تعداد سوالات : تستی : ۳۰ تشریحی : ۰ | زمان آزمون (دقیقه) : تستی : ۷۰ تشریحی : ۰ | سری سوال : یک ۱

عنـــوان درس: مباحث نودرفناوری اطلاعات

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)۱۵۱۱۰۰۸

۱- اهداف امنیت رایانه کدامند؟

۱. محرمانگی، تمامیت، دسترس پذیری
۲. محرمانگی، تمامیت، انکارپذیری
۳. تمامیت، احراز هویت، انکارپذیری
۴. تمامیت، دسترس پذیری، احراز هویت

۲- سرویس های امنیتی به چند دسته عمده تقسیم می شوند و کدامند؟

۱. ۴ دسته: شامل تمامیت، عدم انکار، کنترل دسترسی، محرمانگی
۲. ۶ دسته: شامل محرمانگی، احراز اصالت، تمامیت، عدم انکار، کنترل دسترسی، دسترس پذیری
۳. ۵ دسته: شامل محرمانگی، احراز اصالت، تمامیت، عدم انکار، کنترل
۴. ۵ دسته: شامل محرمانگی، احراز اصالت، تمامیت، کنترل دسترسی، دسترس پذیری

۳- در کدام نوع از رمز نگاری، کلید رمز نگاری بین فرستنده و گیرنده مشترک است؟

۱. نامتقارن ۲. متقارن ۳. تک حرفی ۴. چند حرفی

۴- کدام یک از روش های رمز به صورت زیر بیان می شود؟

" کلمه ای به عنوان کلید انتخاب می شود، جدولی ۵*۵ تشکیل می شود، و ابتدا کلید در جدول نوشته می شود".

۱. رمز چند حرفی ۲. رمز تک حرفی ۳. رمز هیل ۴. رمز پلی فر

۵- کدام یک از موارد زیر از نقاط ضعف رمزگذاری DES ساده شده می باشد؟

۱. جابجایی و انتقال زیادی در متن رخ می دهد.
۲. تعداد حالات آن ۱۰۲۴ می باشد.
۳. به راحتی نمی توان حالات آن را بررسی کرد.
۴. جابه جایی و انتقال کمی در متن رخ می دهد.

۶- کدام یک از الگوریتم های زیر مشابه الگوریتم DES می باشد؟

۱. DES دوتایی ۲. IDEA ۳. RC۵ ۴. BlowFish

۷- کدام یک از موارد از نقاط ضعف روش رمزگذاری پیوند می باشد؟

۱. کاربران دارای اختیار زیادی در مورد امنیت اعمال شده می باشند.
۲. در شبکه های بزرگ رمزگذاری پیوند به تعداد کمی عملگر نیاز دارد.
۳. هر پیوند نیاز به یک کلید نامتقارن دارد.
۴. در رمز گذاری پیوند به اجبار همه پیام ها رمز می شوند.

۸- مولد عدد تصادفی دارای چه خواصی می باشد؟

۱. توزیع نرمال- استقلال
۲. توزیع نرمال- دوره تناوب
۳. دوره تناوب- استقلال
۴. دوره تناوب- بردار کنترلی

۹- به هنگام تولید کلید توجه به کدام یک از نکات زیر مهم می باشد؟

۱. اعداد اول "p و q " انتخابی حتی الامکان بزرگ انتخاب شوند که قابل حدس زدن نباشند.

۲. اعداد اول "p و q " انتخابی حتی الامکان کوچک انتخاب شوند که قابل حدس زدن نباشند.

۳. اعداد اول "p و q " انتخابی به صورت تصادفی انتخاب شوند که قابل حدس زدن نباشند.

۴. برای انتخاب e وd، معمولا e طوری انتخاب شود که gcd (Φ(n) , e)=0

۱۰- چنانچه نفوذگر از طریق $P_B, KP_B\ P_m, KG$ سعی کند K را کشف کند، این مسئله را چه می نامند؟

۱. مسئله توزیع کلید توسط کلید عمومی
۲. مسئله پروتکل توزیع کلید دلفی- هلمن
۳. مسئله لگاریتم منحنی بیضوی
۴. مسئله پیاده سازی RSA

۱۱- در کدام گزینه الگوریتم از ۵ مقدار ۳۲ بیتی استفاده می کند؟

۱. الگوریتم RIPEMD-۱۶۰
۲. الگوریتم درهم ساز امن SHA
۳. الگوریتم MD۵
۴. الگوریتم HMAC

۱۲- حداکثر اندازه پیام در کدام الگوریتم بینهایت می باشد؟

۱. MD5
۲. SHA-1
۳. RIPEMD-160
۴. HMAC

۱۳- کدام گزینه سرویس های مربوط به " تشخیص به مخاطره افتادن " را نشان می دهد؟

۱. احراز اصالت- تمامیت میدان ارتباطی- عدم انکار
۲. محرمانگی داده- محرمانگی جریان ترافیک- مسیر انتخابی
۳. محرمانگی داده- تمامیت میدان ارتباط- مسیر انتخابی
۴. احراز اصالت- محرمانگی جریان ترافیک- عدم انکار

۱۴- یکی از ساده ترین پروتکلها برای بررسی باز بودن مسیر بین دو عنصر را به طور متناوب کدام است؟

۱. NICB
۲. TNI
۳. پروتکل DOS
۴. درخواست/ پاسخ

تعداد سوالات : تستی : ۳۰ تشریحی : ۰ | زمان آزمون (دقیقه) : تستی : ۷۰ تشریحی : ۰ | سری سوال : ۱ یک

عنـــوان درس: مباحث نودرفناوری اطلاعات

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)۱۵۱۱۰۰۸

۱۵- کدام گزینه از ویژگی های نسخه ۵ کربروس می باشد؟

۱. به سیستم رمز گذاری خاص " DES " وابسته است.

۲. به پروتکل اینترنت IP وابسته است.

۳. ساختارهای پیام توسط ASN.1 و BER تعریف شده است.

۴. زمان اعتبار بلیط ها حداکثر ۲۱ ساعت است.

۱۶- در کدام یک از روش های زیر اصالت صاحب کلید در موقع دریافت کلید عمومی قابل احراز است و از ایجاد ترافیک در گره های خاص جلوگیری می کند؟

۱. ارسال مستقیم توسط کاربر

۲. ذخیره دفترچه تلفن

۳. ذخیره در یک گره و دریافت آن با احراز اصالت

۴. استفاده از گواهی

۱۷- کدام یک از گزینه های زیر از محدودیت های پروتکل SMTP/822 می باشد؟

۱. اطلاعات دودویی قابل ارسال نیستند.

۲. سرورهای SMTP پیام های بزرگتر از طول معین را قبول می کنند.

۳. پیاده سازی بر اساس استاندارد RFC82

۴. استفاده از روش های استاندارد مانند unencode/undecode

۱۸- کدام یک از سرویس های زیر توسط هر دو ESP (فقط رمز گذاری) و AH ارائه می شود؟

۱. کنترل دسترسی

۲. تمامیت بدون اتصال

۳. احراز اصالت مبدا داده

۴. محرمانگی

۱۹- عبارت زیر به چه چیز اشاره دارد؟

"حاوی اطلاعاتی است که در طول توافق روی مجمع امنیتی مورد استفاده قرار می گیرد"

۱. بدنه تغییر شکل

۲. بدنه پیشنهاد

۳. بدنه شناسایی

۴. بدنه درخواست گواهی

۲۰- کدام گزینه از روش های مقابله با تمامیت می باشد؟

۱. رمز نگاری

۲. حفاظت

۳. روش های رمز نویسی

۴. جمع آزمای رمز نویسی

۲۱- پروتکل هشدار در SSL از چند بایت تشکیل شده است؟

۱. یک بایت

۲. دو بایت

۳. سه بایت

۴. چهار بایت

تعداد سوالات : تستی : ۳۰ تشریحی : ۰ | زمان آزمون (دقیقه) : تستی : ۷۰ تشریحی : ۰ | سری سوال : ۱ یک

عنـــوان درس: مباحث نودرفناوری اطلاعات

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)۱۵۱۱۰۰۸

۲۲- کدام پروتکل, تبادل پیغام امن را به طور ساده و با استفاده از الگوریتم نامتقارن فراهم می کند؟

۱. SHTTP ۲. HTTP ۳. PEM ۴. SSL

۲۳- از کدام استاندارد برای شبکه های مبتنی بر TCP/IP استفاده می شود و اشیاء مدیریت شده در MIB را توصیف می کند؟

۱. RFC 1213 ۲. RFC 1255 ۳. RFC 1157 ۴. RFC 1011

۲۴- کدام دستور اجازه می دهد که اطلاعات ناخواسته به مرکز مدیریت, قابل ارسال باشد؟

۱. GetNextRequest ۲. Set Request

۳. Get Request ۴. Trap

۲۵- "اندازه بزرگ جدول با خانه های خالی زیاد" از معایب کدام یک از روش های ایجاد کنترل دسترسی محتاطانه می باشد؟

۱. جدول حفاظت ۲. کلمه عبور فایل

۳. مبتنی بر تواناییها ۴. لیست کنترل دسترسی

۲۶- کنترل دسترسی اجباری در چند سطح عمل می کند؟

۱. ۲ سطح: شامل سطح امنیتی و سطح طبقاتی ۲. ۱سطح: شامل سطح امنیتی

۳. ۱ سطح: شامل سطح حفاظتی ۴. ۲ سطح: شامل سطح حفاظتی و سطح طبقاتی

۲۷- قسمت DIDS Director در سیستم تشخیص نفوذگر توزیع شده چه کاری انجام می دهد؟

۱. کشف کاربر غیر متعارف ۲. بررسی رویداد نگاری اطلاعات شبکه

۳. مدیریت تشخیص فعالیت های نفوذگرانه ۴. نظارت بر یک کاربر در شبکه

۲۸- در کدام حالت, معمولا یک مسیریاب نقش دیوار آتش را بازی می کند که توسط نرم افزار بسته های مجاز و غیر مجاز به آن معرفی می شوند؟

۱. دروازه سطح مدار ۲. دروازه فیلتر بسته ها

۳. دروازه در سطح برنامه کاربردی ۴. دروازه در سطح سرویس

۲۹- کدام گزینه در خصوص نقاط ضعف بانکهای اطلاعاتی کاملتر و صحیح تر می باشد؟

۱. استنتاج- اجماع- تمامیت داده ها- اسبهای تراوا ۲. استنتاج- اجماع- تمامیت داده ها- کرم ها

۳. استنتاج- اجماع- عدم انکار- کرم ها ۴. استنتاج- اجماع- عدم انکار- اسب های تراوا

تعداد سوالات : تستی : ۳۰ تشریحی : ۰ | زمان آزمون (دقیقه) : تستی : ۷۰ تشریحی : ۰ | سری سوال : ۱ یک

عنـــوان درس: مباحث نودرفناوری اطلاعات

رشته تحصیلی/کد درس: مهندسی فناوری اطلاعات،مهندسی فناوری اطلاعات (چندبخشی)۱۵۱۱۰۰۸

۳۰- در کدام یک از سیستم های تشخیص نفوذگر شبکه, بر کل ترافیک شبکه نظارت می شود؟

۱. NSM ۲. GSM ۳. NADIR ۴. CSM