امن‌سازی DNS Server

در سیستم‌عامل‌های لینوکس و ویندوز

امن‌سازی DNS Server

در سیستم‌عامل‌های لینوکس و ویندوز

مهندس رحیمه خدادادی

انتشارات پندار پارس

سرشناسه	:	خدادادی، رحیمه، 1363 -
عنوان و نام پدیدآور	:	امن‌سازی DNS Server در سیستم عامل‌های لینوکس و ویندوز/ رحیمه خدادادی.
مشخصات نشر	:	تهران: پندار پارس : مانلی، 1390.
مشخصات ظاهری	:	144 ص.: مصور، جدول.
شابک	:	48000 ریال : 978-964-2989-81-2
وضعیت فهرست نویسی	:	فیپا
موضوع	:	سیستم عامل لینوکس
موضوع	:	ویندوز مایکروسافت، سرور
موضوع	:	شبکه‌های کامپیوتری -- اقدامات تامینی
موضوع	:	کامپیوترها -- ایمنی اطلاعات
موضوع	:	اینترنت -- اقدامات تامینی
موضوع	:	اینترنت -- نام حوزه
رده بندی کنگره	:	TK5105/59/خ4الف8 1390
رده بندی دیویی	:	005/8
شماره کتابشناسی ملی	:	1912942

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره 14، واحد 16 **www.pendarepars.com**

تلفن: 66572335 - تلفکس: 66926578همراه: 09122452348 **info@pendarepars.com**

نام کتاب	:	**امن‌سازی DNS Server در سیستم عامل‌های لینوکس و ویندوز**
ناشر	:	**انتشارات پندار پارس ناشر همکار: مانلی**
ترجمه و تالیف	:	**مهندس رحیمه خدادادی**
چاپ اول	:	**پاییز 90**
شمارگان	:	**1000 نسخه**
طرح جلد	:	**محمد اسماعیلی هدی**
لیتوگرافی، چاپ، صحافی	:	**ترام‌سنج، صالحان، نوین‌برتر**
قیمت	:	**4800 تومان** **شابک** : 978-964-2989-81-2

تلاشی است اندک تقدیم به:

سایه‌ی نوازشگر، پدرم

همیشه همراه، مادرم

و یاوران دانش، همه معلیمن عمرم به‌ویژه:

آقای دکتر رسول جلیلی (استاد دانشگاه صنعتی شریف)

فهرست

مقدمه

DNS یکی از پروتکل‌های زیرساختی اینترنت در لایه کاربرد می‌باشد. مهم‌ترین وظیفه DNS ترجمه اسامی دامنه و میزبان به مفاهیم قابل درک انسان است. همچنین کاربران، بدون DNS قادر به دسترسی به اینترنت نیستند. از طرفی به طور معمول هنگام نصب و راه‌اندازی DNS بر روی سیستم‌عامل‌ها تنظیمات با پیش‌فرض‌های شرکت سازنده، آماده ارائه خدمات هستند. این موضوع باعث می‌شود تا سرویس‌دهنده‌هایDNS به طور ناامن نصب و تنظیم گردند. بنابراین از اساسی‌ترین مراحل ایمن‌سازی، مستحکم‌سازی[1] سرویس‌دهنده‌هایDNS است تا از نفوذ و آسیب‌پذیری ممانعت به‌عمل آید. در خصوص امنیت نرم افزارهای سرویس‌دهنده‌های DNS، توجه به استفاده از آخرین نسخه‌ها و بروزرسانی‌ها حیاتی می‌باشد. علاوه بر این، در سال‌های اخیر مهاجمان توانسته‌اند با استفاده از ضعف امنیتی و پیکربندی نامناسب DNS به سرویس‌دهنده‌ها نفوذ کنند. به همین دلیل این کتاب در راستای امن‌سازی سرویس‌دهنده‌های DNS نوشته شده است تا کمکی برای پیشگیری و جلوگیری از چنین حملاتی باشد.

هدف و لزوم امنیت در سرویس DNS

در صورتی‌که مقصد یک حمله، سرویس‌دهنده[2] DNS باشد یکی از اهداف مهاجم، کنترل اطلاعاتی است که در پاسخ به پرس‌وجوهای کلاینت[3]ها، توسط سرویس‌دهنده DNS برگردانده می‌شود. در شرایطی که مهاجم قادر به کنترل این اطلاعات باشد در این صورت ممکن است کلاینت‌ها ندانسته به کامپیوترهای غیرمجازی تغییر مسیر یابند. IP Spoofing و Cache Poisoning مثال‌هایی از این نوع حملات هستند. در IP Spoofing پاسخ‌گویی به کلاینت از سوی سرویس‌دهنده DNS جعلی صورت می‌گیرد. طی حمله از نوع Cache Poisoning نیز، مهاجم اطلاعات نادرستی به داخل کش سرویس‌دهنده DNS منتقل می‌کند که منجر به تغییر مسیر کلاینت‌ها به سوی کامپیوتر غیرمجاز می‌شود.

علاوه بر این، برخی حملات نیز برای جلوگیری از راه‌اندازی سرویس (DoS[4]) طراحی می‌شوند. در این نوع حملات، سرویس‌دهنده DNS با آدرس‌های نامعتبر[5] به کلاینت‌ها پاسخ می‌دهد. در این شرایط

---

[1] Hardening
[2] Server
[3] Client
[4] Denial of Service
[5] Invalid Address

کلاینت‌های DNS در شبکه قادر به تعیین مکان منابع شبکه مانند کنترل کننده دامنه، سرویس‌دهنده-های وب، فایل‌های به اشتراک گذاشته شده و سایر موارد نخواهد بود.

این کتاب راهنمایی سریع و آسانی برای پیاده‌سازی امن Domain Name System در محیط‌های مختلف سازمان‌ها، به منظور کاهش خطرات و تهدیدات امنیتی منتشر گردیده است. مدیران پیاده‌ساز DNS و همچنین کارمندان امنیتی کامپیوترها و مدیران سیستمی که مسئول اجرای کارهای مرتبط با DNS هستند، می‌توانند با استفاده از این راهنمای عملی، DNS مورد دلخواه خود را سازگار با هر محیطی امن نمایند.