УДК 004.73

КАЛАНЧА Андрій Андрійович,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ;

ОНИЩЕНКО Юрій Миколайович,
кандидат наук з державного управління, доцент,
доцент кафедри кібербезпеки та DATA-технологій факультету № 6
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7755-3071

ОСОБЛИВОСТІ ТЕСТУВАННЯ НА ВРАЗЛИВІСТЬ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ СТАНДАРТУ 5G

Мережа 5G – це перспективна технологія, що дозволяє підвищити швидкість передачі даних, зменшити затримки та забезпечити підтримку великої кількості пристроїв, що підключені до мережі. Перші комерційні мережі 5G були запущені в 2019 році в США та Південній Кореї, а за даними GSMA Intelligence, кількість підключень до мереж 5G у світі досягла 1,3 млрд у кінці 2020 року [1].

Перед тим, як перейти до опису технологій тестування на вразливість мережі 5G, варто розглянути різницю між 4G та 5G технологіями, а також загальні методи та засоби пентестингу стільникових мереж.

5G мережі характеризуються більш розподіленою структурою, яка включає велику кількість різноманітних пристроїв та систем, що взаємодіють один з одним. На відміну від 4G, 5G мережі використовують низку новаторських технологій, таких як Massive MIMO, Beamforming, Network Slicing та інші. Із зростанням швидкості передачі даних в 5G мережах відкривається більше можливостей для атак, а також ускладнюється процес виявлення аномалій та атак. Крім того, 5G мережі розроблені для підтримки великої кількості пристроїв IoT (Internet of Things) та M2M (Machine-to-Machine), що спричиняє появу різноманітних атак, спрямованих на ці пристрої. Тому аудиторам стільникових мереж слід зосереджуватися на безпеці цих пристроїв та їх взаємодії з мережею, оскільки вони можуть стати потенційними уразливими точками [2].

Для аудиту систем безпеки мереж використовуються різні методи та засоби.

– Scanning (сканування) – процес виявлення активних пристроїв та послуг у мережі. Для сканування мережі можна використовувати різні інструменти, наприклад, Nmap, Netcat, Wireshark тощо.

– Enumeration (перерахування) – процес збору детальної інформації про пристрої та послуги, які працюють у мережі. Цей процес дозволяє виявити можливі вразливості та ризики.

– Exploitation (експлуатація) – процес використання виявлених вразливостей для отримання доступу до системи або даних. Для експлуатації вразливостей можна використовувати різні інструменти, наприклад, Metasploit, SET, Armitage тощо.

– Post-Exploitation (післяексплуатація) – процес забезпечення довготривалого доступу до системи або даних після успішної експлуатації вразливостей [3].

Нижче варто розглянути деякі з технологій аудиту безпеки мережі 5G:

– виявлення вразливостей мережі з використанням програмно-визначеного радіо (Software-Defined Radio, SDR). SDR дозволяє фахівцям у цій сфері аналізувати

радіохвилі, що використовуються в мережі, та виявляти можливі вразливості. Це дає можливість проводити аналіз зовнішнього середовища та знаходити вразливі точки входу [4];

– використання інструментів аудиту на вразливість на основі імітації та емуляції мережі. До таких інструментів належать, наприклад, OpenAirInterface та 5G-EmPOWER, які дозволяють моделювати різні сценарії роботи мережі та виявляти можливі вразливості [5];

– використання методів, що базуються на аналізі трафіку мережі. Такі методи включають в себе аналіз пакетів мережі та перехоплення радіосигналів, що використовуються в мережі.

Одним із головних ризиків, що пов'язані з мережею 5G, є підвищена кількість точок доступу до мережі, що збільшує загрозу з боку зловмисників. Крім того, збільшена пропускна здатність мережі може призвести до збільшення кількості атак на мережу, оскільки зловмисники можуть використовувати мережу для розповсюдження шкідливого коду або здійснювати атаки на інші пристрої, що підключені до мережі.

З іншого боку, мережа 5G також має більше можливостей для захисту, в порівнянні з попередніми версіями мереж. Наприклад, мережа 5G має вбудовані функції безпеки, які дозволяють виявляти та блокувати атаки на мережу [6]. Крім того, в 5G мережі використовується новий протокол мережевого рівня – IPv6, який містить додаткові механізми безпеки.

Мережа 5G є майбутнім стандартом зв'язку та має більше можливостей для захисту, в порівнянні з попередніми версіями мереж. Однак, збільшена кількість точок доступу до мережі та збільшена пропускна здатність можуть призвести до збільшення кількості атак на мережу. Тому, для ефективного захисту мережі 5G від зловмисників, необхідно використовувати сучасні технології тестування безпеки, які дозволяють виявляти та блокувати можливі вразливості мережі.

Список використаних джерел

1. Кількість 5G-підключень у всьому світі зростає швидше прогнозів. Компанія DEPS. URL: https://deps.ua/ua/news/novosti-rynka/8209.html (дата звернення: 28.03.2023).

2. Michaela Goss. 5G vs. 4G: Learn the key differences between them URL: https://www.techtarget.com/searchnetworking/feature/A-deep-dive-into-the-differences-between-4G-and-5G-networks (дата звернення: 28.03.2023).

3. Post-Exploitation Tools for Your Next Penetration Test. Bishop Fox. URL: https://bishopfox.com/blog/post-exploitation-tools-for-pen-test (дата звернення: 28.03.2023).

4. DmitrySpb79. Software Defined Radio – Як це працює? URL: https://habr.com/ru/post/451674/ (дата звернення: 28.03.2023).

5. Кайденко М., Шрамко Д., Побудова мобільної проміжної станції зв'язку для важкодоступної місцевості на базі SDR. URL: http://tk-its.kpi.ua/uk/node/281 (дата звернення: 28.03.2023).

6. Що таке 5G? – AWS. Amazon Web Services, Inc. URL: https://aws.amazon.com/ru/what-is/5g/ (дата звернення: 28.03.2023).

Одержано 03.05.2023