



راهبردهای امنیت سایبری

(جلد دوم)

شناسایی و فریب

گردآوری و تدوین
معاونت پژوهش و تولید علم

دانشگاه اطلاعات و امنیت ملی

مؤسسه چاپ و انتشارات

۱۳۹۶

عنوان و نام پدیدآور	راهبردهای امنیت سایبری/ گردآوری و تدوین معاونت پژوهش و تولید علم، [دانشگاه اطلاعات و امنیت ملی].
مشخصات نشر	تهران: دانشگاه اطلاعات و امنیت ملی، مؤسسه چاپ و انتشارات، ۱۳۹۶.
مشخصات ظاهری	۳ ج. ش. ۳۵۶.
شابک	۹۷۸۶۰۰۸۴۱۱۸۸۸: ۳۰۰۰۰۰ ریال
وضعیت فهرست‌نویسی	فیا:
یادداشت	ج. ۳ (چاپ اول: ۱۳۹۶) (فیا).
یادداشت	کتابنامه.
مندرجات	ج. ۱. سیاست‌گذاری. - ج. ۲. شناسایی و فریب. - ج. ۳. حفاظت.
موضوع	شبکه‌های کامپیوتری - تدابیر ایمنی
موضوع	Computer networks - Security measures
موضوع	اینترنت - تدابیر ایمنی
موضوع	Internet - Security measures
شناسه رده	دانشگاه اطلاعات و امنیت ملی. مؤسسه چاپ و انتشارات
شناسه افزوده	دانشگاه اطلاعات و امنیت ملی. معاونت پژوهش و تولید علم
رده‌بندی کنگره	TK۵۱۰/۵/۲ ۱۳۹۶:
رده‌بندی دیویی	۰۰۵/۱
شماره کتابشناسی ملی	۱۷۷۶۱۹۱:

عنوان: راهبردهای امنیت سایبری / جلد ۳، شناسایی و فریب

گردآوری و تدوین: معاونت پژوهش و تولید علم

ناشر: مؤسسه چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی

تاریخ انتشار: ۱۳۹۶

نوبت چاپ: اول

بها: ۳۰۰۰۰۰ ریال

شابک: ۹۷۸۶۰۰۸۴۱۱۸۸۸

شمارگان: ۱۰۰۰ نسخه

«تمامی حقوق این اثر محفوظ است. تکثیر یا تولید مجدد آن کلی یا جزئی به هر صورت (چاپ، فتوکپی، صوت، تصویر و انتشار الکترونیکی) بدون اجازه مکتوب ناشر ممنوع است.»

شماره تلفن: ۲۲۴۶۹۷۳۹

تهران: صندوق پستی ۱۴۳۸-۱۶۷۶۵

مقدمه ناشر

در فصل اول کتاب با عنوان «شناسایی و نظارت دیجیتال» ضمن ارائه اصول پایه‌ای نظارت، نظارت و دفاع سایبری ارائه، تاریخچه و کاربردهای عملی اصول مذکور و چگونگی ورود آنها به دنیای دیجیتال بررسی می‌گردد. در ادامه ضمن تشریح مبانی شناسایی و نظارت دیجیتال، با ارائه پیشنهاد از موضوع، زمینه برای فصول آینده که در آنها به تفصیل چگونگی انجام این اعمال، میزان آسیب‌پذیری‌ها و چگونگی افزایش دفاع و کاهش خطر در سطح شخصی پرداخته می‌شود، مهیا می‌گردد.

فصل دوم به موضوع «جمع‌آوری اطلاعات» می‌پردازد و طی آن شیوه‌های جمع‌آوری اطلاعات برای توسعه اشرافیت بر یک بخش خاص در دنیای سایبری مورد بحث قرار می‌گیرد. رد پایی که هر کنشگر سایبری در دنیای مش‌خون از ابزارها و لوازم همراه دیجیتال و برنامه‌های کاربردی به جا می‌گذارد، مفهوم حریم خصوصی را با چالش اساسی روبرو نموده است. نگارنده به تفصیل بیان می‌دارد که الگوی زندگی بسیاری از امروزی‌ها امکان انزوا از این اسلوب حیاتی را از افراد سلب نموده اما در عین حال در تلاش مطالب فنی، ضمن توسعه بینش سایبری مخاطب نسبت به عمق و گستره میزان نظارت، روش‌هایی را برای ارتقاء نسبی امنیت و کاهش ردهای دیجیتال پیشنهاد می‌دهد.

فصل سوم با عنوان «مهندسی اجتماعی» ضمن ارائه تعریفی از آن دال بر فریب افراد اعتمادکننده برای دور زدن کنترل‌های امنیتی فیزیکی و سایبری محافظت از داده، به تشریح مواردی از تکنیک‌های مهندسی اجتماعی و نیز حملات پیشرفته‌ای که مقدمات و مراحل اولیه آن‌ها از طریق مهندسی اجتماعی انجام می‌شود، اشاره می‌نماید.

در فصل چهارم با عنوان «ردیابی تلفن همراه» آسیب‌پذیری‌های ناشی از کاربری تلفن‌های همراه هوشمند تشریح و ضمن ورود به جزئیات برخی از مدل‌های رایج گوشی‌های تلفن همراه، به انواع مختلف آسیب‌های مربوط به ردیابی از طریق تلفن همراه، اعم از ردیابی خود گوشی، ردیابی توسط برنامه‌های داشبورد گوشی یا برنامه‌های کاربردی که کاربران با اختیار خود نصب و از آنها بهره‌برداری می‌کنند، عطف توجه گردیده است. در انتهای فصل ضمن تشریح یک پرونده قضایی در این رابطه، به قدیمی بودن قوانین ایالات متحده و ناکارآمد بودن آنها به منظور حفاظت از حریم خصوصی شهروندان اشاره گردیده است.

در فصل پنجم با عنوان «ردیابی فیزیکی دستگاه‌ها» ضمن اشاره به توسعه و فراگیری فن ابزارهای جدید قابل پوشیدن و نیز ابزارهای چسبی‌اس ردیابی دستگاه‌ها (نظیر خوردوها) یا سالمندان یا حیوانات خانگی، تهدیدات ناشی از این ابزارها مورد بررسی قرار گرفته‌اند. خدماتی که این قبیل ابزارها در اختیار افراد قرار می‌دهند، موجب استفاده روزافزون از آنها شده، غافل از اینکه این فن‌رها حلقه محاصره افراد را تنگ‌تر کرده و تقریباً تردد و حضور آنها را بصورت نقطه‌ای در تمام ساعات شبانه روز مقدور می‌سازند. فصل ششم به «ردیابی ویدئو و وب کم» اختصاص یافته و امکان ثبت ویدئو و تصویر افراد را بر اساس وجود دوربین‌های متعدد امنیتی در اماکن عمومی و خیابان‌ها، همراه داشتن گوشی‌ها و لپ‌تاپ‌های مجهز به دوربین و خدمات امنیتی نظارت بر اماکن شخصی و منازل به بحث می‌گذارد. نگارنده نتیجه می‌گیرد تقریباً لحظه‌ای و مکانی وجود ندارد که تصویر شما در حال ثبت نباشد یا امکان چنین کاری دور از دسترس باشد. وی ادامه می‌دهد که همه این مسائل غیر از امکان ردیابی با دوربین‌های ماهواره‌ای قدرتمند توسط دولت یا آژانس‌های نظامی و اطلاعاتی است.

«سرقت داده و سوء استفاده از آن» عنوان فصل هفتم است که در آن ضمن تقسیم‌بندی داده به دو گونه ثابت و سیار، تهدیدات مربوط به هر کدام مورد بحث قرار می‌گیرد.

داده‌های ثابت از طریق سرقت فیزیکی تا نفوذ به دستگاه‌های نگهداری آنها و داده‌های سیار با تکنیک‌های مختلف سایبری در مسیر انتقال می‌توانند ربوده شوند. هر چند روش‌های فنی جرم‌شناسی قانونی می‌توانند تا حدود زیادی رد مهاجمان و سارقان اطلاعاتی را مشخص نمایند، اما این اقدامات تضمینی برای امنیت داده ایجاد نمی‌کنند.

در فصل هشتم برخی «روش‌های محافظت» مورد بررسی قرار گرفته و بر اساس ماهیت تهدیداتی که در فصول دوم تا هفتم به تفصیل مورد بحث واقع شد، ضمن معرفی روش‌هایی برای کاهش مخاطرات مجدداً تأکید گردیده که امکان تضمین امنیت کامل داده، دست‌نیافتنی است.

فصل نهم در واقع مقدمه بخش دوم کتاب بوده و اشاره کلی به فصل‌بندی ادامه کتاب و رئوس مطالب مورد بحث در فصل‌های بعدی خواهد داشت.

در فصل دهم با عنوان «برون‌دزدی، ممانعت و فریب کلاسیک با قلمروی امنیت سایبری» تلاش می‌شود ضمن اشاره به چهار باب ممانعت و فریب در دنیای واقعی و در زمینه‌های کلاسیکی چون جنگ، دیپلماسی و سیاست، این ابیات و راهبردهای نسبتاً قدیمی آن، در بافتاری سایبری بومی‌سازی شده و به این حوزه بسط داده شوند. بر این اساس ماتریس ممانعت و فریب معرفی و تاکتیک‌ها، فنون و رویه‌های ممانعت و فریب سایبری در ساختار ماتریس یاد شده تشریح شده است. همچنین به الزامات سازمانی، برنامه‌ریزی و اجرای عملیات موفقیت‌آمیز ممانعت و فریب سایبری نیز اشاراتی شده است.

«نفوذ، فریب و کارزارها» عنوان فصل یازدهم کتاب است که ضمن به اشتراک گذاشتن راهبردهای نفوذ سایبری که در سال‌های اخیر بسط و توسعه یافته‌اند، سطوح چهارگانه حمله‌های تهاجمی، حمله‌ها، زنجیره‌های کشتار و کارزار را معرفی و به ارائه تحلیل‌هایی در خصوص طراحی و اجرای استراتژی‌های ممانعت و فریب سایبری، متناسب با هر کدام از این سطوح می‌پردازد. بر این اساس گزینه‌های ممانعت و فریب سایبری در هر مرحله در قالب مدلی جامع متشکل از فرآیندهای برنامه‌ریزی، آماده‌گری و اجرای عملیات فریب و ممانعت تشریح و طبق مدل

مزبور مراحل هر حمله سایبری و رفتار عاملان این حملات تشریح شده‌اند.

در فصل دوازدهم «مورد کاوی‌های ممانعت و فریب سایبری» مدنظر بوده و دو مطالعه موردی در حوزه فریب و ممانعت و حملات سایبری برای ارائه درک عملیاتی به خواننده از مفاهیم و روندهای فریب در حملات سایبری واکاوی شده است. مورد اول ماجرای حمله «استاکس نت» به تأسیسات غنی‌سازی اورانیوم جمهوری اسلامی ایران و گزارشات امنیتی مرتبط با این حمله ویژه سایبری است و مورد دوم، پرونده‌ای فرضی در خصوص جاسوس سایبری است. پرونده نخست نحوه بکارگیری گسترده ممانعت و فریب تهاجمی در سطوح فنی تاکتیکی، عملیاتی و راهبردی است و پرونده دوم استفاده از عناصر فریب و ممانعت سایبری در فرآیند تهاجمی و مقابله با جاسوسی سایبری را نشان می‌دهد.

در فصل سیزدهم با عنوان «تمرین ممانعت و فریب سایبری» جزئیات یک آزمایش تحقیقی تحت عنوان اس‌ال‌ایکس ۱ که طی آن تیم‌های آبی، سرخ و سفید هر کدام نقش‌های مشخصی را عهده‌دار بوده و یک مانور دفاعی جنگ سایبری را برگزار نموده‌اند، توضیح داده شده است. رویکرد اصلی این تمرین واکاوی میزان تاثیرگذاری افزودن فنون، تاکتیک‌ها و رویه‌های ممانعت و فریب به دفاع سایبری است. این در مقابل نفوذ بوده و نشان می‌دهد که استفاده از فریب و ممانعت اولاً به چه نحوی در فرآیند دفاع سایبری مقدور بوده و ثانیاً تا چه اندازه می‌تواند این فرآیند را کارآمدتر سازد.

فصل چهاردهم با عنوان «ملاحظات، انطباق و اشتراک‌گذاری» در زمینه این موضوع است که عملیات فریب و ممانعت به هر علتی ممکن است با شکست کامل یا نسبی در تحقق اهداف از پیش تعیین‌شده مواجه گردد. در چنین موقعیت‌هایی چه باید کرد؟ انطباق‌پذیری و چالاکي در برنامه ریزی، آماده‌گری و اجرای عملیات فریب حیاتی هستند و طراحان فریب باید برای عکس‌العمل نسبت به شرایط نامطلوب نیز آمادگی داشته باشند. این مهم با شناسایی مخاطرات، پیامدهای ناخواسته، افشا و ناکامی عملیات فریب و داشتن طرحی برای این موقعیت‌ها مقدور خواهد بود. بر این اساس در این فصل برای مراحل

مختلف طراحی و اجرای عملیات فریب فنون، مزایا، چالش‌ها و معایب احتمالی متناظر معرفی و نهایتاً نیز مقوله استانداردسازی مفاهیم و رویه‌ها و به اشتراک‌گذاری تجارب بین سازمان‌ها و طرف‌های قابل اعتماد برای حصول درک و آگاهی موقعیتی جامع‌تر پیشنهاد گردیده است.

«مقابله با ممانعت و فریب» عنوان فصل پانزدهم کتاب است که در آن مفهوم ضد فریب و کاربرد آن در دفاع سایبری مورد بررسی قرار می‌گیرد. غیر از مقوله ممانعت و فریب در سایر دفاع سایبری، مفهوم ضد فریب نیز بر اساس مدلی که در این فصل ارائه گردیده منظور پرده برداشتن از عملیات فریب حریف مهاجم برای اهداف دفاع سایبری ارزشمند خواهد بود. مهاجمین برای افزایش ضریب موفقیت طرح نفوذ و فرار از تورشناسایی مدافعین و اقدامات مقابله‌ای آنان، حملات خود را بر اساس فنون و تاکتیک‌های فریب و مقابله طراحی و عملیاتی می‌کنند. لذا شناسایی این اقدامات در مراحل پیش و پس از بهره‌برداری، مافعین را در اتخاذ تدابیر و راهبردهای دفاعی موثرتر یاری خواهد نمود. یک مطالعه موردی در ارتباط با کاربرد این مفاهیم علیه عملیات گسترده جاسوسی صنعتی و علمی چینی‌ها نیز برای تعمیق درک عملیاتی خوانندگان در انتهای فصل ارائه شده است.

فصل شانزدهم با عنوان «مدل بلوغ توانمندی» بحث فصلی در خصوص بلوغ توانمندی‌های فریب و ممانعت و در هر دو رویکرد تهاجمی و دفاعی سایبری را ارائه می‌دهد. در حقیقت تلاش می‌شود تا معیارها و سنجه‌هایی کاملاً سازگار با استاندارد شده از توانمندی عملیات فریب و ممانعت ارائه گردد تا خواننده قادر به بررسی چارچوبی برای ارزیابی از آمادگی سازمان خودی یا تخمین توانمندی‌های رقبای فرضی باشد. همچنین کاربرد این مدل که پنج سطح از بلوغ سازمانی در حوزه فریب و ممانعت را تبیین می‌کند، می‌تواند در نقش دستورالعملی برای تحکیم و ارتقاء توانمندی‌های راهبردی ممانعت و فریب سایبری مورد استفاده مدیران تحول در حوزه سایبری قرار گیرد.

در فصل هفدهم با عنوان «مدیریت چرخه حیات ممانعت و فریب سایبری» خود مقوله مدیریت عملیات فریب و ممانعت به لحاظ تفکیک اجزای چرخه حیات آن و تشریح هر کدام از گام‌های این چرخه مورد توجه قرار گرفته است. سطح بلوغ، سنجه‌ها، مشهودات و شاخص‌ها، زمینه‌سازی‌ها، فرآیندهای عملیاتی و مدل مدیریتی ابعاد شش‌گانه مدیریت چرخه حیات عملیات فریب و ممانعت هستند که در این بخش معرفی شده‌اند.

فصل پانزدهم نیز «نگاهی به آینده» موضوع و مسیرهای پیش روی عملیات ممانعت و فریب و روش‌های مرتبط با این حوزه داشته و گرایش بیشتر به مدل‌های نظریه‌بازی و مدل‌های زیستی و ... تم امنیتی فیزیولوژیک را بسترهای توسعه فراروی این حوزه معرفی می‌نماید.

امید است مطالعه این کتاب به‌اندازه نگاه درست و عمیقی از تهدیدات سایبری و روش‌های کاهش و مدیریت اثرات مخرب آن را در سطوح مختلف فردی و مدیریتی و راهبردی در اختیار مخاطبان و جامعه علمی و حرفه‌ای مرتبط با این حوزه قرار دهد.

دکتر سید علی حسینی، پژوهش و تولید علم

فهرست مطالب

۲۱	شناسایی، لغات و دفاع سایبری.....
۲۵	فصل اول: شناسایی و نفوذ دیجیتال.....
۲۷	۱-۱. فن و تاریخچه جاسوسی.....
۳۰	۲-۱. تهدیدات شناسایی و نظارت دیجیتال.....
۳۱	۳-۱. چشم انداز تهدیدات.....
۳۵	۴-۱. جاسوسی.....
۳۶	۵-۱. آژانس امنیت ملی و ادوارد اسنودن.....
۳۹	۶-۱. اعتماد عمومی.....
۴۳	۷-۱. جرائم سایبری.....
۴۴	۸-۱. دلیل و انگیزه انجام جاسوسی چیست؟.....
۴۶	۹-۱. دستوراد جاسوسی چیست؟.....
۴۸	۱۰-۱. جرم شناسی قانون دیجیتال.....
۴۹	۱۱-۱. چه کسی مبادرت به انجام جاسوسی می کند؟.....
۵۰	۱۲-۱. نقش های حرفه ای.....
۵۰	۱۳-۱. هکرهای کلاه سفید، خاکستری و سیاه.....
۵۱	۱۴-۱. متخصص جرم شناسی قانونی دیجیتال.....
۵۲	۱۵-۱. تحلیل گر اطلاعات سایبری.....

- ۱۶-۱. مهندسی امنیت سایبری ۵۲
- ۱۷-۱. کارشناس تشخیص رخنه ۵۳
- ۱۸-۱. کارآگاهان خصوصی ۵۴
- ۱۹-۱. حوزه اعمال قانون ۵۴
- ۲۰-۱. مسائل حقوقی و اخلاقی ۵۵
- ۲۱-۱. اصول اخلاقی ۵۵
- ۲۲-۱. رتبه و نمونه قوانین مربوط به جرائم سایبری ۵۷
- ۲۳-۱. جزای ۵۹
- ۲۳-۱. ۱-۲۳-۱. سابق ۶۰
- ۲۳-۱. ۲-۲۳-۱. دلایل مجرم در تنگیری بوکر ۶۶
- ۲۳-۱. ۳-۲۳-۱. درخواست برای حذف اتهامات شماره ۲، ۱ و ۴ از فهرست موارد اتهامی ۷۰
- ۲۳-۱. ۴-۲۳-۱. درخواست برای حذف اتهام شماره ۳ از کیفرخواست ۸۲
- ۲۳-۱. ۵-۲۳-۱. حق خوداظهاری ۸۶
- ۲۳-۱. ۶-۲۳-۱. درخواست استرداد وسایل ضبط شده ۸۷
- ۲۳-۱. ۷-۲۳-۱. درخواست برائت از اتهامات شماره ۲، ۱ و ۴ ۸۹
- ۲۳-۱. ۸-۲۳-۱. درخواست برگزاری جلسه محاکمه در اتهامات شماره ۲، ۱ و ۴ ۹۴
- ۲۳-۱. ۹-۲۳-۱. درخواست محکومیت سنگین تر به دلیل وارد شدن ۹۴
- آسیب روانی شدید بر قربانی ۹۵
- ۲۳-۱. ۱۰-۲۳-۱. شهادت متخصصین در زمینه تعقیب ۹۷
- ۲۳-۱. ۱۱-۲۳-۱. حق خطابه بوکر ۹۹
- ۲۳-۱. ۱۲-۲۳-۱. نتیجه گیری ۱۰۰
- ۲۴-۱. خلاصه فصل ۱۰۰

فصل دوم: جمع آوری اطلاعات ۱۰۳

۱-۲. آیا از من جاسوسی می شود؟ ۱۰۴

۱۰۶	۲-۲. زندگی شما تا چه اندازه خصوصی است؟
۱۰۸	۳-۲. هک شدن سایت هکرها
۱۰۸	۴-۲. نمونه‌هایی از نقض حریم خصوصی
۱۱۱	۵-۲. چگونگی جمع‌آوری اطلاعات
۱۱۲	۶-۲. ابزارهای جمع‌آوری اطلاعات
۱۱۶	۷-۲. شناسایی آنلاین
۱۱۷	۸-۲. تهدید اینترنت
۱۱۸	۹-۲. رنوم، جستجو
۱۲۰	۱۰-۲. بیشینگ
۱۲۱	۱۱-۲. ردیاب
۱۲۲	۱۲-۲. رسانه‌های اجتماعی
۱۲۴	۱۳-۲. سرقت هویت
۱۲۴	۱۴-۲. اسکنینگ، استیفینگ و ...
۱۲۶	۱۵-۲. سیمی و بی‌سیم
۱۲۷	۱۶-۲. زیرساخت
۱۲۸	۱۷-۲. تهدید وسایل همراه
۱۲۹	۱۸-۲. تهدید داده (فراداده)
۱۳۰	۱۹-۲. شناسایی فیزیکی
۱۳۱	۲۰-۲. به دام انداختن و تعقیب کردن
۱۳۲	۲۱-۲. مهندسی اجتماعی
۱۳۴	۲۲-۲. شنود
۱۳۶	۲۳-۲. مسائل حقوقی و اخلاقی
۱۳۷	۲۳-۲. حکم
۱۳۷	۲۳-۲. استدلال
۱۶۲	۲۴-۲. خلاصه فصل

فصل سوم: مهندسی اجتماعی.....	۱۶۵
۱-۳. آیا کسی جاسوسی من را می‌کند؟.....	۱۶۶
۲-۳. مثال اسکم.....	۱۶۸
۳-۳. چگونگی جمع‌آوری اطلاعات.....	۱۷۰
۱-۳-۳. زیاده‌گردی.....	۱۷۰
۲-۳-۳. دیدزنی.....	۱۷۲
۳-۳. فیشینگ.....	۱۷۴
۴-۳. جابزار مهندسی اجتماعی.....	۱۷۵
۵-۳. باکینگ و سیط.....	۱۷۸
۶-۳. کاهش صداها از مهندسی اجتماعی.....	۱۸۰
۷-۳. کاهش صداها از مهندسی اجتماعی.....	۱۸۰
۸-۳. حریم خصوصی اطلاعات.....	۱۸۲
۹-۳. مهندسی اجتماعی معکوس.....	۱۸۲
۱۰-۳. نگرانی‌های حقوقی و اخلاقی.....	۱۸۳
۱۱-۳. دیگر مسائل حقوقی.....	۱۸۴
۱۲-۳. خلاصه فصل.....	۲۰۳
فصل چهارم: ردیابی تلفن همراه.....	۲۰۵
۱-۴. تلفن همراه.....	۲۰۶
۲-۴. آیفون ابل.....	۲۰۷
۳-۴. گوگل اندروید.....	۲۰۸
۴-۴. تلفن ویندوز.....	۲۱۰
۵-۴. بلک‌بری.....	۲۱۱
۶-۴. ردیابی تلفن.....	۲۱۲
۷-۴. قانون میهن پرستی.....	۲۱۴

۲۱۴	۸-۴ ردیابی غیرقانونی
۲۱۵	۹-۴ ردیابی برای نظارت
۲۲۲	۱۰-۴ خدمات موقعیت بنیاد
۲۲۴	۱۱-۴ ردیابی سیم کارت
۲۲۶	۱۲-۴ جی پی اس و موقعیت جغرافیایی
۲۲۷	۱۳-۴ گوگل مپ
۲۲۸	۱۴-۴ ردیابی گوگل گلاس؟
۲۲۹	۱۵-۴ سرازدهای حقوقی و اخلاقی
۲۳۵	۱۶-۴ تنه‌های ناشی از حقایق
۲۴۹	۱۷-۴ خلاصه فصل
۲۵۱	فصل پنجم: ردیابی فیزیکی دستگاه‌ها
۲۵۳	۱-۵ چند مثال تاریخی
۲۵۳	۲-۵ اثر انگشت وسیله
۲۵۶	۳-۵ ردیابی برای شناسایی امروز
۲۵۸	۴-۵ نصب برنامه در مقابل وسیله فیزیکی
۲۶۰	۵-۵ ردیابی وسیله فیزیکی
۲۶۵	۶-۵ وسایل امن مورد استفاده علیه شما
۲۶۹	۷-۵ ردیابی موقعیت و فناوری قابل پوشیدن
۲۷۱	۸-۵ نگرانی‌های حقوقی و اخلاقی
۲۷۳	۹-۵ خلاصه فصل
۲۷۵	فصل ششم: ردیابی ویدئو و وب کم
۲۷۶	۱-۶ مثال‌های ردیابی
۲۷۸	۲-۶ سیستم‌های نظارت امنیتی (منزل شخصی)
۲۸۰	۳-۶ سیستم‌های نظارت امنیتی (تجاری)

۲۸۲	۴-۶. حریم خصوصی یا امنیت؟
۲۸۳	۵-۶. سیستم‌های نظارت امنیتی (عمومی)
۲۸۷	۶-۶. سیستم‌های نظارت ماهواره‌ای
۲۸۸	۷-۶. وسایل رایانه شخصی و وب‌کم
۲۹۰	۸-۶. خزافزار
۲۹۱	۹-۶. وسایل همراه
۲۹۲	۱۰-۶. کسوا، بازی
۲۹۵	۱۱-۶. نگرانی‌های حقوقی و اخلاقی
۳۰۶	۱۲-۶. حق دانستن
۳۰۷	۱۳-۶. وظیفه مالک در حفاظت
۳۰۷	۱۴-۶. نظارت در مدار
۳۰۸	۱۵-۶. نظارت ویدئویی صامت
۳۰۸	۱۶-۶. محافظت از اماکن بالقوه خطرناک
۳۰۸	۱۷-۶. خلاصه فصل
۳۱۱	فصل هفتم: سرقت داده و سوءاستفاده از آن
۳۱۱	۱-۷. تهدید داده
۳۱۲	۲-۷. نظارت و سرقت داده
۳۱۴	۳-۷. شگردهای اصلی سرقت داده
۳۱۵	۴-۷. داده ثابت یا ایستا
۳۱۶	۵-۷. محافظت در قبال بدافزار
۳۱۷	۶-۷. شناسایی، محافظت و پیشگیری از نفوذ
۳۱۸	۷-۷. نرم‌افزار دی‌ال‌پی
۳۲۰	۸-۷. سیستم دیواره آتشین یا فایروال
۳۲۱	۹-۷. ابزارهای جداشتدنی

۳۲۳	۱۰-۷. نگرانی‌های سوءاستفاده از داده‌ها
۳۲۴	۱۱-۷. محافظت از طریق رمزگذاری
۳۲۶	۱۲-۷. داده سیار
۳۲۷	۱۳-۷. اسنiffer
۳۳۰	۱۴-۷. اسنiff کردن و حملات دیگر
۳۳۱	۱۵-۷. اسکیم
۳۳۲	۱۶-۷. جرم‌شناسی قانونی دیجیتال
۳۳۳	۱۷-۷. وسایل و برنامه‌ها
۳۳۵	۱۸-۷. جرم‌شناسی قانونی تصادفی
۳۳۵	۱۹-۷. نگرانی‌ها، حقوق و اخلاقی
۳۶۳	۲۰-۷. خلاصه فصل
۳۶۵	فصل هشتم: روش‌های حفاظت
۳۶۵	۱-۸. از خودتان محافظت
۳۶۶	۲-۸. هوشیار باشید، نه بدبین
۳۶۸	۳-۸. امنیت عمومی و تکنیک‌های کاهش ریسک
۳۶۹	۴-۸. سرقت هویت
۳۷۱	۵-۸. مقاوم‌سازی سیستم‌ها
۳۷۴	۶-۸. شناسایی و نظارت عمومی
۳۷۵	۷-۸. جمع‌آوری اطلاعات
۳۸۰	۸-۸. مهندسی اجتماعی
۳۸۲	۹-۸. ردیابی تلفن همراه
۳۸۴	۱۰-۸. ردیابی فیزیکی وسایل
۳۸۹	۱۱-۸. ردیابی وب‌کم
۳۹۰	۱۲-۸. سرقت داده و سوءاستفاده از آن
۳۹۲	۱۳-۸. توصیه‌های امنیتی کلی
۳۹۳	۱۴-۸. خلاصه فصل

بخش دوم: ممانعت، فریب و ضدفریب سازی..... ۳۹۵

فصل نهم: مقدمه بخش دوم..... ۳۹۷

فصل دهم: پیوند زدن ممانعت و فریب کلاسیک با قلمروی امنیت سایبری..... ۴۰۵

۱-۱۰. ممانعت و فریب کلاسیک..... ۴۰۶

۱-۱۰.۱. افشای واقعیات..... ۴۰۸

۱-۱۰.۲. افشای معمولات - ظاهر سازی..... ۴۰۹

۱-۱۰.۳. مخفی کردن واقعیات - پنهان سازی..... ۴۱۱

۱-۱۰.۴. مخفی کردن معمولات..... ۴۱۳

۱-۱۰.۵. پویای ها، فریب..... ۴۱۶

۱-۱۰.۲. ترجمه معاونت و فریب ریان امنیت سایبری..... ۴۲۳

۱-۱۰.۳. به کارگیری ممانعت و فریب امنیت سایبری..... ۴۲۶

۱-۱۰.۳.۱. افشای واقعیات..... ۴۲۷

۱-۱۰.۳.۲. مخفی کردن واقعیات..... ۴۲۹

۱-۱۰.۳.۳. افشای معمولات..... ۴۳۱

۱-۱۰.۳.۴. مخفی کردن معمولات..... ۴۳۷

۱-۱۰.۴. عملیات ممانعت و فریب..... ۴۳۹

فصل یازدهم: نفوذ، فریب و کارزارها..... ۴۴۹

۱-۱۱. تلاش برای نفوذ..... ۴۵۱

۱-۱۱.۲. زنجیره کشتار جمعی..... ۴۵۳

۱-۱۱.۲.۱. شناسایی..... ۴۵۸

۱-۱۱.۲.۲. سلاح سازی..... ۴۵۹

۱-۱۱.۲.۳. رهاسازی..... ۴۶۱

۱-۱۱.۲.۴. بهره برداری..... ۴۶۲

۴۶۳	 ۵-۲-۱۱ کنترل
۴۶۴	 ۶-۲-۱۱ اجرا
۴۶۶	 ۷-۲-۱۱ استمرار
۴۶۷	 ۸-۲-۱۱ زنجیره کشتار سایبری بازگشتی
۴۶۷	 ۳-۱۱ زنجیره فریب
۴۶۷	 ۱-۳-۱۱ تعریف هدف
۴۶۹	 ۲-۳-۱۱ جمع‌آوری هدف
۴۷۰	 ۳-۱۱ سراحی داستان پوششی
۴۷۱	 ۴-۱۱ برنامه‌ریزی
۴۷۲	 ۵-۳-۱۱ آماده‌سازی
۴۷۳	 ۶-۳-۱۱ اجرا
۴۷۳	 ۷-۳-۱۱ نظارت
۴۷۴	 ۸-۳-۱۱ تقویت
۴۷۵	 ۹-۳-۱۱ زنجیره فریب بازگشتی
۴۷۶	 ۴-۱۱ کارزارهای نفوذ
۴۸۲	 ۱۰-۱۱ منابع

فصل دوازدهم: مورد کاوی‌های ممانعت و فریب سایبری

۴۸۵	 ۱-۱۲ کارزار استاکسنت
۴۸۶	 ۱-۱-۱۲ ممانعت و فریب سایبری تاکتیکی
۴۸۸	 ۲-۱-۱۲ ممانعت و فریب سایبری عملیاتی
۴۹۱	 ۳-۱-۱۲ ممانعت و فریب سایبری راهبردی
۴۹۳	 ۴-۱-۱۲ مزایای ممانعت و فریب سایبری استاکسنت
۴۹۵	 ۵-۱-۱۲ چالش‌های ممانعت و فریب سایبری استاکسنت
۴۹۷	 ۲-۱۲ جاسوسی APT

۱۲-۱. مفروضات.....	۵۰۰
۱۲-۲. مرحله شناسایی.....	۵۰۱
۱۲-۳. مرحله تسلیحاتی سازی.....	۵۰۸
۱۲-۴. مرحله رهاسازی.....	۵۱۲
۱۲-۵. مرحله بهره برداری.....	۵۱۷
۱۲-۶. مرحله کنترل/ اجرا.....	۵۲۰
۱۲-۷. مرحله استمرار.....	۵۲۶
۱۲-۸. منابع.....	۵۳۱
فصل سیزدهم: تمرین، مانور و فریب سایبری.....	
۱۳-۱. به کارگیری ممانعت و فریب در تمرین های تیم سرخ/ آبی.....	۵۴۰
۱۳-۲. مثال: مؤلفه های تمرین اسال ایکس ۲.....	۵۴۵
۱۳-۳. مثال: طرح تمرین اسال ایکس.....	۵۴۵
۱۳-۴. مثال: بازی متقابل سرخ/ آبی در تمرین اسال ایکس ۲.....	۵۵۰
۱۳-۵. مثال: نتایج تمرین اسال ایکس.....	۵۵۲
۱۳-۶. منابع.....	۵۵۴
فصل چهاردهم: ملاحظات، انطباق و اشتراک گذاری.....	
۱۴-۱. خطر، پیامدهای ناخواسته، افشا و ناکامی.....	۵۵۸
۱۴-۲. مزایا، چالش ها و معایب ممانعت و فریب سایبری.....	۵۶۱
۱۴-۳. تعقیب پس از بهره برداری.....	۵۶۹
۱۴-۳-۱. عناصر بنیادین راهبردهای شکارچی.....	۵۷۰
۱۴-۳-۲. راهبردهای شکارچی.....	۵۷۲
۱۴-۳-۳. راهبردهای مظنون.....	۵۷۳
۱۴-۴. استاندارد سازی و اشتراک گذاری.....	۵۷۵

۵۷۸	۵-۱۴. منابع
۵۸۳	فصل پانزدهم: مقابله با ممانعت و فریب
۵۸۳	۱-۱۵. تعریف ضد فریب
۵۸۵	۲-۱۵. ساخت تله
۵۸۷	۳-۱۵. اشتراک گذاری داده‌های مربوط به نفوذ
۵۸۷	۱-۳-۱۵. ساخت تله
۵۸۹	۲-۲-۱۵. اشتراک گذاری داده‌های مربوط به نفوذ
۵۹۱	۱۵. اجرای ضد فریب
۵۹۷	۵-۱۵. به کارگیری مدل ضد فریب سایبری در دفاع از شبکه
۵۹۹	۶-۱۵. مدل فرایند ضد فریب سایبری
۶۰۴	۱-۶-۱۵. مورد کاربردی
۶۱۰	۷-۱۵. منابع
۶۱۵	فصل شانزدهم: مدل بلوغ توانمندی
۶۱۷	۱-۱۶. چهارچوب مدل بلوغ ممانعت و فریب سایبری
۶۲۳	۲-۱۶. مدل بلوغ توانمندی - نیروی انسانی
۶۳۶	۳-۱۶. مدل بلوغ توانمندی - خدمات
۶۳۶	۱-۳-۱۶. فرایندهای خدمات
۶۳۶	۲-۳-۱۶. سطوح بلوغ ارائه خدمات ممانعت و فریب سایبری
۶۴۲	۴-۱۶. مدل بلوغ توانمندی - فرایندها
۶۴۶	۵-۱۶. مدل بلوغ توانمندی - فناوری‌ها و فنون
۶۴۶	۱-۵-۱۶. ویژگی‌های عمومی سطوح بلوغ فناوری
۶۴۶	۲-۵-۱۶. ویژگی‌های خاص بلوغ فناوری در بافتار ممانعت و فریب سایبری
۶۵۹	۶-۱۶. دلالت‌ها
۶۶۱	۷-۱۶. منابع

فصل هفدهم: مدیریت چرخه حیات ممانعت و فریب سایبری.....	۶۶۵
۱-۱۷. نگاهی به مدیریت چرخه مارپیچی حیات ممانعت و فریب.....	۶۶۷
۲-۱۷. برنامه‌ریزی.....	۶۶۸
۳-۱۷. پیاده‌سازی.....	۶۷۲
۴-۱۷. استقرار و اجرا.....	۶۷۳
۵-۱۷. تحلیل پس از استقرار.....	۶۷۵

فصل می‌جدهم: نگاه به آینده.....	۶۷۷
۱-۱۸. ادایات ساعره.....	۶۷۷
۲-۱۸. ارزیابی آمادگی.....	۶۷۸
۳-۱۸. مدل‌های نظریه بازار.....	۶۸۰
۴-۱۸. آموزش و یاددهی.....	۶۸۱
۵-۱۸. پژوهش درباره فریب سایبری.....	۶۸۲
۶-۱۸. مدل‌های زیستی و سیستم ایمنی.....	۶۸۳
۷-۱۸. مدل بلوغ توانمندی ضدفریب سازی.....	۶۸۴
۸-۱۸. دفاع فعال ضدفریب سایبری.....	۶۸۶
۹-۱۸. حرکت به پیش.....	۶۸۸
۱۰-۱۸. منابع.....	۶۸۹

پیوست‌ها.....	۶۹۱
پیوست الف) رده‌بندی ممانعت و فریب سایبری.....	۶۹۱
پیوست ب) چک‌لیست‌های نمایه‌های مجازی ساختگی.....	۷۲۷
پیوست پ) اصول فریب قابل بکارگیری در ممانعت و فریب سایبری.....	۷۴۳
پیوست ت) توانمندی راهبردهای ممانعت و فریب.....	۷۵۰
پیوست ث) تعاریف.....	۷۵۸