УДК 65.012.45

І.І. Пархоменко, Є.В. Крилов

ЗАХИСТ СЕРВЕРІВ DNS, ЯК ЗАСІБ БЕЗПЕКИ INTERNET-КОМЕРЦІЇ

Вступ

Internet-комерція, як і будь який вид комерційної діяльності, потребує захисту від несанкціонованого доступу. Однак, як сама мережа Internet, так і одна з її ключових інфраструктур - DNS, захист був не самою головною метою. Як результат DNS являє собою незахищений протокол.

DNS – це ієрархічна база даних, яка вміщує записи з описом імен, IP-адрес і іншу інформацію про хости. База даних розміщується на серверах DNS які пов'язані з Internet і Intranet мережами. DNS надає мережним додаткам послуги каталогу по перетворенню імен на адреси, коли їм необхідно визначити місцезнаходження конкретних серверів.[2]

Проблема полягає в тому, що немає ніякого способу перевірити, чи отримав DNS відповідь від автентичного джерела і чи вміщує вона автентичні дані. Цей факт викликає особливу занепокоєність у зв'язку з тим, що DNS часто використовується в якості системи наявної ідентифікації.

Неточні або неправильні дані можуть призвести до того, що користувачі зіткнуться з відмовою в обслуговуванні чи будуть перенаправлені на сервери сумнівного змісту.

Постановка проблеми

Серед головних проблем підприємства, яке здійснює Internet-комерцію, хотілося б відзначити наступні:

- віддалені атаки за допомогою підмінних (несправжніх) серверів DNS;
- атаки за допомогою неправдивих відповідей DNS;
- можливість доступу до внутрішньої мережі із зовні.

Розглянемо, чим загрожують зазначені небезпеки Internet-комерції.

Потенційна можливість віддалених атак з використанням помилкових серверів DNS відома давно. У літературі подібні атаки називають підміною DNS (DNS spoofing). Разом з тим до їх ефективності відносяться досить скептично. Так, в одному із авторитетних видань із проблем мережної безпеки "Maximum Security. A Hacker's Guide to Protecting Your Internet Site and Network"видавництва Sams.net Publishing, 1997 стверджується, що незважаючи на небезпеку атаки типу підміни DNS реалізувати її украй важко. Крім того, знайти і знешкодити атаку (а часом навіть її спробу) не так вже і складно. На жаль, це вірно в загальному випадку, а в подробицях усе може бути зовсім інакше.

Тепер щодо самих атак з підміною DNS. Очевидно, що найбільш ефективні атаки, пов'язані з перехопленням запитів DNS. У цьому випадку

помилковий сервер DNS перехоплює запит до справжнього сервера DNS і посилає відповідь клієнту раніше справжнього сервера від імені останнього. Для реалізації такої атаки необхідно, щоб помилковий сервер DNS був підключений до ланцюжка клієнт-справжній сервер DNS. В результаті такої атаки, клієнти, наприклад, Internet-магазину або не зможуть зв’язатися з ним, або одержать неправдиву інформацію, витратять марно час і, можливо, гроші і в наступному більше до такого підприємства не звертатимуться.

Інший тип атаки пов’язаний зі "штормом"помилкових відповідей DNS. Особливість такої атаки в тому, що помилковий сервер DNS не розташовується в ланцюжку клієнт-дійсний сервер і не може перехопити запити DNS. Тому він не знає ні адреси клієнта, ні імені машини, адресу якої шукає клієнт. Помилковий сервер DNS не може навіть вгадати час запиту. На доданок хакер має справу ще з цілим рядом невідомих, наприклад з використовуваним протоколом, номером програмного порту, з якого посилається запит, і порядковим номером DNS-пакета при запиті.[1]

Як об’єкт атаки звичайно вибирається активний клієнт мережі. Ставка робиться на те, що клієнт буде намагатися зв’язатися з відомим йому сервером. Правда, навіть якщо атака удасться, то в кращому (для хакера) випадку він зможе тільки змінити заставку даного сервера на яку-небудь іншу. Методом простого перебору UDP-портів клієнта й ідентифікаторів DNS-запитів помилковий сервер DNS дошкуляє потенційну жертву "штормом"помилкових відповідей. Оскільки помилковий сервер DNS у загальному випадку не знає, коли клієнт звернеться з DNS-запитом по конкретному вузлу, "шторм"помилкових відповідей повинен продовжуватися досить довго, щоб атака була результативною. Але якщо атака такою стане, то клієнти Internet-магазину не зможуть зв’язатися з ним протягом досить довгого часу, що в результаті також приведе до їх відмови від послуг даної компанії.

Найбільш небезпечною загрозою є доступ до внутрішньої мережі кампанії із зовні. Оскільки переважна частина конфіденційної інформації передається всередині мережі підприємства, то підключення до ланцюжка клієнт-локальний сервер DNS було б для хакера найкращим. Перехоплення на рівні Internet хакеру, звичайно, теж цікаве, але там важливу інформацію намагаються передавати в зашифрованому вигляді.[4]

Яким же чином можливо увійти у систему із зовні? Мова йде про додатки, які встановлюють довірчі відносини на основі доменних імен хостів, а не паролів користувачів. До них відносяться NFS, NIS, SMTP, X, rsh, rlogin, rcp і почасти ftp і rexec (коли задіяні конфігураційні файли типу $HOME/.netrc). Якщо використовувати згадані додатки навіть винятково *всередині* мережі підприємства і не задіяти добре продуману систему безпеки, то за допомогою атаки з підміною DNS досить просто одержати доступ до мережі із зовні.

Таким чином можна побачити, що несанкціоновані дії щодо DNS можуть нанести значні збитки компанії, яка здійснює Internet-комерцію,

 ISSN 1562-9945

тому здійснення заходів захисту DNS-серверів є одним з актуальних завдань системного адміністратора такої компанії.

Головні практично-наукові результати

Розглянувши небезпеки для DNS серверів, які несуть загрозу Internet-комерції, охарактеризуємо основні засоби захисту від них.

По-перше, головною запорукою захисту DNS сервера є правильне його конфігурування. Конфігуруючи сервер, адміністратори часто забувають правильно настроїти службу DNS. Після такого настроювання служба DNS працює коректно: IP-адреси переводяться в імена комп’ютерів, а символьні імена без проблем перетворяться на IP-адреси. На цьому більшість адміністраторів і зупиняються: головне, щоб система працювала. Однак, неправильно настроєний сервер DNS може стати величезною дірою в системі безпеки компанії. Одна справа, коли сервер DNS обслуговує локальну мережу без виходу в Інтернет: навіть, якщо хтось і спробує "зламати"сервер, то обчислити "хакера"досить просто. А ось, якщо мережа підприємства підключена до Інтернет, то довідатися, хто ж намагався зламати (або зламав) дану мережу досить складно. Збиток від злому може обійтися компанії в серйозну суму.

Перш, ніж приступити до злому мережі або окремої системи зловмисник (або група зловмисників) намагається зібрати якнайбільше інформації: імена комп’ютерів мережі, імена користувачів, версії встановленого програмного забезпечення.

Якщо адміністратор забув правильно настроїти трансфер зони, то хто завгодно одержить список комп’ютерів нашої мережі.

Щоб не трапилося непоправного, необхідно дозволити передачу зони тільки одному комп’ютерові - вторинному серверові DNS компанії, якщо такий існує. Вторинний сервер DNS, як правило, не передає ніякої інформації про зону, тому обов’язково варто настроїти його для заборони передачі такої інформації, а якщо у компанії немає вторинного сервера DNS, необхідно подібнім чином настроїти основний сервер DNS.

З розумінь безпеки рекомендується запускати всі мережні сервіси в так званому chroot-оточенні. Тобто створюється файлова система, яка повторює структуру кореневої файлової системи, але на цій файловій системі будуть тільки ті файли, які необхідні для запуску мережного сервісу. Зламавши мережний сервіс і одержавши доступ до кореневої файлової системи, зловмисник не зможе зашкодити всій системі в цілому, оскільки він одержить доступ тільки до файлів, які належать даному мережному сервісові. Тепер розберемося, як усе це організовується. Не потрібно створювати окремий розділ на диску для кожного мережного сервісу: потрібно тільки створити каталог, наприклад, root-dns, у який копіюються усі файли, необхідні для запуску сервера DNS. Потім, при запуску сервісу, буде виконана команда chroot для цього сервісу, який підмінить файлову систему. А через те, що в каталозі root-dns, який стане каталогом /, є всі необхідні файли для роботи bind, то для сервісу запуск і робота в chroot-оточенні буде зовсім прозорим.[3]

Крім належного конфігурування системи, важливе місце у забезпеченні захисту DNS серверів належить спеціальним програмним засобам.

Для розв’язання проблеми зовнішніх атак використовується розширення захисту для протоколу DNS – Domain Name System Security (DNSSEC).

Один із головних вкладів DNS в Internet – можливість унікальним чином відображувати однозначно імена хостів, які ідентифікуються на IP-адреси у всесвітньому масштабі. Ця процедура відома, як пряме відображення. Серед деяких інших можливостей DNS – зворотне відображення (тобто визначення імені хоста по IP-адресі), інформація про сервера електронної пошти (ідентифікація поштового сервера для даного хосту чи домену) і канонічне найменування (призначення псевдонімів для імені хосту).

В DNS ця інформація зберігається в записах ресурсів (Resource Records, RR). Ієрархічна впорядкованість DNS забезпечує унікальність імен хостів, структура DNS має вид перевернутого дерева. При переміщенні по дереву від листка до кореня отримуємо повне доменне ім’я (Fully Qualified Domain Name, FQDN). В DNS всяке ім’я FQDN є унікальним. Запит з вказаним ім’ям хосту призводить до перегляду структури дерева від кореня до листка з метою знаходження відповідної до нього IP-адреси. Аналогічне дерево є і для зворотного відображення, у випадку якого запит з IP-адресою призводить до перегляду структури цього дерева для надходження імені хосту чи FQDN, для вказаної IP-адреси.[2]

Верхньому рівню перевернутого дерева відповідає корінь DNS. Цей корінь як правило позначається “.” і є останнім символів в FQDN. Перший рівень нижче кореня ділиться на крупні класи, такі, як некомерційні організації (org), комерційні структури (com), освітні (edu) і т. ін.. Наступний рівень як правило представляє конкретні організацію чи компанію в домені org, edu чи com.

Такий спосіб послідовного ділення імен доменів дозволяє унікальним образом ідентифікувати хост в домені, до якого він належить. Можливість делегування прав адміністрування і локального керування іменами хостів забезпечує суттєву гнучкість і масштабованість DNS.

Метою DNSSEC – є забезпечення автентифікації і цілісності інформації, яка розміщується в DNS. DNSSEC дозволяє досягти цієї мети завдяки шифруванню. DNSSEC базується на шифруванні з відкритим ключем для підпису інформації, яка розміщується в DNS. Такі криптографічні підписи забезпечують цілісність за рахунок обчислення криптографічного хешу (тобто унікальної контрольної суми) даних і потім захисту вирахуваної величини від несанкціонованих змін завдяки його шифруванню. Хеш шифрується за допомогою особистого ключа із пари ключів, для того щоб кожен бажаючий міг скористатися відкритим ключем для його дешифрування. Якщо отримане користувачем дешифроване значення хешу співпадає з вирахуваним, то дані вірні (не було несанкціонованих змін).

Криптографічні підписи і відкритий ключ, який використовується

для верифікації підпису, отримують завдяки запитам і відповідям, як і будь-яку інформацію в DNS. У випадку криптографічного підпису автентифікація відбувається неявно, на основі факту спів падання дешифрованого і вирахуваного значення хешу. Таким чином, будь-яка система на базі технології відкритих ключів повинна забезпечувати надійний захист особистих ключів. Цьому питанню присвячений документ RFC 2541 робочої групи DNSSEC.

Криптографічні підписи DNSSEC застосовуються до даних по зоні, динамічним оновленням і трансакціям DNS. Крім того, вони використовуються для підтвердження відсутності даних DNS. DNSSEC надає три нові записи ресурсів - KEY RR, SIG RR и NXT RR.

KEY RR має відкритий ключ, який належить імені домену, вказаному в KEY RR. Це не сертифікат відкритого ключа. Механізм забезпечення можливостей пошуку сертифікатів відкритих ключів передбачає DNSSEC WG, але не для цілей захисту даних DNS. Він надається в якості додаткового бонусу, дякуючи якому DNS може застосовуватися для запиту сертифікатів відкритих ключів на все, що може бути представлено з допомогою імені домену. Цю можливість забезпечує CERT RR.

SIG RR має переважно криптографічний підпис, дату закінчення терміну придатності, підписи і певні дані DNS, до яких цей підпис відноситься. NXT RR дозволяє перевірити (за рахунок використання криптографії), що RR для даного імені DNS не існує. Таким чином, відсутність даного RR може бути підтверджено доказово.

Іншим аспектом DNSSEC є підпис трансакцій (Transaction Signature, TSIG). TSIG відрізняється від інших підписів DNS тим, що вона створюється з використанням шифрування з секретними ключами.

Протокол DNSSEC не забезпечує конфіденційності даних чи контролю доступу. Але конкретні його реалізації передбачають механізми забезпечення конфіденційності і контролю доступу. Причина відсутності такого стандартного механізму в DNS, полягає в тому, що протокол DNS призначений для роботи з загальнодоступними даними. Неможливість збереження інформації відносно імен і місцезнаходження систем і можливість отак по типу “відмова в обслуговуванні” стимулює попит на механізми забезпечення конфіденційності і контролю доступу. Цей попит відображується в реалізаціях DNS. В даний час конфіденційність частково забезпечується за рахунок застосування брандмауерів і розщепленої DNS для ускладнення доступу із зовнішнього середовища до внутрішньої інформації DNS.[2]

Internet Software Consortium (ISG) – некомерційна організація, яка займається реалізацією базових протоколів Internet у вигляді відкритих кодів, - ввела декілька механізмів захисту для наділення сервера DNS можливостями DNSSEC. Наприклад, один з них визначає автентичність даних в системі на основі перевірки факту їх підпису адміністратором вузла, від якого вони надійшли.

Один із способів перевірити відкритий ключ до використання його для перевірки відповіді – переглянути підпис самого відкритого ключа. Коре-

невий вузол повинен підписувати всі свої відкриті ключі. Для того, щоб бути абсолютно впевненими в тому, що відкриті (перевірочні) ключі кореня дійсно належать йому, вони повинні знаходитися на вашому комп'ютері в файлі, який отриманий захищеним чином. Так як корінь є в основі всіх імен доменів, для всієї DNS потрібен тільки один відкритий ключ. Інший механізм захисту, який ввела ISC, перевіряє факт надходження протокольного повідомлення від джерела, яке заслуговує довіри.

У дев'ятій версії BIND з'явилася можливість створювати підписи транзакцій (TSIG - Transaction SIGnatures). Механізм TSIG працює так: сервер одержує повідомлення, підписане ключем, потім підпис перевіряється, якщо він "правильний", сервер відправляє відповідь, підписану тим же ключем.

Механізм TSIG дуже ефективний при передачі інформації про зону, повідомлень про зміну зони і рекурсивних повідомлень. Перевірка підпису надійніша, ніж перевірка IP-адреси. Зловмисник може вивести вторинний сервер DNS банальною атакою на відмовлення, і, поки адміністратор буде "піднімати"вторинний сервер, він замінить свою IP-адресу адресою вторинного сервера. При використанні TSIG задача зловмисника значно ускладнюється: адже йому доведеться "підібрати"128-бітний MD5-ключ, а імовірність такого підбору майже нульова.[1]

Ще одним способом підвищення рівня захисту мережі є створення двох зон DNS: відкритої для зовнішнього світу і доступної тільки корпоративним користувачам. Деякі фахівці називають таку структуру розділеною (split-brain) DNS. Вона функціонує в такий спосіб.

Одержавши запит на перетворення імені, основний DNS-сервер спочатку звертається до кешу. Якщо імені в кеші немає, а DNS-сервер містить зони, то сервер намагається перетворити ім'я, перевіряючи зони. Сервер звертається до ретранслятора або в Internet лише в тому випадку, якщо не може знайти потрібну адресу в кеші або в зонах. Головна особливість розділеної DNS полягає в тому, що DNS-сервер більше довіряє інформації із зон, чим даним, які одержані з Internet.

Література

1. Пьянзин К. Атака и защита DNS//"LAN/Журнал сетевых решений".- 7.-1997
2. Давидович Д., Викси П. Защита DNS//“LAN/Журнал сетевых решений”.- 2.- 2000
3. Робачевский А.М. Операционная система UNIX.- СПб. BHV - Санкт-Петербург, 1998.
4. Эви Немет, Гарт Снайдер, Скотт Сибасс, Трент Р. Хейн. UNIX руководство системного администратора. -К.: BHV, 1997