بسمه تعالی

مرکز مدیریت راهبردی افتا

عنوان

امن سازی DNS Server

گروه زیر ساخت امن

تیرماه ۱۳۹۳

فهرست مطالب

۱. مقدمه

به منظور دسترسی آسان به منابع اینترنت توسط نام‌های دامنه به جای استفاده از آدرس‌های IP، کاربران به سیستمی نیاز دارند که نام‌های دامنه را به آدرس‌های IP و برعکس ترجمه کند. این امر وظیفه عمده سرور نام دامنه یا همان DNS[۱] است. بیش از ۲۵۰ میلیون دامنه سطح بالا مانند org. و com. و چندین میلیون دامنه سطح دوم مانند google.com و ietf.org در جهان وجود دارد. بنابراین تعداد زیادی سرور نام وجود دارد که هریک شامل بخش کوچکی از فضای نام دامنه می‌شوند. نام دامنه تولید شده توسط DNS، برای تمامی سیستم‌ها، در سراسر فضای اینترنت قابل دسترسی است. دسترس پذیری داده DNS و سرویس آن، بسیار مهم بوده و از این رو هدف مناسبی برای انواع حملات می‌باشد. اهداف اولیه امن سازی DNS، جامعیت داده و تعیین اعتبارسنجی[۲] منابع است. مشتند پیش رو به ارائه راهکارهایی به منظور پیاده‌سازی امن سرویس DNS می‌پردازد.

در بخش اول این سند پس از ارائه مقدمه به بیان تهدیدات، دامنه بکارگیری و معرفی برخی اصطلاحات موجود در متن پرداخته خواهد شد. در بخش دوم موارد کلی امن سازی سرویس DNS به صورت تفصیلی شرح داده می‌شود. در بخش سوم چک لیست های متناسب ارائه می شود و در بخش آخر نیز مراحل انجام بندهایی از چک‌لیست بیان می‌شود.

قبل از مطالعه و اجرای این سند، نکات زیر باید مورد توجه قرار گیرد:

- از آن‌جا که ممکن است تنظیمات امن‌سازی، کارکردهای سیستم را مختل یا غیرفعال کند، لازم است قبل از اجرای تنظیمات، یک نسخه پشتیبان از پیکربندی سیستم تهیه شود.
- برای اجرای الزامات تعیین شده در این سند، اولویت با خط‌مشی‌های سازمان است. به عبارت دیگر اگر برخی از الزامات بیان شده در این سند، با خط‌مشی‌های سازمان تداخل یا تضاد داشت، اولویت با خط‌مشی‌های سازمان است.

---

[۱] -Domain name system

[۲] -Validation

- در تهیه این سند، سعی شده است که حداکثر الزامات مرتبط با حوزه‌ی سند، پوشش داده شود. اما این بدان معنا نیست که پس از اجرای این الزامات، سیستم به صورت صد در صد امن خواهد بود. الزامات بیان شده در این سند، حداقل انتظارات برای امن‌سازی در حوزه‌ی تعریف شده در این مستند است.

۱,۱ تعاریف و مفاهیم

قبل از توضیح انواع حملات و تهدیدات، به توضیح چند نمونه از اصطلاحات کاربردی در متن پرداخته می‌شود:

- **DNS Zone**: ساختار DNS، از زیردامنه‌های سلسله مراتبی ریشه تشکیل شده است، که اطلاعات مربوط به فضای نام دامنه را در Zone ذخیره می‌کنند. هر سرور نام برای یک Zone خاص معتبر است البته همزمان می‌تواند برای چند Zone نیز معتبر باشد. یک Zone بخشی از یک دامنه است. برای مثال ناحیه Microsoft.com تنها شامل اطلاعات مربوط به دامنه Microsoft.com و ارجاعاتی به سرورهای نام معتبر زیردامنه‌های مربوطه است و تنها در صورتی شامل اطلاعات مربوط به زیر دامنه‌ها(مانند marketing.microsoft.com) می‌شود که این اطلاعات به سرور دیگری محول نشده باشد.
- **DNS Resource Record** : پایگاه داده ناحیه DNS از مجموعه‌ای از رکوردهای منبع تشکیل شده که هر یک اطلاعاتی درباره مفهوم خاصی را بیان می‌کنند. برای مثال نگاشت آدرس (A)، نگاشت نام میزبان به آدرس IP را ثبت می‌کند. اشاره‌گر ارجاع معکوس[۳] (PTR)، نگاشت آدرس IP به نام میزبان را ثبت می‌کند. سرور از این رکوردها به منظور پاسخ‌گویی به پرس و جوهای درون ناحیه خودش استفاده می‌کند.
- **Alternative DNS Server** : برخی از سازمان‌ها از سرور پشتیبان یا جایگزین نام دامنه استفاده می‌کنند. این سرورها، DNS ریشه خود را به کار برده و فضای نام دامنه خود را که شامل دامنه‌های سطح بالای سفارشی است مدیریت می‌کنند.
- **Preferred DNS Server**: نخستین سروری است که جهت تعیین نام دامنه مورد استفاده قرار می‌گیرد.

---

[۳] - Reverse-Lookup Pointer

- **بازگشت (recursion)**: تکنیک تفکیک نام است که در آن سرور DNS به منظور تفکیک کامل نام از طرف کلاینت درخواست کننده، سایر سرورهای DNS را پرس و جو می‌کند و پاسخ را به کلاینت بازمی‌گرداند.
- **Root hints**: شامل لیستی از سرورهای DNS معتبر است که بر روی سرور ذخیره شده است و سرویس DNS با استفاده از آن می‌تواند سایر سرورهای DNS برای ریشه[۴] درخت فضای نام دامنه DNS، را بیابد.
- **DNS cache poisoning**: یا همان مسموم سازی کش DNS، به حملاتی اطلاق می‌شود که طی آن اطلاعات اشتباه به صورت عمدی وارد کش سرور DNS می‌شود و این اطلاعات اشتباه همان رکوردهای اشتباه هستند که منجر به نگاشت یک نام به آدرس IP نادرست می‌شود.
- **DNS Spoofing**: واژه‌ای است که به " پاسخ دادن به درخواست DNSای که برای سرور دیگری ارسال شده است" اطلاق می‌شود. مهاجم، آدرس IP سرور DNS را در فیلد آدرس مبدا بسته خود قرار داده و پاسخ DNS را جعل می‌کند.

۱,۲ تهدیدات موجود روی سرورهای DNS

در ادامه به طور مختصر فهرستی از تهدیدات موجود که ممکن است یک سرور DNS در معرض آن‌ها باشد، آورده شده است.

۱. Foot printing: فرآیندی که طی آن داده ناحیه[۵] DNS شامل نام دامنه، نام کامپیوترها، آدرس‌های IP منابع حساس شبکه توسط مهاجم آشکار می‌شود. مهاجم اغلب با استفاده از این داده‌ها حمله را آغاز می‌نماید و با استفاده از آن‌ها به عملکرد و موقعیت شبکه و سیستم‌های آن پی می‌برد.

۲. DDOS: سناریویی که طی آن مهاجم تلاش می‌کند تا جلوی دسترسی به خدمات شبکه را از طریق flooding یک یا چند سرور DNS بگیرد. هنگامی که یک سرور DNS در معرض حمله Flooding قرار گرفت، میزان استفاده از CPU به حداکثر رسیده و سرویس‌های سرور DNS غیر قابل دسترسی می‌گردد.

---

[۴] -Root

[۵] -DNS Zone data

۳. تغییر شکل داده[۶]: این مشکل زمانی رخ می‌دهد که مهاجم از طریق DNS یک شبکه را ردیابی کرده تا آدرس‌های IP معتبر آن شبکه را در بسته های IP جعلی خود استفاده کند، که همان IP Spoofing نامیده می‌شود.

۴. Redirection: سناریویی که در آن مهاجم توانایی تغییر جهت پرس و جوهای DNS به سمت سرورهای تحت کنترل خودش را به دست می‌آورد. یک روش برای redirection آلوده کردن کش سرور DNS با داده‌های اشتباه است، که پرس و جوهای بعدی را به سرورهای تحت کنترل مهاجم هدایت می‌کند.

۱,۳ دامنه

توصیه‌های امن سازی موجود در این مستند قابل بکارگیری بر روی کلیه سرورهای DNS شامل مایکروسافت، BIND و NSD قابل اعمال می‌باشد. البته در برخی موارد سرورهای خاصی استثنا شده‌اند که در متن به آن‌ها اشاره شده است. در بخش ضمیمه نیز مراحل اعمال این تنظیمات روی سرورهای ویندوز BIND آورده شده است.

۲. امن سازی

همان طور که بیان شد، DNS یک سرویس سلسله مراتبی به منظور تعیین آدرس IP میزبان‌ها در شبکه اینترنت است که می‌تواند به دو شیوه بازگشتی[۷] و تکرارشونده[۸] ارائه شود. از آن جا که DNS محل تجمع ارتباطی تمامی clientهاست، حوزه حساسی به شمار رفته و هدف خوبی برای مهاجمین شبکه محسوب می‌گردد. سرورهای DNS، از طریق سوء استفاده از پروتکل‌های DNS و همچنین سوء استفاده از حفره‌های نرم افزاری موجود روی برنامه‌های در حال اجرای سرور، می‌توانند مورد حمله قرار گیرند. این بخش به فهرستی از موارد کلی امن سازی سرویس DNS می‌پردازد که از وقوع حمله به بخش‌های مختلف DNS جلوگیری می‌کند.

در زمان پیاده سازی سرور امن DNS، ابتدا بایستی اطلاعاتی درباره محیط کسب کرد. این اطلاعات شامل ساختار و سلسله مراتب دامنه‌های داخلی و خارجی، شناسایی سرورهای DNSای که برای این نام‌های دامنه باید احراز هویت

---

[۶] -data modification

[۷] -Recursive

[۸] -Iterative

شوند و نیازمندی‌های کلاینت‌های DNS برای تجزیه و تحلیل میزبان‌های شبکه، خواهد بود. پس از جمع آوری این اطلاعات و با توجه به راهنمای آورده شده در این مستند، مدیر سیستم می‌تواند به اعمال مراحل امن سازی روی سرور بپردازد. مراحل مذکور به سه دسته کلی بررسی ارتباطات شبکه‌ای، پیکربندی سرور DNS و اعتبارسنجی داده تقسیم می‌شود. همچنین به منظور تامین کامل امنیت، تنظیماتی نیز برای امن سازی کلاینت‌ها توصیه می‌گردد که در ادامه هر یک به طور مفصل شرح داده خواهد شد. به عنوان توصیه کلی در مورد که از آخرین نسخه سیستم عامل همراه با وصله های به روز شده همان نسخه استفاده شود. همچنین توصیه می‌شود سرور DNS تنها برای این منظور اختصاص داده شده و سرویس دیگری روی آن ارائه نشود.

۲,۱ امن سازی محیط میزبان DNS

۲,۱,۱ امن سازی بستر DNS

لازم است که از آخرین نسخه سیستم عامل همراه با وصله های به روز شده همان نسخه استفاده شود. همچنین توصیه می‌شود سرور DNS تنها برای این منظور اختصاص داده شده و سرویس دیگری روی آن ارائه نشود.

۲,۱,۲ امن سازی نرم افزار DNS

امن سازی نرم افزار DNS شامل موارد زیر می باشد:

- آخرین نسخه نرم افزار نام دامنه به خصوص در مورد BIND عاری از تمامی موارد آسیب پذیری موجود در نسخه های قبلی است و بنابراین توصیه می‌شود مدیر سرور DNS از آسیب پذیری ها، سوء استفاده ها، مشکلات امنیتی و وصله های نسخه ای که در حال اجرا است، مطلع باشد(خواه آخرین نسخه باشد یا نسخه های قبلی آن).
- به منظور جلوگیری از افشای اطلاعات در مورد نسخه سرور DNS قابل اجرا در یک سیستم، این سرور می‌بایست طوری پیکر بندی شده باشد که امکان پرس و جو از اطلاعات نسخه آن وجود نداشته باشد. که

نحوه انجام این گام در ضمیمه ذکر شده است. نسخه سرور نام، مورد استفاده مهاجمی که به دنبال نسخه خاص آسیب پذیری هستند، قرار می‌گیرد.

- نرم افزار DNS نباید روی سیستمی به جز سرور اصلی نصب باشد. از آنجا که نرم افزار BIND به صورت پیش فرض روی برخی از نسخه‌های unix نصب است لازم است تا از پاک شدن این نرم افزار از روی تمامی سیستم ها به جز سرور نام ، اطمینان حاصل گردد

۲,۲ بررسی ارتباطات شبکه

۲,۲,۱ ارتباط با اینترنت

- درصورتی که میزبان‌های شبکه نیازی به تعیین[۹] نام روی اینترنت نداشته باشند، لازم است تمامی ارتباطات روی اینترنت و سرورهای DNS داخلی قطع شوند. برای این کار می‌توان از یک فضای نام خصوصی DNS که کاملا روی شبکه سازمان قرار دارد، استفاده نمود.
- درصورتی که میزبان‌های شبکه نیاز به تعیین نام روی اینترنت دارند، برای ارسال درخواست‌ها به سرور DNS خارجی، یک گروه از سرورهای DNS در FRD[۱۰] پیکربندی می‌شود. پیکربندی سرورهای DNS، باید در دامنه فرزند[۱۱] صورت گیرد تا درخواست‌ها را تنها به سرورهای DNS درون FRD ارسال نمایند. ارتباط بین سرورهای DNS داخلی و خارجی نیز می بایست توسط یک دیواره آتش[۱۲] فیلتر کننده بسته که تنها به ترافیک نوع UDP و TCP روی پورت ۵۳ اجازه ورود به سرور را می‌دهد، حفاظت شود.

۲,۲,۲ فضای نام DNS[۱۳]

- در صورتی که فضای نام DNS سازمان به دو بخش دامنه‌های داخلی و خارجی شکسته شده، می‌بایست فضای نام DNS داخلی روی سرور DNS درون شبکه داخلی قرار گرفته و فضای نام DNS خارجی روی

---

[۹] - Resolve
[۱۰] - Forest Root Domain
[۱۱] -Child
[۱۲] -firewall
[۱۳] - DNS namespace

سرور DNS شبکه محیطی[۱۴] قرار گیرد. سرورهای DNS داخلی نیز باید با قرار گرفتن در پشت فایروال حفاظت شوند. اگر کلاینت‌های داخلی نیازمند تعیین میزبان‌ها در فضای نام خارجی هستند، فضای نام DNS داخلی، می‌تواند زیردامنه‌ای از فضای نام DNS خارجی باشد. برای مثال اگر فضای نام DNS اینترنت سازمان example.com باشد، فضای نام DNS داخلی، برای چنین شبکه‌ای می‌تواند corp.example.com باشد.

- در صورتی که میزبان‌های شبکه داخلی نیازی به تعیین میزبان‌ها روی دامنه خارجی ندارند، فضای نام DNS داخلی می‌تواند همانند فضای نام DNS اینترنت سازمان باشد، اما باید از مجموعه متفاوتی از نام‌های دامنه برای میزبان‌های داخلی و خارجی استفاده کرد (به طوری که هم‌پوشانی نداشته باشند). برای مثال اگر فضای نام DNS والد[۱۵] سازمان .example.com باشد، فضای نام DNS داخلی برای چنین شبکه‌ای می‌تواند corp.example.com باشد.

۲,۳ پیکربندی سرور DNS

۲,۳,۱ محدودسازی انتقال ناحیه

به منظور افزایش امنیت لازم است تمامی انتقال‌های ناحیه به جز در مواقع لزوم غیر فعال شوندو فقط در صورت نیاز، انتقال ناحیه تنها به آدرس‌های IP خاص محدود شود. اجازه انتقال ناحیه به تمام سرورها، احتمال آشکار شدن داده‌های DNS را برای مهاجمی که قصد انجام footprint روی شبکه را دارد، بالا می‌برد. سرورهای پشتیبان[۱۶] تنها سرورهای نامی هستند که نیاز به روزرسانی فایل ناحیه به طور متناوب دارند بنابراین انتقال ناحیه در سرورهای مقدم[۱۷] باید به سرورهای پشتیبان محدود شود. در سرورهای پشتیبان نیز باید انتقال ناحیه به طور کامل غیر فعال شود. تنظیمات مربوطه در مورد BIND در بخش ضمیمه آمده است.

---

۱۴ - Perimeter Network

۱۵ -parent

۱۶ - Secondary

۱۷ -Primary

در مورد سرورهای ویندوزی نیز این محدود سازی به طور پیش فرض برای ناحیه‌هایی که Active Directory یکپارچه می‌باشد، غیر فعال است. برای نواحی غیر یکپارچه AD[۱۸]، تنظیمات پیش فرض تنها اجازه انتقال ناحیه را به سرورهایی می‌دهد که در رکورد منابع سرور DNS فهرست شده‌اند.

- پیکربندی نواحی با Active Directory یکپارچه[۱۹]

استفاده از نواحی با Active Directory یکپارچه، که امکان استفاده از فهرست کنترل دسترسی و به روزرسانی‌های پویای امنیتی را می‌دهد، منجر به افزایش سطح امنیت می‌گردد. از نواحی با Active Directory یکپارچه، تنها در صورتی می‌توان استفاده کرد که سرورهای DNS، Domain controller نیز باشند.

۲,۳,۲ پیکربندی فهرست کنترل دسترسی[۲۰](ACL)

به منظور امن سازی dns zone object container در درخت دایرکتوری از ACL استفاده می‌شود. این ویژگی دسترسی دانه‌ای[۲۱] (محدود) به ناحیه یا رکورد یک منبع خاص در ناحیه را فراهم می‌کند. در برخی پیاده سازی‌های DNS با استفاده از ACL می‌توان میزبان‌هایی را که قرار است در یک تراکنش خاص DNS شرکت داشته باشند، مشخص کرد. که این میزبان‌ها می‌توانند از طریق آدرس IP و یا آدرس زیرشبکه شان مشخص شوند. فهرست‌های کنترل دسترسی مختلفی برای انواع تراکنش‌های DNS وجود دارد. برای مثال در مورد سرورهای ویندوزی رکورد منبع ناحیه می‌تواند طوری محدود شود که اجازه به روزرسانی امنیتی پویا را تنها به یک کلاینت خاص یا یک گروه مانند گروه مدیران دامنه[۲۲] بدهد.

- به روزرسانی پویای امنیتی[۲۳]: در سرورهای ویندوزی به روز رسانی پویا می‌تواند امنیتی یا کلی باشد. برای حفاظت سرورهای DNS از حملات DNS Spoofing ، تنها باید از به روزرسانی پویای امنیتی استفاده شود.

---

۱۸ - Active Directory
۱۹ - AD integrated Zone
۲۰ -Access Control List
۲۱ - granulate
۲۲ - Domain Administrator
۲۳ -Secure Dynamic Update

- به‌روزرسانی پویا در BIND : در سرورهای BIND ، به روزرسانی پویا می‌تواند با عبارت Update-policy محدود می‌شود. عبارت Update-policy حقوق دسترسی به‌روزرسانی را به یک یا چند رکورد منبع انتخابی محدود می‌کند.
- تهیه لیست کنترل دسترسی جهت اجرای وظایف مدیریتی: توصیه می‌شود یک لیست کنترل دسترسی برای سرور DNS پیکربندی شود که تنها به افراد خاص اجازه اجرای وظایف مدیریتی بدهد.
- تهیه لیست کنترل دسترسی جهت اجرای وظایف خاص: توصیه می‌شود یک لیست کنترل دسترسی برای رکوردهای DNS پیکربندی شود که تنها به افراد خاص اجازه ایجاد، تغییر و یا پاک کردن داده‌ها DNS را بدهد.

۲,۳,۳ پیکربندی لیست مسدود پرس و جوی سراسری[۲۴]

استفاده از ویژگی لیست مسدود پرس و جوی سراسری، مانع از ثبت نام میزبان توسط کاربران بدخواه[۲۵] می‌شود. (این قابلیت تنها در سرورهای ویندوزی قابل دسترسی است)

۲,۳,۴ استفاده از پورت مبدا تصادفی (پیکربندی Socket pool[۲۶])

ترافیک خروجی سرور DNS بایستی از پورت های تصادفی ارسال شود تا امکان حدس پورت برای مهاجمین وجود نداشته باشد. این امر امنیت سرور DNS را در برابر حملات مسموم سازی cache، افزایش می‌دهد. در مورد سرورهای ویندوزی مخزن Socket، سرور DNS را قادر می‌سازد از قابلیت پورت مبدا تصادفی در پردازش درخواست‌های DNS استفاده کند.

---

[۲۴] - Global Query Block List

[۲۵]- برای برخی برنامه‌های کاربردی می‌تواند معنی خاص داشته و به آن‌ها اجازه منحرف کردن ترافیک شبکه را بدهد.

[۲۶] - Socket Pool

۲,۳,۵ پیکربندی قفل کش[۲۷]

با فعال سازی قفل cache، سرور DNS به رکوردهای cache اجازه بازنویسی در مدت زمان TTL[۲۸] را نخواهد داد. قابلیت قفل cache، همچنین امنیت سرور DNS را در برابر حملات مسموم سازی cache، افزایش می‌دهد. (این قابلیت تنها در سرورهای ویندوزی قابل دسترسی است)

۲,۳,۶ محدود سازی پاسخ DNS به واسط‌های انتخابی[۲۹]

به طور پیش فرض، سرور DNS به تمامی درخواست‌هایی که به تمام آدرس‌های IP اش ارسال شوند، پاسخ می‌دهد (این آدرس‌ها می‌توانند همگی روی یک واسط شبکه و یا هر کدام بر روی یک واسط شبکه جداگانه پیکربندی شوند). به منظور افزایش سطح امنیت، سرویس DNS بایستی تنها به IP هایی که توسط کلاینت‌های سرور DNS به عنوان سرور مقدم[۳۰] استفاده شده‌اند، پاسخ دهد. در مورد سرورهای BIND با استفاده از عبارت allow-query می‌توان لیست میزبان‌هایی را که پاسخ/درخواست به یا از آن‌ها مجاز است، تعیین نمود که در ضمیمه آمده است.

۲,۳,۷ پیکربندی Root hint داخلی

Root hints به طور معمول، شامل نام سرورها و آدرس منابع ریشه اینترنت می‌باشد. به منظور آگاهی از آسیب پذیری‌های امنیتی و انجام به‌روزرسانی‌های مورد نیاز مدیر سرور باید به طور منظم محتوای فایل Root hint را بررسی کند. چنانچه از سرویس DNS روی یک شبکه خصوصی استفاده شود، می‌توان root hints را با رکوردهای مشابه که به سرورهای DNS ریشه داخلی اشاره می‌کنند، جایگزین کرد. این امر مانع از ارسال اطلاعات خصوصی توسط سرورهای DNS داخلی، روی اینترنت می‌شود.

---

۲۷ - cache locking

۲۸ - Time to live

۲۹ - Selected Interface

۳۰ - preferred

در زمان اجرای سرویس DNS در سرورهای ویندوزی روی کنترل کننده دامنه[۱]، root hints ابتدا از active directory خوانده می‌شود. در صورتی که سرویس DNS روی کنترل کننده دامنه اجرا نشود، یا root hints در active directory وجود نداشته باشد، root hints با استفاده از فایل Cache.dns که در مسیر %systemroot%\System32\Dns قرار دارد، اجرا می‌شود.

۲,۳,۸ غیر فعال سازی بازگشت

جهت حفاظت از سرورهای DNS، بازگشت روی تمام سرورهایی که نیاز به اجرای پرس و جوی بازگشتی ندارند، غیر فعال شود. در صورت فعال بودن بازگشت، مهاجم می‌تواند از فرآیند بازگشت برای تعیین نام دامنه اشتباه برای آدرس‌های IP استفاده کند. بنابراین توصیه می‌شود استفاده از بازگشت تا حد امکان محدود گردد.

۲,۳,۹ امن سازی کش DNS

آلودگی کش زمانی رخ می‌دهد که پاسخ پرس و جو حاوی داده نامعتبر یا بدخواه باشد. گزینه Secure cache against pollution مانع از آلودگی cache سرور DNS، توسط مهاجم با رکوردهای منبع درخواست نشده می‌گردد. این گزینه به طور پیش فرض فعال است. (این قابلیت تنها در سرورهای ویندوزی قابل دسترسی است)

۲,۴ اعتبارسنجی پرس و جوها وپاسخ‌های DNS

تکنولوژی‌های زیر از طریق اعتبارسنجی ارتباطات سرور به سرور، و سرور به کلاینت، امنیت را افزایش می‌دهند.

DNSSEC ۲,۴,۱

توسعه امنیت سیستم نام دامنه[۲] (DNSSEC)، مجموعه‌ای از برنامه‌های افزودنی[۳] است که امنیت را به پروتکل DNS اضافه می‌کنند. DNSSEC، با استفاده از امضاهای رقمی[۴]، پاسخ‌های DNS را برای سرورها قابل اعتماد می‌سازد و حفاظت بسیار خوبی در برابر حملات DNS Spoofing انجام می‌دهد. سرورهای نامی که برای استفاده از

---

۱ -Domain Controller

۲ - Domain Name System Security Extensions

۳ -Suite of extensions

۴ - Digital signatures

DNSSEC توسعه می‌یابند، باید به منظور اجرای پردازش‌های DNSSEC پیکربندی شوند. در مورد سرورهای ویندوزی و NSD چنانچه فایل ناحیه، شامل رکورد منبع DNSSEC باشد به طور خودکار بارگذاری شده و سرور پاسخ را با فعال سازی DNSSEC ارسال می‌کند. اما در صورت استفاده از BIND بایستی فعال سازی در فایل پیکربندی با نام named.conf صورت گیرد. (به ضمیمه مراجعه شود.)

IPsec ۲,۴,۲

IPsec، راه حل مناسبی برای حفاظت از سیستم‌ها و اطلاعات در برابر حملات شبکه است. IPsec، احتمال دستکاری یا قطع داده ارسالی بین دو سرور DNS، را به حداقل می‌رساند. در صورت فعال سازی IPsec هر دو انتهای یک ارتباط پیش از شروع ارتباط، اعتبارسنجی می‌شوند. IPsec همچنین می‌تواند به منظور حفاظت از ارتباط بین سرورهای DNS و کلاینت‌ها در برابر حملات DNS Spoofing (پاسخ اشتباه به پرس و جوی کلاینت توسط منابع غیر مجاز) پیاده‌سازی گردد. لازم به ذکراست که امن سازی از طریق IPsec در لایه شبکه اعمال می‌شود و مستقل از پروتکل DNS و لایه کاربرد می‌باشد.

- امن سازی انتقال ناحیه با استفاده از IPsec : می‌توان با استفاده از IPsec انتقال ناحیه را حفاظت نمود. این امر با درخواست مجوز برای ارتباطات بین سرورهای DNS اولیه[۱] و ثانویه[۲] حاصل می‌گردد.

۲,۴,۳ اعتبارسنجی از طریق کد هش TSIG

در این روش حفاظت از تراکنش و اعتبار سنجی درخواست/ پاسخ DNS با استفاده از کلید TSIG انجام می‌گیرد. فرآیند "اعتبارسنجی مبدا پیام از طریق کد اعتبارسنجی پیام هش شده"[۳] (HMAC) در DNS با نام TSIG شناخته می‌شود. HMAC از پیام ورودی و یک کلید سری [۴] استفاده کرده و خروجی با نام کد اعتبارسنجی پیام[۵] (MAC) یا هش تولید می‌کند. فرستنده پیام از تابع HMAC برای تولید MAC استفاده نموده و آن را برای دریافت کننده پیام

---

۱ - primary

۲ -secondary

۳ - Hash-based message authentication code

۴ - secret

۵ - Message authentication code

ارسال می‌کند. و دریافت کننده‌ای که از همان کلید و تابع HMAC فرستنده استفاده می‌کند، کد پیام دریافتی را محاسبه می‌نماید و سپس MAC محاسبه شده را با MAC دریافتی مقایسه کرده و در صورت یکسان بودن از صحت پیام دریافتی اطمینان حاصل می‌کند. مقدار MAC تولید شده توسط فرستنده در رکورد منبع جدیدی به نام رکورد TSIG قرار می‌گیرد. رکورد TSIG علاوه بر MAC تولید شده شامل نام الگوریتم هش، نام کلید، زمان تولید هش می‌باشد. BIND8.2 اولین نسخه‌ای بود که از قابلیت TSIG پشتیبانی می‌کرد و در حال حاضر نیز آخرین نسخه BIND9.x از این قابلیت پشتیبانی می‌کند. لازم به توضیح است که ویندوز از این قابلیت پشتیبانی نمی‌کند.

عملیات زیر جهت فعال سازی ارتباطات DNS برای استفاده از TSIG مورد نیاز است:

- ساعت سیستمی سرورهای نام شرکت کننده در تراکنش DNS (پشتیبان و مقدم) باید همزمان شوند.
- باید یک تولید کننده کلید سری موجود باشد که کلیدهایی با طول و آنتروپی مناسب تولید کند. فایل کلید که شامل رشته کلید است بایستی به شکل امن بین سرورهای شرکت کننده در تراکنش مبادله گردد.
- اطلاعات کلید بایستی با عبارات خاصی در فایل پیکربندی مشخص گردد(عبارت key و عبارت server در فایل named.conf در BIND 9.x).

۲,۵ کلاینت‌های DNS

به منظور امن سازی کلاینت های DNS نیز توصیه می‌شود موارد زیر روی آن ها اعمال گردد:

۲,۵,۱ تعیین آدرس استاتیک برای سرور DNS

در صورت امکان آدرس IP استاتیک مشخصی برای سرور DNS مقدم[۱] و پشتیبان[۲] برای استفاده کلاینت‌ها در نظر گرفته شود. اما در صورتی که پیکربندی کلاینت‌ها به گونه‌ای است که آدرس سرور DNS را به طور خودکار و از طریق سرور DHCP تعیین می‌کنند، میزان امنیت کلاینت ها به امنیت سرور DHCP بستگی دارد. با تنظیم آدرس سرور DNS مقدم و ذخیره به صورت استاتیک برای کلاینت‌ها، یکی از راه‌های حمله به سیستم ها بسته خواهد شد.

---

[۱] -preferred DNS Server

[۲] -Alternate DNS Server

۲,۵,۲ بررسی کلاینت‌های در ارتباط با سرور

کلاینت‌هایی که به سرور DNS دسترسی دارند باید مورد بررسی قرار گیرند. در صورتی که سرور DNS طوری پیکربندی شده که تنها به آدرس‌های خاصی گوش کند، تنها کلاینت‌هایی که برای استفاده از این سرور به عنوان سرور مقدم و یا ذخیره تنظیم شده‌اند، بایستی با آن ارتباط برقرار کنند.

۳. چک لیست

در ادامه چک لیست متناظر برای امن سازی DNS در سه بخش ارائه شده است.

۳,۱ چک لیست امن سازی سرورهای ویندوزی DNS مستقل از Active Directory

چک لیست اول مربوط به گزینه‌های موجود امن سازی بدون اجرای سرور روی Domain controller و بدون ذخیره DNS Zone در active directory می‌باشد.

ردیف	عنوان فعالیت	وضعیت
۱.	نصب آخرین نسخه نرم افزار نام دامنه و اعمال وصله‌های امنیتی به صورت دوره‌ای	بلی/خیر
۲.	غیر فعال ساختن امکان پرس و جو از اطلاعات نسخه سرور نام (ضمیمه بخش ۵,۱,۱)	بلی/خیر
۳.	فعال ساختن پیکربندی socket pool	بلی/خیر
۴.	فعال ساختن پیکربندی قفل کش[۱]	بلی/خیر
۵.	استفاده از یک فرستنده[۲] برای اشاره به سایر سرورهای DNS در صورت عدم توانایی در پاسخ دهی محلی[۳]	بلی/خیر
۶.	محدود ساختن انتقال ناحیه[۴] به سرورهایی که در منبع سرور نام فهرست شده اند.	بلی/خیر
۷.	پیکربندی سرورهای DNS به منظور گوش کردن به آدرس IP های خاص (به ضمیمه بخش ۵,۱,۵ مراجعه شود).	بلی/خیر
۸.	فعال ساختن گزینه Cache pollution prevention به منظور جلوگیری از آلوده شدن کش، در تمامی سرورهای DNS (به ضمیمه بخش ۵,۱,۶ مراجعه شود).	بلی/خیر
۹.	فعال ساختن به روزرسانی‌های پویای امنیتی برای ناحیه DNS (به ضمیمه بخش ۵,۱,۲ مراجعه شود).	بلی/خیر
۱۰.	برقراری ارتباط با سرورهای DNS خارجی با استفاده از دیواره آتش و تنها از طریق فهرست محدودی از آدرس های مبدا و مقصد.	بلی/خیر
۱۱.	پیکربندی فایل root hint[۵] طوری که به سرورهای root اینترنت اشاره کند.(برای سرورهای DNS خارجی که پیش روی[۶] فایروال قرار دارند، به ضمیمه بخش ۵,۱,۷ مراجعه شود).	بلی/خیر

۱ - cache locking

۲ - forwarder

۳ -local

۴ -zone transfer

۵- فایلی در DNS سرور ها که شامل آدرس های IP ونام Root Zone هاست.

6- in front

۱۲.	اجرای پاسخ های نام اینترنت توسط سرورهای پروکسی و gateway	بلی/خیر
۱۳	اعمال تنظیمات مربوط به DNSSEC	بلی/خیر
۱۴	استفاده از از IPsec برای ارتباطات سرورهای DNS	بلی/خیر

۳,۲ چک لیست امن سازی سرور ویندوزی با ذخیره DNS Zone در Active Directory

چک لیست دوم شامل پیکربندی مشابه بخش قبل است. با این تفاوت که سرور DNS روی یک کنترل کننده دامنه[۱] اجرا شده و ناحیه های DNS در Active Directory ذخیره می‌شوند. این امر منجر به فراهم شدن گزینه‌های امنیتی بیشتر و سطح امنیتی بالاتر می‌گردد. در عین حال برای به دست آوردن این سطح از امنیت فرض شده است که ارتباط DNS با اینترنت کاملا حذف شده است. البته این یک توصیه اجباری نیست اما زمانی که به ارتباط با اینترنت نیازی نیست، شدیدا توصیه می‌شود:

ردیف	عنوان فعالیت	وضعیت
۱.	قطع ارتباط سرورهای DNS داخلی سازمان با اینترنت	بلی/خیر
۲.	نصب آخرین نسخه نرم افزار نام دامنه و اعمال وصله‌های امنیتی به صورت دوره‌ای	بلی/خیر
۳.	غیر فعال ساختن امکان پرس و جو از اطلاعات نسخه سرور نام (ضمیمه بخش ۵,۱,۱)	بلی/خیر
۴.	فعال ساختن پیکربندی Global Query Block List فعال	بلی/خیر
۵.	فعال ساختن پیکربندی socket pool	بلی/خیر
۶.	فعال ساختن پیکربندی قفل کش[۲]	بلی/خیر
۷.	استفاده شبکه سازمان از فضای نام و ریشه DNS[۳] داخلی	بلی/خیر
۸.	استفاده از آدرس‌های IP سرور DNS داخلی برای سرورهای DNS که با فرستنده‌ها، پیکربندی شده‌اند.	بلی/خیر
۹.	محدود ساختن انتقال ناحیه[۴] به آدرس‌های IP خاص(به ضمیمه بخش ۵,۱,۳ مراجعه شود).	بلی/خیر
۱۰.	پیکربندی سرورهای DNS به منظور گوش کردن به آدرس IP های خاص (به ضمیمه بخش ۵,۱,۵ مراجعه شود).	بلی/خیر
۱۱.	فعال ساختن گزینه Cache pollution prevention در تمامی سرورهای DNS (به ضمیمه بخش	بلی/خیر

[۱] -Domain Controller

[۲] - cache locking

[۳] -DNS Root

[۴] -zone transfer

	۵,۱,۶ مراجعه شود).	
۱۲.	پیکربندی فایل Root hint طوری که به سرورهای DNS داخلی اشاره کند(برای سرورهای DNS خارجی که پیش روی[۱] فایروال قرار دارند - ضمیمه بخش ۵,۱,۷)	بلی/خیر
۱۳.	تهیه یک لیست کنترل دسترسی[۲] برای سرو که تنها به افراد خاص اجازه اجرای وظایف مدیریتی[۳] بدهد(اجرای تمام DNS سرورها روی کنترل کننده های دامنه).	بلی/خیر
۱۴.	ذخیره ناحیه های DNS در Active Directory	بلی/خیر
۱۵.	تهیه یک لیست کنترل دسترسی برای رکوردهای DNS که تنها به افراد خاص اجازه ایجاد، تغییر و یا پاک کردن داده‌ها DNS را بدهد.	بلی/خیر
۱۶.	پیکربندی به روزرسانی‌های پویای امنیتی برای ناحیه‌های DNS بجز نواحی سطح بالا[۴] و نواحی ریشه[۵](که اصلا اجازه هیچ نوع به روزرسانی را ندارند- ضمیمه بخش ۵,۱,۲).	بلی/خیر

۳,۳ چک لیست امن سازی سرور BIND

چک لیست زیر مربوط به توصیه‌های امنیتی است که در سرورهای غیر ویندوزی و به طور خاص BIND قابل اعمال است.

ردیف	عنوان فعالیت	وضعیت
۱.	نصب آخرین نسخه نرم افزار نام دامنه و اعمال وصله‌های امنیتی به صورت دوره‌ای	بلی/خیر
۲.	غیر فعال ساختن امکان پرس و جو از اطلاعات نسخه سرور نام (ضمیمه بخش ۵,۲,۱)	بلی/خیر
۳.	حذف نرم افزار DNS از تمامی سیستم ها به جز سرور اصلی (که نرم افزار BIND به صورت پیش فرض روی برخی از نسخه‌های unix نصب است) .	بلی/خیر
۴.	استفاده شبکه سازمان از فضای نام و ریشه DNS[۶] داخلی(اگر ناحیه DNS داخلی باشد)	بلی/خیر
۵.	استفاده از آدرس‌های IP سرور DNS داخلی برای سرورهای DNS که با فرستنده‌ها، پیکربندی شده‌اند.	بلی/خیر
۶.	محدود ساختن انتقال ناحیه[۷] به آدرس‌های IP خاص(ضمیمه بخش ۵,۲,۴).	بلی/خیر
۷.	تعیین لیست میزبان‌هایی که پاسخ/درخواست به یا از آن‌ها مجاز است با استفاده از عبارت allow-query (ضمیمه بخش۵,۲,۴).	بلی/خیر

۱ - in front
۲ - DACL(discretionary access control list)
۳ -Administrative Task
۴ - Top-level zones
۵ - root Zones
۶ -DNS Root
۷ -zone transfer

۸.	محدود ساختن انتقال ناحیه در سرورهای مقدم به سرورهای پشتیبان و فعال ساختن انتقال ناحیه در سرورهای پشتیبان تنها در صورت لزوم (ضمیمه بخش۵,۲,۴).	بلی/خیر
۹.	فعال ساختن انتقال ناحیه در سرورهای پشتیبان تنها در صورت لزوم (ضمیمه بخش۵,۲,۴).	بلی/خیر
۱۰.	محدود ساختن تراکنش‌های درخواست/پاسخ با توجه به نیاز، به محدوه آدرس معین (ضمیمه بخش۵,۲,۴).	بلی/خیر
۱۱.	حفاظت تراکنش ها از طریق اعتبارسنجی کد هش TSIG (ضمیمه بخش۵,۲,۵).	بلی/خیر
۱۲.	ارسال ترافیک خروجی سرور DNS از پورت های تصادفی	بلی/خیر
۱۳.	امن سازی درخواست/پاسخ سرورDNS با استفاده از DNSSEC (ضمیمه بخش ۵,۲,۳).	بلی/خیر
۱۴.	محدود ساختن به روزرسانی پویا با عبارت Update-policy به یک یا چند رکورد منبع انتخابی (ضمیمه بخش ۵,۲,۴).	بلی/خیر

۴. منابع

1. http://technet.microsoft.com/en-us/library/cc770474.aspx
2. Ramaswamy Chandramouli , Scott Rose. Secure Domain Name System (DNS) Deployment Guide. . September 2013 .U.S. National Institute of Standard and Technology Department of Commerce
3. Florent Carli. Security issues dns. 2003.SANS GSEC Practical Assignment
4. Paula Baily, Brian Kipper , Carl Beaudry. Domain Name System (DNS) Security Architecture. 2011. U.S. Department of Homeland Security
5. www.dnssec.net
6. Domain Name System (DNS) Security Strategies. August 2012. Australian Government Department of Defence Intelligence and security

۵. ضمیمه - مراحل اعمال تنظیمات

۵,۱ تنظیمات بخش امن سازی ویندوز

جهت اعمال تنظیمات ذکر شده در بخش امن سازی پس از نصب Dnscmd به طریق زیر عمل شود:

۵,۱,۱ پنهان سازی نسخه DNS

با دستور **config/** و تغییر مشخصه **EnableVersionQuery** و غیر فعال سازی آن می‌توان نسخه DNS را پنهان ساخت.

۵,۱,۲ مراحل اعمال پیکربندی امن به روزرسانی‌های پویا

۱.روی **Start** کلیک کنید، **Administrative Tools** را انتخاب کنید، روی **DNS** کلیک کنید.

۲.در کنسول **DNS**، روی ناحیه قابل اجرا[۱] کلیک راست نموده و **Properties** را انتخاب کنید.

۳.روی تب **General**، نوع ناحیه را **Active Directory-Integrated** انتخاب کنید.

۴.در **Dynamic updates**، روی **Secure only** کلیک کنید.

۵,۱,۳ مراحل اعمال پیکربندی محدودسازی انتقال ناحیه

۱. روی **Start** کلیک کنید، **Administrative Tools** را انتخاب کنید، روی **DNS** کلیک کنید.

۲. در کنسول **DNS**، روی ناحیه DNS کلیک راست نموده و **Properties** را انتخاب کنید

۳. روی تب **Zone Transfers**، یکی از اقدامات زیر را انجام دهید:

- جهت غیر فعال کردن انتقال ناحیه، علامت گزینه **Allow zone transfers** را بردارید.
- جهت فعال سازی انتقال ناحیه، گزینه **Allow zone transfers** را انتخاب کنید.

۴. در صورتی که انتقال ناحیه را انتخاب کردید، اقدامات زیر را نیز انجام دهید:

---

[۱] - applicable

- برای فعال سازی انتقال ناحیه[۲] روی سرورهایی که در تب **Name Servers** (سرور نام) لیست شده‌اند، روی تب **Only to servers listed on the Name Servers** کلیک کنید.
- برای فعال سازی انتقال ناحیه روی سرورهای DNS خاص، **Only to the following servers** را انتخاب کرده و سپس آدرس های مورد نظر را وارد نمایید

۵,۱,۴ مراحل غیر فعال کردن بازگشت

۲. روی **Start** کلیک کنید، **Administrative Tools** را انتخاب کنید، روی **DNS** کلیک کنید.

۳. در کنسول **DNS**، روی سرور DNS قابل اجرا[۳] کلیک راست نموده و **Properties** را انتخاب کنید.

۴. تب **Advanced**را انتخاب کنید.

۵. در بخش **Server options**، گزینه **Disable recursion (also disables forwarders)** را انتخاب و دکمه **ok** را کلیک کنید.

۵,۱,۵ مراحل محدود سازی آدرس IP هایی که سرور به آن‌ها گوش می‌کنند

۱. . روی **Start** کلیک کنید، **Administrative Tools** را انتخاب کنید، روی **DNS** کلیک کنید.

۲. **در** کنسول **DNS**، روی سرور DNS قابل اجرا[۴] کلیک راست نموده و **Properties** را انتخاب کنید.

۳. در منوی **Action**، **Properties** را انتخاب کنید.

۴. در تب **Interfaces**، **Only the following IP addresses** را انتخاب کنید..

۵. در بخش آدرس IP، آدرس سرور مورد نظر را نوشته و **Add** را انتخاب کنید.

۶. مراحل قبلی را به ازای آدرس هر سرور تکرار کنید.

۵,۱,۶ مراحل فعال سازی گزینه Secure cache against pollution

۱. روی **Start** کلیک کنید، **Administrative Tools** را انتخاب کنید، روی **DNS** کلیک کنید.

---

[۲] -zone transfer

[۳] - applicable

[۴] - applicable

۲. **در** کنسول **DNS** ، روی سرور DNS قابل اجرا[۵] کلیک راست نموده و **Properties** را انتخاب کنید.

۳. در منوی **Action**، **Properties** را انتخاب کنید.

۴. در منوی **Action**، **Properties** را انتخاب کنید.

۵. تب **Advanced** را انتخاب کنید.

۶. در بخش **Server options**،گزینه را **Secure cache against pollution** انتخاب کنید

۵،۱،۷ مراحل پیکر بندی فایل Root hint

۱. روی **Start** کلیک کنید، **Administrative Tools** را انتخاب کنید، روی **DNS** کلیک کنید.

۲. **در** کنسول **DNS** ، روی سرور DNS قابل اجرا[۶] کلیک راست نموده و **Properties** را انتخاب کنید.

۳. در منوی **Action**، **Properties** را انتخاب کنید.

۴. تب **Root Hints** را انتخاب کنید

- در این بخش می‌توانید آدرس مورد نظر را به سرورهای فهرست اضافه نموده و یا از آن حذف نمایید. همچنین می توان در این بخش اسامی سرور ها و آدرس های آن ها را ویرایش و یا کپی نمود.

۵،۲ تنظیمات بخش امن سازی BIND

۵،۲،۱ پنهان سازی نسخه DNS

در مسیر /etc/named.conf لازم است دستور زیر وارد شود:

```
Option {
 version none;
```

---

[۵] - applicable

[۶] - applicable

};

۵,۲,۲ غیر فعال سازی بازگشت

در مسیر /etc/named.conf لازم است دستور زیر وارد شود:

```
Option {
 Recursion no;
};
```

۵,۲,۳ فعال کردن استفاده از DNSSEC

در مسیر /etc/named.conf لازم است دستور زیر وارد شود:

```
options {
dnssec-enable yes;
};
```

برای اطلاعات بیشتر در رابطه با استفاده از DNSSEC به [2] مراجعه شود.

۵,۲,۴ محدود سازی تراکنش ها بر اساس آدرس‌های IP

هر یک از دستورات زیر می‌توانند بخشی از تراکنش‌ها را با توجه به لیست دریافتی از آدرس‌های IP و یا فهرستی از زیرشبکه‌ها محدود سازند.

تراکنش DNS	قالب دستور مورد نظر
محدود سازی درخواست/پاسخ بر اساس فهرست آدرس	allow-query { address_match_list }
محدود سازی بازگشت بر اساس فهرست آدرس	allow-recursion { address_match_list }
محدود سازی انتقال ناحیه بر اساس فهرست آدرس	allow-transfer { address_match_list }
محدود سازی به‌روزرسانی بر اساس فهرست آدرس	allow-update { address_match_list }

حذف فهرستی از آدرس‌ها از تراکنش‌های DNS	blackhole { address_match_list }

لازم به توضیح است که هر یک از فهرست ها با نام مربوطه و به وسیله عبارت acl ذخیره می‌شوند:

acl internal_hosts {192.158.43.3; 192.158.43.6; 192.158.44.56;};

سپس با استفاده از عبارات آمده در جدول و به شکل زیر محدود سازی صورت می‌گیرد:

options { allow-query { internal_hosts; };

- or –

allow-recursion { internal_hosts; }; };

۵,۲,۵ فعال سازی استفاده از کد اعتبارسنجی TSIG

به منظور استفاده از کلید TSIG در تراکنش‌ها، ابتدا باید آن را تولید نمود:

dnssec-keygen -a HMAC-SHA256 –b 112 -n HOST ns1-ns2.example.com

که در این دستور a– نام الگوریتم هش، b- طول کلید، n- نوع کلید و عبارت آخر نیز نام کلید می‌باشد.

به منظور استفاده از کلید در تمام تراکنش ها (درخواست/پاسخ، به‌روزرسانی، انتقال ناحیه) باید از دستور زیر استفاده نمود:

server 192.249.249.1 { keys { ns1-ns2.example.com.; };

اما در صورت نیاز به استفاده از کلید در یک نوع خاص از تراکنش از دستور زیر استفاده می‌شود:

(دستور زیر تنها به سرور نام هایی که از کلید ns1-ns2.example.com استفاده می‌کنند، اجازه درخواست انتقال ناحیه را می‌دهد.)

zone “example.com”

{ type master;

file “zonedb.example.com”;

allow-transfer { key {ns1-ns2.example.com.}; }; };