نام درس: مباحث نو در فناوری اطلاعات
تعداد سؤالات: تستی: ۴۰ تشریحی: ۶
رشته تحصیلی/ کُد درس: مهندسی فناوری اطلاعات (۱۵۱۱۰۰۸)
زمان آزمون: تستی: ۶۰ تشریحی: ۵۰ دقیقه
آزمون نمره منفی دارد ○ ندارد ◉

کُد سری سؤال: یک (۱) استفاده از: — مجاز است. منبع:

پیامبر اعظم(ص): روزه سپر آتش جهنم است.

۱. کدام جزء حملات فعال نیست ؟
الف. نقاب زنی ب. تغییر پیام ج. تحلیل ترافیک د. انکار سرویس

۲. ..... وقتی رخ می دهد که یک نهاد یا موجودیت ، خودش را نهاد دیگری معرفی می کند .
الف. تکرار ب. نقاب زنی ج.تغییر پیام د. انکار سرویس

۳. کدام جزء دسته ی راهکارهای امنیتی ویژه به حساب نمی آید ؟
الف. رمزنگاری ب. اضافات ترافیک ج. کنترل دستیابی د. تشخیص رویداد

۴. مهمترین ابزار خودکار برای امنیت شبکه و ارتباطات چیست؟
الف. سخت افزار ب. نرم افزار ج. رمزگذاری د. طراحی شبکه

۵. تمام الگوریتم های رمزگذاری مبتنی بر دو اصل است. آن دو اصل چیست ؟
الف. سخت افزار – نرم افزار ب. برنامه – شبکه
ج. جانشینی – جا به جایی د. طراحی – ساختار

۶. کدام گزینه به ماهیت طرح رمزگذاری و اطلاعاتی که دراختیار داریم بستگی دارد ؟
الف. تحلیل رمز ب. جانشینی ج. متن رمز شده د. کلید رمز

۷. کدام یک جزء رمزگذاری بلوکی متقارن نیست ؟
الف. DES ب. AES ج. 3DES د. فیستل

۸. مشهورترین رمزکننده ی دنباله ای چیست ؟
الف. DES ب. 3DES ج. RC4 د. AES

۹. طول کلید در کدام یک از گزینه ها متغییر است ؟
الف. RC2 ب. RC4 ج. 3DES د.گزینه الف و ب

۱۰. رمزگذاری حفاظت در مقابل چه نوع حمله ای است ؟
الف. فعال ب. غیر فعال ج. انکار سرویس د. تکرار پیام

۱۱. طرح رمزگذاری کلید عمومی چند جزء است ؟
الف. سه ب. چهار ج. پنج د. شش

۱۲ . الگوریتم RSA در کدام یک از موارد زیر کاربرد دارد ؟
الف. امضای دیجیتال ب. مبادله ی کلید
ج.رمزگذاری / رمزگشایی د. همه موارد

۱۳. منحنی بیضوی در کدام یک از موارد زیر کاربرد دارد ؟
الف. امضای دیجیتال ب. مبادله ی کلید
ج.رمزگذاری / رمزگشایی د. همه موارد

نام درس: مباحث نو در فناوری اطلاعات
تعداد سؤالات: تستی: ۴۰ تشریحی: ۶
رشته تحصیلی/ کُد درس: مهندسی فناوری اطلاعات (۱۵۱۱۰۰۸)
زمان آزمون: تستی: ۶۰ تشریحی: ۵۰ دقیقه
آزمون نمره منفی دارد ○ ندارد ◉

کُد سری سؤال: یک (۱) استفاده از: --- مجاز است. منبع:

۱۴. کدام یک از الگوریتم های زیر از مبادله ی کلید استفاده می کند ؟

الف. DSS ب. دایفی هلمن ج.منحنی بیضوی د. همه موارد

۱۵. PGP ...

الف. سیستم ارسال نامه به صورت الکترونیکی است ب. یک سرویس احراز هویت و محرمانگی است

ج. یک نوع کد امنیتی است د. یک نوع رمزگذاری است

۱۶. برای سازگاری پست الکترونیک چه الگوریتمی مورد استفاده قرار می گیرد؟

الف.RSA / SHA ب.DSS / SHA ج.تبدیل مبنای ۶۴ د.IDEA

۱۷. PGP بعد از امضا پیام و قبل رمزگذاری چه عواملی انجام می دهد؟ چرا؟

الف. فشرده سازی- صرفه جویی در فضا برای انتقال و غیره

ب. احراز هویت- امنیت بیشتر برای رمزگذاری

ج. سازگاری پیام و امضا- برای یکسان سازی پیام و امضا

د. قطعه بندی پیام- برای نظم بیشتر برای رمزنگاری

۱۸. اطلاعات موجود در شناسه دیجیتال به چه عواملی بستگی دارد؟

الف. نوع ب. ظرفیت ج. حجم د. آدرس

۱۹. IP SEC کدام ناحیه ی عملیاتی را در بر نمی گیرد؟

الف.احراز هویت ب.محرمانگی ج. مدیریت کلید د. امضای دیجیتالی

۲۰. کدام یک جزء سرویس های امنیتی IPSEC نیست؟

الف.کنترل دستیابی ب.احراز هویت منشا داده ها

ج.رمز گذاری د.مدیریت کلید

۲۱. سرآیند احراز هویت کدام یک از فیلدهای زیر را شامل نمی شود ؟

الف. طول محموله ب. شماره ترتیب

ج. داده ی احراز هویت د. طول کلید

۲۲. دو مفهوم مهم SSL در چیست ؟

الف. نشست و اتصال ب. امنیت و نشست

ج. اتصال و امنیت د. رمزگذاری و امنیت

۲۳. پروتکل رکورد SSL دو سرویس را برای اتصال های SSL فراهم می کند آن دو چیست ؟

الف. نشست و اتصال ب. محرمانگی و تمامیت پیام

ج. قطعه بندی و فشرده سازی د. امنیت و محرمانگی

۲۴. کدام تفاوت های بین مجموعه رمز موجود در SSLV3 و TLS است ؟

الف. قطعه بندی و فشرده سازی ب. الگوریتم و محرمانگی

ج. مبادله ی کلید و اتصال د. مبادله ی کلید و الگوریتم رمزگذاری متقارن

نام درس: مباحث نو در فناوری اطلاعات
تعداد سؤالات: تستی: ۴۰ تشریحی: ۶
رشته تحصیلی/ کُد درس: مهندسی فناوری اطلاعات (۱۵۱۱۰۰۸)
زمان آزمون: تستی: ۶۰ تشریحی: ۵۰ دقیقه
آزمون نمره منفی دارد ○ ندارد ◉

کُد سری سؤال: یک (۱) استفاده از: --- مجاز است. منبع:

۲۵. آندرسون نفوذگران را در چند دسته معرفی می کند ؟

الف.۲ ب.۳ ج.۴ د.۵

۲۶. این تعریف به کدام مورد اشاره دارد ؟" شخصی که مجوز استفاده از کامپیوتر را ندارد و از کنترل های دستیابی سیستم عبور می کند تا خودش را حساب کاربر قانونی جلوه دهد ."

الف. کاربر مخفی ب. MISFEASOR ج. نقاب زنان د. هکر

۲۷. روش های تشخیص نفوذگری کدام است ؟

الف. ناهنجاری آماری و حسابرسی ب. حسابرسی و قانونی

ج. قانونی و ناهنجاری آماری د. تشخیص آستانه و حسابرسی

۲۸. برای شکست در ورود به سیستم از پایانه خاص از چه مدلی استفاده می کنند ؟

الف. انحراف معیار ب. عملیاتی ج. سری های زمانی د. چند متغییره

۲۹. کدام یک از حمله ها از چندین منبع هماهنگ شده انجام می شود ؟

الف. انکار سرویس ب. انکار سرویس توزیع شده

ج. ویروس د. کرم

۳۰. این تعریف برای کدام است " تحت شرایطی فعال می شود"

الف. Virus ب.Worm ج.Back dors د.logic bomb

۳۱. برنامه ای که در ماشین حمله اجرا می شود زمینه را برای حمله به ماشین های دیگر فراهم می کند، برای کدام گزینه است ؟

الف. Flooders ب.Rookit ج.Zombie د.EXploits

۳۲. ابزارهای هکر مغرض که برای رخنه در ماشین راه دور استفاده می شود کدام است ؟

الف. Downloader ب.Auto-rooter ج.Kit د.Virus

۳۳- کدام جزء فازهای طول عمر ویروس نیست ؟

الف. فاز غیر فعال ب. فاز انتشار ج. فاز اجرا د. فاز پایان

۳۴. شکلی از ویروس که طراحی شد تا خودش را در مقابل نرم افزار ضد ویروس مخفی کند کدام ویروس است ؟

الف.ویروس انگلی ب. ویروس فراشکلی

ج. ویروس مخفی د. ویروس مقیم در حافظه

۳۵. کرم ها برای گسترش خود از چه وسیله ای استفاده نمی کنند ؟

الف.پست الکترونیکی ب. اجرای راه دور

ج. کامپیوتر ها د.ورود به سیستم از راه دور

۳۶. کدام حالت فناوری کرم را شامل نمی شود ؟

الف. چند سکویی ب. فراشکلی ج. چند نمایی د. نمایش یک روز

نام درس: مباحث نو در فناوری اطلاعات
تعداد سؤالات: تستی: ۴۰ **تشریحی:** ۶
رشته تحصیلی/ کُد درس: مهندسی فناوری اطلاعات (۱۵۱۱۰۰۸)
زمان آزمون: تستی: ۶۰ **تشریحی:** ۵۰ دقیقه
آزمون نمره منفی دارد ○ **ندارد** ◉

کُد سری سؤال: یک (۱) **استفاده از:** --- **مجاز است.** **منبع:**

۳۷. کدام جزء نسل های نرم افزارهای ضد ویروس نمی شود ؟

الف. پیمایش های ساده
ب. پیمایش های اکتشافی
ج. حفاظت کامل
د. از بین بردن

۳۸. کدام جزء خطهای دفاعی در مقابل حمله DDOS نیست ؟

الف. قبل از حمله
ب. در اثنای حمله
ج. در اثنای حمله و پس از آن
د. پس از آن

۳۹. کدام جزء عناصر اصلی ماتریس دستیابی نیست ؟

الف. موضوع
ب. عنوان
ج.شی ء
د. مجوز دستیابی

۴۰- کدام ۴ تکنیک کلی برای فایروال ها نیست ؟

الف. کنترل حساب
ب. کنترل کاربر
ج. کنترل جهت
د. کنترل رفتار

سوالات تشریحی

بارم هر سوال ۱ نمره می باشد.

۱. اجزای رمزگذاری متقارن را نام برده و توضیح دهید؟

۲. ویژگی های تابع درهم سازی را نام ببرید ؟(۴ مورد)

۳. وظایف S/MIME را نام ببرید ؟(۴ مورد)

۴. ویژگی های الگوریتم Oakley را نام ببرید ؟(۴ مورد)

۵. پشته پروتکل SSl را بکشید و قسمت های آن را بنویسید ؟

۶. مدل فرایند مارکوف را تعریف کنید ؟