

کتاب مرجع آموزش عرضی و کوتاه مدت مباحث تخصصی پدافند سایبری

مؤلف : مهندس محمود خالقی دخت

عضو هیأت علمی پژوهشگاه ارتباطات و فناوری اطلاعات

۱۴۰۱

سرشناسه	: خالقی دخت، محمود
عنوان و نام پدیدآور	: مباحث تخصصی پدافند سایبری / محمود خالقی دخت
مشخصات نشر	: تهران: سبک نو ۱۴۰۰
مشخصات ظاهری	: ۱۶۶ ص- ۱۷،۵ در ۲۴،۵-
شابک	: ۹۷۸-۶۲۲-۹۴۶۳۰-۷-۹
وضعیت فهرست نویسی	: فیبا
رده بندی کنگره	: BP ۵۹ / ۴۴ / م۵ ۱۴۰۰
رده بندی دیویی	: ۱۴۱/۲۹۷
شماره کتابشناسی ملی	: ۶۴۴۲۵۳۰۲
اطلاعات رکورد کتابشناسی	: فیبا



عنوان: مباحث تخصصی پدافند سایبری

تألیف: محمود خالقی دخت

صفحه آرای: عباس چراغ چشم

ناشر: سبک نو

نوبت چاپ: چاپ اول، ۱۴۰۱

چاپ و صحافی: قدرولایت

تیراژ: چاپ اول ۵۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۹۴۶۳۰-۷-۹

تعداد صفحات: ۱۶۶ صفحه

قیمت: ۸۵۰۰۰ تومان

کلیه حقوق، اعم از چاپ و تکثیر، نسخه برداری، ترجمه و اقتباس برای سازمان پدافند غیرعامل محفوظ است.

فهرست

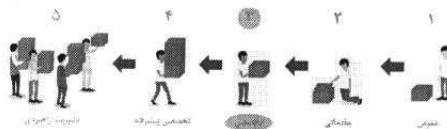
عنوان	صفحه
مقدمه	۱
فصل اول : سرمایه سایبری	۴
۱-۱. تعریف سرمایه سایبری	۴
۲-۱. انواع سرمایه سایبری	۵
۳-۱. نمونه‌های طبقه‌بندی سرمایه‌های سایبری	۶
۴-۱. روش پیشنهادی برای طبقه‌بندی سرمایه‌های سایبری	۱۳
۵-۱. آشنایی با پایگاه داده سرشماری یکپارچه مشترک (CPE)	۱۷
۶-۱. شناسایی و طبقه‌بندی سرمایه‌های سایبری	۲۰
۷-۱. توصیه‌های ضروری	۲۷
فصل دوم : آسیب‌پذیری سایبری	۲۸
۱-۲. تعریف آسیب‌پذیری سایبری	۲۸
۲-۲. انواع آسیب‌پذیری سایبری	۲۹
۳-۲. روش‌های شناسایی آسیب‌پذیری سایبری	۳۱
۴-۲. پویش‌گر آسیب‌پذیری سایبری	۳۲
۵-۲. آشنایی با نمونه‌هایی از پویش‌گرهای آسیب‌پذیری سایبری	۳۴
۶-۲. پایگاه‌های داده آسیب‌پذیری سایبری	۳۵
۷-۲. آشنایی با نمونه‌هایی از پایگاه‌های داده آسیب‌پذیری سایبری	۳۶
۸-۲. تست نفوذ و کاربرد آن در شناسایی آسیب‌پذیری سایبری	۴۷
۹-۲. توصیه‌های ضروری	۴۷
فصل سوم : مخاطره سایبری	۴۹
۱-۳. تعریف تهدید سایبری	۴۹
۲-۳. مخاطرات امنیتی ناشی از تهدید سایبری	۵۰

۵۱		۳-۳. ارزیابی مخاطرات امنیتی
۵۲		۴-۳. مراحل ارزیابی مخاطرات امنیتی
۵۴		۵-۳. پارامترهای ارزیابی مخاطرات امنیتی
۵۶		۶-۳. آشنایی با یک روش فراگیر ارزیابی مخاطرات امنیتی
۶۵		۷-۳. توصیه‌های ضروری
۶۷		فصل چهارم: امنیت سایبری
۶۷		۱-۴. تعریف امنیت سایبری
۷۰		۲-۴. نیازمندی‌های امنیت سایبری
۷۲		۳-۳. نیازمندی‌های امنیتی گوشی تلفن همراه هوشمند
۷۹		۴-۴. نیازمندی‌های امنیتی شبکه ارتباطی
۹۴		۵-۴. توصیه‌های ضروری
۹۵		فصل پنجم: جنگ سایبری
۹۵		۱-۵. تهاجم سایبری
۹۶		۲-۵. انواع تهاجم سایبری
۹۹		۳-۵. آشنایی با پایگاه داده سرشماری و طبقه‌بندی الگوی حمله مشترک (CAPEC)
۱۰۳		۴-۵. روش‌های تشخیص تهاجم سایبری
۱۰۴		۵-۵. فناوری‌های تشخیص انواع تهاجم سایبری
۱۰۶		۱-۵-۵. سامانه‌ی تشخیص و مقابله یا پیش‌گیری از حملات سایبری
۱۰۹		۲-۵-۵. مرکز عملیات امنیت (SOC)
۱۱۵		۶-۵. مرکز اشتراک‌گذاری و تحلیل اطلاعات (ISAC)
۱۲۰		۷-۵. سامانه اشتراک‌گذاری و هشدار سایبری (ISAS)
۱۲۳		۸-۵. توصیه‌های ضروری
۱۲۴		فصل ششم: آمادگی دفاع سایبری
۱۲۴		۱-۶. تمرین و آزمون سایبری
۱۲۷		۲-۶. نمونه‌های تمرین، آزمون و مانور سایبری
۱۲۸		۳-۶. آشنایی با آزمون طوفان سایبری آمریکا
۱۲۸		۴-۶. آشنایی با آزمون پرچم سایبری آمریکا
۱۲۸		۵-۶. آشنایی با آزمون حفاظ سایبری آمریکا

مقدمه

کلیات دوره آموزشی عمومی پدافند سایبری

در نظام آموزش پدافند سایبری کشور، دوره‌های آموزشی کوتاه‌مدت و عرضی در پنج سطح با عناوین دوره‌های عمومی، مقدماتی، تخصصی فنی، تخصصی پیشرفته و مدیریت راهبردی پدافند سایبری طراحی شده است. کتاب حاضر، به عنوان مرجع دوره آموزشی تخصصی فنی پدافند سایبری، توسط مرکز پدافند سایبری کشور، به عنوان عالی‌ترین مرجع برگزاری دوره‌های آموزش عرضی و کوتاه‌مدت پدافند سایبری در کشور، تهیه شده است. شکل (۱)، سطوح پنج‌گانه‌ی نظام آموزشی عرضی و کوتاه‌مدت پدافند سایبری و جایگاه دوره آموزشی عمومی پدافند سایبری در این نظام را نمایش می‌دهد.



شکل (۱): سطوح نظام آموزشی عرضی و کوتاه‌مدت پدافند سایبری و جایگاه دوره آموزشی تخصصی فنی