УДК 004.7

Качур В.В., здобувач,
Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ TELNET ТА SSH ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ МЕРЕЖЕВОГО ОБЛАДНАННЯ

У процесі експлуатації сучасних комп'ютерних мереж критично важливим аспектом є можливість віддаленого керування мережевим обладнанням – маршрутизаторами, комутаторами та серверами. У сучасних комп’ютерних мережах питання безпечного віддаленого адміністрування є одним із ключових для підтримання стабільної та захищеної роботи інфраструктури. Для віддаленого доступу до мережевого обладнання застосовуються різні протоколи, серед яких найбільш поширеними є Telnet та SSH. Незважаючи на схожість функціональних можливостей, їх рівень безпеки суттєво відрізняється.

Telnet (Telecommunication Network) – це один із найстаріших мережевих протоколів, розроблений у 1969 році для віддаленого доступу до комп'ютерних систем. Протокол працює на прикладному рівні моделі OSI та використовує TCP-з'єднання через порт 23. Основним недоліком Telnet є передача всіх даних, включаючи облікові дані користувача, у відкритому вигляді без будь-якого шифрування. Це робить протокол вразливим до атак типу «людина посередині» та перехоплення трафіку, що створює серйозні ризики для безпеки мережі.

SSH (Secure Shell) – це криптографічний мережевий протокол, розроблений у 1995 році як безпечна альтернатива Telnet. SSH забезпечує шифрування всього трафіку між клієнтом і сервером, використовуючи асиметричну криптографію для автентифікації та симетричну криптографію для передачі даних. Протокол працює через порт 22 і підтримує різні методи автентифікації, включаючи парольну автентифікацію та автентифікацію на основі ключів.

Основні переваги SSH над Telnet включають:

1. шифрування всіх даних, що передаються;
2. захист від атак перехоплення та підміни даних;
3. підтримку тунелювання та переадресації портів;
4. можливість передачі файлів через безпечний канал;
5. гнучкі механізми автентифікації.

SSH використовує тришарову архітектуру безпеки: транспортний рівень забезпечує шифрування та цілісність даних, рівень автентифікації підтверджує особу користувача, а рівень з'єднання

мультиплексує кілька логічних каналів через одне захищене з'єднання. Сучасні версії SSH підтримують алгоритми шифрування AES, ChaCha20 та інші, що забезпечують високий рівень криптографічної стійкості.

Telnet продовжує використовуватися лише в ізольованих мережах або для застарілого обладнання, яке не підтримує SSH. Однак навіть у таких випадках рекомендується розглянути можливість оновлення обладнання або використання додаткових засобів захисту, таких як VPN-тунелі.

Порівняльний аналіз продуктивності показує, що додаткові обчислювальні витрати на шифрування в SSH є мінімальними на сучасному обладнанні і цілком виправдані з точки зору забезпечення безпеки. Затримка, викликана процесами шифрування та дешифрування, становить лише кілька мілісекунд і не впливає на ефективність адміністративних операцій.

Порівняння цих протоколів показує, що SSH має суттєві переваги над Telnet за всіма ключовими показниками безпеки. Хоча Telnet може використовуватися в закритих або тестових середовищах, у виробничих мережах застосування цього протоколу недоцільне. SSH, у свою чергу, забезпечує високий рівень захисту і відповідає сучасним вимогам кібербезпеки.

Таким чином, хоча обидва протоколи виконують функцію надання віддаленого доступу, з точки зору інформаційної безпеки вони не є рівнозначними. Використання Telnet у виробничому середовищі створює неприйнятні ризики для безпеки і суперечить сучасним практикам кібербезпеки. Telnet є застарілим протоколом, який не відповідає сучасним вимогам захисту інформації. SSH є галузевим стандартом для адміністрування, оскільки забезпечує комплексний захист від прослуховування, підміни даних та несанкціонованого доступу. Повний перехід на SSH є обов’язковим кроком для забезпечення кіберстійкості будь-якої організації.

Список використаних джерел:

1. William S. Data and Computer Communications. Pearson, 2013. 912 p.

2. Ylonen T., Lonvick C. The Secure Shell (SSH) Protocol Architecture. IETF RFC 4251, 2006.