

به نام خدا



مؤسسه فرهنگی هنری
دیبانگران تهران

امنیت شبکه

و

ابزارهای تست نفوذ

مؤلفان :

مهندس ابوالفضل یوسفی راد

هنرآموز رسمی ا.و.پ و مدرس دانشگاه

مهندس مادح شکری

مدرس دانشگاه

هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

امنیت شبکه و ابزارهای تست نفوذ

مؤلفان : ابوالفضل یوسفی راد، مادح شگری

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه آرایی: خانم نازنین نصیری

طرح روی جلد: سحر نژاد محمدی

چاپ: درج عقیق

نوبت چاپ: سوم

تاریخ نشر: ۱۳۹۸

تیراژ: ۵۰ جلد

قیمت: ۷۰۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۵۱۶-۹

ISBN: ۹۷۸-۶۰۰-۱۲۴-۵۱۶-۹

نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱- تلفن: ۰۴۶-۶۶۴۱۰۰۴۶-

کد پستی: ۱۳۱۴۹۸۳۱۸۵

فروشگاههای اینترنتی:

www.mftbook.ir

www.dibagarantehran.com

نشانی تلگرام: @mftbook

نشانی اینستاگرام: Dibagaran_publishing

سرشناسه : یوسفی راد، ابوالفضل، ۱۳۶۵-

عنوان و نام پدید آور : امنیت شبکه و ابزارهای تست نفوذ/مؤلفان: ابوالفضل یوسفی راد، مادح شگری.

مشخصات نشر: تهران- دیباگران تهران -۱۳۹۵

مشخصات ظاهری: ۲۳۰ ص. مصور.

شابک: ۹۷۸-۶۰۰-۱۲۴-۵۱۶-۹

وضعیت فهرست نویسی : فیبا

موضوع: شبکه های کامپیوتری - تدابیر ایمنی

موضوع : computer networks-security measures

موضوع : کامپیوترها- ایمنی اطلاعات

موضوع: computer security

موضوع : هکرها

موضوع : Hackers

رده بندی کنگره: ۱۳۹۵ الف ۸ ی ۹ / ۵۹ / TK ۵۱۰۵

رده بندی دیویی : ۰۰۵/۸

شماره کتابشناسی ملی : ۴۴۹۹۶۹۸

فهرست مطالب

9.....	مقدمه مؤلف.....
10.....	پیشگفتار.....
11.....	فصل اول: مفاهیم امنیت شبکه.....
12.....	1-1 مقدمه.....
12.....	1-2 مفهوم امنیت.....
13.....	1-3 جنبه های اصلی امنیت.....
13.....	1-3-1 جنبه محرمانگی.....
14.....	1-3-2 جنبه جامعیت.....
15.....	1-3-3 جنبه در دسترس پذیری.....
15.....	1-3-4 مثال هایی از جنبه های امنیت.....
15.....	1-4 تعریف امنیت اطلاعات.....
16.....	1-4-1 تمهیدات لازم برای امنیت اطلاعات.....
16.....	1-4-2 رخدادهای ناخوشایند.....
16.....	1-5 تعریف امنیت شبکه.....
16.....	1-5-1 تاریخچه امنیت شبکه.....
17.....	1-5-2 علل و ضرورت امنیت شبکه.....
17.....	1-5-3 آمار رخدادهای امنیتی.....
19.....	1-6 تعاریف.....
19.....	1-6-1 دارایی.....
19.....	1-6-2 تصدیق اصالت.....
20.....	1-6-3 مجازشناسی.....
20.....	1-6-4 حفظ حریم خصوصی.....
21.....	1-6-5 خط مشی امنیتی.....
21.....	1-6-6 مکانیزم امنیتی.....
21.....	1-6-7 سرویس امنیتی.....
21.....	1-6-8 آسیب پذیری.....
22.....	1-6-9 تهدید.....
22.....	1-6-10 حمله امنیتی.....

23	1-6-11	انواع کامپیوترهای شبکه
23	1-6-12	خط فرمان
24	1-6-13	معرفی IP
25	1-6-14	پورت
26	1-6-15	چگونگی Telnet به یک پورت
27	1-6-16	زبان 133t Speak
29		فصل دوم: مهاجمین و انواع حملات در شبکه
30	2-1	فرایند موجود در حملات
31	2-1-1	مهاجم
33	2-1-2	انواع حملات در شبکه
48	2-1-3	آسیب پذیری
49	2-1-4	نتایج حمله
51	2-1-5	اهداف حمله
52		فصل سوم: روش‌های جمع‌آوری و کسب اطلاعات
53	3-1	مقدمه
54	3-2	روش‌های FOOTPRINTING
55	3-2-1	جمع‌آوری اطلاعات اولیه به کمک Nslookup
56	3-2-2	شناسایی بازه شبکه قربانی به کمک ping Sweep
57	3-2-3	تشخیص و شناسایی نوع سیستم عامل قربانی به کمک NMAP
59	3-2-4	تشخیص و شناسایی پورت‌های باز به کمک NMAP
59	3-2-5	تشخیص و شناسایی اطلاعات دامنه و ماشین‌های فعال به کمک Whois
64	3-2-6	بدست آوردن اطلاعات تماس و شناسایی سیستم‌های فعال به کمک WDE
66	3-2-7	ترسیم نقشه شبکه به کمک Friendly Pinger
71	3-3	جمع‌آوری اطلاعات با ابزار FIREBUG
74	3-4	مهندسی اجتماعی
75	3-4-1	اصول مهندسی اجتماعی
76	3-4-2	چرایی مهندسی اجتماعی
76	3-4-3	انواع مهندسی اجتماعی
78	3-4-4	انجام حملات مهندسی اجتماعی
83	3-5	مراحل بعد از FOOTPRINTING

84	فصل چهارم: معرفی ابزارهای پویش
85.....	4-1 مقدمه
86.....	4-2 ابزار PING
89.....	4-3 ابزار IPEYE
90.....	4-4 ابزار IPSECSAN
91.....	4-4-1 انواع حالات IPsec
92.....	4-4-2 انواع پروتکل های IPsec
95.....	4-5 ابزار HPING2 و HPING3
97.....	4-6 ابزار TRACEROUTE و PATH ANALYZE PRO
99.....	4-7 پویش با ابزار ZENMAP
108.....	4-8 پویش و عیب یابی شبکه توسط MEGAPING
115	فصل پنجم: ابزارهای شکستن کلمه عبور
116.....	5-1 مقدمه
117.....	5-2 چگونگی ایجاد HASH از کلمات عبور به کمک PWDUMP7
119.....	5-3 ابزار LOPHTCRACK
123.....	5-4 ابزار LCP
126.....	5-5 پنج ابزار کاربردی برای شکستن کلمات عبور
126.....	5-6 طول مناسب برای کلمات عبور
128.....	5-7 روش های مقابله با شکستن کلمات عبور
130	فصل ششم: ابزارهای مخفی کردن
131.....	6-1 مقدمه
131.....	6-2 مخفی کردن با ابزار STEALTH FILE TOOL
134.....	6-3 مخفی کردن فایل ها با جریان های NTFS
137.....	6-4 پیدا کردن فایل های مخفی با استفاده از ابزار ADS SPY
139.....	6-5 مخفی کردن داده با SNOW STEGANOGRAPHY
141.....	6-6 پنهان نگاری متون به کمک QUICKSTEGO
145	فصل هفتم: انواع بدافزارها و ابزارهای موجود در آنها
146.....	7-1 مقدمه
146.....	7-2 انواع بدافزارها
146.....	7-2-1 ویروس

146.....	7-2-2 کرم
147.....	7-2-3 اسب تروا
147.....	7-2-4 در پشته
147.....	7-2-5 نرم افزار جاسوسی
148.....	7-2-6 Rootkit
148.....	7-2-7 ابزار نفوذ
148.....	7-2-8 تبلیغات ناخواسته
149.....	7-3 هک REMOTE با PRORAT
155.....	7-4 بسته بندی تروجان با ابزار ONE FILE EXE MAKER
158.....	7-5 کنترل REMOTE با HTTP RAT
161.....	7-6 ساخت سرور تروجان با THEEF
167.....	7-7 ساخت سرور تروجان با ابزار BIODOX TROJAN
170.....	فصل هشتم: ابزارهای شنود.....
171.....	8-1 مقدمه
171.....	8-2 شنود شبکه با CAIN & ABEL
175.....	8-3 شنود شبکه با WINARPAATTACKER TOOL
178.....	8-4 شنود شبکه با WIRESHARKE
181.....	فصل نهم: نفوذ به شبکه های بی سیم.....
182.....	9-1 مقدمه
183.....	9-2 مفاهیم موجود در شبکه های بی سیم
183.....	9-3 مکانیزم های احراز هویت در شبکه های بی سیم
189.....	9-4 حملات موجود در شبکه های بی سیم
190.....	9-5 تغییر MAC ADDRESS در ویندوز
191.....	9-6 تکنیک های نفوذ به شبکه بی سیم
192.....	9-7 روش های افزایش امنیت شبکه های بی سیم
192.....	9-8 راه اندازی سرور احراز هویت
192.....	9-8-1 پیکربندی سرور RADIUS
208.....	ضمیمه 1- دستورات پایه لینوکس.....
209.....	ضمیمه 2- برخی اصطلاحات.....
209.....	1- فایروال
209.....	2- Honeypot

209.....	3- امنیت فیزیکی.....
210.....	ضمیمه 3- مراحل نصب سیستم عامل کالی لینوکس.....
220.....	ضمیمه 4- لیست پورت های کامپیوتر.....
220.....	1- پورت های 0 تا 1023.....
220.....	2- پورت های 1024 تا 49151.....
220.....	3- پورت های 49152 تا 65535.....
230.....	منابع و ماخذ.....

خط‌مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌های است که بتواند خواسته‌های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "مهندس ابوالفضل یوسفی راد-مهندس ماحد شکری" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
Publishing@mftmail.com

مقدمه مؤلف

تقدیم به همسر مهربانم

به پاس قدردانی از قلبی آکنده از عشق و معرفت که محیطی سرشار از سلامت، امنیت، آرامش و آسایش برای من فراهم آورده است .

ابوالفضل یوسفی راد

تقدیم به پدر و مادر عزیز و مهربانم

که در سختی‌ها و دشواری‌های زندگی همواره یآوری دلسوز و فداکار و پشتیبانی محکم و مطمئن برایم بوده‌اند .

مادح شکری

پیشگفتار

به نام خداوند جان و خرد

کزین برتر اندیشه برنگذرد

امروزه امنیت شبکه بخش قابل توجهی از بودجه IT سازمانها را به خود اختصاص می دهد. ترس از خطر حملات اینترنتی ، بودجه بیشتری را به سازمانها تحمیل می کند. مراجع و کتابهای قدیمی که در زمینه امنیت شبکه موجود است ، در دنیای امروز کاربردی ندارد. حتی کتاب هایی که در حوزه رمزنگاری وجود دارد ، چندان کاربردی به نظر نمی رسد ، زیرا آنها مسائل ریاضیاتی موجود در الگوریتمهای رمزنگاری را مطرح می کنند. قاعدتاً مباحث تئوری چندان کمکی به شما در این زمینه نخواهد کرد. بنابراین برای حفظ امنیت سازمان خود باید از منابع مختلف استفاده نمائید. به همین دلیل تصمیم گرفته شد کتابی کاربردی در حوزه امنیت شبکه و معرفی ابزارهای تست نفوذ تالیف گردد. در این کتاب سعی شده مطالب به صورت ساده و گام به گام آموزش داده شود ، به نحوی که مخاطبین محترم براحتی بتوانند مطالب مورد نظر خود را بیاموزند. این کتاب در 9 فصل سازماندهی شده است. در فصول 1 و 2 ، مفاهیم پایه و اصطلاحات موجود در امنیت شبکه و در فصول 3 تا 9 روش های نفوذ و مقابله با هک به صورت عملی آموزش داده شده است. البته امیدواریم مخاطبان این کتاب از مطالب موجود در آن برای افزایش سطح امنیت در شبکه های کامپیوتری استفاده نمایند. نکته قابل توجه در زمینه انتشار این کتاب تلاش و محبت مدیریت و کارکنان انتشارات دیباگران می باشد که لازم است در اینجا از آنان تقدیر و تشکر نمائیم. در پایان از همه مخاطبین ، دانشجویان و اساتید محترمی که این کتاب را انتخاب نموده اند ، تقاضامندیم با ارائه نظرات ، انتقادات و پیشنهادات خود ما را در جهت اصلاح و ارتقای سطح علمی کتاب در ویرایش های بعدی یاری نمایند.

مادح شکری

madeh.shokri@gmail.com

ابوالفضل یوسفی راد

usefirad@gmail.com