جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

سازمان آموزش فنی و حرفه ای کشور

نمونه سؤالات:

تست امنیت سیستم

کد استاندارد: ۲۵۱۱۱۰۰۰۲۳

معاونت پژوهش، برنامه ریزی و سنجش مهارت

دفتر سنجش مهارت و صلاحیت حرفه ای

۱-در کدام لایه امکان ساخت اکانت اپلیکیشن وجود دارد؟

الف -لایه خدمات

ب -لایه کاربردی

ج -لایه دسترسی

د -لایه انتقال

۲- لایه ..... به برنامه نویس این امکان را می دهد که ریسک نفوذ به دیتاهای اصلی و حساس اپلیکیشن را کاهش دهد.

الف -لایه خدمات

ب -لایه کاربردی

ج -لایه دسترسی

د -لایه انتقال

۳- جمله زیر به کدام نوع از حملات سایبری اشاره دارد؟

"بدون انجام هرگونه فعل ظاهری یا ایجاد تغییرات در سیستم های قربانی ، به منظور نفوذ و سوء استفاده از منابع سیستم انجام می شود.

الف- غیر فعال

ب -فعال

ج -سایبری

د -پویا

۴- جمله زیر به کدام نوع از حملات سایبری اشاره دارد؟

"به زیر ساخت های سایبری حیاتی نفوذ می کند ، اطلاعات حساس را دستکاری کرده و باعث بروز حوادث و فجایع ملی و جبران ناپذیر می گردد"

الف -غیر فعال

ب -فعال

ج -سایبری

د -پویا

۵-

ICA مخفف چه کلماتی است؟

الف -یکپارچگی وامن بودن و دردسترس بودن

ب -محرمانگی و در دسترس بودن و محرمانه بودن

ج -یکپارچگی و محرمانه بودن و امن بودن

د -یکپارچگی ،محرمانه بودن و در دسترس بودن

۶- منظور از Network Security چیست؟

الف- امنیت شبکه

ب -مانیتورینگ شبکه

ج -پشتیبانی شبکه

د -گزارشگیری شبکه

۷- کدام یک از موارد زیر از خطرناک ترین تهدید های شبکه محسوب می شود؟

الف -حملات DOS

ب -تخریب اطلاعات

ج -دسترسی غیر مجاز

د -اجرای فرامین غیر قانونی

8-حملات DOS به دلیل ..... خطر ناک می باشند.

الف -به آسانی می توانند اجرا شوند- به سختی رهگیری می شود.

ب -به سختی رهگیری می شوند

ج -سرپیچی از درخواست حمله کننده آسان است

د -سرپیچی از درخواست حمله کننده آسان نیست -به آسانی می توانند اجرا شوند -به سختی رهگیری می شوند

9-حملات سایبری به چند دسته تقسیم می شود؟

الف -حملات فعال و غیرفعال

ب -حملات پدافندی و غیر پدافندی

ج -حملات سایبری و غیر سایبری

د -حملات شبکه ای و سیستمی

10-کدام یک از موارد زیر جزو اهداف حملات سایبری نمی باشد؟

الف -ایجاد اختلال در یک سرور

ب -دسترسی به اطلاعات یک سیستم

ج -مطالعه و زیرنظر گرفتن یک سازمان بصورت غیر مجاز

د -ورود به اتصالات اینترنتی که پهنای باند کمی دارند

11-مورد ..... شامل یک سری پروتکل است که یک شرکت یا فرد برای اطمینان از اطلاعات از ICA خود پیروی می کند.

الف -امنیت شبکه

ب -امنیت سیستم

ج -امنیت سایبری

د -امنیت اطلاعات

12-کدام یک از موارد زیر از مفاهیم اساسی امنیت سایبری می باشد؟

الف -تداوم تجارت و بازیابی فاجعه

ب -تداوم تجارت و حفظ استراتژِی آن

ج -جلوگیری از فاجعه و عدم تداوم آن

د -حفظ سیاستهای تجاری و امنیت

13-کدام یک از موارد زیر از چالشهای امنیت سایبری نمی باشد؟

الف -گسترش فرصت های حمله برای هکرها

ب -مقررات پیچیده

ج -عدم تخصص IT

د -به روزبودن اطلاعات

14-مشکلات امنیتی کدام یک از موارد زیر به صورت باگ مشخص می گردد؟

الف -ایمیل

ب -وب

ج -نرم افزار

د -بی سیم

15-تقسیم بندی شبکه در بحث امنیت شبکه از کدام یک از آسیب های احتمالی را کنترل می کند؟

الف -کنترل ترافیک و درخواست ها در بستر شبکه

ب -چنانچه یک بخش از شبکه مشکل امنیتی پیدا کرد کل شبکه تحت تاثیر آن قرار نمی گیرد

ج -تشخیص باگ ها

د -کنترل دسترسی ها

16-کدامیک از حملات سایبری زیر به عنوان حملات استراق سمع شناخته می شود؟

الف- Phishing

ب- Man-in- the- middle

ج- Mal ware

د- Zero-day

۱۷-کدام یک از گزینه های زیر شامل شرایط احرازهویت از طریق روش های بیومتریکی نیست ؟

الف- سوال از آنچه کاربر می داند.

ب -سوال از آنچه که کاربر دارد.

ج -سوال ازآنچه که کاربرکشف کرده است.

د -استفاده از مشخصات فیزیکی کاربر

۱۸- کدام یک از موارد زیر را می توان از کاربردهای اسکن شبکه ای دانست؟

الف -حسابرسی

ب -تایید هویت

ج -کنترل دسترسی

د -اطلاعات محرمانه

۱۹- کدام تکنولوژی متکی به‌یک ویژگی فیزیکی کاربر برای احراز هویت می باشد؟

الف -کارت هوشمند

ب -زیست سنجی

ج -تایید متقابل

د -علائم

۲۰- درکدام یک از حملات زیر،با آموزش کاربران در مورد اینکه به افراد مختلف اطمینان نکنند می توان تا حد زیادی از بروز حمله جلوگیری کرد؟

الف- حمله replay

ب- Social engineering

ج- Spoofing

د- Computer Forensics

۲۱-کدام یک از حملات زیر حمله Smurf را شامل می شود؟

الف- Spoof

ب- Replay

ج- DOS

د- Sniff

۲۲-کدام روش به نفوذ هایی اشاره می کند که به جای استفاده از ضعف های تکنیکی بر استفاده از ارتباط انسانی و اغلب فریب دادن افراد متکی است.

الف- Social engineering

ب- Spoofing

ج- Computer forensics

د- حمله replay

۲۳-کدام نوع حمله دسترسی تکذیب شده کاربران را به منابع شبکه مجاز می کند؟

الف- DOS

ب- Worm

ج- logical bomb

د- مهندسی اجتماعی

۲۴-یک کاربر گزارش می دهد که خطایی را دریافت کرده که نشان می دهد آدرس TCP/IPدر حال حاضر استفاده است زمانی که به کامپیوترش مراجعه کند یک آدرس IP ثابت برای کاربران کامپیوتر اختصاص داده شمرده و شما مطمئن هستید که این آدرس به طور عمدی به کامپیوتر دیگری واگذار نشده است. کدام حمله احتمال می رود ؟

الف- Back door attack

ب- man in the middle

ج- worm

د- TCP/IP hijacking

۲۵-حمله Phishing چیست؟

الف- نوعی از کوکی‌ها هستند

ب -ارسال وب‌سایتهای مخرب و Email ها برای جلب نظر کاربران جهت دریافت اطلاعات شخصی آنان نظیر اطلاعات مالی

ج -یک نوع حمله DOS است

د -یک نوع حمله به Authentication است.

-26به حملاتی که از طریق واردآوردن ترافیک بالا برای یک پروتکل یا سرویس اقدام به ایجاد اختلال در آن می نمایند، چه می گویند؟

الف- spoofing

ب- man-in-the-middle attack

ج- backdoor

د- Flood

۲۷-در کدامیک از انواع حملات زیر نفوذ گر به ناگاه خود را به جای کاربر وانمود کرده و ضمن آنکه نشست قبلی را ادامه می دهد ،کاربر اصلی را با قطع ارتباط مواجه می کند.

الف- DOS

ب- Replay

ج- Sniff

د- Session Hijacking

۲۸-کدام گزینه نشان دهنده ویژگی های حمله man-in-the-middle می باشد.

الف -بااستفاده از پروتکل tcp/ip انجام می شود.

ب -ارتباط بین ابزار ها را سرقت کرده وپاسخ های جعلی به ارسال کننده داده می شود.

ج -تنها در شبکه های بی سیم انجام می شود.

د -همواره به شکل غیر فعال انجام می شود.

29-یک مدیر در شرکت SISTERگزارش یک تهدید جدید را می دهد که آن را تکمیل کرده است. بنابراین برای او آخرین خطر، خطری است که تلاش می کنـد در یک جلسه ارتباطی بوسیله قرار دادن یک کامپیوتر در سیستمی دخالت کند که در حال ارتباط میباشد. کدام نوع زیر حمله تشکیل می شود؟

الف- Man In The Middle Attack

ب- Tcp/Ip hijacking

ج- worm

د- back door

۳۰-شما متوجه شده اید که یک گواهی مقتضی به طور تکراری برای دستیابی ورودی سیستم استفاده شده است. کدام نوع حمله بیشتر محتمل است.

الف- TCP/IP hijacking

ب- Back door Attack

ج- replay Attack

د- Man In The Middle Attack

۳۱-کدام یک از الگوریتم های نامتقارن زیر دارای امنیت بیشتری نسبت به بقیه است؟

الف- RSA

ب- MD-17

ج- SHA-2

د- ERFGA

۳۲-کدامیک از گزینه های زیر برای سیستم رمزنگاری نادرست است ؟

الف- در سیستم رمزنگاری دو نوع رمزنگاری ، ۱- رمزنگاری کلید عمومی ۲- رمزنگاری نامتقارن

ب -رمزنگاری عمومی ، کلید مورد استفاده برای رمزکردن با کلید مربوط برای رمزگشایی با هم متفاوت است .

ج -رمزنگاری متقارن ، کلید مورد استفاده برای رمز کردن با کلید مربوط برای رمزگشایی یکی هستند .

د -در رمزنگاری نامتقارن ، کاربر یک کلید عمومی و یک کلید خصوصی در اختیار دارد ، کلید خصوصی مخفی ولی کلید عمومی ممکن است به طور وسیع منتشر شود .

-33نام سازمانی که عمل صدور گواهی نامه های دیجیتال را به دیگران انجام می دهد چه نام دارد؟

الف- (server Authority)SA

ب- DS(Directory Server)

ج- CA(Certificate Authority)

د- CS(certificate Server)

۳۴-برای بهره گیری از امنیت بالاتر کدام یک از الگوریتم های نامتقارن زیر پیشنهاد می شود؟

الف- MD-17

ب- ShA-2

ج- RSA

د- ERFGA

۳۵-داده قبل از قرار گیری در الگوریتم رمزنگاری،جه نام دارد؟

الف- متن واضح

ب -متن باز

ج -متن رمز شده

د -متن ساده

-36یک CRL شامل فهرستی از کدام نوع کلید می باشد؟

الف- هم کلید عمومی و هم اختصاصی

ب -کلیدهای عمومی

ج -کلیدهای اختصاصی

د- Stegano graphic

-37سه محور اصلی در کنترل دسترسی به شبکه کدامیک از گزینه‌های زیر می‌باشند؟

الف- Authentication, confidentiality, integrity

ب- Authorization , Authorization ,Accounting

ج- Authentication, Accounting, Authorization

د- Authentication, confidentiality, Authorization

۳۸-تمام گزینه های زیر می توانند در سیاست نگهداری اسناد یافت شوند بجز گزینه؟

الف -کنترل دسترسی فیزیکی

ب -قوانین پیچیده رمز عبور

ج -نوع ذخیره سازی رسانه

د -دوره های نگهداری اسناد

-39کدام جزء امنیت فیزیکی کنترل دسترسی به سطح بیرونی آدرسها می باشد؟

الف -امنیت پیرامون

ب -درهای قفل شده

ج -امنیت مناطق

د -حبس کردن

۴۰- کدامیک از گزینه‌های زیر نادرست است؟

الف -یکی از راه‌های متوقف کردن سرویسها ، بستن درگاه‌ها بوسیله فیلتر کردن می‌باشد

ب -در سیستم عامل ویندوز تنها می‌توان درگاه‌های TCP را فیلتر نمود

ج -موثرترین راه بستن درگاه‌های باز، متوقف کردن سرویس مربوط به آن است

د -در ویندوز می‌توان فیلترهای محلی (برای درگاه‌ها)تعریف نمود

۴۱- به تازگی مدیر جدیدتر استخدام شده، سمت شما را به طور موقت بر عهده خواهد گرفت در حالیکه شما در یک کنفرانس حضور داشنید شما سعی می کنید کـه اصـول امنیـت را برای او در مدت زمان کوتاهی که ممکن است شرح دهید. کدام گزینه زیر بهترین توصیف یک لیست کنترل دستیابی (ACL)

می باشد؟

الف -لیست کنترل دستیابی که کنترل دسترسی افراد را به منابع فراهم میکند.

ب -لیست کنترل دستیابی که در سیستمهای پیشرفته استفاده نشده است.

ج -فرآیند ACLماهیت پویایی دارد

دACLS - برای کاربران مجاز استفاده شده است.

۴۲- راهکاری سیستماتیک و ساخت یافته برای مدیریت احتمال مرتبط با بروز یک تهدید، کدام مورد زیر است؟

الف -مدیریت دارایی

ب -ارزیابی ریسک

ج -مدیریت ریسک

د -کاهش تهدید

۴۳-مورد .....یک روش طراحی تست نرم افزار است که در آن مقادیر ورودی به پارتیشن های معتبر و نامعتبر تقسیم می شود؟

الف -تجزیه و تحلیل آستانه

ب -نمودار علت و معلولی

ج -تست تصمیم گیری

دEquivalence partitioning -

۴۴- کدام نرم افزار به عنوان آنتی ویروس قدرتمند ،تقویت کننده و پاک کننده گوشی اندروید استفاده می شود؟

الف- نرم افزار Web Application Scanner

ب -نرم افزار Security Scanner

ج -نرم افزار Exploit Framework

د -نرم افزار APP Dynamic

۴۵- در کدام لایه حفاظتی نرم افزار Anti-exploit در صورت حمله هر گونه ارتباط شما قطع و برنامه مخرب حذف می شود؟

الف -لایه اول

ب -لایه دوم

ج -لایه سوم

د -لایه چهارم

۴۶- در کدام یک از موارد زیر تست جعبه سیاه اعمال نمی شود؟

الف -یکپارچه سازی آزمون

ب -تست سیستم

ج -تست پذیرش

د -تست آزمون

۴۷- کدامیک از موارد زیر از انواع حوزه های تست نفوذ نمی باشد؟

الف -برنامه های کاربردی وب

ب -امنیت شبکه

ج -تست های امنیت cloud

د -تست امنیت

۴۸- مورد .....یک چرخه حمله سایبری شبیه سازی شده است که هکر های اخلاقی حرفه ای برای پیدا کردن و نشان دادن آسیب پذیری شبکه آن را انجام می دهند.

الف- Pen testing

ب- spoofing

ج- man-in-the-middle attack

د- Backdoor

۴۹-کدام یک از مهارت های زیر از مهارت های فنی کارشناس تحلیل و تست نرم افزار می باشد؟

الف- دانش پایه ای پایگاه داده SQL

ب -دانش پایه ای روی فرمان های لینوکس

ج -دانش و مهارت عملی روی یک ابزار مدیریت تست

د -دانش پایه ای پایگاه داده SQL ، دانش پایه ای روی فرمان های لینوکس، دانش و مهارت عملی روی یک ابزار مدیریت تست

۵۰- کدام یک از موارد زیر از وظایف اصلی کارشناس تست نرم افزار نمی باشد؟

الف -جهت ارائه یک محصول نرم افزاری با کیفیت باگ های نرم افزار را بگیرد.

ب -ایجاد نگهداری و به روزنامه رسانی بانک اطلاعاتی برای ایرادهای شناسایی شده

ج -چگونگی رفع ایرادها از مشکلات شاسایی شده

د -اهداف یک پروژه نرم افزاری را مشخص نماید