МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПЕТРА МОГИЛИ

Тиховід Олександр Васильович

УДК: 004.41

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ТА ВИЯВЛЕННЯ КОЛІЗІЙ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Спеціальність 123 – Комп'ютерна інженерія

Автореферат
магістерської роботи
на здобуття кваліфікації магістр з комп'ютерної інженерії

Миколаїв – 2020

Робота виконана у Чорноморському національному університеті ім. Петра Могили.

Керівник:	доктор педагогічних наук, професор **Олександр Павлович Мєщанінов,** ЧНУ ім. Петра Могили, професор кафедри інтелектуальних інформаційних систем
Рецензент:	канд. фіз.-мат. наук **Кулаковська Інесса Василівна,** ЧНУ ім. Петра Могили, викладач кафедри інтелектуальних інформаційних систем
Консультант:	д-р біол. наук, професор **Григор'єва Людмила Іванівна,** ЧНУ ім. Петра Могили, завідувач кафедри екології Медичного інституту

Захист відбудеться « 26 » лютого 2020 р. о 9^{00} на засіданні Екзаменаційної комісії в ЧНУ ім. Петра Могили, ауд. 2-406

З магістерською роботою можна ознайомитись на сайті ЧНУ ім. Петра Могили за посиланням http://chmnu.edu.ua

Автореферат оприлюднений « 24 » лютого 2020 р.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Робота присвячена актуальним питанням розробки і вдосконалення систем перехоплення та аналізу мережевого трафіку та виявлення колізій і стороннього програмного забезпечення в комп'ютерних мережах.

На сьогоднішній день питання інформаційної безпеки(кібербезпеки) залишається надзвичайно важливим. Не дивлячись на активний розвиток антивірусного програмного забезпечення випадки виявлення небезпечного ПЗ ростуть у геометричній прогресії.

Більшість статистичних даних провідних антивірусних лабораторій показують, що найбільш поширеними є віруси-вимагачі – згадати хоча б найрезонансніші WannaCry та Petya , хоча загалом їх активність в мережі й знизилась на 35%.

Найбільш активно поширюваним є зловмисне ПЗ типу «прихований майнер». Так за даними компанії Symantec за 2017 рік випадки виявлення майнерів почастішали у 340 разів, а в березні 2018 року антивірусна лабораторія Malwarebytes зафіксувала 16 млн. спроб прихованого майнінгу криптовалют. За 2018-2019 роки кількість таких випадків зросла на 4000%.

За даними Національного центру кібербезпеки Великобританії, прихований майнінг буде головною загрозою для інтернет-користувачів.

Тому доцільним є створення програмно-апаратного комплексу аналізу мережевого трафіку та виявлення колізій в локальних мережах , в тому числі з функцією пошуку ПЗ класу CoinMiner в комп'ютерних мережах.

Мета і задачі дослідження. Метою магістерської наукової роботи є покращення процесу моніторингу мережевого трафіку та виявлення мережевих загроз в локальній мережі, шляхом розробки та впровадження програмно-апаратного комплексу, що аналізуватиме і фільтруватиме трафік для пошуку стороннього ПЗ.

Для досягнення поставленої мети було виконано такі завдання:

- виконано аналітичний огляд літератури про відомі результати з розв’язання задачі з прослуховування мережевого трафіку для пошуку та виявлення загроз в локальній мережі;
- виконано огляд програмних застосунків та програмно-апаратних систем для моніторингу мережевого трафіку;
- на основі огляду літератури та аналогів сформулювано вимоги до програмно-апаратного комплексу;
- визначено принцип роботи та підібрані модулі апаратної частини приладу;
- розроблено програмне забезпечення, яке фіксує трафік в певному сегменті локальної мережі, виконує аналіз отриманої інформації на предмет роботи в марежі програмних продуктів, які можуть застосовуватись для майнінгу криптовалют;
- виготовлено робочий прототип програмно-апаратного комплексу;
- виконано експериментальне дослідження роботи комплексу;
- проведено аналіз отриманих результатів;
- розроблено питання з цивільного захисту та охорони праці.

Об’єкт дослідження – методи перехоплення мережевого трафіку та аналізу отриманого трафіку на наявність стороннього програмного забезпечення, яке може використовуватись для майнінгу цифрових валют.

Предмет дослідження – процес виявлення шкідливого трафіку пристроїв однієї локальної мережі, зокрема для виявлення шкідливого ПЗ – майнерів криптовалюти.

Наукова новизна:

- удосконалено метод перехоплення мережевого трафіку, шляхом здійснення отруєння мережі підміною ARP-пакетів для виявлення всіх мережевих пакетів та недопущення виявлення сніффінгу в мережі, що є невластивим для легальних сніферів;

- реалізовано аналіз отриманих даних за декількома критеріями для виявлення ймовірного програмного забезпечення типу CoinMiner.

Практичне значення:

- розроблений комплекс має невеликі розміри й може бути підключений до мережі в будь-якому місці, в тому числі для прихованого зчитування трафіку(в разі потреби);
- пристрій не впливає на роботу мережі, його робота є непомітною для користувачів, а також реалізований захист від виявлення анти-сніферами;
- комплекс може застосовуватись системними адміністраторами та іншими спеціалістами для вирішення будь-яких практичних завдань, які потребують аналізу мережевого трафіку.

Апробація результатів магістерської роботи відсутня.

Структура та обсяг роботи. Магістерська робота складається з анотації на 2 сторінках, вступу, чотирьох розділів, висновків, переліку джерел посилання з ___ найменувань. Основна частина роботи становить ____ сторінок, серед яких ___ рис. та ___ табл.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність напрямку досліджень магістерської роботи, сформульовано мету та завдання дослідження, вказано практичне значення одержаних результатів. Задача розробити програмно-апаратний комплекс аналізу мережевого трафіку та виявлення колізій в комп'ютерних мережах.

У **першому розділі** магістерської роботи «**Аналітичний огляд літератури з прослуховування та аналізу мережевого трафіку ЛОМ**» проведено аналіз літературних джерел систем аналізу вразливостей ЛОМ; виконано класифікацію засобів моніторингу та аналізу мережевого трафіку; проведено аналіз існуючих програмних та програмно-апаратних комплексів

моніторингу та аналізу трафіку ЛОМ, описані їх основні функціональні можливості; визначені призначення і цілі розробки.

Сьогодні, під час активного розвитку інформаційно-телекомунікаційних технологій, й комп’ютерних мереж зокрема, з’являється багато методів й засобів не тільки перехоплення мережевого трафіку, а й протидії йому.

Сніффінг - це процес моніторингу та захоплення всіх пакетів даних, які проходять через комп’ютерну мережу, використовуючи програмне забезпечення (додаток) або апаратний пристрій. Сніффінг зазвичай проводиться мережевим адміністратором. Однак зловмисник може використовувати сніффер для збору даних, і ці дані, часом, можуть містити конфіденційну інформацію, таку як ім’я користувача та пароль. Мережеві адміністратори використовують передачу копії трафіку(відзеркалення) на комутаційний порт SPAN для подальшого його аналізу.

Існує два способи сніффінгу: активний і пасивний. Пасивний сніффінг здійснюється в комп’ютерних мережах побудованих на базі концентраторів. Розмістивши сніффер пакетів в мережі в невпорядкованому режимі, хакер може захоплювати пакети в підмережі. Активний сніффінг проводиться в мережі побудованій на основі комутаторів. Оскільки комутатор «розумніший» від концентратора, він відправляє пакети на комп'ютер після перевірки в таблиці MAC-адреси. Активний сніффінг відбувається за допомогою здійснення атак на комп’ютерну мережу, зокрема підробки ARP-пакетів. Результатом дипломної роботи має бути створення активного сніффера.

Розглянуто найвідоміше та найпопулярніше програмне забезпечення, яке набуло масштабного розповсюдження та позиціонує себе на ринку, як сніфери. Переважна більшість з проаналізованих програмних продуктів є пасивними сніфферами, оскільки можуть фіксувати лише той трафік, який проходить через локальний порт пристрою на якому встановлено ПЗ.

На відміну від програмних сніферів, програмно-апаратні комплекси є менш поширеними. В основному це достатньо великі та складні системи, які

потребують спеціальних знань та вмінь для використання. Також недоліком програмно-апаратних систем, на мою думку, є їх вартість, оскільки вони є дуже дорогими більшості невеликих або державних організацій не можуть собі дозволити їх використання.

На основі проведеного аналізу сформульовано вимоги до програмно-апаратного комплексу, а також визначено ряд задач, вирішення яких відображається в наступних розділах роботи.

У **другому розділі** магістерської роботи **«Розробка апаратної частини системи аналізу мережевого трафіку»** проведено обґрунтування вибору модулів, які використовуються для створення пристрою. Мережевий інтерфейс вбудований в комп'ютер Raspberry Pi3 буде використовуватись в якості TAP-порта. В якості портів Ethernet з яких дублюватиметься трафік використовуватимуться додаткові модулі ENC28J60. Ethernet-модуль ENC28J60 підключається до Raspberry PI через інтерфейс SPI. Після підключення модуля необхідно налаштувати ядро Linux для розпізнавання нового пристрою. Подальше налаштування проводимо за допомогою SSH, через підключення до IP стандартного Ethernet порту.

У **третьому розділі** магістерської роботи **«Розробка програмної частини комплексу аналізу мережевого трафіку»** приведено типи й структуру фрейму та основних мережевих пакетів, таких як: ICMP, IPv4 хедер, TCP . В якості мови розробки програмного забезпечення було обрано мову програмування Python 3.8.1, яка є актуальною і стабільною на момент виконання даної роботи. Сам застосунок складається з декількох модулів, кожен з яких виконує свою притаманну функцію. Перший модуль – модуль віддзеркалення мережевих пакетів, який зберігає копії пакетів, пропущених через пристрій. Другий модуль – це модуль обробки заголовків пакетів, який автоматично розпізнає пакети по типу і дістає заголовочну інформацію з кожного з них. Заголовочна інформація містить усі необхідні для аналізу дані:

- Кадр Ethernet показує MAC-адресу призначення та вихідну MAC-адресу;
- IP-заголовок повідомляє вихідну IP-адресу, звідки приходить пакет, та IP-адресу отримувача – іншої операційної системи, що працює в нашій підмережі;
- Заголовок TCP показує порт відправника, порт призначення та прапор.

Третій модуль – модуль обробки контенту, тіла пакету. Інформація тіла пакету нас цікавить найменше, адже наш пристрій призначений для аналізу трафіку, а не отримання інформації в злочинних цілях, адже в тілі пакету можуть міститись персональні дані користувачів такі як логін, пароль, тощо.

Також для приховування підключення даного пристрою в мережі було розроблено модуль підміни ARP пакетів. ARP використовується для інтерпретації IP-адреси в її відповідну Ethernet (MAC) адресу. Коли пакет надходить на мережевий рівень (OSI), він має IP-адресу та пакет рівня передачі даних, якому потрібна MAC-адреса пристрою призначення. У цьому випадку відправник використовує протокол ARP.

Хост-машина може захотіти надіслати повідомлення на іншу машину в тій самій підмережі. Хост-машина знає лише IP-адресу, тоді як для надсилання повідомлення на рівень посилання даних необхідна MAC-адреса. У цій ситуації відправник транслює запит ARP. Усі машини в підмережі отримують повідомлення. Тип значення протоколу Ethernet - 0x806.

Отримувач відповідає на свою MAC-адресу. Ця відповідь є одноособовою та відома як відповідь ARP.

Щоб зменшити кількість запитів на пошук MAC-адреси, клієнт зазвичай кешує відомі адреси за короткий проміжок часу. Кеш ARP має кінцевий розмір.

Коли будь-який пристрій хоче відправити дані на інший цільовий пристрій в підмережі, він повинен спочатку визначити MAC-адресу цієї цілі,

навіть якщо відправник знає IP-адресу одержувача. Ці відображення IP-MAC-адрес походять від ARP-кеш, що підтримується на кожному пристрої.

Підробка ARP(також називають отруєнням ARP) – це різновид атаки на локальну мережу коли MAC-адреса отримувача в кеш-пам'яті ARP шлюзу, а також MAC-адреса шлюзу в кеш-пам'яті ARP отримувача замінюється адресою прослуховуючого пристрою.

Це зумовлено тим, що кінцевий користувач може довідатися про наявність підключеного до мережі апаратного сніферу, якщо даної підміни пакетів не буде, а це може ускладнити виявлення трафіку, який генерується стороннім програмним забезпеченням.

Проведено експериментальне випробування пристрою та наведені результати роботи.

У спеціальній частині «Охорона праці та безпека у надзвичайних ситуаціях» наведено аналіз факторів виробничого середовища у приміщенні на підприємстві ВГО «Асоціація університетів України», а також визначений вплив цих факторів на здоров’я та працездатність працівників. Проведено розрахунок освітленості приміщень, а також складено рекомендації з техніки безпеки при роботі з програмно-апаратним комплексом. Слід зазначити, що було встановлено відповідність всіх розглянутих показників чинним санітарним нормам та виявлено, що умови праці в ВГО «Асоціація університетів України» є оптимальними.

ВИСНОВКИ

В дипломній науковій роботі на основі виконаних автором досліджень виконано аналіз методів й засобів прослуховування та аналізу мережевого трафіку та виявлення мережевих колізій. Запропоновано покращення методів зняття трафіку з метою недопущення блокування роботи пристрою та непомітності для користувачів, способи аналізу трафіку для виявлення

стороннього програмного забезпечення, яке може використовуватись для майнингу цифрових валют.

Для досягнення поставленої в магістерській дипломній роботі мети було виконано наступні завдання:

- виконано аналітичний огляд літератури про відомі результати з розв’язання задачі з прослуховування мережевого трафіку для пошуку та виявлення загроз в локальній мережі;
- виконано огляд програмних застосунків та програмно-апаратних систем для моніторингу мережевого трафіку;
- на основі огляду літератури та аналогів сформулювано вимоги до програмно-апаратного комплексу;
- визначено принцип роботи та підібрані модулі апаратної частини приладу;
- розроблено програмне забезпечення, яке фіксує трафік в певному сегменті локальної мережі, виконує аналіз отриманої інформації на предмет роботи в марежі програмних продуктів, які можуть застосовуватись для майнінгу криптовалют;
- виготовлено робочий прототип програмно-апаратного комплексу;
- виконано експериментальне дослідження роботи комплексу;
- проведено аналіз отриманих результатів;

У роботі отримано такі основні наукові та практичні результати:

1. Проведений аналіз існуючих моделей і засобів побудови програмного забезпечення та програмно-апаратних комплексів прослуховування та аналізу мережевого трафіку, який виявив їх основні недоліки та шляхи подальшого вдосконалення. Показано, що перспективним напрямком подальшого розвитку є використання захисту сніферів від виявлення користувачами.
2. Удосконалено аналітичну роботу пристрою з урахуванням орієнтації засобу для виявлення стороннього програмного забезпечення CoinMiner.

3. Розроблена апаратна та практична частини пристрою.
4. Експерементальне дослідження розробленого зразка пристрою показало його працездатність, швидкодію та ефективність роботи. Апарат може бути розміщений в будь-якій точці певного сегменту мережі та працювати автономно, без втручання людини до 7 днів.
5. Пристрій може використовуватись для вирішення більшості задач пов’язаних з аналізом мережевого трафікую

Результатом виконання даної дипломної роботи є створений та функціонуючий пристрій, що дозволяє користувачам отримувати дані про мережевий трафік в певному сегменті мережі, що можуть використовуватись для вирішення будь-яких практичних завдань, які потребують цих даних, а також звіт з ймовірного виявлення зловмисного програмного забезпечення. Комплекс має компактні розміри, не потребує додаткових джерел живлення, а також інших апаратних пристроїв, може бути розміщений в будь-якому місці й здійснювати фіксацію прослуховуваного трафіку без втручання користувача до 7 днів роботи.

АНОТАЦІЯ

Тиховід Олександр Васильович. Програмно-апаратний комплекс аналізу мережевого трафіку та виявлення колізій в комп’ютерних мережах. – На правах рукопису.

Магістерська робота на здобуття освітньої кваліфікації «Магістр комп’ютерної інженерії». – Чорноморський національний університет імені Петра Могили, Миколаїв, 2020.

Метою магістерської роботи є покращення процесу виявлення мережевих загроз в локальній мережі, шляхом розробки та впровадження програмно-апаратного комплексу, що збиратиме й аналізуватиме мережевий трафік для пошуку шкідливого ПЗ та мережевих колізій.

Об’єктом дослідження є методи перехоплення мережевого трафіку та аналізу отриманого трафіку на наявність стороннього програмного забезпечення, яке може використовуватись для майнінгу цифрових валют.

Предметом дослідження – процес та способи перехоплення та виявлення шкідливого мережевого трафіку пристроїв однієї локальної мережі, зокрема для виявлення шкідливого ПЗ – майнерів криптовалюти.

Основні завдання:

1. Проведено аналіз існуючого програмно забезпечення та програмно-апаратних комплексів для моніторингу та аналізу комп’ютерних мереж.
2. Проаналізовано типи та структуру основних мережевих пакетів.
3. Проаналізовано сучасну розробку подібних пристроїв, обрано апаратні модулі та програмне забезпечення для створення пристрою.
4. Побудовано апаратну частину на основі мікропроцесорного комп’ютера Raspberry Pi3 Model B.
5. Розроблено програмну частину з використанням об’єктно-орієнтованої мови програмування Python.

Магістерська робота містить наступні розділи:

Пояснювальна записка магістерської роботи складається зі вступу, трьох розділів, висновків, переліку джерел посилання, додатків та спеціальної частини з охорони праці.

Робота містить 30 рисунків, 1 таблицю, 25 літературних джерел та 2 додатки. Загальний обсяг дипломної роботи складає 79 сторінок.

Ключові слова: *сніффінг, мережевий трафік, комп’ютерні мережі, майнінг, sniffer, mining, network traffic , computer network.*

ABSTRACT

Tykhovid Oleksandr: **Software complex of network traffic analysis and collision implication in computer networks.** – On the rights of the manuscript.

Master's work for obtaining an educational qualification "Master of Computer Engineering". – Petro Mohyla Black Sea National University, Mykolaiv, 2020.

The aim of the diploma work is to improve the process of detecting network threats on the local network by developing and implementing a hardware and software complex that will collect and analyze network traffic to find malware and network conflicts.

The object of the study is methods of intercepting network traffic and analyzing the resulting traffic for third-party software that can be used to mine digital currencies.

The subject of the research is the process and methods of intercepting and detecting harmful network traffic of the devices of one local network, in particular for the detection of malicious software - cryptocurrency miners.

Main tasks:

1. An analysis of the existing software and software systems for monitoring and analysis of computer networks.

2. Types and principle of operation of the main network packets are analyzed.

3. Modern development of similar devices is analyzed, hardware modules and software for device creation are selected.

4. Hardware built on a Raspberry Pi3 Model B microprocessor computer

5. A software part has been developed using the object-oriented Python programming language.

The master's thesis contains the following sections:

The explanatory note of the master's thesis consists of an introduction, three sections, conclusions, a list of sources of references, applications and a special part on occupational safety.

The work contains 30 figures, 1 tables, 25 literary sources and 2 applications. The total volume of the thesis is 79 pages.

Keywords: *sniffing, network traffic, mining, computer network.*