УДК 004.056

Микита ОНИЩЕНКО, Андрій ТИМЧАК, Геннадій ПОНЕДЄЛЬНІКОВ

Західноукраїнський національний університет

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІБЕРФІЗИЧНИХ СИСТЕМ ЗА ДОПОМОГОЮ МОНІТОРИНГУ

Вступ. Аналіз і моніторинг трафіку є важливим елементом для розуміння та оптимізації роботи кіберфізичних систем. Вони сприяють виявленню залежностей, підвищенню ефективності та забезпеченню загальної надійності системи.

Програмні засоби захисту КФС та антивірусні рішення також активно застосовують технології моніторингу для виявлення потенційно шкідливих дій. Для перехоплення й запису мережевого трафіку, що проходить через мережеві інтерфейси, використовуються спеціалізовані програми, відомі як сніфери (packet sniffers) [1].

Перехоплені дані містять інформацію про передачу пакетів, включаючи їхнє джерело, місце призначення, протоколи, порти та вміст. Завдяки моніторингу система постійно відстежує всі дії та негайно сповіщає користувачів про можливі загрози, що значно знижує ймовірність проникнення зловмисників у систему та реалізації подальших етапів кібератаки.

Мета: дослідження існуючих методів та способів захисту інформації в кіберфізичних системах шляхом моніторингу.

1. Аналіз і моніторинг трафіку в кіберфізичних системах

Моніторинг і аналіз мережевого трафіку в кіберфізичних системах можна умовно поділити на дві основні категорії: пасивний та інтерактивний.

Пасивний моніторинг передбачає налаштування мережі за допомогою дзеркалювання або використання моніторингового порту для створення копій мережевих пакетів, що передаються між пристроями. Зібрані дані направляються на локальний або хмарний сервер, де за допомогою глибокої перевірки пакетів (DPI) аналізується їхній вміст, визначаються джерело, протоколи, порти, модель пристрою, операційна система тощо.

Однак цей метод має обмеження. Наприклад, він неефективний для пристроїв, які генерують трафік лише у разі відмови або працюють зі специфічними протоколами. Зокрема, протокол Modbus, часто застосовуваний у системах BMS, надає мінімум інформації про пристрої, що ускладнює їхню ідентифікацію, наприклад визначення виробника або версії мікропрограми.

Для підвищення рівня безпеки часто використовують медові пастки (honeypots), які імітують вразливі системи (рисунок 1). Їх мета - привернути увагу зловмисників, допомогти ідентифікувати підозрілий трафік та відвернути атаки від реальних систем.

Розробка програмного забезпечення для ефективного моніторингу та аналізу мережевого трафіку є одним із шляхів вирішення цих проблем. Такі програми здатні захоплювати, структурувати та аналізувати дані, що проходять через мережу.

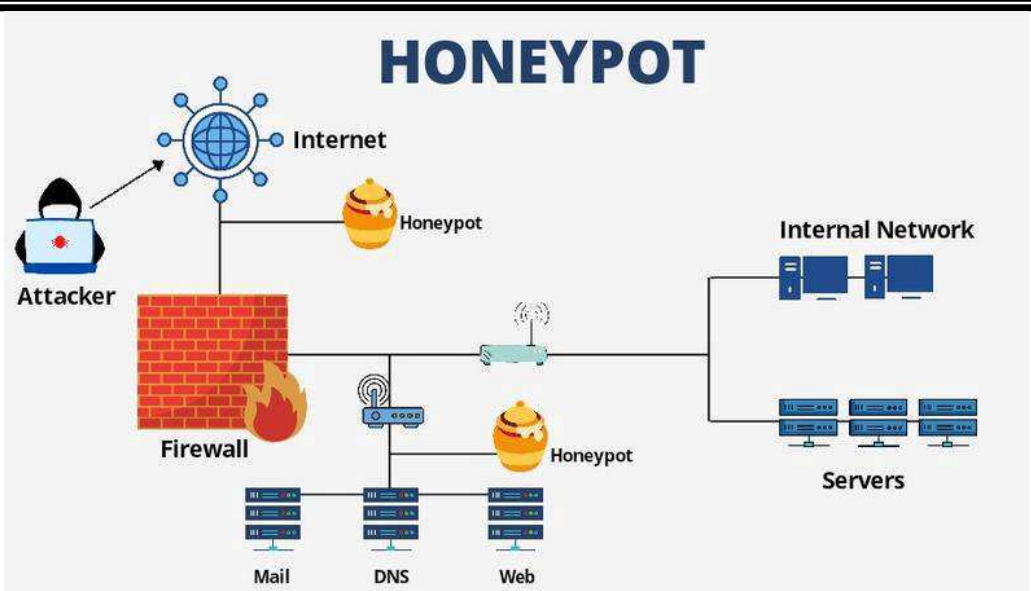

Рисунок 1 - Honeypots

Одним із ключових інструментів у цьому процесі є сніффери пакетів (packet sniffers), або аналізатори мережі [2].

Вони здійснюють атаки з перехопленням пакетів. Атака з перехопленням пакетів (або просто атака з перехопленням) - це мережева загроза, коли зловмисник захоплює мережеві пакети з наміром перехопити або викрасти трафік даних, який, можливо, залишився незашифрованим. Пакети даних збираються, коли вони проходять через комп'ютерну мережу.

Перехоплені пристрої або медіа, які використовуються для здійснення цієї атаки та збору пакетів мережевих даних, називаються перехоплювачами пакетів [3].

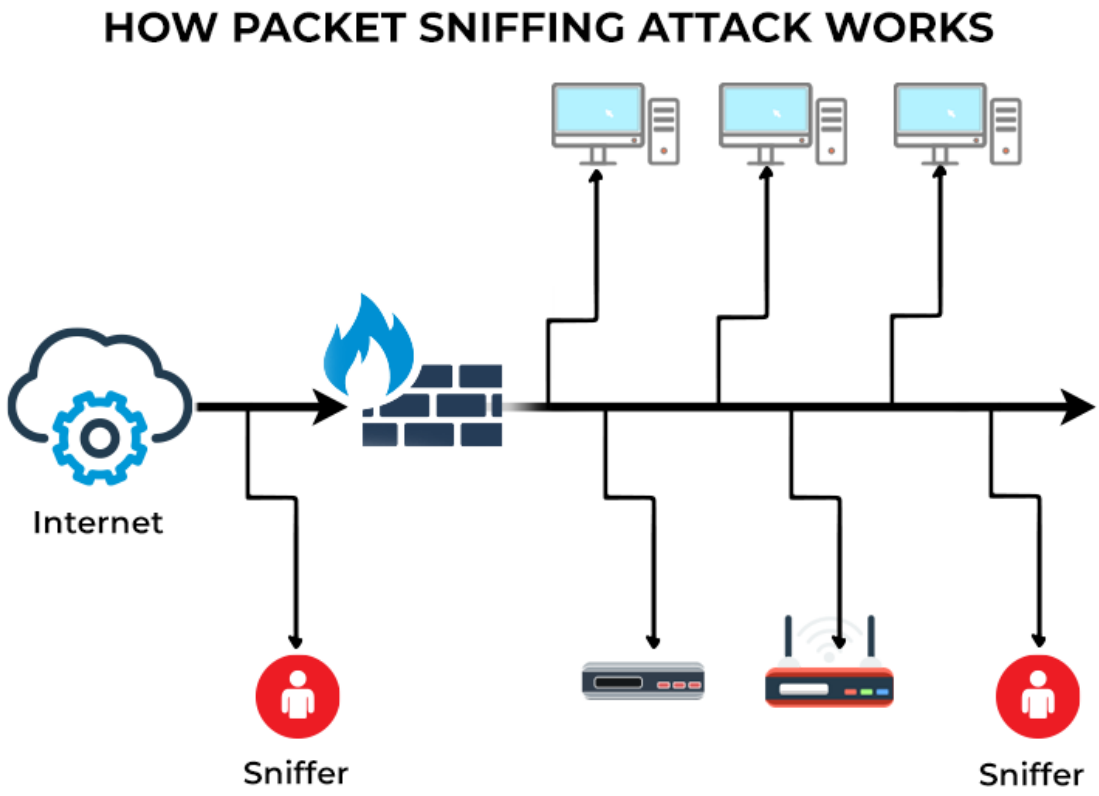

Рисунок 2 - Принцип роботи сніфера пакетів

Сніффери широко використовуються для:

- моніторингу та фільтрації мережевого трафіку,
- діагностики мережевих проблем,
- виявлення некоректних налаштувань,
- аналізу та усунення несправностей у роботі протоколів.

Окрім того, ці інструменти відіграють важливу роль у виявленні підозрілої діяльності в мережі та реагуванні на кіберзагрози [4]. У системах моніторингу вторгнень сніффери допомагають ідентифікувати шкідливу активність ще на етапі її прояву, що підвищує ефективність захисту мережевих інфраструктур.

Одним із таких інструментів є Wireshark [5]. Цей інструмент для аналізу мережевого трафіку, який дозволяє перехоплювати, відслідковувати та аналізувати пакети даних, що передаються через мережу. Він є одним з найбільш відомих сніферів пакетів, що використовується фахівцями з безпеки, адміністраторами мереж і розробниками програмного забезпечення для моніторингу та виявлення проблем у мережах.

Висновок. У світі, де ми все більше покладаємося на мережеві технології для виконання особистої та професійної діяльності, перехоплення даних становить серйозну небезпеку. Завдяки інформації, отриманій від сніфера пакетів, адміністратор може виявляти помилкові пакети та використовувати ці дані для ідентифікації вузьких місць, що допомагає оптимізувати передачу даних у мережі.

На відміну від стандартних мережевих хостів, які отримують лише трафік, адресований їм безпосередньо, аналізатор пакетів дозволяє отримувати дані, спрямовані на інші пристрої. Раніше аналізатори пакетів були дорогими апаратними пристроями, але завдяки новим технологіям розроблено програмні мережеві аналізатори, що робить їх доступнішими та зручнішими у використанні.

Перелік використаних джерел.

1. PlallaviAsrodia, Vishal Sharma. (2013). Network Monitoring and Analysis by Packet Sniffing Method. International Journal of Engineering Trends and Technology (IJETT). - vol 5. -May 2013.

2. S. Ansari, Rajeev S.G. and Chandrasekhar H.S. (2003). Packet Sniffing: A Brief introduction", IEEE Potentials, Dec 2002- Jan 2003, Volume: 21, Issue 5.

3. Awodele Oludele, Otusile Oluwabukola. (2012). The Design and Implementation of a packet sniffer (PSniffer) Model for Network Security. International Journal of Electronics Communication and Computer Engineering. Vol 3, ISSUE 6. ISSN (online): 2249-071X, ISSN (Print): 2278-4209.

4. Mohammed Abdul Qadeer, Mohammad Zahid, Arshad Iqbal, MisbahurRahman Siddiqui. (2010). Network Traffic Analysis and Intrusion Detection using Packet Sniffer. 2010 Second International Conference on Communication Software and Networks, Singapore, 2010, pp. 313-317, doi: 10.1109/ICCSN.2010.104.

5. A. Dabir, A. Matrawy. (2007). Bottleneck Analysis of Traffic Monitoring Using Wireshark. 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov, Page(s): 158- 162.