پیکربندی امن

Bind Name Server

مرکز مدیریت راهبردی افتا

DNSR-LNX-SER-9-0.0

آذر ۹۵

فهرست

پیش‌گفتار

مرکز مدیریت راهبردی افتا[1] به منظور ساماندهی امنیت تجهیزات در حوزه فاوا[2]، پروژه «پیکربندی امن محصولات IT در کشور» را آغاز نموده است. یکی از گام‌های اساسی در این پروژه ارائه چک‌لیست و راهنمای پیکربندی امن برای محصولات IT می‌باشد. ارائه چک‌لیست برای محصولات داخلی بر عهده تولیدکننده محصول می‌باشد. تولید کننده ملزم است، چک‌لیست خود را در غالب ارائه شده از سمت مرکز افتا ارائه دهد. چک‌لیست‌های ارائه شده، توسط مرکز افتا مورد ارزیابی قرار گرفته و منتشر می‌گردد. سازمان‌های دولتی ملزم به استفاده از چک لیست‌های مذکور برای محصولات در حال استفاده خود هستند. همچنین سازمان‌های دولتی موظفند قبل از استفاده از محصولات IT، آن‌را مطابق چک‌لیست امنیتی مورد تایید مرکز افتا پیکربندی نمایند.

توجه به این نکته حائز اهمیت می‌باشد که چک‌لیست‌های ارائه شده، یک امنیت سطح پایه برای محصول ایجاد می‌نماید و سازمان‌ها ملزم هستند که برای رسیدن به سطح امنیت مورد نیاز خود، پس از اجرای مدیریت ریسک[3]، الزامات دیگری را نیز به این تنظیمات اضافه و مستند نمایند.

[1] امنیت فضای تولید و تبادل اطلاعات
[2] فناوری اطلاعات و ارتباطات
[3] Risk management

مقدمه

این سند راهنمایی برای پیکربندی امن Bind Name Server است. در این سند مقادیر و تنظیمات امن برای سیاست‌های پیکربندی محصول مذکور ارائه شده است. مخاطب با استفاده از این سند توانایی پیاده‌سازی تنظیمات ارائه شده را خواهد داشت.

مرکز مدیریت راهبردی افتا ضمن استقبال از نظرات کارشناسان و متخصصان این حوزه برای غنای بیشتر این سند و دیگر اسناد مقاوم سازی، آمادگی دریافت پیشنهادات سازنده از طریق آدرس پست الکترونیکی Hardening@aftasec.ir را اعلام می‌دارد.

در ادامه، تنظیمات مورد نیاز برای پیکربندی امن Bind Name Server آمده است. در این سند هر تنظیم با یک نام لاتین و شماره مختص آن آورده شده است. برای هر الزام دو بخش شرح اجمالی و نحوه پیاده‌سازی ارائه شده است. در بخش شرح اجمالی، توضیحی مختصر از ماهیت الزام بیان گردیده و در بخش نحوه پیاده‌سازی نیز، راهنمایی برای پیاده‌سازی الزام توسط مدیر سامانه ارائه شده است.

جدول ۱: گروه‌بندی و اختصارسازی نام برای محصولات IT

محصولات IT	
نام گروه	شماره گروه
نرم افزار آنتی ویروس	AV
سرویس‌دهنده نرم‌افزارهای کاربردی[۱]	AS
احراز اصالت[۲]	AU
اتوماسیون	AT
نرم‌افزار مدیریت پیکربندی[۳]	CM
سیستم مدیریت پایگاه داده	DB
نرم‌افزار کاربردی رومیزی[۴]	DA
سرویس گیرنده رومیزی[۵]	DC
سرویس دایرکتوری[۶]	DS
DNS سرور	DN
ایمیل سرور	ES
نرم‌افزار کاربردی سازمانی[۷]	EA
دیوار آتش[۸]	FI
تجهیزات قابل حمل[۹]	HD
مدیریت هویت[۱۰]	IM
سیستم تشخیص نفوذ[۱۱]	ID

[۱] Application Server
[۲] Authentication
[۳] Configuration Management System
[۴] Desktop Application
[۵] Desktop Client
[۶] Directory Service
[۷] Enterprise Application
[۸] Firewall
[۹] Handheld Device
[۱۰] Identity Management
[۱۱] Intrusion Detection System

محصولات IT	
نام گروه	شماره گروه
سرویس‌دهنده ایمیل[۱]	MS
راهکارهای موبایلی[۲]	MO
مسیریاب شبکه[۳]	RO
سوئیچ شبکه	SW
سیستم عامل	OS
تجهیزات جانبی[۴]	PD
سرویس دهنده[۵]	SR
نرم‌افزار مجازی‌سازی[۶]	VI
مرورگر وب	WB
سرویس‌دهنده وب	WS

[۱] Mail Server
[۲] Mobile Solution
[۳] Network Router
[۴] Peripheral Device
[۵] Server
[۶] Virtualization Software

تنظیمات

DNSR-1: طراحی و معماری

DNSR-1-1: استفاده از یک معماری Split-Horizon

شرح اجمالی:

اجرای یک معماری Split-Horizon DNS به اجرای DNS سرورها و سرویس‌های قابل‌اعتماد برای پرس‌وجوهای خارجی DNS مجزا از DNS سرورهای قابل‌اعتماد داخلی، اشاره می‌کند. این معماری همه پرس‌وجوهایی که از داخل سازمان سرچشمه می‌گیرند را پاسخ می‌دهد. سرویس‌های خارجی جهت تهیه فقط مقدار محدودی اطلاعات برای سرویس‌هایی که جهت مکاتبه با کلاینت‌ها و سرویس‌های خارجی مورد نیاز هستند، پیکربندی شده‌اند. معمولا، اطلاعات در DNSی که به‌صورت خارجی موجود هست، حداقل مقدار اطلاعات لازم برای سرویس‌هایی مانند: email، web، و سیستم‌های درگاه مانند VPNs می‌باشد. سرویس DNS مجزای داخلی معمولا مجموعه اطلاعات بهتری که برای کلاینت‌های داخلی نیاز است، تهیه می‌نماید.

نحوه پیاده‌سازی:

معماری Split-Horizon را برای جداسازی سرویس‌های داخلی و خارجی DNS اجرا کنید. سرویس‌های خارجی DNS باید فقط به نام‌های مورد قبول از سرویس‌های خارجی، مانند: web، email و سرویس‌های VPN، پاسخ دهد.

DNSR-1-2: عدم نصب یک سیستم Multi-Use

شرح اجمالی:

پیکربندی‌های پیش‌فرض سرور، معمولا یک تنوع وسیعی از سرویس‌های غیر ضروروی را نمایش می‌دهند که ریسک سیستم را افزایش می‌دهد. صرفاً اینکه سرور می‌تواند سرویس‌های زیادی را اجرا کند به معنی اجرا کردن همه آن‌ها نمی‌باشد. تعداد daemons و سرویس‌هایی که روی ISC BIND اجرا می‌شود باید به مواردی که ضروری هستند تا سرویس DNS تنها تابع اصلی سرور شود، محدود گردند.

نحوه پیاده‌سازی:

تمامی سرویس‌های غیر ضروری را غیرفعال کنید یا سرویس‌های ضروری اصلی را با DNS به سرور دیگری انتقال دهید. مدیریت‌کننده پکیج یا سرویس‌ها برای سیستم‌عامل جهت غیرفعال یا حذف کردن سرویس‌های غیرنیاز نصب شده، بکار ببرید. روی سیستم‌های Red Hat، دستورات زیر برای حذف یا غیرفعال کردن یک سرویس ممکن است استفاده شوند.

```
# yum erase
# systemctl disable .service
```

DNSR-1-3: نقش اختصاصی Name Server

شرح اجمالی:

یک name server ممکن است برای یک یا چند دامنه‌ای که برای آن‌ها در راستای فراهم کردن اطلاعات پیکربندی شده است، یک name server قابل‌اعتماد باشد. یک name server فقط قابل‌اعتماد[۱]، فقط به پرس‌وجوهای دامنه‌هایی که برای آن‌ها پیکربندی شده است پاسخ می‌دهد، و پرس‌وجوهای دیگر دامنه‌ها را رد خواهد کرد. یک name server حافظه‌ای[۲] به پرس‌وجوهای همه‌ی دامنه‌ها پاسخ خواهد داد. یک name server حافظه‌ای با ارسال پرس‌وجوهای DNS به‌صورت برگشتی به دیگر name servers و سپس ذخیره پاسخ در حافظه خود جهت فراهم کردن پاسخ سریع‌تر به پرس‌وجوی بعدی برای نام، پاسخ‌ها را می‌گیرد. یک name server فقط حافظه‌ای، برای هر دامنه‌ای قابل‌اعتماد نیست. در واقع BIND DNS names server باید به‌صورت فقط حافظه‌ای یا فقط قابل‌اعتماد باشد نه هر دوی آن‌ها، پیکربندی گردد.

نحوه پیاده‌سازی:

Name server فقط قابل‌اعتماد:

برای پیاده‌سازی حالت "فقط قابل‌اعتماد" عبارت allow-recursion را از داخل فایل name.conf را به مقدار localhost تغییر دهید، یا این مقدار را به آن اضافه نمایید:

```
options {
. . .
allow-recursion { local; };
```

[۱] Authoritative

[۲] Caching

Name server فقط حافظه‌ای:

برای حالت فقط حافظه‌ای، عبارت "non-local zone" را از فایل پیکربندی حذف کنید و سپس سرور را بازنشانی کنید.

DNSR-1-4: استفاده از DNS سرورهای حافظه‌ای upstream امن

شرح اجمالی:

معمولا name servers حافظه‌ای پرس‌وجوها را به name server حافظه‌ای دیگری ارسال می‌کنند تا به سرویس نام اجازه دهند که به‌صورت متراکم کار کند و عملکرد را با استفاده از مزایای حافظه سرور نام upstream، بهبود دهند. در واقع name server حافظه‌ای پیش‌فرض تهیه شده بوسیله‌ی تهیه‌کننده سرویس اینترنت (ISP) معمولا از این روش استفاده می‌نماید. همچنین اینکه به سرورهای ناامنی خارج از خط‌مشی‌های امنیتی و کنترلی سازمان تکیه شود، ممکن است یک ضعف امنتی باشد.

نحوه پیاده‌سازی:

دستورات زیر اجرا گردند:

- معماری شبکه، سرورهای DNS پذیرفته‌شده، و ترافیک خروجی DNS به جز برای سرورهای DNS پذیرفته‌شده، را مرور و بازبینی کنید.
- یک تهیه‌کننده DNS خارجی که به‌طور موثر ترافیک بدخواه DNS را باتوجه به الزمات سازمانی سبک کند، را انتخاب کنید.
- سرورهای DNS خارجی پذیرفته‌شده را مرور، آزمایش و مستندسازی کنید، و سرورهای DNS فقط حافظه‌ای داخلی را جهت استفاده از سرورهای DNS حافظه‌ای خارجی پذیرفته‌شده، پیکربندی کنید.

DNSR-1-5: نصب کردن ISC BIND 9

شرح اجمالی:

محک[1] ISC BIND استفاده از پکیج‌های باینری فراهم شده توسط فروشنده پلت‌فرم، که برای اکثر موقعیت‌ها در راستای کاهش تلاش و افزایش کارایی نگه‌داری و وصله‌های امنیتی می‌باشد، را توصیه می‌کند. این محک برای سیستم RHEL7[2] تست شده است.

نحوه پیاده‌سازی:

بر حسب سیستم عامل خود اقدام به نصب نسخه ISC Bind نمایید. برای Hat Red نسخه ۷ با استفاده از دستورات زیر نصب را انجام دهید.

```
# yum install bind
. . .
# yum install bind-chroot
. . .
```

DNSR-2: محدودسازی مجوزها و مالکیت

DNSR-2-1: اجرای BINDبه عنوان کاربر غیر ریشه

شرح اجمالی:

برای راه‌اندازی BIND، باید به عنوان کاربر ریشه آن را اجرا کرد. بعد از راه‌اندازی اولیه، BIND قابلیت تغییر به کاربر غیر ریشه را دارد، بنابراین بعد از راه‌اندازی اولیه به آن اجازه حذف مجوزهای ریشه داده شود.

نحوه پیاده‌سازی:

با استفاده از دستورات زیر کاربری با نام named و گروهی با همین نام را در صورت عدم وجود ایجاد نمایید. تنظیم shell این کاربر را نیز /dev/null قرار دهید. در نسخه حاضر این کاربر در زمان نصب BIND ایجاد می‌گردد و BIND نیز توسط این کاربر اجرا می شود و نیاز به اقدامی در این مرحله نیست.

```
if ! id named; then
  groupadd -g 53 named
  useradd -m -u 53 -g 53 -c "BIND named" -d /var/named -s /dev/null named
fi 2>/dev/null
```

[1] Benchmark

[2] Red Hat Enterprise Linux 7

همچنین اگر در فایل /etc/sysconfig/named برای پارامتر options، مقدار u named– تنظیم نشده است، آن را تنظیم کنید.

DNSR-2-2: اختصاص یک shell غیرمعتبر به حساب کاربر BIND

شرح اجمالی:

حساب کاربر BIND، که به‌صورت پیش‌فرض named می‌باشد، نباید به عنوان یک حساب ورود معمول استفاده شود، و باید به آن یک ورود نامعتبر یا یک شل nologin اختصاص داده شود تا اطمینان ایجاد شود که این حساب نمی‌تواند برای login استفاده گردد.

نحوه پیاده‌سازی:

برای کاربر named با استفاده از دستور زیر، shell را به nologin تغییر دهید.

```
# chsh -s /sbin/nologin named
```

DNSR-2-3: قفل کردن حساب کاربر BIND

شرح اجمالی:

حساب کاربری پیش‌فرضی که BIND با آن اجرا می‌شود نباید رمزعبور معتبر داشته باشد، ولی باید قفل گردیده باشد.

نحوه پیاده‌سازی:

این کاربر به صورت پیش فرض قفل است. برای اطمینان از قفل بودن آن، دستور زیر را اجرا کنید:

```
# passwd -S named
```

DNSR-2-4: تنظیم مالک فولدرهای BIND به کاربر root

شرح اجمالی:

تمامی فولدرهایی که ISC BIND تحت آن اجرا می‌شود باید مالک آن ریشه باشد. البته، هر فایلی که در زمان اجرای BIND ایجاد شودف مالک آن کاربر named خواهد ماند.

نحوه پیاده‌سازی:

برای درست کردن مالک فولدر، دستور زیر را اجرا نمایید.

```
chown -R root $BIND_HOME $RUNDIR
```

DNSR-2-5: تنظیم مالک فایل‌های پیکربندی BIND به کاربر root

شرح اجمالی:

فایل‌های پیکربندی در فولدرهای ISC BIND باید دارای مالک ریشه باشند. البته، هر فایلی که در زمان اجرای BIND ایجاد شده باشد، مانند: فایل‌های pid، فایل‌های لاگ و فایل‌های slave zone، نیاز است که مالک آن‌ها کاربر named باشد.

نحوه پیاده‌سازی:

دستورات زیر را اجرا کنید:

- هر فایل غیرضروری را حذف، و مطمین شوید که هر فایل زمان اجرا در فولدر زمان اجرای مناسب، ایجاد شده است. فایل nonroot-files.txt فایلی برای اطمینان از مالک بودن ریشه برای فایل‌های پیکربندی می‌باشد.

```
# find $BIND_HOME -type f \! -user root | egrep -v \
\^$DYNDIR\|\^$SLAVEDIR\^$DATADIR\|\^$RUNDIR\|\^$LOGDIR\|\^$TMPDIR > \
$TMPDIR/nonroot-files.txt
```

- فایل‌های باقیمانده که مربوط به زمان اجرا نمی‌باشند، باید به مالک ریشه تغییر داده شوند، این کار با استفاده از دستوری مانند زیر اجرا می‌شود:

```
# cat $TMPDIR/nonroot-files.txt | xargs chown root
# rm $TMPDIR/nonroot-files.txt
```

DNSR-2-6: تنظیم گروه named یا ریشه برای فولدرها و فایل‌های پیکربندی BIND

شرح اجمالی:

تمام فایل‌ها و فولدرهای BIND باید یک گروه named یا ریشه داشته باشند.

نحوه پیاده‌سازی:

دستور زیر را برای تغییر گروه همه فایل‌ها و فولدرهای BIND به named، اجرا کنید:

```
chgrp -R named $BIND_HOME $RUNDIR
```

DNSR-2-7: تنظیم گروه و دیگر مجوزهای دایرکتوری‌های غیر زمان‌اجرای BIND به فقط-خواندی

شرح اجمالی:

تمامی دایرکتوری‌های BIND (به جز آن‌هایی که مربوط به زمان‌اجرا هستند) که در BIND داخل آن‌ها فایل‌ها را ایجاد خواهد کرد، باید گروه و مجوزهایشان به غیر قابل نوشتن تنظیم گردد. هیچ دایرکتوری داخل BIND_HOME یا RUNDIR نباید مجوزهای نوشتن داشته باشد، به جز دایرکتوری chroot'ed tmp که نیاز به قابلیت نوشتن بوسیله گروه named را دارد.

نحوه پیاده‌سازی:

مراحل زیر را انجام گردند:

- فایل‌های که نباید مجوز نوشتن آن‌ها فعال باشد مشخص شود و فایل‌هایی که مربوط به زمان اجرا می‌باشند و بوسیله گروه named قابل نوشتن هستند مشخص گردد و داخل فایل write_dirs.txt قرار گیرد، دستور زیر این فایل‌ها را مشخص می‌سازد:

```
# find $BIND_HOME -type d -perm /020 | egrep -vx
$DYNDIR\|$SLAVEDIR\|$DATADIR\|$RUNDIR\|$LOGDIR\|$TMPDIR
# find $BIND_HOME $RUNDIR -type d -perm /002
```

- هدف دایرکتوری‌های شناسایی شده بازبینی گردد و در صورت عدم نیاز به آن‌ها، حذف گردند یا مجوزهای آن‌ها به غیر قابل نوشتن تغییر داده شود.

- دستور زیر را برای تغییر مجوزهای دایرکتوری‌های مناسب، اجرا کنید:

```
xargs -a write-dirs.txt chmod go-w
```

DNSR-2-8: تنظیم گروه و دیگر مجوزهای همه فایل‌های BIND به فقط-خواندی

شرح اجمالی:

همه فایل‌های داخل BIND home و دایرکتوری‌های زمان اجرا، باید گروه و مجوزهایی با قابلیت نوشتن داشته باشند. فایل‌های پیکربندی باید قابلیت نوشتن به وسیله‌ی named را نداشته باشند، و هر فایل زمان اجرا ایجاد شده بوسیله BIND دارای مالک named و قابل نوشتن بوسیله کاربر باشد. بنابراین، استثنایی برای فایل‌های زمان اجرا لازم نمی‌باشد.

نحوه پیاده‌سازی:

مراحل زیر را انجام گردند:

- دستور زیر را برای اطمینان از فقط-خواندنی بودن فایل‌های BIND برای گروه و دیگران اجرا کنید، و نتیجه را داخل یک فایلی با نام $TMPDIR/write-files.txt قرار دهید.

```
# find $BIND_HOME $RUNDIR -type f -perm /022
```

- هدف فایل‌های شناسایی شده بازبینی گردد و در صورت عدم نیاز به آن‌ها، حذف گردند یا مجوزهای آن‌ها به غیر قابل نوشتن تغییر داده شود.
- دستور زیر را برای تغییر مجوزهای فایل‌های مناسب، اجرا کنید:

```
# find $BIND_HOME $RUNDIR -type f -perm /022 > $TMPDIR/write-files.txt
# xargs -a $TMPDIR/write-files.txt chmod go-w
# rm $TMPDIR/write-files.txt
```

DNSR-2-9: ایزوله کردن BIND با زیردایرکتوری chroot'ed

شرح اجمالی:

فراخوانی سیستمی ()chroot باعث اجرای یک برنامه به دسترسی محدود به سیستم فایل می‌شود که در نتیجه یک زیردایرکتوری به عنوان دایرکتوری ریشه برای یک محیط برنامه، عمل می‌کند. وقتی که این عمل صورت گیرد یک برنامه به اصطلاح زندانی ("jailed") می‌شود و دیگر به همه ساختار فایل دسترسی ندارد و دسترسی آن به زیردایرکتوری مشخص شده، محدود می‌شود.

نحوه پیاده‌سازی:

مراحل زیر انجام گردند:

- دستور زیر را برای متوقف کردن سرویس named و نصب پکیج bind-chroot جهت فراهم کردن دایرکتوری‌های chroot، اجرا کنید:

```
# systemctl stop named.service
# yum install bind-chroot
```

- فایل پیکربندی /etc/sysconfig/named را ویرایش کنید و دستور زیر را جهت تنظیم متغیر محیط ROOTDIR، اجرا کنید:

```
ROOTDIR="/var/named/chroot"
```

- تمامی فایل‌های پیکربندی و هر فایل مربوط به ناحیه اصلی را به داخل دایرکتوری مربوط به آن‌ها در زیردایرکتوری /var/named/chroot قرار دهید.
- ایجاد لینک‌های symbolic از جفتی از فایل‌های /etc مانند /etc/named.conf و /etc/rndc.key به فایل‌های واقعی داخل زیردایرکتوری chroot-ed می‌تواند مفید باشد، بنابراین امکانی مانند rndc مطابق انتظار کار خواهد کرد. لینک‌های hard یا symbolic از داخل chroot به منابع خارجی ایجاد نکنید ولی بالعکس آن را ایجاد کنید.
- برای بازنشانی سرویس named و تست کردن آن، دستور زیر را اجرا کنید:

```
# systemctl start named.service
```

DNSR-3: محدودسازی پرس‌وجوها

DNSR-3-1: نادیده گرفتن پرس‌وجوهای ناخواسته و اشتباه

شرح اجمالی:

سرویس‌دهنده BIND می‌تواند طوری پیکربندی شود تا درخواست‌هایی که از بخش‌های خاصی از شبکه سرچشمه می‌گیرند را نادیده بگیرد. این امکان با پیاده‌سازی گزینه blackhole داخل named.conf بدست می‌آید. توصیه می‌شود که این ویژگی برای نادیده گرفتن درخواست‌هایی که از منابعی غیر از بخش‌های مورد انتظار شبکه سرچشمه می‌گیرند، پیاده‌سازی شود.

نحوه پیاده‌سازی:

جهت اضافه کردن گزینه blackhole برای آدرس‌های لینک محلی و چندپخشی، و همه آدرس‌های خصوصی مربوط به RFC 1918 که استفاده نمی‌شوند، دستور زیر را اجرا کنید:

```
blackhole {
     // Private RFC 1918 addresses
    10/8; 192.168/16; 172.16/12;
    // Multicast
    224/8;
    // Link Local
    169.254/16;
};
```

DNSR-3-2: محدود کردن پرس‌وجوهای بازگشتی

شرح اجمالی:

پرس‌وجوی DNS بازگشتی، پرس‌وجوی DNS معمول از کلاینت به DNS سرور حافظه‌ای می‌باشد. این پرس‌وجو بار پیدا کردن پاسخ را روی DNS سرور حافظه‌ای قرار می‌دهد که آن هم به صورت بازگشتی بقیه DNS سرورهای قابل‌اعتماد را برای دامنه‌های مربوطه استفاده می‌نماید، تا وقتی که پاسخ را دریافت و به کلاینت برگرداند. سپس DNS سرور پاسخ مربوط به پرس‌وجو را تا منقضی شدن زمان اعتبار آن درخواست، جهت پاسخ سریع به پرس‌وجوهای یکسان در آینده، در حافظه نگهداری می‌کند. سرویس‌دهنده BIND می‌تواند به گونه‌ای پیکربندی گردد که اجرای جست‌جوهای برگشتی را فقط به بخش‌ها و هاست‌های دارای مجوز شبکه، محدود نماید. این

امکان با استفاده از گزینه allow-recursion ممکن می‌گردد. سرورهای نام غیر قابل‌اعتماد حافظه‌ای فقط باید اجازه پرس‌وجوهای بازگشتی را به کلاینت‌هایی بدهند که روی شبکه‌های دارای مجوز آن‌ها قرار دارند. سرورهای نام قابل‌اعتماد نباید اجازه پرس‌وجوهای بازگشتی را به جز به هاست محلی، فراهم نمایند.

نحوه پیاده‌سازی:

سرور نام قابل‌اعتماد:

برای یک نام قابل‌اعتماد، دستور زیرا را داخل گزینه‌های سراسری یا داخل هر قسمت ناحیه وارد کنید:

```
allow-recursion { localhost; };
```

سرور نام حافظه‌ای:

- یک لیست کنترل دسترسی با نام trusted_clients تعریف کنید، این لیست شبکه‌ای را که قادر به استفاده از سرور حافظه‌ای DNS و همچنین اجازه ارسال پرس‌وجوهای DNS به‌صورت بازگشتی خواهند بود، را مشخص می‌نماید.

```
acl trusted_clients { 10.19.4.0/28; . . . }
```

- دستور زیرا داخل گزینه‌های سراسری وارد کنید:

```
allow-recursion { localhost; trusted_clients };
```

DNSR-3-3: محدود کردن خاستگاه‌های پرس‌وجو

شرح اجمالی:

سرویس‌دهنده BIND می‌تواند طوری پیکربندی شود تا دسترسی به سرویس‌های پرس‌وجو را بر اساس آدرس IP مبدا، محدود نماید. توصیه می‌شود که گزینه allow-query برای محدود کردن دسترسی فقط به شبکه‌های دارای مجوز جهت استفاده از سرور نام، استفاده گردد.

نحوه پیاده‌سازی:

- با دستور زیر، در فایل named.conf یک لیست کنترل دسترسی برای شبکه‌های مطمئن دارای مجوز، ایجاد کنید:

```
acl authorized_networks { 10.10.32.0/24; 10.10.34.0/24; . . . };
```

- با دستور زیر، عبارت allow-query رادر گزینه‌های سراسری مربوط به named.conf به همراه لیست کنترل دسترسی محلی و شبکه‌های مطمئن دارای مجوز، وارد کنید:

```
allow-query { localhost; authorized_networks };
```

DNSR-3-4: محدود کردن پرس‌وجوهای حافظه نهان

شرح اجمالی:

گزینه allow-query-cache در BIND، ممکن است برای محدود کردن یا اجازه دادن به BIND، در راستای تهیه پاسخ‌هایی برای پرس‌وجوها، از حافظه صحیح پرس‌وجوهایی که قبلا حل شده‌اند، استفاده گردد. یک سرور نام فقط حافظه‌ای، نباید ذخیره پرس‌وجوها به جز پرس‌وجوهایی از localhost را اجازه دهد، همچنین باید این اجازه را به لیست شبکه‌های دارای مجوز، بدهد.

نحوه پیاده‌سازی:

سرور نام فقط قابل‌اعتماد:

برای یک نام قابل‌اعتماد، دستور زیرا را داخل گزینه‌های سراسری یا داخل هر قسمت ناحیه وارد کنید:

```
allow-query-cache { localhost; };
```

سرور نام فقط حافظه‌ای:

- یک لیست کنترل دسترسی با نام trusted_clients تعریف کنید، این لیست شبکه‌ای را که قادر به استفاده از سرور حافظه‌ای DNS و همچنین اجازه ارسال پرس‌وجوهای DNS به‌صورت بازگشتی خواهند بود، را مشخص می‌نماید.

```
allow-query-cache { localhost; trusted_clients };
```

DNSR-4: امضاهای تراکنش--TSIG

DNSR-4-1: استفاده از کلیدهای TSIG با طول ۲۵۶ بیت

شرح اجمالی:

کلیدهای راز TSIG که بوسیله‌ی سرور نام استفاده می‌شوند باید توسط یک منبع خوب آنتروپی تولید شود و حداقل طول ۲۵۶ بیت داشته باشد.

نحوه پیاده‌سازی:

کلیدهایی که طول خیلی کوچک دارند را با کلیدی که به‌صورت امنی تولید شده و طول آن ۲۵۶ یا ۵۱۲ می‌باشد، جایگزین کنید. دستور dnssec-keygen زیر را برای تولید کلید، اجرا کنید:

```
$ dnssec-keygen -a HMAC-SHA256 –b 256 -n HOST ns1-ns2.cisecurity.org.
$ cat Kns1-ns2.cisecurity.org.+163+21730.key
ns1-ns2.cisecurity.org. IN KEY 512 3 163
ezoZopbE4Q73HShuFYlf3FRvLWjtNXI5fd0TeQAYOug=
```

DNSR-4-2: وارد کردن فایل‌های کلید رمزنگاری

شرح اجمالی:

کلیدها را به‌طور مستقیم در named.conf مربوط به BIND قرار ندهید، بلکه از فایل‌های پیکربندی مجزایی برای کلیدها استفاده کنید و آن‌ها را داخل named.conf قرار دهید، این کار کلیدها را از آشکارسازی ناخواسته حفاظت می‌کند.

نحوه پیاده‌سازی:

هر عبارت تعریف کلید را از فایل named.conf به فایل کلید خودش انتقال دهید. توصیه می‌شود که کلید و فایل کلید را به منظور جلوگیری از اشتباه، نام گذاری کنید. سپس با دستور include ، فایل‌های کلید را به داخل named.conf وارد کنید. به عنوان مثال، دستورات زیر را برای انجام مراحل توضیح داده شده، اجرا کنید:

```
# grep -C 1 include /etc/named.conf
// Include the key file used for the host1 and host2 TSIG comms
include "/etc/private/host1-host2.cisecurity.org.key";
# cat /var/named/chroot/etc/private/host1-host2.cisecurity.org.key
```

```
key host1-host2.cisecurity.org {
algorithm hmac-sha256;
secret "1R3DP9D81/yWXjqf3hlg2beRpti1883JnZ3s7RVb1HU=";
};
```

DNSR-4-3: استفاده از کلیدهای منحصربه‌فرد برای هر جفت هاست

شرح اجمالی:

یک کلید TSIG منحصربه‌فرد باید برای هر جفت از هاست‌های مکاتبه‌ای استفاده شود. برای مثال اگر یک سرور نام قابل‌اعتماد اصلی و سه سرور نام قابل‌اعتماد فرعی وجود دارد که توسط سرور اصلی به‌روزرسانی می‌شوند، آنگاه برای هر یک از موارد زیر یک کلید TSIG منحصربه‌فرد نیاز می‌باشد.

- Master <-> Slave1
- Master <-> Slave2
- Master <-> Slave3

نحوه پیاده‌سازی:

برای مکاتبه‌ی هاست به هاست کلیدهای منحصربه‌فرد تولید کنید. دستور زیر را برای تولید دو فایل، و فایل <anem>.key و فایل <name>.private به همراه کلیدهای راز با طول مناسب با کدگذاری base64، اجرا کنید: خود فایل‌ها تولید شده نیاز نیستند، و باید بعد از اینکه مقادیر آن‌ها داخل فایل کلید کپی شد، به صورت امنی حذف گردند.

```
$ dnssec-keygen -a HMAC-SHA256 –b 256 -n HOST ns1-ns2.cisecurity.org
Kns1-ns2.cisecurity.org.+163+13013
$ cat Kns1-ns2.cisecurity.org.+163+13013.key
ns1-ns2.cisecurity.org. IN KEY 512 3 163
9FQ2dYCQ17HJwDi/uHgANh2dlb8M7eb+F4AjML8tTdA=
```

DNSR-4-4: محدود کردن دسترسی به همه فایل‌های کلید

شرح اجمالی:

کلیدهای TSIG باید فقط توسط حساب‌های ریشه و named قابل خواندن باشند. هیچ حساب کاربر دیگری یا گروهی نباید دسترسی خواندن داشته باشد. سرویس‌دهنده BIND اغلب یک کلید نشست هنگام راه‌اندازی برای

استفاده توسط nsupdate –l، ایجاد می‌کند. ضمناً هر دو فایل $BIND_HOME و $RUNDIR وارد می‌شوند زیرا کلید نشست باید مجوزهای توصیه شده داشته باشد.

نحوه پیاده‌سازی:

- دستور زیر را برای پیدا کردن فایل‌های کلید راز، اجرا کنید: همچنین لیست فایل‌های کلید را مرور کنید و فایل‌های بدون استفاده و غیرضروری را حذف کنید و بعد از حذف، لیست را دوباره ایجاد کنید.

```
# find $BIND_HOME $RUNDIR -type f | xargs fgrep -l secret | sort -u >
$TMPDIR/key_files.txt
```

- دستورات زیر رای برای تغییر دادن مالکیت، گروه و مجوزهای فایل‌های کلید، اجزا کنید:

```
# xargs -a $TMPDIR/key_files.txt chown -R root
# xargs -a $TMPDIR/key_files.txt chgrp -R named
# xargs -a $TMPDIR/key_files.txt chmod o-r
```

- دستور زیر را برای حذف فایل موقت، اجرا کنید:

```
rm $TMPDIR/key_files.txt
```

DNSR-4-5: حفاظت از فایل‌های کلید TSIG حین توسعه

شرح اجمالی:

فایل‌های کلید TSIG را از طریق شبکه انتقال ناامن فایل‌ها موقع توسعه، یا از طریق مجوزها یا اشتراک گذاری‌های روی سیستم‌های میانه که برای توسعه کلید استفاده می‌شوند، در معرض افشا قرار ندهید.

نحوه پیاده‌سازی:

- رویه توسعه تصحیح گردد تا انتقال امن و حفاظت ذخیره‌سازی میانی کلیدها حین توسعه، تضمین شود.
- کلیدهای جدید با استفاده از رویه اصلاح شده تولید گردد و همه کلیدهای TSIG قبلی جایگزین شوند.

DNSR-5: احرازهویت به‌روزرسانی‌ها و انتقالات ناحیه

DNSR-5-1: احرازهویت انتقالات ناحیه به صورت امن

شرح اجمالی:

انتقال ناحیه یک مکانیزمی است که معمولا توسط توسعه‌های DNS استفاده می‌شود تا اطلاعات ناحیه را از سرورهای اصلی/اولیه به فرعی/ثانویه کپی کند. هر جفت سرورهای نام که جزیی از انتقالات ناحیه هستند باید درخواست‌ها را احرازهویت کنند و جامعیت پاسخ‌ها را با استفاده از کلید راز TSIG منحصربه‌فرد اشتراکی، تضمین نمایند. سرویس‌دهنده BIND می‌تواند با استفاده از عبارت allow-transfer به همراه عبارت کلید، پیکربندی شود تا فقط به درخواست‌های انتقال احرازهویت شده پاسخ دهد.

نحوه پیاده‌سازی:

کلیدهای TSIG با طول ۲۵۶بیت تولید کنید، که برای هر ارتباط/مکاتبه هاست-به-هاست منحصربه‌فرد باشد. کلیدها را به صورت امنی انتقال و پیکربندی کنید تا در عبارت‌های allow-transfer مورد نیاز باشد.

DNSR-5-2: احرازهویت به‌روزرسانی‌های پویا به‌صورت امن

شرح اجمالی:

به‌روزرسانی‌های پویا برای اتوماتیک کردن به‌روزرسانی نواحی استفاده می‌شوند. معمولا به همراه DHCP استفاده می‌شوند، با این وجود به‌روزرسانی‌ها ممکن است رکوردهای دیگر را وارد کنند. گزینه allow-update اجازه حذف و اضافه کردن هر رکورد منبع یک ناحیه به جز رکوردهای SOA و NS را می‌دهد، و نباید مورد استفاده قرار گیرد. در عوض گزینه update-policy اجازه مشخص کردن خط‌مشی ریزبه ریز بیشتری را فراهم می‌سازد و بنابراین انواع رکورد منبع و زیر دامنه‌های مشخصی می‌تواند به‌روزرسانی گردد. گزینه update-policy باید به صورت امنی با یک شناساننده کلید نسبت به آدرس IP، احرازهویت گردد. شناساننده کلید ممکن است یک کلید TSIG، یک کلید GSS-TSIG، یا یک کلید SIG(0) را مشخص نماید.

نحوه پیاده‌سازی:

- هر گزینه allow-update را از پیکربندی گزینه‌های سراسری پاک کنید.
- گزینه‌های allow-update را به فایل‌های ناحیه اضافه یا جایگزین کنید تا به صورت امنی یک شناساننده کلید TSIG یا SIG(0)، به همراه دامنه یا زیردامنه مناسب و نوع رکورد منبع مناسب تولید کند.

DNSR-5-3: احرازهویت ارسال به‌روزرسانی به‌صورت امن

شرح اجمالی:

یک سرور نام قابل‌اعتماد ثانویه اجازه دارد که به‌روزرسانی‌های ناحیه را از طرف سرور نام اصلی بپذیرد، و آن‌ها را به سرورنام اصلی ارسال نماید، هنگامی که فایل ناحیه امکان به‌روزرسانی شدن دارد. در این مورد، احرازهیت به‌روزرسانی‌های پویا با گزینه allow-update-forwarding پیکربندی شده است. درخواست‌های به‌روزرسانی باید به صورت امنی با یک شناساننده کلید نسبت به آدرس IP، احرازهویت گردد. شناساننده کلید ممکن است یک کلید TSIG، یک کلید GSS-TSIG، یا یک کلید SIG(0) را مشخص نماید.

نحوه پیاده‌سازی:

هر گزینه allow-update-forwarding را برای مشخص کردن یک شناساننده کلید TSIG یا SIG(0) که به صورت امنی تولید شده و با DHCP سرور استفاده می‌شود، اصلاح کنید.

DNSR-6: نشر اطلاعات

DNSR-6-1: پنهان کردن عبارت نسخه BIND

شرح اجمالی:

سرویس‌دهنده BIND یک ناحیه built-in را شامل می‌شود، version.bind ممکن است برای گرفتن نسخه سرور نام مورد استفاده قرار گیرد. نسخ ممکن است برای غیرفعال کردن نسخه اطلاعات به مقدار none تنظیم گردد.

نحوه پیاده‌سازی:

دستور زیر را برای اضافه کردن یا اصلاح کردن گزینه نسخه به مقدار none در گزینه‌های سراسری BIND، اجرا کنید:

```
options {
version none;
. . .
}
```

DNSR-6-2: پنهان کردن ID سرور نام

شرح اجمالی:

گزینه server-id یک شناساننده سرور را تهیه می‌کند که در جواب پرس‌وجوی NSID برگردانده خواهد شد. یک پرس‌وجوی NSID در RFC-5001 تشریح شده است، و یک روش برای شناسایی سرورها در محیطی می‌باشد که چندین DNS سرورهایی وجود دارد که آدرس IP یکسانی را به اشتراک می‌گذارند. با استفاده از تعادل بار و دیگر مکانیزم‌های اشتراک گذاری IP، تشخیص اینکه دقیقا کدام سرور نام به یک پرس‌وجوی مشخص پاسخ می‌دهد، مشکل است. روش NSID به سرور نام اجازه پاسخ با شناسایی اطلاعات را می‌دهد. گزینه server-id باید با مقدار none غیرفعال گردد.

نحوه پیاده‌سازی:

برای اینکه به صورت صریح پشتیبان NSID را غیرفعال کنید، دستور زیر را برای اصلاح یا اضافه کردن گزینه server-id در گزینه سراسری BIND به مقدار none، اجرا کنید:

```
server-id none;
```

DNSR-7: امن کردن مکاتبات شبکه

DNSR-7-1: عدم تعریف یک سورس پورت ثابت

شرح اجمالی:

سرویس‌دهنده BIND می‌تواند طوری پیکربندی گردد که همیشه از یک سورس پورت یکسان برای مکاتبه با دیگر DNS سرورها استفاده کند. این توانایی از طریق گزینه query-source port، و گزینه query-source-v6 port امکان‌پذیر می‌باشد. توصیه می‌شود در صورت استفاده از گزینه query-source، سورس پورت حذف گردد، یا پورت با استفاده از "*" مشخص گردد، بنابراین پورت دیگر یک مقدار ثابت نخواهد داشت.

نحوه پیاده‌سازی:

مشخص کننده پورت را از گزینه query-source یا query-source-v6 حذف کنید یا از "*" برای شماره پورت استفاده کنید.

DNSR-7-2: فعال کردن اعتبار سنجی DNSSEC

شرح اجمالی:

افزونه‌های امنیتی DNS یا به اختصار DNSSEC، احرازهویت سرورهای نام را از طریق کلید رمزنگاری عمومی فراهم می‌آورند. با DNSSEC، سرور نام پاسخ‌ها را با استفاده از کلید خصوصی‌اش امضا می‌کند. این کار به بقیه سرورهای نام اجازه داشتن کلید عمومی سرور نام را برای تایید کردن جامعیت و صحت پاسخ، فراهم می‌سازد. توصیه می‌شود که DNSSEC فعال باشد و پیکربندی شود که دامنه‌ها را اعتبارسنجی کند که امضا شده باشند. به ترتیب DNSSEC و اعتبارسنجی با استفاده از گزینه‌های dnssec-enable و dnssec-validation فعال می‌گردند.

نحوه پیاده‌سازی:

- دستور زیر را برای فعال‌سازی DNSSEC و اعتبارسنجی در فایل‌های پیکربندی BIND، اجرا کنید:

```
dnssec-enable yes
dnssec-validation yes
```

- سرور named را راه‌اندازی مجدد نمایید.

DNSR-7-3: غیرفعال کردن گزینه dnssec-accept-expired

شرح اجمالی:

گزینه dnssec-accept-expired به BIND اجازه می‌دهد که امضاهای منقضی شده را حین اعتبارسنجی، قبول نماید. این گزینه باید غیرفعال گردد تا امضاهای منقضی شده مورد پذیرش واقع نگردند.

نحوه پیاده‌سازی:

گزینه dnssec-accept-expired را تغییر دهید تا مقدار "no" داشته باشد، یا آن را از فایل پیکربندی حذف نمایید.

DNSR-8: عملیات-ثبت گزارش، پایش و نگهداری

DNSR-8-1: إعمال کردن به‌روزرسانی‌های قابل إعمال

شرح اجمالی:

در طول زمان، وصله‌ها برای حل کردن نواقص BIND منتشر می‌شوند. توصیه می‌شود که این وصله‌ها خیلی زود بعد اینکه در دسترس قرار می‌گیرند، بر حسب ریسک آن‌ها، اعمال گردند. آسیب‌پذیری‌هایی با ریسک بالا باید تا ۳۰ روز بعد از گزارش آسیب‌پذیری، وصله شود.

نحوه پیاده‌سازی:

به‌روزرسانی BIND به نسخه جدید موجود را انجام دهید. فرآیند وصله که به منظور إعمال به‌روزرسانی‌های امنیتی انجام می‌گردد را تا ۳۰ از انتشار آن، إعمال کنید. برا بدست آوردن به‌روزرسانی‌های در دسترس برای BIND به bindannounce@lists.isc.org روی وب سایت https://www.isc.org تماس برقرار کنید.

DNSR-8-2: پیکربندی یک کانال فایل ثبت گزارش

شرح اجمالی:

برای گرفتن لاگ‌ها داخل یک فایل محلی، در قسمت پیکربندی ثبت گزارش، یک کانال برای فایل راه‌اندازی کنید. معمولا داشتن یک فایل لاگ برای لاگ‌های مربوط به امنیت، و یک فایل لاگ دوم به همراه سطح شدت پویا که می‌تواند برای رفع‌اشکال استفاده شود، می‌تواند مفید باشد.

نحوه پیاده‌سازی:

داخل named.conf، یک کانال برای فایل لاگ امنیتی محلی با دسته‌بندی‌های config، dnssec، network، security، updates، xfer-in و xfer-out پیکربندی کنید. فایل محلی لاگ داخل دایرکتوری chroot قرار خواهد گرفت.

```
logging {
. . .
    channel local_security_log {
        file "/var/run/named/secure.log" versions 10 size 20m; severity debug;
        print-time yes;
```

```
    };
    // Config file processing
    category config { local_security_log; };
    // Processing signed responses
    category dnssec { local_security_log; };
    // Network Operations
    category network { local_security_log; };
    // Approved or unapproved requests category security { local_security_log; };
    // dynamic updates
    category update { local_security_log; };
    // transfers to the name server
    category xfer-in { local_security_log; };
    // transfers from the name server
    category xfer-out { local_security_log; };
    // Optional debug log file, may be enabled dynamically.
    channel local_debug_log {
            file "/var/run/named/debug.log";
            severity dynamic;
            print-time yes;
    };
   category default { local_debug_log; };
   category general { local_debug_log; };
};
```

DNSR-8-3: پیکربندی یک کانال Syslog ثبت گزارش

شرح اجمالی:

گزینه syslog مربوط به پیکربندی ثبت گزارش اجازه مشخص کردن امکان syslog برای ارسال لاگ رویدادها را فراهم می‌نماید. یک کانال syslog باید با مقدار daemon یا دیگر امکان مناسب syslog پیکربندی گردد. دسته‌بندی‌های default و general باید لحاظ شده باشد و سطح شدت باید در حد info یا پایین‌تر باشد.

نحوه پیاده‌سازی:

یک کانال syslog با حداقل امکان گرفتن لاگ رویدادهای دسته‌بندی‌های default و general پیکربندی کنید. برای سرورهای نام قابل‌اعتماد خارجی، دسته‌ی lame-servers ممکن است به null هدایت شود، بنابراین لاگ نمی‌گردد. استفاده از سرورهای نام lame معمولا برای دامنه‌های SPAM استفاده می‌گردد و ممکن است لاگ با اطلاعاتی که مفید نیستند سرریز کند. دستورات زیر را برای پیکربندی موارد ذکر شده اجرا کنید:

```
logging {
. . .
        // Syslog
        channel default_syslog {
                syslog daemon; # send to syslog's daemon facility
                severity info; # only send priority info and higher
         };
         category default { default_syslog; };
         category general { default_syslog; };
         // Too many lame servers, especially from SPAM
         category lame-servers { null; };
```

DNSR-8-4: غیرفعال کردن سرور HTTP Statistics

شرح اجمالی:

از نسخه BIND 9.5.0 یک وب سرور آمارها جدید درنظر گرفته شده است، که یک ابزار رفع‌اشکال مفید داخل یک محیط غیر-تولید می‌باشد. سرور HTTP داده در مورد شرایط سرور BIND 9 را در قالب XML تهیه می‌کند. سرور آمارها، آمارهای یکسانی تهیه می‌نماید که در statistics-file در دسترس می‌باشد. این سرور نباید غیرفعال گردد.

نحوه پیاده‌سازی:

گزینه statistics-channel را از فایل پیکربندی حذف کنید.

پیوست

در این بخش چک‌لیستی به منظور ممیزی محصول مورد نظر ارائه شده است. چک‌لیست شامل سه جدول است. جدول اول، جدول ممیز می‌باشد. در این جدول، اطلاعات مربوط به شخصی که پیکربندی امن را انجام می‌دهد یا آن را ممیزی می‌کند، وارد می‌شود. همچنین نتایج پیکربندی یا ممیزی به صورت اختصار در این جدول درج می‌گردد. جدول دوم، محل وارد کردن مشخصات سروری است که Bind Name Server روی آن نصب شده است. جدول سوم، جدول تنظیماتی است که باید بررسی یا اعمال شوند. در صورت صحت اعمال تنظیم در هر ردیف، ستون وضعیت مربوط به آن با علامت √ نمایش داده خواهد شد.

ممیز	
ممیز: نام: ---------- ایمیل: ---------- تلفن: ----------	**تاریخ:**

تنظیمات	**تعداد**	**توضیحات**
تطابق		
عدم تطابق		
تنظیمات حذف شده		
تنظیمات اضافه شده		
مجموع تنظیمات اعمال شده		

مشخصات سرور	
آدرس MAC	
آدرس IP	
نام ماشین	
شماره اموال	
مدیر سیستم	نام: ..... ایمیل: ..... تلفن: .....
تاریخ	

جدول ممیزی

جدول ممیزی خلاصه‌ای از تمامی الزامات بیان شده در متن سند می‌باشد. قابل ذکر است که ستون‌های "وضعیت" و "قابلیت پیاده‌سازی" باید توسط ممیز و برای هر سیستم حاوی این برنامه تکمیل گردد. در ستون وضعیت، ممیز باید از عبارت‌های "قبول" و "رد" متناسب با وضعیت الزام در محصول مورد ارزیابی استفاده نماید. در ستون قابلیت پیاده‌سازی، ممیز باید قابلیت پیاده‌سازی الزام برای محصول مورد ارزیابی را با عبارات "دارد" و "ندارد" بیان نماید. در صورتی که الزامی برای محصول مذکور قابلیت پیاده‌سازی نداشته باشد، علت عدم قابلیت پیاده‌سازی آن باید در ذیل جدول توضیح داده شود.

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی تنظیمات	مقدار پیش‌فرض	مقدار مطلوب
DNSR-1		طراحی و معماری			
DNSR-1-1		استفاده از یک معماری Split-Horizon			
DNSR-1-2		عدم نصب یک سیستم Multi-Use			
DNSR-1-3		نقش اختصاصی Name Server			
DNSR-1-4		استفاده از DNS سرورهای حافظه‌ای upstream امن			
DNSR-1-5		نصب کردن ISC BIND 9			
DNSR-2		محدودسازی مجوزها و مالکیت			
DNSR-2-1		اجرای BINDبه عنوان کاربر غیر ریشه			
DNSR-2-2		اختصاص یک shell غیرمعتبر به حساب کاربر BIND			
DNSR-2-3		قفل کردن حساب کاربر BIND			
DNSR-2-4		تنظیم مالک فولدرهای BIND به کاربر root			
DNSR-2-5		تنظیم مالک فایل‌های پیکربندی BIND به کاربر root			
DNSR-2-6		تنظیم گروه named یا ریشه برای فولدرها و فایل‌های			

		پیکربندی BIND			
DNSR-2-7		تنظیم گروه و دیگر مجوزهای دایرکتوری‌های غیر زمان‌اجرای BIND به فقط-خواندی			
DNSR-2-8		تنظیم گروه و دیگر مجوزهای همه فایل‌های BIND به فقط-خواندی			
DNSR-2-9		ایزوله کردن BIND با زیردایرکتوری chroot’ed			
DNSR-3		محدودسازی پرس‌وجوها			
DNSR-3-1		نادیده گرفتن پرس‌وجوهای ناخواسته و اشتباه			
DNSR-3-2		محدود کردن پرس‌وجوهای بازگشتی			
DNSR-3-3		محدود کردن خاستگاه‌های پرس‌وجو			
DNSR-3-4		محدود کردن پرس‌وجوهای حافظه نهان			
DNSR-4		امضاهای تراکنش--TSIG			
DNSR-4-1		استفاده از کلیدهای TSIG با طول ۲۵۶ بیت			
DNSR-4-2		وارد کردن فایل‌های کلید رمزنگاری			
DNSR-4-3		استفاده از کلیدهای منحصربه‌فرد برای هر جفت هاست			
DNSR-4-4		محدود کردن دسترسی به همه فایل‌های کلید			
DNSR-4-5		حفاظت از فایل‌های کلید TSIG حین توسعه			
DNSR-5		احرازهویت به‌روزرسانی‌ها و انتقالات ناحیه			
DNSR-5-1		احرازهویت انتقالات ناحیه به صورت امن			
DNSR-5-2		احرازهویت به‌روزرسانی‌های			

		پویا به‌صورت امن			
DNSR-5-3		احرازهویت ارسال به‌روزرسانی به‌صورت امن			
DNSR-6		نشر اطلاعات			
DNSR-6-1		پنهان کردن عبارت نسخه BIND			
DNSR-6-2		پنهان کردن ID سرور نام			
DNSR-7		امن کردن مکاتبات شبکه			
DNSR-7-1		عدم تعریف یک سورس پورت ثابت			
DNSR-7-2		فعال کردن اعتبار سنجی DNSSEC			
DNSR-7-3		غیرفعال کردن گزینه dnssec-accept-expired			
DNSR-8		عملیات- ثبت گزارش، پایش و نگهداری			
DNSR-8-1		إعمال کردن به‌روزرسانی‌های قابل إعمال			
DNSR-8-2		فعال کردن اعتبار سنجی DNSSEC			
DNSR-8-3		پیکربندی یک کانال Syslog ثبت گزارش			
DNSR-8-4		غیرفعال کردن سرور HTTP Statistics			