پودمان دوم

تحلیل امنیت در فاوا

داده‌ها و منابع اطلاعاتی سرمایه‌های باارزشی هستند که در حال حاضر مدیریت آنها امری اجتناب‌ناپذیر است. سیستم‌های اطلاعاتی در حال یکپارچه شدن هستند و تمرکز اطلاعات به همان اندازه که می‌تواند عملیات جست‌وجو و بازیابی را آسان کند، می‌تواند داده‌ها را در معرض خطر و انواع تهدیدات قرار دهد. زیرا یک تهدید در یک نقطه از سیستم می‌تواند کلیه اطلاعات را در معرض خطر قرار دهد. همین امر سبب می‌شود تا حفظ امنیت و نگهداری صحیح داده‌ها تبدیل به یک مسئله چالش‌برانگیز در این حوزه شود. در این پودمان سعی شده است تا ذهن هنرجویان با مسائل مربوط به امنیت، تهدید، حمله، انواع روش‌های رمزنگاری، روش‌های جلوگیری از خطرات و آسیب‌ها و در نهایت بازیابی اطلاعات پس از حمله آشنا شود. درک مطالب تئوری این پودمان در کنار ابزارهایی که در پودمان چهارم کتاب تجارت الکترونیک و امنیت شبکه مطرح شده است می‌تواند روش‌های عملی و اجرایی برای تست آسیب‌پذیری و نفوذ به سامانه‌های اطلاعاتی را فراهم آورد. هنرجو باید بداند که بحث امنیت را در کنار تمام آموزه‌های خود از قبیل شبکه، برنامه‌نویسی، طراحی تارنما قرار دهد تا میزان آسیب‌پذیری را به حداقل برساند.

شایستگی‌های این پودمان عبارت‌اند از:

- تحلیل امنیت در فناوری
- تحلیل حمله و امن‌سازی

شایستگی تحلیل امنیت در فاوا

مقدمات تدریس

الف) مفاهیم کلیدی

مفاهیم کلیدی			
امنیت	تهدید	حمله	دارایی
جامعیت	ریسک	محرمانگی	رمزنگاری Encryption
دسترس‌پذیری	احراز هویت Authentication	اعتبارسنجی Authorization	حسابداری Accounting
حمله اختلال سرویس (DOS)	شنود (Sniff)	پیام ساده PlainText	رمزگشایی Decryption
متن رمز شده CipherText	رمزنگاری متقارن Symmetric	رمزنگاری نامتقارن Asymmetric	گواهی دیجیتال
Logکردن	IDS	IPS	دیوار آتش
مخاطرات	مدیریت یکپارچه تهدیدها	Open source	نسخه پشتیبان Backup

جلسه	موضوع	شماره صفحات	اهداف توانمندسازی	فعالیت‌های تکمیلی
۸	امنیت و اهداف آن و مراحل کار برای حفظ آن	۲۷-۲۵	آشنایی با تعاریف اولیه امنیت، تهدید، حمله و جنبه‌های اصلی امنیت- اهداف مهم امنیت و مراحل کاری حفظ امنیت	ارائه مثال‌های خارج از کتاب برای اینکه هنرجو به اهمیت موضوع امنیت پی ببرد.
۹	انواع حملات و ریشه آنها	۳۳-۲۷	شناخت انواع حملات شامل مهندسی اجتماعی، اختلال سرویس، شنود و ریشه و پایه تهدیدها	معرفی چندین حمله که اخیراً در فضای سایبری اتفاق افتاده است، تعیین دلیل رخ دادن حمله و راه‌های مقابله با آنها
۱۰	رمزنگاری	۳۵-۳۳	آشنایی با رمزنگاری و انواع آن	معرفی یک یا چند سیستم رمزنگاری و آشنا کردن هنرجو با روش کار هر سیستم
۱۱	ادامه رمزنگاری	۳۷-۳۵	شناخت رمزنگاری متقارن و نامتقارن - گواهی دیجیتال	بحث در مورد اهمیت گواهی دیجیتال در تجارت الکترونیک و اشاره به امضای دیجیتال
۱۲	اهمیت ثبت رخدادها و سیستم‌های تشخیص حمله	۴۰-۳۷	آشنایی هنرجو با انواع سیستم‌های تشخیص حمله و نحوه کار هر یک و اهمیت پشتیبان‌گیری از اطلاعات	بحث و گفتگو در مورد روش‌های شناسایی حملات - معرفی مزایا و معایب انواع روش‌های پشتیبان‌گیری اطلاعات
۱۳	مدیریت خطرپذیری	۴۴-۴۱	آشنایی هنرجو با مدیریت خطر و نقش آن در حفظ امنیت سازمان و نرم‌افزار	رسم جدول مدیریت ریسک هنرستان محل تحصیل خود به عنوان تمرین منزل
۱۴	مدیریت یکپارچه تهدیدها و پدافند غیرعامل	۴۸-۴۴	آشنایی با تعریف مستندسازی، معرفی مدیریت یکپارچه تهدیدها و پدافند غیرعامل	معرفی چند نمونه از پدافند غیرعامل

طرح درس روزانه (هفتگی) پیشنهادی				
پایه: دوازدهم		درس: دانش فنی تخصصی		
پیام جلسه (هدف کلی): آشنایی با مفهوم امنیت و جنبه‌های اصلی آن				
		فعالیت‌ها		زمان
فعالیت	اهداف یادگیری	کار هنرآموز	کار هنرجو	مدت (دقیقه)
ارزشیابی رفتار ورودی	سنجش میزان آگاهی هنرجویان از مفهوم امنیت و کاربرد آن	معطوف کردن توجه هنرجویان به مفهوم امنیت با طرح سؤال، مانند مطرح کردن داستان یک سرقت و بررسی علت وقوع آن و راهکار جلوگیری از آن	مشارکت در پاسخگویی و تعامل و بیان مصادیق مشابه و بررسی آنها	۲۰
ایجاد انگیزه	نتایج مثبت به‌کارگیری امنیت در فناوری در جهت حفظ حریم خصوصی و حفاظت از داده‌ها	با ذکر چند مثال ساده اهمیت امنیت را بیان کند مانند امنیت در کارت‌های اعتباری	پاسخ‌گویی هنرجو در جهت اجرای امنیت در کارت‌های پرداخت الکترونیکی و همچنین ارائه مثال به‌وسیله هنرجو	۲۰
ارائه مفاهیم کلیدی (توضیح هنرآموز)	توضیح و تعریف مفاهیم امنیت، تهدید، حمله، تفاوت‌های تهدید با حمله و جنبه‌های اصلی امنیت (محرمانگی، جامعیت و دسترس‌پذیری) ذکر مثال برای هر کدام از جنبه‌های اصلی امنیت ضروری است.	هنرآموز باید با یادداشت کردن تیتر مطالب روی تابلو و یا استفاده از اسلاید، مطالب را برای هنرجویان توضیح دهد. در نهایت هنگام روخوانی کتاب به‌وسیله هنرجویان توضیحات لازم بیان شود.	هنرجو باید در این مرحله به صحبت‌های هنرآموز گوش دهد و در صورت نیاز در بحث شرکت کند. در انتهای تدریس یکی از هنرجویان مطالب درس را در کتاب روخوانی کند.	۵۵
تمرین هنرجویان	تفکر در مورد مسائل امنیتی در انتخاب گذرواژه	هنرآموز با طرح این سؤال، هنرجویان را متوجه اهمیت امنیت در انتخاب گذرواژه می‌کند.	هنرجو باید تمام راهکارهای امنیتی خود را در این زمینه بیان کند.	۱۵
ارائه تمرین	پاسخ‌گویی به فعالیت‌های کتاب	هنرآموز، هنرجویان را به فعالیت‌های موجود در کتاب ارجاع دهد.	هنرجو باید با مشورت هم‌کلاسی‌های خود نتیجه را در کتاب یادداشت کند.	۲۰
جمع‌بندی	هنرجو باید با امنیت، کاربرد آن، مفاهیم حمله و همچنین هر کدام از جنبه‌های امنیت آشنا شده باشد.	هنرآموز می‌تواند این قسمت را با مطرح کردن سؤالاتی از هنرجویان انجام دهد.	هنرجو باید با مراجعه به کتاب یا مشورت با هم‌کلاسی‌های خود جواب پرسش‌ها را پیدا کند.	۲۰
ارزشیابی پایانی	هنرجو باید فواید به‌کارگیری امنیت در حوزه فناوری را توضیح دهد.	این ارزشیابی می‌تواند به دو صورت کتبی و شفاهی انجام شود.	هنرجو با مراجعه به کتاب و دانسته‌های خود جواب سؤالات هنرآموز را مشخص کند.	۳۰
تعیین تکلیف	یکی از حملات سایبری اخیر را شناسایی و در مورد آن توضیحاتی ذکر کند.	هنرآموز باید هنرجویان را به سمت جست‌وجو در اینترنت و کشف حملات سایبری اخیر هدایت کند.	با مراجعه به اینترنت و جست‌وجو در آن جواب تمرین موردنظر و همچنین توضیحات مربوط به آن را به دست آورد.	۱۰

ج) ورود به بحث

قبل از شروع بحث لازم است ذهن هنرجو را به سمت مفاهیم امنیت و لزوم برقراری آن معطوف کنیم. برخی موارد پیشنهادی:

من روز گذشته، در هنگام خرید، گذرواژه کارت خود را در مرکز خرید برای فروشنده با صدای بلند تکرار کرده‌ام. چه مشکلاتی ممکن است برای من پیش آید؟ در مورد پیامدهای این اتفاق و دلایل به وجود آمدن آن بحث کنید.

از آنها بخواهید بیان کنند برای حفاظت از گذرواژه wifi خود چه اقداماتی انجام می‌دهند؟ چرا؟

در مورد فعالیت‌های پلیس فتا در کلاس بحث کنید.

برای تفهیم بهتر مطالب می‌توانید مواردی از امنیت نظامی، غذایی، بهداشتی را نام ببرید. تا جایی که به بحث امنیت در فناوری بپردازیم. سپس از هنرجویان بخواهید تا برداشت خود از امنیت در شبکه را بیان کنند. در حین توضیحات هنرجویان به برخی از خطرات فضای مجازی مثل هک کردن تارنماهای معروف، برداشت از حساب‌های بانکی، سرقت عکس‌ها و اطلاعات خصوصی کاربران اشاره‌کنید. در حین کار سعی کنید ذهن هنرجویان را به سمت تعریف زیر سوق دهید:

امنیت یعنی دور بودن از هرگونه خطر، شک، عصبانیت یا ترس، داشتن اعتمادبه‌نفس و به‌طور کلی هر چیزی که به ما ایمنی و اعتماد دهد.

در پایان مطالعه این پودمان باید برای هنرجو این نگرش به وجود آید که روش‌های برقراری امنیت نیاز به یادگیری و آموزش دارد. هنرجو در این مرحله باید تفاوت بین شخصی را که با مطالعه منابع معتبر مباحث امنیت را فراگرفته و شخصی که با آزمون و خطا و صرفاً با یادگیری چندین نرم‌افزار مربوط به نفوذ به‌عنوان یک هکر شناخته می‌شود، متوجه شود.

تدریس

امنیت

امنیت اطلاعات	مجموعه تمهیدات لازم جهت جلوگیری از دسترسی غیرمجاز به اطلاعات، نشت اطلاعات محرمانه، از دسترس خارج شدن خدمات یک سرویس‌دهنده، تغییر مخفیانه در داده‌ها، سرقت داده‌ها و اطلاعات، از بین رفتن داده‌ها، جعل داده‌ها و اختلال در عملکرد صحیح در سیستم است.
دارایی	هر آنچه که در سیستم است و ارزش حفاظت دارد، اعم از داده‌ها، کارمندان، فرم‌ها، سیستم‌ها و منابع فیزیکی و...
تهدید	عوامل بالقوه برای وقوع رخدادهای خطرناک و احتمال سوءاستفاده از یک یا چند آسیب‌پذیری در سیستم
حمله	هر فعالیتی که امنیت اطلاعات را به خطر می‌اندازد.

مجموعه تمهیدات لازم برای برقراری امنیت اطلاعات عبارت‌اند از:

۱ جلوگیری از وقوع رخدادهای ناخوشایند

۲ کاهش احتمال وقوع رخدادهای خطرناک

۳ توزیع نقاط حساس و استراتژیک

۴ بازگشت به حالت اولیه با کمترین هزینه

تعریف تهدید با حمله متفاوت است. تهدید رخنه‌ای است که می‌تواند راه نفوذ حمله را باز کند. برای امن‌سازی یک سامانه باید تمام تهدیدها را بررسی کنیم.

جنبه‌های اصلی امنیت اطلاعات معروف به مثلث CIA

سه اصل مهم در امنیت اطلاعات عبارت‌اند از:

۱ـ محرمانگی Confidentiality: به این معنی که فقط افراد خاصی به اطلاعات دسترسی داشته باشند. همچنین افراد غیرمجاز به داده‌های مجاز کاربران دسترسی نداشته باشند. تحقق محرمانگی داده‌ها با رمزنگاری میسر می‌شود.

رمز عابر بانک یک مسئله محرمانه است و نباید در اختیار دیگران قرار گیرد. می‌توان در این قسمت عواقب این کار را تشریح کرد.

شما یک پست حساس در یک اداره دارید، گذرواژه پست الکترونیک اداره را روی برگه‌ای یادداشت کرده و در کیف خود گذاشته‌اید. چه مشکلاتی می‌تواند پیش آید؟

چندین مورد امنیتی در انتخاب گذرواژه را نام ببرید. با این سؤال می‌توان به هنرجویان راهکارهای انتخاب گذرواژه امن را آموزش داد که برخی از آنها عبارت است از:

طول گذرواژه کمتر از ۸ حرف نباشد.

گذرواژه سخت باشد. ترکیبی از اعداد و حروف و علائم خاص باشد.

از واژه‌های فرهنگ لغت برای گذرواژه استفاده نکنیم.

نام کاربری بخشی از گذرواژه نباشد. مثال:

username: ali

password: ali123456

۲ـ جامعیت Integrity: تضمین صحت اطلاعات یا جامعیت در واقع بیان می‌کند آنچه گیرنده دریافت می‌کند همان چیزی است که فرستنده ارسال کرده است. به‌بیانی دیگر به مجموعه سازوکارهای لازم جهت جلوگیری از تحریف، تکرار، حذف و آلوده نمودن اطلاعات جامعیت داده‌ها می‌گویند.

برای تفهیم این قسمت می‌توان از مثال دیگری استفاده کرد. هنگامی که یک خبر را در شبکه‌های اجتماعی دریافت می‌کنیم چگونه می‌توان مطمئن بود که منبع خبر موثق است؟

۳ـ دسترس‌پذیری Availability: منابعی که یک کاربر مجاز است به آنها دسترسی داشته باشد در هنگام نیاز باید در اختیار او قرار بگیرد. برای تفهیم این مورد می‌توان از مثال زیر استفاده کرد:

یک شرکت خودروساز اقدام به پیش‌فروش محصولات خود در بازه زمانی مشخصی کرده است. در این بازه تعداد زیادی از افراد اقدام به بازدید از تارنما مربوطه می‌کنند به‌طوری‌که سرور تارنما توان پاسخگویی به همه درخواست‌ها را ندارد. در نتیجه برای برخی از کاربران، تارنما باز نمی‌شود. در این مورد ویژگی دسترس‌پذیری تارنما خدشه‌دار شده است.

پاسخ به فعالیت‌ها

کنجکاوی ص۲۶

از میان سرقت رایانه قابل‌حمل و مشاهده پرونده‌ها با نفوذ به رایانه قابل‌حمل کدام مورد حمله فعال و کدام مورد حمله غیرفعال به شمار می‌آید؟

پاسخ: سرقت رایانه، حمله فعال و مشاهده پرونده‌ها حمله غیرفعال محسوب می‌شوند.

کنجکاوی ص۲۷

فرض کنید پیام تراکنش ناموفق با کاهش مبلغ از حساب برای شما رخ داده است، بانک مربوطه برای حفظ جامعیت اطلاعاتی بانک چه روشی را پیش‌بینی کرده است؟ آیا این پیش‌بینی بانک باعث افزایش امنیت شما شده است؟

پاسخ: معمولاً هنگام خریدهای اینترنتی پول باید از حساب مبدأ کسر و به حساب مقصد اضافه شود. در برخی موارد هنگام خرید مبلغ از حساب مبدأ کسر شده و به حساب مقصد واریز نمی‌شود. در این‌گونه مواقع بانک ۷۲ ساعت پس از تراکنش ناموفق با بررسی این موضوع که چنین مبلغی با شماره تراکنش مربوطه به حساب مقصد واریز نشده است پول را به حساب شخص بازمی‌گرداند.

فعالیت‌های پیش از حمله

جلوگیری مطلق از حملات دشوار است. چون این کار مستلزم حفاظت فیزیکی از تمام امکانات ارتباطی و مسیرهای شبکه در تمام زمان‌ها است. در حملات فعال هدف تشخیص و ترمیم خرابی یا تأخیرهای ناشی از آن است. بهترین روش در حفظ امنیت، جلوگیری از بروز حمله و از بین بردن تهدیدهای موجود است.

برای ورود به بحث فعالیت‌های پیش از حمله شامل احراز هویت، اعتبارسنجی و حسابداری می‌توان از هنرجویان سؤالاتی از این قبیل پرسید:

۱ برای جلوگیری از حمله به سیستم‌های نرم‌افزاری و رایانه‌ای چه راهکارهایی را پیشنهاد می‌کنید؟

۲ برای اینکه تارنمای یک بانک دچار حمله نشود، چه راهکارهایی وجود دارد؟

عمده فعالیت‌های انجام‌شده برای کاهش اثر حمله عبارت است از:

۱	**پیش از حمله**	تمرکز اصلی بخش امنیت هر سازمانی باید به این مرحله باشد. جلوگیری و کاهش وقوع رخدادهای ناخوشایند در واقع ساده‌ترین و مهم‌ترین بخش است.
۲	**زمان حمله**	در این مرحله با استفاده از تکنیک‌های مشخص باید حمله مربوطه را تشخیص و جلوی آن را گرفت.
۳	**پس از حمله**	بازگشت به حالت اولیه مهم‌ترین بحث پس از حمله است. در صورتی می‌توان این مرحله را به‌درستی انجام داد که در زمان قبل از حمله تمهیدات لازم مثل تهیه نسخه پشتیبان صورت گرفته باشد. با پیش‌بینی‌های صحیح و به‌موقع می‌توان اثرات حمله را به حداقل رساند.

فعالیت‌های پیش از حمله شامل احراز هویت، اعتبارسنجی و حسابداری است.

احراز هویت (تصدیق اصالت) Authentication	اطمینان از اینکه کاربر همانی است که ادعا می‌کند.
اعتبارسنجی (مجازشناسی) Authorization	کاربر به همان میزان حق دسترسی دارد که به او اعطا شده است.
حسابداری Accounting	میزان استفاده کاربر را در طول دسترسی را مشخص می‌کند. Accounting مشخص می‌کند که کاربر مجوز استفاده از چه مدت و به چه مقدار اطلاعات در طول برقراری یک ارتباط را دارد.

مهندسی اجتماعی: در روش مهندسی اجتماعی ابتدا مهاجم با روش‌های گوناگون فرد را ملزم به فاش کردن برخی از اطلاعات خود در جهت جمع‌آوری اطلاعات فرد کرده و در نهایت با استفاده از اطلاعات به‌دست آمده در راستای دستیابی به خواسته‌های خود اقدام می‌کند.

روش مهندسی اجتماعی هنگامی می‌تواند برای یک هکر مفید باشد که کاربر از اطلاعات آماری خود مانند سال تولد، نام پدر، نام فرزند و... در انتخاب گذرواژه خود استفاده کرده باشد. مهاجم با پی بردن به اطلاعات پرسنلی شخص در واقع فهرستی از گذرواژه‌ها را برای شروع عملیات نفوذ در اختیار دارد که این مورد زمان عملی شدن حمله را کوتاه‌تر می‌کند. متأسفانه بسیاری از افراد برای اینکه گذرواژه‌های خود را فراموش نکنند اقدام به انتخاب گذرواژه‌های ساده کرده که در نتیجه به‌راحتی در دام می‌افتند.

انواع حملات: در دنیای فناوری اطلاعات و ارتباطات دو نوع حمله وجود دارد:

حملات غیرفعال Passive	حمله‌کننده از اطلاعات شبکه استفاده می‌کند اما تأثیری بر منابع شبکه ندارد. یعنی اطلاعاتی تولید نمی‌کند و بر ترافیک شبکه نمی‌افزاید.	هدف این نوع حمله به دست آوردن اطلاعات از داده‌های در حال انتقال در شبکه است.
حملات فعال Active	حمله‌کننده سعی می‌کند منابع شبکه را تغییر دهد یا بر عملکرد آن تأثیر بگذارد. یعنی خودش اطلاعاتی تولید کرده و در شبکه منتشر می‌کند. همچنین ترافیکی را تغییر یا حذف می‌کند.	هدف این نوع حمله نفوذ به شبکه، تغییر داده‌ها و خدشه‌دار کردن مسائل امنیتی است.

تشخیص حملات غیرفعال دشوار است. زیرا در این نوع حمله تغییری در داده‌ها ایجاد نمی‌شود و گیرنده خبر ندارد که شخص ثالثی پیام را می‌خواند و یا الگوی ترافیک شبکه را مشاهده می‌کند. رمزنگاری داده‌ها برای جلوگیری از این نوع حملات مناسب است.

برخی از حملات عبارت‌اند از:

حمله اختلال در سرویس DOS	ممانعت ازسرویس، از استفاده عادی یا مدیریت امکانات جلوگیری می‌کند. به‌عنوان مثال مهاجم ممکن است پیام‌های ارسال‌شده به مقصد خاصی را توقیف کند. شکل دیگر این حمله تخریب کل شبکه از طریق غیرفعال کردن شبکه با تحمیل بار اضافی با آن است تا کارایی شبکه کاهش یابد.
شنود Sniff	به برداشت غیرمجاز اطلاعات در یک ارتباط، بدون اطلاع فرستنده و گیرنده شنود گفته می‌شود.

پاسخ به فعالیت‌ها

فعالیت منزل
ص۲۸

برای کنترل دسترسی و احراز هویت روش‌های مختلفی وجود دارد. ساده‌ترین روش نام کاربری و گذر واژه است. در فهرست زیر تعدادی از این روش‌ها معرفی‌شده‌اند. در مورد میزان امنیت هر کدام از این روش‌ها، مکان‌ها و وسایلی که از این روش‌ها استفاده می‌کنند جست‌وجو کنید و نتیجه را در کلاس ارائه دهید.

نام روش	توضیح
اثر انگشت	به برجستگی‌های بسیار ریز و قابل رویت در دست‌ها اثر انگشت می‌گویند که به علت ترشحات چربی زیر پوست، این اثر بر روی اجسام صاف قرار می‌گیرد و از آنجایی که اثر انگشت هر فرد منحصربه‌فرد است، از این ویژگی می‌توان به‌عنوان امضا و سیستم تشخیص هویت استفاده کرد. از مزایای این روش می‌توان به سهولت استفاده، در دسترس بودن و عدم نیاز به خاطر سپاری گذرواژه اشاره کرد.
اسکن عنبیه چشم	در این روش از رگ‌های خونی شبکیه چشم برای شناسایی افراد استفاده می‌شود. رگ‌های خونی شبکیه چشم به‌قدری زیاد و پیچیده هستند که مانند اثر انگشت هیچ دو فردی در این ویژگی یکسان نیستند. درحال‌حاضر از این فناوری در فرودگاه‌ها و دیگر مراکز سری و حساس برای شناسایی افراد و کارکنان استفاده می‌شود.
دستگاه گذر واژه‌ساز یا توکن	توکن یک قطعه سخت‌افزاری کوچک است که می‌تواند برای احراز هویت کاربرانی که خواهان ورود به یک سیستم هستند مورد استفاده قرار گیرد. در واقع توکن به عنوان یک کلید الکترونیکی برای ورود به سیستم عمل می‌کند.
کارت هوشمند	کارت‌های هوشمند یک تراشه حاوی اطلاعات موردنظر نصب شده است. این اطلاعات می‌تواند به‌وسیله دستگاه کارت‌خوان از طریق دسترسی به حافظه آن خوانده شود. این کارت‌ها به کارت‌های تراشه دار یا مدار مجتمع نیز معروف هستند و می‌توانند به‌عنوان جایگزین کارت پول، یا کارت‌های امنیتی برای ورود به سیستم و تشخیص هویت استفاده شود.
اسکن چهره	در سیستم‌های تشخیص چهره، دوربین‌های حساس حالت‌های مختلف صورت افراد را شناسایی می‌کنند. به این صورت که تصاویر باکیفیتی را از چهره یک شخص شامل نشانه‌های خاص در چهره، فاصله چشم‌ها، عرض بینی، شکل گونه‌ها می‌گیرند. سپس سیستم تشخیص هویت این اطلاعات را با اطلاعات موجود در پایگاه داده خود مقایسه و نزدیک‌ترین چهره به این ویژگی‌ها را شناسایی می‌کند. هر چه اطلاعات موجود در پایگاه داده بیشتر باشد دقت تشخیص بیشتر می‌شود.
RFID فناوری رادیو شناسه (Radio Frequency Identification)	سامانه‌ای جهت شناسایی خودکار افراد، اشیا و حیوانات است. به‌این‌صورت که یک تگ الکترونیکی یا دستگاه فرستنده خودکار به شی موردنظر وصل می‌شود. هر شی یک تگ منحصربه‌فرد یا یک کد شناسایی خاص را دارا است. سپس یک دستگاه کد خوان RFID با تولید میدان مغناطیسی در محدوده خود قادر به شناسایی تگ‌های فعال است.

کنجکاوی
ص۳۱

بیشتر دانشگاه‌ها انتخاب درس در هر نیم‌سال تحصیلی را به‌صورت اینترنتی انجام می‌دهند. معمولاً دانشگاه‌ها افراد را براساس حروف الفبا و یا سال ورود به دانشگاه، در روزهای متفاوتی ملزم به انجام انتخاب واحد می‌کنند. دلیل این زمان‌بندی چیست؟
پاسخ: سرور دانشگاه در هر لحظه امکان پردازش و پذیرش تعداد محدودی از درخواست‌ها را دارد. در صورتی که همه دانشجویان به‌یک‌باره اقدام به انتخاب واحد کنند، قاعدتاً تارنمای مربوطه از فعالیت بازمی‌ماند. در نتیجه برای کنترل دسترس‌پذیری تارنما، برنامه زمان‌بندی برای کاهش بار ترافیک تارنما اجرا می‌شود.

اهمیت رمزنگاری

در رمزنگاری در سمت فرستنده قبل از ارسال پیام، متن پیام با استفاده از کلید رمز و الگوریتم رمزنگاری به صورت رمزشده درمی‌آید. سپس در سمت گیرنده، با استفاده از الگوریتم رمزگشایی و کلید رمز، متن از حالت رمزشده خارج می‌شود. قابل‌ذکر است مزیت رمزنگاری این است که در صورت ارسال متن پیام از کانال غیر ایمن، امکان رمزگشایی آن وجود ندارد.
دانش رمزنگاری بر پایه مقدمات بسیاری از قبیل ریاضیات، نظریه اعداد، آمار و تئوری اطلاعات بنا شده است. در این قسمت فقط جهت آشنایی با اصول کلی آن مطالبی ذکر شده است.

اصطلاحات رمزنگاری

متن واضح: PlainText
متن رمزشده: CipherText
رمزنگاری: Encryption
رمزگشایی: Decryption

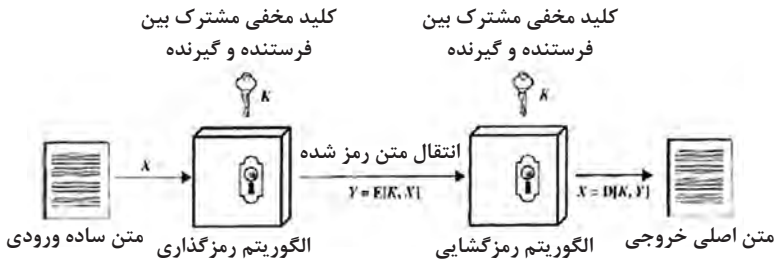
به زبان ساده، در رمزنگاری دو فرد مفروض به‌عنوان مثال شخص الف و ب، قصد ارتباط و تعامل باهم را دارند، اطلاعاتی که شخص الف می‌خواهد برای شخص ب ارسال کند و می‌تواند یک متن انگلیسی، فارسی، یک رشته اعداد یا یک بسته اطلاعاتی باشد، Plain Text نام دارد. شخص الف با رمز کردن Plain Text به وسیله یک کلید از قبل مشخص، متن رمزشده یا Cipher Text را تولید می‌کند و سپس Cipher Text برای گیرنده ارسال می‌شود.

سیستم‌های رمزنگاری به‌طور عمومی از سه بعد دسته‌بندی می‌شوند:

۱	نوع عملیات به‌کار رفته برای تبدیل متن اصلی به متن رمز شده	این دسته شامل الگوریتم‌های رمزنگاری جایگزینی و جابه‌جایی است.
۲	تعداد کلیدهایی که استفاده می‌شود.	در این دسته اگر گیرنده و فرستنده از کلید مشابه استفاده کنند سیستم رمز متقارن و در صورتی‌که فرستنده و گیرنده هر کدام از کلیدهای متفاوتی استفاده کنند سیستم رمز نامتقارن است.
۳	روشی که به وسیله آن متن پردازش می‌شود.	مانند سیستم رمز بلوکی که در هر زمان تنها یک بلوک از ورودی پردازش‌شده و به ازای هر بلوک ورودی یک بلوک خروجی تولید می‌شود و دیگری سیستم رمز جریانی است که به طور مداوم اجزای ورودی پردازش‌شده و در هر زمان یک خروجی تولیدشده و به همین ترتیب ادامه پیدا می‌کند.

رمزنگاری متقارن (کلید خصوصی): در این نوع رمزنگاری هر دو طرف ارتباط که قصد تبادل اطلاعات را دارند، از یک کلید مشترک و محرمانه برای رمزنگاری و رمزگشایی استفاده می‌کنند.

در این نوع رمزنگاری فرایند رمزنگاری و رمزگشایی اطلاعات دو فرایند معکوس یکدیگر است. به همین دلیل به این سیستم‌های رمز، سیستم‌های رمز متقارن نیز می‌گویند.



روش رمزنگاری جابه‌جایی: در این روش حروف متن تغییر نمی‌کند بلکه ترتیب حروف عوض می‌شود. برای نمونه به رمز ریلی که در زیر آمده است دقت کنید. در این نوع سیستم، ابتدا به تعداد دل خواهی ریل یا خط تشکیل می‌شود. سپس حروف مورد نظر که می‌خواهیم رمز شود به‌ترتیب از ابتدای ریل اول به‌صورت زیگزاگ قرار می‌گیرد. به‌عنوان نمونه اگر متن اصلی ما کلمه Informatin باشد

متن رمزشده آن به شکل زیر به دست می‌آید:

I.....r.....i.....

...n...o...m...t...o....

.....f.....a.....n....

بعد از قرار دادن این حروف در خطوط جداگانه، به‌صورت خطی آنها را می‌خوانیم که متن رمزشده زیر حاصل می‌شود. Irinomtofan

در این سیستم فضای کلید برابر تعداد ریل‌هایی است که می‌توان تعریف کرد.

روش رمزنگاری جایگزینی: در این روش هر حرف از متن بر طبق یک سیستم مشخص با یک حرف دیگر جایگزین می‌شود. عمل رمزگشایی عکس عمل رمزنگاری است.

یکی از متداول‌ترین رمزهای جایگزینی روش سزار است. نام آن از ژولیوس سزار گرفته شده است. او از این روش برای ارتباط با فرماندهان خود استفاده می‌کرد.

در این رمز هر حرف در متن اصلی با حرف دیگری با فاصله ثابت جابه‌جا می‌شود. برای مثال با مقدار انتقال ۳، A با D, D با G و به همین ترتیب جانشین می‌شوند. برای مثال برای رمز کردن کلمه Information به روش سزار با کلید ۲، هر حرف را با دو حرف بعد از خود جایگزین می‌کنیم و عبارت رمزشده kphqtcvkqp به‌دست می‌آید.

سیستم رمز نامتقارن (کلید عمومی): در این روش رمزنگاری به جای استفاده از یک کلید مشترک، از یک جفت کلید به نام کلیدهای عمومی و خصوصی استفاده می‌شود. در این روش از کلید عمومی برای رمزنگاری پیام استفاده می‌شود. به‌همین علت این گونه رمز به سیستم رمز کلید عمومی نیز معروف است.

روش کار به شکل زیر است:

در سمت فرستنده با استفاده از کلید عمومی فرد عمل رمزنگاری انجام می‌شود، سپس اطلاعات رمزشده ارسال می‌شود.گیرنده کلید خصوصی خودش را نزد خود به‌طور محرمانه نگه‌داری می‌کند. گیرنده می‌تواند با استفاده از کلید خصوصی خودش، اطلاعات رمزشده دریافتی را رمزگشایی کند و از محتویات اصلی فرستنده مطلع شود. در سیستم‌های رمز نامتقارن کلیدهای رمزنگاری و رمزگشایی متمایز هستند و رابطه پیچیده ریاضی بین آنها حکم‌فرما است. همچنین فرایند رمزنگاری متمایز از فرایند رمزگشایی است. به همین دلیل به این سیستم‌ها، سیستم‌های رمز نامتقارن می‌گویند.

گواهی دیجیتال: گواهی دیجیتال یک سند الکترونیکی است که به یک شخص یا سازمان یک امضای دیجیتال را نسبت می‌دهد. گواهی دیجیتال با نسبت دادن یک کلید عمومی به شخص یا سازمان از طرف مرجع صدور گواهی تأیید می‌کند که امضاکننده واقعی است.

امضای دیجیتال با استفاده از رمزنگاری نامتقارن جامعیت و محرمانه بودن سند را تضمین می‌کند. مشکل این روش زمانی است که طرفین ارتباط نسبت به هم شناختی ندارند. احراز اصالت امضاکننده با روش امضای دیجیتال قابل حل است.
اگر طرفین رابطه حقوقی، تجار بزرگ بین‌المللی یا شرکت‌های چندملیتی باشند و یا موجودیت‌هایی باشند که از قبل برای یکدیگر شناخته شده‌اند، مشکل تعیین هویت واقعی موجودیت‌ها اساساً فرصت بروز نمی‌یابد. چرا که موجودیت‌ها، حتی از توانایی‌های مالی و فنی و انسانی یکدیگر به‌خوبی آگاه هستند. در این گونه موارد، مبادله داده‌های رمزنگاری‌شده برای اثبات وجود رابطه حقوقی و محتوای آن کفایت می‌کند. و در صورت استفاده از کلید خصوصی فرستنده برای رمزنگاری، اصالت سند، اصالت فرستنده و در صورت نیاز محرمانگی، برای گیرنده قابل احراز است.
در صورتی‌که موجودیت‌های شرکت‌کننده در پروتکل یکدیگر را نشناسند، چالش ذکرشده در مورد احراز اصالت امضاکننده، آشکار شده و به یکی از مهم‌ترین دغدغه‌های تجارت الکترونیکی برای قانون‌گذاران ملی و بین‌المللی و اتاق‌های بازرگانی بدل می‌شود.
به عنوان راهکار باید مرجع ثالثی، اعتبار پیام را از طریق تعیین هویت امضاکننده تضمین کند. این مرجع ثالث اصطلاحاً دفتر خدمات الکترونیکی یا دفاتر خدمات صدور گواهی الکترونیکی یا مرجع گواهی نامیده می‌شود. در عمل می‌توان این دفاتر را با دفاتر اسناد رسمی و مدارک دیجیتالی را با اسناد کاغذی مشابه دانست. به عبارت دیگر همان‌طور که دفاتر اسناد رسمی با حضور امضاکنندگان سند و احراز هویت آنها، طی تشریفات قانونی به نوشته، سندیت و رسمیت قانونی می‌بخشند، در عملکردی مشابه، دفاتر گواهی الکترونیکی هویت امضاکنندگان را تضمین کرده و به این ترتیب به اطلاعات الکترونیکی، سندیت قانونی لازم را می‌بخشند.
گواهی دیجیتالی که به‌وسیله دفاتر خدمات الکترونیکی صادر می‌شود، هویت امضاکننده را به کلید عمومی و زوج کلید خصوصی مرتبط با آن مرتبط می‌کند. امضای دیجیتالی دارای دو بخش اصلی و متفاوت اما از نظر ریاضی مرتبط است، بخش اول شامل یک کلید خصوصی است که در اختیار صاحب امضا است و بخش دوم شامل یک کلید عمومی بوده که در فهرست مرجع گواهی قرار داده می‌شود. این مرجع تضمین می‌کندکه کلید عمومی مستقر در فهرست به‌درستی اعلام و ایجاد شده است و به این ترتیب امکان احراز اصالت با کمک امضای دیجیتالی برای گیرنده میسر می‌شود زیرا هویت دارنده کلید خصوصی که منطبق با کلید عمومی است نزد مرجع گواهی وجود دارد.

مرکز صدور گواهی Certificate Authority (CA): این مراکز با تأیید هویت شخص یا سازمان اقدام به صدورگواهی دیجیتال می‌کنند. بنابراین با درخواست گواهینامه از طرف شخص یا سازمان، دو کلید عمومی و خصوصی از طرف مرکز CA به آنها تحویل داده می‌شود، که به‌وسیله مشخصات شخص یا سازمان و کلید عمومی، مراکز CA گواهینامه‌ای صادر می‌کنند که مشمول امضای صادرکننده گواهی، مشخصات شخص یا سازمان و تاریخ اعتبار آن گواهی است. در این میان، کلید خصوصی به‌وسیله شخص یا سازمان در مکان امنی نگهداری می‌شود. آن مراکز امن و دارای اعتبار وظیفه مطابقت کلیدهای عمومی یک شخص برای تأیید هویت و شناسایی آن شخص را دارند و مشخص می‌کنند که این کلید خاص متعلق به شخص خاصی است.

مزایای دریافت گواهی دیجیتال:

۱ افزایش اعتبار سازمان
۲ تضمین پاسخگویی
۳ تسریع بهبود فرایندها
۴ تضمین تعهد مدیریت
۵ تمایل یافتن مشتریان به خرید
۶ ایجاد انگیزه برای کارکنان

پاسخ به فعالیت‌ها

فعالیت منزل
ص۳۳

در مورد شیوه کار و خسارت انواع تهدیدهای بدافزاری زیر در اینترنت جست‌وجو کنید و نتایج را در قالب گزارش به هنرآموز خود تحویل دهید.

بدافزار	شیوه کار
Virus	ویروس یک برنامه کامپیوتری از نوع بدافزار است که بدون اطلاع کاربر از روش‌های مختلفی مانند اتصال به اینترنت، لوح‌های فشرده آلوده و یا حافظه‌های سیار، بدون اطلاع کاربر وارد رایانه شده و شروع به تکثیر خود می‌کند. ویروس‌ها بسته به کدهای خود عملیات تخریبی متفاوتی انجام می‌دهند.
Worm	در اغلب موارد ویروس‌های کامپیوتری با ورود به سیستم باعث خرابی رایانه و برنامه‌های موجود در آن می‌شوند. در واقع هدف ویروس‌های رایانه‌ای آلوده کردن رایانه و از بین بردن اطلاعات است. در حالی که کرم‌ها به‌محض ورود به رایانه شروع به تکثیر یا بازتولید خود می‌کنند. هدف کرم‌ها تکثیر خود در تمام شبکه یا رایانه است به‌طوری‌که با استفاده از منابع شبکه باعث از دسترس خارج شدن آنها و یا اشغال پهنای باند شبکه می‌شوند.

Trojan	کلمه تروجان از افسانه یونانی جنگ تروا گرفته شده است. در این جنگ یونانی‌ها اسب چوبی بزرگی ساختند به طوری‌که سربازان آنها در آن پنهان شدند و به دشمنان خود هدیه کردند. سپس سربازان از غفلت دشمن استفاده کرده و وارد شهر شدند و... عملکرد تروجان نیز به همین صورت است. در قالب یک برنامه جذاب، کاربر را ترغیب به اجرا و یا نصب می‌کند. تروجان‌ها برخلاف ویروس‌ها خود را تکثیر نمی‌کنند، بلکه به قسمت‌های مختلف رایانه نفوذ کرده، سپس عملیاتی را که در کد تروجان گنجانده شده اجرا می‌کنند. برای مثال این عملیات می‌تواند معرفی رایانه شما به ویروس‌ها باشد در حالی‌که در ابتدا شما را به قصد پاک‌سازی رایانه شخصی‌تان از ویروس‌ها ترغیب به نصب کرده است.
RootKit	روت‌کیت یک برنامه است که در سطح سیستم‌عامل فعالیت می‌کند و کاربر متوجه حضور آن در سیستم خود نمی‌شود. معمولاً روت‌کیت‌ها یک فایل یا کلید رجیستری خاص را در سیستم‌عامل پنهان می‌کنند. از این رو شناسایی و پیدا کردن آنها کاری دشوار است. برای مثال یک روت‌کیت می‌تواند با تغییراتی که در سیستم عامل یا منابع آن می‌دهد به اهداف خود برسد که این امر می‌تواند باعث بروز مشکلاتی در سیستم شود. به رایانه‌ای که تحت سلطه روت‌کیت در آمده است زامبی Zombie گفته می‌شود.
Ransomware	باج‌افزارها گونه دیگری از بدافزارها هستند که بعد از ورود به سیستم، برخی دسترسی‌ها به سیستم را محدود می‌کنند و تا زمان پرداخت نشدن وجه یا عملی نشدن خواسته آنها، دسترسی‌ها به حالت قبل باز نمی‌گردد. برای مثال یک باج‌افزارمی‌تواند تمام فایل‌های یک رایانه را به‌صورت رمز در آورد و در ازای دریافت باج آنها را برای کاربر رمزگشایی کند.
SpyWare	به برنامه‌هایی گفته می‌شود که بدون رضایت کاربر و اطلاع او اطلاعات مشخصی از رایانه را به سرقت می‌برند.

اهمیت ثبت رخدادها در امنیت

پاسخگویی به حوادث یکی ازضروری‌ترین کارها در امن‌سازی سامانه‌های اطلاعاتی است چراکه تکرارحملات می‌تواند منجر به افزایش دامنه خسارات و زیان‌هایی بر سرمایه‌های سازمانی گردد. در این بخش سیستم تشخیص حمله (IDS) Intrusion DetectionSystem بررسی خواهد شد.

در شبکه سه نوع مهاجم یا نفوذگر وجود دارد:

Masquerader	فرد غیرمجاز که از حساب کاربری قانونی شخص دیگری سوءاستفاده می‌کند (خارجی).
Misfeasor	کاربر قانونی که از امتیازات داخلی خود سوءاستفاده می‌کند (داخلی).
Clandestine user	کاربرانی که دسترسی سوپروایزری پیدا می‌کنند که هم کاربران داخلی را شامل می‌شود و هم خارجی. در این نوع ابتدا آسیب‌پذیری‌های سیستم شناسایی می‌شود و از طریق این آسیب‌پذیری دسترسی سوپروایزری برای خود فراهم می‌کند وکار خود را انجام می‌دهد.

- اگر نفوذ به سرعت شناسایی شود، مزاحم را می‌توان شناسایی و قبل از آسیب رسیدن به سیستم آن را خارج کرد.
- سیستم تشخیص مؤثر به‌عنوان یک عامل بازدارنده برای جلوگیری از نفوذ عمل می‌کند.

قابل ذکر است که به مرور زمان نرم‌افزارهای مربوط به هک و نفوذ بیشتر ارائه شده و به آسانی در اختیار همگان قرار می‌گیرد. به همین خاطر هنگام توسعه سیستم باید به امنیت آن توجه کرد. یک سیستم تشخیص نفوذ مانند دزدگیر ماشین یک عامل بازدارنده است، اما مانع کامل از نفوذ نمی‌شود.

- تست نفوذ باعث می‌شود که آسیب‌پذیری سیستم برای خود ما هم مشخص شود.

فرایند تست تشخیص نفوذ: مهاجم ابتدا اطلاعاتی درمورد سیستم به‌دست می‌آورد و سعی می‌کند یک‌سری دسترسی اولیه به سیستم پیدا کند و این دسترسی را بالا ببرد. در نهایت پس از پایان کار، ردپای خود را با حذف Logها پاک می‌کند تا قابل شناسایی نباشد. هدف عمده نفوذگران به دست آوردن گذرواژه است.

- یکی از تکنیک‌های تشخیص نفوذ استفاده ازروش‌های آماری در شبکه است. برای مثال ترافیک شبکه یا فعالیت Hostها بررسی می‌شود. در شبکه‌ای که در هر ثانیه ۵۰۰ پیام ارسال می‌شود اگر این مقدار به یک‌باره تغییر کند می‌تواند نشان‌دهنده یک نفوذ باشد.

پاسخ به فعالیت‌ها

فعالیت منزل
ص۳۹

بررسی کنید IDS و IPS مخفف چه واژگانی است؟

IDS (Intrusion Detection System)

یک سیستم محافظتی است که خرابکاری‌های در حال وقوع روی شبکه را شناسایی می‌کند. روش کار به این صورت است که با استفاده از تشخیص

نفوذ که شامل مراحل جمع‌آوری اطلاعات، پویش پورت‌ها، به دست گرفتن کنترل کامپیوترها و نهایتاً هک کردن است، می‌تواند نفوذ خرابکاری‌ها را گزارش و کنترل کند.

IPS (Intrusion Prevention System)

سیستم جلوگیری از نفوذ (IPS) یک وسیله امنیتی است که بر فعالیت‌های یک شبکه و یا یک سیستم نظارت کرده تا رفتارهای ناخواسته یا مخرب را شناسایی کند. در صورت شناسایی این رفتارها، بلافاصله عکس‌العمل نشان داده و از ادامه فعالیت آنها جلوگیری می‌کند.

مدیریت خطر پذیری در سیستم

برای تدریس این بحث بهتر است هنرجویان را گروه‌بندی کرده و از هر گروه بخواهید تا مدیریت خطر را برای یک مکان یا سازمان فرضی انجام دهند. برای مثال برای سیستم مدرسه دارایی‌ها را فهرست کنند و براساس ارزش دارایی آنها را اولویت‌بندی کنند. تهدیدهای موجود را شناسایی و در نهایت راهکارهای مقابله با تهدیدها را در کلاس ارائه دهند.

سازمان‌ها باید محیط‌های امنی را که درآن فرایندهای کسب وکار اجرا می‌شود، ایجادکنند.

مدیریت خطرپذیری: فرایند شناسایی وکنترل خطرات یک سازمان قبل از وقوع حمله است.

کنترل خطرپذیری: استفاده از کنترل‌های لازم به‌منظور کاهش خطرات داده‌ها در یک سازمان و سیستم‌های اطلاعاتی است.

مدیریت خطرپذیری برای امن بودن یک سازمان و دارایی‌های آن نیاز است. مدیریت خطر شرط برآورده شدن امنیت است و اگر همه چیز درست و به‌دقت در نظر گرفته نشود نمی‌توان مدیریت خطر را به‌درستی انجام داد.

مدیریت خطر شامل سه فاز اساسی است که عبارت‌اند از:

۱ **شناسایی خطر:** در این مرحله فهرست دارایی‌های سازمان شناسایی و ایجاد می‌شود. سپس براساس ارزش دارایی، طبقه‌بندی و اولویت‌دهی می‌شوند و در نهایت باید تهدید هر دارایی مشخص شود.

برای مثال در سیستم مدرسه، برگه‌های سؤالات امتحانی یک دارایی محسوب می‌شود و تهدید آن، پخش شدن سؤالات قبل از برگزاری آزمون است.

۲ **ارزیابی خطر:** در این مرحله آسیب‌پذیری مربوط به تهدیدها و خطرات شناسایی و فهرست‌بندی و براساس اولویت به آنها پرداخته می‌شود. تهدیدات

خطرناک باید در اولویت قرار بگیرند و استراتژی مقابله با آنها نیز مشخص شود. بلاهای طبیعی خطر هستند. برای مثال وقوع زلزله یک خطر طبیعی برای سیستم مخابرات است زیرا در هنگام وقوع زلزله به یک‌باره تعداد زیادی از افراد شروع به شماره‌گیری می‌کنند در نتیجه برخی از مشترکین قادر به برقراری تماس نخواهند بود و سیستم مخابرات ویژگی در دسترس‌پذیری خود را از دست خواهد داد.

۳ **کنترل خطر:** این مرحله شامل انتخاب استراتژی مؤثر در هنگام بروز خطر است. فرض کنید در مورد خطر زلزله که در بخش قبل آمد یک استراتژی کنترل آن می‌تواند استفاده از پشتیبان‌گیری و انتخاب سرور مرکزی در مناطق جغرافیایی مختلف و یا استفاده از زیرساخت‌های مناسب باشد.

در مورد برخی از خطرات، عامل بازدارنده‌ای وجود ندارد. در این هنگام باید مشخص کنیم اگر تهدیدی عملی شد چگونه اثر آن را به حداقل برسانیم.

هر سازمان یکسری عناصر کلیدی دارد (سخت‌افزار، نرم‌افزار، داده، مردم، کدهای برنامه‌نویسی، شبکه و...)

مثال ۱:

فرض کنید یک نرم‌افزار امن داریم یعنی در هنگام طراحی نرم‌افزار تمام اصول امنیتی اجرا شده است اما سخت‌افزار امن نداریم. یعنی نرم‌افزار در شبکه‌ای اجرا می‌شود که حفاظت فیزیکی از کابل‌های شبکه انجام نمی‌شود. پس مهاجم با ورود به سازمان با وصل کردن یکی از کابل‌های شبکه به رایانه قابل‌حمل خود می‌تواند از نرم‌افزارهای موجود در شبکه سوءاستفاده کند.

مثال ۲:

قطعی برق می‌تواند در سازمانی یک خطر باشد. حال فرض کنید در این سازمان UPS هم وجود ندارد. مشاهده می‌شود که باز امنیت به دلیل نقص سخت‌افزار خدشه‌دار شده است.

مهم‌ترین دارایی در هر سازمانی داده‌ها هستند و باید برای حفاظت از آن تمام موارد امنیتی اجرا شود. دقت شود یکی از اشتباهات در تأمین امنیت کاهش سطح دسترسی به داده‌ها است. همیشه باید یک تعادل بین امنیت و دسترس‌پذیری باشد. امنیت و دسترس‌پذیری را باید مانند دو کفه ترازو در نظر گرفت که همیشه باید دو کفه ترازو در یک سطح باشند.

دقت داشته باشید امنیت یک امر نسبی است و به‌طور کلی نمی‌توان همیشه امنیت را صددرصد اجرا کرد. هنرجویان باید بدانند که خط مشی اصلی امنیت تأکید بر

پیشگیری از خطر است. پس هنرجویان باید توجیه شوند با فراگیری دانش امنیت نمی‌توان تمام مراحل امنیت را اجرا کرد.

در یک شبکه که تعداد زیادی از افراد با برنامه‌ای در حال کار هستند آن نرم‌افزار به اندازه ضعیف‌ترین عنصر امن است. به این معنی که اگر شما یک زنجیر با مهره‌های بسیار قوی ساخته باشید اما فقط یکی از آنها کمی نازک‌تر باشد، زنجیر ضخیم از همان قسمت نازک کوچک خواهد گسست.

پاسخ به فعالیت‌ها

فعالیت گروهی
ص ۴۳

با دوستان خود در این مورد به بحث و بررسی بپردازید و نتایج را برای کمک به تصمیم‌گیری بهتر در جدول یادداشت کنید.

روش پشتیبان‌گیری	مزیت‌ها	عیب‌ها
کامل	کاهش زمان بازیابی اطلاعات	طولانی بودن زمان پشتیبان‌گیری نیاز به فضای زیاد ذخیره‌سازی
افزایشی	کمترین زمان پشتیبان‌گیری نسبت به دو روش دیگر	طولانی بودن زمان بازیابی اطلاعات نسبت به دو روش دیگر
تفاوتی دوره‌ای	کاهش زمان پشتیبان‌گیری کاهش فضای ذخیره‌سازی	افزایش زمان بازیابی اطلاعات

پژوهش
ص ۴۸

در مورد محتوای دوره‌های آموزشی زیر و شیوه کسب مدرک آن تحقیق کنید.

Security+

امروزه امنیت شبکه در بین سازمان‌ها به موضوع بسیار مهمی تبدیل شده است و شرکت در دوره Security+ باهدف آشنایی با اصول امنیت شبکه می‌تواند کمک بسیار شایانی در جهت رفع این نیاز کند. با شرکت در این دوره و کسب گواهی آن افراد قادر خواهند بود تا از پس مشکلات مربوط به امنیت شبکه و مشکلات مربوط به نفوذ هکرها برآیند.

CEH-Certifiec Ethical Hacker

مدرک CEH یا مدرک تخصصی هکرهای قانونمند است. این مدرک بر روی تکنیک‌ها و روش‌های هک از دیدگاه دفاعی تأکید دارد. تکنیک‌های هک شامل راه‌ها و روش‌هایی است که طی آن برنامه‌ها به‌نحوی طراحی می‌شوند که کارهایی فراتر از آنچه از آنها انتظار می‌رود را در جهت سیاست‌ها و پروسه‌های امنیتی انجام می‌دهند.

CISSP (Certified Information System Security Professional)
مدرک CISSP به‌وسیله کنسرسیوم امنیت اطلاعات (ISC) بنا نهاده شده است و هدف آن ایجاد یک سطح مهارت حرفه‌ای و عملی در زمینه امنیت اطلاعات است. مدرک CISSP به دلیل عدم وابستگی آن به محصولی خاص، به‌عنوان یک عنصر کلیدی در ارزشیابی داوطلبان کار در مؤسسات بزرگ و سیستم‌های Enterprise شناخته می‌شود. افراد دارای مدرک CISSP دارای توانایی لازم در طراحی و پیاده‌سازی سیاست‌های کلان امنیتی هستند. این افراد دارای درک کامل و مستقلی از مسائل مربوط به مهندسی اجتماعی بوده و قادر به ایجاد امنیت اطلاعات در یک سازمان با ارائه خط مشی ویژه با سیاست‌های خاص امنیتی آن سازمان هستند.

پس از تدریس

الف) فعالیت‌های تکمیلی

۱ بهتر است در مبحث امنیت، از هنرجویان خواسته شود تا در مورد امن‌سازی یک محیط راهکارهایی ارائه دهند. هدف از مطرح کردن این فعالیت آشنایی هنرجویان با امنیت فیزیکی محل کار است. مواردی مانند:
- استفاده از درهای ضد سرقت
- استفاده از نگهبان
- استفاده از دوربین‌های مداربسته
- استفاده از سیستم اطفای حریق

۲ هوشیاری امنیتی چیست؟ در مورد جنبه‌های مختلف آن تحقیق کنید.
۳ در مورد APA و مراکز CERT تحقیق کنید.
۴ برای هر یک از جنبه‌های اصلی امنیت (محرمانگی، دسترس‌پذیری و جامعیت) مثال‌هایی ارائه کنید.
۵ چه راهکارهایی برای حفاظت رایانه در برابر حملات غیرفعال وجود دارد.
۶ در مورد AAA تحقیق کنید.
۷ در مورد هر کدام از سیستم‌های رمزنگاری زیر تحقیق کنید.
الف) رمزنگاری DES
ب) رمزنگاری AES
۸ امضای دیجیتال چیست؟ نحوه کار آن به چه صورت است.
۹ بیت‌کوین Bitcoin چیست؟ در مورد مشکلات آن تحقیق کنید.