



تست نفوذ

مؤلف:
رؤيا مرشدی



۱۳۹۹



سرشناسه	مرشدی، رؤیا، ۱۳۶۷ -
عنوان و نام پدیدآور	تست نفوذ/ مؤلف رؤیا مرشدی.
مشخصات نشر	تهران: اساطیر پارسی: چاپار، ۱۳۹۹.
مشخصات ظاهری	۱۲۱ ص.: مصور.: ۵/۱۴×۲۱/۵ س.م.
شابک	۹۷۸-۶۰۰-۸۸۹۰-۸۸-۱
وضعیت فهرست‌نویسی	فیا
یادداشت	یادداشت
موضوع	سیستم عامل لینوکس
موضوع	Linux
موضوع	آزمایش نفوذ(ایمن سازی کامپیوتر)
موضوع	Penetration testing (Computer security)
موضوع	سیستم های عامل(کامپیوتر)
موضوع	Operating systems (Computers)
رده‌بندی کنگره	QAV۶/۷۶
رده‌بندی دیویی	۰۰۵/۴۳۳
شماره کتاب‌شناسی ملی	۷۲۷۴۲۵۰



تهران: ۸۸۹۹۶۸۰ - ۰۹۱۲۱۹۶۰۲۱۴
تهران- خیابان ولی عصر (عج)- بالاتر از زرتشت
کوچه نوربخش- پلاک ۴۰- نشر چاپار
تست نفوذ

مؤلف: رؤیا مرشدی

صفحه‌آرا: رؤیا مرشدی

طراح جلد: سرور محمدی بزنج

ناظر فنی چاپ: محمد محمدی

چاپ اول ۱۳۹۹

شمارگان ۱۰۰۰ نسخه

شابک: ۹۷۸-۶۰۰-۸۸۹۰-۸۸-۱ ISBN: 978-600-8890-88-1

حق هرگونه چاپ و انتشار محفوظ است.

قیمت: ۲۴.۰۰۰ تومان

مقدمه مؤلف

در جوامع امروزی، تلاش برای بهبود وضعیت کنونی در هر زمان و مکان و هر موقعیتی به یک اصل تبدیل شده است. در واقع یکی از اصول مهم در تمامی سطوح و گرایشهای کلیه استانداردها، در پیش گرفتن فرآیندهایی است که بهبود وضعیت را در پی داشته باشد. بخصوص این امر در تکنولوژی اطلاعات یکی از اصول تخطی ناپذیر و غیر قابل اجتناب است. حال اگر وارد حیطه شبکه های کامپیوتر و نیز نرم افزارهای گوناگون شویم، باید برای این فرآیند، راههای متناسب با آن را در اتخاذ کنیم. یکی از عمومی ترین و مهمترین این راه حلها در این کتاب به معرفی آن میپردازیم، استفاده از فرآیند تست نفوذ با کالی لینوکس است. کالی لینوکس یک توزیع از لینوکس بر پایه دبیان می باشد که با هدف انجام تست نفوذ و شناسایی نقاط آسیب پذیری انواع سیستم های کامپیوتری طراحی و توسعه داده شده است. یک متخصص امنیت و حتی یک توسعه دهنده وب یا اپلیکیشن، باید به اندازه کافی با این سیستم عامل و روش های نفوذ آن آشنایی داشته باشد و حتی خود با استفاده از این سیستم عامل یا برنامه های مشابه به تست برنامه ها و پروژه هایی که طراحی کرده است بپردازد تا نقاط آسیب پذیری آن را شناسایی و نسبت به رفع آنها اقدام نماید. یادگیری این کتاب برای مدیران شبکه و متخصصان و کارشناسان امنیتی طراحی شده است تا گام بزرگی در زمینه تست نفوذ بردارند. مطالعه این کتاب برای آنهایی که می خواهند در زمینه تست نفوذ فعالیت داشته باشند توصیه می شود. تمامی مطالب ارائه شده در این کتاب صرفاً جنبه آموزشی دارند و به منظور بهینه سازی امنیت سیستم ها و آموزش متخصصان امنیتی با جدیدترین راهکارهای امنیتی ارائه شده است. در نتیجه هر نوع استفاده نادرست از این مطالب بر عهده شخص می باشد. امید است از مطالب بهره مفید ببرید.

فهرست مطالب

فصل ۱ - فصل اول	۱۲
۱-۱- کالی لینوکس	۱۴
۱-۲- ابزارهای مختلف کالی لینوکس	۱۵
۱-۳- تست نفوذ	۱۷
۱-۴- گزارش دهی	۱۸
۱-۵- مستندات موقت	۱۹
۱-۶- مسیر در کالی لینوکس	۲۰
۱-۷- منو کالی لینوکس	۲۰
۱-۸- دستورهای which, locate, find	۲۱
۱-۹- مدیریت سرویس های کالی لینوکس	۲۲
۱-۱۰- پسورد پیش فرض روت	۲۳
۱-۱۱- سرویس SSH	۲۳
۱-۱۲- سرویس HTTP	۲۵
۱-۱۳- محیط Bash	۲۶
فصل ۲ - فصل دوم	۳۲

- ۱-۲- ابزار Netcat..... ۳۴
- ۲-۲- اتصال به یک پورت TCP یا UDP..... ۳۴
- ۳-۲- گوش دادن بر روی یک پورت TCP/UDP..... ۳۵
- ۴-۲- انتقال فایل به وسیله ابزار Netcat..... ۳۷
- ۵-۲- مدیریت ریموت با استفاده از ابزار Netcat..... ۳۹
- ۶-۲- ابزار وایرشارک..... ۴۰
- ۷-۲- درک صحیح Network Dumps..... ۴۱
- ۸-۲- کپچر و نمایش فیلترها..... ۴۲
- ۹-۲- دنبال کردن جریان TCP..... ۴۵
- ۱۰-۲- ابزار TCP Dump..... ۴۶

فصل ۳- فصل سوم ۵۰

- ۱-۳- Footprinting..... ۵۲
- ۲-۳- گوگل هکنینگ..... ۵۲
- ۳-۳- جمع آوری ایمیلها..... ۵۵
- ۴-۳- متدلوژی های جمع آوری اطلاعات..... ۶۰
- ۵-۳- DNS Enumeration..... ۶۱
- ۶-۳- Nslookup و DNSstuff..... ۶۱
- ۷-۳- مفهوم Whois و ARIN Lookup..... ۶۳
- ۸-۳- تحلیل خروجی Whois..... ۶۴
- ۹-۳- سرشماری whois..... ۶۷
- ۱۰-۳- ابزار ریکان (Recon-ng)..... ۶۸
- ۱۱-۳- پیدا کردن آدرس های بازه شبکه..... ۷۷

۷۸.....	۱۲-۳- شناسایی انواع مختلف رکوردهای DNS
۷۸.....	۱۳-۳- نحوه کار traceroute در footprinting
۸۰.....	۱۴-۳- استفاده از Email Tracking
۸۰.....	۱۵-۳- نحوه کار Web Spider ها
۸۱.....	۱۶-۳- مراحل انجام footprinting
۸۱.....	۱۷-۳- نت گرفت (Netcraft)
۸۲.....	۱۸-۳- مهندسی اجتماعی
۸۳.....	۱۹-۳- انواع رایج حملات
۸۴.....	۲۰-۳- مهندسی اجتماعی مبتنی بر انسان
۸۵.....	۲۱-۳- مهندسی اجتماعی مبتنی بر کامپیوتر
۸۵.....	۲۲-۳- حملات داخلی
۸۵.....	۲۳-۳- حملات phishing
۸۷.....	۲۴-۳- URL obfuscation
۸۷.....	۲۵-۳- پیشگیری از مهندسی اجتماعی

فصل ۴- فصل چهارم..... ۸۹

۹۱.....	۱-۴- اسکن
۹۱.....	۲-۴- اسکن پورت، شبکه و آسیب پذیری
۹۴.....	۳-۴- تکنیک های ping sweep
۹۴.....	۴-۴- تشخیص ping sweep ها
۹۵.....	۵-۴- اسکن پورتها و شناسایی سرویسها
۹۵.....	۶-۴- مقابله با اسکن پورت
۹۶.....	۷-۴- سوئیچ های دستور Nmap

- ۹۹.....HPING2 -۸-۴
- اسکن های SYN, IDLE, NULL, XMAS -۹-۴
- ۹۹.....Stealth
- ۱۰۱.....انواع Flag های ارتباط TCP -۱۰-۴
- ۱۰۳.....ابزارهای هک -۱۱-۴
- ۱۰۴.....تکنیک های War-Dialing -۱۲-۴
- ۱۰۵.....ابزارهای هک -۱۳-۴
- ۱۴-۴ -تکنیک های Banner-Grabbing و شناسایی سیستم عامل
- ۱۰۵.....
- ۱۵-۴ -رسم دیاگرام شبکه ای از دستگاه های آسیب پذیر ۱۰۷
- ۱۶-۴ -چگونه از سرورهای پروکسی در انجام حمله استفاده میشوند؟
- ۱۰۷.....
- ۱۷-۴ -ناشناس کننده ها چگونه کار میکنند؟
- ۱۰۸.....
- ۱۸-۴ -تکنیک های Http Tunneling
- ۱۰۹.....
- ۱۹-۴ -ابزار Httpunnel برای ویندوز
- ۱۰۹.....
- ۲۰-۴ -تکنیک های IP Spoofing
- ۱۱۰.....
- ۲۱-۴ -Enumeration
- ۱۱۲.....
- ۲۲-۴ -مقابله با Null Session
- ۱۱۳.....
- ۲۳-۴ -SNMP Enumeration چیست؟
- ۱۱۵.....
- ۲۴-۴ -مقابله با SNMP enumeration
- ۱۱۶.....
- ۲۵-۴ -مراحل در enumeration
- ۱۱۷.....
- ۲۶-۴ -مراجع
- ۱۱۹.....