امن‌سازی DNS Server

در سیستم‌عامل‌های لینوکس و ویندوز

مهندس رحیمه خدادادی

انتشارات پندار پارس

سرشناسه	:	خدادادی، رحیمه، ۱۳۶۳ -
عنوان و نام پدیدآور	:	امن‌سازی DNS Server در سیستم عامل‌های لینوکس و ویندوز/ رحیمه خدادادی.
مشخصات نشر	:	تهران: پندار پارس : مانلی، ۱۳۹۰.
مشخصات ظاهری	:	۱۴۴ ص.: مصور، جدول.
شابک	:	۴۸۰۰۰ ریال : ۲-۸۱-۲۹۸۹-۹۶۴-۹۷۸
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	:	TK۵۱۰۵/۵۹/خ۴ف۸ ۱۳۹۰
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۱۹۱۲۹۴۲

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ **www.pendarepars.com**

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸همراه: ۰۹۱۲۲۴۵۲۳۴۸ **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 ۹۰
شمارگان	:	۱۰۰۰ نسخه
طرح جلد	:	محمد اسماعیلی هدی
لیتوگرافی، چاپ، صحافی	:	نرام‌سنج، صالحان، نوین‌برتر
قیمت	:	۴۸۰۰ تومان شابک : ۲-۸۱-۲۹۸۹-۹۶۴-۹۷۸

فهرست

مقدمه ۱

هدف و لزوم امنیت در سرویس DNS ۱

فصل اول آشنایی با مفاهیم و اجزای DNS..... ۳

۱-۱ تعریف DNS..... ۳

۱-۲ نام فضای دامنه ٤

۱-۳ اجزای DNS ٥

۱-۳-۱ فایل ناحیه ٥

۱-۳-۲ سرویس‌دهنده‌های نام..... ۷

۱-۳-۳ کلاینت‌های DNS ۸

۱-٤ تراکنش‌های DNS..... ۸

۱-٤-۱ پرسش/پاسخ DNS ۸

۱-٤-۲ انتقال ناحیه ۹

۱-٤-۳ بروزرسانی‌های پویا ۹

۱-٤-٤ DNS NOTIFY ۱۰

۱-٥ روش‌های جستجو در سرویس دهنده‌های نام ۱۰

۱-٥-۱ پرس‌وجوی تکراری..... ۱۱

۱-٥-۲ پرس‌وجوی بازگشتی..... ۱۲

۱-٥-۳ پرس‌وجوی معکوس ۱۳

۱-٦ خطرات و تهدیدات سرویس‌دهنده‌های نام ۱۳

فصل دوم امن‌سازی DNS SERVER در سیستم عامل‌های لینوکس ۱٥

۲-۱ آخرین وصله‌های سیستم عامل باید نصب شود..... ۱٥

۲-۲ پرس‌وجوی نسخه نرم‌افزار سرویس‌دهنده DNS را غیرفعال کنید..... ۱٦

۲-۳ به حداقل رسانیدن خرابی‌های نقاط واحد..... ۱٦

۲-٤ استفاده از سرویس‌دهنده‌های نام مجزا ۱۷

۲-٤-۱ سرویس‌دهنده نام Advertising ۱۷

۲-٤-۲ سرویس‌دهنده نام Resolving ۱۷

۲-۵ فیلتر ترافیک سرویس‌دهنده نام ۱۸

۲-٦ محدودسازی انتقال‌های ناحیه ۱۹

۲-٦-۱ محدودیت انتقال‌های ناحیه در برنامه BIND 4 ..... ۲۰

۲-٦-۲ محدودیت انتقال‌های ناحیه در برنامه BIND 8 ..... ۲۰

۲-۷ احراز هویت انتقال‌های ناحیه با استفاده از TSIG ۲۱

۲-۸ پیکربندی TSIG با برنامه BIND 8.2 و نسخه‌های بالاتر ۲۱

۲-۹ محدودسازی بروزرسانی‌های پویا ۲۲

۲-۹-۱ محدودسازی به‌روزرسانی‌های پویا با استفاده از BIND 8 و نسخه 9 ..... ۲۳

۲-۹-۲ محدودسازی بروزرسانی پویا با استفاده از BIND 9 ..... ۲٤

۲-۱۰ محدودسازی عملیات BIND DNS NOTIFY ۲۵

۲-۱۱ محافظت در برابر Cache-poisoning ۲٦

۲-۱۲ غیرفعال کردن عملیات بازگشتی (نسخه‌های BIND 4.9 تا بالاتر) ۲۷

۲-۱۳ محدود سازی پرس‌وجوها در نسخه‌های BIND8 و بالاتر با دستور allow-query. ۲۸

۲-۱۳-۱ محدودسازی بازگشتی با استفاده از دستور allow-recursion ۳۰

۲-۱۳-۲ محدودسازی عملیات بازگشتی با استفاده از views ۳۱

۲-۱٤ غیرفعال کردن Glue fetching (تنها در نسخه‌های BIND 4.9 و BIND 8) ۳۲

۲-۱۵ محافظت بیشتر در برابر جعل (نسخه BIND 8) ۳۲

۲-۱٦ اجرای برنامه سرویس‌دهنده نام به عنوان کاربری به غیر از root ۳۳

۲-۱۷ اجرای سرویس‌دهنده نام در chroot () "jail" ۳٤

۲-۱۸ امنیت بیشتر از طریق پیاده‌سازی DNSSEC بر روی سیستم عامل‌های لینوکس ۳۵

۲-۱۸-۱ برخی اصطلاحات رایج در DNSSCE ۳۵

۲-۹-۲-۳ پیکربندی اندازه Socket pool به روش خط فرمان ۸۱
۳-۹-۲-۳ پیکربندی SocketPoolExcluded List به‌کمک واسط کاربری ویندوز ۸۱
٤-۹-۲-۳ پیکربندیSocketPoolExcluded List با استفاده از خط فرمان ۸۲
۱۰-۲-۳ پیکربندی قفل‌سازی کش ۸۲
۱-۱۰-۲-۳ پیکربندی قفل‌سازی کش با استفاده از خط فرمان ۸۳
۲-۱۰-۲-۳ پیکربندی قفل‌سازی کش با استفاده از واسط کاربری ویندوز ۸۳
۱۱-۲-۳ محدودسازی شنود سرویس‌دهنده DNS ۸۳
۱-۱۱-۲-۳ پیکربندی محدودسازی شنود سرویس‌دهنده DNS بکمک واسط ۸٤
۲-۱۱-۲-۳ پیکربندی محدودسازی سرویس‌دهنده DNS به‌کمک خط فرمان ۸٤
۱۲-۲-۳ پیکربندی Root Hints داخلی ۸٤
۱۳-۲-۳ غیرفعال کردن عملیات بازگشتی در سرویس‌دهنده DNS ۸۵
۱-۱۳-۲-۳ غیرفعال کردن عملیات بازگشتی سرویس‌دهنده DNS به‌کمک واسط ۸۵
۲-۱۳-۲-۳ غیرفعال کردن عملیات بازگشتی سرویس‌دهندهDNS به‌کمک خط فرمان . ۸٦
۱٤-۲-۳ امن‌سازی کش DNS از آلودگی ۸٦
۱۵-۲-۳ امن‌سازی انتقال‌های ناحیه با استفاده از IPsec ۸٦
۳-۳ پیاده‌سازیDNSSEC روی Windows Server 2008 R2 ..... ۸۸
۱-۳-۳ برخی اصطلاحات رایج در DNSSEC ۸۸
۲-۳-۳ مدیریت DNSSEC به‌کمک Dnscmd.exe و DNS Manager ۸۸
۳-۳-۳ فراهم سازی سرویس‌دهنده جهت پیاده‌سازی DNSSEC ۸۹
٤-۳-۳ بروزرسانی سرویس‌دهنده DNS به نسخه Windows Server 2008 R2 ..... ۸۹
۵-۳-۳ پیاده‌سازی DNSSEC بر روی سرویس‌دهنده‌های DNS ۹۰
۱-۵-۳-۳ تعیین سیستم جهت امضاء ۹۰
۲-۵-۳-۳ اضافه کردن ناحیه به سیستم امن ۹۰
۳-۵-۳-۳ تعیین مکانیزم تعویض کلیدها (Key rollover) ۹۰

٣-٥-٣-٤ تولید کلیدها ٩١
تولید کلید KSK ٩١
تولید کلید ZSK ٩١
٣-٥-٣-٥ پشتیبان‌گیری از کلیدهای خصوصی ٩٣
صدور certificate از MS-DNSSEC ٩٣
٣-٥-٣-٦ امضاء ناحیه ٩٤
امضاء فایل backed zone ٩٤
امضاء ناحیه Active Directory integrated ٩٥
ملاحظات اضافی ٩٦
٣-٥-٣-٧ بارگذاری ناحیه ٩٧
٣-٥-٣-٨ آماده‌سازی رکورد DS برای ناحیه والد ٩٨
٣-٥-٣-٩ ثبت رکورد DS از ناحیه فرزند ٩٨
٣-٥-٣-١٠ اضافه و حذف رکوردهای منابع ٩٨
٣-٥-٣-١١ امضاء مجدد ناحیه ٩٩
٣-٥-٣-١٢ اجرای Key rolloverها ٩٩
اجرای Pre-published ZSK rollover ٩٩
اجرای double signature ZSK rollover ١٠١
اجرای double signature KSK rollover ١٠٢
٣-٥-٣-١٣ برگشت تنظیمات به حالت ناحیه امضاء نشده ١٠٣
٣-٥-٣-١٤ پیکربندی و توزیع trust anchorها ١٠٣
٣-٥-٣-١٥ پیکربندی خط مشی‌های IPsec بر روی سرویس‌دهنده DNS ١٠٤
ایجاد Certificateها ١٠٥
پیکربندی خط مشی IPsec ١٠٦
٣-٥-٣-١٦ پیکربندی DNSSEC و IPsec بر روی کلاینت DNS ١٠٧

۲-۱۸-۲ فعال‌سازی فرایند DNSSEC در نرم‌افزار NSD&BIND ۳۷
۲-۱۸-۳ تولید کلیدهای Key Signing Key و Zone Signing Key ۳۷
۲-۱۸-٤ امضاء ناحیه ۳۹
۲-۱۸-٥رهنمودهای امن‌سازی برای عملیات مدیریتی DNSSEC و نگهداری ناحیه ٤۱
۲-۱۸-٥-۱ زمان‌بندی کردن Key Rollovers ٤۱
۲-۱۸-٥-۲ امضاء مجدد یک ناحیه ٤۲
۲-۱۸-٥-۳ پیکربندی Resolverها ٤۳
۲-۱۸-٥-٤ برطرف کردن مشکلات ٤٥
فصل سوم امن‌سازی DNS SERVER در سیستم عامل‌های ویندوز سرور ۴۹
۳-۱ امن‌سازیDNS در سیستم‌عامل Windows Server 2003 ..... ٤۹
۳-۱-۱ توسعه امن DNS ٤۹
۳-۱-۲ امن‌سازی سرویس DNS ٥۰
۳-۱-۲-۱ محدود کردن شنود سرویس‌دهنده DNS ٥۰
۳-۱-۲-۲ امن‌سازی سرویس‌دهنده کشDNS در برابر آلودگی نام‌ها ٥۲
۳-۱-۲-۳ غیرفعال کردن پرس‌وجوی بازگشتی ٥۳
۳-۱-۲-٤ پیکربندی Root Hintها برای ممانعت از افشای اطلاعات ٥٤
۳-۱-۲-٥ مدیریت کنترل دسترسی به سرویس DNS ٥٤
امنیت سرویس‌دهنده DHCP ٥٦
ممیزی سرویس‌دهنده DHCP ٥٦
فعال‌سازی ممیزی در DHCP Server ٥٦
گروه مدیران DHCP ٥۷
۳-۱-۲-٦ پیکربندی فایل ثبت وقایع سرویس DNS ٥۹
۳-۱-۳ امن‌سازی ناحیه‌ها ٦۱
۳-۱-۳-۱ پیکربندی بروزرسانی‌های پویا به صورت امن ٦۱

۲-۳-۱-۳ مدیریت کنترل دسترسی به ناحیه ٦٢
۳-۳-۱-۳ محدود کردن انتقال‌های ناحیه ٦٣
٤-۱-۳ امن‌سازی رکوردهای منابع ٦٥
۲-۳ پیاده‌سازی و پیکربندی امن DNS در Windows Server 2008 R2 ..... ٦٦
۱-۲-۳ بکارگیری قابلیت RODC جهت حفاظت از ناحیه‌های DNS در مکان‌های نا امن . ٦٨
۲-۳-۳ استفاده از سرویس‌دهنده‌های DNS مجزا برای تحلیل فضای نام داخلی و ٧٢
۱-۲-۲-۳ پیکربندی سرویس‌دهنده DNS داخلی برای استفاده از Forwarderها ٧٢
۳-۲-۳ امن‌سازی دامنه و کنترل کننده دامنه ٧٣
۱-۳-۲-۳ تنظیمات امنیتی Group Policy روی کنترل کننده دامنه ٧٤
۲-۳-۲-۳ تنظیمات امنیتی Group Policy روی دامنه ٧٥
٤-۲-۳ فعال‌سازی امن بروزرسانی‌های پویا ٧٦
۱-٤-۲-۳ فعال‌سازی امن بروزرسانی‌های پویا با استفاده از واسط کاربری ویندوز.. ٧٦
۲-٤-۲-۳ فعالسازی امن بروزرسانیهای پویا با استفاده از خط فرمان ٧٧
٥-۲-۳ محدودسازی تنظیمات انتقال‌های ناحیه ٧٧
۱-٥-۲-۳ محدودسازی تنظیمات انتقال‌های ناحیه با استفاده از واسط کاربری ٧٧
۲-٥-۲-۳ محدودسازی تنظیمات انتقال‌های ناحیه با استفاده از خط فرمان ٧٨
٦-۲-۳ پیکربندی ناحیه‌های AD Integrated ٧٨
۱-٦-۲-۳ پیکربندی ناحیه AD Integrated با استفاده از واسط کاربری ٧٩
۲-٦-۲-۳ پیکربندی ناحیه AD Integrated با استفاده از خط فرمان ٧٩
۷-۲-۳ پیکربندی Discretionary Access Control List (DACL) ٧٩
۸-۲-۳ پیکربندی Globle Query Block List ٨٠
۱-۸-۲-۳ فعال و غیرفعال کردن Globle Qurey Block List ٨٠
۹-۲-۳ پیکربندی Socket pool ٨٠
۱-۹-۲-۳ پیکربندی اندازه Socket Pool با استفاده از واسط کاربری ویندوز ٨٠

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 سرویس‌دهنده‌های DNS به طور ناامن نصب و تنظیم گردند. بنابراین از اساسی‌ترین مراحل ایمن‌سازی، مستحکم‌سازی[1] سرویس‌دهنده‌های DNS است تا از نفوذ و آسیب‌پذیری ممانعت به‌عمل آید. در خصوص امنیت نرم‌افزارهای 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.

پیکربندی NRPT برای کلاینت‌های عضو دامنه ۱۰۸
الف. ایجاد OU ۱۰۸
ب. ایجاد خط مشی DNSSEC ۱۰۸
ج. مراحل ایجاد یک قانون ۱۰۸
پیکربندی NRPT برای کلاینت‌های غیر عضو دامنه ۱۰۹
الف. تخصیص مجوز به خط مشی‌ها به‌کمک Local Group Policy Editor ۱۰۹
ب. پیاده‌سازی خط مشی از طریق اسکریپت رجیستری ۱۱۰
۳-٤ امن‌سازی گروه‌ها و حساب‌های کاربری مدیریتی اکتیو-دایرکتوری در ویندوز سرور 2003 و 2008 ..... ۱۱۰
۳-٤-۱ تغییر نام حساب کاربری پیش‌فرض Administrator ۱۱۱
۳-٤-۲ ایجاد حساب کاربری Administrator تقلبی ۱۱۲
۳-٤-۳ امن‌سازی حساب کاربری Guest ۱۱۳
۳-٤-۳-۱ تغییر نام حساب کاربری Guest ۱۱۳
۳-٤-٤ امنیت بیشتر بر روی سرویس‌های مدیریتی حساب‌های کاربری و گروه‌ها ۱۱٤
۳-٤-٤-۱ ایجاد ساختار OU برای زیر درخت کنترل شده ۱۱٥
۳-٤-٤-۲ تنظیمات مجوزها بر روی زیر درخت کنترلی OUها ۱۱٦
۳-٤-٤-۳ انتقال گروه‌های سرویس‌های مدیریتی به Users and Groups OU ۱۱۸
۳-٤-٤-٤ انتقال‌حسابهای‌مدیریتی ایستگاه‌کاری به Admin Workstations OU ۱۱۹
۳-٤-٤-٥ فعال‌سازی ممیزی در زیر درخت کنترل شده ۱۱۹
منابع ومراجع: ۱۲۲
لغت‌نامه ۱۲۳