به نام خدا

جزوه درس

امنیـــــت شبـــکـــــه

مدرس

استاد عزیز جناب آقای صدیقی

تهیه کننده :

حسین شهریاری

دانشجوی رشته اینترنت و شبکه های گسترده

دانشگاه جامع علمی کاربردی – واحد بیرجند ۱

زمستان ۹۳

منابع شبکه :

در یک شبکه مدرن منابع بسیاری جهت محافظت وجود دارد.در لیست زیرمجموعه ای از منابع شبکه که امکان دارد مورد حمله واقع شود به اختصار آمده است:

۱.تجهیزات شبکه شامل روترها،سوئیچ ها و فایروال ها

۲.اطلاعات عملیاتی شبکه همانند جداول مسیر یابی و پیکربندی روترها

۳.منابع نامحسوس همانند پهنای باند

۴.اطلاعات و منابع اطلاعاتی همانند بانک های داده

۵.ترمینال ها و منابعی که به وسیله آن می توان به شبکه متصل شد.

۶.اطلاعات در حال تبادل بر روی شبکه در هر لحظه از زمان

۷.خصوصی نگه داشتن عملیات کاربران و استفاده آنها از منابع شبکه

حمله TAK :

حمله تلاشی خطرناک یا غیرخطرناک تا یک منبع قابل دسترسی از طریق شبکه به گونه ای مورد تغییر یا استفاده قرارگیرد که مورد نظر نباشد . حملات را می توان به سه دسته تقسیم کرد:

۱.دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه

۲.دستکاری غیر مجاز اطلاعات بر روی شبکه

۳.اختلال در سرویس دهی یک شبکه

هدف از ایجاد امنیت شبکه حفاظت از شبکه در مقابل حملات فوق است لذا می توان اهداف را نیز در سه دسته ارائه کرد:

۱.ثابت کردن محرمانگی داده

۲.نگهداری جامعیت داده

۳.نگهداری در دسترسی بودن داده

تحلیل خطر:

پس از تعیین منابع شبکه و خطرهایی که آنان را تهدید می کند باید خطرها و ریسک ها را در مقابل انواع خطاها و تهدیدات ایمن کنیم.

دو فاکتور اصلی در تحلیل خطر ۱.احتمال انجام حمله ۲.خسارت وارده در صورت بروز حمله موفقیت آمیز

سیاست های امنیتی:

پس از تحلیل خطر باید سیاست امنیتی شبکه را به گونه ای تعریف کرد که احتمال خطرات و میزان خسارت به حداقل برسد.در سیاست های امنیتی باید کلی نگر باشیم و درگیر مسائل جزئی نشویم .در واقع سیاست های امنیتی سه نقش اصلی را بر عهده دارند:

۱.چه و چرا باید محافظت شود. ۲.چه کسی باید مسئولیت حفاظت را بر عهده بگیرد

۳.زمینه ای را به وجود آورد که هر گونه تضاداحتمالی را حل و فصل کند.

سیاست های امنیتی را می توان به طور کلی به دو دسته تقسیم کرد:

۱. هر آنچه که به طور مشخص ممنوع نیست

۲. سیاست های محدود کننده: هر آنچه که به طور مشخص مجاز نیست ممنوع است.

معمولا ایده استفاده از سیاست های محدود کننده ایمنی بیشتری را به همراه می آورد زیرا در مورد آنچه که قانون تعیین تکلیف نکرده است منع استفاده وجود داردادما این سیاست با دشواری هایی نیز همراه است.

نواحی امنیتی:

تعریف نواحی امنیتی نقش مهمی را در ایجاد یک شبکه امن ایفا می کند.در واقع یکی از بهترین شیوه های دفاع در مقابل حملات شبکه طراحی امنیت شبکه به صورت منطقه ای و مبتنی بر تپولوژی است و یکی از مهم ترین ایده های مورد استفاده در شبکه های امن مدرن تعریف نواحی و تفکیک مناطق مختلف شبکه از یکدیگر است. تجهیزاتی که در هر ناحیه قرار می گیرند نیازهای متفاوتی دارند و لذا هر ناحیه بسته به نیاز های امنیتی تجهیزات نصب شده در آن دارای نیاز های متفاوتی خواهد بود همچنین منطقه بندی یک شبکه باعث ایجاد ثبات بیشتر در آن شبکه نیز می شود.

نواحی امنیتی بنا بر استراتژی های اصلی زیر تعریف می شوند:

۱.تجهیزات و دستگاه هایی که بیشترین نیاز های امنیتی را دارند در امن ترین منطقه قرار می گیرند . معمولا اجازه و دسترسی عمومی یا از طریق شبکه های دیگر به این منطقه داده نمی شود . دسترسی به این مناطق به کمک فایروال و با محدودیت انجام می شود. کنترل شناسایی و احراز هویت در این منطقه به شدت انجام می شود.

۲.سرویس هایی که فقط بایداز سوی کاربران داخلی در دسترس باشد در منطقه امن قرار می گیرد . کنترل دسترسی به این تجهیزات با کمک فایروال انجام می شود و بر دسترسی ها نظارت کامل می شود.

۳.سرورهایی که باید از شبکه عمومی مورد استفاده قرار بگیرد باید در منطقه ای جدا و بدون امکان دسترسی به مناطق امن تر شبکه قرار بگیرد . هر یک از این سرور ها بهتر است در منطقه ای مجزا قرار بگیرد تا در صورت حمله سایر حوزه ها مورد تهدید قرار نگیرد.

۴.استفاده از فایروال ها به شکل لایه ای و بکارگیری فایروال های مختلف سبب می شود تا در صورت وجود یک اشکال امنیتی در یک فایروال کل شبکه به مخاطره نیفتد و امکان استفاده از درب پشتی BACK DOOR نیز کم شود.

امنیت تجهیزات شبکه:

برای تامین امنیت بر روی یک شبکه یکی از بحرانی ترین مراحل تامین امنیت دسترسی و کنترل به تجهیزات شبکه است.

اهمیت امنیت تجهیزات به دو دلیل است:

۱. عدم وجود امنیت تجهیزات در شبکه به نفوذگران اجازه می دهد که با دستیابی به تجهیزات امکان پیکربندی آنها را به گونه ای که تمایل دارند انجام دهند . از این طریق هرگونه نفوذ و سرقت اطلاعات توسط نفوذگر امکان پذیر است.

۲. برای جلوگیری از خطرهای DOS تامین امنیت تجهیزات بر روی شبکه الزامی است.

امنیت فیزیکی:

امنیت فیزیکی بازه وسیعی از تدابیر را در برمی گیرد که استقرار تجهیزات در مکان های امن و به دور از خطر حملات نفوذگران و استفاده از افزونگی در سیستم از آن جمله اند.

۱.**افزونگی در محل استقرار شبکه:**یکی از راهکارها در قالب ایجاد افزونگی در شبکه ایجاد سیستمی کامل و مشابه شبکه اولیه است . دراین حالت شبکه ثانویه همتای شبکه اولیه می باشد و در صورت از کار افتادن سیستم اصلی به سرعت میتواند جایگزین سیستم اولیه شود یا در صورت افزایش ترافیک بر روی شبکه اولیه بارترافیک می تواند بر روی دو سیستم تقسیم شود . با همه مزایای این راهکار در شبکه های با حجم پایین این کار مقرون به صرفه نیست و این مکانیزم قالبا برای شبکه های با حجم بالا قابل استفاده است.

۲. **توپولوژی شبکه:** طراحی توپولوژی شبکه یکی از عوامل اصلی است که در زمان رخداد حملات فیزیکی می تواند از شبکه محافظت کند و دارای سه ساختار به شرح زیر است :

الف)طراحی سری: در این طراحی با قطع خط تماس میان دو نقطه کلیه منابع شبکه به دو قسمت تقسیم می شوند و امکان سرویس دهی بین دو ناحیه امکان پذیر نیست

ب)طراحی ستاره ای: دراین طراحی در صورت رخداد حمله فیزیکی و قطع اتصال یک نقطه سرویس دهی به سایر نقاط دچار اختلال نمی شود. با این وجود در این ساختار سرور نقش کلیدی دارد و در صورت از کار افتادن آن کل شبکه از کار می افتد.

ج) طراحی مش : در این طراحی که تمامی نقاط ارتباطی با یکدیگر در ارتباط هستند در این روش هر گونه اختلال در یک نقطه نمی تواند سایر نقاط را تحت الشعاع قرار دهد. اما در این روش به علت محدودیت های اقتصادی فقط در موارد خاص و بحرانی استفاده می شود.

۳.**محل های امن برای تجهیزات:** در تعیین یک محل برای تجهیزات چند نکته را باید مورد توجه قرار داد:

الف)یافتن مکانی که به اندازه کافی از دیگر نقاط مجموعه متمایز می باشد به گونه ای که هر گونه نفوذ در محل آشکار باشد

ب) در نظر داشتن محلی که در ساختمان یا مجموعه ای بزرگتر قرارگرفته است تا تدابیر امنیتی بکارگرفته شده برای امن سازی مجموعه بزرگتربتوان برای امن سازی محل اختیار شده نیز به کار گرفت

ج)محدود سازی دسترسی به تجهیزات شبکه با استفاده از قفل ها و مکانیزم های دسترسی دیجیتال به همراه ثبت زمان ها ، مکان ها و کد های کاربری

د)استفاده از دوربین های مداربسته

ه)اعمال ترفند هایی برای رهایی از اصول امنیتی

۴.**انتخاب کانال ارتباطی امن:**عمل شنود بر روی سیم های مسی چه در نوع کواکسیال و چه در زوج های به هم تابیده هم اکنون نیز از راه های نفوذ به شمار می آید . با استفاده از شنود می توان اطلاعات بدست امده از تلاش های دیگر برای نفوذ در سیستم های کامپیوتری را گسترش داد و به جمع بندی مناسبی برای حمله رسید . هرچند می توان سیم ها را نیز به گونه ای مورد حفاظت قرار داد تا احتمال برای شنود و یا حتی تخریب فیزیکی وجود داشته باشد ولی درحال حاضر امن ترین روش ارتباطی در لایه فیزیکی استفاده از فیبر های نوری است .

۵.**منابع تغذیه :** منابع تغذیه در حکم خون در رگ های شبکه ای ارتباطی است و بدون برقراری جریان الکتریکی فعال نگه داشتن تاسیسات شبکه امکان پذیر نیست در این زمینه باید به دونکته توجه کرد:

الف)طراحی صحیح منابع تغذیه در شبکه براساس محل استقرار تجهیزات شبکه باید به گونه ای باشد که تمامی تجهیزات فعال برق مورد نیاز خود را بدون آنکه به شبکه تامین فشار بیش از اندازه وارد شود بدست آورد.

ب)وجود منابع تغذیه پشتیبان به گونه ای که تعداد و یا نیروی پشتیبانی آنها به نحوی باشد که نه تنها برای تغذیه کل شبکه در مواقع نیاز به منابع تغذیه پشتیبانی کفایت کند بلکه امکان تامین افزونگی مورد نیاز برای تعدادی از تجهیزات بحرانی درون شبکه را به صورت منفرد فراهم کند.

۶.**عوامل محیطی :** علاوه بر آسیب هایی که توسط نفوذ گران به شبکه و تاسیسات آن وارد می شود تهدیدات دیگری نیز همانند حوادث طبیعی نیز می تواند موجب بروز اختلال در کارکرد شبکه شود. عواملی همچون آتش سوزی ، زلزله ، طوفان و دیگر بلاهای طبیعی.

امنیت منطقی:

امنیت منطقی به معنای استفاده از روش هایی برای پایین آوردن خطرات حملات منطقی و نرم افزاری بر ضد تجهیزات شبکه است برای مثال حمله به مسیر یاب ها و سوئیچ ها بخش مهمی از این گونه حملات هستند.

۱.**امنیت مسیریاب ها:** حمله ضد امنیتی بر علیه مسیر یاب ها و دیگر تجهیزات شبکه را می توان به سه دسته تقسیم کرد: الف)حمله برای غیر فعال سازی کامل ب)حمله به قصد دست یابی به سطح کنترلی ج)حمله برای ایجاد نقص در سرویس دهی

۲.**مدیریت پیکربندی:** یکی از مهم ترین نکات در امنیت تجهیزات نگهداری نسخه پشتیبان از پیکربندی سیستم است.نسخه های پشتیبان باید دارای آخرین تغییرات اعمال شده باشد و از طرفی باید کامل باشد به گونه ای که اگر پیکر بندی تجهیزات شبکه مورد حمله قرار گرفت به تنهایی و با اتکا بر این نسخه ها عملکرد سیستم را بتوان به حالت اول برگرداند.

۳.کنترل دسترسی به تجهیزات: دو راه اصلی برای کنترل تجهیزات فعال وجود دارد :

الف) کنترل از راه دور ب)کنترل از طریق درگاه کنسول

در روش الف می توان با اعمال محدودیت در امکان پیکربندی و دسترسی به تجهیزات از آدرس های خاص یا استاندارد ها و پروتکول های خاص احتمال حملات را پایین آورد.در مورد روش دوم دو روش معقول ۱.جلوگیری از دسترسی مستقیم به تجهیزات :توجه کنیم در صورت عدم امنیت فیزیکی امکان برقراری امنیت از راه دور وجود ندارد ۲.قرار دادن تجهیزات در محفظه های دارای کلید

۴.امن سازی دسترسی: علاوه بر پیکر بندی تجهیزات برای استفاده از احرازهویت یکی دیگر از روشهای معمول امن سازی استفاده از کانال فرستنده در حین ارتباط است . یکی از ابزار های معمولی در این روش SSH است. با استفاده از این ارتباط پیام ها رمزنگاری شده و در صورت شنود اطلاعات امنیت سیستم به خطر نمی افتد. از دیگر روش های معمول می توان به استفاده از کانال های VPN مبتنی بر IPSEC اشاره نمود.

۵.مدیریت رمز های عبوری : مناسب ترین محل برای ذخیره رمز های عبور بر روی سرور است.هر چند که در بسیاری از موارد لازم است که بسیاری از این رمز ها بر روی خود سخت افزار نگهداری شوند در این صورت مهم ترین نکته به یاد داشتن فعال کردن سیستم رمز گذاری بر روی مسیر یاب یا دیگر سخت افزار های مشابه است.

ملزومات و مشکلات امنیتی سرور ها :

منظور از سرور ها در اینجا شبکه های بزرگی است که به شبکه های کوچکتر سرویس دهی می کند.

قابلیت های امنیتی:ملزومات امنیتی به صورت خلاصه به شرح ذیل است :

الف)قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع حملات ب)وجود امکان بررسی ترافیک شبکه با هدف تشخیص بسته هایی که به قصد حمله بر روی شبکه ارسال می شود .با استفاده از نرم افزار های IDS می توان حملات را تشخیص داد ج)قابلیت تشخیص منبع حملات :با وجود آنکه راه هایی از قبیل سرقت آدرس و استفاده از سیسیم های دیگر از راه دور برای حمله کننده و نفوذ گر وجود دارد ولی استفاده از سیستم های رد یابی کمک شایانی برای دست یافتن و یا محدود ساختن سیستم ها و منبع مشکوک را می نماید.بیشترین تاثیر مکانیزم زمانی است که حملات از نوع DOS است.

مشکلات اعمال ملزومات امنیتی:یکی از معمول ترین مشکلات پیاده سازی IDS است . خطر یا ترافیکی که برای یک دسته از کاربران به عنوان حمله تعبیر میشود برای دسته دیگر به عنوان جریان عادی داده است لذا تشخیص این دو جریان داده از یکدیگر بر پیچیدگی IDS افزوده و در اولین گام از کارایی و سرعت پردازش ، ترافیک و بسته های اطلاعاتی خواهد کاست . برای جبران این کاهش سرعت تنها می توان متوسل به تجهیزات گران تر و اعمال سیاست های امنیتی پیچیده تر شد.

رویکردعملی به امنیت شبکه لایه بندی شده:

رویکرد های امنیتی لایه بندی شده را در ۵ لایه مختلف ارزیابی می کنیم:

۱.امنیت در محیط بیرونی ۲. امنیت شبکه ۳. امنیت میزبان ۴. امنیت برنامه های کاربردی ۵. امنیت داده

ضریب عملکرد: ضریب عملکرد به عنوان میزان تلاش مورد نیاز توسط یک نفوذگر به منظور تحت تاثیر قراردادن یک یا چندین سیستم و ابزار امنیتی تعریف می شود که باعث رخنه کردن در شبکه می شود . یک شبکه با ضریب عملکرد بالا به سختی مورد دستبرد قرار میگیرد در حالی که یک شبکه با ضریب عملکرد پایین می تواند نسبتا به راحتی مختل شود .

امنیت پیرامون:منظور از پیرامون اولین خط دفاعی نسبت به بیرون و به عبارتی به شبکه غیر قابل اعتماد است پیرامون اولین و آخرین نقطه تماس برای دفاع امنیتی محافظت کننده شبکه است و ناحیه ای است که شبکه به پایان می رسد و اینترنت آغاز می شود . پیرامون به وسیله دیوارهای آتش به شدت کنترل می شود . دیواره ای آتش معمولا وب سرور ها مدخل ایمنی ها آنتی ویروس و سرورهای DNS را در بر میگیرد. دیواره ی آتش معمولا قوانین سختی در مورد اینکه چه چیزی میتواند وارد شبکه شود و یا اینکه چگونه میتوان با اینترنت تعامل داشت دارد.فایروالها معمولا یک فایروال روی سروری نصب می گردد که به بیرون و درون شبکه متصل است.

فایروال سه عمل انجام میدهد: ۱.کنترل ترافیک ۲. تبدیل آدرس ۳. نقطه پایانی VPN

فایروال کنترل ترافیک را با سنجیدن مبدا و مقصد تمام ترافیک ها وارد شونده و خارج شونده انجام می دهد و تضمین می کند که تنها تقاضاهای مجاز اجازه عبوردارند به علاوه فایروالها به شبکه امن در تبدیل آدرس های IP داخلی به آدرس های قابل رویت در اینترنت کمک می کند .

آنتی ویروس شبکه :

آنتی ویروس ها محتوای ایمنی های وارد شونده و خارج شونده را با پایگاه داده ای از مشخصات و ویروس های شناخته شده مقابله می کند . آنتی ویروس ها ایمنی ایمن های آلوده را مسدود میکند و آنها را قرنتینه می نماید سپس به دریافت کنندگان و مدیران شبکه اطلاع می دهد این عمل از ورود یا انتشار یک ایمیل آلوده به ویروس در شبکه جلوگیری می کند.آنتی ویروس شبکه مکملی برای حفاظت ضد ویروسی است به منظور کارکرد موثر دیتابیس و ویروس های شناخته شده باید به روزنگه داشته شود.

VPN:

یک شبکه اختصاصی مجازی از رمزنگاری سطح بالا برای ایجاد ارتباط امن بین ابزار دور از یکدیگر مانند لپ تاپ ها و شبکه مقصد استفاده می کند . VPN اساسا یک تونل رمز شده تقریبا با امنیت و محرمانگی یک شبکه اختصاصی اما از میان اینترنت ایجاد می کند.

پروتکول ها در اینترنت :

دو کامپیوتر در شبکه بر اساس قرارداد ها و پروتکول های مصوب با هم تبادل اطلاعات می کنند . گاه این قراردادها و پروتکول ها دارای نقاط ضعفی است که موجب سوء استفاده توسط نفوذگران قرارمی گیرد به همین دلیل لازم است با هر کدام از این پروتکول ها به اختصار آشنا شویم.

سرایند های پروتکل های IP :

۱.فیلد نسخه:این فیلد برای تعیین ورژن یا نسخه پروتکلIP است

۲.IHL : این سرآیند طول بسته IP را مشخص می کند

۳.TYPE OF SERVICE : نوع سرویسی را که بسته IP در اختیار دارد را نشان می دهد .

۴.TOTAL LENGTH: حداکثر طول بسته را نشان می دهد.

۵.TIME OF LINE:این فیلد باید با یک عدد مقدار دهی شود که نشان می دهد چه مقدار از عمر بسته می گذرد.هرگاه بسته از مسیر یاب عبور می کند یکی از مقداراین عدد کم می شود.اگر این عدد با ۲۰ مقدار دهی شود تا قبل از صفر شدن بیست می تواند در شبکه باقی بماند. از این فیلدبرای تعیین موقعیت مسیر یاب ها و گره ها در شبکه استفاده می شود . همچنین برای بررسی باز یا بسته بودن پورت نیز استفاده می شود.

۶.DESTINATION SOURCE ADDREES:این فیلد مبدا و مقصد بسته را مشخص می کند

۷.پروتکل ICMP :پروتکلی که هدف آن بررسی خطاهایی است که ممکن است در دریافت و یا ارسال بسته های IP رخ دهد . در صورت وجود خطا پیامی را به مبدا فرستنده خواهد فرستاد اسن پروتکول یک سیستم گزارش خطاست و وظیفه ای برای رفع خطا ندارد.

سرآیندها :

مهم ترین سرایند این پروتکل CHECKSUM است جهت مشخص کردن این که آیا اطلاعات بسته ارسالی درست است یا نه ، بسته ICMP حاوی پیامی است که نشان می دهد خطایی رخ داده است.

فهرست پیام های ICMP:

۱.DESTINATIONUDREACHABLE:مقصد در دسترس نیست

۲.TIME EXCEEDED:این پیام تعیین می کند بسته قبلی که ارسال شده است نتوانسته مقصدش را پیدا کند یعنی بسته مدت زمان طولانی در شبکه بوده و عمر آن سر آمده است

۳.PARAMETER PROBLEM :یعنی یکی از فیلدهای بسته IP اشتباه یا بی معنی بوده است.

۴.SOURCE QUENCH: تقاضایی برای کاهش ارسال بسته های یک میزبان می باشد.

۵.REDIRECT:تغییر در مسیر یابی های قبلی را در صورتی که در یک زیر شبکه باشند را نشان می دهند .

۶. ECHOREGAEST و ECHOREPLAY : برای بررسی وجود یک سیستم در شبکه است . برای بررسی کردن در دسترس بودن یک ماشین در شبکه از این پیام استفاده می شود.به فرآیند رفت و برگشت این پیام عمل PING می گویند.

۷.TIME STAMP REGUEST و time stamp replay:این پیام شبیه پیام ecko است با این تفاوت که در این پیام ها علاوه بر اطلاعات ارسال شده در بسته ecko زمان رفت برگشت نیز درج می شود.

پروتکل ARP**:** این پروتکل برای مشخص کردن آدرس مک و ارتباط دادن آن به آدرس IP روی شبکه است . آدرس مک آدرس سخت افزاری کارت شبکه است که توسط سوئیچ ها مورد استفاده قرار میگیرد .هدف پروتکل ARP این است که بداند چه آدرس IP به چه آدرس مک ارتباط دارد . پروتکل ARP بر خلاف پروتکل ICMP اجباری است زیرا اگر نتوانیم تناظر بین آدرس های IP و آدرس های مک را بدانیم نمی توانیم بسته را به مقصد برسانیم .

فیلد های سر آیند ARP**:**

HARD WARE TYPE :این فیلد نوع سخت افزار و نوع کارت شبکه را مشخص می کند.

PROTOCOL TYPE :نوع پروتکل لایه دوم را مشخص می کند.

HARD WARE ADDRESS LENGTH :نشان دهنده طول آدرس سخت افزاری بر حسب بایت است.

PROTOCOL ADDRESS LEHGTH :تعیین کننده طول آدرس IP است.

OPERATION CODE :نشان می دهد بسته ای که ارسال می کنیم یک بسته تقاضا است یا پاسخ

SOURSE HARD WARE ADDRESS :این فیلد آدرس فیزیکی مبدا را نشان می دهد

SOURCE IP ADDRESS :این فیلد آدرس IP مبدا را نشان می دهد .

DESTINATION HARD WARE ADDRESS :این فیلد آدرس فیزیکی مقصد را نشان می دهد.

DESTINATION IP ADDRESS :این فیلد آدرس IP مقصد را نشان می دهد.

چون ارسال و دریافت بسته های ARP ممکن است زمان بر باشد و سرعت ارسال و دریافت بسته های شبکه بکاهد بنابراین از جداول به عنوان جدول آدرس ها استفاده می شود که این جداول به صورت CASHE هستند.

پروتکل tcp **:**

پروتکل tcp پروتکلی است که به صورت اتصال گرا عمل می کند در صورتی که گره بخواهد با گره b ارتباط برقرار می کند .باید تقاضایی از طرف گره a صورت گیرد و از طرف مقابل تفهیمی بر اینکه آمادگی اتصال دارد دریافت شود پس ارتباط تا زمانی که توسط یکی از طرفین قطع نشده است ادامه می یابد.این ارتباط مراحلی دارد و در صورتی که یکی از طرفین نخواهد ارتباط را ادامه دهد با ارسال پیام هایی نسبت به قطع ارتباط ایجاد شده اقدام می کند.

نکته:در پروتکل tcp برای جدا کردن پروسه های فعال روی یک ماشین شماره پرت تعریف می شود.

آدرس سوکت:به ترکیب شماره ip و شماره port آدرس سوکت گفته می شود.

قطعه tcp:بسته های ایجاد شده در لایه tcp را قطعه tcp گویند.

سر آیند های پروتکل tcp **:**

Soruce port وdistination port :نحوه ارسال و دریافت و محل ورود و خروج اطلاعات را مشخص می کند شماره پروت پروسه های فعال روی ماشین را نشان می دهد با تعیین شماهر پورت و وجود پروسه فعال که بتواند این بسته tcp را پردازش کند.زمانی که بسته tcp دریافت می شود مشخص است که به چه پروسه ای باید تحویل داده شود و سرویس مربوط به بسته انجام شود پورت هایی تعریف می شوند شماره هر پورت نشان دهنده ی

فعال بودن آن پروسه است که با کنار هم قراردادن آدرس ip و شماره این پورت تعیین می گردد که در کجا و در چه کاری باید انجام گیرد . با کنار هم قرار دادن آدرس ip و مقابل آن عدد ۸۰ و ۲۵ نشان داده می شود که روی ماشین با چه پروسه ای ارتباط صورت می گیرد اگر این پورت باز باشد و یا به عبارتی دیگر پروسه فعال باشد زمانی که بسته tcp به ماشین می رسد ماشین توسط این پورت اطلاعات را دریافت می کند.دریافت و چه زمان ارسال باید پورت مبدا و مقصد مشص باشد که باعث دریافت سرویس بهتر خواهد شد.

Acknow led gement number : با قرار دادن مقادیر عددی در این فیلد ها تمامی بسته های tcp که قرار است ارسال و یا دریافت شود مشخص می شود هر اتصالی که بین دو طرف ایجاد می گردد از یک شماره شروع می شود مقدار پاسخ یک واحد بیشتر از مقدار جواب است با توجه به این شماره ها بسته های دریافتی کنار هم چیده شده تا اطلاعات بزرگتر را نشان دهد.

Cff set : نشان دهنده اندازه بسته Tcp می باشد .

نحوه برقراری ارتباط در tcp :

برقراری ارتباط در پروتکل tcp در سه مرحله اتفاق می افتد مراحل به این صورت است که ابتدا کامپیوتر مشتری یک بسته را با یک شماره تصادفی به عنوان مثال x به کامپیوتر سرور وشماره تصادفی برابر y=1 را ارسال می کند و پاسخ مشتری y+1 را بر می گرداند.

کنترل جریان داده:

کنترل جریان به معنی تطبیق پیدا کردن بین فرستنده و گیرنده اگر به صورت مقطعی شرایطی پیش آمد که یک طرف فرستنده یا گیرنده کندتر از طرف دیگر باشد و یا نیاز به زمان بیشتری داشته باشد. در این صورت با کنترل جریان داده قابل جبران است گاهی اوغات نیز یکی از طرفین قادر به برقراری ارتباط با سرعت پیش بینی شده نیست برای حل این مشکل ها بافرهایی پیش بینی میشوند.اطلاعاتی که از یک طرف سریع تر به طرف کندتر می رود در این بافرها نگهداری میشود تا در صورت بروز اشکال به صورت مقطعی بتوان با استفاده از بافر این اختلاف سرعت را برطرف کرد . اگر شرایطی پیش بیاید که این بافرها پر شود چون نمی خواهیم بسته ها از بین برود باید جریان اطلاعات را کنترل کرد . کنترل جریان داده را با طول پنجره نشان می دهند که با آن می توان میزان سرعت ارسال و دریافت اطلاعات را کم کرد و یا برای مدتی متوقف نمود .

اندازه گیری زمانی:

برای این کار بسته ای ارسال شده و دریافت پاسخ آن بسته ای دریافت می شود . مدت زمانی که طول می کشد بسته باز گردد جهت اندازه گیری زمان استفاده می شود.

پروتکل udp :

پروتکل udp از نظر موقعیت شبیه پروتکل tcp است که روی پروتکل ip قرار می گیرد اگر قرار باشد بسته های کوچک ارسال شود این پروتکل نسبت به پروتکل tcp دارای سر بار کمتر است در لایه بندی شبکه در لایه انتقال به طور معمول از پروتکل tcp استفاده می شود . در صورتی که حجم بسته ها بزرگ باشد روش اتصال گرا مناسب تراست و سربار زیادی را به شبکه وارد نخواهد کرد ولی در صورتی که طول بسته کوچک باشد تحمیل این سربار مقرون به صرفه نمی باشد.

سرآیند های پروتکل udp **:**

Soruce portوdestination port : این فیلد ها تعیین می کنند که بسته از کجا آمده و به کجا میرود.فیلد length نشان دهنده طول بسته است. بسته هایی که از طریق پروتکل udp ارسال می شود به صورت بسته های تکی ارسال می شود و نیازی به شماره سریال ندارند دستور net ststute شماره پورت های باز را بر ر وی سیستم ها تعیین می کند یکی از تکنیک هایی که مهاجمین از آن استفاده می کنند باز کردن پروسه جاسوس در میان پروسه های فعال ماشین است گاهی اوغات با استفاده از دستور net stute فعال بودن این پروسه نیز مشخص نمی شود این تکنیک همان تکنیک اسب تراوا است . یکی از کارهایی که مهاجمین دنبال می کندد تعیین پورت های باز است .

دیواره آتش:

دیواره آتش ماشینی است که بر اساس قوانین پیش بینی شده در آن به بررسی بسته هایی که ارسال و دریافت می شوند می پردازد . دیواره آتش گرهی در شبکه است که لایه های متناظر با هر لایه دیگر را دارد بنابراین عملیات لایه های مختلف آن مطابق با لایه بندی شبکه می باشد . سه لایه مهم دیواره آتش عبارتند از لایه ip ، tcp و لایه کاربردی .بابررسی بسته ها توسط دیواره آتش در سه لایه ذکر شده یکی از حالات زیر ممکن است رخ دهد :۱.بسته طبیعی است پس به آن اجازه ورود داده می شود ۲. بسته حذف می شود و به آن اجازه ورود داده نمی شود ۳. بسته حذف شده و در قبال آن پیامی برای سیستم ارسال کننده آن فرستاده می شود . در واقع دیواره آتش با بررسی بسته های ورود و خروجی امکان ورود و خروج آنها را فراهم می آورد.

دیواره آتش در لایه ip**:**

سرآیند بسته ip بررسی می شود و بر اساس ویژگی های سرآیند بسته از قبیل آدرس مبدا و مقصد و شماره پروتکل و زمان حیاط بسته دیواره آتش در مورد حذف شدن یا نشدن بسته تصمیم می گیرند . به عنوان مثال ممکن است توسط دیواره آتش از ورود بسته هایی که از آدرس خاص ارسال شده اندو یا ازرسیدن بسته به مقصد خاص جلوگیری شود و یا ممکن است بسته های یک نوع پروتکل خاص حذف گردد.

کار دیواره آتش در لایه tcp **یا** udp **:**

در این لایه نیز بر اساس ویژگی های لایه ی انتقال تصمیم گیری می شود سرآیند های بسته لایه انتقال ویژگی هایی از قبیل شماره port مبدا ، شماره port مقصد ، فیلد شماره سریال و...را شامل می شودکه از آنها در ارسال و دریافت اطلاعات استفاده می شود.دیواره آتش بر اساس همین اطلاعات اجازه ورود و یا خروج اطلاعات را می دهد .مهم ترین کاراین مرحله بستن port ها می باشد.به عنوان مثال port ۸۰مربوط به عملیاتHTTP است یا ۲۵PORT مربوط به عملیات ارسال و دریافت فایل ها می باشد.بسته ها زمانی که توسط ماشین دریافت می شونددر صورتی که پروسه مربوطه فعال باشد آن بسته دریافت می شودبه عبارت دیگر یک PORTباز دریافت بسته مربوط به آن PORT راجهت پردازش بررسی می کند.با وجود باز بودن PORT ممکن است دیواره آتش در دریافت بسته هایی که به سمت مقصد ارسال شده اندنقش داشته باشد و اجازه دریافت بسته را ندهد بنابراین ممکن است روز یک ماشین امکان دریافت اطلاعات به صورت FTP باشد ولی دیواره آتش امکان ورود این بسته ها را ندهد

بنابراین به نظر می رسد این PORT بسته است بنابراین مهم ترین کاری که در لایه دوم یا همان لایه انتقال دیواره آتش انجام می دهد بستن بعضی PORTهای خاص است تا اجازه دریافت و یا ارسال داده را نداشته باشد.

دیواره آتش در لایه کاربردی:

در لایه کاربردی بر اساس سرویس های خاص که ممکن است در این لایه وجود داشته باشد عملیات مختلفی انجام می شود که تنوع این عملیات بسیار زیاد است و پردازش این عملیات بسیار سخت تر از عملیات لایه انتقال است. زمان زیادی از پردازش گر ماشینی که به صورت دیواره آتش طراحی شده صرف این عملیات می شودبنابراین سعی می شود اکثر کارهای مهم توسط دو لایه قبلی در دیواره آتش انجام گیرد به عبارتی دیگر در لایه های پایین ترمحدودیت های بیشتری اعمال می شود.به عنوان مثال پورت های اضافی که از آنها استفاده نمی شود را می بندیم تا حجم کمتری از کار باقی بماندو در نتیجه بین زمان هایی که CPU برای این سه لایه اختصاص می دهد تعادل برقرار شود.و در نتیجه از کندی شبکه که ممکن است دیواره آتش در دریافت و ارسال اطلاعات در شبکه آن را اعمال کند جلوگیری می شود.مجموعه طراحی هایی که برای یک شبکه کامپیوتری انجام می شود به منظور ارسال و دریافت بسته هادر کمترین زمان ممکن است دیواره آتش علاوه بر اینکه کمکی به ارسال و دریافت سریع تر اطلاعات نمی کند بلکه آنرا کندتر هم می کند و اگر به صورت نامناسب طراحی شود گاهی اوقات ممکن است آن را حذف نیز کنید.به عنوان مثال در بسیاری از ماشین هایی که از سیستم عامل ویندوز استفاده می کنند دیواره های آتش هنگام نصب سیستم عامل به صورت پیش فرض بر روی سیستم قرار می گیرندکه در بسیاری از موارد استفاده کنندگان به خاطر کندی که به سیستم آنها تحمیل می شود آن را حذف می کنند .دیواره های آتش معمولا بکارگیری عوامل امنیتی نظیر دیواره آتش تا زمانی که در سیستم مشکلی به وجود نیامده باشد کار اضافی به نظر می رسد یعنی در شرایط عادی چنین به نظر می رسد که وجود دیواره آتش جز کندی چیز دیگری اعمال نمی کند.اما اگر در اثر حملاتی که وارد می شود خسارت قابل توجهی به سیستم شما وارد شود بهتر است که این سربار کندی را بپذیریم تا شبکه ای داشته باشیم که خسارت کمتری به آن وارد می شود.

انواع دیواره آتش:

۱.ساده ترین آنها که فقط بسته ها را بررسی می کند و برخی از آنا را حذف می کند و به بعضی اجازه ورود می دهد و در گزینش آنها هیچ گونه هوشندی به خرج نمیدهد.

۲.دیواره های آتش هوشمند هستند . این دیواره ها براساس قواعدی که در اختیار دارد تصمیم گیری می کند با فیلتر های مختلفی که جهت مقابله با حملاتی که ممکن است وجود داشته باشد و یا در مورد نرم افزار هایی که جهت مقابله با فایروال ها طراحی شده اند می توانند تصمیم بهتری بگیرند.حجم محاسبات لازم برای پیاده سازی چنین دیواره های آتشی بیشتر می باشد.ونیز به حافظه هایی نیاز است که بتوان این تاریخچه را نگهداری کند

دیواره های آتش مبتنی بر پراکس:

پراکس سرور های که به اختصار پراکس می گویند به جای گره اصلی در شبکه بسته ها را دریافت و ارسال می کند و به عنوان واسطه عمل می کند . پراکس در واقع به وکالت از ماشین اصلی اطلاعات را دریافت می کند . دیواره های آتش مبتنی بر پراکس علاوه بر اینکه همانند دیواره های آتش معمولی عمل میکنند هیچ گونه ارتباط سیتسمی با گره های داخلی ندارند اگر فایروالها خود پراکس باشند امکان نفوذ در شبکه را به حداقل می رساند.

حملات مختلف:

حملات مختلف بر حسب ضعفی که ممکن است در لایه های مختلف شبکه وجود داشته باشد به این صورت انجام می شود : ابتدا تلاش برای نفوذاز لایه کاربرد است اگر اطلاعات لایه کاربردی که می توانند درا اختیار مهاجم قرار گیرند وجود نداشته باشد امکان طراحی سایر حملات کم خواهد بود اگر چه سایر حملات ممکن است مهم تر باشند ولی اطلاعاتی که در لایه کاربردی استخراج می شوند برای انجام حملات بسیار لازم خواهند بود بر حسب لایه های شبکه یعنی لایه فیزیکی ، لایه ip و لایه های tcp می تواند حملاتی علیه سیستم انجام شود برخی از نکات عمومی در جهت محافظت از اطلاعات و نیز نکات مهمی که در شبکه از لحاظ طراحی وجود دارد باید به آنها توجه شود بسیاری از اطلاعات جهت انجام حملات بر اساس اطلاعات دریافتی از کاربران شبکه و یا اشتباهاتی که در ارسال و دریافت اطلاعات ممکن است رخ دهد صورت می گیرداز جمله نکات عمومی که باید به آن پرداخت عدم پاسخگویی به سوالاتی است که لزومی ندارد پاسخ داده شوند تا لزومی به دادن اطلاعات نباشد. نمونه ای از نقض اطلاعات در این روش بر ملا شدن یا افشاء رمز های عبور و نام های کاربری است به عنوان مثال فرض کنید اگر سروری که رمز عبور و کد کاربری را دریافت می کند به صورت دقیق بگوید رمز عبور یا نام کاربری اشتباه است در این صورت کار نفوذگر اسانن تر می شود. نکته دوم:عدم دسترسی فیزیکی افراد غیر مسئول به مکانهایی که ارتباط به آنها ندارند نکته سوم:برخی از اطلاعاتی را که داریم از قبیل دیسک های بک آپ(پشتیبان)که هنگام نصب سیستم عامل معمولا برای بازیابی سیستم از آنها استفاده می شود باید جایی نگهداری شوند که کسی به آن ها دسترسی نداشته باشدبه عبارت دیگر اهمیت این قبیل اطلاعات را برای مسئول امنیتی شبکه و برای کاربرانی که به صورت مجاز به آنها دسترسی داشته باشند اطلاع دهیم . تمام اطلاعات کلیدی شامل رمزهای عبور ، شناسه های کاربری،پورت های باز و بسته و ساختار سیستم عامل نصب شده روی دیسک های بازیابی اطلاعات ذخیره شده است .نرم افزار هایی وجود دارد که بدون نیاز به خود سیستم قادر هستند این اطلاعات را بخوانند. اطلاعات کلیدی سیستم بر روی این ابزارها قرار داده می شوند تا در صورت بروز مشکل بتوان آنها را بازیابی کرد. نکته چهارم:پیش بینی دور شدن کاربر از سیستم ،به عبارت دیگر screen saver روی ماشین های حساس باید مجاز به کلمه عبور باشندتا در صورتی که کاربر مجاز اگر سیستم خود را بدون آنکه خاموش کند از آن دور شودفرد مهاجم نتواند از غیبت کاربر سوءاستفاده کند . همین مسئله در مورد میل سرور ها(mail server)نیر وجود دارد یعنی اگر کاربر برای مدتی کامپیوتر خود را ترک کرده و یا به صفحه مراجعه نکند برای دریافت مجدد اطلاعات باید نام و رمز عبور خود را وارد کند. نکته پنجم:پیشگیری از دور ریختن اطلاعات زمانی که دیگر مفید نیستند.این مشکل از آنجایی ناشی می شود که به کاربران این اطلاعات آموزش داده نشده است که هنگامی که می خواهند اطلاعات زایدرا دور برزند ابتدا آنها را نابود کنند و سپس دور بریزند.در اولین مرحله مهاجم سعی می کند به شبکه وارد شود.

راه های نفوذبه شبکه:

مرحله اول:ورود به شبکه :ورود به شبکه می تواند از طریق اتصالات فیزیکی باشد به عنوان مثال با دسترسی به یکی از گره های شبکه ورود به ساختمان یا مکانی که گره های شبکه یا سرور آنجاست . امروز اتصالات فیزیکی کمتر رخ می دهد هر چند که در برخی موارد همچنان مشاهده می شود . اما برخی از امکانات ارتباطی وجود دارد که

ناگزیر به استفاده از آنها هستیم و می تواند به عنام حفره ای برای نفود هکران استفاده شود . از آن جمله می توان مودم ها را نام ببریم مودم ها برای برقراری ارتباط از طریق شبکه تلفن یا شبکه دیتا استفاده می شود.مودم ها می توانند توسط مهاجمین برای کاربردهای غیرمجاز به کار گرفته شوند.

مرحله دوم:بررسی چگونگی ورود به سیستم : دروازه ورود به سیستم معمولا مودم ها می باشند . مثلا ممکن است روی ماشینی که مودم نصب است نرم افزارهای برقرای ارتباط از راه دور از قبیل pc any where نصب شده باشد .این اتفاق می تواند توسط پرسنل سازمان که می خواهنداز راه دوربا سیستم خود در سازمان ارتباط برقرار کنند به وجود می آید . گاه نرم افزار هایی از قبیل team viewer برای کنترل ماشین از راه دور استفاده می شود . زمانی که این نرم افزارها بر روی سیستمی ازسیستم های سازمان نصب می شود نقطه نفوذی برای هکرها به وجود می آید.از آنجایی که معمولا برای آسانی کار این سیستم ها دارای تدابیر امنیتی ضعیف می باشند باعث ضعف در سیاست های امنینی سازمان شده و مشکلاتی را به وجود می آورد. نرم افزار هایی از قبیلwar diaeling برای تعیین خطوط تلفن قابل نفوذ به سازمان استفاده می شود.این نرم افزار خطوط را کنترل کرده و تعیین می کند آیا این خط به مودم متصل است یا خیر؟ پس از تعیین کردن خط متصل به مودم با استفاده از نرم افزارthc login می توان کلمات عبور را جستجو کرده تا به رمز عبور دست یابیم و به این طریق به سیستم مورد نظر نفوذ کنیم . گاهی از اوغات محدوده ای که اتصال بیسیم می تواند برقرار شود فراتر از محدوده ای است که پیش بینی شده است . بنابراین با استفاده از نرم افزار های رمز یاب می توان به رمز شبکه دست یافت . پس از نفوذ به شبکه اولین قدم این است که مهاجم تعیین کند چه ماشین های بر روی شبکه فعال هستند سپس موقعیت ماشین و چگونگی اتصال آنها را در می یابیم برای اینکه مهاجم متوجه شود آیا ماشینی فعال است یا خیر؟به عنوان مثال دستورping با ارسال بسته های تعیین می کند آیا ماشین فعال است یا خیر البته این دستور می تواند ماشین های فعال را شناسایی کند و از تشخیص ماشین های غیر فعال عاجز است.

کلاس های ip :

به چهار دسته a ، b ، c ، d تقسیم می شوند . تعداد امپیوتر هایی که در کلاس a می توانند فعال باشند 2^{24} است در کلاسb 2^{16} و در کلاس c 2^{8} ودر کلاس d 2^{0} است . اگر در کلاسc مهاجم بخواهد ماشین های فعال شبکه را تعیین کند کافی است ۲۵۴ بار عمل ping را انجام دهد .در بسیاری از کاربرد ها توصیه می شود پروکل icmp غیرفعال شود تا به این طریق از شناسایی سیستم ها جلوگیری شود .

شناسایی port :

روش دیگر که مهاجمین از آن برای نفوذ در شبکه استفاده می کنند ارسال بسته های TCP و UDP است. مثلا پورت شماره ۲۵ برای پست الکترونیکی ، پورت ۸۰ برای HTTP ،پورت ۲۱برای FTP و غیره می باشد . با ارسال بسته های به این پورت ها و بررسی پاسخی که ارسال می شود می توان به سیستم فعال پی برد.

تعیین موقعیت ماشین ها :

برای تعیین موقعیت ماشین ها با استفاده از فیلدTTL که نشان دهنده طول عمر بسته می باشد استفاده می شود.مقدار این فیلد زمانی که از مسیر یاب ها عبور می کند یک واحد کم می شود اگر مقدار آن برابر صفر شود مسیر یاب بسته را حذف کرده پیغامی را برای مبدا می فرستد مبنی براینکه بسته به مقصد نرسیده است.نرم افزار cheopc برای تعیین نقشه توپولوژی شبکه است.

روش های تعیین پورت های باز:

مهاجمین در بالاترین لایه نکته دیگری را که مورد توجه قرار می دهند یافتن پورت های باز شبکه می باشد تا بتوانند در مراحل بعدی به ماشینی وارد شوند و آن را در اختیار بگیرند . جهت تعیین پورت های باز نرم افزار هایی وجود دارد که به آنها پویش گر درگاه گفته می شود .نمونه ای از نرم افزارها به شرح زیر است:

1.nmap 2.strpbe 3.altra scan 4.super scan

نحوه پویش درگاه:

۱.**پویش مودبانه:**در این روش مهاجم با ماشینی که می خواهد باز یا بسته بودن پورت را بررسی کند یک ارتباط کامل برقرار می کند.

اشکالات پویش مودبانه:این روش وقت گیر میباشد . یعنی ارسال و دریافت بست ها و انجام سه مرحله جهت برقراری ارتباط و دریافت بسته های پاسخ طرف مقابل زمانبر میباشد در مجموع سه بسته ردو بدل می شود و یک بسته نیز برای ختم ارتباط ارسال می شود که این مجموعه زمانبراست.مشکل دوم بسیاری از سرور ها فایل های log را تشکیل می دهند که ورود افراد درآنجا ثبت می شود و از آن اطلاعات جهت تشخیص انجام یک حجوم می توان استفاده کرد جهت مقابله با این روش میتوان این فایل log را بررسی کرد.

۲.پویش مخفیانه:در این روش پس از دریافت اطلاعات از طریق سرور پویشگر بسته ریست را ارسال می کند یعنی فقط دو مرحله اط سه مرحله برقراری ارتباط انجام می شود . بنابراین به خاطر نبودن مرحله ختم کردن و حذف کردن یکی از این مراحل برقراری ارتباط در زمان تولید بسته های لازم برای ارسال و در زمان تاخیری که در شبکه است صرفه جویی می شود.

نکته:بسیاری از دیواره های آتش با پیگیری بسته ها قابل تشخیص این نوع حملات هستند.

سوال:چرا بسته ریست ارسال می شود؟به این علت که سروربه دنبال انجام مراحل بعدی باشد و از ارسال بسته که موجب گرفتن وقت ماشین مهاجم می شود پرهیز شود..

روش تعیین پورت های باز با استفاده از بسته های نامعتبر:

در این نوع پویش سعی می شود با ارسال بسته های غیر متعارف و بررسی کردن پاسخ تشخیص داده شود که پورتی وجود دارد یا خیر؟به صورت معمول اگر پورتی بسته باشد در پاسخ به بسته ای که جهت برقراری ارتباط ارسال می شود بسته ای ارسال می شود که نشان دهنده بسته بودن پورت است . با ارسال بسته هایی که غیر عادی هستند و با بررسی عکس العمل های آنها می توان پورت های بسته را از پورت های باز متمایز کرد.

پویش پورت ها با استفاده از پروتکل FTP:

در پروتکل های FTP قدیمی برای اینکه بشود نشستی برقرارکرد این امکان فراهم می شودکه یک سرور FTP بتواند به عنوان نماینده گرهی در بیرون از شبکه ارتباطی را با یک پورت برروی ماشین برقرارکند.مهاجم در این روش با برقراری ارتباط با یک سرور FTP ارسال فایلی را به یک پورت روی یک ماشینی که جهت تعیین باز یا بسته بودن پورت مورد هدف قرارگرفته است تقاضا می کند . به ظاهر تقاضایی که داده می شود جهت تعیین پورت های باز یا بسته نیست بلکه ظاهرا تقاضایی به یک سرورFTP داده می شود که فایلی را به سمت ماشین دیگری ارسال کند .اگر آن پورت باز نباشد ماشین FTP به متقاضی گزارش می دهد که پورتی که قرار است فایل برای آن ارسال شود بسته می باشد به این ترتیب هویت کاربر پنهان می ماند و به وسیله ویژگی هایی که در شبکه وجود دارد و یا توسط فرد سومی که همان FTP سرور است با ثبت نام وی و گزارش هایی که می دهد می تواند تشخیص دهد که پورت باز است یا بسته که از طریق آن می توان فایلی را برای یک ماشین ارسال کرد.

مروری بر مطالب گذشته:

مهاجم بسیاری از اطلاعات را از طریق افرادی که اطلاعات مربوط به شبکه را دارند و بی دلیل آنها را در اختیار سایر افراد قرار می دهند بدست می آورند.به عنوان مثال در مورد شکه باز و بسته بودن پورت ها نوع سیستم عامل مودم ها و نوع آنها .اگر مهاجم نتواند این اطلاعات را به آسانی بدست آورد به کارهای مقدماتی زیادی در لایه های مختلف می پردازدتابه این اطلاعات بدست آید. شماره تلفن مودم ها بررسی می شود و مودم های نفوذپذیر تشخیص داده می شوند سپس مهاجم به آنها نفوذ می کند . مرحله دوم:مهاجم فهرست ماشین های فعال را استخراج می کند که با استفاده از دستور PING یا نرم افزارهایی همانند cheaps و با ارسال بسته های tcp و udp ماشین های فعال شناسایی میشوند. مرحله سوم:ساختار تقریبی و نقشه شبکه تعیین می شود که با استفاده از ابزارهایی مثل cheops و traceroute جهت تشخیص فاصله ماشین ها نسبت به هم استفاده می شود مرحله چهارم :فهرست پورت های باز تعیین می شود . نرم افزار هایی از قبیل nmap برای تعیین پورت های باز استفاده می شود.این نرم افزار علاوه بر پورت های باز نوع سیستم عامل را نیز تعیین می کند مرحله پنجم:تعیین وجود و یا عدم وجود دیواره آتش و فهرست پورت های باز روی دیواره آتش و پورت هایی که دیواره آتش از ارسال و دریافت بسته ها به آنها جلوگیری می کند در این مرحله از نرم افزارهایی از قبیل firewak استفاده می شود مرحله ششم:با استفاده از نرم افزارهایی از قبیل nesuse نقاط آسیب پذیر شبکه از قبیل cgi و یا دسترسی های از راه دور و یا سرویس های زایدی که ممکن است از آنها استفاده نشود ولی پورت های آن باز باشد استفاده می شود.

چگونگی حمله در لایه کاربرد:

نرم افزارهایmalware:malware ها برنامه های کاربردی با ظاهری زیبا هستند که اهداف مهاجم را دنبال می کنند . این نرم افزارها به دودسته کلی تقسیم میشوند .الف)انواعی که برای تکثیر اجرا انتشار و ورودشان نیاز به یک برنامه میزبان دارند. ب)انواعی از برنامه ها که مستقل نی باشند و نیاز به یک برنامه میزبان ندارند.

انواع برنامه های مستقل:

۱.اسب تراوا:اسب تراوا برنامه مستقلی است که مانند یک برنامه معمولی بر روی کامپیوتر قربانی نصب و اجرا می گردد و ماشین قربانی در اختیارمهاجم قرار میدهد.ویژگی اسب های تراوا تین است که هدف آنها تکرار خودشان نیست یک بار ک در ماشین مهاجم قرار گیرند آن را در اختیار هکر قرارمی دهند.

۲.ویروس ها:ویروس ها به یک برنامه میزبان نیاز دارند و هدف آنها تکثیر خودشان میباشد.

۳.کرمها:به صورت خودکارمنتشر می شوند.

اسب های تراوا بر روی یک سیستم اجراشده و کنترل آن را به دست می گیرند.

نحوه ورود اسب های تراوا:

۱.استفاده از فایل های زمیمه یا پیوست در اینیل ها :بسیاری از ایمیل ها آلوده به اسب تراوا می باشند که با باز کردن آنها وارد سیستم می شوند .

۲.استفاده از کلیدهایی که ممکن اسن فشردن آنها بر روی صفحه نمایش منجر به ورود اسب تراوا شود.

۳.استفاده از تبلیغات :همزمان با باز شدن صفحات مختلف صفحه ای وجود دارد ه با کلیک کردت yes یا no و یا بستن آن صفحات اسب تراوا به ماشین وارد می شوند.تمام کلید هی درون آن صفحه توسط کسی که آن صفحه را نوشته است به جای دیگری متصل شده است و عملیاتی غیر از آنچه که در ظاهر بیان می کند انجام می دهد.زمانی که اسب تراوا وارد ماشین قربانی می شود ip ماشین را از طریق مختلف مانند ارسال به ایمیل برای مهاجم ارسال می کند.مهاجم با مراجعه به ایمیل خود ip ماشین های قربانی را بدست می آورد.اسب های تراوا بر اساس نوع عملکرد خود نیز جایی که در آن قرار می گیرند به دو دسته اسب تراوا ی معمولی و اسب های تراوادر سطح سیستم عامل تقسیم می شوند . نمونه های معروف اسب های تراوا به شرح زیر می باشند:

1.sub 2.bo2k 3.hack attack 4.vnc

روش های انتشار ویروس ها:

۱.از طریق اجرای برنامه های اجرایی همانند برنامه هایی که با پسوند exe جا هایی که ویروس می تواند تکثیر شود از قبیل فلش ها ، حافظه رم و سیدی ها می باشد ۲. از طریق قرار گرفتن در boot sector

انواع ویروس ها:

۱.ویروس های پنهانی :این نوع ویروسها سیستم عامل را آلوده میکند و در ظاهر فایل های آلوده کاملا طبیعی به نظر می آیند .

۲.ماکروا:این ویروسها از قرارگرفتن در تکه برنامه های اجرایی که در داده های اجرایی برنامه های دیگر وجوددارد باعث آلوده شدن برنامه ها می شود در فایل های داده ای برخی از برنامه ها نظیر word و exel ممکن است ماکروهایی وجود داشته باشد که هنگام باز شدن فایل عملیاتی انجام شود.بنابراین ماکروها ویروسهایی هستند که به فایل های داده متصل می گردند و هنگامی که اجرا میگردند سیستم را آلوده می کنند.۳.ویروس های چند ریختی:ویروس ها به طور معمول ظاهر های متفاوتی دارد و در نتیجه ویروس کشان می توانند آنها را تشخیص دهند

اما اسکنرها با پیمایش کدبرنامه ها و با توجه به الگو هایی که در درون ساختار برنامه ی آنهاست می توانند آنها را شناسایی کنند

نمونه هایی از کانال های پنهان :پس از اینکه برنامه های جاسوسی بر روی سیستم نصب شده اند منتظر ارسال و دریافت اطلاعات در سطح شبکه می باشند از آنجایی که ارسال و دریافت اطلاعات در سطح شبکه های ایمن به شدت کنترل می کنند این برنامه ها لازم است کانال ایمن را ایجاد کرده تا اطلاعات را از سیستم نتقل کند .

نمونه هایی از کانال های پنهان:

۱.ایجاد کانال از طریق بسته های icmp

۲.استفده از مرورگرها به صورت معکوس

۳.استفاده از telnet ها

۱.ایجاد کانال از طریق بسته های icmp **:** بسته های icmp بسته های هستند که مانند یک بسته لایه انتقال در یک بسته ip قرار می گیرند و برای ارسال پیغام های خطای شبکه استفاده می وند.برای برقراری ارتباط ماشین آلوده به جای استفاده از پروتوکول های tcp و udp با قراردادن اطلاعات خود در درون بسته های icmp آنها را به بیرن از شبکه ارسال میکنند .

۲. استفاده از مرورگر به صورت معکوس:مرورگرها معمولا بر روی پورت ۸۰ اطلاعات را منتقل می کنند بنابراین دیوار های آتش آنها را بلوک نمی کند.اگر این پورت بسته شود ارتباط ماشین با بیرون قطع می شود . برای این کار ماشین آلوده در قالب دستور get تقاضای یک صفحه وب را از ماشین مهاجم می کند . در مقابل ماشین مهاجم به جای ارسال جواب دستوراتی را برای ماشین آلوده می فرستد.

۳.استفاده از telnet**:**در این روش از پورت ۲۱ که پورت مورد استفاده برای ترمینال ها از راه دور میباشد همانند مورد قبل مورد سوءاستفاده قرارمی گیرد به این صورت که تقاضایی از سیستم آلوده به سیستم مهاجم ارسال می شود ومهاجم در پاسخ دستوراتی را ارسال می کند .

استراق سمع:

حملات مورد بررسی درق بل حملات لایه های بالایی می باشند به عبارتی یک سیستم را آلوده کرده و مورد سوءاستفاده قرارمی گیرد.اما گاهی در لایه های پایینی نیز اتفاق می افتد به صورتی که امنیت کل شبکه به خطر می افتد نمونه هایی از این حملات حمله استراق سمع یا شنود می باشد.

نرم افزار های شنود یا استراق سمع : این نرم افزار ها برای شنود کردن داده های ارسالی بر روی شبکه استفاده می شود و دارای دو نوع می باشد :

۱.شنود غیر فعال :در این روش فقط اطلاعات شنود میشود و کار اضافه ای انجام نمی شود و برای به دست آوردن رمز عبور و کد کاربری در شبکه استفاده می شود .

۲. شنود های فعال : در این روش پس از شنود اطلاعات گاه محتوای بسته های نیز تغییر می کند . به صورت عادی مهاجم ابتدا یک سیستم را در اختیار گرفته و با درکنار هم قراردادن اطلاعات استخراج شده از شبکه اطلاعاتی

را از سیستم بدست می آورد به طور معمول مهاجم اطلاعات ردو بدل شده را بین تمام هاست ها استراق سمع می کند .

کارت های شبکه در دو مد کار می کند :

۱.حالت مقید ۲. حالت بی قید

در حالت مقید هر کارت شبکه فقط اطلاعات مرتبط با خودرادریافت می کند و به اطلاعات ارسالی از سایر گره های شبکه کاری ندارد اما در حالت بی قید این مکان برای لایه های بالاتر فراهم می شود که تمام بسته های ارسالی که در معرض دید کارت شبکه قرار میگیرد را در اختیار بگیرد برای شنود کردن لازم است کارت شبکه در حالت بی قید قرار بگیرد .

روش های شنود کردن :دو روش برای شنود اطلاعات وجود دارد الف:بردن کارت شبکه به حالت بی قید : در این روش کارت شبکه وسیله ای که در قلب کانال ارتباطی وجود دارد امکان مشاهده و ردیابی اطلاعات وجود دارد .در این صورت که کارت شبکه تمام اطلاعات ردوبدل شده را دریافت می کند .ب)استفاده از سر ریز بافرها:در این روش با استفاده از ویروس ها و نرم افزار های مخرب دیگر سیستم را به هم ریخته و امکان نصب نرم افزار شنود برای سیستم فراهم می شود .پس از نصب برنامه شنود امکان سرقت اطلاعات وجود دارد .

نکته:نرم افزار های شنود لزوما برای کاربردهای تخریبی استفاده نمی شود وبرای مدیریت و سازماندهی ترافیک شبکه از آنها استفاده می شود .

تهدیدات و چگونگی نفوذ به شبکه در لایه های پایینی:

فهرستی از حملات که ممکن است در لایه های فیزیکی اتفاق افتد به صورت زیر میباشد :۱.قطع ارتباط فیزیکی و ایجاد یک اتصال جدید : به این تهدید نشت اطلاعات می گویند.۲.خواباندن شبکه در اثر خرابی کایل:به این حمله حمله dos می گویند.۳.استفاده از قالب های غیر فعال : از این نوع تهدید برای مرز اطلاعات استفاده می شود ۴.فریب کاری در rap :در همه تهدیدات از این آسیب پذیری استفاده می شود .۵.اشباع سوئیچ: از این روش برای حملات dos استفاده می شود .۶.پاسخ دروغ dms : از این روش برای عملیات های غیرقانونی استفاده می شود.

سوئیچ های غیرفعال به طور معمول به آنها هاپ می گوییم .تفاوت هاپ و سوئیچ در این است که هاپ هر بسته ای را که دریافت کرد آن را بر روی همه پورت های خود ارسال می کند تا کامپیوتر مورد نظر آن را بردارد اما در سوئیچ بسته دریافتی فقط با پورتی که مرتبط با آن است اطلاعات را ارسال می کند. برای شنود بر روی سوئیچ ها از فریب کاری arp استفاده می شود به این صورت که زمانی که سوئیچ آدرس مک سیستمی را تقاضا می کند کتمپیوتر هکر آدرس مک خود را در اختیار آن قرار میدهد.

روش های مقابله با سر ریز کردن مک :

اولین گام جلوگیری از دسترسی فیزیکی به تجهیزات شبکه است .در این روش باید تجهیزات شبکه از دسترس غیر مجاز توسط افراد ناشناس جلوگیری شود . گام دوم استفاده از ابزارهای مانیتور arp : در این روش جداول نگاشت آدرس کنترل می شوند تا از تغییرات در جدول مطمئن شویم اگر این تغییرات به صورت مکرر اتفاق بیفتذ نشان دهنده

احتمال حمله می باشد . گام سوم استفاده از آدرس مک به صورت دستی:در این روش به جای اینکه سوئیچ به صورت پویا جداول خود را تنظیم کند از روش دستی برای تنظیم جداول نگاشت استفاده می شود . این روش برای شبکه های با ابعاد کوچک مناسب است اما برای شبکه ها با تعداد کامپیوتر زیاد امکان پذیر نیست . زیرا با ورود هر سیستم جدید باید دوباره تنظیمات سوئیچ به صورت دستی انجام شود.گام چهارم:حفاظت هایی می باشد که پس از رخ دادن سر ریز بافر انجام می گیرد .گام پنجم ریست کردن پاک کردن جدول نگاشت آدرس می باشد .

چند نکته در زمینه افزایش ایمنی در مقابل تهدیدات فیزیکی:

۱.از کارت های شبکه استفاده کنید که امکان رفتن به حالت بی قید را ندهد

۲. سعی کنید به جای هاپ ها از سوئیچ استفاده کنید و از بین سوئیچ ها از سوئیچی استفاده شود که بتواند در مقابل حمله سرریز بافر مقاومت کند یعنی اگر جدول نگاشت آنها سرریز شد یا جدول را ریست کند یا از جدول ثابت و مطمئن استفاده کند .

۳.تغییر جدول به جای اینکه به صورت پویا انجام شود به صورت دستی انجام گیرد.

۴.رمزکردن ترافیک شبکهو استفاده از پروتکول ایمن به منظور رمزکردن اطلاعات .

تهدیدات لایه شبکه:

۱.فریب کاری به کمک پروتکل ip

۲.حمله source routing :این حمله در لایه ip انجام می شود اما اثرات آن در لایه دیگر نمایان میشود ping ofdetoh-joit-teardrop-icmp smur fing.

Ping ofdetoh **فریب کاری با استفاده از پروتکل** ip **:** در این روش آدرس ip بسته های اطلاعاتی به صورتی که ip فرستنده مشخص نباشد تغییر داده می شود .در این روش چون پروتکل tcp مقدار ip را کنترل نمی کند می تواند باعث بروز مشکلات شود در بسیاری از موارد تغیرآدرس ip و امکان قراردادن آدرس ip دیگر به جای آدرس ip واقعی می تواند شبکه را با مخاطراتی روبرو کند .

قراردادن آدرس ip **به غیر از آدرس** ip **مهاجم چه استفاده هایی می تواند داشته باشد:**

۱.مهاجم میتواند بسته هایی را با ip تکراری بر روی شبکه ارسال کند و به این طریق بدون نیاز به شناسه کاربری و رمزعبور می تواند به سایت ها وارد شود . در سایت های قدیمی با استفاده از نام کاربر ورمزعبور آدرسی ایجاد میشود که می توان به سایت وارد شده هکرها با کات کردن این آدرس می توانستند در هرزمانی به سیستم وارد شوند .برای مقابله با این مشکل بر روی بسته ها برچسب زمانی قرار میگیرد تا امکان جعل کردن احراز هویت نباشد.

۲.به این وسیله شخص مهاجم ناشناس باقی می ماند.

سوالات مطرح شده درس آشنایی با مبانی امنیت شبکه توسط استاد:

۱.هفت مورد از منابع شبکه را نام ببرید؟

۲.تفاوت روتر با سوئیچ چیست؟

۳.حمله را تعریف کنید؟

۴.انواع حمله را نام ببرید؟

۵.اهداف ایجاد امنیت چیست؟

۶.فاکتورهای اصلی در تحلیل خطر را نام ببرید؟

۷.نقش هایی که سیاست های امنیتی بر عهده دارد را نام ببرید؟

۸.طبقه بندی سیاست های امنیتی را توضیح دهید؟

۹.دلیل تعریف نواحی امنیتی چیست؟

۱۰.چرا امنیت تجهیزات شبکه مهم می باشد؟

۱۱.افزونگی در شبکه به چه معناست و چه اهمیتی دارد؟

۱۲.انواع تپولوژی شبکه را نام ببرید؟

۱۳.برای حفاظت فیزیکی از تجهیزات از چه تدابیری می توان استفاده کرد؟

۱۴.امن ترین کانال ارتباطی در حال حاضر کدام رسانه می باشد؟

۱۵.در ایجاد شبکه توزیع نیرو (منابع تغذیه)چه نکاتی را باید در نظر گرفت؟

۱۶منظور از امنیت منطقی چیست؟

۱۷.انواع حمله مسیریاب ها را بیان کنید؟

۱۸.به چه روش هایی می توان به تجهیزات شبکه دسترسی داشت؟وچگونه میتوان امنیت آنها را حفظ کرد؟

۱۹.ملزومات امنیتی را به اختصار شرح دهید؟

۲۰.با چه ابزاری می توان ملزومات امنیتی را رعایت کرد؟

۲۱.ضریب عملکرد را تعریف کنید؟

۲۲.وضایف فایروال چیست؟ سه مورد؟

۲۳.نحوه عملکرد آنتی ویروس چگونه است؟

۲۴.VPN را توضیح دهید؟

۲۵.سرآیندهای پروتکل IP یاد گرفته شود!دومورد در امتحان می آید!

۲۶.هدف پروتکل ICMP چیست؟

۲۷.سرآیندهای پروتکل ICMP یاد گرفته شود!دومورد در امتحان می آید!

۲۸.کاربرد پروتکل ARP چیست؟

۲۹. سرآیندهای پروتکل ARP یاد گرفته شود!دومورد در امتحان می آید!

۳۰.منظور از اتصال گرا بودن پروتکل TCP چیست؟

۳۱.سوکت چیست؟

۳۲.در پروتکل TCP چگونه ترتیب بسته های ارسالی مشخص می شود؟
۳۳.کاربرد بافرها چیست؟
۳۴.مزیت و عیب پروتکل TCIP در مقابل UDP چیست؟
۳۵.با چه دستوری میتوان پورت های باز را تعیین کرد؟
۳۶.برای یک بسته دریافتی توسط دیواره آتش چه اتفاقاتی ممکن است رخ دهد؟
۳۷.دیواره آتش در لایه IP چه عملی میتواند انجام دهد؟
۳۸در لایه TCP بر اساس ویژگی های کدام لایه تصمیم گیری می شود؟
۳۹.انواع دیواره آتش را نام ببرید؟
۴۰.دیواره آتش مبتی بر پراکسی را توضیح دهید؟
۴۱.کاربردنرم افزار pc anywai چیست؟
۴۲.با چه ابزاری می توان مودم های فعال را تعیین نمود؟
۴۳.برای جستجوی رمزعبوراز چه نرم افزاری استفاده می شود؟
۴۴.انواع روش پویش پورت را نام ببرید؟
۴۵.روش تعیین پورت های باز با استفاده از وسایل نامعتبر را توضیح دهید؟
۴۶.نرم افزار mal wair برای چگونه حمله هایی استفاده می شود؟
۴۷.اسب تراوا را توضیح دهید؟
۴۸.تفارت اسب تراوا با ویروس چیست؟
۴۹.چند نمونه از اسب تراوا را نام ببرید؟
۵۰.روش های انتشار ویروس را نام ببرید؟
۵۱.انواع ویروس را نام ببرید؟
۵۲.ویروس های چند ریختی را توضیح دهید؟
۵۳.تفاوت شنود فعال با غیر فعال چیست؟
۵۴.منظور از حالت غیر مقید در کارت شبکه چیست؟
۵۵.سوئیچ غیر فعال چیست؟
۵۶.فهرست فعالیت های حمله در لایه فیزیکی را نام ببرید؟
۵۷.سرریز بافر چیست؟
۵۸.روش های مقابله با سرریز کردن آدرس مک چیست؟
۵۹.نحوه مقابه با سرریز بافر را نام ببرید؟