آزمـون عملکردی پودمان دوم: تحلیل امنیت در فاوا(کتاب دانش فنی تخصصی) هنرآموز: معصومه دانیالی

استان : مرکزی شهرستان : اراک

☑	شاخص تحقق: تعیین اجزا مثلث امنیت برای یک کاربرد خاص	در حد انتظار	نمره : ۲

۱ **هر کدام از موارد زیر مرتبط با کدامیک از مفاهیم محرمانگی، دسترس پذیری و جامعیت می باشد.**

جلوی درب ورود به اتاق سرور سیستم تشخیص چهره قرار داده شده است.	
برای ورود به سامانه my medu بعد از ثبت شماره تلفن، رمز یکبار مصرف به گوشی ارسال می شود	
از هر جایی در اینترنت می توانم بر دوربینهای مدار بسته شرکتم نظارت داشته باشم	
آموزش و پرورش سامانه ای راه اندازی کرده که با ورود به آن به راحتی و بدون مراجعه به اداره می توانم آخرین حکم صادره خود را ببینم.	
امروز برای خرید یک مانتو به فروشگاه رفتم متاسفانه بعد از اینکه فروشنده کارت را در دستگاه کشید و پیامک کسر مبلغ از حسابم آمد گفت تراکنش ناموفق بوده و مجدد کارت را کشید و این بار موفقیت آمیز بود قبل از خروج از فروشگاه پیامک دیگری برایم آمد که مبلغ کسر شده اول مجدد به حسابم اضافه شده بود	

☑	شاخص تحقق: • تعیین نقاط آسیب‌پذیر در یک کاربرد خاص و ارائه راهکارهای مناسب جهت اجتناب از حملات • ارائه فهرست اطلاعات ضروری در یک سیستم ثبت رخداد فرضی جهت یک کاربرد خاص	بالاتر از حد انتظار	نمره : ۳

۲ **فرض کنید شما مدیر امنیت یک شرکت بزرگ هستید. اخیراً این شرکت مورد حمله سایبری قرار گرفته است. به سوالات زیر پاسخ دهید و مشخص کنید هر سوال مربوط به کدام مرحله در حفظ امنیت است (پیش از حمله، زمان حمله، پس از حمله):**

چه اقداماتی می‌توانستید انجام دهید تا احتمال وقوع این حمله را کاهش دهید؟

چه نقاط ضعفی در سیستم‌های امنیتی شرکت وجود داشت که منجر به این حمله شد؟

اولین اقداماتی که باید در زمان وقوع حمله انجام دهید چیست؟

چگونه می‌توانید نوع حمله و منبع آن را شناسایی کنید؟

چه اقداماتی برای متوقف کردن حمله و به حداقل رساندن خسارات باید انجام شود؟

چگونه می‌توانید وسعت و عمق نفوذ هکرها را به سیستم‌های شرکتتان تعیین کنید؟

چه اقداماتی برای بازیابی اطلاعات و سیستم‌های آسیب‌دیده باید انجام شود؟

در گزارش‌هایی چه مواردی باید لیست شود و به چه کسانی باید ارائه شود؟

چه اقداماتی برای جلوگیری از تکرار چنین حملاتی در آینده باید انجام شود؟

☑	شاخص تحقق: تعیین و دسته بندی داراییهای یک حوزه کاری و پیشنهاد سطح دسترسی به دارایی ها	در حد انتظار	نمره : ۲

۳	در خبر زیر، سه بخش کنترل دسترسی را تعیین کنید. نرم افزار کتابخوان طاقچه بعد از مطالعه ۱۰۰ کتاب در بخش تخفیفات حساب کاربریم یک کد تخفیف ۶۰ درصدی با کد TG66 تخصیص داد که مدت اعتبار آن ۶ روز است. **Authentication** (احراز هویت) | **Authorization** (اعتبارسنجی) | **Accounting** (حسابرسی) | | |		
	شاخص تحقق: **تعیین عوامل ناامنی برای یک سیستم مشخص**	**پایین تر از حد انتظار**	**نمره : ۱**
۴	فرض کنید شما کارمند یک شرکت بزرگ هستید. یک ایمیل از طرف مدیرتان دریافت می‌کنید که در آن از شما خواسته شده است تا اطلاعات محرمانه شرکت را به یک آدرس ایمیل خارجی ارسال کنید. چه اقداماتی انجام می‌دهید؟ نکات: در پاسخ خود، به نشانه‌های مهندسی اجتماعی در ایمیل اشاره کنید. توضیح دهید که چگونه می‌توانید از صحت ایمیل و فرستنده آن مطمئن شوید. اقداماتی که برای محافظت از اطلاعات محرمانه شرکت باید انجام شود را شرح دهید.		
	شاخص تحقق: **تعیین نوع بدافزار امنیتی و طرح یک سیستم تشخیص یا جلوگیری از حمله برای یک کاربرد خاص**	**در حد انتظار**	**نمره : ۲**
۵	شما مدیر شبکه یک شرکت هستید. ناگهان متوجه می‌شوید که وب‌سایت شرکت شما به دلیل تعداد درخواستهای زیاد از دسترس خارج شده است. این حمله از چه نوعی است و چه اقداماتی برای شناسایی و مقابله با این حمله انجام می‌دهید؟		
	شاخص تحقق: **ارائه یک طرح رمزنگاری برای ذخیره و تبادل اطلاعات**	**بالاتر از حد انتظار**	**نمره : ۳**
۶	خانم دانیالی پیغام رمزشده ای را برای شاگردانش ارسال میکند و ازآنها میخواهد آن را با استفاده از روش رمزگشایی جابجایی حروف و کلید ۲(قبلی) رمزگشایی کنند. YXGX KYL YQFCEFYR FYQRYK		
	شاخص تحقق: **انتخاب رمزنگاری مورد نیاز (یک طرفه یا دو طرفه) در یک کاربرد خاص**	**در حد انتظار**	**نمره : ۲**
۷	نوع رمزنگاری پیامهای زیر را تعیین کنید الف. فرض کنید شما و دوستتان می‌خواهید یک راز را به اشتراک بگذارید، اما نمی‌خواهید کسی دیگر آن را بفهمد. ب. فرض کنید می‌خواهید از صحت یک فایل دانلود شده مطمئن شوید. می‌توانید هش فایل را از وب سایت دانلود دریافت کنید. سپس می‌توانید هش فایل دانلود شده خود را با هش ارائه شده توسط وب سایت مقایسه کنید. اگر دو هش مطابقت داشته باشند می‌توانید مطمئن باشید که فایل دانلود شده شما دستکاری نشده است.		
	شاخص تحقق: **تهیه گزارش نقض امنیت رخ داده**	**در حد انتظار**	**نمره : ۲**

۸	سارا احمدی امروز وارد ایمیلش شد تا ایمیلی برای مدیر شرکت جهت ارسال دعوتنامه کنفرانسی ارسال کند ولی بعد از ارسال نامه متوجه شد که نامه دیگری از طرف او چند روز پیش برای مدیر شرکت ارسال شده در صورتیکه او این نامه را ارسال نکرده و محتوای نامناسبی هم دارد یک گزارش نقض امنیت برای او بنویسید.(شماره همراه سارا احمدی : ۰۹۱۸۵۵۵۵۵۵۵)		
	شاخص تحقق: **ارائه راهکار بهینه پشتیبان گیری برای یک کاربرد خاص**	**در حد انتظار**	**نمره : ۲**
۹	سیما روز جمعه از سیستمش یک بکاپ کامل تهیه کرد و چند روز بعد در روز یکشنبه نرم افزارهای جدیدی نصب کرد و یک بکاپ افزایشی گرفت امروز سه شنبه است و سیما چند نرم افزار جدید نصب کرده پیشنهاد شما به سیما برای تهیه بکاپ امروز چه نوع بکاپی است؟چرا؟ راستی سیما وقت کمی برای بکاپ دارد و می خواهد سریعتر بکاپ را بگیرد و سراغ کارهای دیگرش برود!☺		
	شاخص تحقق: **ارائه راهکار برای افزایش توان پدافند غیر عامل در یک کاربرد خاص در حوزه فاوا**	**بالاتر از حد انتظار**	**نمره : ۳**
۱۰	فرض کنید یک شهر هوشمند با تمام امکانات مدرن و پیشرفته وجود دارد. ناگهان، یک حمله سایبری گسترده به سیستم‌های این شهر رخ می‌دهد و برق، آب، سیستم‌های حمل و نقل و ارتباطات به طور کامل قطع می‌شوند. برای پیشگیری از چنین حملاتی باید از چه نوع پدافندی استفاده شود ؟ چه اقداماتی می‌توان در قالب آن پدافند برای پیشگیری از حملات سایبری انجام داد؟		

سوال	پاسخ
۱	

جلوی درب ورود به اتاق سرور سیستم تشخیص چهره قرار داده شده است.	محرمانگی
برای ورود به سامانه my medu بعد از ثبت شماره تلفن، رمز یکبار مصرف به گوشی ارسال می شود	محرمانگی
از هر جایی در اینترنت می توانم بر دوربینهای مدار بسته شرکتم نظارت داشته باشم	دسترس پذیری
آموزش و پرورش سامانه ای راه اندازی کرده که با ورود به آن به راحتی و بدون مراجعه به اداره می توانم آخرین حکم صادره خود را ببینم.	دسترس پذیری
امروز برای خرید یک مانتو به فروشگاه رفتم متاسفانه بعد از اینکه فروشنده کارت را در دستگاه کشید و پیامک کسر مبلغ از حسابم آمد گفت تراکنش ناموفق بوده و مجدد کارت را کشید و این بار موفقیت آمیز بود قبل از خروج از فروشگاه پیامک دیگری برایم آمد که مبلغ کسر شده اول مجدد به حسابم اضافه شده بود	جامعیت

۲

چه اقداماتی می‌توانستید انجام دهید تا احتمال وقوع این حمله را کاهش دهید؟ این اقدامات مربوط به مرحله پیش از حمله است.

اقدامات مناسب: تامین امنیت سایت به منظوری پیشگیری از حمله

چه نقاط ضعفی در سیستم‌های امنیتی شرکت وجود داشت که منجر به این حمله شد؟ پیدا کردن نقاط ضعف مربوط به مرحله پیش از حمله است.

نقاط ضعفی مانند ورود بدون احراز هویت توسط کاربران،

اولین اقداماتی که باید در زمان وقوع حمله انجام دهید چیست؟ این سوال مربوط به زمان حمله است. در این مرحله باید شیوه حمله شناسایی و حمله متوقف شود.

چگونه می‌توانید نوع حمله و منبع آن را شناسایی کنید؟ این سوال مربوط به زمان حمله است.

۱. جمع‌آوری اطلاعات:

شناسایی اولین نقطه نفوذ: بررسی سیستم‌ها و گزارش‌ها برای یافتن اولین نقطه ورود مهاجم.

نوع داده‌های سرقت شده: شناسایی نوع اطلاعاتی که توسط مهاجم به سرقت رفته است.

ابزارها و روش‌های مورد استفاده:

بررسی logها و ابزارهای امنیتی برای یافتن سرنخ‌هایی از ابزارها و روش‌های مورد استفاده توسط مهاجم.

الگوهای رفتاری: بررسی الگوهای رفتاری غیرمعمول در شبکه و سیستم‌ها.

۲. تجزیه و تحلیل:

تجزیه و تحلیل داده‌های جمع‌آوری‌شده: استفاده از ابزارهای تحلیل و تخصص متخصصان امنیت سایبری برای تفسیر اطلاعات و شناسایی نوع حمله.

بررسی تهدیدات شناخته‌شده: مقایسه اطلاعات جمع‌آوری‌شده با تهدیدات سایبری شناخته‌شده برای یافتن شباهت‌ها.

۳. ردیابی:

ردیابی فعالیت مهاجم: استفاده از ابزارهای ردیابی برای یافتن منبع حمله مانند event viewer.

شناسایی آدرس‌های IP: بررسی logها برای یافتن آدرس‌های IP مرتبط با حمله.

استفاده از ابزارهای تجزیه و تحلیل ترافیک: استفاده از ابزارهای تجزیه و تحلیل ترافیک شبکه برای یافتن الگوهای مشکوک.

۴. همکاری:

همکاری با متخصصان امنیت سایبری: همکاری با متخصصان داخلی و خارجی برای تجزیه و تحلیل و ردیابی حمله.

اطلاع‌رسانی به مراجع قانونی: در صورت لزوم، اطلاع‌رسانی به مراجع قانونی مانند پلیس فتا برای پیگیری و یافتن عاملان حمله.

چه اقداماتی برای متوقف کردن حمله و به حداقل رساندن خسارات باید انجام شود؟ این اقدامات مربوط به پس از حمله است و شامل موارد زیر است:

بروزرسانی سیستم‌ها و نرم‌افزارها: اطمینان از به‌روز بودن سیستم‌ها و نرم‌افزارها برای رفع آسیب‌پذیری‌های امنیتی.

استقرار ابزارهای امنیتی: استقرار ابزارهای امنیتی مناسب برای پیشگیری از حملات مشابه در آینده.

آموزش کارکنان: آموزش کارکنان در مورد آگاهی از امنیت سایبری و نحوه مقابله با حملات.

چگونه می‌توانید وسعت و عمق نفوذ هکرها را به سیستم‌های شرکتتان تعیین کنید؟ این اقدامات مربوط به پس از حمله است.

۱. بررسی گزارش‌ها:

	بررسی گزارش‌های امنیتی: بررسی گزارش‌های امنیتی سیستم‌ها و ابزارهای امنیتی برای یافتن فعالیت‌های مشکوک. بررسی logها: بررسی logهای سیستم‌ها و برنامه‌ها برای یافتن نشانه‌هایی از نفوذ هکرها. بررسی گزارش‌های کاربران: بررسی گزارش‌های کاربران برای یافتن موارد مشکوک مانند فعالیت‌های غیرمعمول در حساب‌های کاربری. ۲. تجزیه و تحلیل داده‌ها: تجزیه و تحلیل داده‌های جمع‌آوری‌شده: استفاده از ابزارهای تحلیل و تخصص متخصصان امنیت سایبری برای تفسیر اطلاعات و یافتن شناسایی نقاط نفوذ: شناسایی نقاطی که هکرها از طریق آنها به سیستم‌ها نفوذ کرده‌اند. شناسایی داده‌های سرقت شده: شناسایی نوع اطلاعاتی که توسط هکرها به سرقت رفته است. شناسایی سیستم‌های آلوده: شناسایی سیستم‌هایی که توسط هکرها آلوده شده‌اند. ۳. استفاده از ابزارهای تخصصی ۴. استفاده از ابزارهای اسکن: استفاده از ابزارهای اسکن برای یافتن آسیب‌پذیری‌های امنیتی در سیستم‌ها. ۵. استفاده از ابزارهای ردیابی: استفاده از ابزارهای ردیابی برای یافتن منبع حمله. ۶. همکاری با متخصصان: همکاری با متخصصان امنیت سایبری: همکاری با متخصصان داخلی و خارجی برای تجزیه و تحلیل و ردیابی حمله. ۷. استفاده از خدمات مشاوره امنیت سایبری: استفاده از خدمات مشاوره امنیت سایبری برای دریافت راهنمایی و کمک در تعیین وسعت و عمق نفوذ هکرها. **چه اقداماتی برای بازیابی اطلاعات و سیستم‌های آسیب‌دیده باید انجام شود؟** این اقدامات مربوط به پس از حمله است **چه اقداماتی برای جلوگیری از تکرار چنین حملاتی در آینده باید انجام شود؟** این اقدامات مربوط به پس از حمله است
۳	**Accounting** (حسابرسی) / **Authorization** (اعتبارسنجی) / **Authentication** (احراز هویت) مدت اعتبار آن فقط ۶ روز است / این تخفیف فقط شامل ۶۰ درصد قیمت کتاب خریداری شده می شود / ورود به نرم افزار طاقچه با نام کاربری ثبت کد تخفیف
۴	اولا ارسال اطلاعات محرمانه از طریق ایمیل و بویژه ایمیل خارجی اصلا درست نیست. ثانیا اگر بخواهیم اطلاعات مهمی را از طریق ایمیل ارسال کنیم ابتدا باید از فرستنده آن اطمینان حاصل کنیم که برای این منظور می توان از اطلاعات رمزنگاری شده با کلید خاصی یا امضای دیجیتال استفاده کرد. ثالثا نباید فریفته اطلاعات گول زننده ایمیل از قبیل بیان علاقمندیهای ما شویم شاید اینها یک حمله مهندسی اجتماعی باشد.
۵	حمله DOS ، **شناسایی:** نظارت بر ترافیک شبکه: افزایش ناگهانی ترافیک شبکه می‌تواند نشان‌دهنده حمله DOS باشد. بررسی log ها : بررسی logها برای یافتن فعالیت‌های مشکوک مانند درخواست‌های غیرمعمول به وب‌سایت. استفاده از ابزارهای امنیتی: استفاده از ابزارهای امنیتی مانند سیستم‌های تشخیص نفوذ (IDS) و سیستم‌های پیشگیری از نفوذ (IPS) برای شناسایی فعالیت‌های مشکوک. **مقابله:** محدود کردن ترافیک: محدود کردن ترافیک ورودی به وب‌سایت برای جلوگیری از از کار افتادن آن. مسدود کردن آدرس‌های IP مخرب: مسدود کردن آدرس‌های IP که از آنها ترافیک مخرب ارسال می‌شود. استفاده از ابزارهای تخصصی برای مقابله با حملات DOS.
۶	متن رمزگشایی شده خانم دانیالی برای شاگردانش: Aziz Man Asheghat Hastam (عزیز من عاشقت هستم)
۷	الف. رمزنگاری دوطرفه ب. رمزنگاری یکطرفه
۸	گزارش نقض امنیت سایبری مشخصات گزارش دهنده: نام: سارا نام خانوادگی: احمدی شماره تماس: ۰۹۱۸۵۵۵۵۵۵۵ تاریخ گزارش: ۱۴۰۲/۰۳/۱۴ فوریت: فوری

	شرح خلاصه اتفاق: امروز صبح، ۱۴/۰۳/۱۴۰۲، زمانی که وارد حساب ایمیل خود شدم، متوجه شدم که ایمیلی از طرف من به آدرس مدیر شرکت ارسال شده است. من این ایمیل را ارسال نکرده‌ام و محتوای آن نامناسب است. **سطح خسارت:** در حال حاضر، سطح دقیق خسارت مشخص نیست. با این حال، احتمال می‌رود که این ایمیل برای مقاصد مخرب مانند کلاهبرداری یا فیشینگ استفاده شده باشد. **راهکار و پیشنهاد:** تغییر رمز عبور حساب ایمیل اسکن کامپیوتر و دستگاه‌های متصل به حساب ایمیل برای یافتن بدافزار گزارش ایمیل مشکوک به مراجع ذیصلاح هشدار به مخاطبین ایمیل در مورد ایمیل جعلی **مدارک پیوست:** اسکرین شات از ایمیل جعلی گزارش اسکن کامپیوتر
۹	بکاپ افزایشی چون بسیار سریع انجام می شود و حجم کمی دارد و در سوال، زمان بکاپ مورد توجه بود نه زمان برگردان آن.
۱۰	پدافند غیرعامل اقداماتی که من به عنوان مسئول پدافند غیرعامل این شهر انجام می دادم عبارت است از : **۱. آموزش و آگاهی‌رسانی:** آموزش کارکنان در مورد اصول امنیت سایبری و نحوه شناسایی و مقابله با حملات سایبری افزایش آگاهی عمومی در مورد تهدیدات سایبری و نحوه محافظت از اطلاعات شخصی **۲. استقرار سیستم‌های امنیتی:** استفاده از فایروال، آنتی‌ویروس و سایر نرم‌افزارهای امنیتی رمزنگاری داده‌های حساس به‌روزرسانی منظم نرم‌افزارها و سیستم‌عامل‌ها **۳. ایجاد و حفظ نسخه‌های پشتیبان:** تهیه نسخه‌های پشتیبان منظم از داده‌های مهم ذخیره‌سازی نسخه‌های پشتیبان در مکانی امن **۴. مدیریت ریسک:** شناسایی و ارزیابی آسیب‌پذیری‌های سیستم‌ها تدوین و اجرای برنامه‌های مدیریت ریسک **۵. ایجاد فرهنگ امنیت سایبری:** ایجاد تعهد و مسئولیت‌پذیری در قبال امنیت سایبری در بین همه افراد سازمان **۶. محدود کردن دسترسی به اطلاعات:** فقط به افرادی که نیاز به دسترسی دارند، مجوز دسترسی به اطلاعات حساس را بدهید. **۷. استفاده از احراز هویت قوی:** از رمزهای عبور قوی و احراز هویت چند عاملی برای محافظت از حساب‌های کاربری استفاده کنید. **۸. نظارت بر شبکه:** فعالیت شبکه را برای شناسایی فعالیت‌های مشکوک نظارت کنید. **۹. ایجاد یک برنامه پاسخگویی به حوادث:** یک برنامه برای پاسخگویی به حملات سایبری تدوین و اجرا کنید.