

فضای سایبر

تکنیک‌های جمع‌آوری، پنهان‌سازی و انتقال اطلاعات

جلد اول

Author: rasoul Lotfi

C Y B E R 1 S P A C E
GATHERING, COVERT, TRANSFER TECHNIQUES OF DATA

تألیف: رسول لطفی



پلیس اطلاعات و امنیت عمومی ناجا
دفتر تحقیقات کاربردی

سرشناسه	: لطفی، رسول، ۱۳۵۹ -
عنوان و نام پدیدآور	: فضای سایبر : تکنیک‌های جمع‌آوری، پنهان‌سازی و انتقال اطلاعات/تالیف رسول لطفی ؛ [برای] پلیس اطلاعات و امنیت عمومی ناجا دفتر تحقیقات کاربردی.
مشخصات نشر	: تهران: شرکت چاپ و انتشارات راه فردا، انتشارات ناجی‌نشر، ۱۳۹۱.
مشخصات ظاهری	: ج. :
شابک	: ۶۵۰۰۰ ریال: ج. ۱ : 978-600-6486-09-3
وضعیت فهرست نویسی	: فیا :
موضوع	: فضای مجازی :
موضوع	: فضای مجازی -- جنبه‌های سیاسی :
شناسه افزوده	: نیروی انتظامی جمهوری اسلامی ایران. پلیس امنیت عمومی. دفتر تحقیقات کاربردی
رده بندی کنگره	: ۱۳۹۱ / ۶۴۶ / HMA51
رده بندی دیویی	: ۳۰۲ / ۲۸۲۳ :
شماره کتابشناسی ملی	: ۳۰۰۸۶۱۲ :

پلیس اطلاعات و امنیت عمومی ناجا، دفتر تحقیقات کاربردی

نشانی: تهران، خیابان ستارخان، خیابان شهر آراء، پلیس مهاجرت و گذرنامه ناجا، ساختمان شماره ۲

تلفن: ۸۱۸۲۷۸۰۳ دورنگار: ۶۶۹۲۷۷۹۹

عنوان کتاب: تکنیک‌های جمع‌آوری، پنهان‌سازی و انتقال اطلاعات در فضای مجازی

مؤلف: رسول لطفی

ناظر: علیرضا طباطبایی

ویراستار ادبی: علی عربی

قیمت: ۶۵۰۰۰ ریال

شمارگان: ۵۰۰ نسخه

چاپ اول ۱۳۹۰ تهران

لیتوگرافی / چاپ / صحافی: شرکت ناجی نشر

صفحه آرا: حمید جمشیدوند

ISBN: 978-600-6486-09-3

شابک: ۹۷۸-۶۰۰-۶۴۸۶-۰۹-۳

انتشار سازمانی: شماره مجوز ۶/۹۱/۹۱۱۰۴۷۰

فهرست مطالب

فصل اول: ورود به فضای فناوری

بخش اول: آغاز

- مقدمه مولف ۱۰
- تعهدات خواننده ۱۱
- سیستم عامل و انواع آن ۱۲
- مقدمه ای بر ویندوز (سطح ابتدایی) ۱۶

بخش دوم: فناوری و تحول در حوزه های تحلیلی

- مقدمه ای بر فناوری ۲۲
- فناوری و تاثیر آن بر مدار اطلاعات ۲۴
- تغییر در روشهای جمع آوری ۲۶
- تحول در تجزیه و تحلیل ۲۸
- جمع آوری با سرعت نور (سرویس ردگیری آنی اخبار) ۳۱
- تحول در انتشار ۳۱
- بانکهای اطلاعاتی ۳۲

فصل دوم: ورود به فضای شبکه ای

بخش اول: جمع آوری اطلاعات در فضای سیستمهای رایانه ای

- جمع آوری در محیط آفلاین ۳۸
- اصول جمع آوری ۳۸
- جستجوی مقدماتی ۴۴
- جستجوی پیشرفته ۴۷
- محیط خط فرمان سیستم عامل (CMD) ۴۷
- فلسفه جمع آوری پنهان ۵۵
- عبور از رمز Bios ۵۵
- عبور از رمز سیستم عامل های ویندوزی ۵۹
- عبور از رمز فایل ها ۶۱
- وایروس ها ۷۲
- نفوذ پنهان ۷۴
- آموزش تصویری ایجاد یک (Backdoor) ساده در ویندوز ۷۴
- نرم افزارهای جاسوسی ۹۰
- انواع نرم افزارهای جاسوسی ۹۱

۹۴	• پروژه اسرائیلی جاسوسی از ویندوز.....
۹۴	• اهداف برنامه ویندوز اسپای.....
۹۵	• ساختار برنامه.....
۹۵	• عملکرد برنامه.....
۹۶	• تشریح عملکرد نرم افزار.....
۱۰۰	• آشنایی با یک نرم افزار جاسوسی (نصب و به کار گیری).....
۱۰۰	• نصب نرم افزار.....
۱۱۰	• جمع آوری آنلاین.....
۱۱۰	• جستجو در اینترنت.....
۱۱۲	• موتورهای جستجو و تکنیکهای استفاده از آنها.....
۱۱۳	- تعریف موتور جستجو.....
۱۱۳	- راهبرد جستجو در اینترنت.....
۱۱۵	- نکات کلیدی جستجو به زبان فارسی.....
	بخش دوم: شناخت فضای اینترنت
	○ قسمت اول: تاریخچه و تحولات
۱۲۱	- آمار جهانی اینترنت و خاورمیانه.....
۱۲۳	- اینترنت در ایران.....
۱۲۵	- ایران در خاورمیانه.....
۱۲۷	• قسمت دوم: فضاهای کاری اینترنت.....
۱۲۸	• وب ۱ چیست.....
۱۲۸	• تاریخچه وب.....
۱۲۹	• چهره های گوناگون وب.....
۱۲۹	- وب ۲ چیست.....
۱۳۰	- تعریف وب ۲.....
۱۳۰	- نمادهای وب ۲.....
۱۳۱	- جنبه های وب ۲.....
۱۳۱	- درک بهتر وب ۲ با انجام چند مقایسه.....

فصل سوم: سازمان‌های اطلاعاتی در فضای مجازی

- سازمان اطلاعاتی در فضای مجازی ۱۳۴
- لزوم حضور در اینترنت ۱۳۴
- ساختار اتصالات شبکه در اینترنت ۱۳۵
- ارتباط از مبدا تا مقصد ۱۳۶
- آدرس‌دهی در اینترنت ۱۳۷
- نگاه کلی به سخت افزار شبکه ۱۳۸
- سرویس دهنده خدمات اینترنت ۱۳۹
- شنود اینترنت ۱۳۹
- شناسایی کاربران و جمع‌آوری از طریق آنالیز شبکه ۱۴۰
- میسرهای و نودهای انتقالی مشخص ۱۴۲
- ایجاد دیتابیس از کلید واژه ۱۴۳
- آنالیز درخواست‌ها ۱۴۴
- نشان‌دار کردن سوژه ۱۴۴
- ضد اطلاعات در وب ۱۴۶
- مقابله با شنود در فضای وب ۱۴۶
- بخش دوم: ملزومات ارتباط با منابع:
- ارتباط با منابع ۱۵۰
- پست الکترونیک ۱۵۰
- سرویس دهنده‌گان ۱۵۲
- نحوه ساخت حساب Gmail ۱۵۲
- ساخت ایمیل در MyWay ۱۶۰
- ساختن ایمیل در سرویس ۱۶۶
- ارتباط امن منبع گردان با منابع ۱۷۰
- تعریف VPN ۱۷۰
- سناریو ۱۷۱
- سرویس گوگل آلرتس (سرویس جمع‌آوری اخبار آنی) ۱۹۰
- اصطلاحات شبکه ۱۹۲
- اصطلاحات اینترنت ۱۹۴

فصل اول:

ورود به فضای فناوری

❖ بخش اول: آغاز

- مقدمه مؤلف
- تعهدات خواننده
- سیستم عامل و انواع آن
- مقدمه‌ای بر ویندوز (آغازگران)

مقدمه مؤلف:

همین باور توانایی، شما را توانا می‌کند.

(امام خمینی ره)

خدا را سپاس می‌گویم که فرصتی بزرگ را به من، بنده کوچکش، عطا کرد تا بتوانم معلومات ناچیزی را که از دریای بیکران نعماتش، قطره‌ای را که در ظرف خویش نگهداشته بودم، به قدم‌های هراس‌انگیز قلم بسپارم و بر لوح سفید منتظر برهانم. دنیای امروز، فضای پرتراکم سیگنال‌ها و حامل‌های داده‌ها است و در آن تمام کشورها و ملت‌ها و فرهنگ‌ها دارای فاصله کمتر از هزارم ثانیه‌اند، راه‌ها کوتاه‌تر است و مسافت‌ها به سرعت نور طی می‌شود.

برای زیستن در این دنیای کوچک، با بی‌نهایت اطلاعات و ابزارها برای ادامه حیات، نیازمند دریافت اطلاعات آنی و کارآمد هستیم. زیستن در این دنیای نوین نیازمند تحول بنیادی در روند انجام کارها، یکارگیری فناوری‌های نو و درک درست از فضای پیرامونی است. کتاب حاضر اولین کتاب کاملاً کاربردی برای ایجاد رابطه میان کارکنان سطح پایین و متوسط با فضای دنیای فناوری و شبکه است. گاهی اوقات کتاب‌هایی را می‌بینیم که هر چند دارای محتوای فنی و پیچیده‌اند اما همین پیچیدگی موجب می‌شود تا خواننده درک درستی از مفاهیم فناوری و کاربردهای آن نداشته باشد. در این کتاب هدف ساده نویسی و ساده انگاری فضای فناوری بوده است تا آشتی را میان خواننده و فضای نوین فناوری برقرار نماید. در تولید این کتاب از اینترنت، منابع گوناگون، تجربیات فنی، جلسات و سخنرانی‌ها و تحلیل‌ها و پرسش‌ها استفاده فراوانی شده است. با در نظر گرفتن قانون نسبی بودن هر پدیده، این کتاب نیز مطمئناً دارای نقص‌های فراوانی است. به این امید به نگارش در آمد تا نقطه آغازی باشد برای رشد دادن نگاه کارکنان از منظر اطلاعاتی به فناوری‌های نو و ادامه این مسیر توسط سایر متخصصین این حوزه برای دستیابی به تکامل نسبی در حوزه پیوند تکنولوژی اطلاعاتی با اطلاعات امنیتی.

مخاطبان این کتاب دانشجویان دانشگاه، کارکنان حوزه‌های جمع‌آوری، عملیات فنی، تحلیل و انتشار اند. امید است با انتقادات و پیشنهادات خود مرا در نگارش جلد بعدی این کتاب یاری نمایند.

در اینجا بر خود واجب میدانم از حمایت‌های دلسوزانه و راهنمایی‌های تفکرزای حجه الاسلام والمسلمین حیدری ریاضی‌المعظم دفتر تحقیقات کاربردی صمیمانه تشکر کنم.

رسول لطفی تهران، شهریور ۱۳۸۹

تعهدات خواننده:

این کتاب برحسب نیازمندیهای معمول در فضای سایبری برای به کارگیری در جهت اهداف سازمانی تدوین شده است. مطالب آن دست یافتنی است و ممکن است تمام این اطلاعات به صورت متفرقه در فضای پیرامون شما موجود باشد. کارکرد این کتاب آماده‌سازی یک ذهن مرتب و هدفمند در تفکرات شماست و این کتاب شما را برای دستیابی به اهداف کاری هدایت می‌کند. آنچه از شما انتظار می‌رود آن است که این دانش برای اهداف ضد اخلاقی (چه در کار و چه در زندگی شخصی) استفاده نکنید.

پیامدهای مثبت این کتاب بر کسی پوشیده نیست و امیدواریم راهگشای برخی از مسائل خواننده بوده و او را به یادگیری بیشتر در این زمینه ترغیب کند.

در ابتدا انتهای کتاب را مطالعه کنید.

برای ورود به فضای مجازی و شبکه‌ها شما لازم است در ابتدا با تعدادی از کلمات رایج که ممکن است برخی از آنها را ندانید، آشنا شوید. این کلمه‌ها مرسوم‌اند و زیاد به گوشتان خواهد خورد. برای این منظور و برای درک بهتر مطالب کتاب ابتدا بخش انتهایی کتاب، آموزش ایمیل و فرهنگ لغات را بخوانید.

WWW.KOOLAB.COM



سیستم عامل و انواع آن

سیستم عامل مهمترین ترین برنامه‌ای است که قبل از هر چیز بر روی کامپیوتر شما اجرا می‌شود و خدمات متنوعی در ابعاد متفاوت ارائه می‌کند. در حقیقت فضای اجرای برنامه‌های دیگر، سیستم عامل است و اگر نباشد شما قادر به استفاده از سخت افزار سیستم رایانه نیستید. سیستم عامل با یک فرایند خاص نقش بین سخت افزار و کاربر را ممکن می‌سازد. خدماتی که به کاربر ارائه می‌کند:

- نوع نرم افزاری را که شما می‌توانید بر روی سیستم خود نصب کنید، مشخص می‌نماید.
- هماهنگی لازم را به منظور اجرای برنامه‌ها انجام می‌دهد.

۱- اطمینان از این موضوع که عناصر سخت افزاری نظیر صفحه کلید، چاپگر و هارد دیسک دارای عملکردی عاری از خطا بوده و امکان ارتباط با آنها وجود دارد.

۲- ایجاد شرایط و امکانات لازم به منظور اجرای صحیح برنامه‌های کامپیوتری نظیر واژه پردازها (مثل MsWord)، برنامه‌های سرویس گیرنده پست الکترونیکی (مانند Outlook^۱)، مرورگرهای وب (مثل Internet Explorer). در صورتی که برنامه‌ها نیازمند استفاده از منابع سیستم نظیر چاپگر یا هارد دیسک باشند، با مدیریت سیستم عامل این امر میسر می‌گردد.

- ارائه پیام‌های خطاء متناسب با مسائل ایجاد شده

سیستم عامل، نوع و نحوه مشاهده اطلاعات و انجام عملیات مورد نظر را نیز مشخص می‌نماید. برخی سیستم‌های عامل از یک رابط کاربر گرافیکی معروف به GUI که از کلمات Graphical User Interface اقتباس شده است، استفاده می‌نمایند. در این نوع از سیستم‌های عامل، اطلاعات با استفاده از تصاویر (آیکون، دکمه‌ها، جعبه‌های محاوره‌ای، پنجره‌ها، ...) و کلمات ارائه می‌گردد (ویندوز نمونه‌ای از اینگونه سیستم‌های عامل است). سایر سیستم‌های عامل ممکن است از یک رابط کاربر مبتنی بر متن به منظور تعامل با کاربر استفاده نمایند. تاکنون سیستم‌عامل‌های متداولی در سطح دنیا طراحی و

۱. اوت لوک به معنای چشم انداز است.