

۱- کدام یک از موارد زیر از تکنیک های محدود کردن طول عمر بسته ها محسوب می گردند؟

مورد اول) شمارنده گام

مورد دوم) مهرزمان

مورد سوم) شناسه اتصال

مورد چهارم) آدرس انتقال یکبار مصرف

۰۱ اول و دوم ۰۲ اول و دوم و سوم ۰۳ سوم و چهارم ۰۴ دوم و سوم و چهارم

۲- کدام گزینه صحیح است؟

۰۱ کنترل ازدحام وظیفه مشترک لایه انتقال و کاربرد است.

۰۲ ازدحام در لایه شبکه تشخیص داده می شود.

۰۳ علت اصلی ازدحام کمبود فضای بافر در سمت گیرنده است.

۰۴ راه حل موثر برای کنترل ازدحام کاهش ترافیک ارسالی از لایه کاربرد است.

۳- در کدام یک از پروتکل های کنترل ازدحام در لایه انتقال، در هنگام بروز ازدحام مسیریاب برای اخطار وقوع ازدحام به

فرستنده یک بیت را در بسته ها **set** می کند اما درباره چگونگی کاهش آهنگ ارسال چیزی بیان نمی کند؟

۰۱ FAST TCP ۰۲ XCP ۰۳ TCP با ECN ۰۴ TCP ترکیبی

۴- در تخصیص کانال به کاربرانی که بر سر پهنای باند یک لینک با یکدیگر رقابت می کنند، کدام ترکیب باعث واگرا شدن

تخصیص از نقطه کار بهینه خواهد شد؟

۰۱ در صورتی که دو کاربر پهنای باند را به صورت ضربی افزایش داده و به صورت ضربی کاهش دهند.

۰۲ در صورتی که دو کاربر پهنای باند را به صورت جمعی افزایش داده و به صورت جمعی کاهش دهند.

۰۳ در صورتی که دو کاربر پهنای باند را به صورت جمعی افزایش داده و به صورت ضربی کاهش دهند.

۰۴ در صورتی که دو کاربر پهنای باند را به صورت ضربی افزایش داده و به صورت جمعی کاهش دهند.

۵- در فراخوانی روال های راه دور (RPC) کدام گزینه نشان دهنده بسته بندی پارامترها در یک پیام است؟

۰۱ مالتی پلکس معکوس ۰۲ قطارسازی ۰۳ خط لوله ۰۴ نیابت انتقال

۶- در پروتکل انتقال بی درنگ (RTP) کدام فیلد از سرآیند بسته مشخص کننده استریمی است که بسته متعلق به آن است؟

۰۱ فیلد شناسه مشارکت مبدا ۰۲ فیلد نوع محموله

۰۳ فیلد شناسه همزمان سازی مبدا ۰۴ فیلد شماره توالی

۷- کدام یک از تایمرهای پروتکل TCP برای بررسی فعال بودن یک اتصال استفاده می شود؟

۱. تایمر پایداری ۲. تایمر مداومت ۳. تایمر ارسال مجدد ۴. TIME WAIT

۸- به منظور کنترل ازدحام در پروتکل TCP Reno در صورتی که یک بسته گم شود، بعد از آنکه بسته گم شده مجدداً ارسال و تصدیق دریافت گردید و مقدار آستانه به نصف مقدار فعلی پنجره ازدحام کاهش یافت کدام گزینه اتفاق خواهد افتاد؟

۱. پنجره ازدحام به نصف مقدار فعلی کاهش می یابد.
۲. پنجره ازدحام از مقدار آستانه شروع آهسته جدید ادامه می یابد.
۳. اندازه پنجره ازدحام به حداکثر اندازه یک قطعه ست می شود.
۴. پنجره ازدحام به نصف مقدار آستانه شروع آهسته جدید ست می شود.

۹- در استاندارد MIME برای کدگذاری پیام هایی که تقریباً به طور کامل ASCII هستند و فقط چند کاراکتر غیر ASCII در آن ها وجود دارد کدام روش کارائی بیشتری دارد؟

۱. ASCII ساده ۲. ASCII با کاراکترهای ۸ بیتی
۳. base64 ۴. کدگذاری به صورت کاراکترهای چاپی

۱۰- در صورتی که فیلد content-type از سرآیند MIME دارای مقدار Message/rfc۸۲۲ باشد، پیام شامل کدام یک از گزینه های زیر خواهد بود؟

۱. یک ایمیل کپسوله شده در یک پیام دیگر ۲. یک پیام کپسوله که به چند تکه تقسیم شده است.
۳. یک پیام واحد با چندین فرمت ۴. چندین پیام که در یک پیام واحد ادغام شده است.

۱۱- کدام گزینه در رابطه با نمایش دهنده ها (viewer) صحیح می باشد؟

مورد اول) افزونه (plug-in) نوعی نمایش دهنده است.

مورد دوم) در مرورگرها مجموعه روال هایی به نام واسط مرورگر جهت انتقال داده ها به افزونه وجود دارد.

مورد سوم) نمایش دهنده ها برای توسعه قابلیت های مرورگر استفاده می گردند.

۱. موارد اول و دوم ۲. موارد اول و سوم ۳. موارد دوم و سوم ۴. موارد اول و دوم و سوم

۱۲- کدام یک از متدهای درخواست پروتکل HTTP به مشتری اجازه می دهد تا اطلاعاتی را در مورد یک صفحه از سرویس دهنده درخواست نماید؟

۱. POST ۲. GET ۳. TRACE ۴. OPTIONS



۱۳- در صدای دیجیتال کدام گزینه نشان دهنده خطائی است که در اثر محدود بودن تعداد بیت ها برای نمایش هر نمونه به وجود می آید؟

۱. ماسک فرکانسی ۲. ماسک زمانی ۳. نویز کوانتاش ۴. محوشدگی

۱۴- کدام گزینه صحیح است؟

۱. استریم زنده اینترنتی از پروتکل های چندپخشی مانند RTP بر روی لینک TCP استفاده می کند.
۲. از دید برنامه پخش رسانه، یک استریم زنده اینترنتی با استریم ضبط شده متفاوت است.
۳. تفاوت عمده استریم زنده اینترنتی با استریم ضبط شده لزوم بافر نمودن داده ها برای حذف پرش است.
۴. از جمله معایب پخش استریم زنده بر روی TCP نیاز به پهنای باند زیاد است.

۱۵- کدام یک از موارد زیر در رابطه با پروتکل های تلفن اینترنتی (VOIP) صحیح است؟

- مورد اول) کنفرانس چندرسانه ای برخلاف پروتکل H.323، در پروتکل SIP وجود دارد.
- مورد دوم) معماری SIP ماژولار است در حالی که معماری H.323 یکپارچه است.
- مورد سوم) فقط در پروتکل H.323 رمزنگاری وجود دارد.

مورد چهارم) SIP نسبت به H.323 انعطاف پذیرتر است اما H.323 پشته پروتکلی کاملتری دارد.

۱. موارد اول و چهارم ۲. موارد دوم و سوم ۳. موارد دوم و چهارم ۴. موارد اول و دوم

۱۶- در شبکه های تحویل محتوا (CDN) کدام تکنیک برای توزیع بسته های بزرگ نرم افزاری و محتویات استاتیک مناسب است اما برای توزیع محتویات وب به طور کامل به انتخاب کاربران وابسته است؟

۱. هدایت DNS
۲. آینه ای کردن
۳. مزرعه سرویس دهنده
۴. درخت توزیع با پروکسی وب

۱۷- کدام گزینه صحیح است؟

۱. جوهره اصلی سیستم های P2P اجتناب از ساختار غیرمتمرکز CDN است.
۲. مجموع ظرفیت بارگیری یک شبکه P2P با N کاربر معمولی تقریباً N/۲ Mbps است.
۳. شبکه های P2P خود مقیاس پذیر هستند.
۴. گره های P2P منحصرأ بدین منظور ایجاد می شوند که محتویات را با سهولت بیشتری به کاربران برسانند.

۱۸- کدام گزینه صحیح است؟

۱. مشکل حالت بازخور رمز، عدم امکان رمزگشائی قبل از دریافت کامل یک بلوک است.
۲. در حالت رمز کتابچه کد الکترونیک، دسترسی تصادفی به داده های رمزگذاری شده ممکن نیست.
۳. در حالت رمز استریمی، یک خطای انتقال یک بیتی در رمز نوشته فقط یک خطای یک بیتی را در فاش نوشته خروجی ایجاد می کند.
۴. برای رمزگذاری بایت به بایت بهتر است از حالت زنجیرسازی بلوک رمز استفاده شود.

۱۹- در پروتکل IPsec، یک اتصال یک طرفه بین دو نقطه پایانی شبکه با شناسه امنیتی مختص خود را چه می نامند؟

۱. AH ۲. SA ۳. ESP ۴. IKE

۲۰- در کدام حمله از گشودن چندین نشست همزمان و موازی به منظور شکستن یک پروتکل استفاده می شود؟

۱. حمله بازپخش ۲. حمله بازتابش ۳. حمله مرد در وسط ۴. حمله فریب DNS

۲۱- از عجالتی (nonce) به منظور جلوگیری از انجام کدام حمله استفاده می شود؟

۱. حمله بازپخش ۲. حمله مرد در وسط ۳. حمله بازتابش ۴. حمله DOS

۲۲- کدام گزینه در رابطه با سیستم ایمیل امن (PGP) صحیح است؟

۱. PGP شبیه یک پیش پردازنده است که متن رمز شده را گرفته و یک فاش نوشته base64 را تحویل می دهد.
۲. PGP علاوه بر امنیت امکان نوشتن و ارسال ایمیل را نیز فراهم می کند.
۳. PGP برای رمزگذاری از الگوریتم IDEA در حالت زنجیرسازی بلوک رمز استفاده می کند.
۴. PGP یک برنامه منبع باز است.

۲۳- کدام یک از موارد زیر بیان کننده سرویس های بنیادی است که توسط DNS امن (DNSsec) ارائه می شود؟

مورد اول) توزیع کلید عمومی

مورد دوم) اثبات آن که داده ها از کجا منشا گرفته است.

مورد سوم) احراز هویت درخواست ها و تراکنش ها

مورد چهارم) حفظ نمودن محرمانگی اطلاعات و مخبره سری داده ها

۱. موارد اول و چهارم ۲. موارد دوم و سوم و چهارم
۳. موارد سوم و چهارم ۴. موارد اول و دوم و سوم

۲۴- کدام گزینه در رابطه با پروتکل لایه سوکت امن (SSL) صحیح است؟

۱. SSL در بالاترین سطح امنیتی از MD5 برای بررسی یکپارچگی پیام ها استفاده می کند.
۲. تفاوت SSL با TLS در نحوه استخراج کلید نشست از پیش شاه کلید و عجالتی ها است.
۳. امنیت SSL وقتی در آن از 3DES استفاده شده باشد، بسیار متزلزل است.
۴. SSL یک لایه امنیتی جدید بین لایه های انتقال و شبکه است.

۲۵- توضیح زیر کدام یک از تکنیک های تامین امنیت کدهای متحرک را توصیف می کند؟

((زمانی که یک اپلت قابل اطمینان نباشد، در یک محیط مقید و محدود اجرا می گردد تا رفتار آن تحت کنترل درآمده و دسترسی آن به منابع با اطلاع و نظارت کاربر صورت گیرد.))

۱. امضای کد
۲. قالب شنی
۳. ناشناس سازی
۴. نشانه گذاری

سوالات تشریحی

۱- هر یک از مفاهیم زیر را به اختصار توضیح دهید:

الف. الگوریتم ناگل

ب. جستجوی معکوس در DNS

ج. حالت رمز استریمی

۱.۴۰ نمره

۲- سه رهیافت سازماندهی فضای بافر در لایه انتقال را به همراه مزایا و معایب هر کدام توضیح دهید.

۱.۴۰ نمره

۳- مشکل اصلی تکنیک حافظه نهان http این است که چگونه باید تشخیص دهیم نسخه موجود در حافظه نهان دقیقاً همان نسخه موجود در سرویس دهنده است. راهبردهای حل این مشکل را به اختصار توضیح دهید.

۱.۴۰ نمره

۴- رهیافت هدایت DNS را برای توزیع محتوای وب در شبکه های تحویل محتوا (CDN) با ذکر یک مثال توضیح دهید.

۱.۴۰ نمره

۵- چهار پیشرفت در تحلیل رمز را بیان نموده و یک پیشرفت را توضیح دهید؟

۱.۴۰ نمره