УДК 004.056

О. В. Костюк
І. О. Дьогтєва

ОСОБЛИВОСТІ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ АВТОРИЗАЦІЇ SSH-ТУНЕЛЮ ДО СЕРВЕРНОЇ ЧАСТИНИ НА ОСНОВІ ЗАХИСТУ ВІД BRUTE-FORCE АТАК

Вінницький національний технічний університет

Анотація

Робота присвячена опису підвищення захищеності авторизації SSH-тунелю до серверної частини на основі захисту від атак типу Brute-force, в контексті попередження появи загроз, втрати або знищення інформації.

Ключові слова: цифрова безпека, SSH, Brute-force атака, підвищення захищеності з'єднання.

Abstract

The paper is devoted to the description of increasing the security of SSH-tunnel authorization to the server part based on protection against Brute-force attacks, in the context of preventing threats, loss or destruction of information.

.**Keywords**: digital security, SSH, Brute-force attack, increase the security of the connection.

Вступ

У сучасних реаліях структура економічної теорії портфеля ресурсів, які природньо використовуються економічними організаціями для реалізації безпосередньої діяльності та досягнення поставлених цілей, зазнає змін через збільшення питомої ваги ресурсів, що мають інформаційну природу. У довгостроковій перспективі інформація дозволяє бізнесу, насамперед, зміцнювати свою конкурентоспроможність. Функціонуючи в умовах інформаційної мережі (процеси створення масивів інформації, їх циркуляції), актуалізується питання щодо удосконалення процесу та розробки дієвих методик забезпечення стійкості та захищеності доступу до інформаційних ресурсів, засобів, що забезпечують властивості цілісності, конфіденційності та доступності інформації за умов впливу на неї загроз [1].

Результати дослідження

Брутфорс один з найпопулярніших методів підбору логіну/паролю до облікового запису чи сервісу. Термін утворений від англомовного словосполучення "brute force" та в перекладі в перекладі означає "груба сила", або повний перебір. Зазвичай використовується в контексті хакерських атак, хоча атаку такого характеру визначають криптоаналітичною, яку можуть використовуватися для спроби розшифрувати зашифровані дані. Серед найбільш вразливих середовищ виділяють онлайн-банкінги та платіжні системи.

Суть підходу полягає у послідовному автоматизованому переборі всіх можливих комбінацій символів через генерацію варіантів паролів, їх відповідної перевірки з метою підбору правильного паролю. З цієї точки зору пошук пароля лежить в площині математичного завдання, розв'язання якого реалізується за досить великої кількості спроб, причому за статистикою збільшення довжини пароля призводить в середньому до зростання в геометричній прогресії кількості часу на пошук правильного пароля [2].

На даний момент в мережі пропонується ряд продуктів брутфорс для злому веб-сайту, Bruteforce Wi-Fi, тощо. Варто зазначити, що переважна більшість подібних програм не є результативними, хоча загалом вирішити завдання в такий спосіб можна практично завжди, також тимчасові витрати на пошуки не завжди виправдовують мету, враховуючи широке поле пошуку рішень.

В класичному розумінні тунель через SSH передбачає створення середовища для шифрування даних, які проходять по конкретному каналу (тунелю). В процесі дані шифруються на одному кінці з'єднання, і дешифруються на іншому, що убезпечує використання таких даних в разі перехоплення їх третіми особами.

Створення тунелю SSH більше нагадує активацію порту через протокол, ніж безпосередню форму тунелювання, причому тунелі SSH потрібно щоразу налаштовувати вручну.

Загалом створення такого середовища (тунелю), може проводитися за кількома сценаріями [3]:

- використання спеціальних програм, які працюють через SSH;
- socks-проксі;
- варіант налаштування з'єднання на потрібний TCP-порт (за необхідності працювати з певним сервером);
- VPN-тунель (даний спосіб можна використовувати для будь-яких додатків).

Основна відмінність тунелів SSH від їх аналогів VPN полягає в тому, що інформація не переміщується в жодному напрямку. Цей канал зв'язку має точку входу, яка має справу виключно з пакетами TCP. В цілому, обидва варіанти покликані забезпечити надійне шифрування та захист даних.

При використанні SSH-тунелювання, виділяється декілька практичних прикладів його застосування [4]:

1. Перекидання (перенаправлення) портів (Port Forwarding). Для цього в локальній системі відкривається порт, а для створення каналу зв'язку користувач повинен вибрати порт на іншому кінці тунелю.
2. Автоматизація копіювання публічного (відкритого) ключа.
3. Зворотний SSH-тунель (SSH reverse tunnel). Для цього достатньо підключити активний порт, до іншого локального порту.
4. Віддалене виконання команд за допомогою SSH.
5. Копіювання, функція rsync-копіювання (rsync через SSH).
6. GUI-програми: віддалений запуск через SSH. Незважаючи на те, що GUI виконується на віддаленому сервері, вікно відображається на локальному робочому столі.
7. Редагування файлів й копіювання їх в задану директорію.
8. "Стрибки по хостам". Тунелювання передбачає перехід через кілька хостів, якщо користувачеві доводиться працювати із сегментацією мережі.
9. Фільтрування трафіку за допомогою iptables. Для встановлення зв'язку з цільовим сервером утиліта порівняє IP-адресу ініціатора підключення з тим списком, який відображний в правилах INPUT, а потім надає доступ до сервера, або забороняє його.

Недолік SSH-тунелювання полягає в тому, що будь-який користувач, який може увійти на сервер, має право включити переадресацію портів. Це широко використовується внутрішніми IT-фахівцями для входу в свої домашні машини або сервери у хмарі, пересилання порту з сервера назад в корпоративну мережу на робочий комп'ютер або відповідний сервер [5].

Висновок

Використання мережевого протоколу SSH є відносно ефективним способом захисту каналів даних. Головна перевага полягає у використанні відкритих і закритих ключів при підключенні клієнтів до сервера, що мінімізує можливість підключення третіх осіб до вашого каналу. На сьогоднішній день використання мережевого протоколу SSH добре підтримується багатьма операційними системами як для клієнта, так і для сервера.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Проблеми кібербезпеки [Електронний ресурс]. – Режим доступу: http://fit.univ.kiev.ua/wp-content/uploads/2016/03/Збірник-матеріалів-конференції.pdf. (дата звернення: 05.04.2022). — Назва з екрана.

2. Brute Force атаки [Електронний ресурс]. – Режим доступу: https://www.anti-malware.ru/threats/brute-force. (дата звернення: 05.04.2022). — Назва з екрана.

3. Протокол SSH (Secure Shell) [Електронний ресурс]. – Режим доступу: https://hostingfanatic.com/uk/protokol-ssh-secure-shell-shho-cze-take-yaki-potribni-nalashtuvannya-dlya-roboti/#__SSH-2. (дата звернення: 05.04.2022). — Назва з екрана.

4. SSH-тунелі: практичні приклади та основні функції [Електронний ресурс]. – Режим доступу: https://cloud.timeweb.com/blog/ssh-tunnels. (дата звернення: 05.04.2022). — Назва з екрана.

5. SSH-тунелювання [Електронний ресурс]. – Режим доступу: https://4systems.ru/inf/ssh-tunnel-kak-polzovatsja/. (дата звернення: 05.04.2022). — Назва з екрана.

Костюк Олег Віталійович *– студент факультету менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: oleg.kostuik14@gmail.com.*

Дьогтєва Ірина Оксентіївна — *асистент кафедри менеджменту та безпеки інформаційних систем, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця.*

Kostiuk Oleh Vitaliyovych *- student of the Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: oleg.kostuik14@gmail.com.*

Dohtieva Iryna — *Assistant of the Department of Management and Security of Information Systems, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia.*