آسیب پذیری:

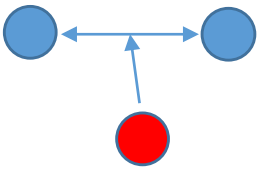
تهدید:

حمله: آسیب پذیری از حالت بالقوه به بلفعل

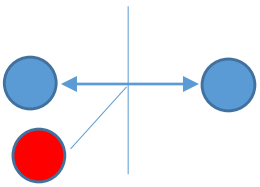
کنترل: هر اقدامی جهت جلوگیری از حمله انجام شود – تغییر رمز اجباری، گیت های ورودی، اثر انگشت، و ...

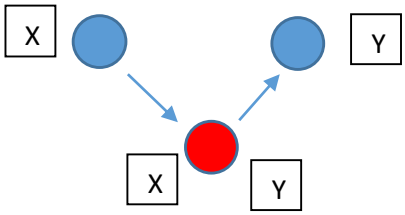
انواع حملات پایه:

۱. شنود



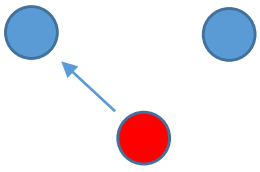
۲. وقفه: سدی ایجاد شود.

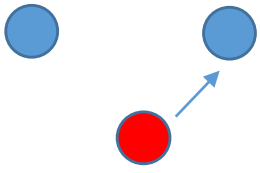




۳.دستکاری: داده ها تغییر کرده و به مقصد می رسد.

۴. جعل: مبدا یا مقصد جعلی هستند.





نفوذگر:

فردی هست که روش، فرصت و انگیزه داشته باشد.

روش: دانش و مهارت و ابزارها

فرصت: زمان طلایی در جایی که بتواند از سیستم سوء استفاده کند.

انگیزه لازم: انرژی و زمان بگذارد.

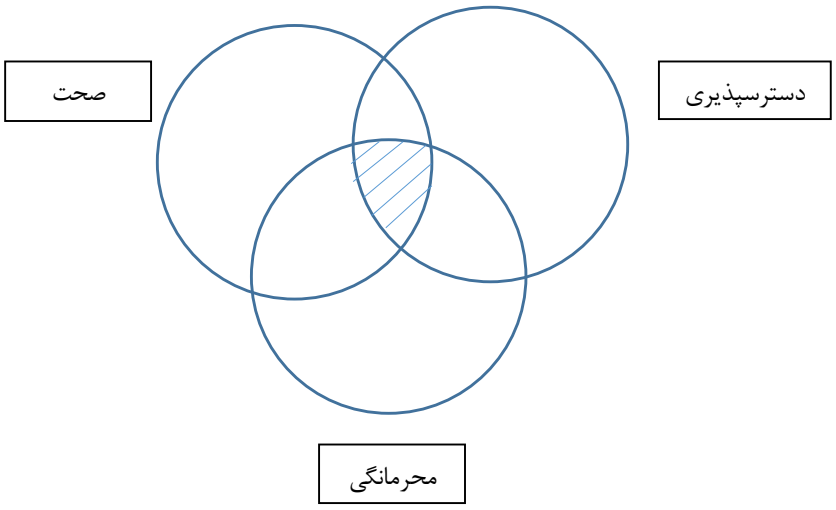
مثال: کارمند ناراضی، چون دسترسی دارد و سیستم را هم می شناسد و انگیزه هم بیشتر باشد حتما نفوذگر خواهد بود.

اهداف امنیت: (ابعاد، وجوه)

۱. صحت: درستی داده ها نقض نشود. (حمله دستکاری)

۲. محرمانگی: داده ها محرمانه باشند. (نفوذ)

۳. دسترس پذیری: موجودیت مجاز در شرایط و زمان مجاز باید دسترسی اش به سیستم فراهم باشد. (وقفه)



قسمت هاشور خورده امنیت مطلق محسوب می شود.

برای ایجاد امنیت مطلق باید لایه بندی داشته باشیم.

صحت و محرمانگی

دسترس پذیری و محرمانگی

صحت

تعداد حملات به صورت زیر محاسبه می شود. ۳ محیط داریم و ۴ حالت حمله داریم که از ضرب این دو مورد عدد ۱۲ بدست خواهد آمد.

آسیب پذیری:

آسیب پذیری های سخت افزاری:

۱. رطوبت ۲. آتش سوزی ۳. کابل های نوری و ... موش ها می خوردند. ۴. دود دما با دود بسیار بالا خواهد رفت.

آسیب پذیری های نرم افزاری:

۱.حذف: یکی غیر ارادی است و غیر آگاهانه است. یک گروه دیگر حذف ها هستند که با هدف ارتقاء نرم افزار نگارش قبلی را حذف می کنیم.

الف) نرم افزارهای امنیتی را بخواهیم بدون مشکل حذف کنیم، یک راهکار هست که اتصال به اینترنت و پورت های ورودی و خروجی را حذف کنیم. روش دیگر هم استفاده از نرم افزارهای پیکره بندی است که دو نگارش را داشته باشیم و بعد از مطمئن شدن از اجرای صحیح نگارش جدید نگارش قدیمی را حذف می کنیم.

ب) نرم افزارهای کاربردی را اگر بخواهیم حذف کنیم، از نظر امنیتی زیاد مشکلی وجود ندارد اما در حالتی که بخواهیم نگارش جدیدی را نصب کنیم، اینجا بحث اعتماد پیش خواهد آمد. اینجا هم نرم افزارهای پیکره بندی به کار خواهد آمد. می توان هر دو نگارش را در کنار هم داشته باشیم و بعد از مدت زمان مشخص و استفاده از نگارش جدید و ثبت کلیه موارد امنیتی و تست آن ها می توانیم نگارش قبلی را حذف کنیم.

نرم افزارهای پیکره بندی:

این نرم افزارها از روش Sandboxing استفاده می کنند. در واقع نرم افزارها در حالت خاصی که ایزوله شده هستند نصب و راه اندازی خواهند شد تا مدت زمانی که کاربر مطمئن شود که مشکل امنیتی وجود ندارد.

۲.دستکاری:

۲,۱ – هدف تخریب نرم افزار خواهد بود.

۲,۲ – نرم افزار را در شرایط خاصی خراب شود. بر اساس زمان یا یک مرحله از نرم افزار کارایی آن مشکل دار شود.

۲,۳ – تزریق ویژگی ها، در این حالت یک سری موارد به نرم افزار اضافه می شود. به عنوان مثال ارسال اطلاعات مالی یک شرکت برای یک ایمیل خاص.

سایر موارد: ویروس ها، تروجان ها، بازکنندگان پورت و ...

۳.سرقت: نقض قوانین کپی رایت

آسیب پذیری داده ها:

داده ها ارزشمندترین موضوع در سازمان ها است زیرا سخت افزار و نرم افزار به مرور زمان از ارزششان کم خواهد شد ولی داده ها بر عکس با گذشت زمان ارزشمندتر خواهند شد.

داده ها برای اکثر آدم ها قابل فهم هستند. ولی سخت افزار و نرم افزار این طور نیست و نیاز به متخصص دارد برای استفاده از این اطلاعات که کمتر اتفاق خواهد افتاد.

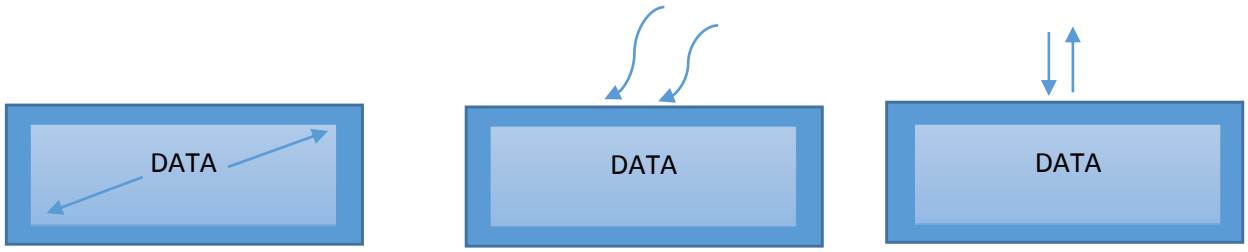
اصول امنیتی:

۲. **اصل کافی بودن محافظت:** موجودیت های کامپیوتری تا زمانی که ارزش دارند باید از آن ها محافظت شوند.

Asset ها: دارایی های امنیتی را به آن Asset گفته می شود. هر موجودیتی که امنیت را برای آن بررسی می کنیم به آن Asset امنیتی می گوییم. بر اساس ارزش و طول عمر امنیت تعیین می شود.

مثال: اسناد مالی سال ۸۳ کل کشور در سال ۱۳۹۴ خیلی نیاز به امنیت ندارند. در این سیستم صحت کامل برقرار است و شاید در نهایت محرمانگی مورد نیاز باشد.

آسیب پذیری داده ها:



دسترس پذیری　　صحت　　محرمانگی

حمله پردازش مجدد داده های پردازش شده: (حمله تکرار) Replay Attack

مانند ارسال چند باره رمز کارت شارژ تلفن همراه اکه از روش Timestamp استفاده می شود برای جلوگیری از این حمله و علت آن خاص بودن عدد تولیدی توسط Timestamp می باشد.

لاگین شدن مثال دیگری است که می توان از این دسته در نظر گرفت. پیام کامل لاگین ذخیره می شود و برای ورود می توانیم از آن استفاده کنیم.