УДК 621.391

ДОСЛІДЖЕННЯ ТА РОЗРОБКА АНАЛІЗАТОРА ТРАФІКА ДОМАШНЬОЇ МЕРЕЖІ НА ОСНОВІ RASPBERRY PI ZERO

Бикова А.О.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського
E-mail: bykova.alien@gmail.com

Research and development of a network traffic analyzer based on the Raspberry Pi Zero

A network traffic analyzer based on Raspberry Pi Zero for IoT is proposed and implemented. It allows users control access to their home network. The effective method of development traffic analyzer is proposed.

Пристрій моніторингу мережі може бути дуже корисним доповненням до домашньої мережі. Оскільки все більше пристроїв стають розумними, а світ Інтернету речей все активніше впроваджується в домашні мережі, важливо, щоб власники повідомлялися про появу нових пристроїв в їх мережі та мали можливість відкликати будь-які небажані пристрої, не впливаючи на всю мережу. Небажані пристрої, які підключилися до мережі без згоди, можуть заподіяти багато шкоди. Мета цих досліджень і проекту - зрозуміти важливість інструментів мережевого моніторингу та запропонувати ефективний інструмент моніторингу, враховуючи мережу, що складається з розумних пристроїв.

В ході дослідження різних інструментів і систем мережевого моніторингу було помічено, що саме сам пристрій часто не приймався до уваги. Існуючі інструменти моніторингу мережі були в основному розроблені для інсталяції на комп'ютер користувача та зрідка розглядалися як окреме апаратне доповнення до існуючої мережі. Беручи до уваги, що інструмент моніторингу мережі найбільш корисний, коли він здійснює моніторинг протягом всього дня, засіб моніторингу домашньої мережі Raspberry Pi Zero призначений для окремого апаратного доповнення до мережі.

На малюнку 1 представлена структура і архітектура засобу моніторингу домашньої мережі на Raspberry Pi Zero. Raspberry Pi Zero підключається до роутера через дротове або бездротове з'єднання. Домовласник може отримати доступ до пристрою моніторингу з будь-якого пристрою в мережі. Якщо власник домашньої мережі хоче заблокувати пристрій, до iptable буде додано відповідний запис. Всі авторизовані пристрої в мережі також будуть підключені до домашнього роутера.

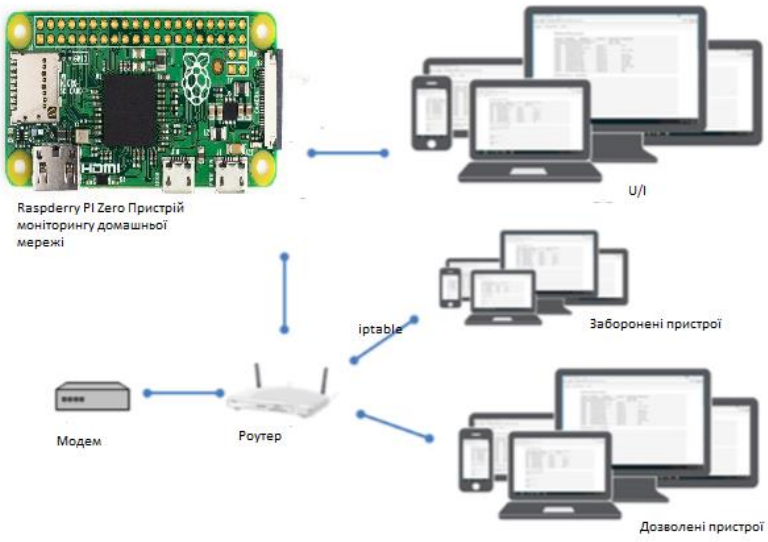

Рис. 1. Структура і архітектура інструменту для моніторингу домашньої мережі на Raspberry Pi Zero.

Kali Linux була обрана через велику кількість інструментів, які вона надає для мережевого моніторингу. Набір інструментів, який надає Kali Linux, багатий мережевими сценаріями і додатками для проникнення і використання слабких місць у мережі[1].

Для частини виявлення використовується NMAP [2]. NMAP - сканер мережевої безпеки, який сканує всю мережу і надає корисну інформацію для кожної системи. NMAP може приймати різні форми команд і дозволяє користувачеві вибирати тип сканування для виконання, від надання мінімальної кількості інформації до вичерпної. За допомогою NMAP ми отримуємо поточну IP-адресу, MAC-адресу і назву виробника мережевого пристрою. Користувач може вибрати і налаштувати час сканування. За замовчуванням сканування виконується кожну хвилину. По завершенні перевірки створюється тимчасовий файл з усією інформацією для кожного пристрою.

Для частині відмови були взяті кілька різних інструментів і методів. У міні-атаці відмови в обслуговуванні Nping [3] був обраний для використання. Nping - це інструмент з відкритим вихідним кодом, який дозволяє налаштовувати мережні пакети для генерації.

Для частини відмови реалізована iptable конфігурація. Iptable - це додаток з відкритим вихідним кодом, який дозволяє налаштувати конфігурацію таблиці брандмауера ядра Linux. Коли власники мереж приймають рішення про заборону небажаного пристрою в своїй мережі, вони відправляють MAC-адресу, яка записується в файл. Буде запущена програма з використанням SSH і SCP для передачі цього файлу на маршрутизатор. Маршрутизатор повинен бути налаштований для підключення по SSH, щоб успішно реалізувати метод відмови в iptable. Для маршрутизатора написано невеликий скрипт, який повинен бути запущений на виконання. Скрипт переглядає файл, який містить MAC-адресу небажаного користувача, яка потім буде вставлена в iptable. Якщо власники мереж не зможуть зконфігурувати свій маршрутизатор для з'єднання

по SSH, вони все одно будуть повідомлені про те, що пристрій, що знаходиться в відкликаному списку, повернувся у свою мережу, після чого власникам необхідно буде увійти в систему на сторінці утиліти налаштування маршрутизатора і заблокувати цей пристрій.

Для описання роботи серверної частини моніторингу мережі використовується кілька різних мов програмування: Bourne Shell, PHP. Основна частина серверної логіки засобу моніторингу мережі написана в Bourne Shell. PHP дозволяє через призначений для користувача інтерфейс взаємодіяти з сервером. PHP також запускає кілька сценаріїв оболонки Bourne.

Повідомлення викликаються по електронній пошті. Щоб настроїти електронну пошту використовуються сервер SSMTP і mailutils. Різні сценарії будуть викликати відповідні повідомлення, які відправляються власнику мережі у вигляді повідомлень.

Фронт-енд інструменту для моніторингу мережі написано з використанням HTML, Bootstrap і JavaScript. Фронт-енд взаємодіє з бек-ендом через PHP.

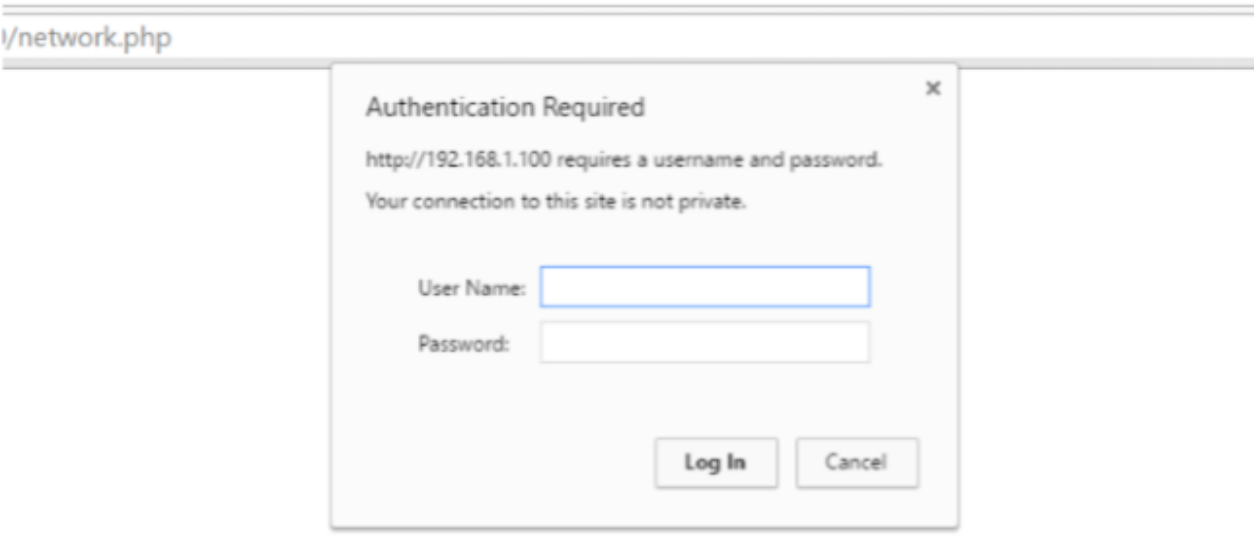

Рис. 2: Сторінка входу для контролю інструменту Raspberry Pi домашньої мережі.

Інструмент мережевого моніторингу розроблений, щоб бути простим і зручним у використанні. Власник мережі зможе взаємодіяти з інструментом моніторингу Raspberry Pi з будь-якого пристрою, який має веб-браузер і знаходиться в мережі. Власник мережі повинен буде вказати ім'я користувача і пароль, щоб отримати доступ до інструмента моніторингу. Веб-сервер Apache2, сконфігурованих на Raspberry Pi 3, дає власникам можливість взаємодіяти з інструментом моніторингу з будь-якого пристрою в своїй мережі.

Література

1. O. Security. Kali linux. https://www.kali.org.
2. G. Lyon. Nmap. https://nmap.org/.
3. L. Gordon. Nping. https://nmap.org/nping/.