Ожга М. М.
доцент кафедра комп'ютерних технологій,
кандидат педагогічних наук,
Тернопільський національний педагогічний
університет імені Володимира Гнатюка
ochga@tnpu.edu.ua
Сіткар Т. В.
доцент кафедра комп'ютерних технологій,
кандидат педагогічних наук, доцент,
Тернопільський національний педагогічний
університет імені Володимира Гнатюка
sitkar@gmail.com

ОСОБЛИВОСТІ ВИКОРИСТАННЯ WIRESHARK ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Як експерту з інформаційної безпеки, важливо мати необхідні інструменти для виявлення та запобігання порушенням безпеки. Одним з найпотужніших інструментів в арсеналі фахівця з інформаційної безпеки є Wireshark - безкоштовний аналізатор мережевих протоколів з відкритим вихідним кодом, який дозволяє відстежувати та аналізувати мережевий трафік. Ми обговоримо, як використовувати Wireshark для пошуку пароля в пакеті даних.

По-перше, важливо розуміти, як паролі передаються по мережі. Зазвичай паролі надсилаються мережею у вигляді простого тексту, а це означає, що будь-хто, хто має доступ до мережі, може легко перехопити і прочитати пароль. Щоб захиститися від цього, багато веб-сайтів і додатків використовують методи шифрування, щоб зашифрувати пароль перед тим, як він буде переданий мережею.

Однак не всі веб-сайти та програми використовують шифрування, і навіть ті, що використовують, можуть використовувати його неправильно. Саме тут на допомогу приходить Wireshark - він дозволяє перехоплювати і аналізувати мережевий трафік для виявлення будь-яких пакетів, що містять конфіденційну інформацію, наприклад, паролі.

Щоб використовувати Wireshark для пошуку пароля в пакеті даних, виконайте наступні кроки:

1. Встановіть Wireshark на комп'ютер і запустіть програму.
2. Виберіть мережевий інтерфейс, з якого ви хочете перехоплювати трафік, і почніть перехоплення пакетів.
3. Увійдіть на веб-сайт або програму, з якої ви хочете перехопити трафік.
4. Зупиніть перехоплення пакетів у Wireshark та відфільтруйте захоплені пакети, щоб показати лише трафік до і з веб-сайту або програми, в яку ви увійшли.
5. Шукайте пакети, які містять ключове слово "пароль" або "логін". Ви можете скористатися функцією пошуку Wireshark, щоб швидко знайти ці пакети.
6. Проаналізуйте пакети, які містять ключові слова "пароль" або "логін". Шукайте пакети, які містять незашифровані дані, що може свідчити про те, що пароль було передано відкритим текстом.
7. Якщо ви знайшли пакет, який містить пароль у відкритому тексті, запишіть IP-адреси та порти джерела та одержувача, а також будь-яку іншу важливу інформацію про пакет.
8. Після того, як ви визначили пароль, повідомте про порушення безпеки відповідним органам і застосуйте заходи для захисту мережі та запобігання подальшим порушенням.

Важливо відзначити, що перехоплення та аналіз мережевого трафіку без дозволу є незаконним і неетичним. Ви повинні використовувати Wireshark для аналізу мережевого

трафіку лише в тих мережах, до яких у вас є дозвіл на доступ, і лише з метою виявлення вразливостей безпеки та запобігання порушень безпеки.

Крім того, важливо відзначити, що багато веб-сайтів та додатків впровадили посилені заходи безпеки, щоб запобігти перехопленню та компрометації паролів. Це включає в себе використання шифрування для скремблювання пароля перед його передачею по мережі, а також впровадження двофакторної автентифікації, яка вимагає другого фактора на додаток до пароля для входу в обліковий запис.

Хоча Wireshark може бути корисним інструментом для виявлення вразливостей безпеки, він не є безвідмовним і на нього не слід покладатися як на єдиний метод захисту від мережевих атак. Важливо впроваджувати низку заходів безпеки, таких як використання надійних паролів, постійне оновлення програмного забезпечення та патчів безпеки, використання брандмауерів та іншого програмного забезпечення для забезпечення безпеки.

Крім того, важливо бути в курсі останніх загроз і вразливостей безпеки та вживати проактивних заходів для їх усунення. Це включає регулярний перегляд та оновлення політик і процедур безпеки, проведення регулярних аудитів і оцінок безпеки, а також постійне навчання і тренінги з безпеки для співробітників.

На закінчення, Wireshark є потужним інструментом для виявлення вразливостей безпеки і запобігання порушенням безпеки. Використовуючи Wireshark для перехоплення і аналізу мережевого трафіку, ви можете виявити пакети, які містять конфіденційну інформацію, наприклад, паролі, і вжити заходів для захисту мережі та запобігання подальшим порушенням. Однак важливо використовувати Wireshark відповідально та етично, і лише з дозволу відповідних органів влади.

Список використаних джерел

1. R. Zafar and M. A. Bajwa, "Password sniffing attacks and their countermeasures: a survey," Journal of Network and Computer Applications, vol. 132, pp. 84-109, Jul. 2019. (DOI: 10.1016/j.jnca.2019.03.011)
2. J. Liu, Y. Wang and Q. Zhang, "Wireless Password Cracking with GPUs and CUDA," Proceedings of the 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, pp. 275-282, Sep. 2018. (DOI: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2018.00051)
3. R. Ahmad, M. A. Bajwa and S. Iqbal, "Enhanced user authentication and password management mechanism for cloud computing," Future Generation Computer Systems, vol. 96, pp. 254-265, Jul. 2019. (DOI: 10.1016/j.future.2019.01.019)
4. S. Ganesan, R. Ganesan and R. M. Shukla, "A Review on Wireshark Analysis for Detecting Cyber Attack," Proceedings of the 2020 International Conference on Inventive Research in Computing Applications, pp. 42-46, Jul. 2020. (DOI: 10.1109/ICIRCA49298.2020.9192215)
5. N. Ahmed, M. U. Siddiqi and A. Tariq, "A survey on Wi-Fi security protocols and their vulnerabilities," Journal of King Saud University - Computer and Information Sciences, vol. 33, no. 3, pp. 266-276, Sep. 2021. (DOI: 10.1016/j.jksuci.2021.03.002)

Оніщенко С. М.,
старший викладач кафедри
інформаційних технологій і програмування,
Український державний університет імені Михайла Драгоманова,
s.m.onishchenko@npu.edu.ua

ОСОБЛИВОСТІ ВИБОРУ МОВИ ПРОГРАМУВАННЯ ДЛЯ ВИВЧЕННЯ В ШКОЛІ

В сучасному інформаційному суспільстві програмування та програмна інженерія відіграють важливу роль в розвитку інформаційно-комунікаційних технологій та відповідного програмного забезпечення. Програмісти створюють програмні засоби для розв'язання складних завдань в науці, медицині, фінансах, транспорті та багатьох інших галузях, для автоматизації різноманітних процесів виробництва, тобто програмування є ключовим