УДК 004.056

АЛГОРИТМ ВИЯВЛЕННЯ MITM-АТАКИ ПІД ЧАС ARP-POISONING

Бурнашов С., Ящук В.
Львівський державний університет безпеки життєдіяльності, м. Львів

Розглянуто методи та способи деструктивного програмного впливу на інформаційні системи. Запропоновано алгоритм виявлення MITM (Man in the middle) атаки під час ARP-poisoning, який зчитує ARP таблицю та перевіряє чи є два або більше ідентичних MAC-адрес. У разі виявлення однакових MAC-адрес алгоритм інформує, від'єднує від мережі або блокує ті хости які мають однакову адресу в залежності де працює алгоритм на маршрутизаторі чи персональному комп'ютері.

Ключові слова: *MITM, Man in the middle, ARP-poisoning, ARP, MAC-адреса.*

The algorithm for detecting MITM (Man in the middle) an attack is considered, namely during ARP-poisoning. The algorithm reads the ARP table and checks if there is two or more identical MAC addresses. If identical MAC addresses are detected, the algorithm informs, disconnects from the network or blocks those hosts that have the same address, depending on where the algorithm works on the router or a personal computer.

Key words: *MITM, Man in the middle, ARP-poisoning, ARP, MAC- address.*

Сьогодні прискорення виробничих процесів, підвищення мобільності та оперативності доступу до інформації та послуг, можливість віддаленого управління банківськими рахунками, замовлення й оплати товарів і послуг – це низка очевидних переваг, що зумовлює значне зростання вартості інформації, що циркулює в комп'ютерних мережах. Забезпечення працездатності мереж, а також працездатності інформаційних систем, залежить не тільки від надійності використовуваної апаратури, але і від здатності мережі протистояти цілеспрямованим діям, які спрямовані на порушення її роботи.

Слід зазначити, що атаки на інформаційні системи з кожним роком стають усе досконалішими, масштабнішими та інтенсивнішими. Тому актуальною є проблема розроблення та вдосконалення систем виявлення вторгнень, головним завданням яких є саме виявлення мережевих атак, спроб несанкціонованого доступу та використання ресурсів мережі. Постійний стрімкий розвиток методів та способів деструктивного програмного впливу на інформаційні системи зумовлює необхідність виявлення атак та запобігання вторгненням з метою визначення найбільш ефективних механізмів захисту інформації.

Розглянемо метод компрометації каналу зв'язку, при якому зловмисник, приєднавшись до каналу між контрагентами, здійснює втручання в протокол

передачі, видаляючи або змінюючи інформацію. Такий вид атак має назву атака «людина посередині», MITM-атака (англ. Man in the middle).

Атака зазвичай починається з прослуховування каналу зв'язку та закінчується тим, що зловмисник намагається підмінити перехоплене повідомлення, витягти з нього корисну інформацію, перенаправити його на який-небудь зовнішній ресурс. Атаки «людина посередині» становлять загрозу для систем, що здійснюють фінансові операції через інтернет — наприклад, електронний бізнес, інтернет-банкінг, платіжний шлюз. Застосовуючи цей вид атаки, зловмисник може отримати доступ до облікового запису користувача та здійснювати різні фінансові махінації.

На рис. 1 наведено мережу для проведення MITM атаки та її виявлення, де ПК1 та ПК3 це користувачі, а ПК2 це комп'ютер зловмисника.

Маршрутизатор має IP-адресу 192.168.1.1 та MAC-адресу 00-00-00-00-00-AA

ПК1 має IP-адресу 192.168.1.2 та MAC-адресу 00-00-00-00-00-BB

ПК2 має IP-адресу 192.168.1.3 та MAC-адресу 00-00-00-00-00-CC

ПК3 має IP-адресу 192.168.1.4 та MAC-адресу 00-00-00-00-00-DD

Рис. 1. Мережа для проведення MITM атаки та її виявлення

Якщо зловмисник на ПК2 здійснить атаку на всі хости то ми побачимо змінену ARP-таблицю з MAC-адресою ПК2, а саме 00-00-00-00-00-CC. Наприклад користувач ПК1 бачитиме таку таблицю:

Interface: 192.168.1.2 – 0x8

192.168.1.1 00-00-00-00-00-CC

192.168.1.3 00-00-00-00-00-CC

192.168.1.4 00-00-00-00-00-CC

Якщо зловмисник на ПК2 здійснить атаку на ПК1 та маршрутизатор то MAC-адреси, для ПК1 матимуть вигляд:

Interface: 192.168.1.2 – 0x8

192.168.1.1 00-00-00-00-00-CC (змінена на MAC-адресу ПК2 зловмисника)

192.168.1.3 00-00-00-00-00-CC (MAC-адреса ПК2)

192.168.1.4 00-00-00-00-00-DD (не змінена)

MAC-адреси для ПК3 матимуть вигляд:

Interface: 192.168.1.4 – 0x8

192.168.1.1 00-00-00-00-00-CC(змінена на MAC-адресу ПК2 зловмисника)

192.168.1.2 00-00-00-00-00-CC(змінена на MAC-адресу ПК2 зловмисника)

192.168.1.3 00-00-00-00-00-CC(MAC-адреса ПК2)

Отже, під час ARP-poisoning атаки маємо 1 або більше збігів з MAC-адресою ПК2 зловмисника. Тому за допомогою методу перебору всіх MAC-адрес та порівняння їх між собою можемо визначити наявність MITM атаки, якщо під час перебору та порівняння маємо збіг 2 або більше MAC-адрес то атака існує.

Цей алгоритм можемо виконати будь-якою мовою програмування за такої послідовності: отримуємо ARP-таблицю; відфільтровуємо данні, та отримуємо тільки два параметри IP та MAC-адреса ПК в мережі; перебираємо та порівнюємо список ПК за їх MAC-адресою; якщо маємо збіг MAC-адрес, виводимо повідомлення з IP та MAC-адресою всіх ПК на які здійснена атака; сповіщаємо користувача, або передаємо IP-адресу для блокування на певний час у фаєрвол.

Література

1. Атака «людина посередині» [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%C2%AB%D0%BB%D1%8E%D0%B4%D0%B8%D0%BD%D0%B0_%D0%BF%D0%BE%D1%81%D0%B5%D1%80%D0%B5%D0%B4%D0%B8%D0%BD%D1%96%C2%BB

2. ARP [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/ARP

3. ARP spoofing [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/ARP_spoofing