با ایران توشه
یک قدم جلوتر
باش!

ایران توشه
توشه ای برای موفقیت



ایران توشه، مرجع دانلود فایل های کمک آموزشی دانش آموزان و کنکوری ها

همه چیز
برای موفقیت
تو!

- دانلود رایگان آزمون های آزمایشی قلمچی، خیلی سبز، گاج و ...
- دانلود رایگان گام به گام تمامی دروس
- دانلود رایگان نمونه سوالات امتحانی (نوبت اول و دوم) و امتحانات نهایی
- دانلود رایگان جزوه های کمک آموزشی و شب امتحانی

کافیست هر فایلی که نیاز دارید را در گوگل به این صورت جستجو کنید:

فایل مورد نیاز + ایران توشه

مثال:

دانلود گام به گام دوازدهم تجربی ایران توشه



irantooshe.ir

t.me/irantooshe

گام به گام دانش فنی تخصصی کامپیوتر پودمان دوم

عنوان فصل: تحلیل امنیت در فاوا

از صفحه‌ی ۲۶ تا صفحه‌ی ۴۸ کتاب

در این فایل پاسخ فعالیت‌ها، کارهای کلاسی، تمرین‌ها و پرسش‌های فصل تحلیل امنیت در فاوا آمده است.

تهیه‌شده در ایران‌توشه، توشه‌ای برای موفقیت

irantooshe.ir

فهرست پرسش‌ها

۱ صفحه ۲۶ · کنجکاوی — سرقت رایانه قابل حمل؛ حمله فعال یا غیرفعال ۴

۲ صفحه ۲۷ · کنجکاوی — تراکنش ناموفق و پیش‌بینی بانک ۴

۳ صفحه ۲۷ · متن — فعالیت‌های پیش از حمله ۴

۴ صفحه ۲۷ · متن — مهندسی اجتماعی ۵

۵ صفحه ۲۸ · متن — انواع حملات ۶

۶ صفحه ۲۸ · فعالیت منزل — روش‌های کنترل دسترسی و احراز هویت ۶

۷ صفحه ۳۱ · کنجکاوی — زمان‌بندی انتخاب واحد دانشجویان ۸

۸ صفحه ۳۳ · فعالیت منزل — شیوه کار و خسارت بدافزارها ۸

۹ صفحه ۳۹ · فعالیت منزل — IDS و IPS مخفف چه واژگانی است ۹

۱۰ صفحه ۴۰ · فعالیت گروهی — روش‌های پشتیبان‌گیری؛ مزیت‌ها و عیب‌ها ۹

۱۱ صفحه ۴۸ · پژوهش — دوره‌های آموزشی امنیت و شیوه کسب مدرک ۱۰

ایران توشه
توشه ای برای موفقیت

۱ صفحه ۲۶ کنجکاوی

از میان سرقت رایانه قابل حمل و مشاهده پرونده‌ها با نفوذ به رایانه قابل حمل کدام مورد حمله فعال و کدام مورد حمله غیر فعال به شمار می‌آید؟

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

۲ صفحه ۲۷ کنجکاوی

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: معمولا هنگام خریدهای اینترنتی پول باید از حساب مبدا کسر و به حساب مقصد اضافه شود. در برخی موارد هنگام خرید مبلغ از حساب مبدا کسر شده و به حساب مقصد واریز نمی‌شود. در این گونه 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.

۳ صفحه ۲۷ متن

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 تاخیرهای 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، اعتبار سنجی و حسابداری می‌توان از هنرجویان سوالاتی 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 انجام شده 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.

ایران توشه
توشه ای برای موفقیت

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**
اعتبار سنجی (مجاز شناسی) 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.

۴ صفحه ۲۷ متن

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 به‌دست‌آمده 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. متاسفانه بسیاری از افراد برای اینکه گذرواژه‌های خود را فراموش نکنند اقدام به انتخاب گذرواژه‌های ساده کرده و در نتیجه به راحتی در دام می‌افتند.

این فایل توسط سایت ایران‌توشه تهیه شده است.

irantooshe.ir

۵ صفحه ۲۸ متن

انواع حملات

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

حملات غیرفعال Passive	حمله‌کننده از اطلاعات شبکه استفاده می‌کند اما تاثیری 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 تاثیر 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 عبارتند از:

حمله اختلال در سرویس DOS	ممانعت از سرویس، از استفاده عادی یا مدیریت امکانات جلوگیری می‌کند. به عنوان مثال مهاجم ممکن است پیام‌های ارسال‌شده به مقصد خاصی را توقیف کند. شکل دیگر این حمله تخریب کل شبکه از طریق غیرفعال کردن شبکه یا 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.

ایران توشه
توشه ای برای موفقیت
این فایل توسط سایت ایران‌توشه تهیه شده است.
irantooshe.ir

۶ صفحه ۲۸ فعالیت منزل

برای کنترل دسترسی و احراز هویت روش‌های مختلفی وجود دارد. نام کاربری و گذرواژه است. در فهرست زیر تعدادی از این روش‌ها معرفی شده‌اند. در مورد میزان امنیت هر کدام از این روش‌ها، مکان‌ها و وسایلی که از این روش‌ها استفاده می‌کنند جستجو کنید و نتیجه را در کلاس ارائه دهید.

پاسخ به فعالیت‌ها

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 منحصر به فرد است، از این ویژگی می‌توان به عنوان امضاء و سیستم تشخیص هویت استفاده کرد. از مزایای این روش می‌توان به سهولت استفاده، در دسترس بودن و عدم نیاز به‌خاطرسپاری 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. در حال حاضر از این فناوری در فرودگاه‌ها و دیگر مراکز سری و حساس برای شناسایی افراد و کارکنان استفاده می‌شود.
دستگاه گذرواژه‌ساز 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 کارتی هستند که بر روی آنها یک تراشه حاوی اطلاعات مورد نظر نصب شده است. این اطلاعات می‌تواند توسط دستگاه کارت‌خوان از طریق دسترسی به حافظه آن خوانده شود. این کارت‌ها به کارت‌های تراشه‌دار یا مدار مجتمع نیز معروف هستند و می‌توانند به‌عنوان جایگزین کارت‌پول، 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 با کیفیتی را از چهره یک شخص می گیرند. به عنوان مثال این تصاویر شامل نشانه‌های خاص در چهره، فاصله چشم‌ها، عرض بینی، شکل گونه‌ها و ... است. سپس سیستم تشخیص هویت این اطلاعات را با اطلاعات موجود در پایگاه داده خود مقایسه و نزدیکترین چهره به ویژگی‌های به‌دست‌آمده را شناسایی می‌کند. قابل ذکر است هر چه اطلاعات موجود در پایگاه داده بیشتر باشد دقت تشخیص این سیستم نیز بیشتر می‌شود.
فناوری رادیو شناسه RFID (Radio Frequency Identification)	سامانه‌ای جهت شناسایی خودکار افراد، اشیاء و حیوانات است. به این صورت که یک تگ الکترونیکی یا دستگاه فرستنده خودکار به شی مورد نظر وصل می‌شود. هر شی یک تگ منحصر بفرد یا یک کد شناسایی خاص را دارا است. سپس یک دستگاه کدخوان RFID با تولید میدان مغناطیسی در محدوده خود قادر به شناسایی تگ‌های فعال است.

۷ صفحه ۳۱ کنجکاوی

بیشتر دانشگاه‌ها انتخاب درس در هر نیم سال تحصیلی را به صورت اینترنتی انجام می‌دهند. معمولا دانشگاه‌ها افراد را بر اساس حروف الفبا و یا سال ورود به دانشگاه، در روزهای متفاوتی دانشجو را ملزم به انجام انتخاب واحد می‌کنند. دلیل این زمان‌بندی چیست؟

پاسخ: سرور دانشگاه در هر لحظه امکان پردازش و پذیرش تعداد محدودی از افراد را دارد. در صورتی که همه دانشجویان به یکباره اقدام به انتخاب واحد کنند، قاعدتا سایت مربوطه از فعالیت باز می‌ماند. در نتیجه برای کنترل دسترس‌پذیری سایت، برنامه زمان‌بندی برای کاهش بار ترافیک سایت اجرا می‌شود.

۸ صفحه ۳۳ فعالیت منزل

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

بدافزار	شیوه کار
Virus	ویروس یک برنامه کامپیوتری از نوع بد افزار 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 به محض ورود به رایانه شروع به تکثیر یا بازتولید خود می‌کنند. هدف کرم‌ها تکثیر خود در تمام شبکه یا رایانه است به طوری که با استفاده از منابع شبکه باعث از دسترس خارج شدن آنها و یا اشغال پهنای باند شبکه می شوند.
SpyWare	به برنامه‌هایی گفته می‌شود که بدون رضایت کاربر و اطلاع او اطلاعات مشخصی از رایانه را به سرقت می‌برند.
Trojan	کلمه تروجان از افسانه یونانی جنگ تروا گرفته شده است. در این جنگ یونانی‌ها اسب چوبی بزرگی ساختند به طوری که 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 بر خلاف ویروس‌ها خود را تکثیر نمی‌کنند، بلکه به قسمت‌های مختلف رایانه نفوذ کرده، سپس عملیاتی را که در کد تروجان گنجانده شده اجرا می کنند. برای مثال این عملیات می‌تواند معرفی رایانه شما به ویروس‌ها باشد در حالی که 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. معمولا 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 باج‌افزار می‌تواند تمام فایل‌های یک رایانه را به صورت رمز در آورد و در ازای دریافت باج آنها را برای کاربر رمزگشایی کند.

۹ صفحه ۳۹ فعالیت منزل

بررسی کنید IDS و IPS مخفف چه واژگانی است؟

IDS (Intrusion Detection System)

یک سیستم محافظتی است که خرابکاری‌هایی در حال وقوع روی شبکه را شناسایی می‌کند. روش کار به این صورت است که با استفاده از تشخیص نفوذ که شامل مراحل جمع آوری اطلاعات، پویش پورت‌ها، به دست گرفتن کنترل کامپیوترها و نهایتا 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.

ایران توشه
توشه ای برای موفقیت

۱۰ صفحه ۴۰ فعالیت گروهی

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

۱۱ صفحه ۴۸ پژوهش

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+ با هدف 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–Certified Ethical Hacker

مدرک CEH یا مدرک تخصصی هکرهای قانونمند است. این مدرک بر روی تکنیک‌ها و روش‌های هک از دیدگاه دفاعی تاکید دارد. تکنیک‌های هک شامل راه‌ها و روش‌هایی است که طی آن برنامه‌ها به نحوی 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 توسط 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.

این فایل توسط سایت ایران‌توشه تهیه شده است.

irantooshe.ir