

امن سازی DNS Server

در سیستم عامل های لینوکس و ویندوز

امن سازی DNS Server

در سیستم عامل های لینوکس و ویندوز

مهندس رحیمه خدادادی

انتشارات پندار پارس

سرشناسه	: خدادادی، رحیمه، 1363 -
عنوان و نام پدیدآور	: امن سازی DNS Server در سیستم عامل های لینوکس و ویندوز / رحیمه خدادادی.
مشخصات نشر	: تهران: پندار پارس : مانلی، 1390.
مشخصات ظاهری	: 144 ص: مصور، جدول.
شابک	: 978-964-2989-81-2 ریال : 48000
وضعیت فهرست نویسی	: فیبا
موضوع	: سیستم عامل لینوکس
موضوع	: ویندوز مایکروسافت، سرور
موضوع	: شبکه های کامپیوتری -- اقدامات تامینی
موضوع	: کامپیوترها -- ایمنی اطلاعات
موضوع	: اینترنت -- اقدامات تامینی
موضوع	: اینترنت -- نام حوزه
رده بندی کنگره	: 1390 8 الف 4 / 5105/59TK
رده بندی دیویی	: 005/8
شماره کتابشناسی ملی	: 1912942

انتشارات پندارپارس



دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتچی، شماره 14، واحد 16 www.pendarepars.com
 تلفن: 66572335 - تلفکس: 66926578 همراه: 09122452348
info@pendarepars.com



نام کتاب	: امن سازی DNS Server در سیستم عامل های 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	: ترام سنج، صالحان، نوین برتر
قیمت	: 4800 تومان

شابک : 978-964-2989-81-2

هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد *

تلاشی است اندک تقدیم به:

سایه‌ی نوازشگر، پدرم

همیشه همراه، مادرم

و یاوران دانش، همه معلمین عمرم به‌ویژه:

آقای دکتر رسول جلیلی (استاد دانشگاه صنعتی شریف)

فهرست

1	مقدمه
1	هدف و لزوم امنیت در سرویس DNS
3	فصل اول آشنایی با مفاهیم و اجزای DNS.....
3	1-1 تعریف DNS.....
4	1-2 نام فضای دامنه
5	1-3 اجزای DNS
5	1-3-1 فایل ناحیه
7	1-3-2 سرویس دهنده های نام.....
8	1-3-3 کلاینت های DNS
8	1-4 تراکنش های DNS
8	1-4-1 پرسش/پاسخ DNS
9	1-4-2 انتقال ناحیه
9	1-4-3 بروزرسانی های پویا
10	1-4-4 DNS NOTIFY
10	1-5 روش های جستجو در سرویس دهنده های نام
11	1-5-1 پرس و جوی تکراری
12	1-5-2 پرس و جوی بازگشتی
13	1-5-3 پرس و جوی معکوس
13	1-6 خطرات و تهدیدات سرویس دهنده های نام
15	فصل دوم امن سازی DNS SERVER در سیستم عامل های لینوکس
15	2-1 آخرین وصله های سیستم عامل باید نصب شود
16	2-2 پرس و جوی نسخه نرم افزار سرویس دهنده DNS را غیرفعال کنید
16	2-3 به حداقل رسانیدن خرابی های نقاط واحد

17	2-4 استفاده از سرویس‌دهنده‌های نام مجزا
17	2-4-1 Advertising سرویس‌دهنده نام
17	2-4-2 Resolving سرویس‌دهنده نام
18	2-5 فیلتر ترافیک سرویس‌دهنده نام
19	2-6 محدودسازی انتقال‌های ناحیه
20	2-6-1 محدودیت انتقال‌های ناحیه در برنامه BIND 4
20	2-6-2 محدودیت انتقال‌های ناحیه در برنامه BIND 8
21	2-7 احراز هویت انتقال‌های ناحیه با استفاده از TSIG
21	2-8 پیکربندی TSIG با برنامه BIND 8.2 و نسخه‌های بالاتر
22	2-9 محدودسازی بروزرسانی‌های پویا
23	2-9-1 محدودسازی به‌روزرسانی‌های پویا با استفاده از BIND 8 و نسخه 9
24	2-9-2 محدودسازی بروزرسانی پویا با استفاده از BIND 9
25	2-10 محدودسازی عملیات BIND DNS NOTIFY
26	2-11 محافظت در برابر Cache-poisoning
27	2-12 غیرفعال کردن عملیات بازگشتی (نسخه‌های BIND 4.9 تا بالاتر)
28	2-13 محدود سازی پرس‌وجوها در نسخه‌های BIND 8 و بالاتر با دستور allow-query
30	2-13-1 محدودسازی بازگشتی با استفاده از دستور allow-recursion
31	2-13-2 محدودسازی عملیات بازگشتی با استفاده از views
32	2-14 غیرفعال کردن Glue fetching (تنها در نسخه‌های BIND 4.9 و BIND 8)
32	2-15 محافظت بیشتر در برابر جعل (نسخه BIND 8)
33	2-16 اجرای برنامه سرویس‌دهنده نام به عنوان کاربری به غیر از root
34	2-17 اجرای سرویس‌دهنده نام در () chroot "jail"
35	2-18 امنیت بیشتر از طریق پیاده‌سازی DNSSEC بر روی سیستم عامل‌های لینوکس
35	2-18-1 برخی اصطلاحات رایج در DNSSEC

37NSD&BIND در نرم افزار DNSSEC فرایند فعال سازی
37Zone Signing Key و Key Signing Key تولید کلیدهای
39 2-18-4 امضاء ناحیه
412-18-5 رهنمودهای امن سازی برای عملیات مدیریتی DNSSEC و نگهداری ناحیه
41Key Rollovers کردن زمان بندی
42 2-18-5-2 امضاء مجدد یک ناحیه
43 2-18-5-3 پیکربندی Resolverها
45 2-18-5-4 برطرف کردن مشکلات
49 فصل سوم امن سازی DNS SERVER در سیستم عامل های ویندوز سرور
49 3-1 امن سازی DNS در سیستم عامل Windows Server 2003
49 3-1-1 توسعه امن DNS
50 3-1-2 امن سازی سرویس DNS
50 3-1-2-1 محدود کردن شنود سرویس دهنده DNS
52 3-1-2-2 امن سازی سرویس دهنده کش DNS در برابر آلودگی نامها
53 3-1-2-3 غیرفعال کردن پرس و جوی بازگشتی
54 3-1-2-4 پیکربندی Root Hintها برای ممانعت از افشای اطلاعات
54 3-1-2-5 مدیریت کنترل دسترسی به سرویس DNS
56 امنیت سرویس دهنده DHCP
56 ممیزی سرویس دهنده DHCP
56 فعال سازی ممیزی در DHCP Server
57 گروه مدیران DHCP
59 3-1-2-6 پیکربندی فایل ثبت وقایع سرویس DNS
61 3-1-3 امن سازی ناحیهها
61 3-1-3-1 پیکربندی بروزرسانی های پویا به صورت امن

- 62 3-1-3-2 مدیریت کنترل دسترسی به ناحیه
- 63 3-1-3-3 محدود کردن انتقال‌های ناحیه
- 65 3-1-4 امن‌سازی رکوردهای منابع
- 66 3-2 پیاده‌سازی و پیکربندی امن DNS در Windows Server 2008 R2
- 68 3-2-1 بکارگیری قابلیت RODC جهت حفاظت از ناحیه‌های DNS در مکان‌های نا امن
- 72 3-2-2 استفاده از سرویس‌دهنده‌های DNS مجزا برای تحلیل فضای نام داخلی و 72
- 72 3-2-2-1 پیکربندی سرویس‌دهنده DNS داخلی برای استفاده از Forwarderها
- 73 3-2-3 امن‌سازی دامنه و کنترل کننده دامنه
- 74 3-2-3-1 تنظیمات امنیتی Group Policy روی کنترل کننده دامنه
- 75 3-2-3-2 تنظیمات امنیتی Group Policy روی دامنه
- 76 3-2-4 فعال‌سازی امن بروزرسانی‌های پویا
- 76 3-2-4-1 فعال‌سازی امن بروزرسانی‌های پویا با استفاده از واسط کاربری ویندوز
- 77 3-2-4-2 فعال‌سازی امن بروزرسانی‌های پویا با استفاده از خط فرمان
- 77 3-2-5 محدودسازی تنظیمات انتقال‌های ناحیه
- 77 3-2-5-1 محدودسازی تنظیمات انتقال‌های ناحیه با استفاده از واسط کاربری
- 78 3-2-5-2 محدودسازی تنظیمات انتقال‌های ناحیه با استفاده از خط فرمان
- 78 3-2-6 پیکربندی ناحیه‌های AD Integrated
- 79 3-2-6-1 پیکربندی ناحیه AD Integrated با استفاده از واسط کاربری
- 79 3-2-6-2 پیکربندی ناحیه AD Integrated با استفاده از خط فرمان
- 79 3-2-7 پیکربندی Discretionary Access Control List (DACL)
- 80 3-2-8 پیکربندی Globle Query Block List
- 80 3-2-8-1 فعال و غیرفعال کردن Globle Query Block List
- 80 3-2-9 پیکربندی Socket pool
- 80 3-2-9-1 پیکربندی اندازه Socket Pool با استفاده از واسط کاربری ویندوز

81	3-2-9-2	پیکربندی اندازه Socket pool به روش خط فرمان
81	3-2-9-3	پیکربندی SocketPoolExcluded List به کمک واسط کاربری ویندوز
82	3-2-9-4	پیکربندی SocketPoolExcluded List با استفاده از خط فرمان
82	3-2-10	پیکربندی قفل‌سازی کش
83	3-2-10-1	پیکربندی قفل‌سازی کش با استفاده از خط فرمان
83	3-2-10-2	پیکربندی قفل‌سازی کش با استفاده از واسط کاربری ویندوز
83	3-2-11	محدودسازی شنود سرویس‌دهنده DNS
84	3-2-11-1	پیکربندی محدودسازی شنود سرویس‌دهنده DNS به کمک واسط
84	3-2-11-2	پیکربندی محدودسازی سرویس‌دهنده DNS به کمک خط فرمان
84	3-2-12	پیکربندی Root Hints داخلی
85	3-2-13	غیرفعال کردن عملیات بازگشتی در سرویس‌دهنده DNS
85	3-2-13-1	غیرفعال کردن عملیات بازگشتی سرویس‌دهنده DNS به کمک واسط
86	3-2-13-2	غیرفعال کردن عملیات بازگشتی سرویس‌دهنده DNS به کمک خط فرمان
86	3-2-14	امن‌سازی کش DNS از آلودگی
86	3-2-15	امن‌سازی انتقال‌های ناحیه با استفاده از IPsec
88	3-3	پیاده‌سازی DNSSEC روی Windows Server 2008 R2
88	3-3-1	برخی اصطلاحات رایج در DNSSEC
88	3-3-2	مدیریت DNSSEC به کمک Dnscmd.exe و DNS Manager
89	3-3-3	فراهم‌سازی سرویس‌دهنده جهت پیاده‌سازی DNSSEC
89	3-3-4	بروزرسانی سرویس‌دهنده DNS به نسخه Windows Server 2008 R2
90	3-3-5	پیاده‌سازی DNSSEC بر روی سرویس‌دهنده‌های DNS
90	3-3-5-1	تعیین سیستم جهت امضاء
90	3-3-5-2	اضافه کردن ناحیه به سیستم امن
90	3-3-5-3	تعیین مکانیزم تعویض کلیدها (Key rollover)

91 3-3-5-4 تولید کلیدها
91 تولید کلید KSK
91 تولید کلید ZSK
93 3-3-5-5 پشتیبان‌گیری از کلیدهای خصوصی
93 صدور certificate از MS-DNSSEC
94 3-3-5-6 امضاء ناحیه
94 امضاء فایل backed zone
95 امضاء ناحیه Active Directory integrated
96 ملاحظات اضافی
97 3-3-5-7 بارگذاری ناحیه
98 3-3-5-8 آماده‌سازی رکورد DS برای ناحیه والد
98 3-3-5-9 ثبت رکورد DS از ناحیه فرزند
98 3-3-5-10 اضافه و حذف رکوردهای منابع
99 3-3-5-11 امضاء مجدد ناحیه
99 3-3-5-12 اجرای Key rolloverها
99 اجرای Pre-published ZSK rollover
101 اجرای double signature ZSK rollover
102 اجرای double signature KSK rollover
103 3-3-5-13 برگشت تنظیمات به حالت ناحیه امضاء نشده
103 3-3-5-14 پیکربندی و توزیع trust anchorها
104 3-3-5-15 پیکربندی خط مشی‌های IPsec بر روی سرویس‌دهنده DNS
105 ایجاد Certificateها
106 پیکربندی خط مشی IPsec
107 3-3-5-16 پیکربندی DNSSEC و IPsec بر روی کلاینت DNS

108.....	پیکر بندی NRPT برای کلاینت‌های عضو دامنه
108.....	الف. ایجاد OU
108.....	ب. ایجاد خط مشی DNSSEC
108.....	ج. مراحل ایجاد یک قانون
109.....	پیکر بندی NRPT برای کلاینت‌های غیر عضو دامنه
109.....	الف. تخصیص مجوز به خط مشی‌ها به کمک Local Group Policy Editor
110.....	ب. پیاده‌سازی خط مشی از طریق اسکریپت رجیستری
110.....	3-4 امن‌سازی گروه‌ها و حساب‌های کاربری مدیریتی اکتیو-دایرکتوری در ویندوز سرور 2003 و 2008
111.....	3-4-1 تغییر نام حساب کاربری پیش‌فرض Administrator
112.....	3-4-2 ایجاد حساب کاربری Administrator تقلبی
113.....	3-4-3 امن‌سازی حساب کاربری Guest
113.....	3-4-3-1 تغییر نام حساب کاربری Guest
114.....	3-4-4 امنیت بیشتر بر روی سرویس‌های مدیریتی حساب‌های کاربری و گروه‌ها
115.....	3-4-4-1 ایجاد ساختار OU برای زیر درخت کنترل شده
116.....	3-4-4-2 تنظیمات مجوزها بر روی زیر درخت کنترلی OUها
118.....	3-4-4-3 انتقال گروه‌های سرویس‌های مدیریتی به OU Users and Groups
119.....	3-4-4-4 انتقال حساب‌های مدیریتی ایستگاه‌کاری به OU Admin Workstations
119.....	3-4-4-5 فعال‌سازی ممیزی در زیر درخت کنترل شده
122.....	منابع و مراجع:
123.....	لغت‌نامه

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^۱ سرویس‌دهنده‌های DNS 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 صورتی که مقصد یک حمله، سرویس‌دهنده^۲ DNS باشد یکی از اهداف مهاجم، کنترل اطلاعاتی است که در پاسخ به پرس‌وجوهای کلاینت‌ها، 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^۳) طراحی می‌شوند. در این نوع حملات، سرویس‌دهنده DNS با آدرس‌های نامعتبر^۴ به کلاینت‌ها پاسخ می‌دهد. در این شرایط

^۱ Hardening

^۲ Server

^۳ Client

^۴ Denial of Service

^۵ 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.