بسم الله الرحمن الرحیم

بررسی امنیت در سخت‌افزار و نرم‌افزار

(تهدیدات و استانداردها)

تدوین و گردآوری:

دکتر فضل‌الله ادیب‌نیا

مهندس مهیلا دادفرنیا

سرشناسه	:	ادیب‌نیا، فضل الله، ۱۳۴۱ -
عنوان و نام پدیدآور	:	بررسی امنیت در شبکه و نرم‌افزار (تهدیدات و استانداردها)
مشخصات نشر	:	یزد: دانشگاه یزد، ۱۳۹۴.
مشخصات ظاهری	:	۲۰۰ص.: مصور ،جدول ،نمودار
شابک	:	978-600-6309-61-3
وضعیت فهرست نویسی	:	فیپای مختصر
یادداشت	:	فهرستنویسی کامل این اثر در نشانی: http://opac.nlai.ir قابل دسترسی است
یادداشت	:	واژه نامه .
شناسه افزوده	:	دادفرنیا، مهیلا،۱۳۶۱-
شناسه افزوده	:	دانشگاه یزد
شماره کتابشناسی ملی	:	۴۸۶۳
کد پیگیری	:	۳۶۲۴۷

مرکز انتشارات دانشگاه یزد

یزد، صفائیه، بلوار دانشگاه، صندوق پستی ۷۴۱- ۸۹۱۹۵ تلفن: ۹- ۳۸۲۱۱۶۷۰ – ۰۳۵

دورنگار: ۸۲۰۰۱ – ۰۳۵۱

عنوان کتاب: بررسی امنیت در شبکه و نرم‌افزار (تهدیدات و استانداردها)

تدوین و گردآوری: دکتر فضل الله ادیب نیا، مهندس مهیلا دادفرنیا

ناشر: انتشارات دانشگاه یزد

لیتوگرافی، چاپ و صحافی: یزد- انتشارات شاهنده

نوبت چاپ: اول

سال چاپ: ۱۳۹۴

شمارگان: ۱۰۰۰ نسخه

قیمت پشت جلد: ۱۲۰،۰۰۰ ریال

شابک: ۳-۶۱-۶۳۰۹-۶۰۰-۹۷۸

مرکز پخش: موسسه کتابیران

تهران، میدان انقلاب، کارگر شمالی، خیابان نصرت، خیابان دکتر قریب، نرسیده به فرصت، پلاک ۷.

تلفن: ۱۵ – ۶۶۵۶۶۵۱۰- ۰۲۱

فهرست

فصل دوم

پیش گفتار

باتوجه به توسعه روزافزون سیستم‌ها و دنیای فناوری اطلاعات، فراهم آوردن امنیت در سامانه‌ها از جایگاه ویژه‌ای برخوردار می‌باشد؛ زیرا همراه با پیشرفت علم و حرفه‌ای‌تر شدن برنامه‌ها، هکرها نیز پیشرفت فوق‌العاده‌ای کرده‌اند و روزانه خبرهای زیادی درباره نفوذ بیگانگان و هکرها در سیستم‌ها شنیده می‌شود. بنابراین آشنایی با امنیت و نحوه برقراری آن و همچنین مقابله با خطرات احتمالی جهت بقای سازمان‌ها ضروری می‌باشد. به همین دلیل در این کتاب سعی شده است، در باره امنیت در سازمان‌ها نوشته شود.

با توجه به اینکه موضوع امنیت در کشورمان در طی سالیان اخیر مطرح و حساس گردیده است و کتاب‌های فارسی کمی درباره امنیت سایبری وجود دارد، تلاش نویسندگان بر این بوده که این کتاب به روزترین مطالب را در ارتباط با استاندارد به‌روز دنیا به زبان ساده بیان کند و مطالب آن به نحوی انتخاب شده که جهت پژوهش و برنامه‌نویسان سازمان‌ها مفید بوده و سوالات کارکنان را نیز پاسخ دهد؛ مخصوصا که نویسندگان کتاب، سابقه اجرایی در سازمان‌ها را دارند. علاوه بر این، نیاز آموزشی دانشجویان را در درس‌های امنیتی مقطع کارشناسی و کارشناسی ارشد پاسخ دهد. همچنین جهت درک بهتر مفاهیم خواننده کتاب، در قسمت‌هایی که جنبه عمومی بیشتری دارد، مثال‌ها و توضیحات بیشتری به متون ترجمه شده اضافه نمودیم.

در خاتمه با سپاس از عنایت الهی در تهیه این کتاب، از حمایت و پشتیبانی ستاد توسعه فناوری اطلاعات، ارتباطات و میکروالکترونیک معاونت علمی و فناوری ریاست جمهوری و مرکز آپای دانشگاه یزد، دکتر کیارش میزانیان جهت بازنگری کتاب، دکتر عبدالمجید انصاری مدیر امور پژوهشی دانشگاه یزد و سایر مسئولین دانشگاه که در چاپ این کتاب همکاری داشته‌اند، تشکر و قدردانی می‌گردد. لازم به یاد آوری است که این کتاب را تعدادی از اساتید صاحب نام در حوزه دانشگاه بازبینی و داوری نموده‌اند و نقطه نظرات آنان در اصلاح، تغییر و تکمیل مندرجات آن لحاظ شده است. با این وصف، اگر همچنان اشتباهی در آن مشاهده شود، به طور قطع به عهده نویسندگان می‌باشد و پیشاپیش تمام کاستی‌های این کتاب را پذیرفته و از هر پیشنهاد یا انتقادی به منظور بهتر شدن کتاب استقبال می‌شود و خواهشمند است نویسندگان را با اشاراتی به آدرس m-dadfarnia@stu.yazd.ac.ir ، [illegible]@[illegible].ces.yazd.ac.ir مستحضر فرمایید تا اصلاحات انجام و تکمیل گردد. امید است این خدمت ناچیز مورد قبول خداوند متعال قرار گرفته و قابل استفاده برای شما عزیزان باشد.

مقدمه

در دنیای سایبری امروز، افزایش تعداد برنامه‌های تحت وب و پیچیدگی تهاجم روی شبکه‌های کامپیوتری باعث شده است که مسئله محافظت و مراقبت یکی از مسائل کلیدی در بحث امنیت کامپیوتر شود و جرایم رایانه‌ای به یکی از مباحث جدی و مهم تبدیل گردد. از آنجا که یک سازمان از صدها فرد تشکیل شده که خود یک شبکه بزرگ‌تری را تشکیل می‌دهند و از طریق رایانه با یکدیگر تعامل دارند، ارتباط اجتماعی در کنار تکنیک‌های فنی باعث چالش‌هایی در زمینه امنیت شده است. به همین منظور، شناسایی حملات ممکن در این ارتباطات اجتماعی به منظور یافتن تکنیک‌های قابل استفاده توسط هکر[1] و همچنین جهت مقابله توسط مدیر سیستم ضروری می‌باشد.

در دنیای کامپیوتر، در یک تعریف ساده می‌توان هکر را فردی نامید که در یک سیستم نفوذ می‌کند و آن سیستم را مجبور می‌کند کاری که می‌خواهد را انجام دهد؛ حتی اگر سیستم نخواهد. اما تعریف دقیق‌تر، هکر را برنامه‌نویس حرفه‌ای و هوشمندی معرفی می‌کند که با استفاده از تخصص و تسلط خود بر حیطه‌های مختلف دنیای کامپیوتر و وب، قادر است در لایه‌های پیچیده‌تر سیستم‌ها نفوذ کرده و موانع آن را برطرف کند و از آن به هر نحو بهره‌برداری و سوء استفاده نماید[2] یا بر آن اساس سیستمی نو خلق کند. از مشخصه‌های یک هکر می‌توان این موارد را عنوان کرد:

- کسی که از یادگیری جزئیات یک زبان برنامه‌نویسی یا سیستم لذت می‌برد.
- کسی که از انجام دادن یک برنامه لذت می‌برد.
- کسی که ارزش هک دیگران را درک کرده و به آن احترام می‌گذارد.

---

[1] Hackers
[2] Exploit

- کسی که در عمق یک سیستم فرو می‌رود تا حداکثر توانایی‌های آن را درک و از آن استفاده کند.
- کسی که معمولا به همان میزان که در یاد گرفتن شوق دارد، یاد دادن را هم دوست دارد.

در واقع، اولین کسانی که هکر نامیده شدند، افرادی بودند که در موسسه فناوری ماساچوست به هر کاری به جز درس خواندن می‌پرداختند. واژه هکر از سال ۱۹۸۶ بین دانشجویان این موسسه شکل گرفت و به کسانی که همواره در پشت بام و محل‌های غیرمجاز بودند، گفته می‌شد. هکرهای امنیتی را می‌توان به چهار مجموعه زیر تقسیم نمود [۸]:

هکر کلاه سفید[1] یا هکرهای خوب : هکری که از دانش خود برای محافظت و ارتقای سطح امنیتی یک سیستم و تشخیص نفوذ استفاده می‌کند و از طرف شرکت‌های زیادی با حقوق بسیار بالا به‌کار گرفته می‌شود.

هکر کلاه سیاه[2] یا هکرهای مخرب : این نوع هکر، نقطه مقابل کلاه سفید می‌باشد؛ تنها به فکر نفوذ است و زیاد به قانون اهمیت نمی‌دهد و معمولا مهارت بالایی دارد. از نفوذ[3] جهت آسیب رساندن به شبکه‌ها و سرورها استفاده می‌کند و بدین وسیله کسب درآمد می‌کند.

هکر کلاه خاکستری[4] یا هکرهای میانه‌رو : هکری که بهتر است بگوییم، گاهی با امن‌سازی و گاهی با نفوذ، هر جا که پول باشد همانجا است. این فرد تمایل خاصی به یک طرف ندارد و بسته به موقعیت، گاهی اعمال خرابکارانه و گاهی هم اعمال مفید انجام می‌دهد.

[1] Whitehat
[2] Blackhat
[3] Hack
[4] Grayhat

هکر کلاه صورتی[1] یا هکرهای خوشحال : هکر کلمه مناسبی برای این گروه نیست، فردی که با استفاده از انواع ابزار و آسیب‌پذیری عمومی با تخریب نرم‌افزارها و سایت‌ها خود را هکر جلوه می‌دهد و سعی بر کسب شهرت دارد.

در رابطه با امنیت اصطلاحات مختلفی مانند تهدید، آسیب‌پذیری و ریسک مطرح می‌شود که در ادامه تعریف آن آمده است:

تهدید[2] : تهدید، خطری است که با استفاده از آسیب‌پذیری، در امنیت شکاف ایجاد می‌نماید و سبب آسیب و زیان می‌گردد. یک منبع (فیزیکی یا منطقی) می‌تواند یک یا چند آسیب‌پذیری داشته باشد که توسط یک عامل تهدید به کار گرفته شده است. مثلا خرابی فنی سخت‌افزار (مثل خرابی تجهیزات) و خرابی در نرم‌افزار (باگ‌ها، مشکلات کد و حفره‌های نا شناخته) و همچنین وقایع طبیعی همچون آسیب به مرکز داده بر اثر وقوع زلزله از انواع تهدید می‌باشند.

آسیب‌پذیری (کاستی)[3] : آسیب‌پذیری یک ضعف در دارایی است که می‌تواند توسط یک یا چند تهدید مورد بهره‌برداری قرار گیرد. به عنوان مثال یک مهاجم می‌تواند از آسیب‌پذیری سرریز برای نصب بدافزار و در نتیجه آسیب رساندن بهره ببرد. در مبحث امنیت کامپیوتر، آسیب‌پذیری ضعفی است که به مهاجم اجازه کاهش تضمین اطلاعات سیستم را می‌دهد، بنابراین برطرف کردن این نوع ضعف‌ها اهمیت زیادی دارد. سه عنصر مستعد بودن و وجود نقص در سیستم، دسترسی مهاجم به نقص و توانایی مهاجم جهت نفوذ از طریق نقص در آسیب‌پذیری نقش دارند.

ریسک : ریسک یا مخاطره احتمال رخ دادن اتفاق ناگواری است که سبب زیان می‌شود. برای وجود ریسک باید هم آسیب‌پذیری و هم تهدید از این آسیب‌پذیری وجود داشته باشد. در صورت

[1] Pink
[2] Threat
[3] Vulnerability

عدم وجود آن دو، ریسک ایجاد نمی‌گردد. یک هکر (تهدید) می‌تواند از یک آسیب‌پذیری سوء استفاده نماید و این دو در مجموع یک ریسک را تشکیل می‌دهند[۹].

حمله سایبری[1] نیز هر گونه آسیب‌پذیری تفسیر می‌شود که از حالت بالقوه به بالفعل تبدیل شود. چنانچه حمله صفر روزه[2] یا حمله روز-صفر باشد، یعنی یک آسیب‌پذیری در یک نرم‌افزار کاربردی که تا پیش از آن ناشناخته بوده است، بهره‌برداری می‌کند و توسعه‌دهندگان برای رفع آسیب‌پذیری صفر روز فرصت داشته‌اند. اما چنانچه بهره کشی از آسیب‌پذیری قبل از افشا شدن آسیب‌پذیری باشد حمله روز منفی و چنانچه بعد از آن باشد، حمله روز مثبت نامیده می‌شود.

برای نشان دادن شدت آسیب‌پذیری‌های امنیتی در بسیاری از پژوهش‌ها، از معیار CVSS استفاده می‌شود که یک استاندارد صنعت و سازمان‌ها می‌باشد. بانک اطلاعاتی آسیب‌پذیری ملی (NVD[3]) نیز شامل اطلاعات آسیب‌پذیری‌ها با بردار اندازه CVSS می‌باشد. در واقع چنانچه مقدار CVSS برای یک آسیب‌پذیری در محدوده [۷.۰و۱۰] باشد، از نظر شدت خطرناک بودن آسیب‌پذیری، خطر جدی محسوب می‌شود و اگر در بانک اطلاعاتی NVD در محدوده [۳.۹و۰.۰] باشد، از نظر شدت خطرناک بودن آسیب‌پذیری، خطر کم محسوب می‌شود.

کلید این مجموعه در بانک اطلاعاتی، CVE ID می‌باشد و عناصر دیگر در CVSS، محدوده حمله آسیب‌پذیری (اعم از سرویس از راه دور یا مشترک محلی یا از راه دور)، نتایج (در دسترس‌پذیری، یکپارچگی، محرمانیت) و غیره می‌باشد. این معیارها، اطلاعات پایه‌ای و مهم را برای تحلیل امنیتی خودکار ایجاد می‌نمایند و تلاش می‌کنند تا معیاری را ایجاد نمایند تا نشان دهد که چقدر آسیب‌پذیری در مقایسه با سایر آسیب‌پذیری‌ها مهم می‌باشد و CVSS نه تنها یک معیار عددی می‌باشد، بلکه یک معیار اندازه‌گیری در توصیف جنبه‌های مختلف آسیب‌پذیری می‌باشد و از سه گروه اصلی تشکیل شده است:

[1] Attack
[2] Zero-day attack
[3] Nvd.nist.gov

۱) معیارهای ذاتی و اصلی یک آسیب‌پذیری که مستقل از زمان و محیط بوده و زیر مجموعه آن، بردار دسترسی، پیچیدگی دسترسی، تصدیق هویت، تاثیر محرمانگی، تاثیر یکپارچگی و تاثیر در دسترس پذیری می‌باشد.

۲) معیارهای زمانی که خصوصیات آسیب‌پذیری را نشان می‌دهد و در طول زمان تغییر می‌یابند (نه با محیط کاربر) و شامل قابلیت سوء استفاده، سطح بازسازی و اطمینان گزارشی می‌باشد.

۳) معیار محیطی خصوصیات آسیب‌پذیری مرتبط با محیط کاربر در گروه معیار محیطی ذخیره می‌شود که شامل سرباز موازی، توزیع هدف، نیازمندی امنیتی می‌باشد. این معیارها در [۲] برای اولویت‌بندی در ماهیت ریسک، استفاده شده‌اند. با این وجود، معیارها به خودی خود می‌توانند بدون در نظر گرفتن تعاملات امنیتی در یک محیط سرمایه گذاری فقط اطلاعات محدودی را در اختیار قرار دهند.

این کتاب شامل ۳ فصل می‌باشد که برای ترجمه اصلاحات متن کتاب، از ترجمه انجمن رمز استفاده شده است و بخش عمده آن بر اساس استانداردهای OWASP تهیه شده و برای درک بهتر مفاهیم مرتبط با آن، بیشتر از مثال‌ها و توضیحات استفاده شده است.OWASP سازمانی بین‌المللی می‌باشد که در راستای ایمن‌سازی طراحی، پیاده‌سازی، توسعه و تست پروژه‌های نرم‌افزاری فعالیت می‌کند و استانداردهای مختلفی انتشار داده است. در این کتاب در فصل اول، به مقدمات و مفاهیم امنیتی، در فصل دوم به مطرح‌ترین ریسک‌های سازمان‌ها و چگونگی پیشگیری از این خطرات در سال‌های اخیر پرداخته می‌شود و در نهایت، فصل سوم به استاندارد مطرح بررسی امنیت نرم‌افزار می‌پردازد.