تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰ | **سری سوال :** یک ۱

عنـــوان درس: مباحث نودرفناوری اطلاعات،مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات ۱۱۱۵۰۶۱ - ، مهندسی فناوری اطلاعات (چندبخشی)، مهندسی فناوری اطلاعات۱۵۱۱۰۰۸

۱- بیشترین تحقیقات در امنیت رایانه در کدامیک از حیطه های ذیل می باشد؟

۱. محرمانگی ۲. تمامیت ۳. ایمنی ۴. دسترسی پذیری

۲- چنانچه اطلاعات مستلزم مرتبه بیشتری از اعتبار و صحت باشد؛ کدامیک از معیارهای ارزش دارایی درجه بیشتری خواهد داشت؟

۱. محرمانگی ۲. دسترس پذیری ۳. امانت داری ۴. آسیب پذیری

۳- نوع حمله های دستبرد و تغییر به ترتیب کدامیک است؟

۱. فعال - فعال ۲. غیرفعال - فعال ۳. غیرفعال - غیرفعال ۴. فعال - غیرفعال

۴- در کدام روش رمزگذاری هر حرف با حرف بعدی که فاصله ثابت و یکسانی از حرف قبلی دارد، جایگزین می شود؟

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

۵- نقطه قوت کدام رمز این است که به دلیل رمز کردن حروف با کلیدهای مختلف تکرار حروف تا حدی محو می شود؟

۱. رمز چند حرفی ۲. رمز تک حرفی ۳. رمز ورنام ۴. رمز هیل

۶- عبارت زیر نقطه ضعف کدام روش است؟

"کلید ۱۰ بیتی کلید کوچکی است و مقدار حالات مختلف آن ۱۰۲۴ است . لذا به راحتی می توان حالات ممکن آنرا بررسی کرد"

۱. DEC ۲. IDEA ۳. S-DEC ۴. RC5

۷- در کدام الگوریتم ورودی و خروجی ۵۴ بیتی است و کلید طول متغیری بین ۸ تا ۱۰۲۴ بیت دارد، و برای پردازنده های ۱۶ بیتی طراحی شده است. از ساختار فیستل استفاده نمی کند بلکه MD5 است؟

۱. RC5 ۲. RC2 ۳. IDEA ۴. CAST

۸- از نقاط ضعف کدام روش رمزگذاری این است که، نمی توان اطلاعات مربوط به بسته (مانند آدرس گیرنده و فرستنده) را هم رمز کرد؛ یعنی فقط اطلاعات متن رمز می شود؟

۱. پیوند ۲. انتها به انتها ۳. سزار ۴. چرخشی

۹- کدام روش حمله به RSA ، دربرگیرنده روشهای مختلف است که معادل تجزیه اعداد می باشد؟

۱. جستجوی جامع ۲. حمله ریاضیاتی ۳. حمله توان مصرفی ۴. حمله زمانی

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰ | **سری سوال :** ۱ یک

عنوان درس: مباحث نودرفناوری اطلاعات،مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات ۱۱۱۵۰۶۱ - ، مهندسی فناوری اطلاعات (چندبخشی)، مهندسی فناوری اطلاعات۱۵۱۱۰۰۸

۱۰- روش های اصلی احراز اصالت کاربران شامل کدام کلیدها می باشد؟

۱. کلیدهای اطلاعاتی - کلیدهای فیزیکی - کلیدهای عمومی
۲. کلیدهای بیولوژیکی - کلیدهای مجازی - کلیدهای اطلاعاتی
۳. کلیدهای اطلاعاتی - کلیدهای فیزیکی - کلیدهای بیولوژیکی
۴. کلیدهای فیزیکی - کلیدهای مجازی - کلیدهای اطلاعاتی

۱۱- کارتهای مغناطیسی، کارتهای هوشمند و یا ماشین حساب های خاص جزء کدام یک از کلیدهای ذیل می باشند؟

۱. کلید های اطلاعاتی
۲. کلیدهای فیزیکی
۳. کلیدهای بیولوژیکی
۴. کلیدهای متقارن

۱۲- یکتا بودن و همیشه در اختیار کاربران بودند؛ از مزایای کدام نوع از کلیدها می باشد؟

۱. کلیدهای عمومی
۲. کلیدهای اطلاعاتی
۳. کلیدهای فیزیکی
۴. کلیدهای بیولوژیکی

۱۳- مزیت کدامیک از روش های احراز اصالت، عدم امکان انکار امضاء توسط فرستنده است؟

۱. استفاده از داور
۲. مهر زمانی
۳. چالش و پاسخ
۴. استفاده از شمارنده

۱۴- کدام روش مانند توپولوژی ستاره و حلقه نوع دوم است، در هر لحظه فقط دو رایانه می توانند با هم ارتباط برقرار کنند؟

۱. پخشی
۲. نقطه به نقطه
۳. لایه ای
۴. بسته ای

۱۵- کدام روش از جمله روش های کنترلی جهت ایجاد امنیت می باشد؟

۱. عدم سرویس دهی
۲. تغییر دادن
۳. روش رمزگذاری
۴. دستبرد

۱۶- کدامیک از عبارات ذیل جزء سرویس های تمامیت ارتباطات است؟

۱. تداوم عملکرد
۲. مدیریت شبکه
۳. محرمانگی داده
۴. عدم انکار

۱۷- کربروس، سرویس دهنده کدامیک از موارد ذیل می باشد؟

۱. عدم انکار
۲. احراز اصالت
۳. وقفه
۴. مدیریت شبکه

۱۸- در عملکرد کربروس کدام گزینه به AS این اجازه را می دهد که پالس ساعت کارفرما با پالس ساعت AS همزمان باشد؟

۱. TS1
۲. IDC
۳. TS2
۴. IDv

۱۹- در کدامیک از روش های توزیع کلید عمومی، اصالت صاحب کلید در موقع دریافت کلید عمومی قابل احراز است و از ایجاد ترافیک در گره های خاص جلوگیری می شود؟

۱. ارسال مستقیم توسط کاربر
۲. ذخیره در یک گره و دریافت آن با احراز اصالت
۳. استفاده از گواهی
۴. ذخیره در دفترچه تلفن

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰ | **سری سوال :** ۱ یک

عنـــوان درس: مباحث نودرفناوری اطلاعات،مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات ۱۱۱۵۰۶۱ - ، مهندسی فناوری اطلاعات (چندبخشی)، مهندسی فناوری اطلاعات۱۵۱۱۰۰۸

۲۰- بیت warnonly از مثالهای کدامیک از میدان های کلید می باشد؟

۱. اعتماد به مالک ۲. درستی کلید ۳. اعتماد به امضاء ۴. اعتماد به ارتباطات

۲۱- کدام کلمه کلیدی به منظور شناسایی عناصر MIME به طور یکتا در زمانی که چند قطعه همزمان در پیام درج شده باشند، به سرآیه اضافه می شود؟

۱. نوع محتوا ۲. شناسه محتوا

۳. نوع کد گذاری روی محتوا ۴. توصیف محتوا

۲۲- در کدام نوع کدگذاری در محتوای MIME، عمل کدگذاری داده به گونه ای است که قطعات ۶بیتی ورودی به قطعات ۸ بیتی خروجی نگاشته می شوند؟

۱. ۷bit ۲. ۵bit ۳. Base64 ۴. x-token

۲۳- جعل داده از تهدیدات کدامیک از خطرات است که وب با آن مواجه می شود؟

۱. تمامیت ۲. محرمانگی ۳. عدم سرویس ۴. احراز اصالت

۲۴- استفاده از کدام گزینه در مرورگرها جهت سادگی ارتباط چند صفحه مربوط به یک جلسه برای کاربر فراهم می شود؟

۱. اسکریپت ۲. پول الکترونیکی ۳. کوکی ۴. SSL

۲۵- کدام استاندارد توصیف کننده چگونگی تعریف مدیریت در MIB است و برای ساختارهای مدیریت اطلاعاتی شبکه های مبتنی بر TCP/IP استفاده می شود؟

۱. RFC1155 ۲. RFC1213 ۳. RFC1157 ۴. RFC1000

۲۶- داشتن جدولی شامل کلیه کاربران و کلیه اشیاء، که یکی از راه های اعمال کنترل دسترسی است، چه نامیده می شود؟

۱. جدول تطبیق ۲. جدول حفاظت

۳. کلمه عبور فایل ۴. لیست کنترل دسترسی

۲۷- اساس کدام سیستم مبتنی است بر پرونده کاربر و یک سیستم خبره جهت بررسی فعالیت هایی است که با سناریوهای حملات شناخته شده مطابقت دارند و یا سعی می کنند از نقاط ضعف شناخته شده سیستم استفاده کنند؟

۱. IDES ۲. MIDAS ۳. Haystack ۴. DDOS

۲۸- در کدام سیستم از رویدادنگاری برای عمل تشخیص نفوذگرانه استفاده نمی شود، بلکه کل ترافیک شبکه نظارت می شود؟

۱. CSM ۲. NADIR ۳. NSM ۴. DIDS

تعداد سوالات : تستی : ۳۰ **تشریحی :** ۰ | **زمان آزمون (دقیقه) : تستی :** ۶۰ **تشریحی :** ۰ | **سری سوال :** ۱ یک

عنوان درس: مباحث نودرفناوری اطلاعات،مدیریت امنیت سیستم اطلاعاتی

رشته تحصیلی/کد درس: مدیریت فناوری اطلاعات ۱۱۱۵۰۶۱ - ، مهندسی فناوری اطلاعات (چندبخشی)، مهندسی فناوری اطلاعات۱۵۱۱۰۰۸

۲۹- کدامیک از موارد ذیل از نتایج بررسی و ارزیابی ریسک می باشد؟

۱. اضافه یا تغییر دادن سرویس های شبکه ای

۲. محدود کردن دستورالعمل هایی که نفوذگر می تواند استفاده کند

۳. تعیین اجزاء حساس و بحرانی سازمان

۴. تغییر در پوسته سیستم

۳۰- کدام مدل مبتنی بر چارچوب سلسله مراتبی از سطوح دسترسی است و سطح درستی یک شی بر اساس میزان خرابی ناشی از استفاده نادرست یک موضوع، تعیین می شود؟

۱. BLP

۲. Biba

۳. Clark-Wilson

۴. Goguen-Meseguer