УДК 004.056

Матусяк І.В., Козак Р.О.
*Тернопільський національний технічний університет імені Івана Пулюя*

# Види атак на протокол SSH

Одним з найпопулярніших криптографічних протоколів є SSH, що дає змогу виконувати віддалене управління операційною системою та тунелювання TCP-з'єднань. За функціональністю подібний до протоколів Telnet і rlogin, але, на відмінну від них, шифрує весь трафік, включаючи й паролі, які передаються. Саме тому протокол SSH завжди був і досі залишається об'єктом для атак.

Як відомо, якщо у SSH-сервер відкритий для доступу через Інтернет, а довжина даних авторизації є меншою, ніж 8 символів, то сервер практично буде «зламано» або буде «зламано» найближчим часом. При цьому неважливо, про який пристрій ідеться – нападники доказали свою здібність зламувати як iMac так і роутери Cisco.

*SSH Brute-force.* Однією з найпопулярніших атак є атака методом перебору паролів. Якщо запустити сервіс SSH, доступ до якого можливий з Інтернету, то в журналі автентифікації користувачів можна спостерігати багато записів невдалого підключення користувача admin/root, так начебто він постійно вводить невірний пароль. Саме так і виглядає атака методом перебору паролів, більш відома як brute-force. Найпростішим способом захисту може бути написання правила, що блокує весь доступ. Але це призведе до ряду проблем, першим з яких – як надати доступ до сервісу легітимним користувачам. Інший варіант – переведення роботи протоколу на інший порт. Статистика цього підходу показує, що зміна порта SSH на порт з верхнього діапазону, в значній мірі зменшує кількість спроб несанкціонованого доступу, але звичайно не виключає їх. Важливо відмітити, що той хто сканував порт 22 з таким же успіхом може знайти і порт 22222, на який, ймовірно, буде налаштовано роботу SSH. Однак це слугує одним із запобіжних заходів для досягнення успіху. Також бажано використовувати нетандартні ім'я користувача і паролі, щоб зменшити ефективність brute-force атаки.

Ще одним з способів для запобігання таких атак, можна відзначити написання правила доступу в між мережному екрані таким чином, щоб вони підтримували певні обмеження на можливості хостів, що підключаються. На всякий випадок рекомендується направляти порушників в таблицю адресів, для якої обмежений весь доступ або лише деякі види доступу. Також можна вказувати блокування всіх підключень від комп'ютерів, які перекрили свої ліміти. Ефект від написання цих додаткових правил буде доволі значущим. Після декількох спроб підбору пароля, адреса хоста, з якого здійснювалась атака, буде занесена в таблицю хостів з обмеженнями. А це значить, що всі його існуючі підключення відкидаються, а будь-які нові спроби з'єднання будуть заблоковані. Таким чином, можна створити адаптивний брандмауер, який автоматично налаштовується на умови потрібного середовища і самостійно реагує на небажану активність.

Однак вказані адаптивні правила діятимуть лише для захисту від традиційних і простих методів підбору паролів. Розподілені спроби підбору, які відбуваються з низькою інтенсивністю, не проявляли аналогічної активності та не будуть відповідати параметрам даних правил.

*MITM атаки.* Man in the Middle («Атака посередника» або «Людина посередині») – вид атаки, що ґрунтується на перенаправленні трафіка між двома комп'ютерами для перехоплення інформації, в подальшому її вивчення, знищення або модифікації, тобто порушення

цілісності та конфіденційності інформації. Атакуюча сторона отримує дані авторизації користувача і здійснює журналювання усього сеансу зв'язку, запуск команд та їх виконання.

Існує декілька ефективних засобів захисту від MITM-атак, але майже всі вони реалізуються в самому маршрутизаторі або на серверах, до яких звертається потенційна жертва. Одним із способів захисту від такої атаки є використання стійкого шифрування між клієнтом і сервером. В такому випадку сервер може ідентифікувати себе за допомогою представлення цифрового ключа, після чого між користувачем і сервером встановлюється шифрований канал для обміну конфіденційними даними. Ще одним варіантом захисту від деяких типів MITM-атака є повна відмова від використання відкритих Wi-Fi мереж для роботи. Також для захисту від деяких MITM-атак можна використовувати режим автентифікації відкритим ключем, тому як цей спосіб не схильний до атаки і гарантує безпечне підключення до сервера. І звичайно ж уважніше відноситися до попередження про зміну відбитку ключів.

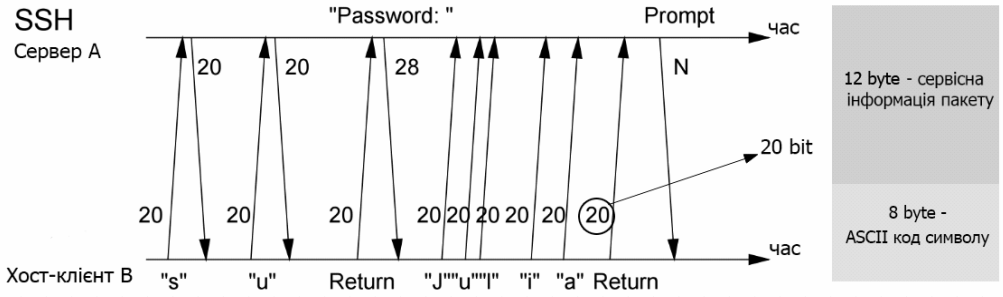


*Рис. 1. Сигнатура трафіку під час введення пароля користувачем SU*

*Timing attack.* Атака по часу представляє собою атаку стороннім каналом, в якій нападник загрожує криптосистемі, аналізуючи час, потрібний для виконання різних операцій. Кожна дія на комп'ютері вимагає певного часу, і цей час може різнитися залежно від даних на вході. У випадку атаки по часу на SSH зловмисник може дізнатися коли користувач вводить дані авторизації і перехопити їх. На рис. 1 зображено, що після натискання клавіші виконується певна операція відправлення символу на SSH сервер.

В даному випадку зловмисник може переглянути коли користувач використовував команду "su" яка виглядає як два 20 бітові пакети після яких слідує пакет "Password:" розміром 28 біт, всі наступні пакети до пакету "Prompt" є символами паролю, діставши які зловмисник може отримати доступ до серверу.

Незважаючи на механізми шифрування та автентифікації, які використовує протокол SSH, він має дві слабкості, які уможливлюють атаки по часу: по-перше, передані пакети обмежені лише восьми байтами (у випадку блокового шифру), який показує приблизний розмір вихідних даних. По-друге, в інтерактивному режимі, кожне натискання клавіші, яке користувач відправляє на віддалену машину, надсилається в окремому IP-пакеті відразу після того, як натиснута кнопка, що розкриває інформацію про часові інтервали між натискання різних клавіш.

**Список використаних джерел**

1. *Перенаправление SSH и HTTP трафика. : [Електронний ресурс]. – Режим доступу: https:// xakep.ru/ 2005/10/26/28514/.*
2. *Preventing Brute Force SSH Attacks. : [Електронний ресурс]. – Режим доступу: https://rimuhosting.com/knowledgebase/linux/misc/preventing-brute-force-ssh-attacks.*
3. *Четыре шага в защите SSH. : [Електронний ресурс]. – Режим доступу: https://xakep.ru/2006/11/20/35288/*
4. *Timing Analysis of Keystr ok es and Timing Attacks on SSH. : [Електронний ресурс]. – Режим доступу: https://people.eecs.berkeley.edu/~daw/papers/ssh-use01.pdf.*
5. *MiTM атака на SSH. : [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/176693/.*
6. *Атака на SSH методом подбора паролей (SSH Brute-Force). : [Електронний ресурс]. – Режим доступу: http://system-repair.net/2012/08/ataka-na-ssh-metodom-podbora-parolej-ssh-brute-force/.*
7. *Перенаправление SSH и HTTP трафика. : [Електронний ресурс]. – Режим доступу: https:// xakep.ru/ 2005/10/26/28514/.*