

دیوار آتش در سیستم عامل لینوکس

(از دیدگاه یک هکر)

مؤلف : حمیدرضا فندی

با همکاری : گروه پیشگامان فناوری اطلاعات و امنیت



**NAGHOOS
PUBLICATION**

سرشناسه
عنوان و نام پدیدآور

: قنبری ، حمید رضا ، ۱۳۶۸-

: دیوار آتش در سیستم عامل Linux (از دیدگاه یک هکر)/مؤلف: حمید رضا قنبری
با همکاری گروه پیشگامان فناوری اطلاعات پریزاد

: تهران: انتشارات ناقوس، ۱۳۹۵.

مشخصات نشر
مشخصات ظاهری

: ۷۰ص : مصور، جدول.

: ۹۷۸-۹۶۴-۳۷۷-۹۶۱-۰۰۰ بها : ۹۵۰۰۰ ریال (به همراه CD)

شابک

: سیستم عامل لینوکس

موضوع

: Linux

موضوع

: فایروال (ایمن سازی کامپیوتر)

موضوع

: Firewalls(Computer security)

موضوع

: شبکه های کامپیوتری-تدابیر ایمنی-برنامه های کامپیوتری

موضوع

: Computer networks—Security measures—Computer programs

موضوع

: موسسه فنی و مهندسی کیان نیکی پریزاد گروه پیشگامان فناوری اطلاعات پریزاد

سازمان

: TK5۱۰۵/۵۹/ق۹۹۹ ۱۳۹۵

رده بندی کنگره

: ۰۰۵/۸

رده بندی دیویی

: ۳۵۶۶۲۰۱ شماره کتابخانه ملی

شماره کتابخانه ملی



NAGHOOS
PUBLICATION

برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoospress.ir

انتشارات ناقوس

چاپ اول

: دیوار آتش در سیستم عامل Linux (از دیدگاه یک هکر)

نام کتاب

: انتشارات ناقوس

ناشر

: حمید رضا قنبری

مؤلف

S.M.S : ۳۰۰۰۴۵۲۳۲۳

: با همکاری گروه پیشگامان فناوری اطلاعات پریزاد

چاپ اول

: ۱۳۹۵

« در نوبت چاپ اول از دستگاه چاپ

تیراژ

: ۲۰۰ جلد

دیجیتال استفاده شده است »

چاپ و صحافی

: نارنجستان

ناظر چاپ

: یاسمن تجملی محدث

سرپرست صفحه آرا

: معصومه صیادی

قیمت (به همراه CD)

: ۹۵۰۰۰ ریال

شابک

: ۹۷۸-۹۶۴-۳۷۷-۹۶۱-۰۰۰

ISBN

: 978-964-377-961-0

مرکز پخش: انتشارات ناقوس

۱- خیابان انقلاب-خیابان ۱۲ فروردین- بین وحیدنظری و روانمهر- بن بست حقیقت- پلاک ۴

تلفن و فاکس: ۶۶۴۷۸۹۵۸-۶۶۴۷۸۹۵۷

۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴

۳- کتابفروشی گلریزان: ضلع جنوب شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰

«دیوار آتش» پیاده سازی مدرنی از روش قدیمی حصارهای امنیتی است. در دنیای شبکه های کامپیوتری، همین راهکار ممکن خواهد بود: یک سازمان می تواند هر تعداد شبکه محلی داشته باشد که به صورت دلخواه به هم متصل شده اند، اما تمام ترافیک ورودی یا خروجی سازمان صرفاً از طریق یک پل متحرک (همان دیوار آتش) میسر است.

در این کتاب در دو فصل به بررسی و نحوه عملکرد دیواره های آتش در سیستم عامل لینوکس از دیدگاه یک هکر خواهیم پرداخت.

کار حاضر بدون شک خالی از اشکال نیست، امید است از ارشاد و راهنمایی خبرگان و اهل فن بی بهره نباشیم.

حمیدرضا قنبری

با همکاری: گروه پیشگامان فناوری اطلاعات پریراد

پاییز ۱۳۹۵

۹	فصل اول: دیوارهای آتش در شبکه های کامپیوتری
۱۱	۱-۱: مقدمه
۱۲	۲-۱: یک دیوار آتش چیست؟
۱۳	۳-۱: دیوارهای آتش چه کاری انجام می دهند؟
۱۳	۱-۳-۱: اثرات مثبت
۱۴	۲-۳-۱: اثرات منفی
۱۴	۴-۱: دیوارهای آتش، چه کارهایی را نمی توانند انجام دهند؟
۱۵	۵-۱: چگونه دیوارهای آتش عمل می کنند؟
۱۶	۶-۱: انواع دیوارهای آتش
۱۷	۱-۶-۱: فیلتر کردن بسته ها (Packet Filtering)
۲۱	۲-۶-۱: بازرسی هوشمندانه (Stateful Packet Inspection)
۲۲	۳-۶-۱: دروازه برنامه های کاربردی (Application Gateways / Proxies)
۲۷	۴-۶-۱: پراکسی های قابل تطبیق (Adaptive Proxies)
۲۸	۵-۶-۱: دروازه سطح مداری (Circuit-Level Gateway)
۲۸	۶-۶-۱: وانمود کننده ها (Impostors)
۳۰	۷-۱: جنبه های مهم دیوارهای آتش کارآمد
۳۰	۸-۱: معماری دیوار آتش (FIREWALL ARCHITECTURE)
۳۱	۱-۸-۱: مسیر یاب فیلتر کننده بسته (Packet Filtering Router)
۳۱	۲-۸-۱: میزبان غربال شده یا میزبان سنگر (Screened Host or Bastion Host)
۳۲	۳-۸-۱: دروازه دو خانه ای (Dual-homed Gateway)
۳۳	۴-۸-۱: زیر شبکه غربال شده یا منطقه غیر نظامی (Screened Subnet or Demilitarized Zone)
۳۳	۵-۸-۱: دستگاه دیوار آتش (Firewall Appliance)
۳۴	۹-۱: انتخاب و پیاده سازی یک راه حل دیوار آتش
۳۴	۱-۹-۱: آیا شما نیاز به یک دیوار آتش دارید؟
۳۵	۲-۹-۱: دیوار آتش، چه چیزی را باید کنترل یا محافظت کند؟
۳۵	۳-۹-۱: یک دیوار آتش، چه تأثیری روی سازمان، شبکه و کاربران شما خواهد گذاشت؟
۳۶	۱۰-۱: سیاست امنیتی (SECURITY POLICY)
۳۷	۱-۱۰-۱: موضوعات اجرایی (Administrative Issues)
۳۷	۲-۱۰-۱: موضوعات فنی (Technical Issues)
۳۸	۱۱-۱: نیازهای پیاده سازی

۳۸	 ۱-۱۱-۱ : نیازهای فنی
۳۸	 ۲-۱۱-۱ : معماری
۳۹	 ۱۲-۱ : تصمیم گیری
۳۹	 ۱۳-۱ : پیاده سازی و آزمایش
۳۹	 ۱-۱۳-۱ : آزمایش، آزمایش، آزمایش!
۴۰	 ۱۴-۱ : خلاصه
۴۱	فصل دوم: پیاده سازی دیوار آتش با استفاده از IPTABLES
۴۳	 ۱-۲ : مقدمه
۴۴	 ۲-۲ : واژگان علمی مربوط به فیلترسازی بسته (PACKET FILTERING TERMINOLOGY)
۴۵	 ۳-۲ : ساختار یک ماشین برای دیوار آتش مبتنی بر لینوکس
۴۶	 ۴-۲ : به کار بردن MASQUERADING و IP FORWARDING
۴۹	 ۵-۲ : حسابداری بسته (PACKET ACCOUNTING)
۴۹	 ۶-۲ : جداول و زنجیرها برای یک دیوار آتش مبتنی بر لینوکس
۵۲	 ۷-۲ : قوانین (RULES)
۵۳	 ۸-۲ : تطبیق ها (MATCHES)
۵۳	 ۹-۲ : اهداف (TARGETS)
۵۴	 ۱۰-۲ : پیکربندی IPTABLES
۵۴	 ۱۱-۲ : استفاده از IPTABLES
۵۵	 ۱-۱۱-۲ : مشخصات فیلترسازی (Filtering Specifications)
۵۷	 ۲-۱۱-۲ : تصمیم هایی برای iptables (تطبیق های بسته)
۶۳	 ۳-۱۱-۲ : مشخصات هدف (Target Specifications)
۶۵	 ۴-۱۱-۲ : عملیات روی یک زنجیر کامل
۶۷	 ۱۲-۲ : ترکیب NAT با فیلترسازی بسته
۶۷	 ۱-۱۲-۲ : ترجمه آدرس شبکه (NAT)
۶۷	 ۲-۱۲-۲ : NAT مبدأ و Masquerading
۶۸	 ۳-۱۲-۲ : NAT مقصد
۶۹	 ۱۳-۲ : ذخیره نمودن و برگرداندن قوانین