УДК 004.492

РИЗИКИ ВИКОРИСТАННЯ SSH ТА МЕТОДИ ЇХ УСУНЕННЯ

Д. Ю. Андреєв[1,a], С. А. Смирнов[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

В даній роботі розглянуто використання протоколу SSH в комп'ютерних мережах організацій з точки зору безпеки. Приділено увагу як організаційним проблемам, таким як `key sprawl`, так і технічним–налаштуванню серверів та тунелюванню зловмисного трафіку.

Окремий розділ присвячено аналізу нещодавно знайдених та доданих у базу `CVE` вразливостей–`Terrapin Attack` та вразливості алгоритму створення цифрового підпису у певних версіях `PuTTY` (`CVE-2024-31497`).

Ключові слова: SSH, ключ, сервер, тунелювання, `key sprawl`, `terrapin attack`

Вступ

На сьогоднішній день SSH є одним із найпоширеніших засобів віддаленого доступу. Встановлюючи захищений канал зв'язку між двома системами, цей протокол дозволяє безпечно обмінюватися даними, виконувати адміністрування або навіть тунелювати роботу інших протоколів у мережі. Безпека цього протоколу головним чином спирається на застосування асиметричних криптографічних механізмів для обміну ключами та симетричних для передачі даних [1].

1. Аналіз ризиків при використанні SSH

1.1. Організаційні ризики

Численні атаки на SSH виявляються успішними через неправильне управління ключами, слабкі паролі, використання застарілого програмного забезпечення тощо. Помилки організаційного характеру, що можуть призвести до компрометації SSH серверів [2]:

1. `Key sprawl`. Вхід на SSH сервер можливо виконувати без пароля, згенерувавши публічний ключ та передавши його на сервер. При цьому, термін дії такого ключа необмежений і неможливо відстежити, скільки дійсних ключів взагалі існує.
2. Використання засобів віртуалізації. Часто SSH сервери клонують, використовуючи засоби оркестрації, не генеруючи нових ключів, що може призвести до компрометації.
3. Використання застарілого ПЗ та алгоритмів. Якщо в компанії відсутні політики щодо оновлення програмного забезпечення або використовується застаріле обладнання, її інформаційна система стає більш вразливою [3].

1.2. Технічні проблеми

З технічної точки зору, головною причиною компрометації SSH серверів часто стає неправильна конфігурація. Можливі проблеми при використанні SSH [4]:

1. Неправильні налаштування. Увімкнення або вимкнення деяких параметрів сервера може призвести до зниження рівня захищеності. Небезпеку можуть також становити слабкі криптографічні алгоритми, такі як DES або MD5.
2. Обхід фаєрволів. Весь трафік що проходить по SSH, тунелюється, тобто його неможливо прочитати ззовні.
3. Поширення через довірені відносини між SSH серверами. Компрометація одного сервера може дозволити зловмиснику швидко отримати доступ до інших.
4. `Man-in-the-middle`. При атаці типу «Людина посередині» зловмисник може втрутитися в процес встановлення з'єднання між сутностями та отримати доступ до каналу комунікації, перехоплювати чутливу інформацію [5, стор. 101].

1.3. Аналіз реальних вразливостей

Для наочності проаналізуємо декілька вразливостей, пов'язаних з SSH, що були занесені до бази даних CVE:

1. CVE-2023-48795 (`Terrapin Attack`) [6]. Одна із відносно нещодавно знайдених вразливостей була опублікована у CVE в грудні 2023 року. Атака працює лише для шифру `ChaCha20-Poly1305` або іншого з режимом ланцюга блоків (`CBC`) та `Encrypt-then-MAC`, проте згідно з [6], 77% серверів підтримують цей шифр та 57% вказують його як той, якому надається перевага. Зловмисник атакує `BPP` (`Binary Packet Protocol`) і усікає префікс, що дозволяє прибрати повідомлення `EXT_INFO`, яке відповідає за узгодження

[a]dandre-ipt24@lll.kpi.ua

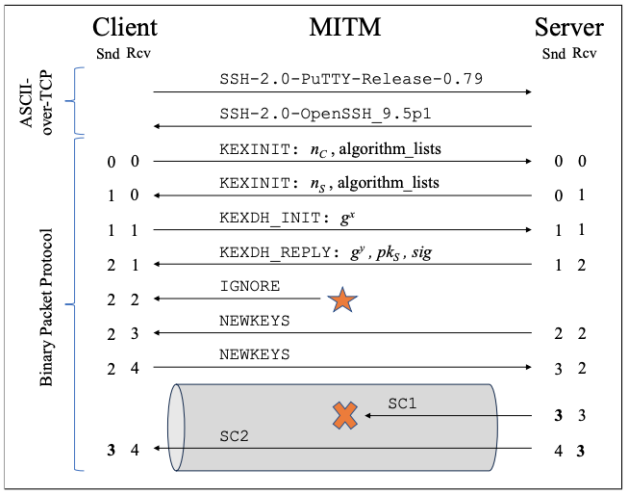

Рис. 1. Схема SSH `handshake` при `Terrapin attack`

розширень протоколу непомітно для сторін. Це знижує рівень безпеки протоколу та відкриває можливості для подальших зловмисних дій.

2. CVE-2024-31497 [7]. Дана вразливість була знайдена в `PuTTY` (реалізації SSH клієнта для Windows) версій 0.68-0.80. Вразливість актуальна лише для ключів типу `521-bit ECDSA`. Усі схеми підпису DSA вимагають випадкового значення під час підписання, яке позначають буквою `k`. Якщо зловмисник зможе вгадати значення `k`, яке було використано, або знайти будь-які два підписи, які згенеровано з тим самим `k`, то він зможе негайно відновити закритий ключ.

2. Усунення проблем з SSH

2.1. Рекомендації щодо роботи з SSH в корпоративних мережах

Щоб створити умови для безпечного використання SSH в організації та знизити потенційні ризики до прийнятного рівня, необхідно застосовувати ряд організаційних заходів та інструментів контролю. Рекомендації щодо використання SSH в мережах організацій [2]:

1. Впровадження системи контролю ключів. Використання спеціального програмного забезпечення для управління SSH ключами дозволяє значно знизити ймовірність витоку секретних ключів та компрометації серверів [2].
2. Моніторинг активності. Активний моніторинг логів SSH серверів значно підвищує рівень безпеки та швидкість реагування на інциденти, пов'язані з протоколом. Досвідчений системний адміністратор може швидко виявляти `brute-force` атаки або атаки типу `man-in-the-middle`.

2.2. Безпечна конфігурація SSH

Існує велика кількість способів, які можуть підвищити рівень безпеки SSH серверів. Вони включають як налаштування самого сервера, так й інші технічні заходи. Загальні рекомендації щодо впровадження та конфігурації SSH [8]:

1. Вимкнути автентифікацію за паролем. Використання лише автентифікації за ключем повністю виключає можливість атаки методом підбору паролів.
2. Відключення `root` користувача. Варто відключити можливість автентифікації `root` користувача на сервері та створити нових користувачів з підходящими повноваженнями.
3. Перенесення сервера на інший порт. Зміна порту SSH сервера з 22 на інший менш популярний дозволяє уникнути мережних сканувань, а також атак `script-kids`.
4. Резервне копіювання файла конфігурації. Перед внесенням значних змін до файлу конфігурації, необхідно робити його резервну копію (файл `ssh_config`).

Висновки

Сьогодні протокол SSH широко використовується для організації віддаленого доступу. Проте незважаючи на доволі високий рівень захищеності, сервери часто можуть піддаватись атакам та мережному скануванню. Застосовуючи запропоновані організаційно-технічні заходи та рекомендації, можна запобігти багатьом типам атак та знизити ризики до прийнятного рівня. Важливо впроваджувати всі заходи комплексно та системно, у тісній взаємодії один з одним, тому що немає сенсу забороняти використовувати паролі, якщо в організації велика кількість неконтрольованих SSH ключів, що схильні до витоку.

Перелік використаних джерел

1. *Lucas M.* SSH Mastery. — 2-е вид. — Tilted Windmill Press, 06.02.2018. — 242 с. — ISBN 9781642350029.
2. *Miller M.* SSH Key Management Overview & 10 Best Practices. — 22.11.2022.
3. *Robert A.* Mistakes to Learn From: Common SSH Misconfigurations for Technology Security Managers. — 10.01.2021.
4. *Bhagwat R.* A Research on Secure Shell (SSH) Protocol // International Journal of Advanced Research in Science, Communication and Technology (IJARSCT). — 2020. — 10 вер.
5. *Barrett D., Silverman R., Byrnes R.* SSH, The Secure Shell: The Definitive Guide. — 2-е вид. — O'Reilly Media, Inc., 14.06.2005. — 564 с. — ISBN 9780596008956.
6. *Bäumer F.* Terrapin Attack: Breaking SSH Channel Integrity By Sequence Number Manipulation. — 19.12.2023.
7. *Bäumer F.* Mitre CVE-2024-31497. — 2024.
8. *Garn D.* Eight ways to protect SSH access on your system. — 29.10.2020.