بسم الله الرحمن الرحیم

مقدمه‌ای بر آزمون نفوذپذیری و رایانش امن

(ابزار کالی)

تألیف و گردآوری:

پیام محمودی نصر

(عضو هیأت علمی دانشگاه مازندران)

محمد رجبی نسب

انتشارات دانشگاه مازندران

۴۴۴

سرشناسه	: محمودی نصر، پیام-۱۳۵۰
عنوان و نام پدیدآور	: مقدمه‌ای بر آزمون نفوذپذیری و رایانش امن (ابزار کالی)/ تالیف و گردآوری پیام محمودی‌نصر، محمد رجبی‌نسب؛ ویراستار ادبی سیدصادق بردبار
مشخصات نشر	: بابلسر: دانشگاه مازندران، ۱۳۹۹.
مشخصات ظاهری	: ۲۳۳ ص.
فروست	: انتشارات دانشگاه مازندران؛ ۴۴۴.
شابک	: ۹۷۸-۶۲۲-۶۵۰۶-۲۹-۸
وضعیت فهرست نویسی	: فیپا
یادداشت	: کتابنامه : ص. [۲۱۹].
موضوع	: کامپیوترها -- ایمنی اطلاعات -- راهنمای آموزشی (عالی)
موضوع	: Computer security-- Study and teaching (Higher)
موضوع	: شبکه‌های کامپیوتری -- تدابیر امنیتی -- راهنمای آموزشی (عالی)
موضوع	: Computer networks -- Security measures -- Study and teaching (Higher)
موضوع	: داده‌پردازی -- پردازش توزیع شده -- راهنمای آموزشی (عالی)
موضوع	: Electronic data processing -- Distributed processing-- Study and teaching (Higher)
شناسه افزوده	: رجبی نسب، محمد، ۱۳۷۶-
شناسه افزوده	: دانشگاه مازندران، انتشارات.
شناسه افزوده	: University of Mazandaran, Publishers
رده بندی کنگره	: QA۷۶/۹
رده بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۸۴۱۳۵۹۶

- عنوان : مقدمه‌ای بر آزمون نفوذپذیری و رایانش امن (ابزارکالی)
- تألیف و گردآوری : دکتر پیام محمودی نصر، محمد رجبی نسب
- ویراستار ادبی : سیدصادق بردبار
- ناشر : دانشگاه مازندران
- تاریخ انتشار : ۱۳۹۹
- نوبت چاپ : اول
- محل انتشار : بابلسر
- تعداد صفحات : ۲۳۳
- شمارگان : ۲۵۰ نسخه
- قیمت : ۱.۰۵۰.۰۰۰ ریال
- حروفچینی و صفحه آرایی : فاطمه ابراهیمی
- لیتوگرافی، چاپ و صحافی : انتشارات؛ صحافی کتیبه

بابلسر، خیابان پاسداران، دانشگاه مازندران، حوزه معاونت پژوهش

شابک: ۹۷۸-۶۲۲-۶۵۰۶-۲۹-۸

ISBN: 978-622-6506-29-8

پیشگفتار

پس از بیان مطالب نظری در درس رایانش امن، جهت مواجهه دانشجویان با آزمایش ها و مثال‌های عملی در این حوزه نیازی مبرم حس می‌شود. با توجه به فقدان کتابی جامع و مناسب در حوزه‌ی امنیت شبکه و رایانش امن که با یک رویکرد عملی به بیان موارد امنیتی مختلف بپردازد، ایده ی تالیف این کتاب به وجود آمد و پس از ماه ها تلاش، ثمره ی آن در قالب کتابی که در دستان شماست، گردآوری شده است.

این کتاب با بیان مطالب عملی، جنبه های جذاب رایانش امن را برای دانشجویان و علاقه مندان فراهم کرده و درک آنها را نسبت به مطالبی که به صورت نظری در درس رایانش امن مطرح شده، افزایش می‌دهد. این کتاب همچنین می‌تواند به عنوان یک کتاب کمک آموزشی در درس رایانش امن مورد استفاده دانشجویان کارشناسی، کارشناسی ارشد و همچنین علاقه مندان این حوزه قرار گیرد.

لازم به ذکر است که این کتاب قرار نیست به‌عنوان مرجعی برای درس رایانش امن مورد استفاده قرار بگیرد، بلکه تنها به عنوان یک کتاب جانبی و کمک آموزشی، دانشجویان را به صورت عملی با مباحث و ابزارهای مختلف رایانش امن آشنا کرده و مفاهیم ارزیابی امنیتی و تست نفوذ را به دانشجویان آموزش می‌دهد.

شالوده ی کتابی که در دست دارید، به شرح زیر است :

در فصل اول، کتاب به بیان مقدمه ای در رابطه با امنیت و اهمیت و جایگاه آن در زندگی امروز پرداخته شده است و اصطلاحات و مبانی مختلف امنیتی شرح داده شده‌اند.

در فصل دوم ،کتاب در مورد توپولوژی امن شبکه و اهمیت نحوه‌ی قرارگیری اجزای مختلف در شبکه‌ی جهت برقراری امنیت بحث شده است.

در فصل سوم، از کتاب به بیان نحوه‌ی جستجوی اتوماتیک آسیب‌پذیری‌های امنیتی پرداخته شده و ابزاری در این زمینه معرفی و آموزش داده شده است.

در فصل چهارم از کتاب، نحوه‌ی جستجو و جمع آوری اطلاعات در مورد درگاه[1] های یک رایانه‌یا کارپذیر[2] در شبکه مورد بررسی قرار گرفته است و ابزاری جهت انجام هرچه بهتر این عملیات معرفی و آموزش داده شده است.

در فصل پنجم کتاب، ابزار جامع و کاربردی Burp مورد بررسی قرار گرفته و اجزای مختلف آن شرح و آموزش داده شده‌اند.

در فصل ششم کتاب، در رابطه با آسیب‌پذیری معروف تزریق SQL بحث شده است و با ذکر مثال، ابعاد مختلف این آسیب‌پذیری و انواع آن بررسی شده‌اند. در ادامه این فصل، روش‌های مقابله با این آسیب‌پذیری و پیش گیری از بروز آن مورد بحث قرار گرفته است و در پایان، ابزاری جهت استفاده از این آسیب‌پذیری و استخراج اطلاعات مختلف معرفی و آموزش داده شده است.

در فصل هفتم از کتاب، آسیب‌پذیری معروف تزریق دستور مورد بررسی قرار گرفته است و مانند فصل قبل، با ذکر مثال ابعاد مختلف این آسیب‌پذیری مورد بحث واقع شده است. در ادامه، روش‌های مقابله با این آسیب‌پذیری و پیش گیری از وقوع آن بررسی شده‌اند و در پایان، ابزاری جهت استفاده هرچه بهتر از این آسیب‌پذیری جهت استخراج اطلاعات و اخذ دسترسی به سیستم قربانی معرفی شده است.

در فصل هشتم از کتاب، آسیب‌پذیری XSS و انواع آن مورد بررسی واقع شده است و نحوه استفاده از انواع این آسیب‌پذیری جهت انجام حمله شرح داده شده است.

در فصل نهم کتاب، در مورد آسیب‌پذیری سرریز بافر بحث شده است و انواع مختلف این آسیب‌پذیری در قالب مثال‌های متنوع بررسی شده‌اند.

در فصل دهم از کتاب، در مورد شکستن کلمات عبور مختلف بحث شده است و روش‌ها و ابزار مختلفی جهت انجام این عملیات در شرایط مختلف، معرفی و آموزش داده شده‌اند.

---

[1] Port

[2] Server

در فصل یازدهم و پایانی این کتاب نیز در مورد مهندسی اجتماعی بحث شده است و همچنین ابزاری جهت انجام عملیات مهندسی اجتماعی معرفی و آموزش داده شده است.

این کتاب همچنین شامل سه پیوست می‌باشد. در پیوست اول، نصب سیستم عامل Kali که محیط اصلی ابزارهای معرفی شده در این کتاب به شمار می‌آید آموزش داده شده است. در پیوست دوم، در رابطه با امن سازی مقدماتی یک کارپذیر لینوکسی به اختصار بحث شده است و در پیوست سوم و پایانی کتاب به معرفی محیط های تمرینی مختلف جهت تمرین هرچه بیشتر موارد آموزش داده شده در کتاب پرداخته شده است.

لازم به ذکر است که هدف این کتاب، آموزش به علاقه‌مندان حوزه‌ی امنیت و رایانش امن بوده و به منظور ارائه‌ی دانش جهت انجام اقدامات خراب‌کارانه، تألیف نگردیده است. بدیهی است که نویسندگان اثر هیچ گونه مسئولیتی در قبال استفاده نادرست از موارد آموزش داده شده در این کتاب نداشته و هرگونه عواقب ناشی از استفاده نادرست، برعهده ی شخص خاطی است.

امید است تا این کتاب، مورد توجه خوانندگان قرار گیرد و با جبران بخشی از فقدان مطالب علمی در زمینه‌ی عملیاتی رایانش امن، باعث ارتقای سطح علمی و مهارتی خوانندگان و علاقه‌مندان به حوزه‌ی امنیت و رایانش امن باشد.

فهرست مطالب

عنوان — صفحه

فصل پنجم: کار با ابزار Burp

فصل ششم: تزریق SQL

فصل هفتم: تزریق دستور

فصل هشتم: حملات XSS

فصل نهم: حملات سرریز بافر

فصل دهم: شکستن کلمات عبور

فصل یازدهم: مهندسی اجتماعی