به نام خدا

جزوه درس

حریم خصوصی و امنیت شبکه

(Privacy and Security)

مدرس

سرکار خانم پریسا خیاط

تهیه کننده:

امیرحسین حسینی

بهار ۹۴

مقدمه

امنیت ، مبحثی کاملا پیچیده ولی با اصولی ساده است . در بسیاری از مواقع همین سادگی اصول هستند که ما را دچار گمراهی می کنند و دور نمای فعالیت های ما را از لحاظ سهولت و اطمینان در سایه ای از ابهام فرو می برند. باید گفت که امنیت یک پردازش چند لایه است. تعیین نوع و نحوه تلقین لایه های دفاعی مورد نیاز ، فقط پس از تکمیل ارزیابی قابل ارائه است . تهیه لیستی از سیاست های اجرایی بر مبنای اینکه چه چیزی برای سازمان مهم تر و انجام آن ساده تر است در اولویت قرار دارد. پس از آنکه این اولویت ها به تایید رسیدند هر یک از آنها باید به سرعت در جای خود به اجرا گذارده شود. ارزیابی امنیتی یک بخش بسیار مهم تراز برنامه ریزی امنیتی است. بدون ارزیابی از مخاطرات ، هیچ طرح اجرایی در جای خود به درستی قرار نمی گیرد. ارزیابی امنیتی خطوط اصلی را برای پیاده سازی طرح امنیتی که به منظور حفاظت از دارایی ها در مقابل تهدیدات است را مشخص میکند.
برای اصلاح امنیت یک سیستم و محقق کردن شرایط ایمن، می بایست به سه سوال اصلی پاسخ داد:
چه منابع و دارایی هایی در سازمان احتیاج به حفاظت دارند؟
چه تهدیداتی برای هر یک از این منابع وجود دارد؟
سازمان چه مقدار تلاش ،وقت و سرمایه می بایست صرف کند تا خود را در مقابل این تهدیدات محافظت کند؟
اگر شما نمی دانید علیه چه چیزی می خواهید از دارایی های خود محافظت کنید موفق به انجام این کار نمی شوید. رایانه ها محتاج آن هستند که در مقابل خطرات از آنها حفاظت شود ولی این خطرات کدامند؟ به عبارت ساده تر خطر زمانی قابل درک است که یک تهدید، از نقاط ضعف موجود برای آسیب زدن به سیستم استفاده کند. لذا، پس از آنکه خطرات شناخته شدند، می توان طرح ها و روش هایی را برای مقابله با تهدیدات و کاهش میزان آسیب پذیری آنها ایجاد کرد. اصولا شرکت ها و سازمان ها ، پویا و در حال تغییر هستند و لذا طرح امنیتی به طور مدام باید به روز شود. به علاوه هر زمان که تعییرات عمده ای در ساختار و یا عملکردها به وجود آمد، می بایست ارزیابی مجددی صورت گیرد. بنابراین حتی زمانی که یک سازمان به ساختمان جدیدی نقل مکان می کند، کلیه دستگاه های جدید و هرآنچه که تحت تغییرات اساسی قرار می گیرد، مجددا باید مورد ارزیابی قرار گیرد.

عناوین درس:

۱. مروری بر لایه های شبکه(OSI,TCP/IP)
۲. مبانی امنیت شبکه
۳. نمونه هایی از تهدیدات و حملات متداول و آشنایی با روش های مقابله
۴. مدیریت ایمن و ایمنی در شبکه
۵. پروتکل های ایمن

لایه های OSI

لایه فیزیکی: همان کانالی است که اطلاعات در آن منتقل می شود جهت انتقال اطلاعات از کابل مسی،فیبر نوری و... استفاده کرد.
نکاتی در رابطه با چگونگی انتقال بیت روی کانال، وضعیت آنها، نوع کابل بندی شبکه، سیگنال های الکتریکی و... دراین لایه مطرح می شوند.

لایه پیوند داده: مهمترین وظیفه آن برقراری ارتباط بدون خطا است، استفاده از مکانیزم هایی چون **Check sums parity,CRC code** درلایه به کاربرده می شود.

وظایف:

- شکستن داده به فریم با الگوی خاص
- اتصال سخت افزاری بین لایه، لایه پایین تر(لایه فیزیکی)
- کنترل جریان فریم ها

لایه شبکه: هدف این لایه مسیریابی است و از مکانیزم بدون اتصال برای ارتباطات استفاده میکند یعنی بسته های اطلاعاتی بصورت مجزا از هم ارسال می شوند و در مقصد دریافت می شوند. مهمترین وظیفه این لایه فراهم آوردن آدرس های شبکه و مکانیزم های آدرس دهی، مسیریابی بسته های اطلاعاتی در شبکه و کنترل شلوغی و تغییر آدرس در شبکه هایی که نوع شبکه تغییر می کند می باشد.

لایه انتقال: ایجاد بسته های کوچکتر و ارسال آن به صورت مکانیزم اتصال گرا.

وظایف:

- تضمین دریافت صحیح اطلاعات به گیرنده
- مرتب سازی داده ها
- بررسی Time outو کنترل جریان داده

لایه جلسه: برپا سازی جلسات بین ماشین ها و مدیریت جلسه (مدیریت **Token**) یعنی استفاده از منابع مشترک و نوبت بندی در استفاده ار آنها.

وظایف:

- کنترل دیالوگ یعنی کدام طرف در یک ارتباط Half Duplex میتواند داده ارسال و دریافت کند.

لایه نمایش: وظیفه اصلی این لایه نمایش داده هاست.

وظایف:

- فشرده سازی اطلاعات(کد های اسکی یا فرمت های مختلف تصویری و رمزکردن اطلاعات در این لایه صورت می گیرد.

لایه کاربرد: انواع سرویس هایی که استفاده می شود مخصوص این لایه است.

این سرویس ها عبارتند از:

SMTP
POP3
HTTP
FTP
JMAP
و ...

TCP/IP

Massage	APP	Data	24 بایت		
Packet	TCP	Data	TCP Heder	24 بایت	
Datagram	IP	Data	TCP Heder	IP Heder	24 بایت
Frame	Physical	Data	TCP Heder	IP Heder	Physical Heder

ریسک های شبکه:

۱. لو رفتن اطلاعات
۲. آسیب زدن به اطلاعات
۳. DOS(Deny Of Service)
۴. جنگ اطلاعاتی یا سایبری

سه هدف اصلی ایمنی CIA:

۱. **محرمانگی:** یعنی اطلاعات بدون آنکه کسی ببیند به مقصد انتقال دهیم.
۲. **صحت:** یعنی اطلاعاتی را که ارسال می کنیم در طرف مقابل بدون آنکه چیزی از آن حذف ویا اضافه شود تغییر داده شود دریافت کنیم.
۳. **دسترسی:** یعنی اطلاعاتی که قرار است در اختیار افراد مجاز قرار بگیرد همیشه در دسترس آن باشد.

دلایل آسیب پذیری:

- ضعف در طراحی
- ضعف در پیاده سازی
- ضعف در مدیریت

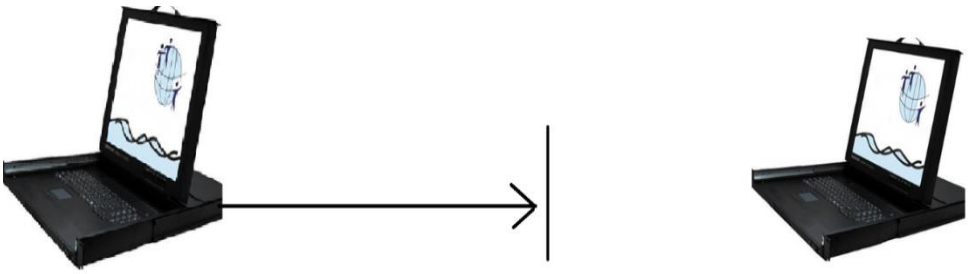
طیف های تهدید:

۱. تهدیدات محلی
۲. تهدیدات مشترک
۳. تهدیدات امنیت ملی

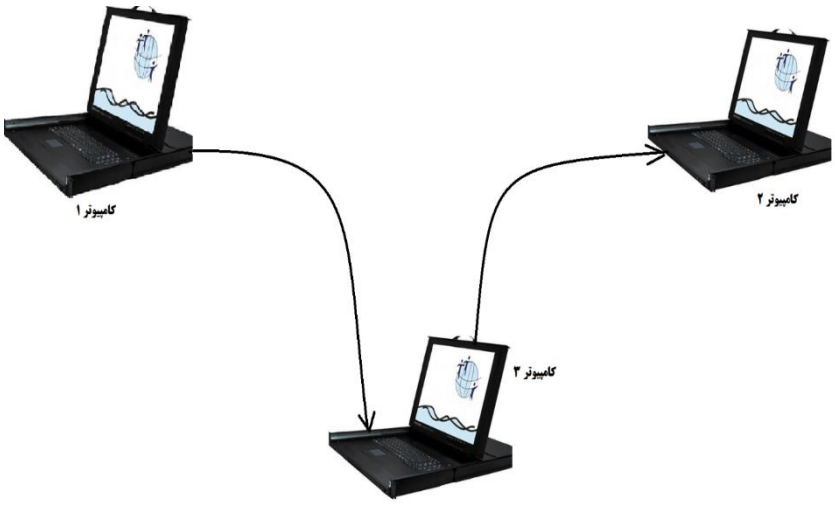
تهدیدات:

- عمدی
  - فعال
  - غیر فعال
- تصادفی

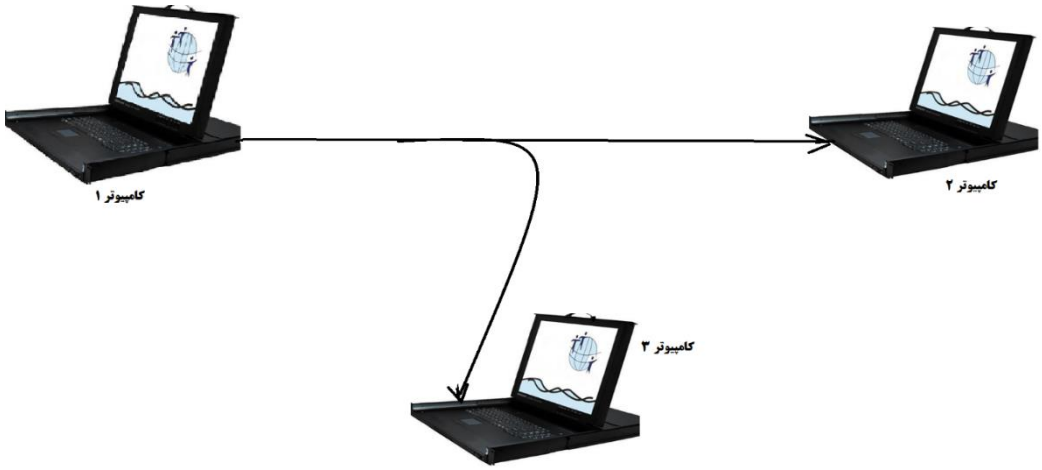
مدل برای توصیف حملات:



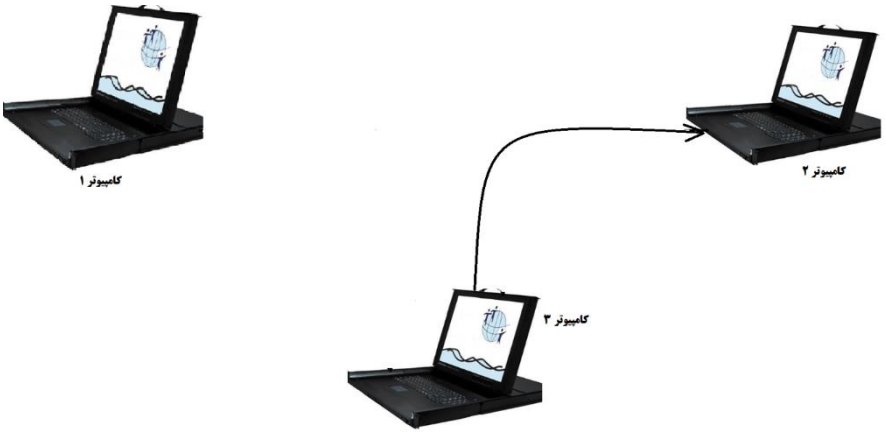
Interception قطع دائم



Modifiction تغییر دادن



Interception **کپی برداری**



Fabrication **جعل کردن**

تهدید: **هر پدیده ای که خطری را در رابطه با اهداف ایمنی شبکه(محرمانگی، صحت و دسترسی) اعمال کند.**

سرویس های مربوط به ایمنی(پنج دسته اصلی):

1. **سرویس های اعتبار سنجی یا احراز هویت**
2. **سرویس های کنترل دستیابی**
3. **سرویس های محرمانگی اطلاعات**
4. **سرویس های صحت داده ها**
5. **عدم رد سرویس**

سرویس اعتبار سنجی یا احراز هویت:

یعنی آیا طرف مقابل همانیکه ادعا می کند هست یا نه؟

یعنی آیا این بسته ای که فرستاده شده است، از نظر هویت فرستنده یل چیزی که ادعا می کند(می شود) یکی هست یا نه؟

Entity Authentication: تعیین هویت و اصلیت کاربر با هویت ادع شده که در زمان های مشخص مثل شروع یا در هنگام ارتباط بررسی می شود.

Origin Authentication: تعیین مبداء داده است مشخص می کند که کسی این اطلاعات را تولید کرده کیست.

سرویس های کنترل دستیابی:

جلوی دسترسی های غیر مجاز را می گیرد انواع دسترسی های غیر مجاز که می تواند وجود داشته باشد مثل خواندن، نوشتن منابع پردازشی.

سرویس های محرمانگی اطلاعات:

اگر همان اطلاعات فرستاده شده تولید گردد، یعنی اطلاعات ارسال شده، همان اطلاعات فرستاده شده است چون هیچ کس نمی تواند در طول مسیر هم متن و هم محتویات دنباله را تغییر دهد بطوریکه باز هم با هم تطبیق داشته باشد.

سرویس های صحت داده:

زمانیکه اطلاعات در طرف مقابل دریافت می شود و صحت اطلاعات مورد بررسی قرار میگیرد، در بعضی موارد اطلاعات ترمیم و بازیابی می شود.

سرویس های عدم رد سرویس:

- عدم انکار مبداء
- عدم انکار تحویل

عدم انکار مبداء: سرویسی که مبداء ارسال کننده اطلاعات، نتواند ارسال اطلاعات را انکار کند یعنی گیرنده نشانه ای از فرستنده داشته باشد که نشان دهد این اطلاعات از او بوده است.

عدم انکار تحویل: هیچ گیرنده ای نتئاند دریافت اطلاعات را انکار کند.

فهرست پیام های ICMP:

Datination Host Unreaohable: یعنی بسته ی قبلی که ارسال شده است نتوانسته مقصدش را پیدا کند.

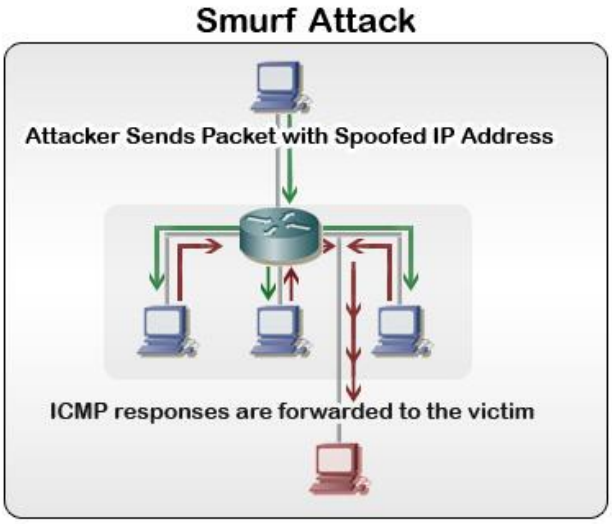
Time Exceeded: یعنی بسته ی قبلی که ارسال شده نتوانسته مقصدش را پیدا کند. یعنی بسته مدت زمان طولانی در شبکه بوده و عمر آن سرآمده است. (TTL=0)

- **Parameter Problem:** یعنی که یکی از فیلد های بسته IP، اشتباه یا بی معنا بوده است.

هدف از دستور Ping:

با استفاده از این پیغام، وجود یا عدم وجود ماشینی(سیستمی) در شبکه کشخص می شود.

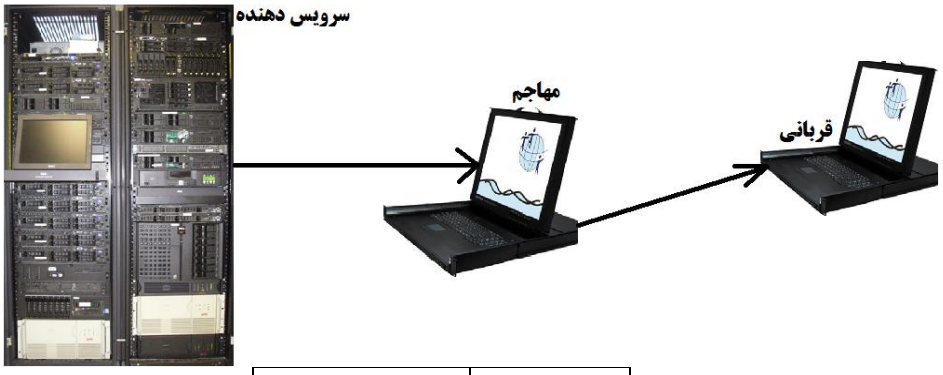
Smurfing: حمله ای است که بر اساس پروتکل ICMP صورت می گیردو بیشتر با نام Ping شناخته می شود.



دراین نوع حملات مهاجم اقدام به ارسال بسته های اطلاعاتی Ping به آدرس های Broad Cast شبکه نمود که در آنان آدرس مبداء هر یک بسته های اطلاعاتی Pingشده با آدرس کامپیوتر قربانی جایگزین می شود. به این ترتیب یک ترافیک کاذب در شبکه ایجاد و امکان استفاده از منابع شبکه با اختلال مواجه می شود.

MAC	IP
3D-4F-1D-5A	192.168.25.11
APR Cache	

جدول صحیح



MAC	IP
MACهکر	192.168.25.11
APR Cache	

جدول غلط (هک شده)

حمله بوسیله پروتکل APR:

باتغییر جدول APR Cache می توان تطابق بین آدرس های MAC وآدرس های IP که آدرس های فیزیکی هستند را تغییر داده بنابراین با اینکه آدرس IP بسته های ارسالی درست است، ولی با ایجاد تغییر در جدول آدرس ها به مقصد اشتباه فرستاده می شوند سپس مهاجم اطلاعات تغییر یافته را به آدرس گیرنده می فرستد، ولی تطابق آدرس ها در جدول طوری است که

آدرس IP فرستنده اصلی است به این ترتیب مهاجم بدون ایجاد تغییر در کارهای شبکه و رفتار هر یک از عناصر شبکه با تغییر اطلاعات جدول آدرس ها باعث ایجاد تغییر در بسته های ارسالی یک فرستنده می شود.

سرآیند TCP

پورت مقصد	**پورت مبداء**	ACK	Seq Num	…

سرآیندIP

پورت مقصد	**پورت مبداء**	TTL

دیواره آتش(Fire Wall):

- TCP
- IP
- Application

دیواره آتش در لایه IP:

سرآیند بسته IP بررسی می شود و بر اساس ویژگی های سرآیند بسته IP از قبیل آدرس مبداء یا آدرس ماشین فرستنده آدرس مقصد، شماره پورت، TTL در زمان حیات بسته دیواره آتش درمورد حذف شدن یا نشدن آن تصمیم می گیرد.

دیواره آتش در لایه TCP:

تصمیم گیری بر اساس ویژگی های لایه انتقال است سرآیند بسته انتقال شامل ویژگی های، شماره پورت مبداء، شماره پورت مقصد، فیلد Seq Num،ASK Num، می باشد دیواره آتش بر اساس همین ویژگی ها اجازه ورود بسته را می دهد مهمترین کار این مرحله بستن پورت های خاص می باشد.

دیواره آتش هوشمند(Fire Wall Sagacious):

این دیواره آتش، براساس قواعدی که بر اساس تاریخچه عمل می کنند، تصمیم گیری می کند.

نکته:دیواره های آتش هوشمند،در مرحله اول نیاز به حافظه و در مرحله بعد نیاز به محاسبات دارند.

دیواره آتش مبتنی بر Proxy:

Proxy به جای گره های اصلی در شبکه بسته ها را دریافت و ارسال می کند.

به زبانی ساده تر Proxy ها واسطی هستند بین گره هایی که در Subnetوجود دارد، جهت برقراری ارتباط با کل شبکه.

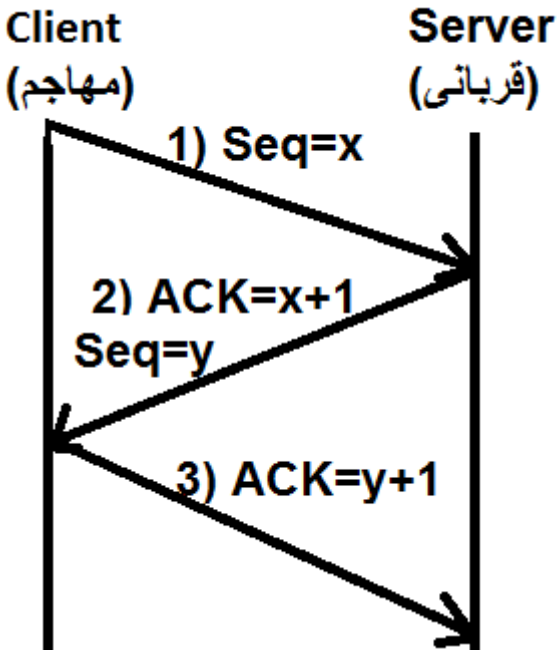
دیواره آتش مبتنی بر Proxyعلاوه بر اینکه مانند یک Fire Wall عمل می کنند هیچ ارتباط مستقیمی بین طرف اول ارتباط و گره های داخلی وجود نخواهد داشت.

ماشین های دیواره ی آتش مبتنی برProxy بسته هایی را که دریافت می کنند به سمت شبکه داخلی ارسال نمی کنند بلکه همان جا نشست را خاتمه می دهند و سپس نشست دیگری را بین خودشان و ماشین های داخلی ایجاد می کنند. بنابراین ارتباط مستقیمی بین ماشین های داخلی و مهاجم برقرار نخواهد شد که این به جلوگیری از حملاتی که ممکن است با دور زدن Fire Wall طراحی شوند کمک می کند.

***بسیاری از اطلاعات دریافتی از کاربران شبکه ویا اشتباهاتی که در ارسال و دریافت اطلاعات ممکن است رخ دهد صورت می گیرد.**

بدین منظور:

۱. عدم پاسخ به سوالاتی که لزوم به پاسخ دهی آنها نیست و دادن پاسخ سربسته به سوالات.
۲. عدم دسترسی فیزیکی افراد غیر مسئول به مکان هایی که ارتباطی به آنها ندارد.
۳. برخی از اطلاعاتی که داریم نظیر دیسکت های BackUp که معمولا برای بازیابی از آنها استفاده می شود، باید جایی نگهداری شود که کسی به آنها دسترسی نداشته باشد.
۴. پیش بینی کنار رفتن کاربران از سیستم و بازماندن برنامه هایی که روی سیستم مربوطه در حال اجرا بوده است.
۵. پیشگیری از دور ریختن اطلاعاتی که زمانی مفید بوده اند.
۶. جهت تعیین پورت های باز یا بسته روی ماشین فعال باید از امکانات لایه انتقال یا TCP استفاده کرد.



۱. بسته جهت همزمانی ارسال می گردد. Seq Num با عددی به طور تصادفی مقدار می گیرد.

۲. این بسته، بسته ACK است که در مرحله برپاسازی ارتباط ارسال می گردد. Seq Num با عدد دیگری به طور تصادفی مقدار می گیرد.

۳. بسته ی ACK ارسال می شود.

روش های تعیین پورت باز:

۱. **پویش مودبانه:** در بسته های **TCP** که ارسال می شود،**Seq Num** و شماره پورت مبداء و مقصد جهت بررسی باز یا بسته بودن پورت، بسته **TCP** را اجرا کرده و ارسال می کند ،سعی میکند ارتباط را برقرار سازد. در صورتیکه از طرف مقابل پاسخی مبنی بر برقراری ارتباط داده شود، مهاجم تشخیص می دهد که پورت باز است و در صورتیکه پیامی که از طرف مقابل بر میگردد نشان دهنده بسته بودن پورت باشد(یعنی **Code Bit** مربوط به **Set،Reset** خواهد شد)در نتیجه مهاجم تشخیص می دهد که پورت بسته است، برای ختم ارتباط **TCP** باید از طرف یکی از طرفین بسته اضافه شود که در آن **Code Bit** مربوطه به تمام شدن ارتباط یک شده باشد. بنابراین پس از برقراری ارتباط و تعیین باز یا بسته بودن پورت، بسته دیگری جهت ختم ارتباط ارسال می شود.

اشکالات این روش:

a. وقت گیر است.
b. بعضی از سرور ها Log گیری می کنند و این باعث می شود که مهاجم شناسایی شود.

۲. **پویش مخفیانه:** پس از ارسال **ACK**از طرف سرور، پویشگر بسته، بسته ی **Reset** را ارسال میکند. بدلیل نبودن مرحله ختم کردن و حذف کردن یکی از مراحل در زمان صرفه جویی می شود.

۳. **نقص اصول پروتکل:** در این نوع پویش ها با ارسال بسته های غیر متعارف و بررسی کردن پاسخ تشخیص داده شود که پورتی باز است یا بسته. معمولا پورتی که بسته است در پاسخ به بسته ای که جهت برقراری ارتباط ارسال می کند که کد بیت **Reset** در آن به یک مقدار گرفته باشد.

IDS یا سیستم تشخیص نفوذ:

سیستم هایی هستند که بر اساس Log File ها یا History می توانند تشخیص بدهند که نفوذی در حال رخ دادن می باشد یعنی با تفسیر اطلاعات و انجام مقایسه می توانند تشخیص دهند که اتفاقی رخ می دهد. مثلا با مقایسه ترافیک موجود با ترافیک در حالتی که حمله رخ نداده است می توتند به این نتیجه برسد که خطری در حال تهدید شبکه است.

تفاوت IDS با Fire Wall:

Fire Wall با استفاده از یک سری قواعد ثابت تصمیم می گیرند بسته ها را عبور بدهند یا نه ولی IDS به صورت پویا و بر اساس اطلاعاتی که در طول زمان تولید می شود نفوذ در حال انجام را تشخیص می دهد.
IDS می تواند طول داده هایی که به پورت باز ارسال می شود را کنترل کند.

حملات لایه کاربردی:

۱. **Malware:** به برنامه هایی گفته می شود که در لایه کاربردی در ظاهری زیبا قرار می گیرند، ولی اهداف مهاجم را دنبال می کنند گفته می شود. (گفته می شود که **Malware**ها از نرم افزار های بد خواه(**Mali cious**)و نرم افزار هایی که مخرب هستند می باشد.)
Malware به دو گروه تقسیم می شوند:

- انواعی از برنامه ها که برای تکثیر، اجرا و انتشار و ورود شان نیاز به یک برنامه میزبان دارد.
- انواعی از برنامه که مستقل هستند و نیاز به یک برنامه میزبان ندارد.

۲. **اسب تروا(Trojan):** برنامه ای بصورت مستقل و مانند یک برنامه معمولی بر روی کامپیوتر قربانی نصب شده و اجرا می گردد و ماشین قربانی قرار گرفته و آن را در اختیار مهاجم قرار می دهد.

۳. **ویروس ها(Virus):** نیاز به یک برنامه میزبان دارند و هدف آنها تکثیر کردن خودشان است. البته در اسب منظور از اینکه خود را تکثیر نمی کنند این نیست که از سیستمی یه سیستمی دیگر انتقال نمی یابند ولی هدف ویروس ها تکثیر بر روی ماشین تکی می باشد.

۴. **کرم ها(Worms):** به صورت خودکار منتشر می شوند و بسترشان شبکه است.

۵. **درب پشتی (Back Door):** یا در سیستم وجود دارند و یا به صورت نرم افزاری نصب می شوند که وقتی روی سیستم نصب می شوند به مهاجم اجازه می دهند که بدون شناسه و رمز احراز هویت شوند و بتوانند به سیستم قربانی دسترسی داشته باشند.

روش های ورود اسب تروا(Trojan):

- ورود Atachment های Emailها و یا فایل ها
  (Email هایی که حاوی پیام برنده شدن مبلغی پول است)
- کلیدهایی هستند که ممکن است فشردن آن ها بر روی صفحه نمایش منجرب به ورود اسب تروا شود.
- تبلیغاتPOP UP می باشد.

چگونگی حمله اسب تروا:

پس از اینکه اسب تروا همراه با یک فایل وارد سیستم شد از آن جدا شده و بصورت جداگانه وارد عمل می شود. جهت نصب اسب تروا کاربر باید اعمال و کارهایی که باعث نصب اسب تروا شود که این اعمال می توان کلیک بر روی دکمه هایی در صفی باشند با این فرضیات گفته شده مهاجم نمیتواند تشخیص دهد که اسب تروا کجا نصب خواهد شد. اسب تروا یک پدیده ی نسبتا تصادفی می باشد که توسط کاربران مختلف و بسته به کار هایی که انجام می دهند در جاهای مختلف نصب بشوند. زمانی که اسب تروا وارد ماشین قربانی می شودIP ماشین را از طریق مختلف مانند ارسال یک Email برای مهاجم ارسال می کند، مهاجم به این Inboxها IPهای ماشین های مختلف را برای ادامه حمله بدست می آورد.

اسب تروا با هر بار روشن شدن کامپیوتر فعال می شود.

اسب های تروا بر اساس نوع عملکرد به دو دسته کلی تقسیم می شوند:

۱. **اسب های تروا معمولی:** این نوع اسب تروا مثل یک برنامه کاربردی نصب می شود و شروع به فعالیت می کند.

۲. **اسب های تروا در سطح سیستم عامل:** این نوع اسب تروا در سطح سیستم عامل نصب و شروع به فعالیت می کند.

این نوع اسب تروا فقط بر روی سیستم عامل هایی نصب می شود که ابزاری در آن ها وجود داشته باشد که بتوان با آن تغییراتی در سیستم عامل بوجود آورد. این نوع از نوع قبلی زیاد تر هستند و به نفع مهاجم تاثیر بیشتری می توانند داشته باشند.

روش های انتشار ویروس ها:

۱. از طریق اجرای برنامه های اجرایی یا همان برنامه های میزبان که به آنها متصل شده اند، به برنامه های با پسوند Exe,Com متصل می شوند.
۲. از طریق قرار گرفتن در Boot Sector.

Boot Sector: بخشی از سیستم می باشد که، سیستم هنگام روشن شدن اولین برنامه ی خود را از آنجا دریافت می کند.

با هربار روشن شدن سیستم از Boot Sector جهت اجرای ویروس ها استفاده خواهد شد.

انواع ویرس ها:

۱. **ویروس های پنهان(**Hidden virus**) :** این ویروس ها سیستم عامل را آلوده می کنند و در ظاهر فایل های آلوده کاملا طبیعی به نظر می رسند.

۲. **ماکرو ها(Macro):** ویروس هایی هستند که به فایل های داده متصل می گردند و هنگامی که اجرا می شوند سیستم را آلوده می کنند.

روش کار ماکرو ها(Macro): با یک بار اجرا شدن یک **Auto Macro** تولید می کند. یعنی ماکرویی که در هربار باز شدن فایل های غیر آلوده از همان نوع نیز اجرا شده و خود را تکثیر می کنند.

۳. **ویروس های چند ریختی(**Viruses polymorphism**):** این نوع ویروس از روش های رمزسازی استفاده می کنند که با کلیدهای مختلفی این کار انجام می گیرد، هدف از رمز کردن تغییر شکل می باشد یک کلید بصورت تصادفی انتخاب می شود و خود کلید نیز همراه ویروس منتقل می گردد در طرف مقابل عکس این عملیات توسط برنامه رمزگشایی که آنجا وجود دارد انجام می پذیرد و ویروس هنگام اجرا خودش را بر روی سیستم قربانی بازیابی می کند و در نتیجه ویروس یاب نمی تواند آن را پیدا کند.

انواع ویروس های چند ریختی:

۱. یک تکه از کد تمام شکل های آن ثابت می باشد، مهاجم برای اینکه شکل های متفاوتی را به وجود آورد قسمتی از کد را رمز و قسمت هایی را باقی می گذارد. تکه ثابت را امضاء نامیده می شود. آنتی ویروس با جستجوی امضا ثابت ویروس را شناسایی می کند.
۲. برخی تکه ثابتی ندارند و همه قسمت هارا تغییر می دهند در این نوع از روی قسمت رمزکننده که در همه ثابت است شناسایی می شود. در مورد ویروس هاس با رمزکننده ثابت به جستجو الگوی رمزکننده بر روی ماشین قربانی می گردد.
۳. انواعی که رمزکننده آنها نیز متفاوت است ولی ساختار بدنه آنها شکل مشابهی دارند جستجو براساس ساختار بدنه می باشد چون ساختار بدنه یکسان است.
۴. انواعی که علاوه بر اینکه خود رمز کننده متفاوتی است از روش های مختلف رمز سازی استفاده می کنند.
۵. انواعی که در ساختار بدنه تغییر به وجود می آورند بطوریکه از روی ساختار بدنه نمی توان تشخیص داد که از چه نوعی هستند.

جهت مقابله با ویروس های Poly Morphic و Met Morphic پس از فعال شدن ویروس فایلی که توسط آن ایجاد می گردد مورد بررسی قرار داده ودر نتیجه فقط با شبیه سازی (Emulation) باز شدن ویروس و رسیدن آن به شکل نهایی بدون اینکه آثار مخربی بر روی قسمت های مختلفی داشته باشد انجام می گیرد. الگوی نهایی ویروس یکسان است و فقط شکل ظاهری آنها متفاوت می باشد. بنابراین با شبیه سازی می توان الگوی نهایی را بدست آورد که با الگوی ویروس می توان مطابقت و شناسایی کرد.

مقایسه کرم ها و ویروس ها:

کرم ها بر خلاف ویروس ها که بر اساس یک برنامه میزبان و بر اساس تحریکی که ممکن است کاربر به آن پاسخ دهند شروع به ورود به سیستم می کنند و منتشر می شوند کرم ها به صورت خودکار منتشر می شوند و نیاز به تحریکی از طرف کاربر ندارد.
به طور معمول کرم ها از آسیب پذیری های سیستم استفاده می کنند و سرعت کمی بر روی سیستم ها حرکت می نمایند.
***شباهت کرم ها با اسب تروا این است که روی یک سیستم تکثیر نمی شوند.**

هدف از ایجاد Malware:

1. **خواندن اطلاعات از روی ماشین قربانی**
2. **در اختیار گرفتن از ظرفیت محاسباتی ماشین برای استفاده در حملات DDOS یکی از حملات DOS و DDOS می باشد که آنها چندین ماشین به یک ماشین حمله می کنند و از ارائه سرویس مناسب توسط آن جلوگیری می کنند باید مهاجم برای این نوع حمله یا چندین ماشین داشته باشد ویا از ماشین هایی که در شبکه موجود هستند استفاده کنند که این راه دوم از طریق نصب Malwareها انجام خواهد شد.**