## أمن نظام أسماء النطاقات ومستخدميه (DNS Security)

سأتحدث في هذه الورقة عن أمن نظام أسماء النطاقات(Domain Name System DNS) وخادمات هذا النظام والمخاطر الأمنية التي قد تواجه هذا النظام ومستخدميه وكيفية التغلب عليها مع ذكر بعض الأمثلة باستخدام برنامج البايند (Bind) الذي يعد من أشهر برامج هذا النظام وأكثرها انتشارا (وهو يعمل على بيئة اليونكس و الوندوز).

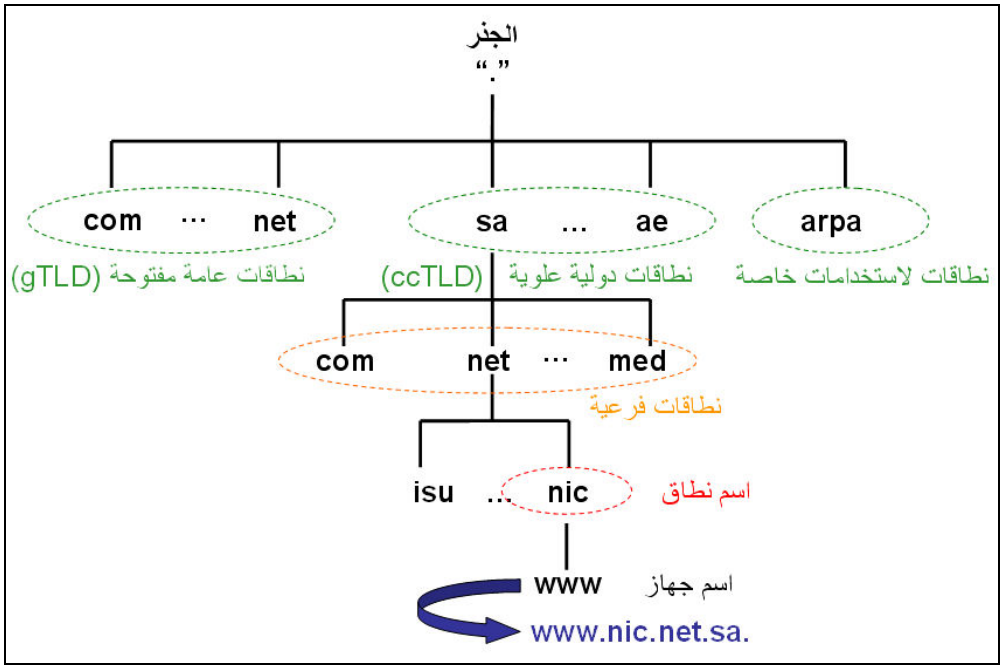
إن نظام أسماء النطاقات يعد من أهم الأنظمة الموجودة على الانترنت والشبكات وأكثرها حساسية فبدونه لا يمكن الوصول إلى الأجهزة أو المواقع باستخدام أسمائها، و إذا تعرض هذا النظام للتعطيل أو التخريب من قبل المهاجمين فان ذلك سيؤدي لحدوث أضرار كبيرة وخطيرة لمستخدمي الانترنت والشبكات، مثل توجيه المستخدمين لمواقع وهمية ومن ثم سرقة معلوماتهم الشخصية(اسم المستخدم وكلمة المرور ، أرقام البطاقات الائتمانية)، وقد يؤدي أيضا لتعطيل المواقع و الخدمات المتوفرة على الانترنت والشبكات أو حتى تعطيل شبكة الانترنت كاملة (فلا يمكن الوصول للمواقع باستخدام أسماء النطاقات).

### ما هو نظام أسماء النطاقات (DNS)؟

إن طريقة التخاطب بين الأجهزة على الانترنت تعتمد بشكل أساسي على العنوان الرقمي لبرتوكول الإنترنت (IP address) وهذا العنوان الرقمي مكون من 32 خانة ثنائية يمكن تمثيلها بالشكل التالي (192.168.1.2). فيتحتم على أي جهاز على شبكة الانترنت معرفة العنوان الرقمي للطرف الأخر حتى يمكن تبادل المعلومات معه، ولكن مستخدمي الإنترنت غير قادرين على التعامل مع هذه الأرقام مباشرة لصعوبة حفظها. لذلك تم بناء نظام أسماء النطاقات (الذي يقوم باستخدام الأسماء عند التخاطب ومن ثم تحويلها إلى ما يقابلها من أرقام) للتغلب على هذه المشكلة ولإضافة مزايا عديدة تخدم الانترنت ومستخدميها.

ويمكن تعريف نظام أسماء النطاقات بأنه قاعدة معلومات غير مركزية (موزعة) على شبكة الإنترنت تحتوي على معلومات النطاقات و أسماء الأجهزة وعناوينها الرقمية تحت كل نطاق. وهذا النظام يقوم بتجزئه معلومات الشبكة إلى أجزاء يتم إدارتها محليا والوصول إليها عن طريق الشبكة , ويتم زيادة الاعتمادية و تحسين سرعة الرد باستخدام التعددية (replication) و الحفظ المؤقت (caching).

وهذا النظام له جذر رئيسي تندرج تحته نطاقات علوية (نطاقات مفتوحة ونطاقات دولية ونطاقات ذات استخدامات خاصة) وتحت كل نطاق علوي يوجد نطاقات فرعية أخرى، الصورة التالية توضح التفرع للنطاقات:



و نظام أسماء النطاقات يستخدم نموذج الخادم و العميل (client server model) حيث يحتفظ الخادم (المسمى خادم أسماء النطاقات Domain Name server) بجزء بسيط من قاعدة المعلومات على ملف النطاق (zone file) و يوفرها للعميل ( المسمى المقرر أو المترجم Resolver). فالخادم يستمع إلى استفسارات المقررين على المنفذ رقم (53 UDP) ويقوم بتلقي طلبات تبادل ملفات النطاقات ( zone transfer) مع الخادمات الأخرى على المنفذ رقم (53 TCP). كما يجدر التنبيه إلى أن طبيعة تبادل الرسائل (الاستفسارات و الردود) يتم بشكل مبسط ومن دون أي تشفير خلال النظام، مما يتيح لأي شخص على الشبكة معرفة الاستفسارات والرسائل المتبادلة المتعلقة بالنظام ، ولقد تم وضع حلول معينة تحد من خطورة هذا الأمر.

**مكونات النظام وطريقة عملة:**

قبل التحدث عن المخاطر الأمنية التي قد تواجه النظام يتحتم علينا أولا التعرف على مكوناته مع ذكر نبذة بسيطة عن عناصر هذا النظام، فهذا النظام يتكون من العناصر التالية:

- **اسم النطاق(Domain Name):** هو اسم يستخدم على الانترنت والشبكات لتمثيل جهة معينة الكترونيا، وتستخدمه الجهة للدلالة على اسمها(domain.com.sa) أو أقسامها أو فروعها (ruh.domain.com.sa) أو للدلالة على خدماتها أو أسماء أجهزتها ( www.domain.com.sa srv1.domain.com.sa) أو حتى عناوين البريد الالكترونية (user@domain.com.sa). ويمكن تسجيل ذلك الاسم عن طريق المركز المسئول عن النطاق العلوي التابع له (مثلا: لتسجيل أي نطاق تحت sa يمكن الاتصال بالمركز السعودي لمعلومات الشبكة www.nic.net.sa).

- **سجل المصدر (Resource Record):** وهو سجل تعريفي يحدد معلومة معينة داخل النظام وله أنواع عديدة:
  - **سجل تعريف العنوان ("A": Address):** ويستخدم لربط الأسماء بالعناوين الرقمية المقابلة لها، ويمكن تمثيل ذلك في ملف النطاق على الشكل التالي:

```
A 192.168.1.2 www.domain.com.sa.
```

  - **سجل تعريف خادم البريد ("MX": Mail eXchange):** ويستخدم لتعريف خادم البريد الالكتروني لاسم النطاق الأسماء بالعناوين الرقمية المقابلة لها ، ويمكن تمثيل ذلك في ملف النطاق على الشكل التالي:

```
domain.com.sa. MX 10 mail.domain.com.sa.
```

  - **سجل تعريف خادم اسم النطاق ("NS": Name Server):** ويستخدم لتعريف خادم اسم النطاق المسئول عن النطاق، ويمكن تمثيل ذلك في ملف النطاق على الشكل التالي:

```
domain.com.sa. NS  ns1.domain.com.sa.
```

  - **سجل تعريف المترادفات ("CNAME": Canonical Name):** ويستخدم لتعريف مترادفات للأسماء, ويمكن تمثيل ذلك في ملف النطاق على الشكل التالي:

```
www.domain.com.sa. CNAME  ns1.domain.com.sa.
```

  - **سجل تعريف معلومات النطاق ("SOA": Start Of Authority):** ويستخدم لتعريف بعض المعلومات الأساسي حول النطاق (مثل من هو خادم الأسماء الرئيسي، عنوان البريد الكتروني للمسئول الفني، ... الخ) وله صيغة معينة وبعض الأرقام الأخرى الهامة المستخدمة بين الخادمات الرئيسية والثانوية التي تخدم اسم النطاق، وتمثل كالتالي:

```
domain.com.sa. SOA ns1domain.com.sa. hostmaster.domain.com.sa.1558
7200 3600 604800 86400
```

  - **سجل التعريف العكسي للرقم ("PTR": Pointer):** ويستخدم لتعريف اسم النطاق المقابل لرقم برتوكول الانترنت فهو معاكس من حيث الوظيفة لسجل تعريف العنوان، ويستخدم عادة للتأكد من صحة سجل تعريف، ويمكن تمثيل ذلك في ملف النطاق العكسي على الشكل التالي:

```
2.1.168.192.in-addr.arpa. PTR  www.domain.com.sa.
```

- **وغيرها من السجلات الأخرى:** التي لها استخدامات خاصة وهي أقل استخداما وانتشارا من السجلات السابقة (مثل:...TXT,AAAA,SRV,SIG,RP,LOC).

- **ملف النطاق (Zone File):** وهو الملف الذي يحوي جميع سجلات المصادر(المعلومات) المتعلقة باسم نطاق معين, ويتم حفظ و إدارة ملف النطاق من خلال خادم أسماء النطاقات.

- **خادم أسماء النطاقات (Domain Name Server):** وهو الخادم الذي يقوم بالرد على استفسارات المستخدمين أو المقررين بناء على ما هو موجود في ملف اسم النطاق المستفسر عنه. ويوجد خادم رئيسي على الأقل لكل اسم نطاق، ويتم من خلاله إدارة جميع سجلات النطاق و إجراء التحديثات عليها ويعد هذا الخادم المالك الرئيسي للنسخة الأصلية لملف اسم النطاق، كما توجد أيضا خادمات فرعية عديدة تأخذ نسخة من ذلك الملف بالتنسيق مع الخادم الرئيسي.

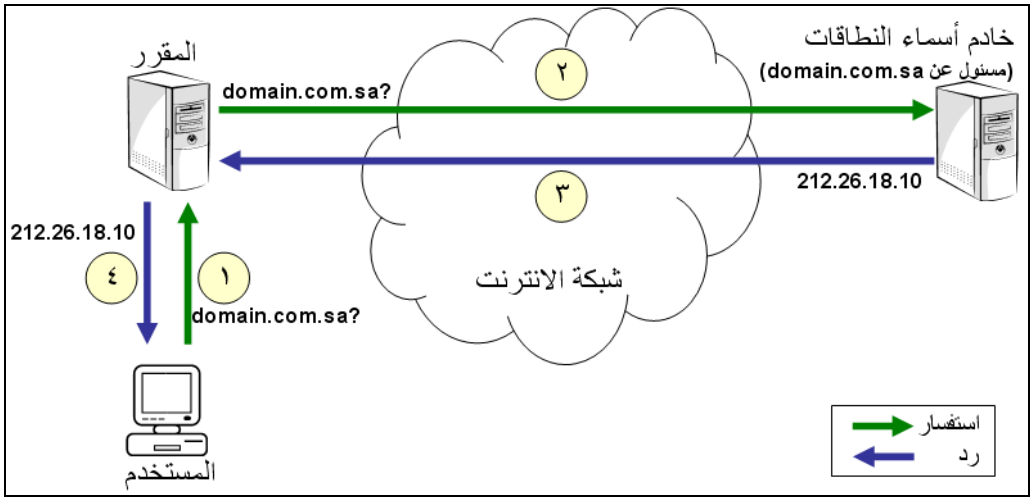
- **المقرر (Resolver):** وهو الجهاز الذي يقوم (نيابة عن المستخدمين) بإرسال الاستفسارات حول أي معلومة موجودة في النظام إلى خادمات أسماء النطاقات ومن ثم إرسال النتيجة النهائية إلى المستفسرين ( المستخدمين أو الأجهزة)، وعادة ما يوضع على كل شبكة منفصلة (خاصة) جهاز مقرر حتى يقوم بترجمة الأسماء إلى العناوين لجميع المستخدمين والأجهزة الموجودة على تلك الشبكة من خلال نظام أسماء النطاقات، كما يقوم المقرر أيضا بتخزين جميع نتائج الاستفسارات السابقة في السجلات المؤقتة (DNS Caching) وذلك لتوفير الجهد و لتحسين الأداء بدلا من البحث عن نتيجة نفس الاستفسار مرة أخرى خلال مدة معينة (تحدد من قبل الخادم الرئيسي لاسم النطاق).

- **المستخدم (user):** وهو المستفيد النهائي من النظام (شخص أو برنامج أو جهاز) بحيث يتعامل مع النظام من خلال المقرر للحصول على المعلومة المطلوبة، كما يمكن أن يكون هذا المستخدم هو الشخص الذي يقوم بتسجيل اسم النطاق للاستفادة منه لاحقا.

**وطريقة عمل النظام يمكن تمثيلها بكل بساطة من خلال المثال التالي:**

1. المستخدم يطلب من أقرب خادم مقرر (Resolver) العنوان الرقمي لاسم النطاق (domain.com.sa)، وعادة ما يكون المقرر معرف في إعدادات الشبكة على جهاز المستخدم.
2. المقرر يقوم بالبحث عن الخادم الرئيسي لاسم النطاق المطلوب وذلك من خلال سؤال الخادمات الرئيسية العامة (Root Server) و من ثم الخادمات المسئولة عن النطاق العلوي الذي يتبع له النطاق إلى أن يصل إلى أحد الخادمات المسئولة عن ذلك النطاق ويرسل الاستفسار إليها.
3. خادم أسماء النطاقات المسئول عن النطاق يقوم بالبحث في ملف النطاق المتوفر لديه عن المعلومة المطلوبة ومن ثم يرد على ذلك الاستفسار بالعنوان الرقمي لذلك النطاق.
4. المقرر يقوم بالرد على استفسار المستخدم بالنتيجة التي حصل عليها ويقوم بتخزينها في السجلات المؤقتة لديه (حتى يستخدم عند طلب نفس الاستفسار من قبل مستخدم آخر خلال مدة معينة).

والصورة التالية توضح طريقة عمل النظام حسب الخطوات السابقة:

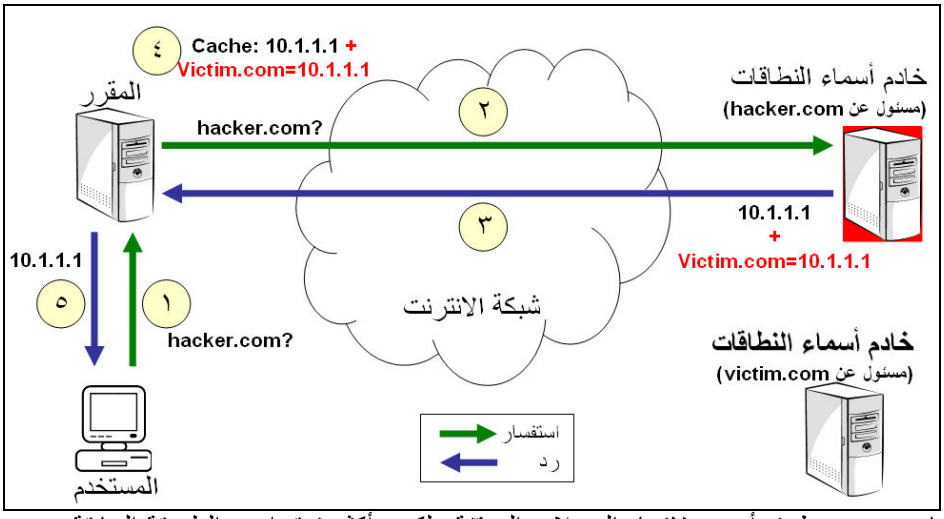



**مخاطر تهدد النظام:**

الآن وبعد التحدث عن نظام أسماء النطاقات ومكونات هذا النظام يمكننا التطرق إلى بعض المخاطر الأمنية التي تهدد هذا النظام الهام، ويمكن تلخيصها في عدد من المخاطر منها:

- **إفساد السجلات المؤقتة (Cache Poisoning):** وهذا الخطر عادة ما يواجه المقررين (المترجمين)، بحيث يتم استغلال فكرة حفظ السجلات المؤقتة التي تساعد على تحسين الأداء وتوفير الجهد إلى إفساد ما تم تخزينه فيه بحيث يتم استبدال المعلومة الصحيحة بمعلومة خاطئة لتوجيه الأجهزة و المستخدمين إلى عناوين خاطئة بدلا من الحقيقية ويمكن تبسيطها من خلال المثال التالي:.

1. المستخدم يقوم بطلب استفسار من المقرر (المترجم) المعرف لديه على الشبكة عن نطاق معين (hacker.com).
2. المقرر يبحث من خلال نظام أسماء النطاقات عن خادمات الأسماء المسئولة عن النطاق (hacker.com) ويرسل الاستفسار إليها (في حالة عدم توفره في السجلات المؤقتة).
3. خادمات اسم النطاق تقوم بإعطاء المقرر معلومات عن اسم النطاق المستفسر عنة (hacker.com) وتضيف معها معلومات أخرى غير حقيقية (مثلا: تخبر أنها مسئولة عن اسم نطاق آخر victim.com).
4. المقرر يقوم بتخزين الرد على شكل سجلات مؤقتة بجميع النتائج التي حصل عليها الخاصة بالنطاق (hacker.com) وأيضا النطاق (victim.com).
5. يقوم المقرر بعد ذلك بإعطاء نتيجة الاستفسار إلى المستخدم.
6. أي مستخدم يسأل المقرر بعد ذلك عن (victim.com) سيتم إعطاءه النتيجة من السجلات المؤقتة لأنها متوفرة ولا يحتاج لإعادة السؤال مرة أخرى(لأن المهاجم سبق وأعطي النتيجة على شكل رد إضافي) وهنا يكمن الخطر.

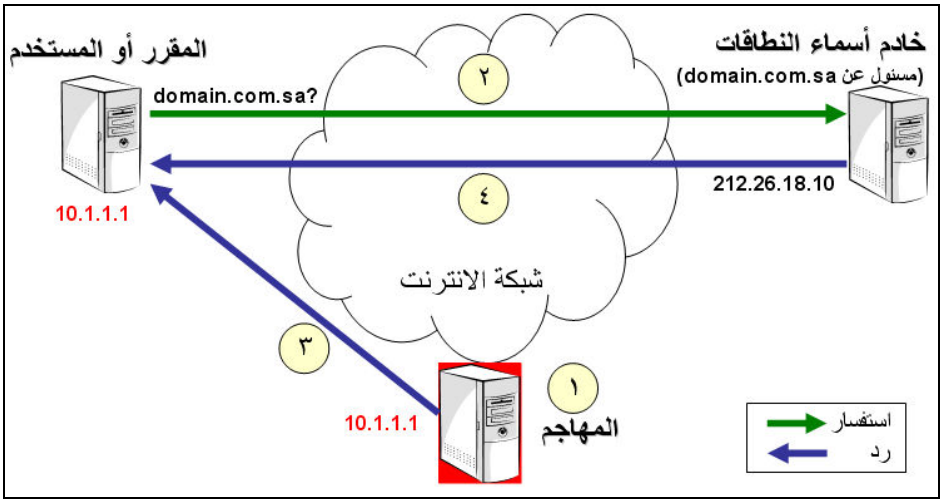



كما يوجد عدة طرق أخرى لإفساد السجلات المؤقتة ولكنهم أكثر تعقيدا من الطريقة السابقة وجميعها تعطي نفس النتيجة (تضليل المستخدمين وخداعهم).

- **هجمات تعطيل الخدمة (Denial of Service):** خادمات أسماء النطاقات معرضة (كباقي الخادمات والأجهزة على الانترنت) لهجمات تعطيل الخدمة، بحيث يقوم المهاجم بإرسال رسائل تحوي كميات كبيرة من البيانات أو رسائل كثيرة جدا بأحجام صغيرة إلى خادم أسماء النطاقات ليستنفذ مصادر الجهاز مما يؤدي إلى تعطيله عن العمل. وقد يقوم المهاجم بتغيير عنوان مصدر الرسائل إلى عنوان غير حقيقي وقد يرسل رسائل على شكل ردود لطلبات لم تطلب (Spoofed, SYN packets) كما يمكن أن يقوم أيضا بعمل هجمات موزعة لتعطيل الخدمة (Distributed DoS) وقد يصل بعضها إلى أكثر من مليون رسالة في الثانية الواحدة (وخصوصا بعد انتشار الأدوات والطرق التي تساعد على ذلك). كما تسمى أيضا هذه الهجمات بهجمات إغراق العميل (Client Flooding).

- **تخريب الذاكرة (Buffer overflow):** خادمات أسماء النطاقات تتعامل مع الآخرين من خلال استقبال الاستفسارات والرد عليها, وقد يستغل المهاجم هذه النقطة بحيث يستغل هذا التفاعل مع الخادم بحيث يرسل بيانات بشكل معين (على شكل استفسارات) تجعل البرنامج يقوم بتخطي المساحة المخصصة له بالذاكرة والوصول إلى مساحة أخرى قد تسبب مشاكل حرجة للخادم أثناء تنفيذه لبرنامج آخر يستخدم تلك المساحة التي تم التعديل عليها.

- **هجمة "الرجل الوسيط" (Man in the middle attack):** إذا تمكن المهاجم من إقحام نفسه بين المستخدم و خادم أسماء النطاقات( أو المقرر) فان ذلك يمكنه من إرسال رسائل رد غير صحيحة لاستفسارات المستخدمين. ويمكن أن يحصل ذلك من خلال عدة طرق وعدة أساليب، ولكن الأسلوب الأسهل والأكثر انتشارا يمكن سياقه من خلال الخطوات التالية:
  1. أن يقوم المهاجم بوضع نفسه بين المستخدم/المقرر وخادم أسماء النطاقات ثم التصنت على الشبكة.
  2. المستخدم/المقرر يرسل استفسار معين لخادم أسماء النطاقات وينتظر الرد.
  3. يقوم المهاجم وبسرعة بإرسال رسالة رد وهمية بمعلومات غير صحيحة للمستخدم قبل أن يقوم بذلك خادم أسماء النطاقات.
  4. خادم أسماء النطاقات يرسل رد صحيح إلى المستخدم ولكن للأسف بعد فوات الأوان (سبقه المهاجم بذلك).




- **استغلال خدمة خادمات أسماء النطاقات المشتركة ( DNS Vulnerabilities in Shared Host Environments):** مع انتشار الانترنت وانتشار المواقع ظهرت خدمات جديدة مثل المشاركة في استضافة المواقع (Shared Hosting) بحيث يتم استضافة أكثر من موقع على جهاز واحد للمشاركة في المصادر وتقليل سعر الاستضافة، والتي نتج عنها استخدام خادمات أسماء نطاقات مشتركة (Shared DNS servers) –وغالبا ما تكون على نفس الجهاز- وهي تعمل كخادمات أسماء النطاقات و مقررات في نفس الوقت. وتقوم هذه الخادمات بتوفير خدمات عديدة لأصحاب المواقع مثل خدمة إضافة نطاق رئيسي (Main Domain)، وخدمة إضافة نطاق فرعي (Sub-Domain)، وخدمة تسكين نطاق فوق النطاق الرئيسي (DNS Parking) بحث يصبح كلا النطاقين يصبان في موقع واحد، وخدمة توجيه نطاق إلى نطاق آخر (DNS forwarding) وجميعها خدمات جيدة ومطلوبة. ولكن مع كل أسف قد تستغل هذه الخدمات من قبل المهاجمين وذلك باستغلال خدمة التوجيه مثلا وتوجيه المواقع الهامة إلى مواقع وهمية بحيث يؤثر على جميع الاستفسارات والمراسلات الواردة إلى ذلك الخادم.

- **استغلال ثغرات في نظام التشغيل أو برنامج خادم أسماء النطاقات (Security Holes/Bugs):** كما يمكن للمهاجم أن يقوم باستغلال الثغرات الأمنية التي يتم الإعلان عنها من قبل الجهات المختصة عن نظام التشغيل أو برنامج خادم أسماء النطاقات، فيقوم المهاجم بالبحث عن الأجهزة التي لم تطبق التحديثات الخاصة بتلك الثغرات ويهاجم الجهاز من خلالها ويستولي علية.

- **سرقة/اختطاف اسم النطاق (Domain Hijacking):** كما هو معلوم فان اسم النطاق اسم ثمين جدا لأنه يمثل الجهة على الانترنت، ويمكن تسجيله مباشرة من خلال المركز المسئول عن إدارة النطاق العلوي المندرج تحته (سواء كان مفتوح أو دولي)، كما يمكن تسجيل اسم النطاق من خلال جهات أخرى تقدم خدمات تسجيل النطاقات(مسجلين Registrar) وعادة ما تكون هذه الجهات مرخصة للقيام بتلك المهمة من قبل المراكز المسئولة عن النطاقات العلوية (فمثلا هذه قائمة بالمسجلين المسئولين عن النطاقات العامة المفتوحة http://www.internic.net/regist.html). وعند تسجيل النطاق يطلب تحديد المنسق الإداري المسئول عن النطاق ويكون لديه كامل الصلاحيات على النطاق بحيث يستطيع تغيير معلومات النطاق ونقلة من جهة إلى جهة أخرى (وعادة ما يحصل الشخص الذي يخاطب جهة التسجيل على هذه الصلاحيات). وتختلف الخدمات المقدمة من قبل مراكز التسجيل و المسجلين المعتمدين لأصحاب النطاقات، فمنهم من يوفر كامل الخدمات الالكترونية لإدارة معلومات النطاق من خلال لوحة تحكم يتم الدخول عليها باستخدام اسم مستخدم وكلمة مرور، وآخر يقدم خدمات بسيطة جدا بحيث تكون جميع المعاملات ورقية فلا يتم التسجيل أو التعديل إلا بإرسال خطابات معتمدة ومصدقة لكل عملية، ومنهم من وازن بين الطريقتين السابقتين (فيقدم خدمات الكترونية بسيطة وأخرى يدوية

للتحقق من صحة الطلبات)، وتحديد الطريقة المتبعة في التسجيل يعتمد على السياسة المطبقة للمركز المسئول عن النطاق العلوي المراد التسجيل تحته أو الجهة المسجلة. وقد تتعرض الجهة إلى خطر سرقة اسم النطاق الخاص بها ومن ثم للابتزاز أو التهديد، وعادة ما يحدث ذلك بسبب أمور عديدة منها:

- استخدام كلمة سر سهلة يمكن تخمينها أو كسرها ومن ثم الوصول إلى لوحة التحكم الخاصة بإدارة اسم النطاق.
- سرقة البريد الالكتروني للمنسق الإداري للنطاق أو الشخص صاحب صلاحية التعديل ومن ثم مراسلة مركز التسجيل أو الجهة المسجلة لنقلة أو تغيير كلمة السر للوحة التحكم الخاصة بالنطاق.
- الوثوق في أشخاص ليسو أهلا للثقة فيقومون بتغيير كلمة السر أو تعديل معلومات النطاق بدافع الانتقام أو الابتزاز (وعادة ما تكون في الموظفين الذين طردوا من أعمالهم).
- الاعتقاد بأن النطاق مسجل للجهة لوجود موقع يعمل على اسم النطاق، ولكن اسم النطاق لم يسجل أصلا لتلك الجهة.
- قيام بعض شركات الاستضافة بتغيير المنسق الإداري المسئول عن النطاق، عند رغبة صاحب النطاق بنقل الاستضافة إلى جهة أخرى أو عند وجود أي مشكلة أو خلاف مع صاحب النطاق.
- عدم تجديد تسجيل اسم النطاق ومن ثم استحواذ جهة أخرى علية ومن ثم الضغط على صاحب النطاق.
- فقدان معلومات تسجيل النطاق وذلك بسب عدم توثيقها أو حفظها، وعادة ما يحدث ذلك عدما يكون تسجيل اسم النطاق هو بسبب اجتهاد شخصي يفقد بفقد ذلك الشخص.

- **خداع وتضليل المستخدمين باستخدام أسماء نطاقات مشابهة للأصلية (Domain Fishing):** كما يمكن للمهاجم أن يقوم باستغلال تشابه أسماء النطاقات لتضليل المستخدمين وخداعهم (يمكن أن نطلق عليها الاصطياد في الماء العكر)، بحيث يقوم المهاجم بتسجيل أسماء نطاقات وهمية تشبه نطاقات مشهورة وحساسة (وذلك باستبدال حرف برقم مشابه له أو بتغيير ترتيب حروف النطاق الأصلي)، ومن ثم استخدام البريد الالكتروني لجذب الزوار وإرسالهم إلى مواقع تلك النطاقات الوهمية (التي تشبه الموقع الأصلي من حيث التصميم)، ومن ثم أخذ معلوماتهم الزوار الشخصية أو معلومات بطاقاتهم الائتمانية أو ليقوم المهاجم بتشويه سمعة صاحب الوقع الأصلي. ومثال على ذلك بأن يقوم المهاجم بتسجيل النطاق التالي (paypa**1**.com) الذي يشبه إلى حد كبير الموقع (paypa**l**.com) لاحظ استبدال الحرف "L" بالرقم واحد "1"، أو أن يقوم بتسجيل النطاق (micros**0**ft.com) أو(micros**a**ft.com) دلالة عن موقع (micros**o**ft.com) لاحظ استبدال الحرف "O" بالرقم "0" أو الحرف "a" كخطأ إملائي شائع لمستخدمي الانترنت.

- **وجود بعض الأخطاء التقنية الشائعة في إعداد ملفات أسماء النطاقات ( Common errors in the Zone files):** كما سبق وأن بينا فان ملف اسم النطاق يحتوي على المعلومات والسجلات اللازمة لعمل النطاق والخدمات القائمة عليه بشكل صحيح، وعند وجود أي خطأ داخل ذلك الملف أو أحد سجلاته فان ذلك سيؤثر سلبيا على أداء اسم النطاق و/أو الخدمات القائمة عليه. فقد تسبب بعض الأخطاء إلى تعثر الوصول إلي مواقع أو خدمات نطاق معين أو حتى إلى توجيه المستخدمين إلى خادمات أخرى غير صحيحة. ولتوفير الأمن اللازم لمستخدمي نظام أسماء النطاقات فان بعض المراكز المسئولة عن النطاقات العلوية تقوم بالتحقق من صحة استضافة اسم النطاق على الخادمات المسئولة عنه قبل تسجيل اسم النطاق(مثل المركز السعودي لمعلومات الشبكة).

- **إفساد أو تغيير إعدادات نظام أسماء النطاقات أو ملفات الترجمة الداخلية للأجهزة:** قد يقوم المهاجم بتغيير إعدادات نظام أسماء النطاقات (في القسم الخاص بإعدادات الشبكة) داخل الأجهزة وذلك إما بالوصول المباشر للجهاز أو عن طريق برامج أو فيروسات معينة تقوم بتغيير الإعدادات الافتراضية للنظام، مما يؤدي إلى تعطيل أو تخريب نظام أسماء النطاقات على ذلك الجهاز. كما يمكن أيضا أن

يستخدم المهاجم نفس الطرق السابقة لتغيير ملفات الترجمة الداخلية التي يستخدمها الجهاز قبل استخدام نظام أسماء النطاقات، مثل تغيير معلومات ملف "hosts" المتوفر على معظم أنظمة التشغيل. وهو ملف بسيط يحتوي على أسماء الأجهزة وعناوينها الرقمية (IP Address) التي يقوم الجهاز باستخدامها قبل سؤال نظام أسماء النطاقات، ويمكن الوصول إلي الملف في نظام اليونكس أو اللينكس من خلال "/etc/hosts"، بينما في نظام تشغيل الوندوز يكون عادة موجود في "c:\windows\system32\drivers\etc\hosts". ويستطيع المهاجم تعطيل مواقع معينة أو إرسال المستخدم لمواقع وهمية وذلك عند قيامه بإضافة اسم جهاز مشهور في ذلك الملف وربطه بعنوان رقمي وهمي وهنا يكمن الخطر.

**طرق حماية النظام (خادمات أسماء النطاقات + المقررين):**

هناك عدة طرق ونقاط يمكن تطبيقها على خادمات أسماء النطاقات و خادمات المقررات لتفادي الأخطار التي يمكن أن تتعرض لها ومنها:

- **حماية الاتصال الشبكي لخادمات أسماء النطاقات(Network Security):** ويمكن تطبيق الحماية باستخدام جدار ناري أو موجة ووضع شروط وآلية معينة لفلترة رسائل الشبكة بحيث لا يتم فتح إلا المنافذ التي يحتاجها الخادم لتأدية عمله، فبالنسبة لنظام أسماء النطاقات يجب فتح المنفذ رقم 53 للبروتوكول (UDP) للسماح بتلقي الاستفسارات من أي جهة حول معلومة معينة، كما يجب فتح المنفذ رقم 53 للبروتوكول (TCP) و (UDP) للسماح فقط للخادمات الثانوية التي تحتاج نقل ملف النطاق كاملا إليها. كما يمكن استخدام جهاز التعرف على التطفل (Intrusion Detection) لتوفير الحماية اللازمة للخادمات والتعرف على الهجمات أو الاختراقات عند حدوثها.

- **حماية نظام التشغيل (OS Security):** كما يجب حماية نظام التشغيل وذلك بعمل التحديثات اللازمة بشكل دوري، والتأكد من صحة ودقة إعدادات نظام التشغيل وإزالة جميع الخدمات والبرامج الغير مستخدمة أو التي لا توجد حاجة لوجودها.

- **تحديث برنامج الخادم باستمرار (Update DNS server):** كما يجب تحديث البرنامج الذي يعمل كخادم لأسماء النطاقات بشكل مستمر ودوري، والذي يساعد على ذلك الاشتراك في القوائم البريدية الخاصة بالبرنامج نفسه و القوائم البريدية الأخرى المختصة في أمن الشبكات والمعلومات بشكل عام.

- **التنوع في خادمات أسماء النطاقات (Diversity):** من أهم التوصيات المقترحة عند إعداد خادمات أسماء النطاقات هو تجهيز خادمين (على الأقل) لتوفير خدمة استضافة أسماء النطاقات (أحدهما رئيسي والآخر ثانوي)، كما يوصى بأن تكون هذه الخادمات على شبكات منفصلة وذلك لتفادي مشاكل تعطل جميع الخادمات بسبب تعطل الشبكة. كما يفضل أن تكون هذه الخادمات تعمل على أنظمة تشغيل مختلفة ( مثلا: لينكس Linux و سن سولارس Sun Solaris)، ليس فقط ذلك بل ينصح أيضا باستخدام برامج مختلفة تعمل كخادمات أسماء النطاقات (مثلا: بايند Bind و مارا دي ان اس MaraDNS) والسبب الرئيسي في هذا التنوع هو عدم توقف عمل جميع الخادمات أو سهولة اختراقها جميعا عند وجود ثغرة معينة في نظام التشغيل أو البرنامج الذي يقوم بدور خادم أسماء النطاقات عند اعتماد نوع معين على جميع الخادمات (ويمكننا القول بأن هذا التنوع قائم على مبدأ عدم وضع البيض في سلة واحدة).

- **إخفاء الخادم الرئيسي لأسماء النطاقات (Hiding the Primary Name server):** كما هو معلوم فانه يوجد على الأقل خادم رئيسي معلن لكل نطاق ولكن في الحقيقة يفضل وضع خادم آخر رئيسي مخفي (يمكن وضعة في شبكة داخلية آمنة) بحيث لا يعلم عنه أحد ولا يخاطبه إلا الخادم الرئيسي المعلن (الذي يأخذ منه ملفات النطاقات المستضافة) ثم يقوم بعد ذلك بتوزيعها على الخادمات الثانوية، والهدف من ذلك التأكد من الاحتفاظ بنسخة صحيحة من ملفات النطاقات المستضافة في مكان آمن بعيدا عن أيدي العابثين.

- **تخصيص جهاز مستقل يعمل كخادم لأسماء النطاقات ( Dedicated Machine for DNS servers):** والهدف من ذلك تقليل الخدمات الموجودة على الجهاز والاكتفاء بخدمة أسماء النطاقات وسيؤدي ذلك إلى التقليل من احتمالية اختراق الجهاز عن طريق الخدمات الأخرى، والتركيز فقط على متابعة أمن نظام التشغيل و برنامج خادم أسماء النطاقات.

- **عزل أنواع خادمات أسماء النطاقات عن بعضها البعض (Split-Function Name Servers):** كما يفضل وبشدة فصل خادمات أسماء النطاقات عن المقررات وذلك لتفادي مشاكل إفساد السجلات المؤقتة وأيضا يبسط ويسهل إعدادات الخادمات والتحكم فيها كما يزيد الأمن على هذه الخادمات. فمثلا خادمات أسماء النطاقات الرئيسية والثانوية يفضل عدم تفعيل خدمة التقرير عليها (Resolving) ويمكن ذلك بإضافة المتغير التالي في ملف إعدادات الخادم:

**In Bind Configuration File (named.conf) for DNS Name servers:**

```
options {
   recursion no; };
```

- **مراجعة ملف إعدادات الخادم باستمرار وتتبع التوصيات المقترحة علية ( review your configuration file):** كما يوصى بمراجعة ملف إعدادات الخادم من وقت لآخر والتأكد أنه متوافق مع الخطة الأمنية للجهة (Security Plan) وتطبيق التوصيات المقترحة من الخبراء والمختصين لجعل الخادم أكثر أمانا وصلابة.

- **استخدام خدمة امتدادات نظام أسماء النطاقات الأمن ( Domain Name Service Security Extension-DNSSEC):** وهي خدمة جديدة ومهمة تقوم بالتأكد من أمرين مهمين هما: صحة مصدر المعلومة ومن صحة المعلومة نفسها (لم يتم تغييرها أو العبث بها) وتستخدم بين الخادمات التي تخدم نفس اسم النطاق لتبادل الملفات بينها (الخادمات الرئيسية والثانوية) كما يمكن استخدامها في أمور أخرى. ويتم ذلك باستخدام سجلات خاصة من نوع (SIG,KEY) التي تستخدم التواقيع الرقمية (digital signatures) المشفرة بواسطة(MD5/RSA and DSA algorithms) والمفاتيح العامة والخاصة (Public and Private Keys). بحيث يقوم الخادم بالتوقيع (تشفير) على كل معلومة (سجل مصدر) مخزنة عليه باستخدام المفتاح الخاص وربطها بالمعلومة الرئيسية ومن ثم يقوم الخادم الآخر (الثانوي) باستخدام المفتاح العام للخادم للتأكد من صحة المعلومة. والعيب الرئيسي في هذه الطريقة هي كونها صعبة التمثيل والتطبيق وعليها بعض الملاحظات، وهي أفضل من الوضع الحالي وعادة ما تستخدم للخادمات وأسماء النطاقات الهامة والحساسة. وللمزيد من المعلومات حول هذا الموضوع يمكن زيارة الرابط التالي: (http://www.dnssec.net ).

- **إخفاء نوع وإصدار الخادم(Hiding Server Version):** وينصح أيضا بإخفاء رقم إصدار خادم أسماء النطاقات و المقررات وهذا الأمر يعطي صعوبة على المهاجم بتحديد نوع خادم أسماء النطاقات أو الإصدار الحالي له، حتى لا يستغل الثغرات الأمنية على الخادم في حال اكتشافها.

**In Bind Configuration File (named.conf):**

```
options {
   directory "/var/named";
   version "Unknown"; };
```

- **حصر وتحديد الاستفسارات (Restricting Queries):** ومن أهم الإعدادات التي يجب عملها هو حصر وتحديد مصدر الاستفسارات التي يقوم الخادم (المقرر) بخدمتها. وعادة ما تكون الأجهزة الداخلية على الشبكة هي التي يوم المقرر بخدمتها، ويمكن القيام بذلك باستخدام المرشحات ( Access Lists) و المناظر (Views):

**In Bind Configuration File (named.conf):**

```
acl "internal" {
```

```
    192.168.1.0/24;
    192.168.2.0/24; };
view "internal" {
    match-clients { "internal"; };
    recursion yes; };
view "external" {
    match-clients { any; };
    recursion no; };
```

كما يمكن وضع بعض الشبكات الغير مستخدمة ( مثل شبكات العناوين الرقمية الخاصة) في القائمة السوداء لتجاهلها (والتي يستخدمها المهاجمون كمصدر للرسائل )، ويمكن عمل ذلك في المثال التالي:

**In Bind Configuration File (named.conf):**

```
acl "bogus-nets" {
   10.0.0.0/8
   172.16.0.0/12
   192.168.0.0/16; };
options {
   blackhole { "bogus-nets"; }; };
```

- **منع خدمة نقل ملفات النطاقات للجهات الغير مصرحة ( Preventing Unauthorized Zone Transfers):** نظرا لأن ملف النطاق يحتوي على جميع أسماء وعناوين الأجهزة والخدمات المتوفرة لتلك الجهة فانه من المهم عدم السماح لأي شخص بالحصول على هذه المعلومات كاملة، لذلك يتم تحديد الخادمات التي تستطيع نقل ملف النطاق، ويمكن ذلك بتعريف هذه الخادمات على مستوى الخادم وجميع النطاقات المستضافة علية مثل:

**In Bind Configuration File (named.conf):**

```
options {
   allow-transfer { 212.26.18.10; }; };
```

أو يمكن تحديدها على مستوى كل نطاق مثل:

**In Bind Configuration File (named.conf):**

```
zone "domain.com.sa" {
   type master;
   file "dbdomain.com.sa";
   allow-transfer { 212.26.18.10; }; };
```

- **التحقق من طالب خدمة نقل الملفات (Authenticate Zone Transfers):** وهذه الطريق مشابهة لامتدادات نظام أسماء النطاقات الآمن ولكنها أكثر بساطة (لا يتم تخزين التواقيع في ملف اسم النطاق)، إذ يتفق الخادمان على كلمة سر وطريقة تشفير معينه تمكنهم من تبادل ملفات النطاقات مع بعضهم البعض بعد التحقق من هوية كل واحد منهم وذلك بوضع توقيع على كل رسالة باستخدام كلمة السر وطريقة التشفير المتفق عليها:

**Bind Configuration File (named.conf) in the Master Server(212.26.18.10):**

```
key server1-server2-key. {
   algorithm hmac-md5;
   secret "La/E5CjG9O+os1jq0a2jdA="; };
server 212.26.18.11 {
   keys { server1-server2-key.; }; };
zone "domain.com.sa" {
```

```
    type master;
    file "db.domain.com.sa";
    allow-transfer { 212.26.18.11; }; };
```

**Bind Configuration File (named.conf) in the Slave Server(212.26.18.11):**

```
key example-key. {
    algorithm hmac-md5;
    secret "La/E5CjG9O+os1jq0a2jdA="; };
server 192.168.1.10 {
    keys { server1-server2-key.; }; };
zone "example.com" {
    type slave;
    masters {212.26.18.10;};
    file "db.example.com"; };
```

- **حصر وتقليل خدمة التحديث الآلي لملفات النطاق (Restrict Dynamic Updates):** تفيد خدمة التحديث الآلي لملفات النطاق المستخدمين المتنقلين (Mobile users) فعند دخول المستخدم على الشبكة يعطى عنوان رقمي خاص به ومن ثم يتم تحديث نظام أسماء النطاقات وربط ذلك العنوان بالمستخدم بالتضافر مع بروتوكول تعريف الأجهزة آليا ( Dynamic Host Configuration Protocol-DHCP)، ولكن يجب التعامل معها بحذر وحرص، كما يجب إعطاء إمكانية التعديل الآلي (على ملفات النطاق) إلى خادم (DHCP) فقط وباستخدام كلمة سر وطريقة تشفير معينة حتى يتم التوقيع على كل طلب تحديث يتم على ملف النطاق. وللمزيد من المعلومات يمكنكم زيارة الرابط التالي: ( http://ops.ietf.org/dns/dynupd/secure-ddns-howto.html).

- **تشغيل خادم أسماء النطاقات بأقل صلاحيات على نظام التشغيل ( Running BIND with Least Privilege)** : يجب تشغيل برنامج خادم أسماء النطاقات عن طريق مستخدم معين له صلاحيات محدودة جدا في استخدام موارد النظام ،فلا يمكنه مثلا الوصول إلى الملفات الحساسة (مثل ملف كلمات المستخدمين السرية) أو حتى تشغيل أو استخدام برامج أخرى موجودة على الخادم، وتكمن الفائدة من ذلك عند اختراق برنامج خادم أسماء النطاقات فان المهاجم لا يستطيع الحصول على موارد النظام ولا تخريب أشياء أخرى وذلك لأننا قد قمنا بحصر الصلاحيات المستخدم الذي قام بتشغيل برنامج خادم أسماء النطاقات. وللمزيد من المعلومات يمكنكم زيارة الرابط التالي: (http://www.faqs.org/docs/Linux-HOWTO/Chroot-BIND-HOWTO.html) أو الرابط التالي ( http://www.losurs.org/docs/howto/Chroot-BIND.html).

- **وضع مدة قصوى للسجلات المؤقتة ومساحة محددة لها**: و الفائدة الرئيسية من هذا الأمر هو تحديد المصادر المتاحة لبرنامج خادم أسماء النطاقات بدلا من استنفاذ جميع مصادر الجهاز، وأيضا عدم الاحتفاظ بالسجلات المؤقتة لفترات طويلة حتى وان أراد الخادم المسئول عن ذلك النطاق الاحتفاظ بالسجلات لمدة طويلة، لأنه قد يكون ذلك حصل بسبب خطأ أو لأن خادمهم قد تم اختراقه ومن ثم استرجاعه فيجب علينا عدم الاحتفاظ بالسجلات لوقت طويل.

**In Bind Configuration File (named.conf):**

```
options {
    max-cache-size 20M;
    max-cache-ttl 3600; // Seconds
    max-ncache-ttl 3600; // Seconds
};
```

- **عدم ربط أسماء الأجهزة بمالكها أو طبيعة استخدامها:** وهذه قاعدة معروفة تقوم على إخفاء نوع الجهاز أو مكانه أو حتى اسم صاحب الجهاز حتى لا نسهل على المهاجمين استغلال هذه المعلومات لاختراق الأجهزة أو استغلال المعلومة في الهندسة الاجتماعية (Social Engineering). فمثلا إذا قمنا بتسمية جهاز قاعدة البيانات الخاص بالشركة باسم (mysql-ser.domain.com.sa) نكون بذلك بينا أن هذا الجهاز يعمل كقاعدة بيانات للشركة ونوعه (MySQL) فيمكن للمهاجم البحث عن الثغرات الخاصة بهذا البرنامج ومحاولة مهاجمة الجهاز من خلالها، وبهذا نكون قد سهلنا العملية له.

- **التأكد من صحة ملفات أسماء النطاقات وتجنب الأخطاء الشائعة التي يمكن الوقوع فيها**: بعد إعداد أو تحديث ملف اسم النطاق يجب التأكد من أن ذلك تم على الوجهة الصحيح، ويمكن استخدام بعض الأدوات الخاصة بنظام أسماء النطاقات (مثل: nslookup أو dig أو host) و التي قد تساعد على اكتشاف الأخطاء من ثم تصحيحها تفاديا للوقوع في المشاكل التي قد تؤثر على عمل اسم النطاق أو أحد خدماته. وهذه قائمة بالأخطاء الشائعة التي قد تحدث عند بناء أو تحديث ملف اسم النطاق:

1. نسيان وضع نقطة "." عند نهاية أي نص (يمثل اسم جهاز أو خدمة أو نطاق فرعي) داخل ملف اسم النطاق، لأن ذلك سيؤدي إلى إلصاق اسم النطاق في نهاية ذلك النص:

```
; The zone file for "example.com"
ns1                 IN     A     212.26.18.1
www.example.com     IN     A     212.26.18.2
; The result of the previous 2 lines are equivalent to:
;    ns1.example.com.     IN A 212.26.18.1
;    www.example.com.example.com. IN A 212.26.18.2
; as you can see ns1 is accepted but www is incorrect!
```

2. عدم استخدام أرقام عناوين الانترنت الداخلية (Private IP addresses) أو أرقام العنوان المحلي (loopback) في ملفات أسماء نطاقات المستخدمة على الانترنت، لأنه على الانترنت لا يمكن الوصول إلا إلى الأرقام العامة (Public IP addresses):

```
; The zone file for "example.com"
ns1.example.com.    IN     A     127.0.0.1
www.example.com.    IN     A     10.1.1.1.
ftp.example.com.    IN     A     172.16.1.1.
mail.example.com.   IN     A     192.168.1.1.
; all of the previous hosts will not be reached on the internet.
```

3. التقليل من استخدام سجلات المترادفات (CNAME) قدر المستطاع، لأنها قد تسبب بعض المشاكل خصوصا عند استخدام أسماء الأجهزة أو الخدمات المعرفة من خلالها في بناء سجلات أخرى داخل ملف اسم النطاق.

```
; The zone file for "example.com"
ns1.example.com.    IN     A     212.26.18.1
ns2.example.com.    IN     CNAME    ns1.example.com.
mail.example.com.   IN     CNAME    ns1.example.com.

; These 2 lines will not work properly!
example.com.        IN     MX    10 mail.example.com.
example.com.        IN     NS       ns2.example.com.

; Both ns2 & mail should have their own "A" recode not "CNAME"
```

4. عدم استخدام السجلات الملصقة (Glue Records) إلا عند الحاجة لأن ذلك يؤدي إلى مشاكل في التزامن وصحة المعلومات عند تغير قيم السجلات في ملفاتها الأصلية، ويمكن استخدام السجلات

الملصقة فقط عن توكيل (delegate) نطاقات فرعية من النطاق الرئيسي بحيث تكون أسماء الخادمات المسئولة عن النطاق الفرعي تقع داخل النطاق الرئيسي أو النطاق الفرعي فقط.

```
; The zone file for "example.com"
Sub.example.com.       IN     NS    ns1.example.com.
Sub.example.com.       IN     NS    ns2.hosting.com.

ns1.example.com.       IN     A     212.26.18.1
ns2.hosting.com.       IN     A     212.26.18.2
ns3.sub.example.com.   IN     A     212.26.18.3

; Both ns2.hosting.com& ns3.sub.example.com are glue records.
; But there is no need for ns2.hosting.com to be in this zone file!
;     It should be in the zone file for hosting.com.
```

5. استخدام القيم الموصى بها عند تعريف أو تحديث سجل معومات ملف النطاق الـ "SOA" وكذلك زمن التحديث العام الخاص بسجلات ملف النطاق (TTL):

```
; The zone file for "example.com"
$TTL 2d ; default value for the TTL of all RRs in this zone file
example.com.  3600  SOA  dns.example.com. hostmaster.example.com. (
                    1999022301   ; serial YYYYMMDDnn
                    86400        ; refresh (  24 hours)
                    7200         ; retry   (   2 hours)
                    3600000      ; expire  (1000 hours)
                    172800 )     ; minimum (   2 days)
; for more information check: http://www.ripe.net/ripe/docs/ripe-203.html
```

6. عند تحديث ملف اسم النطاق يجب زيادة رقم تعريف الملف (serial) الموجود في سجل الـ "SOA"، حتى يمكن للخادمات الثانوية معرفة أن ملف اسم النطاق تم تحديثه ويجب عليهم الحصول على النسخة المحدثة.
7. يجب أن لا تكون سجلات البريد الالكتروني "MX" والخادمات الرئيسية للنطاق "NS" تؤشران على عناوين انترنت رقمية (IP Addresses)، بل تؤشران على أسماء أجهزة (لها عناوين انترنت رقمية مباشرة وليست CNAME).

```
; The zone file for "example.com"
example.com.       IN     NS    212.26.18.1
example.com.       IN     MX    10  212.26.18.2

; These two lines can't work and dose not mean any thing!.
```

8. عند توكيل خادمات أخرى لنطاق فرعي يجب التأكد من أن هذه الخادمات مستضيفة للنطاق الفرعي على الوجه الصحيح وأن في ملف النطاق الفرعي يوجد سجل "NS" خاص لكل خادم لأن عدم توفر ذلك قد يؤدي إلى مشاكل عديدة (Lame Delegation).
9. وأيضا من أكثر المشاكل انتشارا هو عدم التزامن بين الخادمات الرئيسي والثانوية، بحيث يعطي كل خادم رد مختلف عن الخادمات الأخرى. ويجب التأكد دوما من إمكانية وصول الخادمات بعضها ببعض (عدم وجود عوائق على الشبكة مثل جدار ناري أو موجة يمنع التراسل بينها) حتى يتم تبادل الملفات بشكل صحيح.

- **نسخ ملفات أسماء النطاقات وحفظها في مكان آمن:** كما يفضل أن نقوم بنسخ جميع ملفات النطاقات ووضعها في مكان آمن وعلى جهاز مستقل ولا يمكن الوصول إليه من قبل الآخرين، وذلك تحسبا

لوجود أي مشاكل قد تطرأ على الخادمات فيتم فقد الملفات من عليها. والأفضل بناء برامج تقوم بأتمتته هذه العملية بدلا من العمل اليدوي.

- **متابعة ملفات تتبع حالة الخادم (Monitor the log file) وملف الإحصاءات (Statistics File):** كما يجب إعداد ملفات تتبع حالة الخادم لمعرفة رسائل التحذير والخطأ التي قد تواجه الخادم أثناء تأدية عملة، كما يجب إعداد ملف الإحصاءات التي تعطي تقارير عديدة عن الخادم (مثل عدد الاستفسارات التي قام بخدمتها حسب نوعها).

**In Bind Configuration File (named.conf):**

```
logging {
    channel simple_log {
        file "/var/log/named/bind.log" versions 3 size 5m;
        severity warning;
        print-time yes;
        print-severity yes;
        print-category yes;  };
    category default{
        simple_log;  }; };
options {
   statistics-file "bind.stats";
};
```

- **الاشتراك في القوائم البريدية الخاصة بالمخاطر التي تهدد النظام**: ومن أهم هذه القوائم البريدية قائمة الإعلانات الخاصة ببرنامج بايند (Bind) ويمكن الاشتراك فيها من خلال الرابط التالي: (http://www.isc.org/index.pl?/sw/bind/bind-lists.php) ، كما يمكن الاشتراك أيضا بالقائمة البريدية الخاصة بنظام أسماء النطاقات بشكل عام من خلال إرسال رسالة اشتراك إلى العنوان البريدي التالي: (namedroppers-request@ops.ietf.org ).

- **تسجيل اسم نطاق بشكل صحيح وآمن**: سبق وأن بينا المخاطر التي قد تواجهه المستخدم الذي يقوم بتسجيل اسم النطاق وما يترتب عليها من أمور، ولتجنب هذه المخاطر يمكن للمستخدم إتباع النقاط التالية عند تسجيل اسم النطاق:

1. عدم الاعتماد على أشخاص غير موثوقين أو على شركات الاستضافة في تسجيل اسم النطاق.
2. تسجيل اسم النطاق لفترة طويلة (أكثر من سنة) إذا أمكن ذلك.
3. الاحتفاظ بمعلومات التسجيل في مكان آمن.
4. التأكد من صحة معلومات المنسق الإداري وأنه هو الشخص الصحيح.
5. تحديث معلومات التسجيل باستمرار وإتباع إجراءات تمديد التسجيل و التأكد من دفع المبالغ المطلوبة في الوقت المناسب.
6. استخدام كلمة مرور قوية (مكونة من حروف وأرقام ورموز خاصة وطولها على الأقل ثمانية خانات) لإدارة اسم النطاق أو للبريد الالكتروني المسئول عن النطاق.
7. كما يفضل تسجيل أسماء النطاقات المشابه لاسم النطاق وخصوصا إذا كان اللبس وارد عند مستخدمي الانترنت.
8. يجب وجود عقد بين مسجل النطاق ومستضيف النطاق يضمن تطبيق التوصيات الفنية اللازمة لتشغيل اسم النطاق و الخدمات القائمة عليه. كما يفضل التحقق من صحة الجهة المستضيفة ومصداقيتها في التعامل وإمكانية مقاضاتها قانونيا عند إخلالها بالاتفاق (لا سمح الله).

- **التأكد من صحة أسماء النطاقات والخدمات المعتمدة عليها:** كما يجب على المستخدمين التأكد جيدا من صحة أسماء النطاقات أو الأجهزة (المستخدمة في المواقع الشبكة أو عناوين البريد الالكتروني) حتى لا يقعوا فريسة سهلة للمهاجمين من خلال (DOMAIN FISHING).

- **التأكد جيدا من صحة تعريف نظام أسماء النطاقات في إعدادات الشبكة على الأجهزة:** كما يجب التأكد من صحة تعريف نظام أسماء النطاقات (داخل إعدادات الشبكة) على جميع الأجهزة وأنه لم يتم العبث بها ولا بملف الترجمة الداخلي (hosts) الموجود عليها.

**الخاتمة:**

بعد هذا السرد السابق عن نظام أسماء النطاقات وبيان أهمية وحساسية هذا النظام، وبعد التطرق إلى المخاطر التي قد تواجهه وكيفية التغلب عليها، تبقى لنا أمر واحد مهم وهو ضرورة نشر الوعي التقني والأمني بين مهندسي الشبكات (Network Admin) ومسئولي الأجهزة (System Admin) ومستخدمي النظام (End Users) حول هذه النظام والمخاطر التي تواجهه حتى لا تكون شبكاتهم فريسة سهلة للمهاجمين. كما يجب التنبيه إلى حقيقة مؤلمة وهي أن المهاجمين يطورون أساليبهم وطرقهم باستمرار لذلك يجب الحذر منهم وإتباع وسائل الحماية الممكنة بعد التوكل على الله عز وجل أولا وأخيرا.

وفي الختام أدعوا الله عز وجل أن يحفظ الجميع من كل شر ومكروه والسلام عليكم ورحمة الله وبركاته.

**مع تحيات ،،،**
**أخوكم/ رائد بن إبراهيم الفايز**
**المركز السعودي لمعلومات الشبكة - وحدة خدمات الانترنت – مدينة الملك عبد العزيز للعلوم والتقنية**
**1426/2005هـ**
**raed@isu.net.sa**

**المراجع:**

1. ***Dr. Abdullaziz Al-Zoaman, "عناوين شبكة الانترنت ماذا تعرف عنها"*, كتاب الطبعة الأولى, 2004**

2. ***P. Albitz and C. Liu*, "DNS and BIND", 4th edition, O'Reilly & Associates, 2001**

3. ***Seán Boran*, "Running the BIND9 DNS Server securely",Boran , 2004**
**http://www.boran.com/security/sp/bind9_20010430.html**

4. ***Rob Thomas*, "Secure BIND Template", version 4.7, 30 Mar 2005**
**http://www.cymru.com/Documents/secure-bind-template.html**

5. ***Seng Chor, Lim*, "DNS Security Considerations and the Alternatives to BIND", version 1.0, 2 Oct 2001**
**http://www.sans.org/rr/whitepapers/dns/567.php**

6. ***Wezel* , "Understanding and Attacking DNS", Linux Exposed, 13 May 2004**
**http://www.linuxexposed.com/Articles/Hacking/Understanding-and-Attacking-DNS.html**

7. *Diane Davidowicz* ,"Domain Name System (DNS) Security", 1999
http://compsec101.antibozo.net/papers/dnssec/dnssec.html

8. *Expert Security Associate*, "Attacking the DNS Protocol", ESA, version 2, 29 Oct 2003
http://www.secinf.net/uplarticle/WebSecurity/AttackingtheDNSProtocol.pdf

9. *Internet Systems Consortium (ISC)*, "BIND 9 Administrator Reference Manual (9.3.1)", HTML File, Mar 2005
http://www.bind9.net/manuals

10. *Jeff Holland*, "DNS Security", Whitehats.Ca, 23 Jul 2000
http://www.whitehats.ca/main/members/Jeff/jeff_dns_security/jeff_dns_security.html

11. *Luis Grangeia*, "DNS Cache Snooping", Version 1.1, Feb 2004
http://community.sidestep.pt/~luis/DNS-Cache-Snooping/DNS_Cache_Snooping_1.1.pdf

12. *Florent Carli*, "Security Issues with DNS", SANS GSEC Practical Assignment, Version 1.4b
http://www.sans.org/rr/whitepapers/dns/1069.php

13. *Thomas Lee*, "The Domain Name Service", 2004,
http://www.reskit.net/DNS/

14. *Allen Householder and Brian King*, "Securing an Internet Name Server", CERT® Coordination Center, 2002