

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

آموزش هک ویپ

رویکرد بالا به پایین

www.ketab.ir

مترجمان:

کبری خورشیدفار علیرضا پوربهرام

سرشناسه

دوی و دی، هیمانشو

Dwivedi, Himanshu

عنوان و نام پدیدآور: آموزش هک ویپ رویکرد بالا به پایین/ نویسنده هایمن شودویدی؛ مترجمان کبری خوشرفتار، علیرضا

پوربھرام۔

مشخصات نشر

رشت: دلکام، ۱۴۰۰.

٢٤٧: ص.

مشخصات ظاهری

978-622-6229-96-8: ٩٥٠٠٠٠ ریا

شاہک

فيا

وضعیت فهرست نویسی

Hacking VoIP : protocols, attacks, and countermeasures, c2009. عنوان اصلي:

یادداشت

:کتابنامه: ص. ۲۴۷.

یادداشت

تلفن اینترنتی -- تدابیر ایمنی

موضوع

Internet telephony -- Security measures:

موضوع

شبکه‌های کامپیوتری -- تدابیر ایمنی

موضوع

Computer networks -- Security measures:

موضوع

خوشرفتار، کبری، ۱۳۶۳، مترجم

شناسه افزوده

پوربھرام، علیرضا، ۱۳۷۰-، مترجم

شناسه افزوده

TK 51-511165 :

رده بندی کنگره

• ۱۹۹۵:

ردہ بندی دیوپی

AFZDQFY:

شماره کتابشناسی ملی

اطلاعات رکورد کتابشناسی: فیپا



لنام کتاب: آموزش هک ویپ، رویکرد بالا به پایین / مترجمان: کبری خوشرفتار، علیرضا پوربهرام /

/ نوبت چاپ و تاریخ انتشار: چاپ اول - سال ۱۴۰۰ / شمارگان: ۲۰۰ جلد /

/ تعداد صفحات: ۲۴۷، وزیري / شماره استاندارد بين المللي، کتاب: ۸-۹۶-۶۲۲۹-۶۲۲-۹۷۸/

ناشر: انتشارات دلکام

/ تلفن: ۰۹۳۸۷۶۵۳۰۹۲ / - قیمت در سراسر کشور: ۶۵۰۰۰۰ ریال

آدرس، وب سایت انتشارات دلکام: www.delkampus.ir

E-Mail: nikdelpb95@gmail.com

کلیه حقوق برای مولف محفوظ است

پیشگفتار

نزدکی صوفی کلماتی به نرسندی هست... هر گاهی نغمه خود را در سینه روز...

صحنه پرستاره هست... نغمه آن نغمه دردم بهانه یار...

اصطلاح وب به استفاده از تلفن بر روی شبکه‌ی اینترنت جهت برقراری تماس‌های صوتی و حتی تصویری، اشاره دارد و در واقعیت، یک تلفن تحت شبکه می‌باشد که مجهز به تکنولوژی IP و دارای پروتکل‌های مرتبط با انتقال داده در شبکه‌های کامپیوتری نیز است. تلفن‌های تحت شبکه بسیار شبیه به تلفن‌های عادی از نظر ظاهری هستند ولی دارای فناوری IP و نرم افزارها و سیستم عامل‌های مخصوص به خود نیز می‌باشند و قابلیت اتصال به یک شبکه LAN یا WAN را نیز دارا هستند. یکی از اصلی ترین کاربردهای استفاده از تکنولوژی وب در کشور، کاهش هزینه‌های مخابراتی است که البته به راحتی می‌توان با استفاده از تجهیزات مبتنی بر وب، دفتر کاری یک شرکت را در شهرهای مختلف به یکدیگر متصل نمود. مسئله بسیار مهم در مورد وب، مباحث امنیتی و هک می‌باشد. از زمینه‌های مهمی که هکرها می‌توانند نفوذ کنند، اطلاعات آرسو شده در سازمان‌ها و شرکت‌ها بوده که بدون توجه و استفاده نکردن از فایروال‌ها و سرویس‌ها (یعنی سرویس‌هایی که باعث محافظت اطلاعات محرمانه شما می‌شود)، موجب می‌شوند تا سرویس‌های شبکه از کار بیفتد و عملاً باعث روبرو شدن با خسارات جبران ناپذیری هم از لحاظ مالی و هم از دست دادن اعتماد مشتریان سازمان خواهد شد. شایع‌ترین مسئله پیرامون وب، مربوط به هک شدن وب بوده که می‌تواند به سوء استفاده از خط تلفن اشاره کرد که در این کتاب نیز به آن پرداخته می‌شود.

این کتاب، برگردان کتاب مرجع وب، اثر هایمن شو دوییدی می‌باشد و به صورت تخصصی، تمرکز کتاب بر روی مسئله هک وب می‌باشد. باید توجه داشت که در هر کتابی، کاستی‌هایی وجود دارد و مطمئناً اشکالاتی نگارشی، دور از چشمان تیم ترجمه کتاب نیز وجود داشته است، از همه آنهایی که این کتاب را می‌خوانند و به خصوص مدیران، کارشناسان، مهندسين و دانشجویان عزیز می‌خواهیم که نقدها و پیشنهادات سازنده‌ی خود را از طریق راه‌های ارتباطی زیر، به اطلاع برسانند.

✉ کبری خوشرفتار (کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار)

✉ علیرضا پورپیرام (کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار)

k.khosrafar@gmail.com

Alirezapourbahram@gmail.com

پایباسب فریدون

فهرست مطالب

شماره صفحه

عنوان

فصل اول: مقدمه ای بر امنیت VoIP

۱۱	۱-۱ مقدمه
۱۲	۲-۱ چرا VoIP
۱۳	۳-۱ اساس VoIP
۱۳	۱-۳-۱ نحوه کار
۱۴	۲-۳-۱ پروتکل ها
۱۸	۴ اصول امنیت VoIP

۲۱	۵-۱ بردارهای حمله
۲۲	۶-۱ جمع بندی فصل

فصل دوم: سیگنالینگ-امنیت SIP

۲۵	۱-۲ مقدمه
۲۶	۲-۲ اساس SIP
۲۷	۳-۲ پیام های SIP
۲۹	۱ ۳-۲ ایجاد یک تماس VoIP با روش های SIP
۳۱	۲ ۳-۲ سرشماری و ثبت نام
۳۲	۳-۳-۲ سرشماری دستگاه های SIP در یک شبکه
۳۲	۴ ۳-۲ ثبت با دستگاه های تصدیق هویت SIP
۳۴	۵-۳-۲ تصدیق
۳۶	۶-۳-۲ رمزگذاری
۳۷	۷ ۳-۲ انتخاب SIP با TLS

۳۸	۴-۲- اساس SIP با S/MIME
۳۹	۴-۲-۱- حملات امنیت SIP
۴۵	۴-۲-۲- ابزارهایی برای انجام حمله
۴۷	۴-۲-۳- حمله مرد میانی
۴۸	۴-۲-۴- سرقت ثبت
۵۱	۴-۲-۵- اسپوofینگ سرورهای پروکسی SIP و رجسترها
۵۲	۴-۲-۵-۱- انکار سرویس از طریق پیام BYE
۵۴	۴-۲-۵-۳- انکار سرویس از طریق REGISTER
۵۵	۴-۲-۵-۴- انکار سرویس از طریق ثبت مجدد
۵۶	۴-۲-۵-۵- اساس SIP فای
۵۷	۴-۲-۶- جمع بندی فصل
	فصل سوم: سیگنال دهی و امنیت H.323
۶۰	۳-۱- مقدمه
۶۱	۳-۲- اصول امنیتی H.323
۶۴	۳-۳- تصدیق
۶۴	۳-۳-۱- رمزگذاری متقارن
۶۴	۳-۳-۲- تبدیل رمز عبور
۶۶	۳-۳-۳- کلید عمومی
۶۶	۳-۳-۴- اساس مجوز
۶۸	۳-۴- اساس H.323 حمله امنیتی
۷۱	۳-۴-۱- بازیابی رمز عبور H.323
۷۳	۳-۴-۲- حمله پاسخ H.323

۷۷	۳-۴-۳- اسپوفینگ نقطه پایانی H.323
۸۰	۴-۴-۳- شمارش اسم مستعار E.164
۸۲	۵-۴-۳- حملات هاب E.164
۸۳	۶-۴-۳- انکار سرویس از طریق NTP
۸۹	۵-۳- جمع بندی فصل

فصل چهارم: رسانه و امنیت RTP

۹۲	۱-۴- مقدمه
۹۳	۲-۴- اصول RTP
۹۴	۳-۴- حملات امنیتی RTP
۹۵	۴-۴- ضبط بسته از نقاط پایانی مختلف MITM
۹۸	۵-۴- استفاده از Cain & Abel برای حملات MITM
۱۰۰	۶-۴- استفاده از Wireshark
۱۰۲	۷-۴- استراق سمع فعال
۱۰۳	۱-۷-۴- درج صوتی
۱۰۸	۲-۷-۴- جایگزینی صدا
۱۰۹	۳-۷-۴- حملات انکار سرویس
۱۱۱	۴-۷-۴- پارگی جلسه یا RTCP BYE
۱۱۳	۸-۴- جمع بندی فصل

فصل پنجم: سیگنالینگ و امنیت رسانه IAX

۱۱۶	۱-۵- مقدمه
۱۱۷	۲-۵- تأیید هویت IAX
۱۲۰	۳-۵- حملات امنیتی IAX

۱۳۷ ۴-۵- جمع بندی فصل

فصل ششم: حمله به زیرساخت VoIP

۱۴۰ ۱-۶- مقدمه

۱۴۰ ۲-۶- اسنiff VoIP ویژه فروشنده

۱۴۳ ۳-۶- تلفن سخت

۱۴۳ ۱-۳-۶- سازش پرونده پیکربندی تلفن

۱۴۵ ۲.۳-۶- بارگذاری پرونده پیکربندی مخرب

۱۴۷ ۳-۳-۶- بهره برداری از نقاط ضعف SNMP

۱۴۹ ۴-۳-۶- مدیریت تماس سیسکو و مرکز تماس آوایا

۱۵۰ ۵-۳-۶- استفاده از Nmap برای پویش دستگاه‌های VoIP

۱۵۱ ۶-۳-۶- پویش رابط مدیریت و Nikto

۱۵۲ ۴-۶- کشف خدمات آسیب‌پذیر با Nessus

۱۵۳ ۱ ۴-۶- سیستم پست صوتی پیام رسانی مدولار

۱۵۶ ۲-۴-۶- جعل هویت سرور زیرساخت

۱۵۹ ۵-۶- جمع بندی فصل

فصل هفتم: تهدیدات امنیتی غیرمرسوم VoIP

۱۶۲ ۱-۷- مقدمه

۱۶۴ ۲-۷- فیشینگ VoIP

۱۶۵ ۳-۷- پخش پیغام

۱۶۸ ۴-۷- دریافت تماس‌ها

۱۷۱ ۵-۷- ایجاد درخواست آزاد

۱۷۳ ۶-۷- اسپوفینگ شناسه تماس

۱۸۱	۷-۷- استراق سمع ناشناس و تغییر مسیر تماس
۱۸۳	۷-۷-۱- هرزنامه از طریق تلفن اینترنتی
۱۸۵	۷-۷-۲- SPIT و شهر
۱۸۷	۷-۷-۳- SPIT سبک با اسکایپ/گوگل تالک
۱۸۹	۷-۸- جمع بندی فصل

فصل هشتم: راه‌حل‌های ویپ خانگی

۱۹۲	۸-۱- مقدمه
۱۹۳	۸-۲- راه‌حل‌های ویپ تجاری
۱۹۷	۸-۳- تماس با استراق سمع (RTP)
۲۰۲	۸-۴- تزریق صدا (RTP)
۲۰۶	۸-۵- نام کاربری/ بازیابی گذرواژه (SIP)
۲۰۸	۸-۶- راه‌حل‌های VoIP مبتنی بر PC
۲۱۵	۸-۷- راه‌حل‌های تلفن SOHO
۲۱۹	۸-۸- جمع بندی فصل

فصل نهم: ویپ ایمن

۲۲۱	۹-۱- مقدمه
۲۲۳	۹-۲- اساس RTP امن
۲۲۴	۹-۲-۱- حفاظت از رسانه و رسانه‌ها با رمز AES
۲۲۵	۹-۲-۲- تأیید صحت و حفاظت تمامیت با HMAC-SHA1
۲۲۶	۹-۲-۳- روش توزیع کلید SRTP
۲۲۶	۹-۲-۴- اساس ZRTP و ZFONE
۲۲۹	۹-۳- دیوار آتش و کنترلرهای پهنای جلسه