نمونه سوالات درس نفوذگری شبکه استاد میر عابدینی زهرا میثاقیان

۱- بر اساس تعریف دانشگاه MIT هکر و کرکر چه تعریفی دارد؟ آنها را با مثال تشریح کنید؟

* Hacker یا نفوذگر کسی است که از سرکشی کردن به جزئیات سیستم‌های قابل برنامه ریزی و نفوذ و رسوخ در آن لذت می‌برد و مصمم به شکست دادن توانایی محاسباتی ماشین در مقابل هوش و ذکاوت بشری خویش است. فردی که با سماجت و به گونه‌ای لجوجانه شیفتهٔ برنامه نویسی است. نفوذگر، بدخواه نیست و صدمه نمی‌زند.
* Cracker موجود بی ارزش و بیماری است که با فراگیری برخی از مهارتهای نفوذگری به کارهای بی‌ارزشی همانند دزدیدن User ID & Password دیگران ، مزاحمت و عملیات غیرقانونی و ضد اخلاقی می‌پردازد و با شکستن حریم امنیت یک سیستم اهداف غیرشرافتمندانهٔ خود را دنبال می کند.

۲- انواع گروه های هکری را نام برده و ویژگی هر کدام از آن ها را بیان کنید؟

۱. گروه هَکِرها یا نفوذگران کلاه سفید (WhiteHat Hacker Group) : نفوذگران خوب!
۲. گروه نفوذگران کلاه سیاه (BlackHat Hacker Group) : نفوذگران بد و مخرّب!
۳. گروه نفوذگران کلاه خاکستری (GrayHat Hacker Group) : نفوذگران کمی خوب، اندکی مخرّب!
۴. گروه نفوذگران کلاه صورتی (PinkHat Hacker Group) : نفوذگران لوس ، بیمزه و بی خاصیت!

۳- ویژگی هکر کلاه سفید را بنویسید؟ ۷ مورد

۱. کلاه سفید هرگز به یک سیستم صدمه نمی زند .
۲. کلاه سفید هرگز به شبکه های دولتی یا امنیتی که مشغول انجام وظیفهٔ ملی هستند نفوذ نمی کند .
۳. کلاه سفید هرگز به فایلهای یک سیستم دستبرد نمی زند و سعی در انتقال آنها ندارد .
۴. کلاه سفید هرگز اثری از خود در سیستمی که بدان نفوذ کرده باقی نمی گذارد .
۵. کلاه سفید هرگز در مورد دانش و مهارتهای نفوذگری خود به کسی اطلاعات نمی دهد .(مگر افراد متخصص و مورد اطمینان ، آنهم به منظور بالا بردن مهارتهای تخصصی و تبادل افکار)
۶. کلاه سفید هیچگاه بر روی شبکهٔ اینترنت در مورد جزئیات نفوذگری خود اطلاعاتی مبادله نمی کند .
۷. کلاه سفید برای بار دوم به سیستمی که یکبار رخنه کرده است نفوذ نمی کند . (هیچ کلاه سفید عاقلی یک مسئله را دو بار حل نمی کند!)
۸. ممارست ، پشتکار و شکیبایی اصول اساسی عملیات یک نفوذگر کلاه سفید است .
۹. کلاه سفید باید به اندازهٔ دیگران خلاقیت داشته باشد و حداقل یکبار روشی نو ارائه کند!

۴- انواع تهدید های بالقوه برای امنیت شبکه های کامپیوتری کدامند؟

۱. فاش شدن غیر مجاز اطلاعات در نتیجهٔ استراق سمع داده ها یا پیام های در حال مبادله روی شبکه
۲. قطع ارتباط و اختلال در شبکه به واسطه یک اقدام خرابکارانه
۳. تغییر و دستکاری غیر مجاز اطلاعات یا یک پیغام ارسال شده

۵- هر یک از مفاهیم و اصطلاحات زیر بعنوان سرویس های شبکه را با ذکر مثال توضیح دهید؟

۱. محرمانه ماندن اطلاعات (Confidentiality) : دلایل متعددی برای یک سازمان یا حتی یک فرد عادی وجود دارد که بخواهد اطلاعات خود را محرمانه نگاه دارد. مثال: رمز اول و دوم بانکی ، رمز ایمیل
۲. احراز هویت (Authentication): قبل از آنکه محتوای یک پیام یا اطلاعات اهمیت داشته باشد باید مطمئن شوید که پیام حقیقتاً از شخصی که تصور می کنید رسیده است و کسی قصد فریب و گمراه کردن یا (آزار) شما را ندارد. مثال: آیا پیام های آمده از طرف شخص مورد نظر است یا خیر مانند پیامک درخواست رمز از طرف دوست شما می باشد.
۳. سلامت داده ها (Integrity): یعنی دست نخوردگی و عدم تغییر پیام و اطمینان از آنکه داده ها با اطلاعات مخرب مثل یک ویروس کامپیوتری آلوده نشده اند. مثال: داده ها کامل از طرف دوست شما ارسال شده به شما برسد.
۴. کنترل دسترسی (Access Control): یعنی بتوان دسترسی افرادی غیرمُجاز به شبکه را با دقت کنترل کرد و توانایی منع افراد غیر قابل اعتماد از دسترسی به شبکه ، وجود داشته باشد. به آن Authorization به معنای مجوز. مثال: اپراتور یا تایپیست حق تغییر مطلب را ندارد و فقط مجوز تایپ دارد.
۵. در دسترس بودن (Availability): با این تفاصیل ، باید تمام امکانات شبکه بدون دردسر و زحمت در اختیار آنهائی که مجاز به استفاده از شبکه هستند ، باشد و در ضمن هیچکس نتواند در دسترسی به شبکه اختلال ایجاد کند. مثال: سیستم بانکی، موبایل، در اینترنت مانند گوگل ، سیستم‌های آنلاین مانند خطوط هواپیمایی

۶- انواع مکانیزم های حملات در یک شبکه کامپیوتری کدام است آن ها را نام ببرید و به اختصار توضیح دهید؟

۱. حمله از نوع وقفه (Interruption) : بدین معنا که حمله کننده باعث شود شبکه مختل شده و مبادله اطلاعات امکان پذیر نباشد.
۲. حمله از نوع استراق سمع (Interception/Eavesdropping) : بدین معنا که حمله کننده به نحوی توانسته اطلاعات در حال تبادل روی شبکه را گوش داده و بهره برداری نماید.
۳. حمله از نوع دستکاری داده ها (Modification) : یعنی حمله کننده توانسته به نحوی اطلاعاتی که روی شبکه مبادله می شوند را تغییر دهد یعنی داده هایی که در مقصد دریافت می شود متفاوت با آن چیزی باشد که از مبداء ارسال شده است.
۴. حمله از نوع افزودن اطلاعات (Fabrication) : یعنی حمله کننده اطلاعاتی را که در حال تبادل روی شبکه است تغییر نمی دهد بلکه اطلاعات دیگری را که میتواند مخرب یا بنیانگذار حملات بعدی باشد، به اطلاعات اضافه می نماید (مثل ویروسها)

۷- نفوذگرها به دو طریق به شبکه حمله می کنند این دو نوع حمله کدامند با مثال؟

به حملهای که هنگام شروع با بروز اختلال در شبکه علنی می شود و در کار ارسال یا دریافت داده ها مشکل ایجاد می کند "حمله فعال (Active)" می گویند . بر عکس حملهای که شبکه را با اختلال مواجه نمی کند و ظاهراً مشکلی در کار ارسال و دریافت بوجود نمی آورد "حمله غیر فعال (Passive) " نامیده می شود و از خطرناکترین انواع حمله به شبکه به شمار می رود.

۸- الف)انگیزه های ناشی از نفوذگری در شبکه چه می باشد؟ (۶ مورد) ب) مهم ترین دشمنان داخلی که عملیات نفوذگری در شبکه سازمانی را انجام می دهند کدامند؟

- انگیزه های رقابتی ناسالم ، انتقام جوئی و ضربه زدن به رقیب
- اهداف سیاسی
- اهداف تروریستی و کسب اخبار جهت اعمال خرابکارانه و موذیانه
- اهداف دولتی
- کسب نامشروع ثروت از طریق جابجا کردن مستقیم پول و اعتبار از حسابهای بانکی و دزدیدن
- شماره کارتهای اعتباری
- تفریح یا اندازهگیری ضریب توانائی فردی یا کنجکاوی (معمولاً دانشجویان)
- دزدیدن دانشی که برای تهیه آن بایستی صرف هزینه کرد. (راهزنان دانش)
- آزاررسانی و کسب شهرت از طریق مردم آزاری (بیماران روانی)
- جاسوسی و کسب اطلاع از وضعیت نظامی و سیاسی یک کشور یا منطقه
- رقابت ناسالم در عرصه تجارت و اقتصاد

مهمترین این دشمنان داخلی در گروههای زیر دسته بندی می شوند:

- کارمندان ناراضی
- مشتریان ناراضی یا طماع با اهداف سودجویی یا انتقام گیری
- پیمانکاران یا مشاورین شبکه با انگیزۀ اخاذی
- شرکای تجاری با انگیزۀ سودجویی

۹- به طور کلی سطوح مهارت نفوذگران از لحاظ سطح دانش و فنی به چند گروه تقسیم بندی می شوند آن ها را نام برده و به اختصار توضیح دهید؟

۱- بی تجربه :

گروه اول، نفوذگران بی تجربه ، جوان و ماجراجویی هستند که اصطلاح کودک (Kindergartner) بیشتر برازندۀ آنهاست تا نفوذگر! آنها را در محیط های گپ اینترنتی (Chatroom) به وفور می یابید. این گروه بیش از همه ادعا دارند، در مورد کارهای بی ارزش خود داستان می سازند و هدفی جز عقده گشایی ، خودنمایی و تلف کردن زمان با هیجان های کاذب ندارند. اینان بی آنکه حوصله خواندن چند صفحۀ کتاب داشته باشند بصورت تقلیدی از ابزارهای نفوذگری بهره می گیرند.

مقابله با این افراد کار مشکلی نیست. با تکیه بر روشهای فنی یا اِعمال قانون آنها را تنبیه کنید تا یاد بگیرند شبکه جولان گاه افراد بی تخصص نیست!!

۲- متوسط :

گروه دوم ، نفوذگرانی هستند که بر اساس ذوق و علاقۀ شخصی با یک سیستم عامل و برخی از اصول فنی اینترنت آشنا شده اند و در سطح معلومات متوسطی هستند. جولان گاه آنها بطور، معمول سرویس دهنده های وب FTP و گروههای خبری است. این گروه از نفوذگران قادرند نقاط ضعف سیستم‌ها را کشف کنند و از آن طریق در سیستمی نفوذ یا به آن حمله کنند ولی قادر به خلق ابزار یا تکنیک جدیدی برای رسوخ در سیستم‌ها نیستند.

مقابله با این گروه اگرچه هزینۀ اقتصادی و روانی به شما تحمیل می کند ولی غیرممکن نیست.

۳- خبره :

گروه سوم ، نفوذگران خبره و هوشمندی هستند که کمتر هیاهو می کنند در حالی که پیچیده‌ترین تکنیکها و تاکتیکهای نفوذ و حمله را ابداع می نمایند. بر بعضی از شبکه ها برای مدتهای طولانی سیطره دارند امّا هیچ ردّ پایی بجا نمی گذارند و در حدّ کمال به برنامه نویسی مسلطند و هیچگاه کور و بی هدف دست به حمله نمی زنند ضمن اینکه در هدف خود مصمم و شکیبا هستند.

مقابله با این نفوذگران ساده نیست و برای مدیران شبکه های حساس یک کابوس شده است !لذا سعی می کنند برای مقابله با حملات آنها از خودشان استفاده کنند!

۱۰- مهمترین مسئله طراحی شبکه ها و مشکلاتی که در آن ها ممکن است بوجود آید کدام است آن ها را بنویسید؟ ۵ مورد

۱- موضوع چگونگی ارسال و دریافت بیت های اطلاعات:

اولین موضوع چگونگی ارسال و دریافت بیتهای اطلاعات بصورت یک سیگنال الکتریکی ، الکترومغناطیسی یا نوری است، بسته به اینکه آیا کانال انتقال سیم مسی ، فیبر نوری ، کانال ماهوارهای یا خطوط مایکروویو است. بنابراین تبدیل بیتها به یک سیگنال متناسب با کانال انتقال یکی از مسائل اولیهٔ شبکه به شمار می رود.

۲- موضوع ماهیت انتقال:

مساله دوم ماهیت انتقال است که می تواند به یکی از سه صورت زیر باشد:

- Simplex: ارتباط یکطرفه (یک طرف همیشه گیرنده و طرف دیگر همیشه فرستنده) مانند ماهواره.
- Half Duplex : ارتباط دوطرفهٔ غیرهمزمان (هر دو ماشین هم میتوانند فرستنده یا گیرنده باشند ولی نه بصورت همزمان ، بلکه یکی از طرفین ابتدا ارسال می کند ، سپس ساکت می‌شود تا طرف مقابل ارسال داشته باشد). مانند تلگراف، دستگاه واکی تاکی
- Full Duplex : ارتباط دو طرفه همزمان (مانند خطوط مایکروویو) مانند خط تلفن

۳- موضوع خطا و وجود نویز روی کانال های ارتباطی:

مساله سوم مسئلهٔ خطا و وجود نویز روی کانالهای ارتباطی است بدین معنا که ممکن است در حین ارسال داده ها بر روی کانال فیزیکی تعدادی از بیتها دچار خرابی شود؛ چنین وضعیتی که قابل اجتناب نیست باید تشخیص داده شده و داده های فاقد اعتبار دور ریخته شود مبدأ آنها را از نو ارسال کند.

۴- موضوع وجود مسیرهای مختلف بین مبدا و مقصد:

با توجه به اینکه در شبکه ها ممکن است مسیرهای گوناگونی بین مبدأ و مقصد وجود داشته باشد؛ بنابراین پیدا کردن بهترین مسیر و هدایت بسته ها ، از مسائل طراحی شبکه محسوب می شود. در ضمن ممکن است یک پیام بزرگ به واحدهای کوچکتری تقسیم شده و از مسیرهای مختلفی به مقصد برسد بنابراین بازسازی پیام از دیگر مسائل شبکه به شمار می آید.

۵- موضوع هماهنگی و کنترل جریان بین مبدا و مقصد:

ممکن است گیرنده به دلایلی نتواند با سرعتی که فرستنده بستههای یک پیام را ارسال می کند آنها را دریافت کند ، بنابراین طراحی مکانیزم های حفظ هماهنگی بین مبدأ و مقصد از دیگر مسائل شبکه است.

۶- موضوع کنترل اذهام، تداخل و تصادم در شبکه:

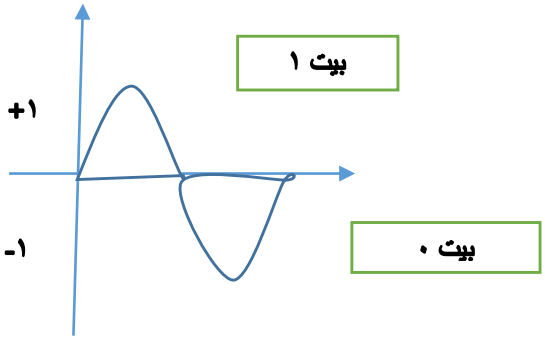
چون ماشینهای فرستنده و گیرندهٔ متعددی در یک شبکه وجود دارد مسائلی مثل ازدحام ، تداخل و تصادم در شبکه ها بوجود می آید که این مشکلات به همراه مسائل دیگر باید در سخت افزار و نرم افزار شبکه حل شود.

نکته: روش های ارسال به ترتیب صفر و یک

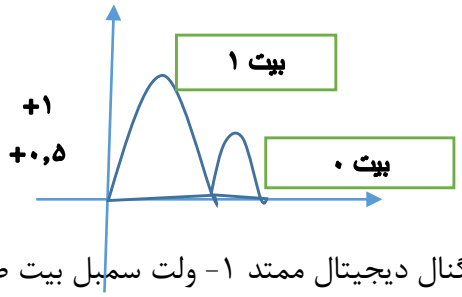
۱- روش منچستر (manchester) : در این روش دو سیگنال دیجیتال به ترتیب صفر و یک یا لبه بالا رونده بیت یک را نشان می دهد و دو سیگنال دیجیتال یک و صفر یا لبه پایین رونده بیت صفر را نشان می دهد.

* در هنگام آسیب دیدگی هر دو سیگنال باید خراب یا آسیب ببینند.

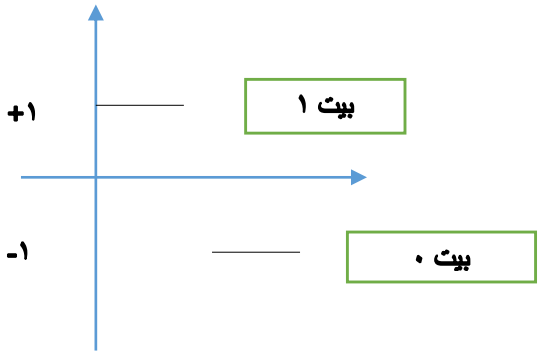
۲- روش ۱+ و ۱- ولت : سیگنال سینوسی ۱+ ولت گویای بیت یک و سیگنال سینوسی ۱- ولت گویای بیت صفر است.



۳- روش Hi/Lw ولتاژ : High ولتاژ بین (0.5,1) ولت است بیت یک را نشان می دهد. Low بین (0.1,0.5) بیت صفر را نشان می دهد.



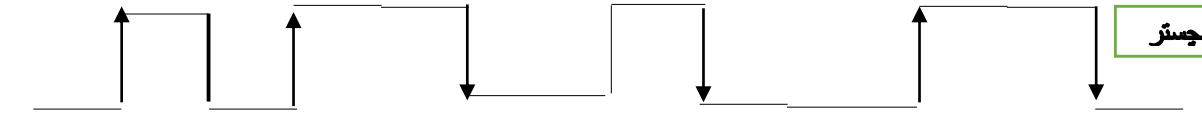
۴- سیگنال ممتد یک ولت نمایش بیت یک و سیگنال دیجیتال ممتد ۱- ولت سمبل بیت صفر می باشد.

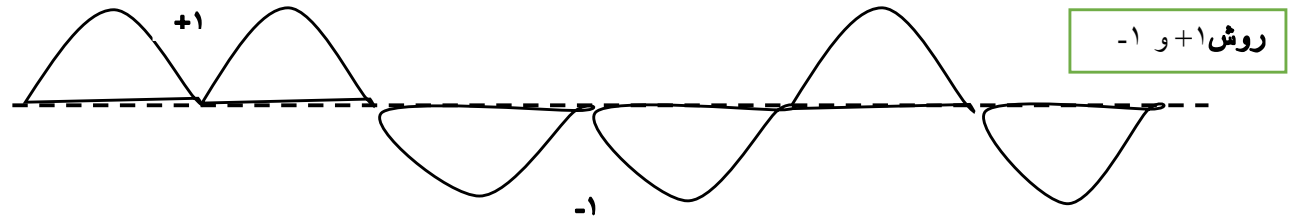


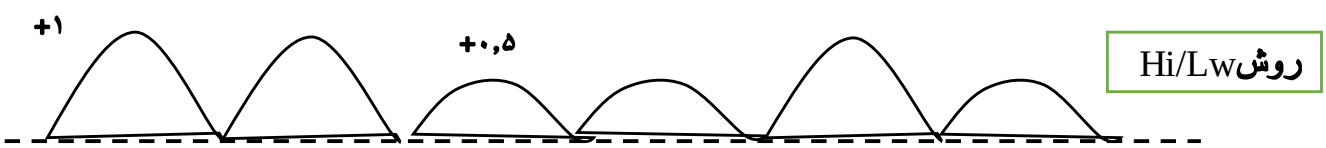
۵- فیبر نوری

مثال به ۴ روش فوق بیت های ۱۱۰۰۱۰ را نشان دهید؟

1	1	0	0	1	0







روش منچستر : مزایا : امنیت و اطمینان بالا است چون هر دو سیگنال حاصل یک بیت است
معایب : سرعت پایین هست

روش دیجیتال : مزایا : سرعت بالا، دقت نسبی چون هر دو سیگنال حاصل یک بیت است. اختلاف ۲
معایب : احتمال خطا

روش ۱+ و ۱- : مزایا : سرعت و دقت نسبی چون هر دو سیگنال حاصل یک بیت است. اختلاف ۲
معایب : احتمال خرابی

روش Hi/Lw : مزایا : ارسال بیت مزایا ندارد اختلاف ۰,۵ است
معایب : احتمال خرابی و تغییر بالا است. از این روش استفاده نمی کنند مگر تکنولوژی درون سیمی

۱۱- استفاده از طراحی لایه شبکه چه ویژگی ها و اصولی دارد؟

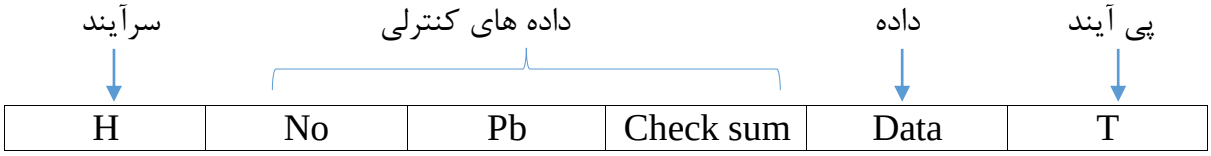
- هر لایه وظیفه مشخصی دارد و طراح شبکه باید آنها را به دقت تشریح کند.
- هرگاه سرویس هایی که باید ارائه شود از نظر ماهیتی متفاوت باشد ، باید لایه به لایه و جداگانه طراحی شود.
- وظیفه هر لایه باید با توجه به قراردادها و استانداردهای جهانی مشخص شود.
- تعداد لایه ها نباید آنقدر زیاد باشد که تمایز لایه ها از دیدگاه سرویسهای ارائه شده نامشخص باشد و نه آنقدر کم باشد ، که وظیفه و خدماتِ یک لایه ، پیچیده و نامشخص شود.
- در هر لایه جزئیات لایه های زیرین نادیده گرفته می شود و لایه های بالایی باید در یک روال ساده و ماجولار از خدمات لایهٔ زیرین خود استفاده کنند.
- باید مرزهای هر لایه به گونه ای انتخاب شود که جریان اطلاعات بین لایه ها ، حداقل باشد.

۱۲- مدل هفت لایه ای OSI را ترسیم نمایید و لایه ها را به اختصار توضیح دهید؟

لایه فیزیکی : انتقال بیت های صفر و یک با استفاده از سیگنال از مبدا به مقصد(۵ نوع سیگنال)

لایه پیوند داده : ۱- فریم بندی یعنی داده ها را از لایه شبکه می گیرد در قالب فریم درآورده و بصورت صفر و یک به لایه فیزیکی می دهد تا ارسال شود. ۲- کنترل جریان داده بین مبدا و مقصد (یعنی اینکه فرستنده پر سرعت ابتدا با گیرنده کم سرعت ارتباط برقرار نمود و فریم ها با توجه به توانمندی و میزان دریافت گیرنده می فرستد تا ازدهام موجود نیاید). ۳- کنترل خطا یعنی چک می کند که فریمی دریافت نمود بین راه دچار خطا نشده است. روش های کشف خطا با اضافه کردن بیت های کنترل مانند CRC ، Check sum و Parity انجام می شود.

ساختار کلی فریم در لایه پیوند داده بصورت زیر است:



روش Parity : دو نوع بیت توازن داریم توازن زوج و توازن فرد است. مثلا در توازن زوج می گوییم بایستی کل فریم تعداد یک های آن زوج باشد و در توازن فرد می گوییم کل بیت های فریم تعداد یک های آن باید فرد باشد. بنابراین یک بیت به عنوان بیت توازن اضافه می کنیم.

نکته : بیت توازن تنها می تواند تعداد خطاهای فرد را تشخیص دهد.

مثال: مشخص کنید که بیت Parity چه باید باشد؟

توازن زوج Even Parity

Pb

1	001101

0	00111100

توازن فرد Odd Parity

1	1010101

0	00111011

روش Check sum : در این روش فرض کنیم که اندازه ۵ بیتی است لذا داده های فریم را بصورت دسته های ۵ بیتی زیر هم قرار می دهیم و Xor می کنیم و نتیجه را در فیلد Check sum ذخیره می کنیم آنگاه فریم با Check sum ارسال می شود. در مقصد Check sum محاسبه می شود و با مقدار Check sum موجود در فریم مقایسه می گردد. اگر یکسان بود یعنی خرابی رخ نداده است و اگر متفاوت بود خطا رخ داده است.

مثال: می خواهیم ۱۷ بیت زیر را با روش Check sum کنترل و ارسال نمایم اگر Check sum ۵ بیت باشد مقدار آن کدام است؟

پاسخ: ابتدا تعداد بیت ها را ضریبی از بیت ها Check sum قرار دهیم با اضافه کردن بیت های کم ارزش سمت چپ پر می کنیم.

تعریف Xor هر گاه مقدار هر بیت ورودی متفاوت باشند یک است و در غیر اینصورت صفر است.

۱ ⊕ ۱ = ۰ ۰ ⊕ ۱ = ۱ ۰ ⊕ ۰ = ۰ ۱ ⊕ ۰ = ۱ ۱ ⊕ ۱ = ۰

01111001001101010
00001 11100 10011 01010

01010
Xor 10011
11100
00001

00100

Check sum

00100

نکته ۱ : هر گاه در هر ستون تعداد یک ها فرد باشد خروجی یک است در غیر این صورت صفر است.
نکته ۲ : اگر در یک ستون دو خطا رخ دهد قابل تشخیص نیست.
تمرین اگر در مثال قبل ۱۷ بیتی اندازه Check sum الف) ۸ بیت ب) ۴ بیت باشد مقدار نهایی Check sum کدام است؟ اگر بیت های چهارم ، هشتم و ۱۲ دچار خرابی شوند آیا مقصد قادر به کشف خطا خواهد بود؟

الف) ۸ بیت

01111001001101010

00000000 11110010 01101010

$$\begin{array}{r} 01101010 \\ \oplus\ 11110010 \\ 00000000 \\ \hline 10011000 \end{array}$$

Check sum

10011000

خرابی

$$\begin{array}{r} 11100010 \\ \oplus\ 11111010 \\ 00000000 \\ \hline 00011000 \end{array}$$

قابل تشخیص است چون بیت هشت خراب شده در ستون آخر باعث شده که بیت حاصل تغییر کند. ولی در ستون ۴ چون دو بیت خراب شده بیت حاصل شده قابل تشخیص نیست و اگر در سوال بیت ۸ نبود خرابی قابل تشخیص نبود.

Check sum

10011000

بعد خرابی

Check sum

00011000

ب) ۴ بیتی

01111001001101010

0000 1111 0010 0110 1010

$$\begin{array}{r} 1010 \\ 0110 \\ \oplus \quad 0010 \\ 1111 \\ 0000 \\ \hline 0001 \end{array}$$

Check sum

0001

بعد خرابی

$$\begin{array}{r} 0010 \\ 1110 \\ \oplus \quad 1010 \\ 1111 \\ 0000 \\ \hline 1001 \end{array}$$

Check sum

0001

Check sum

1001

قابل تشخیص است چون Check sum بعد خرابی تغییر کرده.

لایه شبکه : مهم ترین وظیفه این لایه این است که بسته های داده را از مبدا به مقصد مسیر دهی کند. این لایه توسط دستگاه هایی مانند مسیریاب (Router) همواره بهترین مسیرهای ممکن را یافته و در جدول مسیریابی خود ذخیره می کند. لذا با دیدن یک بسته داده یا Packet مسیریاب سریعا بسته وارده را با توجه به آدرس مقصد آن بر روی پورت خروجی مقصد آن قرار می دهد.

ساختا کلی یک بسته:

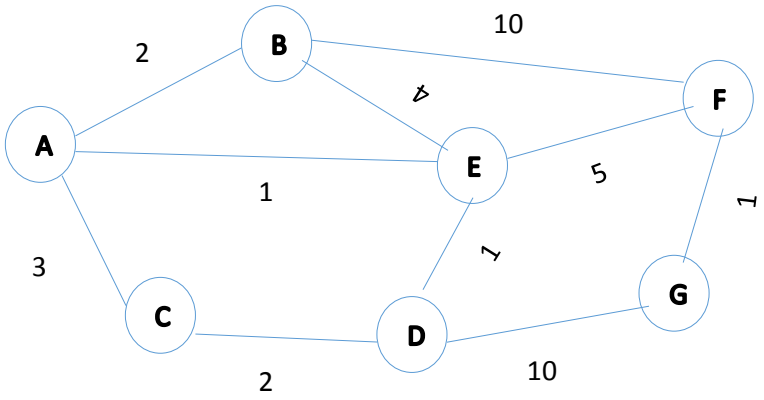
سرآیند	مبدا	مقصد	طول عمر	اولویت	داده	پی آیند
H	SRC	DST	TTL	PRIO	Data	T

اولویت : میزان اهمیت یک بسته

طول عمر : مدت زمان اعتبار یک بسته

مثال: مشخص کنید که جدول مسیریابی گره ABCDEFG حاوی چه رکوردهایی می باشد؟

هر گره را مبدا تصور کنید و جدول مسیریابی را پر کنید؟



گره A :

مقصد	بعدی	هزینه	تعداد HOP
Dst	Next	Cast	Hop Count
A	-	0	0
B	B	2	1
C	C	3	1
D	E	2	2
E	E	1	1
F	E	4	4
G	E	3	3

از A به B ۶ راه وجود دارد که باید کم هزینه ترین را انتخاب کنیم.

	تعداد HOP	هزینه
A -- B	2	1
A -- E -- B	5	2
A -- C -- D -- E -- B	10	4
A -- E -- F -- B	16	3
A -- C -- D -- G -- F -- B	17	5
A -- C -- D -- G -- F -- E – B	16	6

چون ترافیک زیادی را E دریافت می کند با عث می شود که از کار بیفتد و باعث از کار افتادن شبکه می شود. همچنین در هر گره میانی احتمال حمله است و دارای خطر می باشد و هر چقدر تعداد HOP در هر مسیر بیشتر باشد احتمال حمله بیشتر است.

گره B:

مقصد	بعدی	هزینه	تعداد HOP
Dst	Next	Cast	Hop Count
B	-	0	0
A	A	2	1
C	A	5	2
D	A	4	3
E	A	3	2
F	A	6	5
G	A	5	4

گره C:

مقصد	بعدی	هزینه	تعداد HOP
Dst	Next	Cast	Hop Count
C	-	0	0
A	A	3	1
B	A	5	2
D	D	2	1
E	D	3	2
F	D	4	3
G	D	3	2

گره D:

مقصد	بعدی	هزینه	تعداد HOP
Dst	Next	Cast	Hop Count
D	-	0	0
A	E	2	2
B	E	4	3
C	C	2	1
E	E	1	1
F	G	2	2
G	G	1	1

گره E:

مقصد	بعدی	هزینه	تعداد HOP
Dst	Next	Cast	Hop Count
E	-	0	0
A	A	1	1
B	A	3	2
C	D	3	2
D	D	1	1
F	D	3	3
G	D	2	2

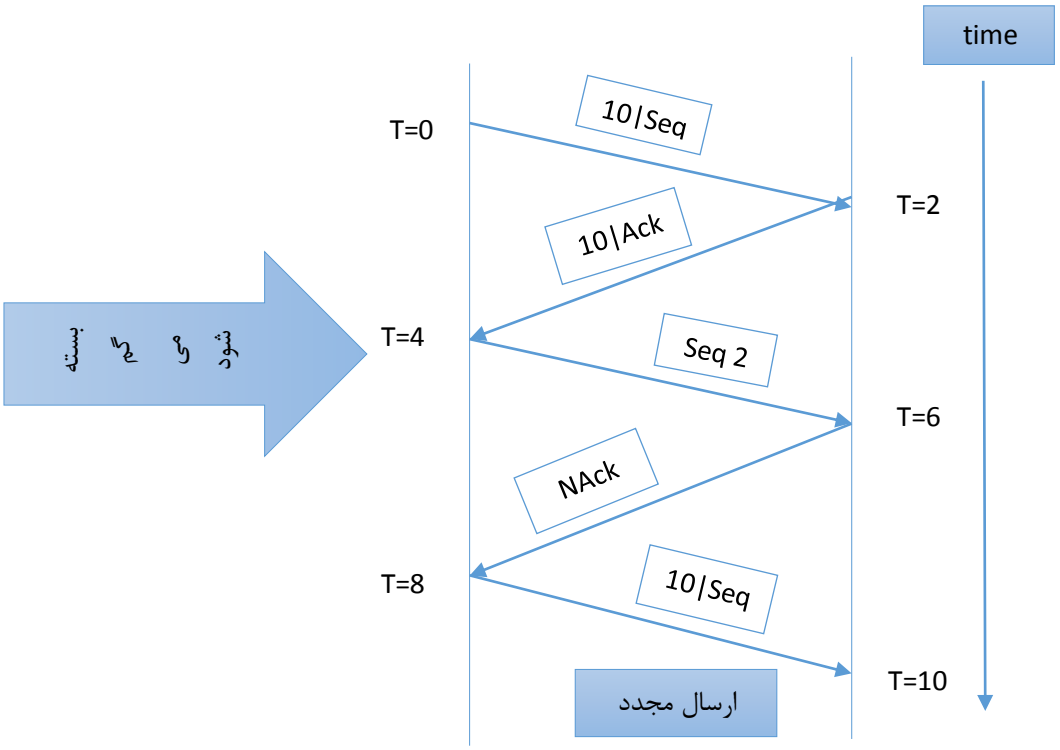
گره F:

مقصد	بعدی	هزینه	تعداد HOP
Dst	Next	Cast	Hop Count
F	-	0	0
A	G	4	4
B	G	6	5
C	G	4	3
D	G	2	2
E	G	3	3
G	G	1	1

گره G:

مقصد	بعدی	هزینه	تعداد HOP
Dst	Next	Cast	Hop Count
G	-	0	0
A	D	3	3
B	D	5	4
C	D	3	2
D	D	1	1
E	D	2	2
F	F	1	1

لایه انتقال: مهم ترین وظیفه این لایه آن است که کیفیت خدمت (Qos) در شبکه تضمین نماید. واحد انتقال داده در این لایه سگمنت (segment) است. در واقع داده ها از لایه فوقانی وارد این لایه شده و در قالب قطعه قرار گرفته و یک شماره ترتیب (seq.no) به آن ها تخصیص می یابد. زمانی که مقصد این قطعه را می گیرد بر اساس seq.no آن اعلان وصول (Ack) می نماید و اگر قطعه ای گم شود و فرستنده آن را عدم اعلان وصول (NAck) می نماید تا ماشین مبدا مجدد آن را بفرستد.
همچنین لایه انتقال وظیفه دارد که قطعات داده را به نحوی ارسال نماید که این قطعات سالم و مرتب و منظم و بدون تاخیر به مقصد برسند.



لایه نشست (جلسه): این لایه وظیفه دارد که تنظیمات مربوط به برقراری جلسات، ثبت جلسات، تعیین زمان شروع، زمان خاتمه جلسه و سایر اطلاعات مربوط به این نشست را ثبت و گزارش نماید. مثل مسئول دفتر که مسائل مربوط به تنظیم اسناد را انجام می دهد.

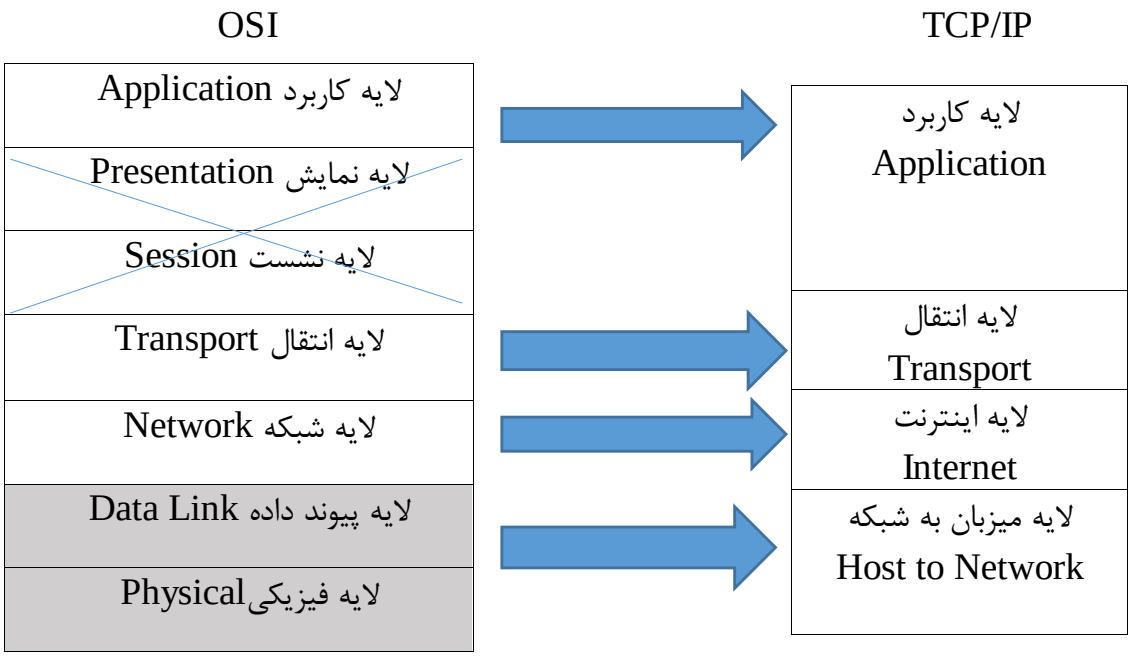
لایه نمایش: این لایه وظیفه دارد اولا فرمت و قالب داده را بین ماشین مبدا و مقصد را بر اساس استاندارد تعیین شده یکسان نماید. مثلا اگر ماشین مبدا با فرمت ANSI داده را می فرستد اما ماشین مقصد تنها با فرمت UTF8 داده را بتواند بخواند این لایه تبدیل فرمت ANSI به UTF8 را انجام می دهد. همچنین برای حالت ارتباط مقصد به مبدا تبدیل فرمت بصورت معکوس انجام می شود. وظیفه دوم لایه ارائه یا نمایش عملیات رمزنگاری بر روی داده ها می باشد. یعنی داده ها می باشد یعنی داده ها هنگام ارسال از ماشین مبدا ابتدا رمزنگاری می شوند با رسیدن به مقصد داده های رمز شده با توجه به پروتکل مشترک رمزگشایی می گردند.

لایه کاربرد: این لایه وظیفه دارد در قالب برنامه کاربردی سرویس ها و خدمات شبکه را در اختیار برنامه ها، نرم افزاران و کاربران قرار می دهد. پروتکل هایی زیر در این لایه می باشند.

انتقال فایل(شماره پورت ۲۱)	FTP(File Transport Protocol)
صفحات وب(شماره پورت ۸۰)	HTTP(Hypertext Transfer Protocol)
انتقال دهنده ایمیل(شماره پورت ۲۵)	SMTP(Simple Mail Transfer Protocol)
انتقال دهنده پست الکترونیک (شماره پورت ۱۱۰)	POP(Post Office Protocol)

۱۳- مدل TCP/IP را بیان کنید؟

مدل TCP/IP مشابه مدل OSI می باشد فقط هفت لایه OSI به چهار لایه کاهش می یابد. شکل مدل را نشان می دهد.



لایه یک شامل ترکیب دو لایه فیزیکی و پیوند داده می باشد و تحت عنوان میزبان به شبکه معرفی شده است. مثل کارت شبکه در رایانه مثالی از این شبکه است.

لایه فیزیکی : انتقال بیت های صفر و یک با استفاده از سیگنال از مبدا به مقصد(۵ نوع سیگنال)

لایه پیوند داده : ۱- فریم بندی یعنی داده ها را از لایه شبکه می گیرد در قالب فریم درآورده و بصورت صفر و یک به لایه فیزیکی می دهد تا ارسال شود. ۲- کنترل جریان داده بین مبدا و مقصد (یعنی اینکه فرستنده

پر سرعت ابتدا با گیرنده کم سرعت ارتباط برقرار نمود و فریم هابا توجه به توانمندی و میزان دریافت گیرنده می فرستد تا ازدهام موجود نیاید). ۳- کنترل خطا یعنی چک می کند که فریمی دریافت نمود بین راه دچار خطا نشده است. روش های کشف خطا با اضافه کردن بیت های کنترل مانند CRC ، Check sum و Parity انجام می شود.

لایه اینترنت: وظایف آن دقیقا مانند لایه شبکه است. مهم ترین وظیفه این لایه این است که بسته های داده را از مبدا به مقصد مسیر دهی کند. این لایه توسط دستگاه هایی مانند مسیریاب (Router) همواره بهترین مسیرهای ممکن را یافته و در جدول مسیریابی خود ذخیره می کند. لذا با دیدن یک بسته داده یا Packet مسیریاب سریعا بسته وارده را با توجه به آدرس مقصد آن بر روی پورت خروجی مقصد آن قرار می دهد.
وظایف آن با لایه انتقال مدل OSI یکی است.

لایه انتقال: مهم ترین وظیفه این لایه آن است که کیفیت خدمت (Qos) در شبکه تضمین نماید. واحد انتقال داده در این لایه سگمنت (segment) است. در واقع داده ها از لایه فوقانی وارد این لایه شده و در قالب قطعه قرار گرفته و یک شماره ترتیب (seq.no) به آن ها تخصیص می یابد. زمانی که مقصد این قطعه را می گیرد بر اساس seq.no آن اعلان وصول (Ack) می‌نماید. و اگر قطعه ای گم شود و فرستنده آن را عدم اعلان وصول (NAck) می نماید تا ماشین مبدا مجدد آن را بفرستد.

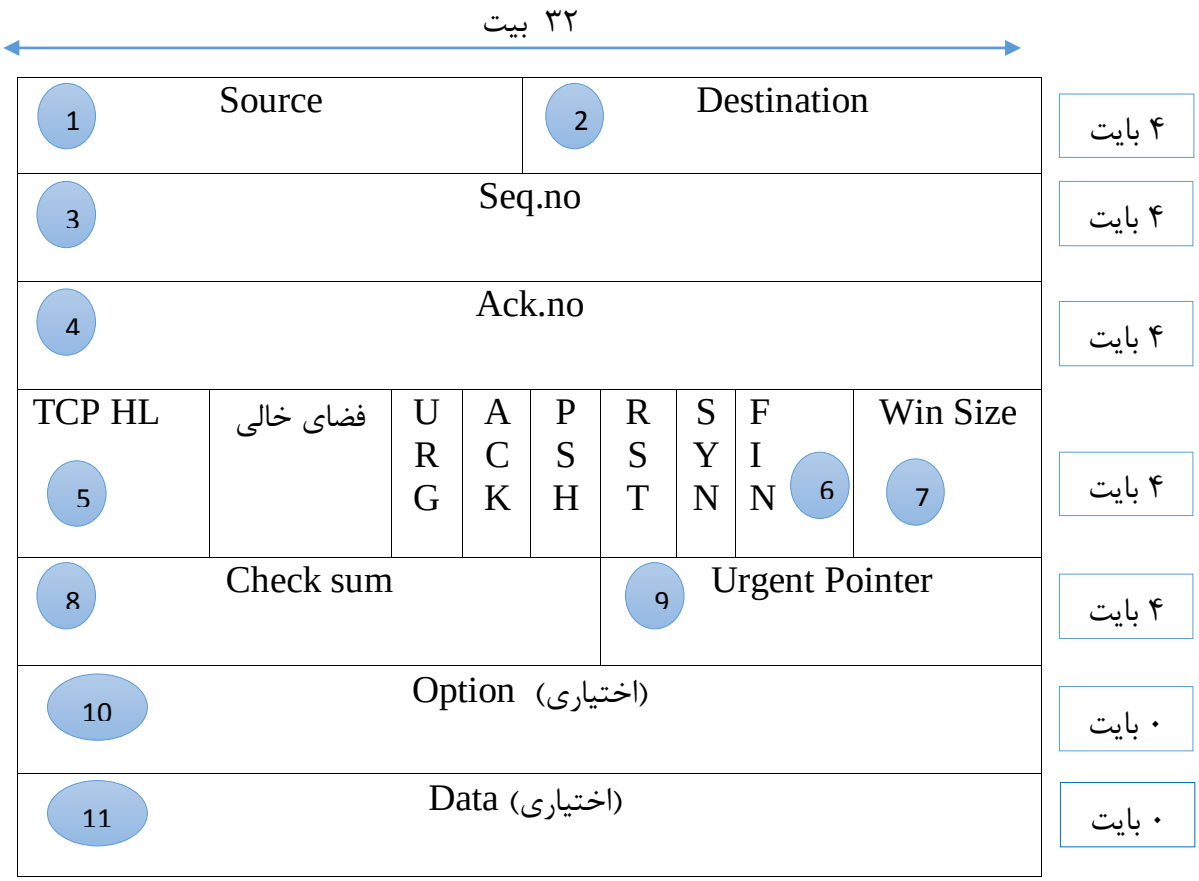
لایه کاربرد: در برخی مواقعه عملیات رمزنگاری نیز در این لایه انجام می شود.

این لایه وظیفه دارد در قالب برنامه کاربردی سرویس ها و خدمات شبکه را در اختیار برنامه ها، نرم افزاران و کاربران قرار می دهد. پروتکل هایی زیر در این لایه می باشند.

انتقال فایل(شماره پورت ۲۱)	FTP(File Transport Protocol)
صفحات وب(شماره پورت ۸۰)	HTTP(Hypertext Transfer Protocol)
انتقال دهنده ایمیل(شماره پورت ۲۵)	SMTP(Simple Mail Transfer Protocol)
انتقال دهنده پست الکترونیک (شماره پورت ۱۱۰)	POP(Post Office Protocol)

۱۴- قالب قطعه TCP چیست؟

قطعه TCP که در لایه انتقال وظیفه انتقال داده ها بصورت تضمین شده و با کیفیت را بر عهده دارد که شامل ۱۱ بخش کلی به صورت زیر می باشد. شناخت فیلدها و مشخصات این قطعه مهم است که نفوذ از اینجا انجام می شود.



اگر نفوذگر قطعه TCP را دستکاری کند و تغییرات ناشی یا کم باشد نفوذگر از نوع کلاه خاکستری است. اگر تغییرات مخرب و هدفمند انجام دهد از نوع کلاه سیاه است. و اگر بسته را بگیرد و بطور هرزنامه بفرستند کلاه صورتی است.

پنج سطر اول قطعه TCP همیشه ۲۰ بایت است ولی دو سطر آخر اختیاری می باشد.

اجزاء یا فیلدهای قطعه TCP به شرح زیر می باشد:

۱- Source (مبدا):

آدرس پورت مبدا است و یک عدد ۱۶ بیتی می باشد.

۲- Destination (مقصد):

آدرس پورت مقصد است و یک عدد ۱۶ بیتی می باشد.

نکته ۱ : چون یک پورت پردازشی ۱۶ بیت است ما می توانیم ۶۵۵۳۵ پورت تعریف کنیم. بنابراین یک سرور می تواند همزمان از چندین پورت پردازشی داده دریافت و یا ارسال نماید.

انتقال فایل(شماره پورت ۲۱) FTP(File Transport Protocol)

صفحات وب(شماره پورت ۸۰) HTTP(Hypertext Transfer Protocol)

انتقال دهنده ایمیل(شماره پورت ۲۵) SMTP(Simple Mail Transfer Protocol)

انتقال دهنده پست الکترونیک (شماره پورت ۱۱۰) POP(Post Office Protocol)

تمرین: نام ۱۰ پورت پردازشی را نام ببرید؟

نکته ۲ : بطور کلی سه نوع آدرس دهی شبکه داریم:

۱- آدرس فیزیکی که همان MacAddress می باشد. که شامل ۱۲ رقم ۴ بیتی هگزا می باشد.

Mac : 6A-52-3B-00-2F-FA

۲- ادرس دهی منطقی: این نوع آدرس دهی بر اساس آدرس IP که بصورت X.Y.W.Z بین ۰ تا ۲۵۵ می باشد ۸ بیتی هستند و هر آدرس ۳۲ بیتی، IP است. آدرس IP در چهار کلاس A,B,C,D قرار دارند و هر کلاس شناسه و زیر شبکه شناسه میزبان خود را دارد.

class	بازه	Net IP	Host IP	Mask Net IP	Mask Host IP
A	0-127	X	Y.Z.W	255.0.0.0	0.255.255.255
B	128-191	X.Y	Z.W	255.255.0.0	0.0.255.255
C	192-223	X.Y.Z	W	255.255. 255.0	0.0.0.255
D	224-239	X.Y.Z.W		255.255.255.255	0.0.0.0
E	240-248	X.Y.Z.W		255.255.255.255	0.0.0.0

مثال ۱ : از سوی یک IP با شماره 122.10.10.9 حمله صورت گرفته است در این صورت شماره ISP و مربوط و شناسه Host IP کدام است؟

کلاس A X . Y .Z .W

122.10.10.9

ISP=122 Host IP = 10.10.9

مثال ۲ : از سوی یک IP با شماره 189.90.10.16 حمله صورت گرفته است در این صورت شماره ISP و شماره شناسه کاربر مهاجم و همچنین Mask Host IP کدام است؟

کلاس B

189.90.10.16

Net IP & ISP=189.90

Mask Host IP = 0.0.255.255

۳- آدرس دهی پردازشی: این آدرس دهی در لایه انتقال تحت عنوان آدرس های پورت شناخته می شود و ما می توانیم برای سرویس های مختلف پورت های متفاوت داشته باشیم.

انتقال فایل(شماره پورت ۲۱)	FTP(File Transport Protocol)
صفحات وب(شماره پورت ۸۰)	HTTP(Hypertext Transfer Protocol)
انتقال دهنده ایمیل(شماره پورت ۲۵)	SMTP(Simple Mail Transfer Protocol)
انتقال دهنده پست الکترونیک (شماره پورت ۱۱۰)	POP(Post Office Protocol)
شماره پورت ۱۴۴۳	Sql

نکته ۳ : اندازه بیت پورت مبدا و مقصد هر کدام ۱۶ بیت است و برای همین حداکثر $۲^{۱۶}$ که معادل ۶۵۵۳۵ پورت می توان تعریف کرد.

۳- Seq.no (شماره ترتیب):

یک عدد ۳۲ بیتی است که ماشین مبدا برای ارسال قطعه جدید به آن شماره ترتیب می دهد.

۴- Ack.no :

زمانیکه ماشین مقصد قطعه ارسالی با Seq.no=x را دریافت می کند در بخش Ack.no عدد x+1=101 را قرار می دهد. و بسته Ack یا بسته اعلان وصول را می فرستد. مثلا اگر x=100 باشد یعنی ماشین مبدا تا بیت ۱۰۰ را فرستاده و وقتی Ack.no=101 است یعنی ماشین مقصد تا بیت ۱۰۰ را گرفته است و می‌گوید بیت ۱۰۱ را بفرست.

۵- TCP HL :

Header Length یک نسخه ۴ بیتی است و طول سرایند را نشان می دهد. عدد داخل TCP HL ضرب در ۴ می شود و معادل بایتی آن اندازه سرآیند را نشان می دهد.

نکته ۱ : کلاه سیاه می تواند با گرفتن بین راهی یک قطعه TCP و تغییر TCP HL ساختار و قطعه ها را دچار اشغال کند.

نکات: حداقل مقدار TCP HL برابر ۵ است ۵=۲۰/۴ (۰۱۰۱) و حداکثر TCP HL آن ۶۰=۴*۱۵ (۱۱۱۱) است.

در اینصورت چون سرآیند ۶۰ بایت است فیلد Option حداکثر ۴۰ بایت می باشد.

۶۰-۲۰=۴۰

مثال: فرض کنیم که مقدار TCP HL برابر (۰۱۰۱) ۵ بوده است و یک نفوذگر آن را به (۰۱۰۰) ۴ تغییر داده است به نظر شما آیا این تغییر قابل شناسایی است و تغییر دهنده در کدام مرحله است(کلاه صورتی، کلاه سیاه و کلاه خاکستری)؟

۴*۴=۱۶ <۲۰ (۰۱۰۰) ➔ (۰۱۰۱)

Header آن ۱۶ است و کمتر از ۲۰ است کاملا مشخص است که قطعه ارسالی دچار تغییرات شده است و کشف می شود چون نفوذگر ناشی بوده و رده کلاه خاکستری می باشد.

مثال: یک قطعه داده با مقدار (۱۱۱۱) ۱۵ در بخش TCP HL توسط یک نفوذگر (۱۰۱۰) ۱۰ تغییر داده شده است اگر مقدار داده واقعی قطعه برابر ۱۰۰ بایت باشد گیرنده چه مقدار داده را اشتباه برداشت می‌کند؟

۲۰ اصلی ، ۴۰ Option ، داده ۱۰۰ ۱۵*۴=۶۰ (۱۱۱۱)

۲۰ اصلی ، ۲۰ Option ، داده ۱۲۰=۲۰+۱۰۰ ۱۰*۴=۴۰ (۱۰۱۰)

اگر گیرنده ۲۰ Option بایت فرض کند و ۲۰ بایت مابقی Option همراه داده خوانده می شود که برداشت کاملا غلطی است که این رده مربوط به کلاه سیاه است و توسط گیرنده قابل شناسایی نیست.

بعد از TCP HL مقدار ۶ بیت فضای خالی است. عملا این ۶ بیت بصورت استراتژیک می تواند در تشخیص $۲^۶$ که معادل ۶۴ است نوع متفاوت قطعه تشخیص دهد. نوع کد کاملا محرمانه است.

۶- Flag (پرچم) :

URG : اگر این پرچم ۱ باشد یعنی مقدار داخل فیلد Urgent مقدار واقعی و ارزشمند است و باید خوانده شود و بلعکس که صفر باشد هیچ ارزشی ندارد.

ACK : اگر این پرچم ۱ باشد یعنی این قطعه حاوی اعلان وصول ارزشمند است Ack.no واقعی است و باید خوانده شود و بالعکس.

PSH : اگر این پرچم ۱ باشد یعنی این قطعه شامل داده های زمان واقعی بوده(مثل پخش زنده سخنرانی یا فیلم یا فوتبال که باید سرعت توسط مسیریاب بر روی پورت خروجی قرار گیرد و بدون تاخیر ارسال شود).

RST : اگر این پرچم ۱ باشد یعنی ماشین مبدا یک طرفه ارتباط را قطع کرده است (بنابر دلایل نامعلوم) مثلا شاید احساس خطر کرده است مبنی بر اینکه یک کلاه سیاه داده ها را مانیتور می کند یا طرف مقابل قابل اعتماد نیست.

SYN : اگر این پرچم ۱ باشد یعنی ماشین مبدا می خواهد با ماشین مقصد در فاز تنظیم ارتباط برقرار نماید.

FIN : اگر این پرچم ۱ باشد یعنی ماشین مبدا قطعه جاری که ارسال نموده آخرین قطعه داده وی است.

ماشین مقصد به محض دریافت این آخر قطعه داده پورت داده را برای این ماشین می بندد تا مورد سوء استفاده قرار نگیرد.

نکته: اگر نفوذگر پرچم ها را دستکاری کند ممکن است موارد زیر اتفاق بیفتد:

اگر نفوذگر پرچم URG را صفر کند مقدار اشاره گر مهم Urgent خوانده نمی شود.

اگر نفوذگر پرچم ACK را صفر کند مهم Ack.no (اعلان وصول) خوانده نمی شود.

اگر نفوذگر پرچم PSH را صفر کند داده های زمان واقعی با تاخیر زیاد فرستاده می شود(کیفیت خدمات از دست می رود).

اگر نفوذگر پرچم RST را صفر کند برخلاف خواسته ماشین مبدا ارتباط را ادامه می دهد.

اگر نفوذگر پرچم SYN را صفر کند فاز تنظیم ارتباط از بین رفته و هیچ برقراری ارتباط و تبال داده صورت نمی گیرد.

اگر نفوذگر پرچم FIN را صفر کند یعنی ماشین مبدا داده هایش تمام شده اما پورت هنوز باز می ماند و موقعیت مناسبی برای نفوذگر خواهد بود.

۷- Win Size :

فیلد Win Size اندازه پنجره Buffer گیرنده است. این عدد نشان می دهد مقدار بافر آزاد موجود در گیرنده است یعنی اگر Win Size برابر ۱۰۰۰ بایت باشد فرستنده بایستی حداکثر به اندازه ۱۰۰۰ بایت قطعه داده بفرستد اگر بیشتر بفرستد بعلت کمبود فضای بافر، بافر ورودی گیرنده قطعه دور انداخته خواهد شد.

نکته ۱ : اگر نفوذگر با دیدن Win Size ۱۰۰۰ قطعه ارسال ماشین مبدا را که ۱۰۰۰ بایت است یک بایت بی ارزش اضافه کند این قطعه در مقصد دور انداخته خواهد شد.

نکته ۲ : نفوذگر Win Size را که ماشین گیرنده مثلا ۱۰۰۰ اعلام کرده تغییر داده و آن را ۱۰۰ می کند. با این حرکت عملا نرخ ارسال داده برای ماشین مبدا 0.1 می گردد یعنی از منابع و پهنای باند استفاده بهینه نمی شود.

۸- Check sum :

این فیلد شامل ۱۶ بیت است و تمامی بایت های سرایند قطعه (حداکثر ۶۰ بایت و حداقل ۲۰ بایت خواهد بود) آن ها را در دسته های ۲ بایتی یا ۱۶ بیتی زیر هم قرار داده و XOR می کند و نتیجه را در فیلد Check sum قرار می دهد. در مقصد مجددا محتوای سرایند Check sum آن محاسبه می شود و با مقدار داخل Check sum مقایسه می گردد. اگر این دو مقدار یکی باشد یعنی سرایند درست است در غیر اینصورت دچار تغییر شده و قطعه بی ارزش است.

۹- Urgent Pointer :

اشاره ضروری است. اگر این اشاره گر مقدار مهمی داشته باشد پرچم URG ، یک می شود این اشاره گر به موقعیتی در داخل داده ها اشاره می کند که آنجا داده ی مهمی مثلا رمز بانک مرکزی وجود دارد.

۱۰- Option :

داده های اضافی در این بخش قرار می گیرند و مقدار آن بین ۰ تا ۴۰ می باشد.

۱۱- Data :

اندازه این فیلد به همراه سرایند می تواند حداکثر ۶۴ کیلو بایت معادل ۶۵۵۳۵ بایت است.

مثال: اگر فیلد Option صفر باشد حداکثر ماشین مبدا چند بایت می تواند ارسال کند؟ اگر فیلد Option ، ۴۰ باشد ماشین مبدا چند بایت می تواند ارسال کند؟

Option=0 Data= 65535-20=65515

Option=40 Data= 65535-60=65475