

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

مقدمه ای بر آزمون نفوذپذیری و رایانش امن

www.ketab.ir
(ابزار کالی)

تألیف و گردآوری:

پیام محمودی نصر

(عضو هیأت علمی دانشگاه مازندران)

محمد رجیبی نسب

انتشارات دانشگاه مازندران

۴۴۴

سرشناسه	محمودی نصر، پیام-۱۳۵۰
عنوان و نام پدیدآور	مقدمه‌ای بر آزمون نفوذپذیری و رایانش امن (ایزار کالی) / تألیف و گردآوری پیام محمودی نصر، محمد رجیب نسب؛ ویراستار ادبی سیدصادق بردبار
مشخصات نشر	پابلسر: دانشگاه مازندران، ۱۳۹۹.
مشخصات ظاهری	۲۳۳ ص.
فروست	انتشارات دانشگاه مازندران: ۴۴۴.
شابک	۹۷۸-۶۲۲-۶۵۰۶-۲۹-۸
وضعیت فهرست نویسی	فیبا
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	رجیب نسب، محمد، ۱۳۷۶-
شناسه افزوده	دانشگاه مازندران، انتشارات.
شناسه افزوده	University of Mazandaran, Publishers
رده بندی کنگره	۵۸۷.۶۹
رده بندی دیویی	۰۰۵/۸
شماره کتابشناسی ملی	۸۴۱۳۵۹۶

عنوان	مقدمه‌ای بر آزمون نفوذپذیری و رایانش امن (ایزار کالی)
تألیف و گردآوری	دکتر پیام محمودی نصر، محمد رجیب نسب
ویراستار ادبی	سیدصادق بردبار
ناشر	دانشگاه مازندران
تاریخ انتشار	۱۳۹۹
نوبت چاپ	اول
محل انتشار	پابلسر
تعداد صفحات	۲۳۳
شمارگان	۲۵۰ نسخه
قیمت	۱۰۵۰,۰۰۰ ریال
حروفچینی و صفحه آرایی	فاطمه ابراهیمی
لیتوگرافی، چاپ و صحافی	انتشارات: صحافی کتیه

«کلیه حقوق برای دانشگاه مازندران محفوظ است»

پابلسر: دبیران پابلسر، دانشگاه مازندران، حوزه معاونت پژوهش

ISBN: 978-622-6506-29-8

شابک: ۹۷۸-۶۲۲-۶۵۰۶-۲۹-۸

پیشگفتار

پس از بیان مطالب نظری در درس رایانش امن، جهت مواجهه دانشجویان با آزمایش ها و مثال های عملی در این حوزه نیازی مبرم حس می شود. با توجه به فقدان کتابی جامع و مناسب در حوزه ی 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 می دهد. این کتاب همچنین می تواند 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 فوراً نیست به عنوان 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 می دهد.

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 شده اند.

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

در فصل سوم، از کتاب به بیان نحوه ی جستجوی اتوماتیک آسیب پذیری های امنیتی پرداخته شده و ابزاری در این زمینه معرفی و آموزش داده شده است.

در فصل چهارم از کتاب، نحوه‌ی جستجو و جمع‌آوری اطلاعات در مورد درگاه^۱ های یک رایانه یا کارپذیر^۲ 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 پیش‌گیری 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 پیش‌گیری 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 کاربر لاینوکسی به اختصار بحث شده است و در پیوست سوم و پایانی کتاب به معرفی محیط‌های 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، برعهده‌ی 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 اشتکای سطح علمی و مهارتی خوانندگان و علاقه‌مندان به حوزه‌ی امنیت و رایانش امن باشد.

فصل اول: مفهوم امنیت

۱-۱- مقدمه.....	۱
۱-۲- آسیب پذیری.....	۳
۱-۳- آزمون نفوذپذیری.....	۵
۱-۴- سایر تهدیدهای امنیتی.....	۶
۱-۵- ابزارهای امنیتی.....	۷
۱-۶- طرح یک پرسش.....	۹
۱-۷- سخن پایانی.....	۹

فصل دوم: توپولوژی امن شبکه

۲-۱- مقدمه.....	۱۱
۲-۲- اهمیت موضوع.....	۱۱
۲-۳- مفاهیم کلی.....	۱۳
۲-۴- روش مسیریاب سرند یا Screening Router.....	۱۵
۲-۵- روش میزبان سرند یا Screening Host.....	۱۷
۲-۶- روش منطقه‌ی غیر نظامی یا DMZ.....	۲۰

فصل سوم: پویش آسیب پذیری های وب

۳-۱- مقدمه.....	۲۳
۳-۲- پویشگر امنیتی OWASP ZAP.....	۲۴

فصل چهارم: پویش درگاه ها

۴-۱- مقدمه.....	۳۹
-----------------	----

۴۰	۲-۴- مفاهیم کلی
۴۰	۳-۴- انواع پویس درگاه
۴۱	۴-۴- پویشگر ZENMAP

فصل پنجم: کار با ابزار Burp

۵۱	۱-۵- مقدمه
۵۲	۲-۵- شروع به کار با Burp Suite
۵۴	۳-۵- تنظیمات Proxy مرورگر برای استفاده از Burp
۵۵	۴-۵- استفاده از قابلیت Proxy ابزار Burp
۵۶	۵-۵- استفاده از قابلیت Repeater ابزار Burp
۵۷	۶-۵- استفاده از قابلیت Intruder ابزار Burp
۵۹	۷-۵- استفاده از قابلیت Spider ابزار Burp
۶۰	۸-۵- استفاده از قابلیت Decoder ابزار Burp

فصل ششم: تزریق SQL

۶۳	۱-۶- مقدمه
۶۴	۲-۶- تزریق SQL
۶۵	۳-۶- مثال‌هایی از تزریق SQL
۶۸	۴-۶- تکنیک‌های تشخیص آسیب‌پذیری تزریق SQL
۷۳	۵-۶- تشخیص نوع کاربرپذیر پایگاه‌داده
۷۵	۶-۶- استفاده از تزریق SQL
۸۳	۷-۶- مقابله با تزریق SQL
۸۷	۸-۶- دور زدن مکانیزم‌های امنیتی
۹۱	۹-۶- ابزار Sqlmap

فصل هفتم: تزریق دستور

۹۹	۱-۷- مقدمه
----	------------

۱۰۰	۷-۲- مثال‌هایی از تزریق دستور
۱۰۵	۷-۳- پوسته‌ی سیستم عامل
۱۰۵	۷-۴- کار با ابزار Metasploit
۱۱۱	۷-۵- استفاده از Meterpreter
۱۱۸	۷-۶- سایر پوسته‌ها

فصل هشتم: حملات XSS

۱۲۳	۸-۱- مقدمه
۱۲۴	۸-۲- انواع حملات XSS
۱۲۵	۸-۳- روش‌های انجام حملات XSS
۱۲۷	۸-۴- مثال‌هایی از حملات XSS
۱۳۴	۸-۵- محافظت در برابر حملات XSS

فصل نهم: حملات سرریز بافر

۱۳۵	۹-۱- مقدمه
۱۳۶	۹-۲- آسیب‌پذیری سرریز بافر
۱۳۷	۹-۳- راهکارهای عمومی جلوگیری از حملات سرریز بافر
۱۳۸	۹-۴- انواع حملات سرریز بافر و روش‌های محافظت در برابر آن‌ها

فصل دهم: شکستن کلمات عبور

۱۴۹	۱۰-۱- مقدمه
۱۵۰	۱۰-۲- حملات Brute-Force
۱۵۴	۱۰-۳- حملات Dictionary Attack
۱۵۵	۱۰-۴- ابزار Hydra
۱۵۷	۱۰-۵- ابزار Johnny
۱۶۰	۱۰-۶- ابزار Rainbowcrack
۱۶۱	۱۰-۷- ابزار Aircrack

فصل یازدهم: مهندسی اجتماعی

۱۱-۱- مقدمه..... ۱۶۷

۱۱-۲- مهندسی اجتماعی و ابزار SET..... ۱۶۸

پیوست یک: نصب سیستم عامل Kali..... ۱۷۷

پیوست دو: ایمن سازی عمومی کاربرپذیر لینوکسی..... ۲۱۰

پیوست سه: معرفی محیط های تمرینی..... ۲۱۵

منابع و مآخذ..... ۲۱۷

www.ketab.ir