УДК 004.272, 004.032.24

Р. І. Банах*, А. З. Піскозуб*, Я. Я. Стефінко**
Національний університет "Львівська політехніка",
*кафедра захисту інформації,
**кафедра безпеки інформаційних технологій

АВТОМАТИЗАЦІЯ РОЗГОРТАННЯ WI-FI ТОЧКИ ДОСТУПУ ЯК ЗОВНІШНЬОГО ЕЛЕМЕНТА СИСТЕМИ ПРИМАНКИ

Показано механізм автоматизації розгортання безпровідної точки доступу технології Wi-Fi та його імплементація на інтерпретаторі bash. Запропоновано концепцію віддаленого керування Wi-Fi точкою доступу як елементом системи приманки для безпровідної мережі.

Ключові слова: Wi-Fi, система приманки, автоматизація, одномодульний комп'ютер.

An automation mechanism of deploying Wi-Fi wireless network and its implementation on bash command language is presented in this article. A concept of remote control by Wi-Fi access point as an element of honeypot for wireless network is suggested.

Key words: Wi-Fi, honeypot, automation, single board computer.

Вступ

Розширення функціональності безпровідного устаткування Wi-Fi є фактично нереальним завданням. Причина цього – найчастіше обмежені апаратні ресурси. Закритий програмний код не дає змоги кінцевому користувачеві задіяти налаштування, які не передбачені виробником. Усе це унеможливлює створити додаткову обробку інформації, а відповідно і зв'язок із рештою елементів системи приманки.

Wi-Fi точку доступу можна розгорнути на будь-якій сучасній операційній системі, яка підтримує роботу із безпровідними пристроями. Та застосування персональних комп'ютерів чи серверного обладнання як середовища для розгортання Wi-Fi точки доступу є не зовсім доречним через високу вартість та великі розміри, чого не можна сказати про одномодульні комп'ютери.

Використання одномодульного комп'ютера, наприклад Raspberry Pi, в такому режимі є доречним разом з іншими елементами системи-приманки. Через достатню кількість ресурсів і можливість встановлення операційної системи Linux можна збирати і обробляти дані вже на самому комп'ютері.

Оскільки базові засоби операційної системи Linux дають змогу компілювати / інтерпретувати програмне забезпечення (ПЗ), написане такими мовами програмування, як Python, Ruby, C, C++ та ін., то така платформа може бути використана як одна із компонент системи приманки у безпровідній мережі, а саме: як маршрутизатор-приманка.

Автоматизація процесу розгортання такої точки доступу дасть змогу кінцевому користувачеві без його безпосередньої участі якнайшвидше отримати у користування цей сервіс. Такий підхід уможливить скоротити час, який використовується для рутинних завдань, та уникнути людського фактора.

Аналіз досліджень та публікацій

В [1] запропоновано концепцію зовнішнього пристрою як компонента системи приманки у безпровідній мережі та конкретний обчислювальний пристрій для її реалізації, що взято за основу розроблення автоматизації розгортання Wi-Fi точки доступу. Предметом дослідження роботи [3] є застосування одномодульних робочих станцій у безпровідних мережах як компоненти системи приманки.

У [2] запропоновано вирішення проблеми хмарних обчислювальних рішень, здійснено порівняння сервісів, які повинні бути використані у публічних та приватних хмарних рішеннях, а в [4] описуються існуючі системи, призначені для віддаленого керування мережевими ресурсами. Здійснено

порівняння запропонованої концепції [2] з комерційними рішеннями із [4], і взято за основу для віддаленого розгортання та керування Wi-Fi точки доступу як елемента системи приманки.

Постановка завдання

З метою досягнення результатів у проектуванні системи приманки для бездротових мереж стандарту Wi-Fi постає завдання розроблення механізму автоматизації розгортання кожного елемента цієї системи, у цьому разі – точки доступу. Для того, щоб отримати функціональну Wi-Fi точку доступу, потрібно виконати такі операції:

- перевірку прав користувача;
- перевірку драйвера безпровідної карти;
- встановлення ПЗ;
- встановлення конфігураційних файлів;
- налаштування брандмауера;
- встановлення сервісів в автозапуск.

На основі цієї послідовності постає таке завдання: розробити механізм автоматизації розгортання Wi-Fi точки доступу як елемента системи приманки. Це і є предметом дослідження.

1. Опис необхідних операцій для автоматизації процесу розгортання Wi-Fi точки доступу

Сформульований ряд операцій, який потрібен для того, щоб отримати функціональну точку доступу. Він був трансформований у блок-схему (рис. 1), на основі якої розроблений сценарій на командній мові програмування bash (лістинг 2).

Блок перевірки прав користувача дасть змогу виключити можливість запуску сценарію для користувача, який не має прав суперкористувача. Права суперкористувача потрібні для того, щоб отримати доступ до системних файлів та пристроїв. У разі запуску сценарію користувачем, який не має таких прав, процес буде закінчений з помилкою на етапі доступу до системних даних чи до пристроїв. Тому після запуску сценарію користувач повинен бути повідомлений про те, що запуск був здійснений без належних прав.

Були проведені дослідження двох типів мережевих карт із набором мікросхем Atheros AR9271 і Realtek RTL8188EUS. Під час дослідження було виявлено, що базова інсталяція пакета hostapd некоректно працює із набором мікросхем RTL8188EUS і потребує встановлення додаткового пакета виправлень.

На основі зібраних даних на етапі перевірки драйвера безпровідної карти сценарієм повинно прийматись рішення щодо набору ПЗ і встановлення пакета виправлень.

Після встановлення ПЗ потрібно замінити стандартні конфігураційні файли, які належать до програмних пакетів hostapd, isc-dhcp-server, та деякі файли, які належать до налагодження мережевого з'єднання, а саме:

- */etc/default/isc-dhcp-server,* – в який встановлюється інформація про інтерфейс, до якого буде прив'язаний DHCP сервер;
- */etc/dhcp/dhcpd.conf* – головний файл конфігурації DHCP сервера, який відповідає за розподіл IP-адресів для нових клієнтів;
- */etc/network/interfaces* – містить налаштування усіх мережевих інтерфейсів;
- */etc/default/hostapd* – файл, у якому вказаний шлях до головного файла із конфігураціями безпровідної точки доступу;
- */etc/hostapd/hostapd.conf* – основний файл конфігурацій безпровідної точки доступу, в якому міститься ім'я точки доступу, метод автентифікації, частота, на якій вона працює тощо.

Для того, щоб встановити зв'язок між інтерфейсом точки входу у внутрішній мережевий ресурс (eth0) та інтерфейсом точки доступу користувачів (wlan0), потрібно встановити перелік налаштувань брандмауера, а саме:

- видалити усі наявні налаштування брандмауера;
- уможливити передачу даних із внутрішнього мережевого ресурсу на зовнішній;
- уможливити передачу даних із зовнішнього мережевого ресурсу на внутрішній.

Після вказаної послідовності операцій конфігурація повинна бути збережена. Окрім того, на робочій станції потрібно увімкнути режим ip-forward, що дасть змогу забезпечити маршрутизацію пакетів.

Встановлене раніше ПЗ повинно бути налагоджене для подальшого автоматичного запуску після старту системи для уникнення додаткового втручання з боку кінцевого користувача.

Після того, як усі вищеописані операції будуть успішно виконані, комп'ютер автоматично перезавантажиться. Зі стартом системи до неї можна буде підключитись за інтерфейсом Wi-Fi.

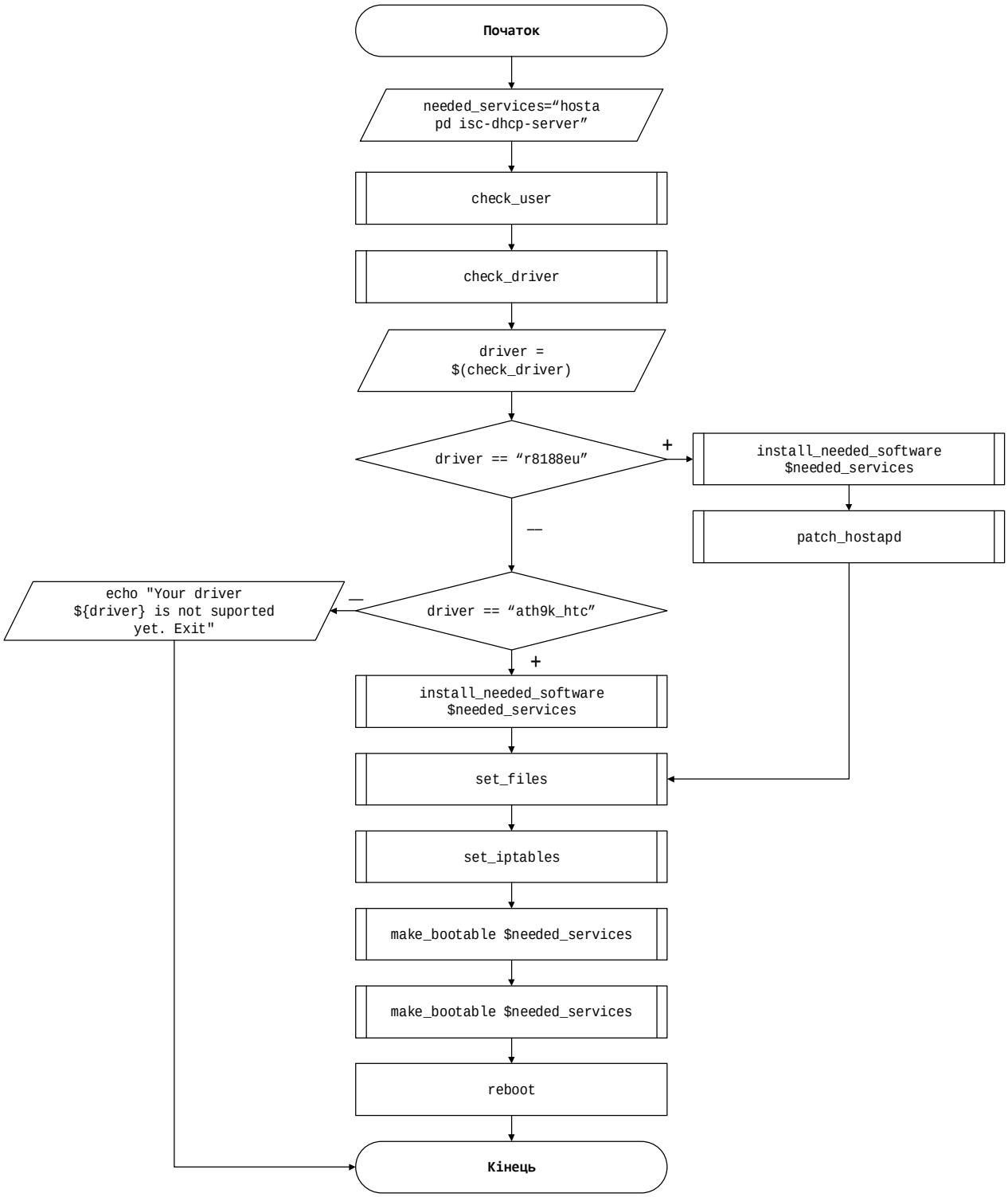

Рис. 1. Блок-схема автоматизації розгортання Wi-Fi точки доступу

2. Результати роботи bash-сценарію

У сценарій розгортання Wi-Fi точки доступу додані інформаційні підказки, які дадуть змогу слідкувати за тим, що відбувається під час її розгортання (Лістинг 1). В результаті невдачі у користувача є можливість зрозуміти, що пішло не так. Цей сценарій був виконаний протягом семи з половиною хвилин.

ЛІСТИНГ 1

ІНФОРМАЦІЙНИЙ СУПРОВІД У РОЗГОРТАННІ WI-FI ТОЧКИ ДОСТУПУ ЯК ЕЛЕМЕНТУ СИСТЕМИ ПРИМАНКИ

```
[+] Installation is launched. It will take several minutes
[+] Update repositories data
[!] hostapd is absent and will be installed
[+] hostapd has been installed
[!] isc-dhcp-server is absent and will be installed
[+] isc-dhcp-server has been installed
[!] Fixing issue with hostapd
[!] Setup configuration files
[!] IPTables settings update
[+] Service hostapd has been added to startup
[+] Service isc-dhcp-server has been added to startup
```

3. Концепція віддаленого розгортання Wi-Fi точки доступу

Для того, щоб здійснювати маніпуляції над точкою доступу, потрібно, щоб оператор і точка доступу знаходились в одній підмережі або ж вона повинна мати публічну IP-адресу. Іншим методом об'єднання мереж або ж підключення окремих робочих станцій до мережі є технологія VPN (Virtual Private Network).

VPN сервер очікує на з'єднання із клієнтом. Після авторизації на клієнті створюється новий мережевий інтерфейс (наприклад, tun0), до якого прив'язується IP-адреса із пулу адресів VPN.

Командна робоча станція призначена для того, щоб відправляти команди на пристрої, які були підключені до VPN сервера і надіслали запит на автоматичне інсталювання і налаштування.

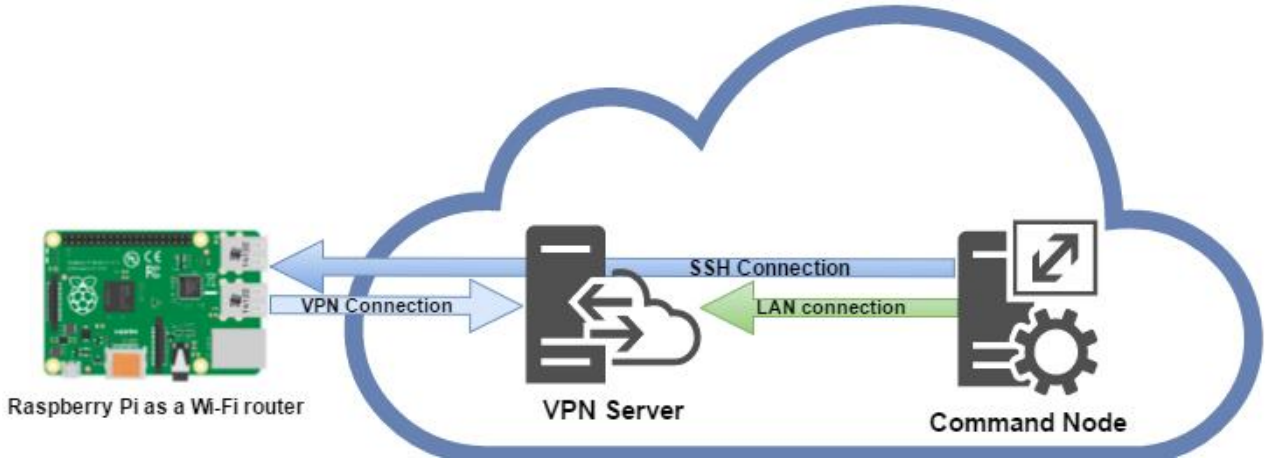

Рис. 2. Комунікація між точкою доступу та командною робочою станцією

Висновки

Одномодульні комп'ютери є доброю альтернативою звичайним персональним комп'ютерам, оскільки вони є дешеві, не споживають багато ресурсів і можуть задовольнити мінімальні обчислювальні потреби. Саме такі вимоги ставляться до вхідної точки у системну приманку.

Сценарій, представлений у цій роботі, дає змогу автоматично розгорнути Wi-Fi маршрутизатор як зовнішній елемент системи приманки для бездротової мережі. Такий підхід допоможе скоротити час розгортання та уникнути помилок з боку оператора.

ЛІСТИНГ 2

Код сценарію автоматичного розгортання Wi-Fi точки доступу

```
#!/bin/bash

check_user() {
    user=$(whoami)
    if [ ${user} != 'root' ]; then
        echo -e "\033[1;31m[-]\033[0m This script should be launched with root
permissions, for example \"sudo $0\""
        exit 1
    else
        echo -e "\033[1;32m[+]\033[0m Installation is launched. It will take several
minutes"
    fi
}

check_driver() {
    readlink /sys/class/net/wlan0/device/driver | rev | cut -d '/' -f 1 | rev
}

install_needed_software() {
    echo -e "\033[1;32m[+]\033[0m Update repositories data"
    apt-get update -y > /dev/null
    for item in $@; do
        search_package=$(dpkg --get-selections ${item})
        if [ `echo ${search_package} | cut -d " " -f 2` != 'install' ]; then
            echo -e "\033[1;33m[!]\033[0m ${item} is absent and will be installed"
            apt-get install ${item} -y --force-yes > /dev/null
            if [ $? == 0 ]; then
                echo -e "\033[1;32m[+]\033[0m ${item} has been installed"
            fi
        else
            echo -e "\033[1;32m[+]\033[0m ${item} is already installed"
        fi
    done
}

patch_hostapd() {
    echo -e "\033[1;33m[!]\033[0m Fixing issue with hostapd"
    wget http://adafruit-download.s3.amazonaws.com/adafruit_hostapd_14128.zip
    if [ $? != 0 ]; then
        echo -e "\033[1;31m[-]\033[0m Can't download patch adafruit_hostapd_14128.zip.
Exit"
        exit 1
    fi
    unzip adafruit_hostapd_14128.zip
    mv hostapd /usr/sbin
    chmod 755 /usr/sbin/hostapd
}

set_iptables() {
    echo -e "\033[1;33m[!]\033[0m IPTables settings update"
    iptables -F
    iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

```
    iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j
ACCEPT
    iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
    echo "1" > /proc/sys/net/ipv4/ip_forward
    iptables-save > /etc/iptables.ipv4.nat
}

set_files() {
echo -e "\033[1;33m[!]\033[0m Setup configuration files"

cat << EOF > /etc/dhcp/dhcpd.conf
ddns-update-style none;
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;

subnet 192.168.42.0 netmask 255.255.255.0 {
range 192.168.42.10 192.168.42.50;
option broadcast-address 192.168.42.255;
option routers 192.168.42.1;
default-lease-time 600;
max-lease-time 7200;
option domain-name "local";
option domain-name-servers 8.8.8.8, 8.8.4.4;
}
EOF

cat << EOF > /etc/default/isc-dhcp-server
INTERFACES="wlan0"
EOF

cat << EOF > /etc/network/interfaces
auto lo
iface lo inet loopback

iface eth0 inet dhcp

allow-hotplug wlan0
iface wlan0 inet static
    address 192.168.42.1
    netmask 255.255.255.0

up iptables-restore < /etc/iptables.ipv4.nat
EOF

cat << EOF > /etc/hostapd/hostapd.conf
interface=wlan0
ssid=Pi_AP
hw_mode=g
channel=6
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
```

```
wpa_passphrase=Raspberry
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
EOF

cat << EOF > /etc/default/hostapd
DAEMON_CONF="/etc/hostapd/hostapd.conf"
EOF
}

make_bootable() {
    for item in $@; do
        update-rc.d ${item} enable
        if [ $? == 0 ]; then
            echo -e "\033[1;32m[+]\033[0m Service ${item} has been added to startup"
        else
            echo -e "\033[1;33m[!]\033[0m Something went wrong. Service ${item} has
not been added to startup"
    done
}

check_user
driver=$(check_driver)
needed_software='hostapd isc-dhcp-server'
if [ ${driver} == 'r8188eu' ]; then
    install_needed_software $needed_services
    patch_hostapd
elif [ ${driver} == 'ath9k_htc' ]; then
    install_needed_software $needed_services
else
    echo "Your driver ${driver} is not suported yet. Exit"
    exit 1
fi
set_files
set_iptables
make_bootable $needed_services
reboot
```

1. Banakh R. / External elements of honeypot for wireless network / Banakh R., Piskozub A., Stefinko Y. "Modern Problems of Radio Engineering, Telecommunications, and Computer Science": Proceedings of the XIIIth International Conference TCSET'2016. Lviv-Slavsko, Ukraine February 23–26, 2016 // Lviv Publishing House of Lviv Polytechnic, 2016. – 480–482 p. 2. Створення концепції захищеної хмарної обчислювальної мережі з використанням систем приманок / Р. І. Банах, А. З. Піскозуб, Я. Я. Стефінко // Вісник Національного університету "Львівська політехніка" " Автоматика, вимірювання та керування". – 2015. – № 821. – С. 74–78. 3. Одноплатна робоча станція як станція компонент системи приманки у безпровідних комп'ютерних мережах / Р. Банах, Я. Стефінко // Захист інформації в інформаційно-комунікаційних системах: зб. тез доп. І Міжвузівської наук.-практ. конф. студентів і курсантів. – Львів: ЛДУ БЖД, 2015. – 52 с. – С. 6–7. 4. Разработка прототипа интернет-маршрутизатора/шлюза с распределенной облачной системой управления / И. В. Алексеев, М. Н. Захарова, А. В. Лукьянов // Интернет и современное общество: сб. тез. докл. Труды XVI Всероссийской объединенной конференции "Интернет и современное общество" (IMS-2013). – СПб., 9–11 октября, 2013 г. – СПб.: НИУ ИТМО, 2013. – 84 с. – С. 35–36