УДК 004.057.4

DNSSEC ЯК УНІВЕРСАЛЬНИЙ ЗАХИСТ DNS

В. І. Кравчук[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

В роботі представлені основні принципи роботи служби DNS (Domain Name System), розглянуто існуючі види атак та механізмів захисту даної служби, а також проаналізовано можливості Dnssec як сучасного механізму захисту від атак даних типів.

Ключові слова: домен, DNS, фішинг, кеш, спуфінг, резолвер, цифровий підпис

Вступ

Сучасні користувачі Інтернету вже давно звикли до символьних адрес сайтів, наприклад: «kpi.ua» чи «ukr.net». Проте, для адресації вузлів Інтернету використовуються саме IP-, а не символьні адреси. Для зручності запам'ятовування було вирішено співставляти IP адреси вузлів в їх символьними адресами. Цю функцію виконує система доменних імен (DNS). Дана система була сформована на початку формування мережі Інтернет [1] і є одним з ключових життєвоважливих компонентів. Метою даної роботи є аналіз існуючих механізмів захисту від атак на DNS та формування найбільш ефективного підходу боротьби з ними.

1. Об'єкт досліджень

Об'єктом досліджень роботи є **система доменних імен (DNS)**, інсуючі вразливості, а також методи захисту від цих вразливостей.

1. Принципи роботи DNS Зі схемою роботи системи домених імен можна ознайомитись на рис. 1: ПК користувача відправляє запит на DNS сервер з бажанням дізнатись IP адресу вузла, що має вказану у запиті символьну адресу; DNS сервер, знайшовши у себе в базі даних відповідну пару, відсилає ПК IP адресу запитуваного вузла; ПК переходить за отриманою IP адресою. Нажаль, в часи формування сучасної мережі Інтернет, розробники не могли передбачити можливі вразливості DNS на декілька наступних десятиліть. Саме тоді для реалізації даної системи було використано протокол UDP (User Datagram Protocol). Єдина передавага протоколу *UDP* в порівнянні, наприклад, з протоколом TCP (Transmission Control Protocol) – це швидкість, яка досягається завдяки малому розміру UDP пакету. Для порівняння схеми пакетів протоколів TCP та UDP вказані на рис. 2 та рис. 3 відповідно.

З вище описаних схем (рис. 2, рис. 3) чітко видно що заголовок TCP пакету – 20 байт, а заголовок UDP пакету – всього 8 байт. Різниця – 12 байтів еко-

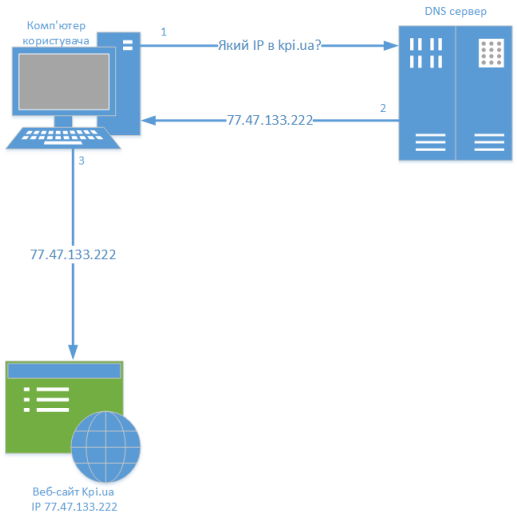

Рис. 1. Спрощена схема роботи системи DNS

2 байти - номер порту відправника								2 байти - номер порту одержувача
4 байти – номер послідовності								
4 байти – номер підтвердження								
Довжина заголовка 4 біти	Зарезервовано 6 біт	URG	ACK	PSH	RST	SYN	FIN	2 байти – розмір вікна
2 байти – контрольна сума TCP								2 байти – вказівник терміновості
Опції								
Дані								

Рис. 2. Структура пакету TCP

2 байти - номер порту відправника	2 байти - номер порту одержувача
2 байти - байти довжина пакета UDP	2 байти - значення контрольної суми UDP
Дані	

Рис. 3. Структура пакету UDP

[a] vadimkravchuk1994@gmail.com

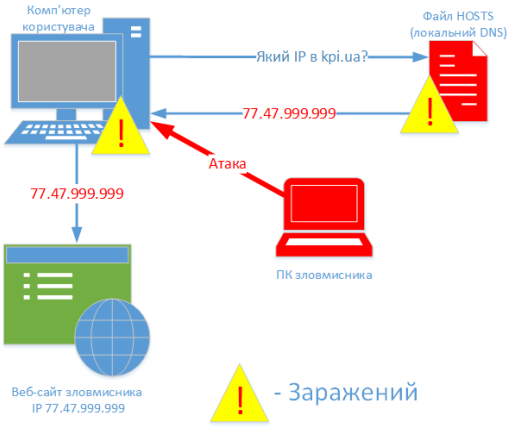

Рис. 4. Підміна локального DNS кешу

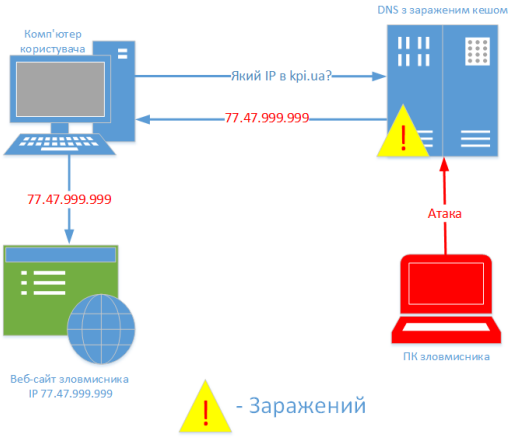

Рис. 5. Підміна локального кешу DNS серверу

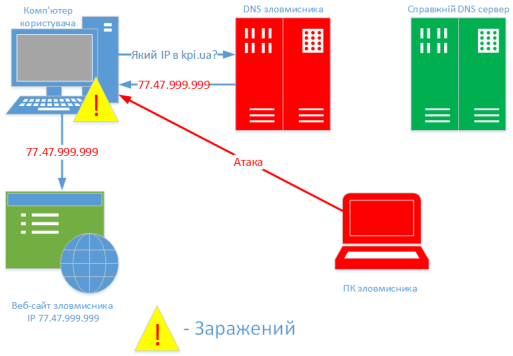

Рис. 6. Підміна DNS-сервера

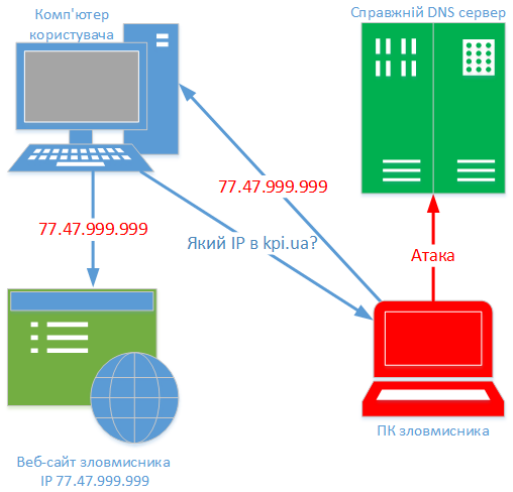

Рис. 7. DNS спуфінг

номії для кожного пакету. Саме ця різниця робить протокол UDP найшвидшим серед своїх аналогів.

2. Різновиди атак на DNS [2]

- **Модифікація кешу DNS (DNS cache poisoning)**

Перший спосіб (рис. 4) При використанні першого способу зловмисник встановлює шкідливе програмне забезпечення на, що має контролювати локальний кеш DNS на машині жертви. Після цього записи в локальному кеші DNS модифікуються для вказівки на інші, потрібні зловмиснику IP-адреси. Наприклад, якщо браузер намагається отримати доступ до сайту за адресою `http://www.kpi.ua/`, замість IP-адреси `kpi.ua` він отримає адресу, встановлену програмним забезпеченням зловмисника, який зазвичай веде на сайт, розташований на сервері, що безпосередньо підконтрольний зловмисникові.

Другий (рис. 5), більш небезпечніший для жертви спосіб, полягає в тому, що зловмисник атакує DNS-сервер і модифікує його локальний кеш. Таким чином, всі вузли, що використовують цей сервер для дозволу імен, отримуватимуть некоректні IP-адреси, що призведе в до масового переходу клієнтів на сайт зловмисника.

- **Підміна DNS-сервера (DNS hijacking)**

Дана атака (рис. 6) часто використовується для зміни принципу роботи систем DNS. В даному випадку не вноситься ніяких змін в кеш DNS клієнта, але виконуються зміни в настройках, після яких всі запити дозволу імен адресуються DNS-серверу зловмисника.

- **Спуфінг(підробка) DNS-запитів (DNS spoofing)**

Ця атака (рис. 7) є найпоширенішою та найпопулярнішою з усіх DNS атак. Вона відноситься до MITM (Man in the middle) атак. В ході атаки зловмисник за допомогою методів соціальної інженерії отримує доступ до мережі, в якій працює DNS-сервер. Потім модифікує ARP-кеш за допомогою спуфінгу пакетів. Як тільки зловмисник отримує контроль над мережею рівня MAC-адресів, зловмисник виявляє IP-адреси DNS-сервера, бере на себе роль DNS-сервера та починає відстежувати та модифікувати запити. Всі запити з мережі проходять через комп'ютер зловмисника і досягають реального DNS-сервера. Ця атака може мати серйозні наслідки, оскільки всі комп'ютери в мережі жодним чином не будуть фіксувати факт атаки і відправлятимуть все DNS-запити на адресу комп'ютера зловмисника.

2. Результати досліджень

Дослідивши вище перелічені атаки, було знайдено єдине рішення, яке дозволяє запобігти реалізації усіх наявних атак. У 2010 році було створене розширення для служби DNS під назвою DNSSEC (Domain Name System Security Extensions) [3], покликане вирішити абсолютно усі проблеми безпеки DNS. Го-

ловна його особливість – це криптографічний підпис доменної зони. DNSSec використовує два типи ключів – одним підписується зона (ZSK, zone signing key), іншим підписується набір ключів (KSK, key signing key) Розглянемо механізм роботи детальніше:

1) Користувач запитує доменне ім'я у Резолвера (кешуючий DNS сервер) [4];
2) Резолвер запрошує kpi.ua у DNS-сервера (припустимо, в кеші локальних серверів інформації про домен не знайшлося і запит дійшов до сервера провайдера);
3) При відсутності інформації в кеші серверів провайдера запит перенаправляється на кореневий сервер, також виставляється біт DO, що інформує про те, що використовується DNSSec;
4) Кореневий сервер повідомляє, що за зону 'ua' відповідає сервер qwerty.net. При цьому сервер відправляє набір NS-записів для зони ua, записи DS і підпис записів NS і DS;
5) Резолвер проводить валідацію отриманого ZSK шляхом перевірки відповідності підпису, виконаної ключем KSK кореневої зони. Потім Резолвер перевіряє цифровий підпис записів DS кореневої зони. Якщо і тут все вірно, то сервер довіряє отриманим даним і перевіряє з їх допомогою підпису запису DNSKEY рівня нижче – зони org;
6) Тепер, після отримання адреси сервера, відповідального за зону ua (сервера qwerty.net), Резолвер переправляє йому той самий запит;
7) Сервер qwerty.net повідомляє про те, що сервер, відповідальний за зону kpi.ua, має адресу asd.net. Також він відправляє підписані за допомогою закритого KSK зони ua набір ключів підпису (DS) зони ua і підписаний за допомогою ZSK зони ua дайджест KSK зони kpi.ua;
8) Резолвер проводить порівняння отриманого від кореневого сервера хешу з тим, що він порахував самостійно з KSK зони ua, отриманого від сервера qwerty.net, і в разі збігу починає довіряти цьому KSK. Після цього Резолвер перевіряє підписи ключів із зони ua і починає довіряє ZSK зони ua. Потім Резолвер перевіряє KSK зони kpi.ua. Після всіх цих перевірок у Резолвер є дайджест (DS) KSK зони kpi.ua та адресу сервера asd.net, де зберігається інформація про зону kpi.ua;
9) Нарешті Резолвер звертається на сервер asd.net за сайтом kpi.ua, і при цьому виставляє біт про те, що використовує DNSSec;
10) Сервер asd.net розуміє, що зона kpi.ua знаходиться на ньому самому, і відправляє Резолверу відповідь, що містить підписаний за допомогою KSK зони kpi.ua набір ключів підпису (ZSK) зони kpia і підписаний за допомогою ZSK зони kpi.ua адресу сайту kpi.ua;
11) Також, як у пункті 7 Резолвер перевіряє KSK зони kpi.ua, ZSK зони kpi.ua та адресу сайту kpi.ua;
12) При вдалій перевірці в пункті 10 Резолвер повертає користувачеві відповідь, що містить в собі адресу сайту kpi.ua і підтвердження, що відповідь верифікована (виставлений біт AD).

Висновок

В результаті проведеного аналізу існуючих механізмів захисту, було виявлено систему, яка забезпечує найбільш ефективний підхід до захисту DNS від існуючих типів атак. Обране рішення було впроваджено та налаштовано з метою зібрати та проаналізувати статистичні дані про атаки.

Перелік використаних джерел

1. Система DNS. Немного истории и принципы построения иерархии имен. [Електронний ресурс]. – 2003. – Режим доступу до ресурсу: http://www.info.nic.ru/st/54/out_14.shtml.
2. Радивилова Т. А. Анализ основных атак на dns-сервер и методы использования dnssec при защите dns-сервера / Т. А. Радивилова, В. С. Бушманов. // Технологический аудит и резервы производства. – 2013. – №1. – С. 16–19.
3. Тульев М. DNSSEC на защите доменов. [Електронний ресурс] / Максим Тульев – Режим доступу до ресурсу:http://ukrainaforever.narod.ru/domain/protection-domen1.htm.
4. DNSSec: Что такое и зачем [Електронний ресурс] // Habrahabr. – 2011. – Режим доступу до ресурсу: http://habrahabr.ru/post/120620/.
5. Пьянзин К. Атака и защита DNS [Електронний ресурс] / Константин Пьянзин // Журнал сетевых решений/LAN. – 1997. – Режим доступу до ресурсу:http://www.osp.ru/lan/1997/07/132968/.
6. Медведовский И. DNS под прицелом [Електронний ресурс] / Илья Медведовский // Журнал сетевых решений/LAN. – 1997. – Режим доступу до ресурсу:http://www.osp.ru/lan/1997/05/132801/.
7. Краснов В. Хакеры атакуют: как уберечь DNS-сервер [Електронний ресурс] / Виталий Краснов // CNews. – 2010. – Режим доступу до ресурсу: http://www.cnews.ru/reviews/2010/08/13/405098.