بسم الله الرحمن الرحیم

مبانی Security+

نگارندگان:

پیمان میرهادی

رضا خلج

مهدی باصفا

انستیتوایزایران

سرشناسه: میرهادی، پیمان، ۱۳۶۱
عنوان و نام پدیدآور: مبانی Security+/ نگارندگان پیمان میرهادی، رضا خلج، مهدی باصفا.
مشخصات نشر: تهران: انستیتو ایز ایران، ۱۳۹۰.
مشخصات ظاهری: ۱۷۸ص.: مصور(بخشی رنگی)، جدول.
شابک : ۵-۰۳۵-۲۰۱-۹۶۴-۹۷۸
وضعیت فهرست نویسی: فیپا
موضوع: شبکه‌های کامپیوتری — اقدامات تامینی
موضوع: شبکه‌های کامپیوتری — اقدامات تامینی — آزمون‌ها
موضوع: کامپیوترها — ایمنی اطلاعات
موضوع: کامپیوترها — ایمنی اطلاعات — آزمون‌ها
موضوع: پایگاه‌های اطلاعاتی — امنیت
شناسه افزوده: خلج، رضا، ۱۳۵۵
شناسه افزوده: باصفا، مهدی، ۱۳۵۹
شناسه افزوده: انستیتو ایز ایران
رده بندی کنگره:TK ۵۱۰۵/۵۹ /م۸۶م۲ ۱۳۹۰
رده بندی دیویی: ۰۰۵/۸
شماره کتابشناسی ملی: ۲۳۹۸۰۳۲

انتشارات انستیتو ایز ایران

- نام کتاب: مبانی Security+
- نگارندگان: پیمان میرهادی، رضا خلج، مهدی باصفا
- نوبت چاپ: چاپ اول - پاییز ۱۳۹۰
- شمارگان: ۲۰۰۰ جلد
- قیمت: ۶۰۰۰ تومان
- شابک: ۵-۰۳۵-۲۰۱-۹۶۴-۹۷۸
- ناظر چاپ: علی نورا... اوغلی
- طراح جلد: مرتضی محمد صادقی

ناشر از همکاری گروه صنایع امنیت فاوا صاایران در چاپ این کتاب به منظور توسعه فناوری اطلاعات و ارتباطات در کشور قدردانی می کند.

خیابان میرداماد- خیابان شهید حصاری (رازان جنوبی) پ۳۶
تلفن: ۲۲۲۵۴۰۷۸ نمابر: ۲۲۲۲۵۲۶۵
www.isishop.ir www.isibook.ir

نمایندگان پخش

انتشارات آتی نگر	۶۶۵۶۵۳۲۶-۰۲۱	انتشارات آگاه	۶۶۴۶۰۹۲۲-۰۲۱
نیه نشر آستان قدس	۶۶۴۰۱۵۲۳-۰۲۱	مهریان	۶۶۹۷۳۱۷۵-۰۲۱
سها دانش	۶۶۵۶۹۸۸۱-۰۲۱	مرکز تحقیقات هسته‌ای	۸۸۳۰۰۹۷۲-۰۲۱
بکتا	۸۸۹۲۰۳۰۲-۰۲۱	رشد اهواز	۲۲۱۷۰۰۰-۰۶۱۱

پیشگفتار

مستند حاضر خلاصه‌ای از مفاهیم کلی امنیت فناوری اطلاعات است که طبق سرفصل‌های آزمون که توسط شرکت معتبر CompTIA ارائه می‌شود گردآوری شده است. به طور کل برای آمادگی آزمون +Security مفاهیم زیر باید پوشش داده شوند:

- ✓ مفاهیم کلی امنیت
- ✓ شناسایی خطرات بالقوه
- ✓ زیرساخت و اتصالات
- ✓ نظارت بر فعالیت و کشف نفوذ
- ✓ پیاده سازی و نگهداری یک شبکه امن
- ✓ امن سازی شبکه و محیط
- ✓ مفاهیم، متدها و استانداردهای رمزنگاری
- ✓ سیاست‌ها و روال های امنیت
- ✓ مدیریت امنیت (Administration)
- ✓ رفع عیب مفاهیم مرتبط با مدیریت امنیت (Troubleshooting)

در آزمون +Security که توسط CompTIA برگزار می‌شود، درصد هر سرفصل در آزمون به این شرح است:

امنیت سیستم ٪۲۱

زیرساخت شبکه ٪۲۰

کنترل دسترسی	٪۱۷
ارزیابی و بررسی	٪۱۵
رمزنگاری	٪۱۵
امنیت سازمانی	٪۱۲

برای نگارش این مستند از کتاب CompaTIA Security+ Deluxe Study Guide نوشته Emmett Dulaney که توسط Wiley Publishing, Inc در سال ۲۰۱۰ منتشر شده بهره برده‌ایم.

این کتاب به دید کاربردی امنیت و نه به محوریت آزمون، نگارش شده است، یعنی اگر خواننده‌ای خود را برای شرکت در آزمون Security+ به جهت دریافت مدرک آن از شرکت ComptTIA آماده می‌کند بهتر است بعد از مطالعه کتاب حاضر، از کتب مرجع معرفی شده خود CompTIA هم بهره برده و سایر سرفصل‌های مرتبط با موضوع را از مرجع معرفی مذکور دریافت نماید.

در پایان شایان ذکر است بی نقصی از آن خداوند متعال است، بنابراین از تمامی خوانندگان عزیز خواهشمندیم نظرات سازنده خود را در مورد این کتاب با مؤلفان در میان بگذارند.

peyman.mirhadi@gmail.com
khalaj@scitco.ir
basafa@scitco.ir

رئیس گروه صنایع امنیت فاوا صاایران

بهمن آصفی

فهرست مطالب

مقدمه: ۱

تست خودارزیابی: ۴

فصل اول: مقدمه

مقدمه ۱۳

۱-۱- امنیت اطلاعات ۱۴

۱-۲- آشنایی با اصول امنیت اطلاعات ۱۵

۱-۲-۱- امن سازی محیط فیزیکی ۱۵

۱-۲-۲- بررسی امنیت محیط فیزیکی ۱۶

۱-۲-۳- امنیت عملکردی ۴۳

۱-۲-۴- امنیت مدیریتی ۴۳

۱-۳- یکپارچه سازی فرآیند امنیت ۴۸

۱-۳-۱- استفاده از آنتی‌ویروس‌ها ۴۸

۱-۳-۲- اعمال سیاست‌های کنترل دسترسی ۴۸

۱-۳-۲-۱- متد کنترل دسترسی اجباری ۴۹

۱-۳-۲-۲- روش کنترل دسترسی اختیاری ۴۹

۱-۳-۲-۳- روش کنترل دسترسی مبتنی بر نقش ۴۹

۱-۳-۳- احراز هویت ۵۰

۱- ۴- توپولوژی‌های امنیت ۶۰

۱-۴-۱- اهداف طراحی ۶۱

۱-۴-۱-۱- قابلیت اطمینان ۶۱

۱-۴-۱-۲- جامعیت ۶۱

۱-۴-۱-۳- دسترس پذیری ۶۱

۱- ۴-۱-۴- مسئولیت پذیری ۶۱

۱-۵- ایجاد مناطق امن ۶۲

۱-۵-۱- اینترنت ۶۲
۱-۵-۲- اینترانت ۶۳
۱-۵-۳- اکسترانت ۶۳
۱-۵-۴- DMZ ۶۴
۱-۶- تکنولوژیهای جدیدتر ۶۵
۱-۶-۲- شبکه‌های محلی مجازی ۶۶
۱-۶-۳- NAT ۶۷
۱-۶-۴- تونل سازی ۶۸
۱-۷ – خلاصه فصل ۷۲

فصل دوم: شناسایی تهدیدات بالقوه

مقدمه ۷۵
۲-۱- شناسایی استراتژی‌های حمله ۷۵
۲-۲- انواع حملات دسترسی ۷۶
۲-۳- حملات تغییر ۷۶
۲-۴- حملات Dos ۷۷
۲-۵- تشخیص حملات معمول ۷۹
۲-۵-۱- حملات در پشتی ۷۹
۲-۵-۲- حملات Spoofing ۷۹
۲-۵-۳- حملات حمله کننده در میان ۸۰
۲-۵-۴- حملات حدس زدن پسورد ۸۱
۲-۵-۵- حملات Replay ۸۱
۲-۵-۶- بالا رفتن اختیارات ۸۲
۲-۶- آشنایی با مفاهیم امنیت IP /TCP ۸۲
۲-۶-۱- لایه کاربرد ۸۳
۲-۶-۲- لایه انتقال ۸۴
۲-۶-۳- لایه اینترنت ۸۴
۲-۶-۴- لایه اتصال به شبکه (فیزیکی) ۸۵
۲-۷- کپسوله سازی ۸۵

۲-۸- کار با پروتکل‌ها و سرویس‌ها ۸۶
۲-۸-۱- پورت ۸۶
۲-۸-۲- دست دادن ۸۷
۲-۸-۳- API ۸۷
۲-۹- شناسایی حملات TCP/IP ۸۸
۲-۹-۱- Sniffing ۸۸
۲-۹-۲- اسکن کردن پورت‌ها ۸۹
۲-۱۰- حملات TCP ۸۹
۲-۱۰-۱ حمله شماره ترتیبی ۸۹
۲-۱۱- حملات UDP ۹۰
۲-۱۲- OVAL ۹۰
۲-۱۳- کدهای مخرب ۹۲
۲-۱۳-۱- ویروس‌ها ۹۲
۲-۱۳-۱-۱- نشانه‌های آلودگی به ویروس ۹۳
۲-۱۳-۱-۲- ویروس‌ها چطور کار می‌کنند؟ ۹۳
۲-۱۴- انواع ویروس‌ها ۹۴
۲-۱۴-۲- اسب‌های تروجان ۹۷
۲-۱۴-۳- کرم‌ها ۹۷
۲-۱۴-۴- مهندسی اجتماعی ۹۷
۲-۱۵- خلاصه فصل ۹۸
۲-۱۶- آزمایشگاه ۹۸

فصل سوم: زیرساخت و اتصالات

مقدمه ۱۰۱
۳-۱- آشنایی با تجهیزات زیرساختی شبکه ۱۰۱
۳-۱-۱- فایروال‌ها ۱۰۱
۳-۱-۱-۱- فایروال‌های فیلترکننده بسته‌ها ۱۰۲
۳-۱-۱-۲- فایروال‌های پروکسی کننده ۱۰۲
۳-۱-۱-۳- فایروال Inspection Stateful ۱۰۲

۳-۱-۲- هاب ۱۰۳
۳-۱-۳- مودم ۱۰۳
۳-۱-۴- RAS ۱۰۳
۳-۱-۵- روترها ۱۰۴
۳-۱-۶- سوئیچ‌ها ۱۰۷
۳-۱-۷- VPN ۱۰۷
۳-۱-۸- WAP ۱۰۸
۳-۲- نظارت و تشخیص عیب شبکه‌ها ۱۰۹
۳-۲-۱- مانیتور کننده‌های شبکه ۱۰۹
۳-۲-۲- IDSها ۱۰۹
۳-۲-۳- امن‌سازی ایستگاه‌های کاری و سرورها ۱۱۰
۳-۲-۴- تجهیزات بی‌سیم ۱۱۰
۳-۳- دسترسی از راه دور ۱۱۱
۳-۳-۱- پروتکل PPP ۱۱۱
۳-۳-۲- پروتکل‌های تونل سازی ۱۱۱
۳-۳-۳- RADIUS ۱۱۲
۳-۳-۴- TACACS+ ۱۱۲
۳-۴- امن سازی ارتباطات اینترنتی ۱۱۳
۳-۵- اتصالات وب امن ۱۱۵
۳-۶- آسیب پذیری‌های Web add – ins ۱۱۵
۳-۷- خلاصه فصل ۱۱۶
۳-۸- آزمایشگاه ۱۱۶

فصل چهارم: نظارت بر فعالیت‌ها و تشخیص نفوذ

مقدمه ۱۱۹
۴-۱- آشنایی با انواع مختلف ترافیک شبکه ۱۱۹
۴-۱-۱- ICP/IP ۱۱۹
۴-۱-۲- پروتکل‌های Novell ۱۲۰
۴-۱-۳- پروتکل‌های مایکروسافت ۱۲۱

۴-۲- آشنایی با IDS ها ۱۲۳
۴-۲-۱- IDS های مبتنی بر شبکه ۱۲۳
۴-۲-۲- IDS های مبتنی بر میزبان ۱۲۴
۴-۳- آشنایی با سیستم‌های بی‌سیم ۱۲۶
۴-۳-۱- WTLS ۱۲۶
۴-۳-۲- WAP/WEP ۱۲۶
۴-۴- آنالیز کننده‌های پروتکل ۱۲۷
۴-۵- آنالیز و هوش سیگنال ۱۲۷
۴-۶- خلاصه فصل ۱۲۸
۴-۷- آزمایشگاه ۱۲۸

فصل پنجم: پیاده سازی و نگهداری شبکه امن

مقدمه ۱۳۱
۵-۱- خطوط پایه امنیت ۱۳۱
۵-۲- ارتقا و به روز نگه داشتن سیستم عامل ۱۳۲
۵-۳- مقاوم سازی برنامه‌های کاربردی ۱۳۳
۵-۳-۱- مقاوم سازی سرورهای وب ۱۳۳
۵-۳-۲- پیکربندی پروتکل‌های شبکه ۱۳۳
۵-۳-۳- Binding Network ۱۳۴
۵-۴- مخازن داده ۱۳۴
۵-۴-۱- سرویس‌های دایرکتوری ۱۳۴
۵-۴-۲- LDAP ۱۳۴
۵-۴-۳- Active Directory ۱۳۵
۵-۴-۴- eDirectory ۱۳۵
۵-۵- کنترل دسترسی ۱۳۵
۵-۵-۱- موانع فیزیکی ۱۳۵
۵-۵-۲- مناطق امن ۱۳۵
۵-۵-۳- بیومتریک ۱۳۶
۵-۶- برنامه‌ریزی پیوستگی کار ۱۳۶

۵-۶-۱- تحلیل تأثیر کسب و کار ۱۳۶
۵-۶-۲- ارزیابی خطر ۱۳۶
۵-۷- سیاست‌ها، استانداردها و خطوط راهنما ۱۳۸
۵-۷-۱- سیاست‌ها ۱۳۸
۵-۷-۲- تعریف استانداردها ۱۳۸
۵-۷-۳- خطوط راهنما ۱۳۸
۵-۸- استانداردهای امنیت و ISO17799 ۱۳۹
۵-۹- دسته بندی اطلاعات ۱۳۹
۵-۱۰- پایگاه داده و تکنولوژیها ۱۴۰
۵-۱۱- خلاصه فصل ۱۴۱
۵-۱۲- آزمایشگاه ۱۴۱

فصل ششم: رمزنگاری

مقدمه ۱۴۵
۶-۱- رمزنگاری فیزیکی ۱۴۵
۶-۲- رمزنگاری محاسباتی ۱۴۵
۶-۳- PKI ۱۴۶
۶-۳-۱- CA ۱۴۷
۶-۳-۲- پیاده سازی مجوزها ۱۴۷
۶-۳-۳- لغو مجوزها ۱۴۸
۶-۴- حملات به رمزنگاری‌ها ۱۴۸
۶-۵- استانداردها و پروتکل‌های رمزنگاری ۱۴۹
۶-۵-۱- PKI X-509 ۱۵۰
۶-۵-۲- SSL و TLS ۱۵۰
۶-۵-۳- پروتکل مدیریت مجوز ۱۵۱
۶-۵-۴- MIME/S ۱۵۱
۶-۵-۵- SET ۱۵۱
۶-۵-۶- Secure Shell ۱۵۲
۶-۵-۷- IP Security ۱۵۳

۶-۵-۸- Common Criteria و WTLS ۱۵۳
۶-۶- مدیریت کلید ۱۵۴
۶-۶-۱- تولید کلید متقارن و نامتقارن ۱۵۴
۶-۷- خلاصه فصل ۱۵۶
۶-۸- آزمایشگاه ۱۵۶

فصل هفتم: سیاستهای امنیت

مقدمه ۱۵۹
۷-۱- تداوم کسب و کار ۱۵۹
۷-۲- پشتیبانی سازنده (Vendor) ۱۶۱
۷-۳- مدیریت دسترسی ۱۶۱
۷-۴- بازرسی ۱۶۲
۷-۵- سیاست‌ها و روال‌ها ۱۶۳
۷-۶- سایت‌های مهم ۱۶۴
۷-۷- آزمایشگاه ۱۶۴

مقدمه:

چنانچه شما خود را برای امتحان +Security آماده می‌کنید، بدون شک اطلاعات فراوانی را در خصوص رایانه و امنیت فیزیکی خواهید یافت. این اطلاعات در دسترس شما بوده و با آنها تمرین می‌کنید و با آسودگی خاطر و دستی پر به استقبال امتحان خواهید رفت. این کتاب به عنوان راهنمای آموزش با ذهنیت افزایش دید کاربردی امنیت طراحی شده است. بنابراین سعی داریم تا در این کتاب اطلاعات مورد نظر را در خصوص امنیت رایانه در اختیار شما قرار دهیم.

این کتاب در فصل‌های مختلف همراه با ارائه مواد امتحانی سازماندهی شده است. اگر شما به موارد خاصی نیاز دارید، می‌توانید هر نکته ای را در فصلی که این موارد در آن قرار دارد، بیابید. کتاب حاضر موادی را در سطح متوسط فنی و تخصصی همراه با آزمون، درک مفاهیم امنیتی، سیستم عامل و نرم افزارهای کاربردی به شما ارائه خواهد نمود تا درک کامل و جامعی از امنیت رایانه را به عنوان حرفه امنیتی کسب نمایید. در انتهای هر فصل به مرور سؤالات تستی مشابه آزمون و امتحان پرداخته شده است.

چنانچه فیلد کاری یا رشته شما امنیتی است، پیشنهاد می‌کنیم تا به منظور محک سطح مهارت شما، در ابتدا به این سؤالات بپردازید. سپس شما می‌توانید از کتاب در جهت رفع کاستی‌ها و نقاط ضعف و شکاف موجود در دانش‌تان بهره بگیرید. استفاده از این راهنمای امنیتی شما را در جهت کسب دانش ابتدایی قبل از امتحان، یاری خواهد نمود. چنانچه شما به سؤالات ارائه شده در هر فصل بطور صحیح پاسخ دهید، شما می‌توانید با اطمینان فصل‌های بعدی را ادامه دهید و اگر قادر نباشید که به بیشتر سؤالات پاسخ صحیح بدهید، فصل را مجدداً بازخوانی کرده و سعی کنید به سؤالات به صورت صحیح پاسخ دهید. نمره امتحان شما می‌بایست بهبود داشته باشد.

اخطار:

تنها سؤالات و پاسخ‌ها را مطالعه نکنید. سؤالات در امتحان واقعی، از تمرین و تست موجود در این کتاب متفاوت خواهد بود. آزمون به منظور تست و آزمایش میزان دانش شما از مفاهیم یا اهداف طراحی شده است. بنابراین استفاده از این کتاب برای یادگیری و آموزش موضوعات امنیتی قبل از سؤالات مفید خواهد بود.

گواهینامه Security+ چیست؟

امنیت رایانه حوزه ای است که شروع به رشد نموده و جای خود را در میان علوم مختلف رایانه‌ای باز نموده است. این رشته شامل قلمرو وسیعی از مفاهیمی است که دریافت همه جنبه های مرتبط با امنیت در آن امری است مشکل. انتشار ویروس‌ها، کدهای مخرب، خرابکاری بین المللی و حتی تروریسم تنها بخشی از حوزه‌هایی است که مشاغل امنیتی می‌بایست به آن توجه نمایند. چالش‌های شما هم شامل مساعدت در اجرای موضوعات امنیتی است و هم شامل همفکری سازمانتان در مورد آنچه که موجب بهبود امنیت می‌گردد.

آزمون Security+ درک و فهم شما را از تکنولوژی‌های رایج مورد استفاده در رایانه‌های امروزی و نیز دانش و آگاهی شما را از چگونگی تأثیرات امنیتی در یک سازمان محک می‌زند. شما می‌توانید منتظر سؤالاتی باشید که بر هر دو موضوع سیاست یا خط‌مشی و تکنیکی یا فنی تأثیر گذار خواهند بود. از دیدگاه این امتحان، هر دو این حوزه‌ها به هم مرتبط بوده و می‌بایست با یکدیگر دیده شده و مورد بحث قرار گیرند. این آزمون به همه استانداردهای فنی مختلف نمی پردازد، لکن بر روی فهم آنچه این تکنولوژی‌ها بتوانند درجهت بهبود امنیت انجام دهند، متمرکز می‌شود. آزمون چند گزینه‌ای است و سؤالات نیز نسبتاً آسان هستند.

چرا گواهینامه Security+ پیشنهاد می‌شود؟

چند دلیل برای اخذ گواهینامه Security+ وجود دارد:

۱. نشان دهنده مدرک تحصیل حرفه ای و تخصصی است.
۲. قابلیت حضور شما در عرصه بازار را گسترش می‌دهد.
۳. فرصت‌های پیشرفت بیشتری را برای شما فراهم می‌آورد.
٤. تاحدود زیادی نیاز برخی انواع آموزش‌های پیشرفته را برآورده می‌کند.
۵. اطمینان مشتری از شما و شرکتتان را ارتقاء می‌بخشد.

چه انتظاراتی از آزمون وجود دارد؟

آزمون Security+ شامل ۱۰۰ سؤال بوده و به شما ۹۰ دقیقه زمان برای امتحان اختصاص می‌یابد، بنابراین لازم است از وقت و زمان اختصاص یافته نهایت استفاده را ببرید. حداقل امتیاز ۷٦٤ بوده که برمبنای امتیاز ۱۰۰ تا ۹۰۰ امتیازبندی شده است. به محض اتمام امتحان، نتایج شما مشخص خواهد

شد. متأسفانه داوطبین قادر به مشاهده پاسخ‌های تست نادرست خود نیستند. این پروسه در مکانی است که صحت و درستی آزمون گواهینامه را تضمین کرده و آن را برای همیشه ایمن نگاه دارد. این موضوع این تداعی را در ذهن ایجاد می‌کند که آزمون یک امتحان امنیتی قانونی است. بعد از اینکه شما توانستید از امتحان سربلند بیرون آیید و در امتحان +Security نمره قبولی را کسب نمایید، CompTIA به شما گواهینامه قبولی اهداء می‌کند که در امور مختلف کاری و فعالیتهای بعدی زندگی مورد استفاده شما قرار خواهد گرفت. معمولاً بین چهار تا شش هفته پس از قبولی در آزمون، گواهینامه +Security به همراه کارت شناسایی به صورت رسمی به شما ارائه خواهد شد. (چنانچه شما تا هفته هشتم پس از قبولی در امتحان، گواهینامه را دریافت نکردید، مستقیماً به CompTIA مراجعه تا اطلاعات شما در بسته ثبت نامی مجدداً مورد بررسی قرار گرفته و برای شما گواهینامه صادر گردد)

نحوه استفاده از این کتاب:

دراین کتاب چندین ترکیب تست برای شما آورده شده است. این ابزارها به شما در جهت حفظ مندرجات آزمون اصلی کمک خواهد کرد و شما را برای آزمون حقیقی به خوبی آماده خواهد نمود. با بکارگیری هریک از این تستهای مرسوم، شما قادر به شناسایی صحیح نقاط ضعف خواهید بود و سپس می‌توانید استراتژی مطالعات منسجم خود را با استفاده از هریک از ویژگیهای قوی تست، بسط و گسترش دهید. قبل از آنکه مطالعه فصول کتاب را آغاز نمایید، در قسمت شروع کتاب(بعد از مقدمه) یک بخش تست خودارزیابی وجود دارد که شما می‌توانید با استفاده از آن، میزان آمادگی خود را برای آزمون نهایی محک بزنید. پیشنهاد می‌شود قبل از شروع مطالعه کتاب حتماً این تستها را پاسخ دهید. انجام این اقدام شما را در تعیین نقاط و حوزه‌هایی که نیازمند تجدید نظر هستید، یاری خواهد نمود. پاسخ هرتست ارزیابی، پس از آخرین پرسش تست، در صفحه‌ای جداگانه آمده است. هرپاسخ شامل یک شرح و توضیح و یک نکته ای است که به شما جهت درک بیشتر مطالب کتاب کمک می‌کند.

سؤالات مرور فصل‌ها:

میزان آگاهی شما از پیشرفت در کتاب را ارزیابی می‌کند. پاسخ‌ها در انتهای هرفصل موجود می‌باشد. هنگامی که مطالعه هرفصل به پایان رسید، به پرسش‌های مروری پاسخ داده و سپس بررسی کنید که به هریک پاسخ صحیح داده‌اید یا خیر. پاسخ صحیح تستها در صفحه بعد از آخرین سؤال

مروری آورده شده است. شما می‌توانید با مطالعه مجدد بخشی که پاسخ اشتباه داده اید، پاسخ صحیح را دریافت نمایید. نهایتاً در مورد درک موضوعات کتاب ارزیابی خواهید شد.

ماشین تست:

برای شما دو نمونه آزمون آورده شده است: تست ارزیابی اولیه و تست‌های مرور فصول

چنانچه صرفاً قصد دارید در امتحان نهایی شرکت کنید(به عنوان مثال بدون وجود منبع مطالعاتی) توصیه می‌شود تا به این نمونه سؤالات پاسخ دهید. هنگامی که شما موفق به پایان اولین آزمون شدید، به آزمون بعدی مراجعه تا مهارتهای تستی شما محک زده شود. اگر شما موفق شدید به ۹۰ درصد سؤالات پاسخ صحیح بدهید، شما آمادگی لازم برای شرکت در آزمون اصلی و اخذ گواهینامه را کسب نمودید.

تست خودارزیابی:

۱. کدامیک از انواع ممیزی‌ها تعیین می‌کند چه حسابهای کاربری بطور صحیح ایجاد شده و مراحل حقوق دسترسی اتفاق نمی افتد؟

الف) ممیزی حقوق دسترسی ب) ممیزی کاربردی

ج) ممیزی افزایشی د) ممیزی گزارشی

۲. یک سخت افزار دسترسی فیزیکی که در میزان دسترسی تعداد اندکی از افراد، ایجاد محدودیت می‌نماید چه نام دارد؟

الف) Checkpoint ب) Perimeter Security

ج) Security Zone د) Mantrap

۳. کدامیک از موارد زیر به عنوان مجموعه قوانین استاندارد اختیاری رمزنگاری به شمار می‌رود؟

الف) PKI ب) PKCS

ج) ISA د) SSL

٤. کدام پروتکل‌های زیر به منظور ایجاد یک محیط امن در شبکه بی‌سیم مورد استفاده قرار می‌گیرد؟

الف) WAP ب) WEP

ج) WTLS د) WML

۵. واسط کاربری (اینترفیس) سرور اینترنت همراه با TCP/IP در کدام لایه مدل DOD قرار دارد؟
الف) لایه انتقال ب) لایه شبکه
ج) لایه پردازش د) لایه اینترنت

۶. فرض کنیم شما قصد دارید تا یک ارتباط شبکه ای را میان دو LAN با استفاده از اینترنت برقرار نمایید. کدام توپولوژی بهتر این کار را برای شما انجام می‌دهد؟
الف) IPSec ب) L2TP ج) PPP د) SLIP

۷. کدام طراحی مفهومی دسترسی کاربران بیرونی به سیستم‌های حفاظتی LAN داخلی را محدود می‌کند؟
الف) DMZ ب) VLAN
ج) I&A د) Router

۸ در فرآیند بازیابی کلید، کدام کلید می‌بایست قابل بازیابی باشد؟
الف) Rollover key ب) Secret key
ج) Previous key د) Escrow key

۹. جمله‌ای که به منظور ایجاد اضافه بار در پروتکل یا سرویس خاص می‌گردد، چه نام دارد؟
الف) Spoofing ب) Back door
ج) Man in the middle د) Flood

۱۰. بخشی از IDS که داده‌ها را جمع آوری می‌کند چه نام دارد؟
الف) منبع داده ب) سنسور
ج) رویداد د) تحلیل‌گر

۱۱. فرآیندی که امنیت سیستم‌عامل را در برابر حملات ایجاد می‌کند چه نام دارد؟
الف) Hardening ب) Tuning
ج) Sealing د) Locking down

۱۲. آدرس‌های واقعی یکپارچه مرتبط با کدام خصوصیت امنیت اطلاعات هستند؟
الف) تأیید اطلاعاتی که صحیح هستند.
ب) تأیید اصولی که بطور صحیح نگهداری می‌شوند.
ج) ایجاد کنترل دسترسی شفاف داده‌ها
د) تأیید داده‌هایی که به‌صورت خصوصی و امن نگهداری شده‌اند.

۱۳. کدام مکانیزم بوسیله PKI به منظور بررسی سریع صحت تأییدیه مورد استفاده قرار می‌گیرد؟

الف) CRL ب) MD5

ج) SSHA د) OCSP

۱٤. کدامیک از موارد زیر معادل یک VLAN از چشم‌انداز امنیت فیزیکی است؟

الف) امنیت پیرامونی(Perimeter security)

ب) جداسازی و قسمت‌بندی(Partitioning)

ج) مناطق امنیتی (Security zones)

د) حصار پیرامونی (Physical barrier)

۱۵. گزارش رسیده از کاربر شما، حاکی از دانلود فایلی از یک کلاینت با استفاده از IM بوده است. اطلاعات کاربر نشان می‌دهد که فایل خوانده شده account.doc نام دارد. سیستم از زمان دانلود رفتار غیرعادی داشته است. کدام مورد مشابه اتفاق روی داده است؟

الف) کاربر شما سهواً ویروسی را با استفاده از IM دانلود کرده است.

ب) کاربر شما مستعد خرابی درایو هارد می‌باشد.

ج) کاربر شما دچار ناراحتی بوده و نیاز به افزایش دارو دارد.

د) سیستم مبتلا به امواج قوی شده است.

۱٦. مکانیزم فعال یا غیرفعال کردن دسترسی به منابع شبکه برمبنای آدرس IP چه نام دارد؟

الف) NDS ب) ACL

ج) Hardening د) Port blocking

۱۷. کدامیک از موارد زیر امنیت بیشتری را برای سرور WWW اینترنت فراهم می‌آورد؟

الف) تغییر آدرس پورت به ۸۰

ب) تغییر آدرس پورت به ۱۰۱۹

ج) افزودن فایروال به منظور انسداد پورت ۸۰

د) سرورهای WWW نمی توانند امن باشند

۱۸. برنامه‌ای که قابلیت انتشار و گسترش به سایر سیستم‌ها به صورت ابتدایی را دارد، چه نامیده می‌شود؟

الف) ویروس ب) اسب تروجان

ج) بمبهای منطقی د) کرم

۱۹. شخصی به عنوان تعمیرکار خدماتی در اداره شما حضور می‌یابد. او قصد دارد تا در زمینه تنظیمات سرورهای رایج شما گفتگو کند. این موضوع ممکن است مثالی از کدام نوع حمله باشد؟

الف) مهندسی اجتماعی ب) کنترل دسترسی

ج) استتار پیرامونی د) مهندسی رفتار

۲۰. کدامیک از موارد زیر به عنوان یک مشکل اصلی در سرورهای FTP شناخته می‌شود؟

الف) فایل‌های پسورد در ناحیه ناامن روی دیسک ذخیره می‌شوند.

ب) بخشهای حافظه می‌توانند دسترسی به فایل را با مشکل مواجه نمایند.

ج) شناسه کاربری و پسورد کاربران رمز نمی شوند.

د) سایتهای FTP ثبت نشده اند.

۲۱. کدام سیستم را به منظور محافظت فعال و اعلام مشکلات امنیتی در یک شبکه متصل به اینترنت، نصب می‌کنید؟

الف) IDS ب) مانیتورینگ شبکه

ج) روتر د) VPN

۲۲. فرآیند بررسی و تعیین مراحل حفظ صحت مدارک چه نام دارد؟

الف) رسیدگی و تجسس امنیتی

ب) زنجیره حفاظتی

ج) سه AAA از فرآیند رسیدگی و تجسس

د) سیاست امنیتی

۲۳. فرآیند رمزنگاری پیام به منظور مخفی کردن آن از دیگران چه نام دارد؟

الف) پنهان‌نگاری ب) درهم‌سازی

ج) MDA د) Cryptointelligence

۲٤. سیاستی که تعیین‌کننده نحوه استفاده از رایانه‌ها در یک سازمان است، چه نام دارد؟

الف) سیاست امنیتی ب) سیاست کاربری

ج) سیاست کاربردی د) سیاست اجرایی

۲۵. کدام الگوریتم به منظور ایجاد نشست امن موقتی برای تبادل اطلاعات کلید مورد استفاده قرار می‌گیرد؟

الف) KDC ب) KEA

ج) SSL د) RSA

۲۶. شما برای انجام مشورت در زمینه امنیت تجهیزات قابل حمل مانند PDA فراخوانده شده اید. به شما گفته می‌شود که باید از سیستم نامتقارن استفاده نمایید. کدام استاندارد امنیتی را پیشنهاد می‌کنید؟

الف) ECC ب) PKI

ج) SHA د) MD

۲۷. کدامیک از روشهای پشتیبان‌گیری زیر بطور معمول سریعترین زمان ایجاد پشتیبان را فراهم می‌آورد؟

الف) Full backup ب) Incremental backup

ج) Differential backup د) Archival backup

۲۸. کدام روش امنیتی زیر مورد استفاده در خصوصیت فیزیکی به عنوان روش تعیین هویت مورد استفاده قرار می‌گیرد؟

الف) کارت هوشمند ب) I&A

ج) بیومتریک د) CHAP

۲۹. اصولاً کدام روش کنترل دسترسی مرتبط با نقش افراد در سازمان است؟

الف) MAC ب) DAC

ج) RBAC د) STAC

۳۰. فرآیند رسیدگی به سیستم رایانه‌ای به منظور دریافت سرنخ‌های حادثه، چه نام دارد؟

الف) قوانین رایانه ای ب) اسکن ویروس

ج) سیاست امنیتی د) جمع‌آوری مدارک

پاسخ تست خودارزیابی:

۱. الف) ممیزی حقوق دسترسی به منظور تعیین کلیه گروه‌ها، کاربران و سایر حسابهای کاربری مرتبط با حقوق دسترسی واگذارشده برابر سیاست امنیتی یک سازمان، مورد استفاده قرار می‌گیرد.

۲. د) mantrap سخت افزاری است مانند یک اتاق کوچک که میزان دسترسی به افراد را محدود می‌کند. این تجهیزات معمولاً از قفلهای الکترونیکی و سایر روشهای دیگر به منظور کنترل دسترسی استفاده می‌کنند.

۳. ب) استانداردهای رمزنگاری کلید عمومی یک مجموعه استانداردهای اختیاری برای رمزنگاری کلید عمومی به‌شمار می‌روند. این مجموعه استانداردها متناسب با کمپانی RSA هستند.

٤. ب) Wired Equivalent Privacy (WEP) به منظور تأمین امنیت شبکه بی‌سیم طراحی شده است. WEP معروف به دارا بودن آسیب‌پذیری‌ها و عدم توجه به امنیت سطح بالا است.

۵. ج) واسط کاربری (اینترفیس) لایه پردازش همراه با نرم‌افزارهای کاربردی و ترافیک فشرده درون HOST-to-HOST یا لایه انتقال، لایه اینترنت و لایه دسترسی شبکه.

٦. ب) L2TP پروتکل تونلینگ است که می‌تواند مابین شبکه‌های LAN مورد استفاده قرار گیرد. این پروتکل امن نیست، درنتیجه به منظور تأمین داده‌های امن می‌بایست همراه با آن از IPSec نیز استفاده نمایید.

۷. الف) DMZ ناحیه‌ای درشبکه است که برای کاربران نامعتبر ایجاد محدودیت می‌نماید و دسترسی کاربران و سیستمهای خارجی را به شبکه داخلی ایزوله می‌کند. این امر با استفاده از روترها و فایروال‌ها به منظور محدودیت در دسترسی به منابع حساس شبکه صورت می‌گیرد.

۸. ج) فرآیند بازیابی کلید باید قادر به بازیابی کلید قبلی باشد. چنانچه کلید قبلی یافت نشد، کلیه اطلاعاتی که با کلید تبادل شده است، یافت نخواهد شد.

۹. د) حمله flood به منظور اضافه بار پروتکل‌ها یا سرویس‌ها از طریق تکرار یک درخواست برای سرویس طراحی شده است. این نوع حمله معمولاً در حمله DoS نتیجه بخش خواهد بود. این حمله ممکن است از طریق پروتکل freezing یا از پهنای باند بسیار زیاد مورد استفاده در شبکه به سبب درخواستها صورت پذیرد.

۱۰. ب) سنسور اطلاعات را از منبع داده جمع آوری نموده و آن را به تحلیل‌گر(آنالایزر) انتقال می‌دهد. اگر تحلیل‌گر مشخص نماید که فعالیت غیرعادی رخ داده، آلارم می‌دهد.

۱۱. الف) Hardening یا به عبارتی مقاوم سازی اصطلاحی است که فرآیند امنیت سیستم را توصیف می‌کند. این مورد برای بسیاری از روش‌ها شامل غیرفعال سازی پروتکل‌های غیرضروری مورد استفاده قرار می‌گیرد.

۱۲. الف) هدف صحت و یکپارچگی، بررسی و تأیید نمودن اطلاعات از نظر صحیح بودن و عدم تحریف می‌باشد. یکپارچگی علاوه بر مسئولیت اطمینان از صحت اطلاعات، درصورت نیاز مجوز نهایی را برای تأیید این موضوع صادر می‌کند.

۱۳. د) Online Certificate Status Protocol (OCSP) مکانیزمی است که به منظور تسریع در اینکه آیا یک گواهی معتبر است یا خیر، مورد استفاده قرار می‌گیرد. CRL برمبنای قانونی منتشر می‌شود، اما یک بار انتشار آن رایج نیست.

۱۴. ب) قسمت بندی و جداسازی فرآیند تجزیه یک شبکه به اجزاء کوچکتر است تا هرکدام بطور مجزا حفاظت شوند. مفهوم آن شبیه دیوارهای ساختمان در یک ساختمان اداری است.

۱۵. الف) IM و سایر سیستمهای دیگر به کاربران مشکوک اجازه می‌دهند تا فایلهای حاوی ویروس را دانلود نمایند. به دلیل ضعف در قراردادهای نام پسوند فایل، فایلی که ظاهر می‌شود و حاوی یک پسوند است ممکن است عملاً پسوند دیگری داشته باشد. برای مثال فایل mydocument.doc.vbs در بسیاری از نرم‌افزارهای کاربردی به عنوان mydecument.doc ظاهر می‌شود، اما در واقع اسکریپتی از Visual Basic است که می‌تواند حاوی کدهای مخرب باشد.

۱۶. ب) لیستهای کنترل دسترسی (ACL) به منظور اجازه یا رد دسترسی آدرس IP در شبکه بکار می‌روند. مکانیزم‌های ACL در بسیاری از روترها، فایروال‌ها و سایر تجهیزات شبکه کاربردی هستند.

۱۷. ب) پورت پیش‌فرض برای سرویس WWW، پورت ۸۰ است. از طریق تغییر پورت به ۱۰۱۹، کاربران را وادار به استفاده از این پورت در هنگام استفاده از مرورگر(browser) نموده‌اید. این اقدام در فراهم آوردن ارتقاء کوچک امنیتی در وب‌سایت مؤثر است. بکارگیری فایروال به منظور مسدودنمودن پورت ۸۰، امنیت وب‌سایت شما را به میزانی که دسترسی به آن از این طریق امکان‌پذیر نباشد، ارتقاء می‌دهد.

۱۸. د) کرم به منظور تکثیر و انتشار طراحی شده است. کرم‌ها ممکن است حاوی ویروس‌هایی باشند که موجبات تخریب سیستم‌ها را فراهم آورند، اما این مأموریت اصلی‌شان نیست.

۱۹. الف) مهندسی اجتماعی روشی است که افراد زیرک و باهوش به منظور دستیابی به اطلاعات سازمانی شما بکار می‌برند.

۲۰. ج) FTP در اکثر محیط‌ها، اطلاعات حساب‌کاربری و پسوردهای رمزنشده را ارسال می‌کند. در اثر این اقدام و بواسطه حسابهای کاربری آسیب‌پذیر، شبکه مورد شنود قرار خواهد گرفت.

۲۱. الف) سیستم تشخیص نفوذ(IDS) مانیتورینگ فعال و پاسخگویی و واکنش ضابطه‌مندی است در برابر فعالیتهای غیرعادی شبکه. فایروال امنیت غیرفعال را بوسیله جلوگیری از دسترسی ترافیک غیرمجاز فراهم می‌آورد. چنانچه فایروال به مخاطره افتاد، IDS برمبنای قوانین طراحی شده در آن، آلارم می‌دهد.

۲۲. ب) زنجیره حفاظتی اطمینان می‌دهد که هر مرحله اخذ مدارک، از بخش جمع‌آوری مستند و گزارش شده است. زنجیره حفاظتی شامل پرسش‌های چه‌کسی، چه‌چیزی، چه‌وقت، چه‌موقع و چرا از مدارک ذخیره شده است.

۲۳. الف) پنهان‌نگاری (Steganography) فرآیند مخفی‌سازی یک متن در جای دیگر است. همچنین ممکن است در معنای نامرئی نوشتن الکترونیکی بکار رود.

۲٤. ج) استفاده خط‌مشیء به عنوان سیاست کاربردی نیز بکار می‌رود که وضعیت قابل قبول بکارگیری سیستمها و منابع سازمانی توسط کارمندان را تعیین می‌کند. این سیاست می‌بایست شامل خروجی نتایج عدم موفقیت باشد.

۲۵. ب) الگوریتم تغییر کلید(KEA) به منظور ایجاد یک نشست موقتی در جهت تغییر اطلاعات کلید مورد استفاده قرار می‌گیرد. این نشست کلید رمزی را که قبلاً استفاده شده، تولید می‌کند. وقتی کلید تغییر می‌یابد، نشست قانونی و معین، شروع می‌شود.

۲٦. الف) Elliptical Curve Cryptosystem (ECC) یا سیستم رمز منحنی بیضی شکل، شاید بهترین انتخاب شما برای PDA باشد. ECC به منظور کار با پروسسورهای کوچک طراحی شده است. ممکن است سیستمهای دیگر انتخاب شوند، اما آنها نیازمند پردازش قوی‌تر از ECC هستند.

۲۷. ب) incremental backup به دلیل اینکه تنها از فایلهایی نسخه پشتیبان تهیه می‌نماید که از زمان آخرین تغییرات(اضافه یا کاهش) یا پشتیبان‌گیری کلی (full backup) تغییر کرده‌اند، لذا معمولاً سریعترین روش پشتیبان‌گیری به شمار می‌رود.

۲۸. ج) بیومتریک فرآیند احراز هویتی است که برای خصوصیات فیزیکی مورد استفاده قرار می‌گیرد. مانند اسکن کف دست یا الگوی شبکیه چشم درجهت احراز هویت افراد.

۲۹. ج) کنترل دسترسی برمبنای نقش (RBAC) اصولاً مرتبط با تأمین دسترسی به سیستمهایی که کاربر نیازمند آن برمبنای نقشی که در سازمانی ایفا می‌کند، است.

۳۰. الف) قوانین رایانه‌ای فرآیند بررسی و رسیدگی یک سیستم رایانه‌ای است در جهت تعیین علت حادثه. بخشی از این فرآیند شامل جمع‌آوری مدارک و شواهد خواهد بود.