

راهنمای سریع

# ارزیابی شبکه‌های کامپیوتری با

# NMAP

امید توکلی

زهره بهمن اصفهانی

سارا صادقیان

سرشناسه : مارش، نیکلاس

Marsh, Nicholas

عنوان و نام پدیدآور : راهنمای سریع ارزیابی شبکه‌های کامپیوتری با NMAP [نیکولاس مارش]؛ امید توکلی، زهره بهمن اصفهانی، سارا صادقیان.

مشخصات نشر : اصفهان: امید توکلی، ۱۳۹۴.

مشخصات ظاهری : ۱۶۰ ص: مصور (بخشی رنگی)، جدول.

شابک : 978-600-04-4531-7

وضعیت فهرست‌بندی : فیسبا

یادداشت عنوان ملی: Nmap 6 cookbook: the fat-free guide to network scanning, 2015.

موضوع : شبکه‌های کامپیوتری -- نظارت -- برنامه‌های کامپیوتری

موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی -- برنامه‌های کامپیوتری

موضوع : کتاب‌ها -- رمزها -- اطلاعات

شناسه افزوده : توکلی، امید، ۱۳۵۶ - مترجم

شناسه افزوده : بهمن اصفهانی، زهره، ۱۳۵۰ - مترجم

شناسه افزوده : صادقیان، سارا، ۱۳۶۶ - مترجم

رده بندی کنگره : ۵۰۴/۲۴ ۱۳۹۴م/۱K۵۴۸۵

رده بندی دیویی : ۰۰۴/۲۴

شماره کتابشناسی ملی: ۴۱۶۹۶۹۷

راهنمای سریع ارزیابی شبکه‌های کامپیوتری با NMAP

پدید آورندگان: امید توکلی، زهره بهمن اصفهانی، سارا صادقیان

چاپ: پیشگام

صحافی: پیشگام

شمارگان: ۵۰۰

قیمت: ۱۰۰۰۰ تومان

چاپ: اول / ۱۳۹۴

شابک: 978-600-04-4531-7

فهرست مطالب

|    |                               |
|----|-------------------------------|
| ۱۲ | فصل ۱                         |
| ۱۲ | ۱-۱: مروری بر شبکه            |
| ۱۲ | ۱-۲: مدل OSI                  |
| ۱۳ | ۱-۳: لایه فیزیکی              |
| ۱۳ | ۱-۴: لایه پیوند داده          |
| ۱۴ | ۱-۵: لایه شبکه                |
| ۱۴ | ۱-۶: لایه انتقال              |
| ۱۶ | ۱-۷: لایه جلسه                |
| ۱۶ | ۱-۸: لایه نمایش               |
| ۱۶ | ۱-۹: لایه کاربرد              |
| ۱۶ | ۱-۱۰: مدل TCP/IP              |
| ۱۷ | ۱-۱۱: لایه دسترسی             |
| ۱۷ | ۱-۱۲: لایه شبکه               |
| ۱۷ | ۱-۱۳: لایه انتقال             |
| ۱۷ | ۱-۱۴: لایه کاربرد             |
| ۱۷ | ۱-۱۵: پروتکل IP               |
| ۱۸ | ۱-۱۶: کلاس های آدرس IP        |
| ۱۹ | ۱-۱۷: Subnet Mask             |
| ۲۰ | ۱-۱۸: مروری عملی بر Nmap      |
| ۲۱ | فصل ۲                         |
| ۲۱ | ۲- مقدمه ای بر Nmap           |
| ۲۲ | ۲-۱: اطلاع رسانی در مورد Nmap |
| ۲۲ | ۲-۲: گزارش اشکالات            |
| ۲۳ | ۲-۳: همکاری در کد نویسی       |

|    |                                              |
|----|----------------------------------------------|
| ۲۳ | ۲-۴: پیشنهاد در مورد روش های بررسی در TCP/IP |
| ۲۳ | ۲-۵: حمایت از Nmap                           |
| ۲۳ | ۲-۶: قرار دادهای به کار رفته در این کتاب     |
| ۲۵ | فصل ۳                                        |
| ۲۵ | ۳-۱: نصب Nmap                                |
| ۲۵ | ۳-۲: نظر نویسنده                             |
| ۲۶ | ۳-۳: نصب Nmap بر روی ویندوز                  |
| ۲۹ | ۳-۴: نصب Nmap بر روی Linux و Unix            |
| ۲۹ | ۳-۵: نصب بسته های مورد نیاز Nmap در Linux    |
| ۳۲ | ۳-۶: نصب Nmap روی Mac OS X                   |
| ۳۵ | فصل ۴                                        |
| ۳۵ | ۴-۱: مروری بر پویش پایه                      |
| ۳۶ | ۴-۲: پویش یک هدف                             |
| ۳۸ | ۴-۳: پویش چندین هدف                          |
| ۳۹ | ۴-۴: پویش محدوده ای از آدرس های IP           |
| ۴۰ | ۴-۵: پویش زیر شبکه                           |
| ۴۱ | ۴-۶: پویش لیستی از اهداف                     |
| ۴۲ | ۴-۷: پویش تصادفی اهداف                       |
| ۴۳ | ۴-۸: حذف اهداف از پویش                       |
| ۴۴ | ۴-۹: حذف اهداف با استفاده از لیست            |
| ۴۵ | ۴-۱۰: پویش تهاجمی                            |
| ۴۵ | ۴-۱۱: پویش ، هدف IPv6                        |
| ۴۷ | فصل ۵                                        |
| ۴۷ | ۵-۱: مروری بر گزینه های شناسایی              |
| ۴۷ | ۵-۲: Don't ping                              |
| ۴۸ | ۵-۳: انجام پویش ping                         |
| ۵۰ | ۵-۴: TCP SYN ping                            |

|    |                                      |
|----|--------------------------------------|
| ۵۰ | TCP ACK Ping : ۵-۵                   |
| ۵۱ | UDP Ping: ۵-۶                        |
| ۵۲ | SCTP INIT Ping : ۵-۷                 |
| ۵۳ | ICMP ECHO Ping : ۵-۸                 |
| ۵۳ | ICMP Timestamp ping : ۵-۹            |
| ۵۴ | ICMP Address Mask ping : ۵-۱۰        |
| ۵۵ | IP Protocol Ping: ۵-۱۱               |
| ۵۶ | ARP ping: ۵-۱۲                       |
| ۵۶ | Traceroute: ۵-۱۳                     |
| ۵۷ | DNS معکوس: ۵-۱۴                      |
| ۵۸ | ۵-۱۵: غیر فعال کردن DNS معکوس        |
| ۵۹ | ۵-۱۶: روش های دیگر بازگرداندن Nmap   |
| ۶۰ | ۵-۱۷: تعیین سرور DNS به صورت دستی    |
| ۶۰ | ۵-۱۸: ایجاد لیست میزبان              |
| ۶۲ | فصل ۶                                |
| ۶۲ | ۶-۱: مروری بر گزینه های پویش پیشرفته |
| ۶۳ | ۶-۲: پویش TCP SYN                    |
| ۶۳ | ۶-۳: پویش TCP connect                |
| ۶۴ | ۶-۴: پویش UDP                        |
| ۶۵ | ۶-۵: پویش TCP NULL                   |
| ۶۶ | ۶-۶: پویش TCP FIN                    |
| ۶۷ | ۶-۷: پویش xmas                       |
| ۶۷ | ۶-۸: پویش TCP تنظیم شونده            |
| ۶۹ | ۶-۹: پویش TCP ACK                    |
| ۶۹ | ۶-۱۰: پویش پروتکل IP                 |
| ۷۰ | ۶-۱۱: ارسال بسته های Raw Ethernet    |
| ۷۱ | ۶-۱۲: ارسال بسته های IP              |

|    |                                        |
|----|----------------------------------------|
| ۷۲ | فصل ۷                                  |
| ۷۲ | ۷-۱: مروری بر گزینه های پویش پورت      |
| ۷۳ | ۷-۲: پویش سریع                         |
| ۷۳ | ۷-۳: پویش پورتهای خاص                  |
| ۷۴ | ۷-۴: پویش پورتهای با استفاده از نام    |
| ۷۵ | ۷-۵: پویش پورتهای بر اساس پروتکل       |
| ۷۶ | ۷-۶: پویش تمام پورتهای                 |
| ۷۶ | ۷-۷: پویش پورتهای با آرایش             |
| ۷۷ | ۷-۸: پویش بی علامت پورتهای             |
| ۷۸ | ۷-۹: نمایش پورت های باز                |
| ۷۹ | فصل ۸                                  |
| ۷۹ | ۸-۱: مروری بر تشخیص سیستم عامل         |
| ۷۹ | ۸-۲: تشخیص سیستم عامل                  |
| ۸۰ | ۸-۳: اعمال TCP/IP Fingerprint          |
| ۸۱ | ۸-۴: حدس سیستم عامل های نامشخص         |
| ۸۲ | ۸-۵: تشخیص ویرایش سرویس                |
| ۸۲ | ۸-۶: رفع اشکالات مربوط به پویش نسخه ها |
| ۸۳ | ۸-۷: پویش RPC                          |
| ۸۵ | فصل ۹                                  |
| ۸۵ | ۹-۱: مروری بر گزینه های زمان بندی      |
| ۸۶ | ۹-۲: پارامترهای زمان بندی              |
| ۸۶ | ۹-۳: الگوهای زمانی                     |
| ۸۷ | ۹-۴: حداقل تعداد عملیات های موازی      |
| ۸۸ | ۹-۵: حداکثر تعداد عملیات های موازی     |
| ۸۸ | ۹-۶: حداقل تعداد اهداف                 |
| ۸۹ | ۹-۷: حداکثر تعداد اهداف                |
| ۹۰ | ۹-۸: مقدار اولیه RTT Timeout           |

|     |                                             |
|-----|---------------------------------------------|
| ۹۱  | ۹-۹: حداکثر مقدار RTT Timeout               |
| ۹۱  | ۹-۱۰: حداکثر تکرارها (تلاش مجدد)            |
| ۹۲  | ۹-۱۱: تنظیم مقدار TTL بسته ها               |
| ۹۲  | ۹-۱۲: زمان سپری شده میزبان                  |
| ۹۳  | ۹-۱۳: حداقل تاخیر درپویش                    |
| ۹۴  | ۹-۱۴: حداکثر تاخیر درپویش                   |
| ۹۴  | ۹-۱۵: حداقل تعداد بسته ها                   |
| ۹۵  | ۹-۱۶: حداکثر اندازه بسته ها                 |
| ۹۶  | فصل ۱۰                                      |
| ۹۶  | ۱۰-۱: مروری بر تکنیک های گریز دیوار آتش     |
| ۹۷  | ۱۰-۲: بسته های چند قسمتی                    |
| ۹۷  | ۱۰-۳: تعیین MTU                             |
| ۹۸  | ۱۰-۴: استفاده از طعمه                       |
| ۹۹  | ۱۰-۵: پویش zombie                           |
| ۱۰۰ | ۱۰-۶: تنظیم دستی شماره پورت مبدأ            |
| ۱۰۰ | ۱۰-۷: اضافه نمودن اطلاعات تصادفی            |
| ۱۰۱ | ۱۰-۸: پویش تصادفی                           |
| ۱۰۱ | ۱۰-۹: جعل کردن آدرس MAC                     |
| ۱۰۳ | ۱۰-۱۰: ارسال checksums اشیاء                |
| ۱۰۴ | فصل ۱۱                                      |
| ۱۰۴ | ۱۱-۱: مروری بر گزینه های خروجی              |
| ۱۰۵ | ۱۱-۲: ذخیره خروجی در فایل متنی              |
| ۱۰۵ | ۱۱-۳: ذخیره خروجی در فایل XML               |
| ۱۰۶ | ۱۱-۴: خروجی grep                            |
| ۱۰۷ | ۱۱-۵: خروجی از تمام فایل های پشتیبانی شونده |
| ۱۰۸ | ۱۱-۶: نمایش آمار پویش                       |
| ۱۰۹ | فصل ۱۲                                      |

|     |                                         |
|-----|-----------------------------------------|
| ۱۰۹ | ۱۲-۱: مروری بر رفع مشکلات و اشکال زدایی |
| ۱۱۰ | ۱۲-۲: دریافت کمک                        |
| ۱۱۰ | ۱۲-۳: نمایش نسخه Nmap                   |
| ۱۱۱ | ۱۲-۴: خروجی verbose                     |
| ۱۱۱ | ۱۲-۵: اشکال زدایی                       |
| ۱۱۳ | ۱۲-۶: دلایل وضعیت پورت                  |
| ۱۱۳ | ۱۲-۷: نمایش انحصاری پورت های باز        |
| ۱۱۵ | ۱۲-۸: دنبال نمودن بسته ها               |
| ۱۱۵ | ۱۲-۹: پیکربندی زبان                     |
| ۱۱۶ | ۱۲-۱۰: نتایج رابط شبکه مورد استفاده     |
| ۱۱۷ | فصل ۱۳                                  |
| ۱۱۷ | ۱۳-۱: مروری بر Zmap                     |
| ۱۱۸ | ۱۳-۲: کاربران ویندوز                    |
| ۱۱۸ | ۱۳-۳: کاربران یونیکس و لینوکس           |
| ۱۱۸ | ۱۳-۴: کاربران Mac OS X                  |
| ۱۱۸ | ۱۳-۵: عملیات های اصلی zenmap            |
| ۱۱۹ | ۱۳-۶: نتایج zenmap                      |
| ۱۱۹ | ۱۳-۷: الگوی پوشش                        |
| ۱۲۱ | ۱۳-۸: ویرایشگر الگو                     |
| ۱۲۱ | ۱۳-۹: مشاهده پورت های باز               |
| ۱۲۲ | ۱۳-۱۰: مشاهده نقشه شبکه                 |
| ۱۲۴ | ۱۳-۱۱: نمایش نقشه های شبکه              |
| ۱۲۴ | ۱۳-۱۲: مشاهده جزئیات میزبان             |
| ۱۲۴ | ۱۳-۱۳: مشاهده تاریخچه پوشش              |
| ۱۲۶ | ۱۳-۱۴: مقایسه نتایج پوشش                |
| ۱۲۶ | ۱۳-۱۵: ذخیره پوشش ها                    |
| ۱۲۸ | فصل ۱۴                                  |



|     |                                                   |
|-----|---------------------------------------------------|
| ۱۲۸ | ۱۴-۱: موتور اسکریپت nmap (NSF).....               |
| ۱۲۹ | ۱۴-۲: اجرای اسکریپت.....                          |
| ۱۲۹ | ۱۴-۳: اجرای چند اسکریپت.....                      |
| ۱۳۰ | ۱۴-۴: دسته های اسکریپت.....                       |
| ۱۳۱ | ۱۴-۵: اجرای اسکریپت ها بر اساس دسته های کاری..... |
| ۱۳۲ | ۱۴-۶: اجرای چندین دسته اسکریپت.....               |
| ۱۳۳ | ۱۴-۷: رفع اشکال اسکریپت ها.....                   |
| ۱۳۴ | ۱۴-۸: به روز رسانی پایگاه داده اسکریپت.....       |
| ۱۳۵ | فصل ۱۵.....                                       |
| ۱۳۵ | ۱۵-۱: مروری بر Ndiff.....                         |
| ۱۳۵ | ۱۵-۲: مقایسه پوشش ها با استفاده از Ndiff.....     |
| ۱۳۶ | ۱۵-۳: نمود جزئیات Ndiff.....                      |
| ۱۳۷ | ۱۵-۴: نمود خروجی XML.....                         |
| ۱۳۸ | فصل ۱۶.....                                       |
| ۱۳۸ | ۱۶-۱: نکات و ترفندها.....                         |
| ۱۳۸ | ۱۶-۲: ترکیب چند گزینه.....                        |
| ۱۳۹ | ۱۶-۳: پوشش با نمود تعاملی.....                    |
| ۱۴۰ | ۱۶-۴: پوشش شبکه از راه دور.....                   |
| ۱۴۰ | ۱۶-۵: Wireshark.....                              |
| ۱۴۲ | ۱۶-۶: Scanme.insecure.org.....                    |
| ۱۴۳ | فصل ۱۷.....                                       |
| ۱۴۳ | ۱۷-۱: Nping.....                                  |
| ۱۴۳ | ۱۷-۲: Nping بدون گزینه.....                       |
| ۱۴۴ | ۱۷-۳: پنهان کردن بسته های ارسالی.....             |
| ۱۴۴ | ۱۷-۴: پنهان سازی کلیه بسته ها.....                |
| ۱۴۵ | ۱۷-۵: تعیین تعداد بسته های ارسالی.....            |
| ۱۴۵ | ۱۷-۶: Ping چندین هدف.....                         |

- ۱۴۶..... ۱۷-۷: تعیین نرخ و سرعت ارسال
- ۱۴۶..... ۱۷-۸: تاخیر میان ارسال ها در Ping
- ۱۴۷..... ۱۷-۹: ایجاد و ارسال داده :
- ۱۴۷..... ۱۷-۱۰: Ping با استفاده از TCP و UDP
- ۱۴۹..... ۱۷-۱۱: ARP PING
- ۱۵۰..... ۱۸: فصل
- ۱۵۰..... ۱۸-۱: Ncat
- ۱۵۰..... ۱۸-۲: تست سرور وب:
- ۱۵۱..... ۱۸-۳: تست سرور SMTP
- ۱۵۲..... ضمیمه A
- ۱۵۳..... ضمیمه B
- ۱۵۶..... ضمیمه C
- ۱۵۷..... ضمیمه D
- ۱۵۸..... ضمیمه E