

بنام ایزد یکتا

مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

انتشارات پندار پارس

فهرست

فصل اول: مروری کلی بر مفاهیم نفوذگری و امنیت	۱
امنیت	۲
سه گام تا ایمن سازی	۳
گام نخست: بررسی خطرات یا Threat Analysis	۴
گام دوّم: سیاست گذاری امنیتی یا Security Policy	۵
گام سوّم: مکانیزم‌های امنیتی یا Security Mechanisms	۵
بررسی امنیت شبکه لایه‌بندی شده با نگاه عملیاتی	۶
مفاهیم کلی در امنیت شبکه	۷
۱. منابع شبکه	۱۰
۲. حمله	۱۱
۳. تحلیل خطر	۱۱
۴. سیاست امنیتی	۱۲
۵. طرح امنیت شبکه	۱۲
۶. نواحی امنیتی	۱۳
اهداف امنیت	۱۴
اهمیت امنیت اطلاعات و ایمن سازی کامپیوترها	۱۵
مدل امنیت لایه‌بندی شده	۱۶
امنیت پیرامون	۱۷
امنیت شبکه	۱۹
امنیت میزبان	۲۲
امنیت برنامه کاربردی	۲۴
امنیت داده	۲۶
مدیریت خطر	۲۶
پوشش تمامی مقادیر امنیتی	۲۸
شناسایی تهدیدات	۱۹
منابع تهدیدات	۳۰
حوادث ناشی از تهدیدات	۳۰
حملات ناشی از تهدیدات	۳۲
داده‌ها و اطلاعات حساس در معرض تهدید	۳۵
حملات	۳۵

۵۳ حملات شناسایی
۵۴ حملات دستیابی
۵۴ حملات از کار انداختن سرویس‌ها
۵۴ حملات برپایه استراق سمع (Interception)
۵۴ حملات برپایه دستکاری اطلاعات (Modification)
۵۴ افزودن اطلاعات و جعل (Fabrication)
۵۵ حمله از نوع وقفه (Interruption)
۵۶ حملات برپایه تزریق کد دو مرحله‌ای
۵۶ دسته‌بندی تزریق کد دو مرحله‌ای
۵۷ محل‌های ذخیره سازی
۵۸ روش‌های کشف تزریق کد دو مرحله‌ای
۵۹ محافظت در برابر تزریق کد دو مرحله‌ای
۶۰ احتمال حمله
۶۰ اثرات این نوع حمله
۶۱ طبقه‌بندی کلی کدهای مُخرَب
۶۲ چه کسانی حملات را طرح ریزی می‌کنند؟
۶۲ هکر (Hacker)
۶۵ انگیزه‌های نفوذگری و حمله به شبکه
۶۷ نقاط نفوذ
۶۸ زیربنای شبکه
۶۸ برنامه‌های کاربردی مورد استفاده بر روی فضای اینترنت
۶۹ پروتکل‌های ارتباطات
۷۰ دفاع در مقابل تهدیدات
۷۰ ساختار یک دفاع
۷۱ امن سازی زیربنای شبکه
۷۱ بهره‌گیری از پروتکل‌های ارتباطی ایمن
۷۲ امن سازی سیستم‌ها
۷۳ امن سازی برنامه‌های کاربردی
۷۳ احراز هویت کاربر
۷۳ احراز هویت کارت هوشمند
۷۳ گواهینامه‌ها
۷۴ احراز هویت از نوع زیست‌سنجی (Biometric)

۷۴.....	فعال نمودن قابلیت بازبینی
۷۵.....	امنیت عملی و سازمانی
۷۵.....	محافظت از داده
۷۵.....	رشته‌ای از حفاظت
۷۶.....	روابط منابع انسانی و موضوعات پنهانی
۷۷.....	شاخه‌های امنیت - هزینه‌های تحمیلی نفوذ
۷۸.....	ایجاد یک استراتژی امنیت شبکه
۸۰.....	نکات اولیه در خصوص ایمن سازی اطلاعات و شبکه‌های کامپیوتری
۸۳.....	فصل دوم : حملات مبتنی بر شناسایی
۸۵.....	شناسایی مقدماتی
۸۵.....	بهره گیری از وب جهت جمع‌آوری اطلاعات و اخبار شبکه هدف
۸۶.....	جستجوی سندها با بهره گیری از مکانیزم آشغال گردی
۸۷.....	دفاع در مقابل جستجوی سندها براساس مکانیزم آشغال گردی
۸۸.....	حملات برپایه دسترسی مستقیم به شبکه هدف
۸۹.....	دفاع در مقابل حملات برپایه دسترسی مستقیم
۹۰.....	جستجو در سایتهای وب سازمان و یا مؤسسه هدف
۹۱.....	بهره گیری از اطلاعات پنهان شده در کدهای منبع صفحات HTML
۹۱.....	استفاده از موتورهای جستجو در اینترنت
۹۵.....	گروههای خبری Usenet
۹۵.....	مقابله با مکانیزم‌های مختلف شناسایی از طریق وب
۹۶.....	بهره گیری از بانک اطلاعاتی Whois در جهت شناسایی
۹۸.....	جمع‌آوری اطلاعات در خصوص نامهای حوزه با پسوند متداول
۱۰۳.....	بهره گیری از سایتهای وب جهت تحقیق در مورد آدرس IP
۱۰۴.....	مقابله با جمع‌آوری اطلاعات از طریق مکانیزم Whois
۱۰۵.....	بهره گیری از ابزارها جهت شناسایی مقدماتی شبکه هدف
۱۰۵.....	ابزار Sam Spade
۱۰۸.....	بهره گیری از ابزارهای شناسایی شبکه مبتنی بر وب
۱۱۰.....	نقشه برداری از شبکه هدف
۱۱۴.....	بهره گیری از نرم‌افزارهای معروف در نقشه برداری از شبکه
۱۱۵.....	جلوگیری از نقشه برداری شبکه
۱۱۶.....	انواع پوشش
۱۱۷.....	تعیین پورتهای باز روی سرور هدف

۱۲۲.....	بررسی مکانیزم‌های مختلف پویش پورت
۱۲۲.....	بررسی مکانیزم پویش مؤدبانه (Polite Scan)
۱۲۳.....	بررسی پویش مخفیانه TCP SYN Scan
۱۲۴.....	بررسی پویش به روش نقض اصول پروتکل
۱۲۵.....	بررسی پویش به روش TCP ACK Scan
۱۲۷.....	بررسی پویش به روش FTP Bounce Scan
۱۲۸.....	بررسی مکانیزم بهره‌گیری از بسته‌های UDP
۱۲۸.....	بررسی مکانیزم عمل Ping بدون بهره‌گیری از پروتکل ICMP
۱۲۹.....	شناسایی و بررسی برنامه‌های RPC
۱۳۰.....	بهره‌گیری از مکانیزم‌های ردّ گم کردن و پنهان ماندن
۱۳۱.....	بهره‌گیری از مکانیزم TCP Stack Fingerprinting جهت تعیین سیستم عامل ماشین هدف
۱۳۳.....	ایجاد یک زمانبندی صحیح جهت پویش پورتهای باز
۱۳۳.....	جستجو جهت یافتن دیوارهای آتش و مسیریابها
۱۳۴.....	آزمایش دیواره آتش و لیست‌های کنترل دسترسی
۱۳۷.....	فصل سوم: حملات مبتنی بر مکانیزم‌های رمزنگاری و کلمات عبور
۱۴۷.....	۱. کلیدهای محرمانه (Secret keys)
۱۴۷.....	۲. کلیدهای عمومی و اختصاصی (Public and Private keys)
۱۴۷.....	۳. کلیدهای اصلی و کلیدهای مشتق شده (Master keys and Derived keys)
۱۴۸.....	۴. کلیدهای رمزکننده کلید (Key-encrypting keys)
۱۴۸.....	۵. کلیدهای نشست (Session keys)
۱۴۹.....	شکستن کلید در الگوریتم‌های متقارن
۱۵۰.....	شکستن کلید در الگوریتم‌های نامتقارن
۱۵۱.....	آزمون جامع فضای کلید
۱۵۱.....	حمله مکملیت
۱۵۲.....	حمله از طریق ویژگی بسته بودن
۱۵۲.....	حمله‌ای که تنها برپایه متنهای رمز شده استوار است
۱۵۳.....	حمله‌ای که برپایه نمایان بودن متن اصلی استوار است
۱۵۳.....	حمله متن اصلی منتخب
۱۵۳.....	حمله تطبیقی متن اصلی منتخب
۱۵۴.....	ملزومات و توصیه‌هایی درخصوص طرح مؤثر نرم‌افزاری الگوریتم رمز
۱۵۵.....	کلمات عبور
۱۶۹.....	حفاظت کلمات عبور مستحکم:

۱۶۹.....	کنترل مستمر حسابهای کاربری:
۱۷۰.....	نگهداری و پشتیبانی از سیاست کلمه عبور:
۱۷۰.....	خط مشی برای کلمات عبور قوی
۱۷۱.....	آگاهی دادن به کاربران
۱۷۱.....	تنها آموزش کافی نیست
۱۷۱.....	اما یک کلمه عبور قوی چیست؟
۱۷۱.....	نرم افزارهای فیلترگذاری کلمات عبور
۱۷۵.....	فصل چهارم: حملات مبتنی بر کدهای مُخرَب
۱۷۹.....	سکتور بوت (Boot Sector)
۱۸۱.....	ویروسهای ماکرو (کلان دستور)
۱۸۲.....	ویروسهای انگلی (File infecting viruses)
۱۸۳.....	ویروسهای مخفی
۱۸۳.....	ویروسهای چندبخشی
۱۸۴.....	ویروسهای مبتنی بر پست الکترونیکی
۱۸۵.....	Hoaxها چیستند؟
۱۸۸.....	ویروسهای دوزیست
۱۸۸.....	ویروسهای تلفن همراه
۲۰۷.....	بررسی علائم وجود و عدم وجود ویروس در سیستمهای کامپیوتری
۲۰۹.....	تصورات غلط
۲۱۰.....	بررسی تکنیکهای جدید حمله ویروسها
۲۱۸.....	بررسی عملکرد ویروس I LOVE YOU
۲۲۰.....	بررسی عملکرد ویروس Melissa
۲۲۱.....	تأثیرات برخی از اینگونه ویروسها
۲۲۱.....	سرقت اطلاعات
۲۲۲.....	ایجاد - تغییر - حذف فایلها
۲۲۲.....	کاهش کارایی سیستم
۲۲۲.....	ایجاد یک Backdoor
۲۲۲.....	ارسال حجم بالایی از ایمیلهای ناخواسته (SPAM)
۲۲۲.....	راه حل برخورد با اینگونه ویروسها
۲۲۵.....	تعریف سیاستهای امنیتی برای سازمان
۲۲۵.....	کنترل و محافظت تمام نقاط ورودی در سازمان
۲۲۵.....	پروژ کردن نرم افزارهای ضدویروس

۲۲۵.....	استفاده کاربران از نرم‌افزارهای ضدویروس.....
۲۲۶.....	پروژه رسانی کلیه نرم‌افزارهای مورد استفاده.....
۲۲۶.....	تهیه بایگانی بطور دائم و مستمر.....
۲۲۶.....	سازمان خود را مشترک مراکز اطلاع رسانی کنید.....
۲۲۶.....	آموزش کاربران سازمان.....
۲۳۴.....	وضعیت آینده.....
۲۳۵.....	محدودیت راه‌های واکنشی.....
۲۳۶.....	وظایف مدیران سیستم.....
۲۳۷.....	اتخاذ روشهای امنیتی.....
۲۳۷.....	بهنگام نمودن دانش و اطلاعات.....
۲۳۷.....	آموزش کاربرانی که از سیستمها استفاده می‌نمایند.....
۲۳۸.....	وظایف ارائه دهندگان تکنولوژی.....
۲۳۸.....	نرم‌افزار ضدویروس / مقاوم در مقابل ویروس.....
۲۳۹.....	کاهش خطای پیاده سازی.....
۲۳۹.....	پیکربندی پیش فرض با امنیت بالا.....
۲۴۰.....	وظایف تصمیم گیرندگان.....
۲۴۰.....	تحقیق در رابطه با تضمین ایمن سازی اطلاعات.....
۲۴۱.....	استفاده از متخصصین فنی بیشتر.....
۲۴۱.....	ارائه آموزش و آگاهی لازم به کاربران اینترنت.....
۲۴۴.....	توابع استاندارد اسبهای تروا.....
۲۴۴.....	طبقه‌بندی اسبهای تروا.....
۲۴۴.....	Backdoor Trojans (اسبهای تروای ایجاد کننده در پشتی):.....
۲۴۵.....	General Trojans (اسبهای تروای عمومی):.....
۲۴۶.....	PSW Trojans (اسبهای تروای ارسال کننده رمز):.....
۲۴۷.....	Destructive Trojans.....
۲۴۷.....	Trojan Clickers.....
۲۴۷.....	Trojan Downloaders.....
۲۴۷.....	Trojan Droppers.....
۲۴۸.....	Denial of Service (DoS) Attack Trojans.....
۲۴۹.....	Trojan Proxies.....
۲۴۹.....	Trojan Spies.....
۲۴۹.....	FTP Trojans.....

۲۵۰ Trojan Notifiers
۲۵۰ Security Software Disablers Trojans
۲۵۰ ArcBombs
۲۵۵ پوشه شروع خودکار (StartUp)
۲۵۵ فایل Win.ini
۲۵۵ فایل System.ini
۲۵۶ فایل Explorer.exe
۲۵۶ فایل Wininit.ini
۲۵۶ فایل Winstart.bat
۲۵۶ فایل Autoexec.bat
۲۵۷ فایل Config.sys
۲۶۲ نرم افزار جاسوسی خانگی (Domestic Spyware)
۲۶۲ نرم افزار جاسوسی تجاری (Commercial Spyware)
۲۶۳ ثبت کنندگان نشانی های وب و صفحات نمایش
۲۶۳ ثبت کنندگان چت و نامه الکترونیکی
۲۶۳ ثبت کنندگان کلید و کلمات عبور
۲۶۴ حشرات وبی
۲۶۴ مرورگر ربایان!
۲۶۴ مودم ربایان
۲۶۴ ربایندگان کامپیوترهای شخصی
۲۷۱ تغییر در سطح دسترسی محلی
۲۷۱ اجرای فرمانهای منفرد از راه دور
۲۷۱ دسترسی به یک سطر فرمان از سیستم هدف از راه دور
۲۷۱ دسترسی از راه دور به ماشین هدف از طریق برنامه های GUI
۲۷۷ پویشگرها
۲۷۸ Checksummerها
۲۷۸ نرم افزارهای کاشف (Heuristic)
۲۸۷ (Network Address Translation) NAT
۲۸۸ فیلترینگ پورتها
۲۸۹ ناحیه غیرنظامی یا DMZ
۲۹۰ ارسال پورتها
۲۹۴ اجرای یک برنامه ضد ویروس و پویش کامل کامپیوتر:

۲۹۴.....	اجرای یک برنامه معتبر که مختص حذف جاسوس افزار طراحی شده است:
۲۹۷.....	فصل پنجم: حملات مبتنی بر استراق سمع.....
۲۹۸.....	مفهوم شنود یا استراق سمع
۳۰۱.....	استراق سمع از هاب
۳۰۲.....	استراق سمع از سویچ
۳۰۳.....	بهره گیری از مکانیزم انتشاری به منظور استراق سمع از شبکه
۳۰۳.....	استراق سمع مکالمات مخابراتی
۳۰۵.....	شنود از طریق تلفنهای معمولی بی سیم
۳۰۸.....	استراق سمع و شنود از طریق تلفنهای ثابت
۳۰۸.....	شنود مکالمات تلفنی در شبکه‌های تلفن همراه
۳۱۰.....	روشهای خنثی سازی اقدامات عوامل غیرقانونی
۳۱۱.....	ابزارهای Sniffer مشهور جهت استراق سمع از شبکه
۳۲۰.....	مقابله با حملات مبتنی بر استراق سمع
۳۲۳.....	فصل ششم: حملات مبتنی بر وب و سرویس پست الکترونیکی.....
۳۲۴.....	مفهوم تور جهان گستر
۳۲۶.....	مفهوم URL.....
۳۲۸.....	مقدمه‌ای بر سیستم وب
۳۲۹.....	برنامه سمت سرویس دهنده وب
۳۳۱.....	پروتکل انتقال ابر متن (HTTP)
۳۳۷.....	اطلاعات اساسی و کلیدی در مورد URL
۳۳۷.....	جستجو در ساختمان URL.....
۳۳۸.....	Server
۳۳۸.....	Path/to/resource
۳۳۸.....	Parameters
۳۴۰.....	رمزنگاری URL
۳۴۱.....	Meta-Characters
۳۴۲.....	مشخص کردن کاراکترهای خاص در یک رشته URL.....
۳۴۳.....	سوء استفاده از روزهای URL
۳۴۳.....	آسیب پذیریهایی Unicode
۳۴۵.....	آسیب پذیری رمزگشایی مجدد و یا رمزگشایی زاید
۳۴۵.....	امنیت در سرورهای وب
۳۴۷.....	فرض‌های امنیتی سرور وب

۳۴۸.....	روشهای پنهان سازی سرورهای وب
۳۴۸.....	سرآیند سرورها همه چیز را می گویند
۳۴۹.....	استفاده از پسوند فایلها برای تشخیص سیستم عامل سرور وب
۳۴۹.....	زبان ASP جهت تشخیص سیستم عامل سرور وب هدف
۳۵۰.....	استفاده از مکانیزم WebDAV جهت تشخیص سیستم عامل سرور وب هدف
۳۵۰.....	بهره گیری از سرآیندهای مختلف جهت تشخیص سیستم عامل سرور وب هدف
۳۵۰.....	کسب اطلاعات مفید از احراز هویت ویندوز توسط نفوذگر
۳۵۰.....	شناسایی سرور وب هدف توسط پیامهای پیش فرض
۳۵۱.....	بهره گیری از سرویسها جهت شناسایی سرور وب هدف
۳۵۱.....	استفاده از ورودیهای غیرمجاز جهت کسب اطلاعات از سرور وب هدف
۳۵۱.....	استفاده از پشتهها جهت کشف نوع سیستم عامل سرور وب هدف
۳۵۲.....	بهره گیری از سایت Netcraft جهت کسب اطلاعات از سرور وب هدف
۳۵۲.....	شناسایی سیستم عامل سرور وب هدف توسط پیش فرضهای TCP/IP
۳۵۲.....	برنامههای کاربردی وب
۳۵۵.....	برنامههای CGI
۳۵۸.....	حملات مبتنی بر URL و سرورهای معروف وب (Apache, IIS)
۳۵۸.....	حمله علیه سرور وب IIS
۳۵۸.....	حمله علیه مؤلفههای IIS
۳۶۰.....	حمله علیه خود IIS
۳۶۹.....	پیمایش پوشه IIS
۳۷۱.....	دریافت فایلها با استفاده سرویسهای SMB, FTP, TFTP
۳۷۲.....	استفاده از دستور echo>file جهت ایجاد کردن فایلها
۳۷۲.....	روش مقابله با آسیب پذیریهایی موجود در پیمایش پوشه IIS
۳۷۲.....	وصلههای امنیتی جدید را نصب کنید
۳۷۴.....	پوشههای سایت وب خود را در درایوی به جز درایو سیستم نصب کنید
۳۷۴.....	با استفاده از ابزار URLScan با رمزگشایی URLها درخواستها را نرمال کنید
۳۷۴.....	هر کدام از ابزارهای قوی را حذف، تغییر نام، جابجا و یا محدود نمایید
۳۷۶.....	حمله علیه سرور وب آپاچی
۳۷۶.....	لیست کردن پوشهها بوسیله کاراکترهای اسلش (Slash) طولانی
۳۷۷.....	روش مقابله با لیست کردن پوشهها بوسیله Slashهای طولانی
۳۷۸.....	روش مقابله با Multiview
۳۷۸.....	تزریق ماژول mod_auth_sq

۳۷۹.....	نحوه تشخیص آسیب پذیری‌های موجود در سرویس دهنده وب آپاچی
۳۷۹.....	روشهای کلی حفاظت از سرویس دهنده وب آپاچی
۳۸۲.....	حملات بر علیه برنامه‌های کاربردی تحت وب
۳۸۴.....	منظور از حفره‌ها و اشکالات
۳۸۵.....	حملات از نوع کسب آگاهی و افشاء گری (Disclosure)
۳۸۵.....	انواع حملات کسب آگاهی و افشاء گری
۳۸۶.....	حملات کسب آگاهی و افشاء گری چگونه صورت می‌گیرند؟
۳۸۷.....	چگونه سرور خود را در برابر اینگونه حملات ایمن کنیم؟
۳۸۸.....	حملات در معرض گذاری و افشاء آشکار (Exposure)
۳۸۸.....	حملات در معرض گذاری یا Exposure جهت دریافت صفحات پویا
۳۸۹.....	حملات در معرض گذاری و افشاء آشکار چگونه صورت می‌گیرند؟
۳۸۹.....	یک نفوذگر چگونه با استفاده از حملات در معرض گذاری حمله می‌کند؟
۳۹۰.....	چگونه سایت خود را از این دسته حملات حفظ کنیم؟
۳۹۱.....	حمله تزریق اسکریپت
۳۹۳.....	حمله Cross-Site-Scripting (CSS/XSS)
۳۹۶.....	به چه دلیل یک سایت نسبت به حملات XSS آسیب پذیر است؟
۴۰۴.....	مقابله با حملات Cross-Site-Scripting (XSS/CSS)
۴۰۶.....	حملات مبتنی بر حفره‌های موجود در CGI
۴۰۶.....	آسیب پذیری آزمون CGI
۴۰۶.....	عملکرد سیستم IDS در سطح کاربرد و روشهای فرار از آن
۴۰۷.....	حمله بر علیه IDS جهت کشف برنامه‌های CGI آسیب پذیر
۴۰۹.....	بهره گیری از مکانیزمهای Whisker جهت فریب دادن IDS
۴۱۱.....	حملات مبتنی بر دستکاری فیلدهای Forumها
۴۱۳.....	مشخصه نشست (Session ID)
۴۱۵.....	منظور از مدیریت وضعیتها ؛ Cookies
۴۱۶.....	کوکی چیست؟
۴۱۷.....	انواع کوکی
۴۱۸.....	نحوه تشخیص وجود کوکیهای ماندگار بر روی سیستم
۴۱۹.....	موارد استفاده کوکیها
۴۲۱.....	مزایا و معایب کوکیها از دید کاربران اینترنت
۴۲۱.....	بررسی مسائل امنیتی مربوط به کوکیها
۴۲۳.....	کار با کوکیها

۴۲۳.....	حملات بر علیه مشخصه نشست یا Session ID
۴۲۴.....	افزایش افقی اختیارات
۴۲۴.....	افزایش عمودی اختیارات
۴۲۴.....	یافتن حامل حالت
۴۲۵.....	رمزگشایی اطلاعات حالت
۴۲۵.....	استفاده مجدد از اطلاعات حالت
۴۲۵.....	تغییر اطلاعات حالت
۴۲۶.....	مقابله با حملات علیه مشخصه نشست
۴۲۸.....	حملات بر علیه کوکیها
۴۳۰.....	حمله به کوکیهای موقت
۴۳۳.....	حملات Cookie Snarfing
۴۳۴.....	حملات Cookie Munching
۴۳۵.....	درو کردن حسابهای کاربری در وب (Account Harvesting)
۴۳۷.....	روش مقابله با دروی حسابهای کاربران وب
۴۳۷.....	امنیت نامه‌های الکترونیکی
۴۵۳.....	پروتکل‌های مرتبط با نامه‌های الکترونیکی
۴۵۴.....	منظور از پورت ۲۵
۴۵۶.....	ارتباط با پورت ۲۵
۴۶۰.....	ارتباط با پورت ۱۱۰
۴۶۲.....	روشهای استفاده شده جهت حمله به سیستم پست الکترونیکی
۴۶۲.....	ضمیمه‌هایی با محتوای آسیب رسان
۴۶۳.....	نامه‌های راه انداز اکسپلویتهای شناخته شده
۴۶۵.....	فصل هفتم: حملات مبتنی بر جعل هویت و ربودن نشستها
۴۶۶.....	حمله از نوع تعقیب نشستهای وب (Web Session Tracking)
۴۶۸.....	ارتباط ربایی
۴۶۸.....	ارتباط ربایی نوع اول
۴۷۱.....	ارتباط ربایی نوع دوم
۴۷۱.....	سرقت هویت (Phishing)
۴۷۲.....	Phishing چیست؟
۴۷۳.....	Phishing چگونه کار می‌کند؟
۴۷۴.....	روشهایی جهت محافظت در مقابل حملات Phishing
۴۷۷.....	اثبات هویت فرستنده نامه الکترونیکی و حفاظت از آن (DomainKeys)

۴۷۸.....	استانداردسازی مکانیزم DomainKeys
۴۷۹.....	نحوه کار مکانیزم DomainKeys
۴۸۰.....	حملات Pharming
۴۸۲.....	روشهای مقابله با حملات Pharming
۴۸۵.....	حملات مبتنی بر جعل آدرسها
۴۸۶.....	انواع تکنیکهای جعل آدرس
۴۹۰.....	حمله شماره سریال TCP/IP
۴۹۰.....	فریب ماشینها با آدرسهای IP جعلی و دروغین (IP Spoofing)
۴۹۱.....	فریب ساده از طریق آدرسهای اشتباه IP
۴۹۲.....	فریب دادن یک ماشین با آدرسهای IP دروغین در محیط یونیکس
۴۹۳.....	فریب یک ماشین با آدرسهای IP از طریق تکنیک Source Routing
۴۹۶.....	منظور از عبارت HTTP:arrow چیست؟
۴۹۸.....	Referer URLها برای امنیت به کار می‌روند
۴۹۸.....	عبور کردن از روش امنیتی Referer
۴۹۹.....	جعل کردن وب
۵۰۰.....	اثرات جعل کردن وب
۵۰۰.....	جعل کردن کل وب
۵۰۱.....	بازبینی فرمها و ارتباطات ایمن
۵۰۱.....	آغاز حمله جعل کردن وب
۵۰۲.....	مقابله با انواع فریبکاری متکی به آدرسهای IP جعلی
۵۰۴.....	راه‌حلهایی جهت جلوگیری از حمله وب‌های جعلی
۵۰۵.....	روشهای مقابله در برابر جعل آدرسها
۵۰۶.....	بهره‌گیری از روش ورودی ثابت برای شبکه‌های کوچک
۵۰۷.....	بهره‌گیری از روش امنیت پورت برای شبکه‌های بزرگ
۵۰۷.....	بهره‌گیری از روش آشکارسازی برای اکثر شبکه‌ها
۵۰۹.....	فصل هشتم: حملات مبتنی بر پایگاه‌های داده
۵۱۰.....	پایگاه داده
۵۱۲.....	پرس و جو یا جستجو چیست؟
۵۱۲.....	پایگاه داده SQL Server
۵۱۳.....	امنیت در پایگاه‌های داده
۵۱۵.....	معماری امن شبکه با نگاه به پایگاه داده
۵۱۵.....	۱. در نظر گرفتن سخت‌افزار جداگانه جهت سرور وب و سرور پایگاه داده

۵۱۶.....	۲. قرار ندادن پایگاه داده در محیط DMZ.....
۵۱۹.....	۳. رمزنگاری اطلاعات مابین سرور وب و سرور پایگاه داده.....
۵۲۰.....	۴. عدم استفاده از هاب (Hub) و بهره‌گیری از سویچ (Switch).....
۵۲۰.....	ارائه امن اطلاعات.....
۵۲۱.....	تولید اطلاعات به صورت ایستا یا استاتیک و مسائل امنیتی آن.....
۵۲۱.....	تولید اطلاعات به صورت پویا یا دینامیک.....
۵۲۲.....	سطح امنیتی پایگاه داده.....
۵۲۳.....	پایگاه داده وظایف و نقش‌ها.....
۵۲۳.....	پایگاه داده MySQL.....
۵۲۳.....	حمله به برنامه‌های کاربردی وب به روش SQL Injection.....
۵۲۳.....	(SQL Piggybacking).....
۵۲۴.....	تزریق SQL در ASP براساس پایگاه داده SQL Server.....
۵۲۸.....	روش تشخیص آسیب‌پذیری تزریق SQL در سایتها و نحوه بهره‌برداری از آن.....
۵۳۲.....	بدست آوردن نام جدول و ستونهای موجود در پایگاه داده SQL.....
۵۳۳.....	استفاده از حمله Union در SQL جهت کسب اطلاعات بیشتر از سرور.....
۵۳۵.....	بدست آوردن نام کاربری و کلمه عبور از جداول در پایگاه داده SQL.....
۵۳۸.....	تزریق SQL در PHP براساس پایگاه داده MySQL.....
۵۴۰.....	تکنیک بهره‌گیری از عبارات و علامات.....
۵۴۰.....	تکنیک استفاده از علامت ?.....
۵۴۱.....	تکنیک استفاده از علامت #.....
۵۴۱.....	نحوه بهره‌گیری مهاجم از این عبارات و علامات.....
۵۴۲.....	روشهای مقابله در برابر حملات تزریق SQL.....
۵۴۳.....	روشهای کلی جهت مقابله در برابر حملات تزریق SQL.....
۵۴۴.....	معتبرسازی ورودی‌ها.....
۵۴۹.....	فصل نهم: حملات سرریزی بافر.....
۵۵۰.....	پشته چیست؟.....
۵۵۵.....	بافر چیست؟.....
۵۵۶.....	Heap چیست؟.....
۵۵۶.....	سرریزی بافر چیست؟.....
۵۵۶.....	انواع سرریزی بافر.....
۵۵۷.....	پیدا کردن نقاط آسیب‌پذیر.....
۵۵۸.....	EBX=00F41130.....

۵۵۸.....	EAX=00F7FCC8
۵۵۹.....	سازماندهی و آرایش بافر پیش از سرریز شدن
۵۶۰.....	مقابله ابتدایی با حمله به پشته از طریق سیستم IDS
۵۶۰.....	مقابله با حملات مبتنی بر سرریزی پشته یا بافر
۵۶۱.....	مقابله در سطح مسئول سیستم و گروه امنیتی
۵۶۲.....	مقابله با سرریز شدن پشته در سطح برنامه نویسی
۵۶۳.....	منظور از UnderFlow در بافر
	فصل دهم: حملات مبتنی بر بهره برداری از نرم افزارها، سرویس‌ها، ضعف‌های پیکربندی،
۵۶۵.....	آسیب پذیری‌ها و پورت‌ها
۵۶۷.....	حملات مبتنی بر سرویسها
۵۶۷.....	پیچیدگی سرویس
۵۶۸.....	سوء استفاده از سرویس
۵۶۸.....	اطلاعات ارایه شده توسط سرویس
۵۶۸.....	میزان دیالوگ با سرویس گیر
۵۶۹.....	قابلیت پیکربندی سرویس
۵۶۹.....	نوع مکانیزم احراز هویت استفاده شده توسط سرویس
۵۷۱.....	تجزیه و تحلیل سرویس‌ها
۵۷۲.....	حملات مبتنی بر بهره گیری از پورت‌ها
۵۷۲.....	پورتهای آسیب پذیر
۵۷۵.....	شروع کار با پورتهای
۵۷۶.....	صحبت کردن با پورت ۷
۵۷۷.....	صحبت کردن با پورت ۱۳
۵۷۷.....	صحبت کردن با پورت ۲۱
۵۷۹.....	صحبت کردن با پورت ۶۹
۵۸۰.....	پورت ۸۰ چیست ؟
۵۸۰.....	صحبت کردن با پورت ۸۰
۵۸۲.....	پورت ۱۳۵
۵۸۴.....	بررسی پورتهای ۱۳۷، ۱۳۸ و ۱۳۹
۵۸۵.....	صحبت کردن با پورت ۱۳۹
۵۸۷.....	بهره گیری از ابزارهای کمکی جهت صحبت کردن با سرویس NetBIOS
۵۸۷.....	enum
۵۸۸.....	دریافت Password Policy Information

۵۸۸.....	استفاده از روش درهم شکستن کلمه عبور
۵۸۹.....nbtscan
۵۹۰..... winfo
۵۹۲..... NAT
۵۹۳.....پورت ۴۴۵
۵۹۴..... پورتهای ۱۰۲۵ تا ۱۰۲۹
۵۹۵..... پورتهای ۱۴۳۳ و ۱۴۳۴
۵۹۵..... پورت ۵۰۰۰
۵۹۶..... حملات مبتنی بر ضعف‌های موجود در پیکربندی
۵۹۷..... حملات مبتنی بر آسیب پذیری‌های موجود در سیستم عاملها و برنامه‌ها
۵۹۷..... Vulnerability چیست ؟
۵۹۹..... بهره‌گیری از ابزارها و مکانیزم‌های مختلف جهت آزمایشهای نفوذپذیری
۶۰۷.....	فصل یازدهم: حملات نوع DoS
۶۰۸..... حملات DoS (عدم پذیرش سرویس)
۶۱۰..... هدف از حملات نوع DoS
۶۱۲..... عملکرد ویروس Blaster جهت ایجاد یک حمله DoS
۶۱۵..... حملات DoS علیه سرورهای وب
۶۱۵..... متوقف کردن سرویس دهنده از درون
۶۱۷..... طریقه مقابله با توقف سرویس دهنده‌ها
۶۱۸..... حمله از نوع اشباع منابع سیستم
۶۱۸..... روش پیشگیری از اشباع منابع سیستمی
۶۱۹..... حملات DoS از بیرون
۶۱۹..... حمله نوع Land
۶۲۰..... حمله Latierra
۶۲۰..... حمله نوع Ping of Death
۶۲۰..... حمله نوع Jolt2
۶۲۱..... حمله نوع قطعه قطعه سازی بسته‌های IP
۶۲۳..... حملات نوع بمباران سرور بوسیله نامه‌های الکترونیکی
۶۲۳..... فراخوانی صفحات وب به صورت پشت سرهم
۶۲۳..... حمله Chargen
۶۲۴..... حمله نوع Winnuke
۶۲۴..... جلوگیری از سرویس دهی سرورهای غیرمتمرکز

۶۲۵.....	روش پیشگیری از حملات DoS از بیرون.....
۶۲۶.....	حمله DoS از راه دور در جهت تلف کردن منابع سیستم.....
۶۲۶.....	حمله نوع SYN Flood.....
۶۲۹.....	مقابله با حملات طغیان SYN (SYN Flood).....
۶۲۹.....	بلاک‌های کوچک.....
۶۲۹.....	کوکیهای SYN.....
۶۲۹.....	کوکیهای RST.....
۶۳۱.....	حمله نوع Smurf.....
۶۳۳.....	حمله نوع Fraggle.....
۶۳۴.....	مقابله با حملات Smurf و Fraggle.....
۶۳۵.....	آسیب پذیری عدم سرویس دهی در برخی محصولات TCP/IP و ICMP.....
۶۳۷.....	روش مقابله با حملات DoS در برخی محصولات TCP/IP و ICMP.....
۶۳۸.....	بهره گیری از حملات نوع DoS جهت درهم شکستن مسیریابهای سیسکو.....
۶۳۸.....	حملات ناقص و بدفرم.....
۶۳۹.....	حملات توزیع شده DoS.....
۶۴۰.....	ماشینهای زامبی (Zombie).....
۶۴۱.....	انواع حملات DDoS.....
۶۴۱.....	Trinoo.....
۶۴۲.....	TFN/TFN2K.....
۶۴۴.....	Stacheldraht.....
۶۴۴.....	معرفی ابزارهای معروف جهت انجام حملات DoS و DDoS.....
۶۴۵.....	روشهای مقابله با حملات DDoS.....
۶۴۶.....	بهره گیری از سیاه چاله.....
۶۴۶.....	مسیریابها و دیوارهای آتش.....
۶۴۷.....	بهره گیری از سیستمهای کشف نفوذ (IDS).....
۶۴۷.....	سرورها.....
۶۴۷.....	ابزار تخفیف DDoS.....
۶۴۷.....	پهنای باند زیاد.....
۶۴۸.....	نحوه اطلاع یافتن از وقوع حملات DoS و یا DDoS.....
۶۴۹.....	اقداماتی که باید در صورت بروز یک تهاجم انجام داد.....
۶۵۱.....	فصل دوازدهم: حملات مهندسی اجتماعی.....
۶۵۳.....	منظور از مهندسی اجتماعی.....

۶۵۷.....	مهندس اجتماعی چه کسی است؟
۶۵۸.....	یک حملهٔ مهندسی اجتماعی چیست؟
۶۵۹.....	بررسی روان شناختی حملات مهندسی اجتماعی
۶۶۱.....	محرکهای روانشناسی جهت ایجاد حملات مهندسی اجتماعی
۶۶۱.....	معامله متقابل
۶۶۲.....	قدرت
۶۶۲.....	هماهنگی و یکپارچگی
۶۶۲.....	کمیابی
۶۶۳.....	زیبایی دوستی
۶۶۳.....	اثر گذاری شدید
۶۶۳.....	بارگذاری اضافی
۶۶۴.....	روابط فریبنده
۶۶۴.....	حس مسئولیت و وظیفه شناسی اخلاقی
۶۶۵.....	مبارزه با حملات مهندسی اجتماعی از دیدگاه روانشناسی
۶۶۵.....	بررسی نمونه‌های کلی و کاربردهای مهندسی اجتماعی
۶۶۵.....	جاسوسی صنعتی
۶۶۶.....	راههای جلوگیری از حملات جاسوسی صنعتی
۶۶۸.....	هک شدن سایت شرکت AOL
۶۶۹.....	منشا حملات مهندسی اجتماعی
۶۶۹.....	چرخهٔ حملات مهندسی اجتماعی
۶۷۰.....	انگیزه‌ها جهت ایجاد حملات مهندسی اجتماعی
۶۷۱.....	تکنیک‌های پیاده سازی حملات مهندسی اجتماعی
۶۷۱.....	تکنیک‌های مبتنی بر کامپیوتر
۶۷۱.....	تکنیک‌های مبتنی بر انسان
۶۷۲.....	مهندسی اجتماعی معکوس
۶۷۳.....	نحوهٔ پیشگیری از حملات مهندسی اجتماعی
۶۷۵.....	ایمن سازی در مقابل حملات مهندسی اجتماعی
676.....	دفاع در مقابل حملات مهندسی اجتماعی
۶۷۷.....	شناسایی سطوح مختلف دفاع
۶۷۸.....	سطح پایه‌ای: سیاستهای امنیتی در برابر مهندسی اجتماعی
۶۷۸.....	سطح پارامتر: آموزش آگاهی امنیتی برای همه
۶۷۹.....	سطح سنگرگیری

۶۸۰	سطح تثبیت و یادآوری
۶۸۰	سطح غیررسمی: مین‌های زمینی مهندسی اجتماعی
۶۸۱	سطح تهاجمی: پاسخ دهی به رویداد
۶۸۱	استراتژی‌های دفاع
۶۸۱	سیاستهای امنیتی
۶۸۲	مدیریت آگاهانه
۶۸۲	امنیت فیزیکی
۶۸۳	آموزش و آگاهی
۶۸۳	معماری صحیح زیرساختهای امنیتی
۶۸۳	محدودیت در پراکندگی داده‌ها
۶۸۳	استراتژی‌های رویارویی با حملات مهندسی اجتماعی
۶۸۴	استراتژی‌های محافظت از کلمه عبور و روشهای صحنه گذاری
۶۸۴	استفاده از رویه‌های خوب و مناسب جهت کاهش خطر
۶۸۵	فرهنگ امنیت
۶۸۵	بررسی اعتبار
۶۸۶	کاهش ضرر با استفاده از بیمه
۶۸۷	ممیزی پذیرش و کاربری سیاستها
۶۸۷	توصیه‌های امنیتی برای مدیران امنیتی سازمانها
۶۸۸	اقدامات لازم در صورت بروز تهاجم
۶۸۹	فصل سیزدهم: حملات مبتنی بر شبکه‌های بی‌سیم
۶۹۱	مفاهیم کلی در شبکه‌های بی‌سیم
۶۹۸	انواع شبکه‌های بی‌سیم از دیدگاه مقیاس بزرگی
۶۹۹	آدرسها در شبکه‌های بی‌سیم
۷۰۰	بررسی معماری و امنیت شبکه‌های محلی بی‌سیم
۷۰۲	عناصر موجود در شبکه‌های محلی بی‌سیم
۷۰۴	حملات مبتنی بر شبکه‌های محلی بی‌سیم
۷۰۷	تغییر هویت
۷۰۷	پاسخهای جعلی
۷۰۷	تغییر پیام
۷۰۸	حملات نوع Denial-of-Service (DoS)
۷۰۸	Jamming
۷۰۸	Man in the Middle

۷۰۹.....	نفوذ به شبکه‌های بی‌سیم
۷۱۳.....	ابزار War-driving
۷۱۴.....	ابزار Net Stumbler
۷۱۸.....	نقاط دسترسی جعلی
۷۱۹.....	ضعفهای اولیه امنیت WEP
۷۱۹.....	۱. استفاده از کلیدهای ثابت WEP:
۷۲۰.....	۲. IV
۷۲۰.....	۳. ضعف در الگوریتم
۷۲۰.....	۴. استفاده از CRC رمز نشده
۷۲۲.....	حمله به WEP
۷۲۳.....	روش دوم:
۷۲۴.....	فناوری بلوتوث و تهدیدات
۷۲۵.....	پوشش آدرسهای مخصوص بلوتوث
۷۲۶.....	ساده سازی آدرسهای بلوتوث
۷۲۷.....	یافتن آدرسهای بلوتوث در هنگام ارتباط
۷۲۸.....	خطرات ناشی از وجود نقاط دسترسی جعلی
۷۲۹.....	منظور از مهندسی عمومی در سرویس بلوتوث
۷۲۹.....	معرفی و بررسی برخی نرم‌افزارهای مُخرَب منتشر شده توسط سرویس بلوتوث
۷۳۰.....	اتصال از طریق بلوتوث به دستگاه هدف بدون کسب مجوز
۷۳۱.....	موقعیت یابی در بلوتوث
۷۳۳.....	بررسی انواع حملات مبتنی بر بلوتوث
۷۳۳.....	حملات مبتنی بر نظارت و کنترل ترافیک
۷۳۴.....	حملات نوع Paging
۷۳۵.....	حملات مبتنی بر جابه جایی در فرکانسها
۷۳۵.....	حملات مبتنی بر نامهای کاربرپسند
۷۳۵.....	حملات نوع Backdoor
۷۳۵.....	حملات نوع Bluejacking (Blue Jack)
۷۳۶.....	حملات نوع Blue Snarf
۷۳۷.....	حملات نوع Blue Bug
۷۳۸.....	بررسی امنیت در بلوتوث
۷۴۰.....	اساس ضعفهای امنیتی در شبکه‌های بی‌سیم
۷۴۱.....	حفره‌های امنیتی مهم در شبکه‌های بی‌سیم 802.11

مسأله شماره ۱: دسترسی آسان	۷۴۲
راه حل شماره ۱: تقویت کنترل دسترسی قوی	۷۴۲
مسأله شماره ۲: نقاط دسترسی نامطلوب	۷۴۳
راه حل شماره ۲: رسیدگی‌های منظم به سایت	۷۴۴
راه حل شماره ۳: طراحی و نظارت برای تأیید هویت محکم	۷۴۶
مسأله شماره ۴: محدودیتهای سرویس و کارایی	۷۴۶
راه حل شماره ۴: دیدبانی شبکه	۷۴۷
امنیت در شبکه‌های محلی بر اساس استاندارد 802.11	۷۴۸
سرویسهای امنیتی احراز هویت در استاندارد IEEE 802.11	۷۵۰
سرویسهای امنیتی محرمانگی و بی عیب و نقصی در استاندارد 802.11	۷۵۳
نکاتی درخصوص بهبود امنیت شبکه‌های بی‌سیم	۷۵۵
بهره‌گیری از استاندارد IEEE 802.11i و دسترسی محافظت شده	۷۵۹
فیلترینگ آدرسهای MAC به منظور افزایش امنیت	۷۶۰
بهره‌گیری از سیستمهای شناسایی مهاجم برای شبکه‌های بی‌سیم	۷۶۰
Vigilant Minds AirXone Managed Security Service	۷۶۱
AirMagnet Distributed 4.0	۷۶۲
فصل چهاردهم: حملات مبتنی بر DNS	۷۶۵
تاریخچه DNS	۷۶۶
پروتکل DNS	۷۶۶
ساختار سرویس دهندگان نام دامنه‌ها در اینترنت	۷۶۸
تکنیکهای پرس و جو در سرویس دهنده‌های نام	۷۷۱
کسب اطلاعات از سرویس دهنده DNS در راستای حمله	۷۷۳
حملات مبتنی بر DNS	۷۷۶
مقابله با نشئت اطلاعات حساس شبکه از طریق DNS	۷۸۹
مقابله با حملات DNS	۷۹۱
مراجع این فصل	۷۹۲
فصل پانزدهم: حملات War Dialing	۷۹۳
جمع‌آوری شماره‌های تلفن هدف	۷۹۴
یافتن مودمهای موجود در شبکه هدف	۷۹۵
بهره‌گیری از مکانیزمهای حمله علیه احراز هویت جهت ورود به سیستم	۷۹۷
بررسی ابزارهای حملات War Dialing	۷۹۹
مقابله با نفوذ از طریق حملات War Dialing	۸۰۵

سخنی با خوانندگان

امروزه امنیت اطلاعات در هر شاخه ای از جایگاه خاصی برخوردار است که روز به روز بر ارزش آن افزوده می‌شود. در حال حاضر تقریباً تمامی صنایع و حرفه‌ها به نوعی نیازمند امنیت اطلاعات و ایجاد مکانیزم‌هایی جهت محرمانگی آنها هستند. البته در برخی موارد به این امر مهم اهمیت خاصی داده نمی‌شود. متأسفانه برخی مدیران، متخصصان شبکه اطلاعات کافی در خصوص ایمن سازی شبکه‌ها ندارند و با دید کاملاً ابتدایی با آن برخورد می‌کنند. همین موضوع باعث می‌شود تا تمامی طراحی‌ها و پیاده سازی‌های آنها در سطح شبکه و برنامه نویسی بدون در نظر گرفتن اصول و استانداردهای امنیتی صورت گیرد. به همین دلیل ممکن است هر لحظه تمامی اطلاعات حساس و مهم آنها تحت تأثیر مهاجمان و نرم افزارهای مُخرب قرار گرفته و هرچه را که در طول سالیان طولانی به دست آورده اند، به یکباره از دست بدهند.

در این میان نیز افرادی بسیار باهوش و تیزبین (نفوذگران)، با معلوماتی که شاید یک مهندس کامپیوتر یا یک مدیر شبکه به ندرت با آنها آشنا باشد، نیز وجود دارند که همراه با پیشرفت علم کامپیوتر و حرفه ای تر شدن برنامه‌های کاربردی، آنها نیز پیشرفت فوق العاده ای دارند. امروزه محیط شبکه‌ها بستر مناسب و خوبی برای فعالیت و جولان نفوذگران به شمار می‌رود. البته نفوذگران هر چند در برخی موارد باعث بُروز مشکلاتی می‌شوند، اما نمی‌توان از تلاش بعضی از آنها درگسترش و پیشرفت علم کامپیوتر، سیستم عامل، اینترنت و وب چشم پوشی نمود.

اینجانب به عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تألیف کتابی مرجع به منظور افزایش آگاهی متخصصین، دانشجویان و مدیران شبکه در زمینه امنیت و شبکه بودم تا آنها را با اصول فنی حملات مختلف هکری آشنا و آگاه سازم. (گرچه مدیران و متخصصین امنیت شبکه حُکم اساتید اینجانب را دارند، اما به حُکم وظیفه بر خود لازم دانستم که این آگاه سازی را انجام دهم.)

شاکله کتاب حاضر برگرفته از کتابها و منابع معتبر و استاندارد شاخه نفوذگری (هک) و ضدهک بوده که با تجربیات اینجانب در امر شبکه و نفوذگری آمیخته شده است، که به فرم کاملاً آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن همراه بوده است. پیشاپیش تمام کاستی‌های آنرا می‌پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنماییهای دلسوزانه آنها را به دیده منت پذیرا هستم.

(m_Davari@TOP-co.ir)

(m_Davary@Parshack.zzn.com)

این کتاب صرفاً برای افزایش آگاهی‌ها و رشد علمی متخصصین کامپیوتر تألیف گردیده است. در نتیجه عواقب ناشی از هرگونه سوء استفاده از مطالب این کتاب بر عهده شخص خاطی بوده و مؤلف و انتشارات هیچ گونه مسئولیتی در این مورد بر عهده نخواهند گرفت.

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید عزیزی که مهربانانه دست مرا درانجام اینکار ناچیز فشردند، تشکر می‌کنم. بر خود لازم می‌دانم از زحمات بی دریغ سرکار خانم مهندس سیده پونه مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانه ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است. همچنین از زحمات و همکاری جناب آقای مهندس محمد داوری دولت آبادی کمال تشکر را دارم.

در پایان از مدیریت فرزانه انتشارات پندار پارس، جناب آقای مهندس حسین یعسوبی و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده اند، صمیمانه قدردانی می‌نمایم.

نتوان وصف تو گفتن که تو در وهم نگنجی

نتوان شبه تو جستن که تو در فهم نیائی

همه درگاه تو جویم، همه از فضل تو پویم

همه توحید تو گویم که به توحید سزائی

(مجید داوری دولت آبادی - زمستان ۱۳۸۷)