

متخصص امنیت شبکه‌های بی‌سیم

Certified Wireless Security Professional

اولین مرجع فارسی آزمون بین‌المللی CWSP



مترجم: مهندس سید محمد

نویسندگان: دیوید نکولمن
دیوید وستگات



نشر گستر

به نام خدا

عنوان و نام پدیدآور	متخصص امنیت شبکه‌های بی سیم = Certified Wireless security professional
اولین مرجع فارسی آزمون بین‌المللی CWSP نویسندگان دیوید وستکات... (و دیگران)	
مترجم رضا مقدم	
مشخصات نشر	تهران: نشر گستر، ۱۳۹۲.
مشخصات ظاهری	۵۶۰ ص: مصور، جدول.
شابک	978-600-5883-68-8 ریال: ۳۵۰۰۰۰
وضعیت فهرست‌نویسی	فیا
یادداشت	نویسندگان دیوید وستکات، دیوید کولمن، پیتر مکنتزی، بن میلر.
ناشر	عنوان اصلی:
	CWAP : certified wireless security professional official study guide , c2011.
عنوان دیگر	تألیف گر شبکه‌های بی سیم.
موضوع	مباحثات بی سیم -- آزمون‌ها -- راهنمای مطالعه
موضوع	داده پردازی -- کارمندان -- گواهی‌نامه -- راهنمای مطالعه
شناسه افزوده	دیوید ا.، ۱۹۶۲ - م.
شناسه افزوده	Westcott, David.
شناسه افزوده	مقدم، رضا، -، مترجم
رده بندی کنگره	TK۵۱۰۵/۴
رده بندی دیویی	۶۲/۶۸
شماره کتابشناسی ملی	۸۸۱۲۵



نشر گستر

نام کتاب: متخصص امنیت شبکه‌های بی سیم
 نویسندگان: دیوید کولمن و دیوید وستکات
 مترجم: مهندس رضا مقدم
 نوبت چاپ: اول
 تاریخ چاپ: ۱۳۹۲
 تیراژ: ۱۰۰۰ جلد
 قیمت: ۳۵۰۰۰ تومان
 چاپ: پژمان
 ناشر: انتشارات نشر گستر (۶۶۵۹۱۵۶۱-۳)
 پخش: انتشارات نشر گستر (۶۶۴۳۲۷۰۵)

فهرست مطالب

۱۷	فصل اول: مروری بر امنیت در شبکه‌های بی‌سیم
۲۰	سازمان‌های امنیتی
۲۰	سازمان بین‌المللی استاندارد (ISO)
۲۱	چرا نام آن به جای IOS باشد ISO است؟
۲۲	انجمن مهندسين برن (IEEE)
۲۳	نیروی ضربت مهندسی اینترنت (IEI)
۲۵	اتحادیه Wi-Fi
۲۸	مبانی شبکه‌های بی‌سیم 802.11
۳۰	مبانی امنیتی 802.11
۳۱	محرمانه ماندن داده‌ها
۳۴	احراز هویت، مجوزدهی، اکانتینگ (AAA)
۳۴	قسمت‌بندی
۳۵	مانیتورینگ
۳۵	سیاست
۳۶	تاریخچه امنیت 802.11
۳۶	اصلاحیه امنیتی 802.11i و گواهینامه‌های WPA
۳۸	شبکه امنیتی مستحکم (RSN)
۳۹	آینده امنیت 802.11
۴۳	فصل دوم: امنیت اولیه در شبکه‌های بی‌سیم
۴۶	احراز هویت
۴۶	احراز هویت سیستم باز
۴۸	احراز هویت کلید اشتراکی
۵۱	تمرین 2.1: دیدن فریم‌های احراز هویت کلید اشتراکی و سیستم باز
۵۳	رمزنگاری حریم شخصی معادل سیمی (WEP)

۵۷	تمرین 2.2: دیدن پابلود MSDU فریم‌های داده‌های 802.11
۵۹	شبکه‌های خصوصی مجازی (VPN)
۶۱	پروتکل تونل‌زنی نقطه به نقطه (PPTP)
۶۱	پروتکل تونلینگ لایه 2 (L2TP)
۶۲	امنیت پروتکل اینترنت (IPSec)
۶۳	پیچیدگی پیکربندی
۶۳	مقیاس‌گیری
۶۴	فیلتر MAC
۶۶	قسمت‌بندی SSID
۶۸	مخفی‌سازی SSID
۷۰	تمرین 2.3: دیدن SSIDهای مخفی
۷۳	فصل سوم: رمزنگاری و رمزگزاری
۷۵	مبانی رمزنگاری
۷۶	الگوریتم‌های متقارن و نامتقارن
۷۸	رمزهای دنباله‌ای و بلوکی
۷۹	الگوریتم RC4
۷۹	الگوریتم RC5
۸۰	الگوریتم DES
۸۰	الگوریتم 3DES
۸۱	الگوریتم AES
۸۲	روش‌های رمزنگاری شبکه بی‌سیم
۸۴	الگوریتم WEP
۸۵	WEP در MPDU
۸۷	الگوریتم TKIP
۹۱	TKIP MPDU
۹۳	تمرین 3.1: فریم‌های رمزنگاری شده TKIP
۹۴	الگوریتم CCMP
۹۸	CCMP MPDU
۱۰۰	تمرین 3.2: فریم‌های رمزنگاری شده CCMP
۱۰۱	الگوریتم WPA و WPA2
۱۰۲	پایاده‌سازی‌های لایه دو اختصاصی

فصل چهارم: روش‌های احراز هویت لایه دو پیشرفته.....	۱۰۵
مروری بر احراز هویت شبکه‌های بی‌سیم.....	۱۰۷
مکانیزم AAA.....	۱۰۹
احراز هویت.....	۱۰۹
سناریوی دنیای واقعی.....	۱۱۱
مخزن.....	۱۱۱
اکانت.....	۱۱۳
مکانیزم 802.....	۱۱۴
درخواست‌کننده.....	۱۱۵
سناریوی دنیای واقعی.....	۱۲۱
احراز هویت.....	۱۲۲
بان‌زنی بی‌سیم.....	۱۲۴
سرور احراز هویت.....	۱۲۶
اطلاعات اعتباری درخواست‌کننده.....	۱۳۰
نام‌های کاربری و رمز عبورها.....	۱۳۱
سناریوی دنیای واقعی.....	۱۳۲
گواهینامه‌های دیجیتال و PACها.....	۱۳۲
رمزهای یکبار مصرف.....	۱۳۶
کارت‌های هوشمند و توکن‌های USB.....	۱۳۷
احراز هویت ماشین (کامپیوتر).....	۱۳۹
سناریوی دنیای واقعی.....	۱۴۰
کلیده‌های پیش اشتراکی.....	۱۴۱
کلیده‌های مجاورتی و برجسپهای RFID.....	۱۴۱
بیومتریک.....	۱۴۲
اطلاعات اعتباری سرور احراز هویت.....	۱۴۲
سناریوی دنیای واقعی.....	۱۴۷
رمز اشتراکی.....	۱۴۸
پروتکل‌های احراز هویت قدیمی.....	۱۴۹
پروتکل احراز هویت PAP.....	۱۴۹
پروتکل احراز هویت CHAP.....	۱۵۰
پروتکل احراز هویت MS-CHAP.....	۱۵۰
پروتکل احراز هویت MS-CHAPv2.....	۱۵۰

۱۵۱	پروتکل احراز هویت EAP
۱۵۵	پروتکل‌های EAP ضعیف
۱۵۵	پروتکل EAP-MD5
۱۵۶	پروتکل EAP-LEAP
۱۵۹	پروتکل EAP قوی
۱۶۱	پروتکل EAP-PEAP
۱۶۴	پروتکل EAP-PEAPv0 (EAP-MSCHAPv2)
۱۶۵	پروتکل EAP-PEAPv0 (EAP-TLS)
۱۶۵	پروتکل EAP-PEAPv1 (EAP-GTC)
۱۶۶	پروتکل EAP-TLS
۱۶۸	پروتکل EAP-TLS
۱۷۰	پروتکل EAP-TLS
۱۷۱	PAC ها
۱۷۴	پروتکل‌های EAP مختلف
۱۷۶	پروتکل EAP-SIM
۱۷۶	پروتکل EAP-AKA
۱۷۷	تمرین 4.1: تغییرات فریم 802.1X/EAP
۱۸۱	فصل پنجم: تولید کلید رمزنگاری دینامیک
۱۸۳	مزایای رمزنگاری دینامیک
۱۸۷	تمرین 5.1: WEP پویا
۱۸۹	شبکه امنیتی قوی (RSN)
۱۹۶	عنصر اطلاعات RSN
۲۰۱	احراز هویت و مدیریت کلید (AKM)
۲۰۵	تمرین 5.2: احراز هویت و مدیریت کلید
۲۰۷	سلسله مراتب کلید RSNA
۲۰۸	کلید سشن اصلی (MSK)
۲۰۸	کلیدهای اصلی
۲۱۰	کلیدهای موقتی
۲۱۲	هندشیک چهار طرفه
۲۱۵	تمرین 5.3: هندشیک چهار طرفه
۲۱۶	هندشیک کلید گروه

۲۱۸	هندشیک کلید نظیر
۲۱۹	پیوستگی‌های امنیتی RSNA
۲۲۰	ایجاد عبارت عبور در PSK
۲۲۳	رومینگ و کلیدهای دینامیک
۲۲۵	فصل ششم: امنیت شبکه‌های بی‌سیم SOHO
۲۲۷	WPA, WPA2- Personal
۲۲۹	کلیدهای پیش‌اشتراکی (PSK) و عبارات عبور
۲۳۲	تجهیز 6.1: ایجاد PSK عبارت عبور
۲۳۳	ریسک‌های WPA, WPA2- Personal
۲۳۴	آنتروپی
۲۳۸	PSK منحصر به فرد
۲۴۰	ساختار حفاظت شده WPS, WPA2- Personal
۲۴۰	معماری WPS
۲۴۱	گزینه‌هایی ساختار امنیتی
۲۴۲	پروتکل ثبت نام کننده
۲۴۳	حالت پیکربندی درون باندی
۲۴۳	حالت پیکربندی خارج از باند
۲۴۴	راهنمایی‌ها و الزامات برای مقادیر PIN
۲۴۴	تنظیمات اولیه شبکه‌های بی‌سیم
۲۴۵	سناریوی دکمه فشاری WPS
۲۴۵	افزودن ثبت نام شده دکمه فشاری WPS
۲۴۷	روش‌های برتر امنیتی SOHO
۲۴۹	فصل هفتم: رومینگ امن سریع 802.11
۲۵۲	تاریخچه رومینگ 802.11
۲۵۲	آستانه‌های رومینگ کلاینت
۲۵۴	دست به دست شدن اکسس پوینت به اکسس پوینت
۲۵۶	RSNA
۲۵۷	ارتباط امنیتی کلید اصلی جفتی PMKSA
۲۶۱	کشینگ PMK
۲۶۳	پیش احراز هویت
۲۶۵	کشینگ کلید فرصت طلب (OKC)

۲۶۸	سناریوی دنیای واقعی
۲۶۹	FSR اختصاصی
۲۶۹	انتقال BSS سریع (FT)
۲۷۳	عناصر اطلاعاتی
۲۷۴	دامنه اتصال تحرک‌پذیری اولیه FT
۲۷۶	انتقال BSS سریع از طریق هوا
۲۷۷	انتقال BSS سریع از طریق DS
۲۷۹	استاندارد 802.11
۲۸۰	Voice Enterprise و Voice Personal
۲۸۱	رومینگ لایه 3
۲۸۴	رفع اشکال
۲۸۵	SCA رومینگ
۲۸۹	فصل هشتم: ریسک‌های امنیتی شبکه بی‌سیم
۲۹۱	دسترسی راگ (ناهنجار) غیرمجاز
۲۹۲	دستگاه‌های راگ
۲۹۵	ممانعت در برابر راگ
۲۹۸	سناریوی دنیای واقعی
۲۹۸	استراق سمع
۲۹۹	استراق سمع اتفاقی
۳۰۱	سناریوی دنیای واقعی
۳۰۱	استراق سمع بدخواهانه
۳۰۲	ریسک‌های استراق سمع
۳۰۴	ممانعت از استراق سمع
۳۰۵	حملات احراز هویت
۳۰۸	حملات محرومیت از سرویس
۳۰۹	حملات DoS لایه یک
۳۱۵	حملات DoS لایه دو
۳۲۰	جعل مک آدرس
۳۲۵	ربایش بی‌سیم
۳۲۷	شکستن رمزنگاری
۳۲۹	حملات نظیر به نظیر

۳۳۱	 سوء استفاده‌ها از اینترفیس مدیریت
۳۳۲	 حملات. اختصاصی تولیدکننده
۳۳۳	 آسیب‌رسانی فیزیکی و ربایش
۳۳۵	 مهندسی اجتماعی
۳۳۶	 سناریوی دنیای واقعی
۳۳۷	 دستیابی عمومی و هات اسپات بی‌سیم
۳۳۹	 فصل چهارم: حسابرسی امنیتی شبکه‌های بی‌سیم
۳۴۲	 حسابرسی امنیتی شبکه‌های بی‌سیم
۳۴۴	 حسابرسی لایه OSI
۳۴۹	 حسابرسی لایه SI
۳۵۲	 تست نفوذ
۳۵۵	 حسابرسی زیرساخت بی‌سیم
۳۵۵	 حسابرسی مهندسی اجتماعی
۳۵۶	 سناریوی دنیای واقعی
۳۵۶	 حسابرسی WIPS
۳۵۷	 مستندسازی حسابرسی
۳۵۸	 توصیه‌های حسابرسی
۳۵۹	 ابزارهای حسابرسی امنیتی بی‌سیم
۳۶۳	 ابزارهای مبتنی بر لینوکس
۳۶۷	 ابزارهای مبتنی بر ویندوز
۳۶۹	 فصل دهم: مانیتورینگ امنیتی بی‌سیم
۳۷۱	 سیستم‌های تشخیص و ممانعت از نفوذ بی‌سیم (WIDS و WIPS)
۳۷۲	 اجزاء زیرساختی WIDS / WIPS
۳۷۶	 مدل‌های معماری WIDS / WIPS
۳۸۳	 سنسورهای رادیوی چندگانه
۳۸۴	 قرار دادن سنسورها
۳۸۶	 طبقه‌بندی دستگاه
۳۸۸	 تشخیص راگ
۳۹۳	 تضعیف راگ
۳۹۶	 ردگیری دستگاه
۳۹۹	 ستاریوی دنیای واقعی

۴۰۳	تحلیل WIDS / WIPS
۴۰۳	تحلیل امضا
۴۰۴	تحلیل رفتاری
۴۰۶	تحلیل پروتکل
۴۰۸	تحلیل طیف
۴۱۰	تمرین 10.1: تحلیل طیف
۴۱۱	تحلیل قانونی
۴۱۲	تجسس غیرمجاز
۴۱۳	مانیپولیشن
۴۱۳	اعمال سیاست
۴۱۵	آلارمها و تذکرات
۴۱۹	مشبتهای کاذب
۴۲۰	گزارشها
۴۲۰	استاندارد 802.11n
۴۲۴	WIPS اختصاصی
۴۲۴	کلوکیگ
۴۲۵	حفاظت فریم مدیریت
۴۲۶	استاندارد 802.11w
۴۲۷	سناریوی دنیای واقعی
۴۲۹	فصل یازدهم: VPNها، دسترسی از راه دور و سرویسهای دسترسی میهمان
۴۳۱	تکنولوژی VPN در معماری 802.11
۴۳۲	سرویس VPN
۴۳۳	سناریوی دنیای واقعی
۴۳۴	کلاینت VPN
۴۳۵	کنترلرهای بی‌سیم: سرور VPN برای دسترسی کلاینت
۴۳۶	امنیت کلاینت VPN در هات اسپات عمومی
۴۳۷	VPNهای کنترلر به کنترلر و VPNهای سایت به سایت
۴۳۸	VPNهای مورد استفاده برای حفاظت از لینکهای پل
۴۳۹	دسترسی از راه دور
۴۳۹	اکسس پوینت دوردست
۴۴۱	تونلینگ RAP

۴۴۲	برجینگ RAP
۴۴۳	تونلینگ انشعاب RAP
۴۴۴	شبکه دفتر شاخه مجازی
۴۴۵	هات اسپات و شبکه‌های دسترسی عمومی
۴۴۶	پورتال محدود
۴۴۷	قابلیت‌ها
۴۴۸	قسط بندی
۴۴۸	مکان‌های احراز هویت مبتنی بر کاربر
۴۵۱	فصل دوازدهم: ترانزیت امنیتی شبکه‌های بی‌سیم
۴۵۳	مروری بر قابلیت‌های امنیتی بی‌سیم
۴۵۴	تلفیق سرویس (SIP)
۴۵۴	سیستم توزیع (DS)
۴۵۵	اکسس پوینت‌های مستقل
۴۵۷	کنترل‌های بی‌سیم
۴۶۴	جداسازی آدرس MAC
۴۶۴	شبکه‌های توری یا مش
۴۶۷	برجینگ بی‌سیم
۴۶۷	کنترل مشترک
۴۶۸	انتخاب فرکانس دینامیک
۴۶۹	فرکانس‌های رادیویی دینامیک
۴۷۰	کنترل دسترسی مبتنی بر مکان
۴۷۰	بروز خطا و آماده باش
۴۷۱	مدیریت دستگاه
۴۷۲	پروتکل‌هایی برای مدیریت
۴۷۲	پروتکل SNMP
۴۷۳	اجزاء
۴۷۳	ساختار اطلاعات مدیریتی
۴۷۴	ویرایشها و تفاوتها
۴۷۴	پروتکل SNMPV1
۴۷۴	پروتکل SNMPV2
۴۷۵	پروتکل SNMPV3

۴۷۵	مدیریت مبتنی بر CLI
۴۷۶	پورتهای کنسول و سریال
۴۷۷	پروتکل تلنت
۴۷۷	پروتکل امن SSH
۴۷۸	پروتکل HTTPS
۴۷۹	پروتکل CAPWAP و LWAPP
۴۸۰	سیستم مدیریت شبکه بی‌سیم
۴۸۲	سرویس‌های RADIUS / LDAP
۴۸۲	سرویس‌های پراکسی
۴۸۳	قابلیت‌ها و اجزاء
۴۸۳	مقادیر خصوصیات (Attribute-Value)
۴۸۴	نسبتهای اختصاصی
۴۸۴	تخصیص VLAN
۴۸۴	پراکسی دیتابیس‌های کار
۴۸۵	سناریوی دنیای واقعی
۴۸۵	پراکسی از یک پراکسی (Realm)
۴۸۶	تلفیق سازی
۴۸۷	پروتکل LDAP
۴۸۷	سرویس Active Directory
۴۸۸	دیتابیس‌های SQL
۴۸۸	انتخاب نوع EAP
۴۸۸	ساختار معماریها و مقیاس بندی
۴۸۹	ساختار تک سایتی
۴۹۰	سایت‌های مستقل توزیع شده
۴۹۱	شبکه‌های بی‌سیم چندگانه موجود در مکانهای مختلف
۴۹۱	سایت‌های توزیع شده، احرازهویت متمرکز و امنیت
۴۹۲	امنیت و سایت‌های توزیع شده، احرازهویت متمرکز
۴۹۴	سرورهای RADIUS تعبیه شده داخلی
۴۹۴	خطایابی RADIUS
۴۹۵	مقادیر تایمر
۴۹۶	تایمرهای EAP
۴۹۶	درخواست EAP

۴۹۶	درخواست هویت EAP
۴۹۷	تایمرهای RADIUS
۴۹۷	تایم‌اوت ارسال مجدد احراز هویت RADIUS
۴۹۷	تایمرهای مبتنی بر اکسس پوینت
۴۹۸	تایم‌وات سشن
۴۹۸	تایمر عدم فعالیت
۴۹۹	پیما: شبکه بی‌سیم
۵۰۰	سیاست‌های احراز هویت تولیدکننده
۵۰۰	زیورساز کلید عمومی (PKI)
۵۰۳	گونه‌های نام‌های دامنه
۵۰۳	PKI پیشرفته
۵۰۴	کنترل دسترسی شبکه بی‌سیم
۵۰۵	تخصیص نقش
۵۰۵	فایروال‌های تعبیه شده داخلی/تلفظ شده
۵۰۷	لیست کنترل دسترسی
۵۰۸	کنترل دسترسی شبکه (NAC)
۵۰۹	گیتوی‌های رمزنگاری پیشرفته
۵۱۱	فصل سیزدهم: سیاست‌های امنیت بی‌سیم
۵۱۴	سیاست کلی
۵۱۵	سیاست‌گذاری
۵۱۸	مدیریت سیاست
۵۲۰	سیاست کاربردی
۵۲۰	سیاست رمز عبور
۵۲۲	سیاست RBAC
۵۲۳	سیاست کنترل تغییر
۵۲۴	احراز هویت و سیاست رمزنگاری
۵۲۵	سیاست مانتورینگ شبکه بی‌سیم
۵۲۵	سیاست نقطه انتهایی
۵۳۰	سیاست استفاده قابل قبول
۵۳۰	امنیت فیزیکی
۵۳۱	سیاست دفتر دوردست

۵۳۲	 مقررات دولتی و صنعتی
۵۳۳	 امریه 8100.2 وزارت دفاع آمریکا (DoD)
۵۳۵	 استانداردهای پردازش اطلاعات فدرال (FIPS) ۱۴۰-۲
۵۳۸	 قانون Sarbanes-Oxley(SOX) ۲۰۰۲
۵۴۳	 قانون پاسخگویی و قابلیت حمل بیمه سلامت (HIPAA)
۵۴۵	 استاندارد صنعت کارت پرداخت (PCI)
۵۵۰	 شبکه‌های دنیای واقعی
۵۵۲	 گزارش‌های تحقیقی
۵۵۳	 توصیه‌ها سیاست شبکه‌های بی‌سیم 802.11