جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

سازمان آموزش فنی و حرفه ای کشور

نمونه سؤالات:

کارور امنیت فناوری اطلاعات

کد استاندارد: ۱۳۳۰۲۰۵۳۱۴۴۰۰۱۱

معاونت پژوهش، برنامه ریزی و سنجش مهارت

دفتر سنجش مهارت و صلاحیت حرفه ای

کارور امنیت فناوری اطلاعات - ۳۵۱۱۳۰۵۳۱۰۳۰۱۵۱

۱-کدام مورد جزء جرایم سایبری محسوب می گردد؟

الف- Phishing

ب- Decryption

ج- Social Engineering

د- Ethical hacking

۲-بهترین تعریف برای هک اخلاقی چیست؟

الف- درخواست از مردم برای انجام دادن فعالیتهای غیر مجاز

ب- وادار کردن افراد به افشای اطلاعات محرمانه

ج- در معرض خطر قرار دادن داده های محرمانه توسط کارمندان داخلی

د- انجام آزمایشات مجاز برای مشخص کردن مشکلات امنیتی سیستم

۳-فایروالها چه مواردی را می توانند کنترل کنند؟

الف- IP-Virus-Data Header-User

ب- Virus-Port -Data-Hacker

ج- IP-Port-Data Header -Data

د- IP-Port-Data-Email

۴-فایروال ویندوز چه مواردی را می توانند کنترل کنند؟

الف- TCP & UDP Port-program

ب- User & password -Virus

ج- TCP Port-program

د- UDP Port- Predefined

۵-روند اضافه شدن header و trailer به داده ها را چه می گویند؟

الف- رمزنگاری Encryption

ب- تغییردهنده‌های دسترسی Access Modifier

ج- دسترسی شبکه Network Access

د- کپسوله سازی Encapsulation

۶-IPS چیست؟

الف- یک سیستم محافظتی است که خرابکاریهای در حال وقوع روی شبکه را شناسایی می کند.

ب- ابزارهای ارزیابی آسیب پذیری که خطاها و یا ضعف در تنظیمات را گزارش می دهند.

ج- یک سیستم محافظتی است که خرابکاریهای در حال وقوع روی شبکه را شناسایی و بلافاصله سیستم خرابکار را بلاک می کند

د- نرم افزاری جهت جلوگیری از ورود و تشخیص انواع کرمها، ویروسها و ...

۷-کدام یک از محدودیت های آنتی ویروس به شمار می آیند؟

الف- هنگامی که کاربر به یک شبکه محلی متصل می شود، غیر فعال می گردد

ب- برای فعال کردن آنتی ویروس نیاز به دیوار آتش (Firewall) است.

ج- برای اطمینان از حداکثر مصونیت باید به صورت منظم به روز رسانی شود.

د- برای اسکن درایوهای خارجی قابل استفاده نمی باشد.

۸-لایه اول فایروال که براساس تحلیل بسته آی پی و فیلدهای سرآیند کارمیکند، کدام بخش زیر را بررسی نمی کند؟

الف -آدرس آی پی مبدا و مقصد

ب -شماره شناسایی بسته اطلاعا تیGram Data

ج- شماره پورت و پروسه مبدا و مقصد

د- زمان حیات بسته

۹-DHCP ، مسئولیت اختصاص..... به هر یک از دستگاه های موجود در شبکه را برعهده دارد .

الف- آدرس های MAC

ب- اسامی Host

ج- آدرس های IP

د- URL

۱۰-ویروس جز کدام یک از بدافزارهای ذیل می باشد؟

الف- بدافزارهایی که مخفی می شوند.

ب- بد افزارهایی که با دخالت کاربر تکثیر می شوند.

ج- بدافزارهایی که برای سازنده منفعت دارند.

د- بد افزارهایی که اتوماتیک تکثیر می شوند

۱۱-----، رایانه و یا دستگاه موبایلی است که پس از اتصال به اینترنت بدون اطلاع کاربر توسط یک "کراکر" و یا "ویروس" آلوده می شود و تحت کنترل یک شخص ثالث قرار می گیرد.

الف- زامبی

ب- بوت نت

ج- بوت مستر

د- فیشینگ

۱۲------، شبکه ای از رایانه ها است که به اینترنت متصل هستند و همگی تحت کنترل یک رایانه واحد قرار دارند.

الف- زامبی

ب- بوت نت

ج- بوت مستر

د- فیشینگ

۱۳-در صورتی که یک فایل عکس با یک تروجان یا ویروس ترکیب شده باشد چه پسوندی دارد؟

الف- JPG

ب- BMP

ج- EXE

د- PDF

۱۴-بدافزاری که به ظاهر برنامه ای مفید است و پس اجرا اعمال بدخواهانه خود را بصورت مخفی اجرا می کند چه نام دارد؟

الف- تروجان

ب- ویروس

ج- بمب منطقی

د- کرم

۱۵-به بدافزاری که انواع فایلها را بصورت رمزنگاری شده در می آورد و پس از نمایش متنی، یک ایمیل جهت مکاتبه و واریز وجه برای رمزگشایی فایل های رمزشده می دهد چه می گویند؟

الف- Spyware

ب- Rootkit

ج- Trojan

د- Ransomware

۱۶-راه مقابله با keylogger ها در زمان خرید الکترونیکی چیست؟

الف- استفاده از رمز عبور طولانی

ب- رمزنگاری رمز عبور

ج- ورود رمز عبور به صورت برعکس

د- استفاده از صفحه کلید مجازی

۱۷-به انواع بدافزاری که از نقاط ضعف برنامه نویس و نرم افزار استفاده می کند و به سیستم نفوذ می کند چه نام دارد؟

الف- Rootkit

ب- Back Door

ج- Adware

د- Worm

۱۸-------- بدافزار و یا قطعه کدی است که معمولا توسط برنامه نویسان حرفه ای نوشته شده و دارای زمانی خاص برای اجرا است و پس از اجرا اقدام به دانلود سایر بدافزارها و یا اقدام به حذف و آسیب رساندن به سیستم و فایلها می کند.

الف- درب پشتی Back Door

ب- جاسوس افزار Spyware

ج- بمب منطقیLogical Bomb

د- تروجان Trojan

۱۹-کدام یک از گزینه های زیر نمونه ای از یک تکنیک بیومتریک برای کنترل دسترسی است؟

الف- اسکن چشم

ب- رمز عبور

ج- دیوار آتش

د- امضای دیجیتال

۲۰-کدام یک جز معایب شبکه های بی سیم می باشد؟

الف- راحتی

ب- امنیت

ج- جابجایی

د- اشتراک منابع

۲۱-قابلیتی که به مدیران شبکه امکان کنترل ورود و خروج دستگاه‌هایی با آدرس مک مشخص می دهد چه نام دارد؟

الف- MAC Spoofing

ب- MAC Filtering
ج- MAC Address
د- Wireless MAC
۲۲-آی پی broad cast در شبکه ۲۶/۱۹۲,۱۶۸,۱۱۰,۱ چیست؟
الف- ۱۹۲,۱۶۸,۱۱۰,۱۲۷
ب- ۱۹۲,۱۶۸,۱۱۰,۰
ج- ۱۹۲,۱۶۸,۱۱۰,۲۵۵
د- ۱۹۲,۱۶۸,۱۱۰,۱
۲۳-کدام مورد جز مزایای استفاده از وی پی ان نمی باشد؟
الف -ترافیک رمز شده تا از استراق سمع جلوگیری شود
ب -کاربر احساس مجزا بودن می کند.
ج -با قطع اینترنت ارتباط برقرار می ماند
د -ارتباط از نوع نقطه به نقطه می باشد
۲۴- تکنولوژی ------ یکی از قابلیت هایی است که برای کاربران آماتور ساخته شده است تا بتوانند به راحتی و بدون استفاده از رمز عبور و با وارد کردن پین و یا سایر روشها به مودم وصل شوند.
الف- WiFi Protected Setup (WPS)
ب- MAC Address
ج- Authentication
د- Service set identifier (SSID)
۲۵------- یک پروتکل لایه ۷ برای دسترسی و به اشتراک گذاری فایلها، پیرینتر ها و پورت ها در شبکه می باشد.
الف- Server Message Block (SMB)
ب- NetBIOS
ج- DHCP
د- Sharing
۲۶-کدام گروه جز پروتکهای Tunneling است؟
الف- TCP,UDP,TUNEL,PPP
ب- RIP,RGP,IRGP,OSTP
ج- WEP,WPA,WPA2,WPA3
د- IPSec,PPTP,L2TP,GRE
۲۷-بزرگ ترین اشکال امنیتی شبکه های بی سیم چیست؟
الف- استفاده از پروتکل های نا امن برای انتقال داده
ب- انتشار اطلاعات در فضا و در دسترس بودن
ج- فاصله زیاد کاربران مجاز با تجهیزات بی سیم
د- کمبود پهنای باند
۲۸-عمل Pharming به چه معناست؟

الف- ارجاع دادن کاربران به یک وب سایت اشتباه بدون اطلاع آنها
ب- تشخیص مشکلات امنیتی سیستم از طریق سنجش مجاز
ج- جمع آوری اطلاعات شخصی افراد از طریق تماسهای تلفنی ناخواسته
د- جمع آوری اطلاعات مرورگر یک کاربر، بدون اجازه او
۲۹-اگر به یک سایت پرداخت الکترونیکی مشکوک شدیم، کدام نشانه بهترین روش شناخت سایت جعلی است؟
الف- پس از بروز سازی (Refresh) جای شماره ها در صفحه کلید مجازی تغییر می کند .
ب- بعد از بروز رسانی (Refresh) تصویر حروف نمایش داده شده تغییر می کند
ج- وجود علامت قفل در کنار نام سایت
د- پس از ورود اطلاعات اشتباه پیام عدم ارتباط با سرور را می دهد.
۳۰-امضای دیجیتال چیست؟
الف- نوعی رمزنگاری متقارن است که این اطمینان را به گیرنده میدهد که نامه جعلی نیست.
ب- امضای اسکن شده از امضای واقعی فرد از روی کاغذ
ج- امضا با مدادی نوری بر روی سیگنچر پد (Signature Pad) است
د- هر نوع علامت منضم شده یا به نحو منطقی متصل شده به داده است که برای شناسایی امضاء کننده داده مورد استفاده قرار می‌گیرد
۳۱-سخت افزاری کوچک شبیه فلش که از ریزپردازنده برای رمزنگاری و از حافظه برای ذخیره سازی اطلاعات هویتی و کلید خصوصی استفاده می کند چه نام دارد.
الف- Smart Card
ب- Token
ج- CA
د- Dongle
۳۲-کدام نوع گواهینامه در سامانه ثبت سفارش وزارت بازرگانی جهت احراز هویت تجار بکار می رود.
الف- SSL
ب- IOMS
ج- TMIS
د- Email Source
۳۳------ در مرورگر امکانی هستند که بعضی قسمت های وب سایت ها مانند تصاویر و کد ها را ذخیره سازی می کنند و با این کار در بارگذاری های بعدی وب سایت تسریع ایجاد می شود.
الف- تاریخچه(History)
ب- کوکی (Cookie)
ج- علاقه مندی ها (Favorites)
د- کش (Cache)
۳۴-رمزی که تنها یک بار برای ورود به سیستم اعتبار دارد و دارای مدت زمان استفاده می باشد چه نام دارد؟
الف- OTP
ب- SSL
ج- IOMS

د- TMIS

۳۵-در مرورگرها به ذخیره خودکار اطلاعات وارد شده برای فرم ها که با وارد کردن حرف اولیه در فرم مربوطه ظاهر می شود چه می گویند؟

الف- Notify when Downloads complete

ب- Use inline AutoComplete

ج- Auto Complete

د- Use smooth scrolling

۳۶-در مرورگر اینترنت اکسپلورر جهت مسدود کردن و یا اجازه ورود کوکی ها کدام Tab از Internet Option مناسب می باشد؟

الف- Advanced

ب- Privacy

ج- Security

د- Content

۳۷-در سرویس کنترل والدین نوع User ای که می بایست برای فرزندان انتخاب کرد کدام است؟

الف- Administrator

ب- Child

ج- Standard

د- Parental

۳۸-کدام محدودیت را نمی توان برای کنترل فرزندان در Parental Controls اعمال کرد؟

الف- محدودیت زمانی

ب- محدودیت استفاده از برنامه ها در کامپیوتر

ج- محدودیت اجرای بازی ها

د- محدودیت ایجاد و حذف فایلهای موجود در کامپیوتر

۳۹-کدام یک از گزینه های زیر اطلاعات متنی است که هنگام بازدید شما از یک وب سایت توسط مرورگر وب شما ذخیر ه می شود؟

الف- Definition File

ب- Back Door

ج- Cookie

د- Macro

۴۰-هدف از امضای دیجیتال چیست؟

الف- جهت تایید هویت فرستنده ایمیل بکار می رود

ب- درج یک امضاء در پایین یک سند الکترونیکی به وسیله یک ماکروی در حال اجرا

ج- تایید می کند که ایمیل تحویل داده شده و به دریافت کنندگان غیر مجاز نرسیده است.

د- کلیدی کدگذاری شده است که برای رمزگشایی یک ایمیل مورد استفاده قرار می گیرد.

۴۱-نوعی از کوکی ها که پس از خروج از مرورگر به طور اتومات حذف می گردند چه نام دارد؟

الف- Session Cookie

ب- Persistent Cookie

ج- Secure Cookie

د- Authentication Cookie

۴۲-در تنظیمات تب Security در اینترنت اکسپلورر انتخاب گزینه Local Internet به چه معناست؟

الف- قبول شرایط موجود در شبکه داخلی سازمان

ب- قبول تمام سایتها با ضریت امنیت متوسط

ج- انتخاب ضریب امنیت بسیار بالا برای سایتهای لیست شده

د- انتخاب ضریب امنیت پایین برای سایتهای لیست شده

۴۳-بهترین گزینه بعنوان هدف اصلی از حذف کوکی ها در سیستم کاربر کدام است؟

الف- جلوگیری از تشخیص سایتهای مشاهده شده

ب- جلوگیری از سرقت اطلاعات کارت اعتباری و یا رمز عبور

ج- امکان استفاده بدافزارها از کوکی ها برای نفوذ به سیستم

د- بالا رفتن سرعت بازکردن سایتها

۴۴-امضای دیجیتال به چه منظور مورد استفاده قرار می گیرد؟

الف- تایید هویت شخص ارسال کننده ایمیل

ب- امکان ردیابی سایتهای بازدید شده

ج- جلوگیری از هک ایمیلهای ارسالی

د- تایید صحت فایل ارسال شده به مقصد

۴۵-یک نامه الکترونیکی فوری که از یک منبع غیرمتداول ارسال و خبر از وجود و یا شیوع یک ویروس می نماید و از شما می خواهد که با فوروارد نمودن نامه الکترونیکی ، موضوع را سریعا به اطلاع سایر دوستان خود برسانید ، عموما یک ..... است .

الف- گزارش دروغین (Hoax)

ب- خبرنامه امنیتی

ج- ویروس

د- کرم

۴۶-برای کنترل IP هایی که به جی میل مان دسترسی داشته اند، کدام گزینه را باید بررسی کنیم؟

الف- Last account activity

ب- Forwarding and POP/IMAP

ج- IP checking

د- Access control

۴۷-برای اینکه همزمان ایمیلهایی که برای شما ارسال می گردد، به یک ایمیل دیگر نیز ارسال گردد از کدام گزینه در تنظیمات جی میل استفاده می شود؟

الف- Merging Email

ب- Forwarding address

ج- POP forward

د- IMAP forward

۴۸-سایت هائی که امکان درج داده را برای کاربران فراهم نموده ولی بدرستی وضعیت داده ورودی را به منظور وجود تگ های اسکریپت آسیب پذیر بررسی نمی نمایند ، می توانند در مقابل ..... آسیب پذیر باشند .

الف- ویروس ها

ب- حملات Cross-site Scripting و یا XSS

ج- Blue Screens of Death

د- شبکه های P2P

۴۹-جهت افزایش امنیت کاربران در زمان استفاده از اینترنت، کدام یک از ویژگی های زیر را می بایست در نواحی Restricted و Internet مرورگرهای وب غیر فعال نمود ؟

الف- دستیابی به اینترنت

ب- فعال نمودن نرم افزار

ج- کدهای مخرب

د- Active Scripting

۵۰-نویسندگان کدهای مخرب از ..... به منظور جلب توجه کاربران و ترغیب آنان به باز نمودن نامه های الکترونیکی استفاده می نمایند.

الف- عنوان نامه های الکترونیکی

ب- ضمائم نامه های الکترونیکی

ج- محتویات یک نامه الکترونیکی

د- اسپم

۵۱-از چه نوع نرم افزاری می بایست به منظور تشخیص کدهای مخرب موجود در نامه های الکترونیکی استفاده نمود ؟

الف- Windows Update

ب- سیستم تشخیص مزاحمین (IDS)

ج- آنتی ویروس

د- فایروال

۵۲-یکی از راه ها برای بستن ایمیل های اسپم و تبلیغاتی و ناخواسته استفاده از Open mail relays است، برای تنظیم و جلوگیری از ورود این ایمیل های غیر مجاز به سراغ کدام سرویس می بایست رفت؟

الف- SMTP Server

ب- Firewall

ج- POP3 Server

د- IMAP Server

۵۳-برای پاک کردن اطلاعات دیسک سخت از کدام روش استفاده می شود؟

الف- نرم افزار Eraser

ب- نرم افزار Ccleaner

ج- استفاده از ابزار Degausser

د- استفاده از Schedule

۵۴-کدام یک از معایب VPN در حالت site-to-site است؟

الف- Confidentiality

ب- Authentication
ج- Continuous cut
د- Data integrity
۵۵-برای بررسی IP هایی که Gmail شما از طریق آن سیستم ها لاگین کرده است کدام گزینه را می بایست چک کرد؟
الف- Activity on this account
ب- Show an alert for unusual activity
ج- Sign-in & Security
د- Device activity & notifications
۵۶-کدام یک از حملات جزء حملات غیر فعال (Passive) محسوب می گردد.
الف- تصدیق سندیت
ب- دست کاری کردن
ج- استراق سمع
د- جعل شخصیت
۵۷--------- پردازشی است که در آن اطلاعات به شکلی دیگر درمی آیند و آن را از دید مزاحمان پنهان و فقط برای دریافت کننده اصلی قابل شناسایی می کنند
الف- Encryption
ب- Decryption
ج- Hashing
د- Coding
۵۸-چگونه متوجه دستکاری ایمیل دریافتی گردیم؟
الف- امضای دیجیتال حذف و یا تغییر می کند
ب- فرستنده نامه تغییر می کند.
ج- پیام هشدار بر روی سیستم ظاهر می گردد
د- ایمیل در لیست ایمیلهای خوانده شده قرار می گیرد.
۵۹--------- نوعی سرویس ارتباطات است که امکان ایجاد اتاق گفتگو برای برقراری ارتباط همزمان در اینترنت را فراهم می کند.
الف- امضاء دیجیتال
ب- پیام فوری
ج- شبکه اجتماعی
د- ایمیل
۶۰-به امضای الکترونیکی که به طور اتوماتیک به انتهای ایمیل های ارسالی شما از طریق آن اکانت اضافه می‌شود چه می گویند؟
الف- Responder
ب- Footer E-mail
ج- Autograph
د- Signature
۶۱-کدام نوع پسورد امنیت بالاتری دارد؟
الف- Numbers Password

ب- Complex password

ج- Date Password

د- Simple Password

۶۲-تهیه نسخه پشتیبان از داده های مهم شرکت از وظایف چه شخصی است؟

الف- برنامه نویس پایگاه داده

ب- مسئول پشتیبانی

ج- مدیر شبکه

د- طراح سایت

۶۳-مکانیزم دست تکانی سه‌طرفه یا Three way Handshaking جهت برقراری یک اتصال مطمئن شامل چه مراحلی است؟

الف- الف)(۱)SYN-(2)SYN/ACK-(3)ACK

ب- ب) (۱)SYN-(2)SYN-(3)ACK

ج- ج) (۱)SYN-(2)ACK-(3)FIN

د- د) (۱)SYN-(2)ACK-(3)RST

۶۴-نرم افزار ارایه شده توسط مایکروسافت برای رمزگذاری یک درایو چه نام دارد؟

الف- Windows defender

ب- Bit Locker

ج- EFS

د- Hardwar Lock

۶۵-کدام روش پارتیشن بندی امنیت بالاتری دارد؟

الف- Mirror

ب- Stripe

ج- Raid-5

د- Raid-6

۶۶-در صورتی که اولین بوت در BIOS بجای هارد دیسک USB Flash تنظیم شده باشد چه مشکلی ممکن است رخ دهد.

الف- امکان اتصال فلش وجود ندارد

ب- مهاجم با استفاده از فلش بوت اقدام به استخراج اطلاعات کند

ج- چون هارد بعنوان دومین بوت معرفی شده بالا نمی آید.

د- حتما می بایست هارد اکسترنال داشته باشیم تا ویندوز بالا بیاید.

۶۷-خطرناک ترین افرادی که ممکن است به اطلاعات شبکه تحت کنترل شما آسیب بزنند کدام است؟

الف- کارمندان خود شرکت بصورت خواسته یا ناخواسته.

ب- پیمانکارانی که به صورت مقطعی مشغول بکار می شوند.

ج- هکرها و کرکرها

د- برنامه نویسان خبره

۶۸-کدام نرم افزار قابلیت حذف فایلهای موقت اضافی تولید شده توسط ویندوز را دارد؟

الف- Shredder

ب- CCleaner

ج- Degausser

د- Eraser

۶۹-------- ویژگی است در سیستم عامل ویندوز ۸ و بالاتر که امکان ترکیب چندین هارد دیسک را با هم داشته و باعث افزایش ایمنی و نگهداری اطلاعات می شود و به Raid نرم افزاری در ویندوز مشهور است.

الف- Bit Locker

ب- resiliency

ج- Storage spaces

د- Windows To Go

۷۰-کدام قابلیت برتری Backupنسبت به RAIDمحسوب نمی شود؟

الف -درRaid تمام کپی ها یکسان تهیه می شوند

ب- در صورت ویروسی شدن بازگردانی اطلاعات در Backup ساده تر است

ج- در صورت خرابی فایل سیستم این خرابی به تمام هاردها منتقل می گردد.

د- در صورت سوختن یک هارد در Raid5 نیاز به فایل Backup می باشد