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

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۱- کدام هدف امنیت رایانه ای، تصریح می کند که اطلاعات در سیستم رایانه ای و نیز اطلاعات مبادله شده بین سیستم های رایانه ای از تغییرات یا حذف غیر مجاز به دور باشند؟

۱. محرمانگی ۲. تمامیت ۳. دسترس پذیری ۴. جعل

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- "عدم دسترسی به اطلاعات غیرمجاز" تعریف کدام گزینه می باشد؟

۱. محرمانگی ۲. عدم انکار ۳. دسترس پذیری ۴. کنترل دسترسی

۴- "تغییر" و "دستبرد" به ترتیب از کدام نوع حملات می باشند؟

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

۵- اساس این روش مبتنی بر جابجا نمودن حروف متن اصلی است. بدین صورت که جدولی هر حرف از حروف الفبا یا هر نویسه را به حرف یا نویسه مشخصی تبدیل می کند؟

۱. سزار ۲. پلی فر ۳. جانشینی ۴. تک حرفی

۶- نقطه قوت این رمز این است که تکرار حروف تا حدی محو می شود زیرا حروف با کلیدهای مختلف رمز می شوند؟

۱. سزار ۲. پلی فر ۳. ویجنر ۴. جانشینی

۷- از خواص این الگوریتم، فشرده بودن می باشد بطوریکه به ۵ کیلوبایت حافظه نیاز دارد؟

۱. DEC ۲. IDEA ۳. BLOWFISH ۴. CAST

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

۱. S-DEC ۲. RC5 ۳. RC2 ۴. CAST

۹- از نقاط ضعف این 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

۱۰- کارتهای مغناطیسی، کارتهای هوشمند، و یا ماشین حساب های خاص، جزء کدام نوع از کلیدها می باشند؟

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

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

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۱۱- کدامیک از کلیدها نسبت به سایر کلیدهای اطلاعاتی دارای مزایای زیر هستند؟

- **یکتا هستند**
- **رونوشت برداری و دوباره سازی آنها سخت است**
- **همیشه در اختیار کاربرند**

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

۱۲- 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

۱۳- این 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

۱۴- کدام گزینه یکی از دسته بندی های روش های کنترلی جهت ایجاد امنیت میباشد؟

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

۱۵- کدام گزینه، جزء سرویس های تمامیت ارتباطات می باشد؟

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

۱۶- کربروس، چه نوع سرویس دهنده ای می باشد؟

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

۱۷- کدام جزء از پیام به AS این اجازه را می دهد که پالس ساعت کارفرما همزمان با پالس ساعت AS باشد؟

۱. TS1 ۲. IDC ۳. TS2 ۴. IDv

۱۸- کدامیک از روش های توزیع کلید عمومی از بقیه روشها بهتر است. چون 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

۱۹- 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

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

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

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

۱. نوع محتوا
۲. شناسه محتوا
۳. نوع کد گذاری روی محتوا
۴. توصیف محتوا

۲۱- عبارت زیر تعریف کدام نوع از انواع کدگذاری در محتوای MIME است؟

"عمل کدگذاری داده به گونه ای است که قطعات ۶ بیتی ورودی به قطعات ۸ بیتی خروجی نگاشته می شوند"

۱. ۷bit
۲. ۵bit
۳. Base64
۴. x-token

۲۲- عبارت زیر مربوط به معایب کدام پروتکل می باشد؟

"به دلیل نیاز به عملیاتی محاسباتی سنگین امکان حمله پابند وجود دارد. یعنی دشمن با تعداد زیاد درخواست کلید جلسه ، می تواند ماشین را از کار بیندازد."

۱. IKE
۲. Oakely
۳. دیفی - هلمن
۴. ISAKMP

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- در یک مرورگر جهت ساده شدن ارتباط چند صفحه مربوط به یک جلسه برای یک کاربر، از چه چیزی استفاده می شود؟

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

۲۵- این 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- یکی از راه های اعمال کنترل دسترسی، داشتن جدولی شامل کلیه کاربران و کلیه اشیاء است. این جدول اصطلاحا چه نام دارد؟

۱. جدول تطبیق
۲. جدول حفاظت
۳. کلمه عبور فایل
۴. لیست کنترل دسترسی

۲۷-اساس این سیستم، استفاده از روش مبتنی 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

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

عنـــوان درس: مباحث نودرفناوری اطلاعات

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

۲۸- در این 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

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-این مدل مبتنی بر چارچوب سلسله مراتبی از سطوح دسترسی است. 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