УДК 004.056.53

Алімов Р.А.
Науковий керівник: к. т. н., доц. Куперштейн Л.М.

АНАЛІЗ АТАКИ ТИПУ ARP-SPOOFING

Вінницький національний технічний університет

Анатація *У проекті досліджена атака типу ARP-Spoofing, був проаналізований протокол arp і його вразливості, а також було проаналізовані методи виявлення та захист від цієї атаки.*

Ключові слова: *ARP-Spoofing, захист локальних мереж, ARP*

Abstract: *The project investigated the attack type ARP-Spoofing, arp protocol was reviewed and its vulnerability, and were analyzed by methods of detection and protection against this attack.*

Key words: *ARP-Spoofing, protection of local networks, ARP*

Актуальність. В сучасному світі з кожним днем збільшується використання комп'ютерів та комп'ютерних мереж. Все більш розповсюдженими є як мобільні пристрої – телефони та планшети. Всі ці пристрої підключені до локальної мережі. Однією з найбільш розповсюджених загроз локальних мереж є атака ARP-Spoofing [1].

Стан проблеми. При збройному пограбуванні банку втрати в середньому становлять 19 тисяч доларів, а при комп'ютерному злочині - вже 560 тисяч. За оцінкою американських фахівців, збитки від комп'ютерних злочинів протягом останніх десяти років щорічно збільшується в середньому на 35%. При цьому виявляється в середньому 1% комп'ютерних злочинів, а ймовірність того, що за розкритий комп'ютерне шахрайство злочинець потрапить до в'язниці, - не більше 10%. Дуже велика частина атак проводиться у локальних мережах, цей вид атак називається «людина посередині». Одним з видів такої атаки є ARP-Spoofing яка стала дуже поширена в наш час. В глобальній мережі інтернет є дуже велика кількість способів реалізації атаки ARP-Spoofing у відкритому доступі [2].

Сучасні системи виявлення атаки ARP-spoofing ще не досконалі і недостатньо ефективні з точки зору безпеки рішень. Тому методи роботи в цьому напрямку необхідні і актуальні.

Постановка задачі. Проаналізувати протокол ARP та визначити які вразливості він має. Проаналізувати методи атаки типу ARP-Spoofing та засоби захисту від неї.

Розв'язання задачі. ARP-spoofing (ARP - poisoning) - різновид мережевої атаки типу MITM що застосовується в мережах з використанням протоколу ARP, в основному атака застосовується в мережах Ethernet. Атака заснована на недоліках протоколу ARP.

Аналіз безпеки протоколу ARP показує, що, перехопивши на атакуючому вузлі усередині даного сегмента мережі широкомовний ARP-запит, можна послати помилковий запит - ARP-відповідь, в якому можливо оголосити себе потрібним вузлом (наприклад, маршрутизатором), і в подальшому активно контролювати мережевий трафік вузла, впливаючи.

Протокол ARP є абсолютно незахищеним. Він не володіє ніякими способами перевірки автентичності пакетів: як запитів, так і відповідей. Ситуація стає ще більш складною, коли може використовуватися мимовільний ARP [3].

Незважаючи на ефективність мимовільного ARP, він є особливо небезпечним, оскільки з його допомогою можна запевнити віддалений вузол в тому, що MAC-адресу будь-якої системи, що знаходиться з нею в одній мережі, змінився і вказати, яку адресу використовується тепер[3].

До виконання ARP-spoofing в ARP-таблиці вузлів A і B існують записи з IP- і MAC-адресами один одного. Обмін інформацією здійснюється безпосередньо між вузлами A і B.

В ході виконання ARP-spoofing'а комп'ютер C, виконує атаку, відправляє ARP-відповіді (без отримання запитів):

вузлу A: з IP-адресою вузла B і MAC-адресою вузла C;

вузлу B: з IP-адресою вузла A і MAC-адресою вузла C.

В силу того що комп'ютери підтримують мимовільний ARP (gratuitous ARP), вони модифікують власні ARP-таблиці і поміщають туди записи, де замість справжніх MAC-адрес комп'ютерів A і B варто MAC-адресу комп'ютера C.

Після того як атака виконана, коли комп'ютер А хоче передати пакет комп'ютера В, він знаходить в ARP-таблиці запис (вона відповідає комп'ютера С) і визначає з неї MAC-адресу одержувача. Відправлений у цій MAC-адресу пакет приходить комп'ютера С замість одержувача. Комп'ютер С потім ретранслює пакет того, кому він дійсно адресовано - тобто комп'ютера В [4].

Незважаючи на те що напади відбуваються на мережевому рівні, організація атаки не представляє проблем навіть для дилетантів: в Internet чимало програм такого призначення.

- ARPoison - додаток для командного рядка під UNIX. Воно дозволяє генерувати і пересилати підроблені відгуки ARP.

- dsniff - бібліотека інструментів для спуфинга ARP або DNS. Додатково вона допомагає проводити атаки Man in the Middle на сеанси HTTP.

- Ettercap можна назвати «швейцарським ножем» серед інструментів для прослуховування і спуфінга: поряд з наведеними функціями перерахованих програм це ПО успішно проводить атаки Man in the Middle на з'єднання SSH і HTTP [5].

Всі ці програми знаходяться у відкритому доступі, і використати їх може будь хто завгодно.

Методи для виявлення і запобігання ARP-Spoofing:

1) Організація VLAN. Якщо в локальній мережі є поділ на кілька VLAN, то атака ARP-spoofing може бути застосована тільки до комп'ютерів, які знаходяться в одному VLAN. Ідеальною ситуацією, з точки зору безпеки, є наявність тільки одного комп'ютера і інтерфейсу маршрутизатора в одному VLAN. Атака ARP-spoofing для такого сегмента неможлива.

2) Використання статичного ARP. Можна уникнути атаки ARP-spoofing шляхом настроювання ARP-таблиці вручну. Тоді зловмисник не зможе оновлювати ARP-таблиці шляхом посилки ARP-відповідей на інтерфейси комп'ютерів.

3) Використання шифрування. Для запобігання атаки ARP-spoofing (як і будь-якої атаки "людина посередині") в локальній мережі можна використовувати протоколи шифрування даних, для захисту переданої інформації від зловмисника. Наприклад такі протоколи як PPPoE або IPSec.

4) Виявлення атак за допомогою програмних засобів. Програмні засоби відстежують ARP активність на заданих інтерфейсів. Можуть виявити атаку ARP-spoofing, але не можуть запобігти її. Для запобігання атаки потрібне втручання адміністратора мережі, прикладами таких програм є програми arpwatch, BitCometAntiARP[6].

Висновки: В результаті аналізу був проаналізований протокол ARP, та було визначено що протокол є абсолютно незахищеним. Був проаналізований механізм за допомогою якого працює атака типу ARP-Spoofing. Також проаналізовані методи захисту від цієї атаки такі як: використання шифрування, статичний ARP та організація VLAN, та були знайдені програмні засоби які виявляють атаку. Так як програмні засоби можуть лише виявити атаку ARP то доцільно розробити програмний засіб який нейтралізує атаку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Разработка локальной сети и защита передачи данных на основе перспективных технологий [Електронний ресурс].– Режим доступу:URL: http://www.dissercat.com/ Назва з екрану.
2. Какими бывают компьютерные атаки [Електронний ресурс].– Режим доступу:URL: http://argon.pro/internet/attack Назва з екрану.
3. ARP-Spoofing [Електронний ресурс].– Режим доступу:URL: http://xgu.ru/wiki/ARP-spoofing Назва з екрану.
4. ARP-spoofing: старая песня на новый лад [Електронний ресурс].– Режим доступу:URL: http://www.securitylab.ru/contest/313500.php Назва з екрану.
5. Опасности спуфинга ARP [Електронний ресурс].– Режим доступу:URL: http://www.osp.ru/lan/2004/06/139202/Назва з екрану.
6. Защита WiFi-сети от ARP-спуффинга [Електронний ресурс].– Режим доступу:URL: http://bgbilling.ru/v6.1/doc/ch14s22s04.html Назва з екрану.

Алімов Роман.Андрійович, ВНТУ, ФІТКІ, група БС-12б, nemesis4m@mail.ru
Куперштейн Леонід Михайлович, к. т. н., доцент кафедри ЗІ, ВНТУ