکانات و محدودیت های خودشان رادارند.

همه آنها دارای امکان کنترل سرور فعال به صورت شبانه روزی ، و یا حتی(suPHP) به بالا رجوع کنید نیستند ، پس انتخاب یک میزبان که امنیت شما را جدی می گیرد و در این زمینه امکانات خوبی دارد کاملا ضروری است.

۸ -نگاهی به سرویس میزبانی مشترک

اگر وب سایت شما وسیله امرار معاش تان است ، پس ممکن است برای شما این تصور پیش بیاید که هیچ حدی از بحث امنیت رمز عبور نخواهد توانست باعث احساس امنیت شما شود. اگر سایت برای شما اهمیت حیاتی دارد و به خصوص کسب و کار شما به ان گره خورده است ، پس باید به سمت استفاده از سرور مجازی (VPS) بروید تا بتوانید با آرامش خاطر بیشتری از وب سایت خود استفاده نمایید.

سرور مجازی به علت جدایی از سایت های دیگر، ذاتا امن تر از هاست های معمولی است. شما می توانید روی آن فایروال را سفارشی کرده و به نصب تدابیر امنیتی دیگر که اکثر میزبان ها اجازه استفاده از آن را در هاست های معمولی نمی دهند، بپردازید. در واقع ، سرور مجازی اجازه می دهد تا شما نقش فعال تری در زمینه امنیت وب سایت خود ایفا کنید.

۹ -باید زرنگ بود! و حواستان به فایل های لاگ باشد

اگر دقیقا بدانید دنبال چه چیزی هستید، کار هکر را سخت تر کرده اید.

اکثر هکرها، اگر با سایتی روبه رو شوند که شدیدا محافظت می شود، به سرعت از خیر نفوذ به آن گذشته و راه خود را به سمت سایت های دیگر که روش های ساده تری برای هک شان وجود دارد کج می کنند.

به طور مرتب با کنترل فایل های لاگ (logfiles)کدهایی را که متعلق به سایت نیست شناسایی کنید، پلاگین های مشکوک و خطرساز را نصب نکنید، مواظب ورودهای غیرمجاز و ناشناس به بخشهای ویژه سایت تان باشید.

۱۰- همیشه از نرم افزار های به روز استفاده کنید اپدیت مداوم فراموش نشه.

۱۱ - سعی کنید به نکانت بالا اهمیت دهید و به آن عمل کنید.

این۱۱ راهنمایی، تنها مختصری از اصول امنیت سایت بود. در واقع آنها راه را برای فکر کردن عمیق روی تمام عواملی که می تواند در داشتن یک سایت امن به ما کمک کند باز می کنند.

اگر شما عادت کنید همواره مراقب همه چیز باشید و همه چیز را مرتب آپدیت کنید، انگاه به نسبت بسیاری از سایت های دیگر دنیای وب، هیچ جذابی برای هکرها نخواهید داشت.

فهرست منابع و مآخذ

منابع پارسی

۱. بهشتی، محمد تقی و سروی، معین،" رایانش ابری ساختارها و چالش ها " آبان ۱۳۹۱ اولین کارگاه ملی رایانش ابر در ایران دانشگاه صنعتی امیرکبیر

۲. ذبیحی،حامد و نیشابوری، عبدا...،پایان نامه کارشناسی،دانشگاه پیام نور سبزوار دی۹۱

۳. عرب، فاطمه و علی دوستی " استفاده از عامل های هوشمند با رایانش ابری در ایجاد امنیت "، اولین همایش منطقه ای کاربرد علوم برق و کامپیوتر در صنعت مخابرات،دانشگاه آزاد بندر گز آذر ۹۱

۴. کریم زاده، فاطمه و منتظری، محمد " ارائه ی روشی جدید برای ذخیره ی امن داده ها در ابر با استفاده از ترکیب رمزنگاری متقارن ونامتقارن و شاخص گذاری"

منابع خارجی

[۱] Mr. P. R Ubhale, Proff. A. M. Sahu, “Securing Cloud Computing Environment by means of Intrusion Detection and Prevention System (IDPS),” International Journal of Computer Science and Management Research, Vol. ۲, Issue ۵, May. ۲۰۱۳, pp. ۲۴۳۰-۲۴۳۴.

[۲] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande, “ Intrusion Detection System for Cloud Computing,” International Journal of Scientific & Technology Research Vol. ۱, May. ۲۰۱۲.

[۳] K. Panagiotis and K. Panagiotis, “Cloud Computing Learning,” IEEE,۲۰۱۱.

[۴] A. Bakhshi, and B. Yogesh ,” Securing cloud from DDOS Attacks using Intrusion Detection System in Virtual Machine,” Second International Conference on Communication Software and Networks, IEEE, ۲۰۱۰, pp. ۲۶۰-۲۶۴.

[۵] A. Mohammad sharifi, S. Amirgholipour, M. Alirezanejad, B. shakeri aski, and M. Ghiami, “Availability challenge of cloud system under DDOS attack,” Indian Journal of Science and Techology, Vol. ۵, No. ۶, June. ۲۰۱۲, pp. ۲۹۳۳-۲۹۳۷.

[۶] http://en.wikipedia.org/wiki/Denial-of-service_attack.

بسمه تعالی

فرم تایید و دریافت پایان نامه کاردانی رشته ☐کامپیوتر/ ☐ فن‌آوری اطلاعات

مشخصات دانشجو

نام و نام خانوادگی : **ابوالفضل خلفی** شماره دانشجویی : ۹۸۱۱۱۱۱۱۱۱۱۱ تاریخ دفاعیه : / /۱۴۰۰

عنوان پروژه :

امنیت در سرور های وب

سمت	تاریخ و امضاء
استاد راهنما : محمد مهدی باغستانی تایید نهایی پایان نامه از نظر محتوا و نگارش	
استاد مدعو : محمود شاهچراغی تایید نهایی پایان نامه از نظر محتوا و نگارش	
مسئول کتابخانه تایید فرمت کلی و رعایت دستورالعمل دریافت یک نسخه صحافی شده	
مدیر گروه آموزشی : محمد مهدی باغستانی تایید فرمت کلی و دستورالعمل	

تذکر : دانشجو موظف است طبق اولویت (از بالا به پایین) این فرم را به تایید برساند.