

نفوذ چیست؟

یک نفوذ به مجموعه ای از
فعالیت‌هایی گفته می‌شود که می
تواند موارد ذیل را از یک منبع
به خطر اندازد:

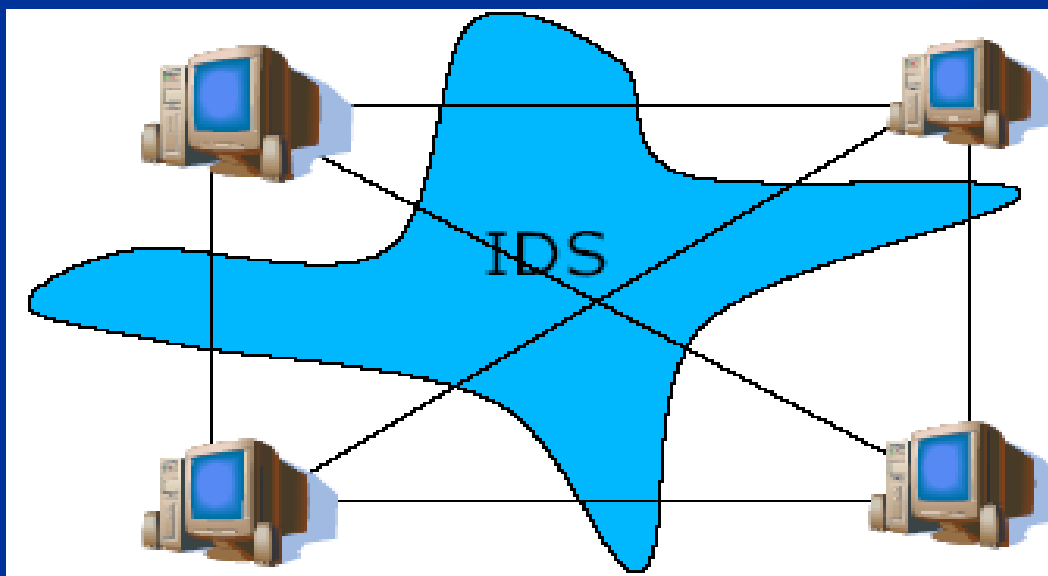
- یکپارچگی
- قابلیت اعتماد
- قابلیت استفاده و در دسترس بودن

نفوذگر کیست؟

- کارمند داخلی و خودی : در واقع شخصی که با در دست داشتن مجوز دسترسی از اختیار خود سوء استفاده می نماید
- Hacker : شخصی که با استفاده از لینکهای ارتباطی از قبیل اینترنت به شبکه داخلی سازمان نفوذ می کند.
- نرم افزارهای بداندیش: نرم افزارهایی از قبیل 'MalWare' ، 'Trojan Horse' و ویروسها که با اجرا شدن این نرم افزارها بر روی سیستم گونه ای از حمله و نفوذ علیه سیستم تلقی می گردد.

سیستم تشخیص نفوذ چیست؟

سیستم تشخیص نفوذ یا همان IDS در واقع سیستمی می باشد که قابلیت شناسایی حملات را بر روی سیستم های کامپیوتری دارا می باشد.



فعالیت های اساسی IDS

✓ استراق سمع کردن یا Monitoring :

جمع آوری اطلاعات از شبکه

✓ تحلیل نمودن یا Analyzing :

تصمیم گیری هر آنچه اتفاق می افتد.

گزارش دهی با Reporting :

تولید نتیجه و یا در غیر این صورت

فعالیت بر روی نتایج مرحله

Analyzing

شبکه اختصاصی مجازی (VPN)

یک VPN ، شبکه ای اختصاصی بوده که از اینترنت برای ارتباط با سایت های از راه دور و ارتباط کاربران با یکدیگر استفاده می نماید. این نوع شبکه ها بجای استفاده از خطوط واقعی نظیر خطوط Leased ، از یک ارتباط مجازی به کمک اینترنت برای ایجاد شبکه اختصاصی استفاده می کنند .

نکات مرتبط با کلمات عبور

اغلب کاربران کامپیوتر، به طور معمول از رمزهای عبور ساده و آسان استفاده می کنند. اما دقت داشته باشید که این سهل انگاری در انتخاب رمز عبور، عواقب خطرناکی به دنبال خواهد داشت. رمزهای عبور آسان و معمولی در ظرف چند ثانیه لو خواهند رفت و اطلاعات شخصی شما در سیستم مورد نظر به راحتی در معرض دید هکرها قرار خواهند گرفت. در ادامه تهدیدهای ممکن در این رابطه بررسی خواهند شد :

تهدیدهای مرتبط با کلمات عبور

: Passive Online Attacks □

در این روش هکرها از نرم افزار یا سخت افزارهای جاسوسی یا Snifferها استفاده میکنند. به این ترتیب که این نرم افزار یا سخت افزار با قرار گرفتن بر روی شبکه، اطلاعات در حال انتقال بر روی سیمها را Sniff کرده و برای هکر ارسال میکنند.

تهدیدهای مرتبط با کلمات عبور

■ Active Online Attacks :

این روش در واقع حدس زدن رمز کاربران است که روش تجربی و با توجه به فرهنگ و ذهنیات فرد است. به طور معمول کاربران از مبتدی تا حرفه‌ای سعی می‌کنند رمزی را برای خود در نظر بگیرند که به راحتی بتوانند آن را در خاطر نگهدارند. که همگی قابل حدس زدن می‌باشند را به عنوان رمز خود در نظر می‌گیرند. کاربران زرنکتر از ترکیب آنها استفاده می‌کنند که یافتن و حدس زدن آن کمی مشکل‌تر خواهد بود. هکرها نیز با توجه به این اصل که کارایی بسیاری نیز برای آنها دارد، ابتدا اطلاعات پرسنلی افراد را یافته و با آنها به حدس‌زنی رمز می‌پردازند.

تهدیدهای مرتبط با کلمات عبور

■ Offline Attacks :

در این روش از ابزاری برای یافتن رمز استفاده میشود. این ابزارها معمولاً بر دو نوع هستند:

الف - Dictionary Attack : ابزاری این روش، با کمک گرفتن از ذهن هکر، به یافتن رمز در کلمات لغتنامه میپردازند.

ب - Brute Force : در این روش نرم افزار ابتدا تعداد حروف رمز را با کمک هکر یا بدون کمک یافته و با استفاده از حروف و کلمات پیشنهادی هکر، به صورت منظم و یک به یک جایگزینی آنها، سعی در یافتن رمز میکند در این روش بدیهی است که انتخاب رمز مناسب و قوی میتواند به شکست این نرم افزار بیاچامد.

تهدیدهای مرتبط با کلمات عبور

■ Electronic Attacks :

در این روش از راه‌های غیر معمول و غیر کامپیوتری برای یافتن رمز دیگران استفاده می‌شود. برخی از این روش‌ها عبارتند از:

الف- نگاه کردن به کی‌بورد هنگام تایپ کاربر

ب- از پشت سر فرد نگاه کردن

ج- کاغذ فسفري: با دادن يك کاغذ مخصوص فسفري به کاربر بدون اینکه او متوجه شود، دستانش به فسفر آغشته شده، سپس بر روی کی‌بورد اثر کلماتی که تایپ می‌کند، برجای خواهد ماند.

د- مهندسي اجتماعي: هکرها اعتقاد بسیاری به این مهندسي دارند. در این روش با استفاده از فرهنگ، ذهنیات، کمبودهای روحی و ... افراد مختلف، اطلاعات مهمی را به دست می‌آورند.

تهدیدهای مرتبط با کلمات عبور

■ Key Loggers :

این نوع نرم افزارها با قراگیری بر روی یک سیستم، کلیه استفاده های کاربر از ماوس و کیبورد را ضبط کرده و برای هکر ایمیل می کند. در این روش حتما می بایست نرم افزار بر روی کامپیوتر شما نصب شود پس دقت کنید هیچ نرم افزاری را بدون شناسایی و نوع عملکرد بر روی کامپیوتر خود نصب نکنید.

تهدیدهای مرتبط با کلمات عبور

■ Fishing :

در این روش، صفحه‌ای مشابه یکی از سایت‌های معتبر جهان ساخته و برای شما ارسال می‌شود یا اینکه شما را تشویق به ثبت نام برای شرکت کردن در یک قرعه‌کشی بزرگ می‌کند و شما نیز بدون توجه، تمام اطلاعات خود را وارد می‌کنید. توجه داشته باشید حتی اگر این کار را انجام می‌دهید، از رمز ایمیل یا رمزهای مهم خود در این صفحات استفاده نکنید و به صفحاتی که از شما اطلاعات می‌خواهند به راحتی پاسخ ندهید.

راهکارهای امنیتی مرتبط با کلمات عبور

۱. به هیچ وجه از اسامی استفاده نکنید فرقی نمی کند که اسم فامیلتان باشد، یا باشگاه فوتبال مورد علاقه تان. بسیاری از برنامه های هکر، رمزهای عبور را با کمک فرهنگ لغت هک می کنند. فقط چند ساعت طول خواهد کشید که با کمک لغات یک فرهنگ لغت، دستیابی به رمز عبور امکان پذیر شود.

۲. برای رمز عبور خود حداقل از ۸ حرف استفاده کنید:

برای رمز عبوری که از ۴ حرف تشکیل شده است، حدود ۴۵۰۰۰ حالت وجود دارد. اما برای رمز عبوری که از ۸ حرف و علامتهای ویژه تشکیل شده است، یک میلیارد حالت مختلف وجود دارد!

راهکارهای امنیتی مرتبط با کلمات عبور

۳. برای رمز عبور، از حروفی که در کنار هم قرار گرفته اند استفاده نکنید! رمزهای عبوری مانند qwert یا asdf کار هکرها را برای دستیابی به رمز عبور بسیار آسان می کند، این مطلب در ترکیب اعداد نیز به همین صورت است؛ مثل " ۱۲۳۴۵۶۷۸ ".

۴. برای رمز عبور خود، ترکیبی از حروف بزرگ و کوچک یا اعداد و علامتهای ویژه را انتخاب کنید. استفاده از علامتهای ویژه به تنهایی کافی نیست. پنج درصد همه کاربرها بر این امر اتفاق نظر دارند که رمز عبوری حداقل یکی از کاراکترهای خاص (@=\$-% و ...) را دارا باشند. در این صورت نرم افزارهای Brute Force از یافتن رمز عاجز می شوند.

راهکارهای امنیتی مرتبط با کلمات عبور

۵. رمز عبور خود را تا حد امکان جایی ننویسید حتی اگر کاغذی که رمز عبور خود را بر روی آن نوشته اید، در جای امنی مانند کیف تان باشد، از این کار اجتناب کنید. عنوان کاغذی که رمز عبور خود را بر روی آن نوشته اید، به هیچ عنوان زیر صفحه کلید یا به مانیتور خود نچسبانید!

۶. رمز عبور خود را همواره تغییر دهید. هر قدر، مدت زمان استفاده از رمز عبورتان بیشتر باشد، خطر هک شدن شما بیشتر خواهد بود. اداره فناوری اطلاعات آلمان فدرال، توصیه می کند که هر ۹۰ روز یکبار رمز عبور خود را تغییر دهید.

راهکارهای امنیتی مرتبط با کلمات عبور

۷. رمز عبور خود را در کامپیوتر ذخیره نکنید!

کامپیوتر قادر است رمز عبور شما را ذخیره کند تا شما مجبور نباشید هر بار آن را وارد کنید.

۸. رمز عبور خود را به شخص دیگری ندهید!
اگر از شما تلفنی یا با ایمیل، رمز عبورتان را خواستند، آن را بازگو نکنید! هکرها معمولاً خود را به عنوان همکاران شرکتهای بزرگ معرفی می کنند.

هفت روش حرفه ای برای ایجاد رمز عبور

۱. برای ایجاد کلمه عبور، از حروف بزرگ و کوچک و به صورت یک در میان استفاده کنید. مثال:

cOmPuTeR

۲. حروف اول کلمات یک جمله را به عنوان رمز عبور خود انتخاب کنید.

مثلاً در جمله: "If sentence is longer password would be safer"

که رمز عبور آن به این صورت تبدیل می شود: "

Isilpwbs"

۳. عدد یا تاریخی را برای خود در نظر بگیرید و آن را با دکمه Shift تایپ کنید.

مثلاً: تاریخ: ۲۰۰۲, ۰۶, ۱۳ با دکمه Shift به این

کلمه تبدیل می شود: @((@<^(<#!

هفت روش حرفه ای برای ایجاد رمز عبور

۴. لغتی را در نظر بگیرید و سپس حروف سمت راست آن را که بر روی صفحه کلید قرار دارد، بنویسید:
مثال: Hardware تبدیل می شود به: Jstfestr
۵. لغت یا ترکیبی را برای خود در نظر بگیرید مانند "۲۴ Oktober" و بعد آن را بهم بریزید به این صورت که حروف اول آن را با حرف آخر، حرف دوم را با حرف ماقبل آخر و به همین ترتیب بقیه را بنویسید: ۲۴ r4eObkot
۶. لغات یک جمله را به اختصار بنویسید این اختصارات را خود شما تعیین می کنید و از قاعده خاصی پیروی نمی کنند. مثلاً عبارت White meat with cabbage تبدیل می شود به: "whtmtwtcabge"
۷. در رمز عبور از علائم ویژه استفاده کنید. مثال:
c/Om%ou\t\$E~"

نکات امنیتی مرتبط با مرورگرها

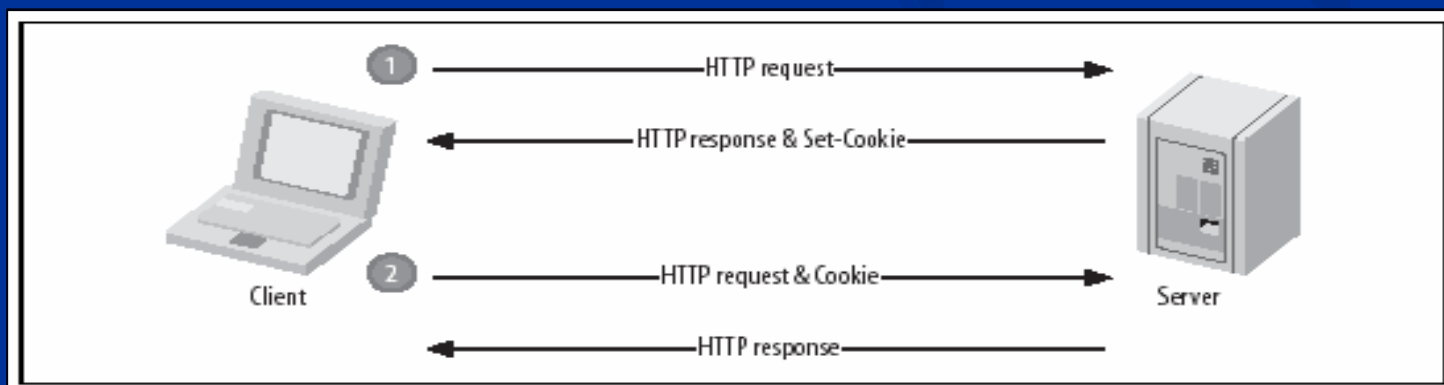
مرورگرهای وب ، اولین نقطه ارتباطی کاربران با اینترنت بوده و همین موضوع توجه جدی به آنان را مضاعف می نماید . بدیهی است وجود نقاط آسیب پذیر و یا عدم پیکربندی مناسب آنان، کاربران اینترنت را در معرض تهدیدات و حملات گسترده ای قرار خواهد داد .

با توجه به توسعه ی روزافزون وب و نیاز به تعاملی شدن هر چه بیشتر سایت های وب، استفاده از امکانات نشست ها و کوکیها در زبان PHP بیشتر می شود. از آنجایی که استفاده نامحاطانه از این امکانات و ویژگیها می تواند نقاط نفوذ بسیار مهمی را برای نفوذگران و مهاجمان سایت ها فراهم نماید. پروتکل HTTP پروتکلی فاقد حالت است، بدین معنا که در حرکت کاربر بین صفحات مختلف يك سایت وب و یا بین درخواست های متوالی، اطلاعات کاربر حفظ نمی شود و یا به عبارتی HTTP آن ها را به یاد نمی آورد.

نکات امنیتی مرتبط با مرورگرها

کوکی ها در حقیقت یکی از توسعه های پروتکل HTTP به شمار می روند. در استفاده از آن ها نیاز به دو سرآیند HTTP است :

۱- سرآیند پاسخ Set-Cookie ۲- سرآیند درخواست Cookie



نکات امنیتی مرتبط با مروگرها

با پیکربندی مناسب مروگرها ، می توان یک سطح مناسب امنیتی را ایجاد نمود. گرچه ممکن است به موازات افزایش سطح ایمنی ، امکان استفاده از برخی قابلیت های یک سایت بخصوص وجود نداشته باشد ، ولی شما در مقابل برخی از حملات محافظت شده و پیشگیری اولیه را انجام داده اید . برنامه های مروگر ، اولین نقطه ارتباطی شما با اینترنت می باشند و ممکن است چندین برنامه دیگر نیز به منظور ارائه خدمات و سرویس ها در ارتباط با آنان باشند و همین موضوع پیکربندی امنیتی مروگرها را مضاعف می نماید.

نکات امنیتی مرتبط با مرورگرها

تعداد زیادی از برنامه های وب با بکارگیری برخی از قابلیت های مرورگرها ، خدمات و سرویس های خاصی را در اختیار کاربران قرار می دهند .
رویکرد فوق علیرغم وجود برخی نکات مثبت، می تواند کاربران را مستعد انواع حملات نماید .
مطمئن ترین سیاست امنیتی ، غیرفعال نمودن اکثر ویژگی های ارائه شده همراه مرورگرها می باشد .
در صورتی که پس از غیرفعال نمودن برخی از ویژگی های مرورگرها در زمان استفاده از یک سایت تائید شده و مطمئن ، مشکلات خاصی ایجاد گردد ، می توان موقتا " آنان را فعال و پس از اتمام کار و استفاده از سایت مورد نظر ، مجددا " آنان را غیرفعال نمود .

نکات امنیتی مرتبط با مرورگرها

- علیرغم ارائه پتانسیل های مثبت توسط تکنولوژی های نظیر اکتیو ایکس و یا اسکریپت های فعال ، مهاجمان با استفاده از آنان قادر به نادیده گرفتن و یا دور زدن تنظیمات امنیتی سیستم می باشند .
- نقاط آسیب پذیر Spyware/Adware که تمامی مرورگرها و سیستم های را که از منابع موجود بر روی وب استفاده می نمایند ، تحت تاثیر قرار می دهد .
- تلفیق مرورگر IE با سیستم عامل باعث شده است که مشکلات IE به سیستم عامل ویندوز نیز سرایت نموده و بر نحوه عملکرد آن تاثیر منفی داشته باشد .

نکات امنیتی مرتبط با مروورگرها

مهاجمان با استفاده از نقاط آسیب پذیر
مروورگرها قادر به انجام عملیات متفاوتی می
باشند :

- افشای کوکی ها
- افشای فایل ها و داده های محلی
- اجرای برنامه های محلی
- دریافت و اجرای هرگونه کد دخواه
- در اختیار گرفتن کنترل کامل سیستم آسیب پذیر و
انجام هر گونه عملیات دخواه

نکات امنیتی مرتبط با مرورگرها

تنظیمات امنیتی در مرورگرها

این مسئله به نوع مرورگر وب بستگی داشته و هر یک از آنان امکانات خاصی را در اختیار استفاده کنندگان قرار می دهند . مثلاً " در مرورگر Internet Explorer، می توان پس از انتخاب منوی Tools گزینه Internet Options را انتخاب و در ادامه با کلیک بر روی Security tab و نهایتاً " دکمه Custom Level، سطح امنیتی مورد نظر را انتخاب نمود . در مرورگر Mozilla، پس از انتخاب منوی Edit می توان گزینه Preferences را انتخاب و با کلیک بر روی Privacy & Security، سطح امنیتی مورد نظر را تعریف نمود .

نکات امنیتی مرتبط با مرورگرها

مرورگرهای وب از اصطلاحات متفاوتی در
ارتباط با پیکربندی امنیتی استفاده می
نمایند :

Zones ✓

مرورگرهای وب، گزینه های مختلفی را به
منظور استقرار وب سایت ها در سگمنت ها
و یا نواحی متفاوت ارائه می نمایند . هر
ناحیه می تواند دارای تنظیمات امنیتی
مختص به خود باشد . مثلاً "مرورگر Internet
Explorer دارای نواحی زیر است :

نکات امنیتی مرتبط با مروگرها

□ Internet :

ناحیه فوق یک سگمنت عمومی و برای وب
سایت های عمومی است. در زمان استفاده
از اینترنت، تنظیمات تعریف شده برای
این ناحیه به صورت اتوماتیک در ارتباط
با سایت هائی که مشاهده می گردد،
اعمال خواهد شد. به منظور تامین بهترین
سطح حفاظتی و امنیتی مروگر، می
بایست این ناحیه دارای بالاترین سطح
امنیتی و یا حداقل سطح medium باشد.

نکات امنیتی مرتبط با مروگرها

□ Local Intranet :

در صورتی که سازمان شما دارای یک اینترانت است ، می توان از این ناحیه استفاده نمود . ناحیه فوق شامل تنظیمات امنیتی به منظور استفاده از صفحات داخلی است . با توجه به این که محتویات وب توسط یک سرویس دهنده وب داخلی مدیریت می گردد ، می توان محدودیت های به مراتب کمتری را در ارتباط با اینگونه از صفحات اعمال نمود .

نکات امنیتی مرتبط با مروگرها

Trusted Sites : □

در صورتی که برخی از سایت ها با رعایت مسائل امنیتی پیاده سازی شده باشند و تهدیدی از جانب آنان متوجه شما نمی باشد ، می توان آنان را در ناحیه فوق قرار داد . مثلاً " می توان سایت هایی را که با استفاده از تکنولوژی SSL پیاده سازی شده اند را در این ناحیه قرار داد ، چراکه همواره امکان شناسائی هویت سایت مورد نظر وجود خواهد داشت . سطح امنیتی این ناحیه ، می بایست بگونه ای تعریف شود که اگر سایت های مستقر در این ناحیه مورد تهاجم قرار گرفتند ، تهدیدی متوجه شما نباشد (پیشگیری از اختصاص یک سطح امنیتی پائین) .

نکات امنیتی مرتبط با مرورگرها

□ Restricted Sites :

در صورتی که وب سایت های خاصی وجود دارد که نسبت به غیرایمن بودن آنان اطمینان حاصل شده است ، می توان آنان را در این ناحیه قرار داد و برای آن بالاترین سطح امنیتی را تعریف نمود . با توجه به این که تنظیمات امنیتی برای حفاظت شما در مقابل اینگونه سایت ها به اندازه کافی مناسب نمی باشند ، بهترین گزینه عدم استفاده از سایت های غیرایمن است .

نکات امنیتی مرتبط با مروگرها

✓ جاوا اسکریپت

برخی وب سایت ها از زبان های اسکریپت نویسی نظیر جاوا اسکریپت به منظور ارائه قابلیت های خاصی استفاده می نمایند . از اسکریپت های فوق ممکن است به منظور انجام حملات متفاوتی استفاده گردد .

✓ کنترل های اکتیوایکس و جاوا

از برنامه های فوق به منظور اجرای محتویات فعال و ارائه برخی قابلیت ها در وب سایت ها استفاده می گردد . از این نوع برنامه ها همانند کدهای جاوا اسکریپت، ممکن است به منظور انجام حملات متفاوتی استفاده گردد .

نکات امنیتی مرتبط با مرورگرها

Plug-ins ✓

در برخی موارد مرورگرها به منظور ارائه خدمات ، نیازمند نصب نرم افزارهای اضافه ای با نام Plug-ins می باشند . از این نوع برنامه ها همانند کدهای جاوا اسکریپت ، کنترل های اکتیو ایکس و جاوا ، ممکن است به منظور انجام حملات متفاوتی استفاده گردد . بنابراین لازم است در زمان نصب اینگونه نرم افزارها از صحت عملکرد و اطمینان آنان اطمینان حاصل گردد . در صورتی که برنامه های فوق می بایست از طریق اینترنت دریافت و نصب گردند ، بررسی هویت سایت ارائه دهنده ، امری ضروری است .

فقدان امنیت در پست الکترونیکی

به طور کلی پست الکترونیکی ناامن است. در این مرحله، بسیار مهم است که ناامنی در مسیر تحویل پیام آشکار شده و بررسی شود:

□ Webmail : اگر اتصال به سرویس دهنده Webmail ناامن باشد در این صورت همه اطلاعات شامل کلمه عبور و نام کاربری به صورت رمز نشده بین سرویس دهنده Webmail و کامپیوتر کاربر ارسال می شود.

□ SMTP : SMTP پیام ها را رمز نمی کند (مگر این که از سرویس دهندگان درخواست شود تا از TTS پشتیبانی کنند.) ارتباطات بین سرویس دهندگان SMTP به صورت متن آشکار ۲ است که ممکن است پیام ها را برای هر استراق سمع کننده ای قابل رویت سازد.

فقدان امنیت در پست الکترونیکی

■IMAP-POP: در صورتی که POP و IMAP درخواست کلمه عبور و نام کاربری برای ورود کند؛ این اعتبار نامه ها رمز شده نیستند. بنابراین، اعتبارنامه ها و پیام ها ممکن است توسط استراق سمع کنندگان در جریان ارسال اطلاعات بین کامپیوتر کاربر و کامپیوتر فراهم کننده سرویس پست الکترونیکی شنود شوند.

■نسخه های پشتیبان: پیام ها در سرویس دهندگان SMTP به صورت متن آشکار و رمز نشده ذخیره می شوند. بر روی این سرویس دهندگان، نسخه های پشتیبان در هر زمانی ممکن است ساخته شوند و با این مکانیزم هر داده ای توسط مدیر قابل خواندن است. پیام های الکترونیکی که ارسال می شوند ممکن است به صورت ناخواسته یا نامحدود ذخیره شده و یا توسط

افراد ناشناس خوانده شوند.

تهدیدات امنیتی در ارتباطات پست الکترونیکی

در اینجا بسیاری از مشکلات امنیتی معمول در
رابطه با ارتباطات و پست الکترونیکی اشاره
میشود:

- ❑ استراق سمع
- ❑ سرقت هویت
- ❑ نقض حریم خصوصی
- ❑ تغییر و تبدیل در پیام ها
- ❑ ارسال پیام های جعلی
- ❑ تکرار پیام ها
- ❑ نسخه های پشتیبان محافظت نشده
- ❑ انکار

امن سازي پست الكترونيكي توسط SSL و TLS

ساده ترين راهي كه براي امن سازي پست الكترونيكي وجود دارد اين است كه از يك سرويس دهنده پست الكترونيكي استفاده شود كه از SSL براي سرويس دهندگان SMTP و IMAP، POP، Webmail پشتيباني مي كند.

TLS نيز يك نوع از SSL است كه مي تواند در طي يك نشست پست الكترونيكي راه اندازي شود. بر خلاف TLS، SSL بايد قبل از ارسال پست الكترونيكي راه اندازي شود.

SSL مركبي از مكانيزمهاي رمزگذاري متقارن و نامتقارن است.

نکات امنیتی مربوط با پست الکترونیکی

در نهایت چند توصیه را نیز همواره در ایمیل می بایست رعایت نمود:

- هیچگاه ایمیل کسی را که نمی-شناسید اصلا باز نکنید.
مخصوصا ایمیل-هایی را که جذاب به نظر می-رسند. چون ممکن است دچار حملات XSS شوید.

- هیچگاه هیچ برنامه-ای را که از ایمیل یا چت دریافت کرده-اید نصب یا اجرا نکنید. چون ممکن است Trojan روی سیستم شما نصب شده و تمام اطلاعات شما را بدزدد.

- فایل-های عکس و صوتی و تصویری و متنی (مانند pdf و doc) را تنها در صورتی که مطمئن هستید فرد آشنا و مطمئنی آن را برای شما فرستاده است باز و استفاده کنید. چون ممکن است توسط این فایل-ها Trojan روی سیستم شما نصب شود.

نکات امنیتی مربوط با پست الکترونیکی

امنیت ایمیل این روزها یک نیاز حیاتی محسوب شده و چیزی بیش از فیلترینگ ضد اسپم یا ضد ویروس را شامل می شود. کلاهبرداری های Phishing، کاربران سازمانی را تهدید به سرقت رمزهای عبور آنها می کند تا بتوانند به شبکه های سازمانی دسترسی یابند؛ سایر حملات، سرور میل را مستقیماً هدف قرار می دهند و تلاش خود را بر دستیابی به نام های کاربری یا آدرس های ایمیل معتبر یا دسترسی به سرور میل متمرکز می نمایند. این امکان وجود دارد که سازمان ها از جانب اشخاص حقیقی که ایمیل های مهاجم را از سوی کاربران شرکت دریافت می کنند یا حتی از جانب کارمندان خودشان که محتویات مهاجم را از سایر کارمندان یا منابع خارجی دریافت می کنند، تحت پیگرد قرار گیرند.

نکات امنیتی مربوط با پست الکترونیکی

شرکت ها همچنین با تهدید سرقت اسرار سازمانی یا دارایی های فکری- معنوی از طریق ایمیل مواجه می باشند. ابزارهای امنیت ایمیل از قبیل،

Series Mirapoint Message Server M-، IronPort C-Series

نه تنها می توانند با کوتاه کردن دست اسپم ها موجب صرفه جویی در وقت کاربران شوند، بلکه می توانند همه مسایل امنیتی دیگر را نیز مدنظر قرار دهند. این ابزارها در نسخه های متعدد قابل دستیابی هستند و برای سازمان های متوسط تا بزرگ با ۵۰۰ تا ۵۰۰۰ کاربر طراحی شده اند.

!