Jurnal Education and Information Technology
https://e-journal.undikma.ac.id/index.php/jedit
Email: jedit@undikma.ac.id
DOI: https://doi.org/

Juli 2023. Vol.1, No.1
e-ISSN:
pp.1-5

ANALISIS PENGGUNAAN METODE ROOT SHELL EXPLOIT DALAM PROSES FLASHING FIRMWARE OPENWRT PADA PERANGKAT XIAOMI MI ROUTER 4A

[1]Edy Haryanto, [2]Jarir
[1,2]Prodi Pendidikan Teknologi Informasi, FSTT, Universitas Pendidikan Mandalika
Email: [1]edy.haryanto@undikma.ac.id,

Informasi Artikel:
Received:
Revised:
Published:

Keywords:
Firmware OpenWrt; Router; Xiaomi MI Router 4A; Root Shell Exploit

Abstract

This research aims to optimize the hardware performance of the Xiaomi MI Router 4A by replacing the original firmware with OpenWrt firmware. The original firmware of the router has inherent feature limitations, and the adoption of OpenWrt firmware is anticipated to enhance the router's capabilities. However, the conventional firmware replacement process typically necessitates physical access to the ROM and direct reprogramming, which is impractical and carries the risk of hardware damage. Hence, this study employs the root shell exploit method to remotely install firmware via the network, eliminating the need for physical interaction with the ROM. This method is expected to facilitate the firmware installation process and mitigate the risk of hardware damage. The research provides insights into the utilization of the root shell exploit method for firmware replacement on the Xiaomi MI Router 4A, while also offering practical recommendations for users seeking to optimize their router's performance through the utilization of OpenWrt firmware.

Kata Kunci:
Firmware OpenWrt; Router; Xiaomi MI Router 4A; Root Shell Exploit

Abstrak

Penelitian ini bertujuan untuk mengoptimalkan kinerja perangkat keras router Xiaomi MI Router 4A dengan mengganti firmware asli menjadi firmware OpenWrt. Firmware asli pada router tersebut memiliki keterbatasan fitur, sehingga penggunaan firmware OpenWrt diharapkan dapat meningkatkan kemampuan router tersebut. Namun, proses penggantian firmware umumnya melibatkan akses fisik ke ROM dan memprogram ulang secara langsung, yang tidak praktis dan berisiko merusak perangkat keras. Oleh karena itu, penelitian ini menggunakan metode root shell exploit untuk melakukan instalasi firmware secara remote melalui jaringan, tanpa perlu menyentuh ROM secara fisik. Metode ini diharapkan dapat mempermudah proses instalasi firmware dan mengurangi risiko kerusakan perangkat keras. Penelitian ini memberikan pemahaman tentang penggunaan metode root shell exploit dalam mengganti firmware pada router Xiaomi MI Router 4A, serta menghasilkan rekomendasi praktis bagi pengguna yang ingin mengoptimalkan kinerja router mereka melalui penggunaan firmware OpenWrt.

*Koresponden: Edy Haryanto

1. PENDAHULUAN

Teknologi wireless WiFi telah populer di dunia sebagai jaringan komputer lokal (LAN) berdasarkan standar IEEE 802.11 [1]. Router yang tersedia di pasaran umumnya menggunakan standar 802.11n dan memiliki keterbatasan kinerja [2]. Contohnya, router Xiaomi MI Router 4A hanya dapat dikonfigurasi sebagai access point dan repeater. Untuk meningkatkan kemampuan router ini, perlu mengganti firmware asli menjadi firmware OpenWRT [3]. Open WRT merupakan salah satu distribusi *linux*, dimana *linux* adalah sistem operasi yang bersifat multi user dan multi-tasking, dapat berjalan di berbagai *platform* termasuk prosesor Intel 386 maupun yang lebih tinggi. [4].

Penggantian firmware bertujuan untuk menggunakan firmware Open Source [5]. Proses ini umumnya melibatkan akses fisik ke ROM. Namun, metode ini tidak praktis dan berpotensi merusak hardware. Penelitian ini menggunakan metode root shell exploit untuk menginstal firmware secara remote melalui jaringan tanpa menyentuh ROM fisik.

Tujuan penelitian ini adalah menjelaskan penggantian firmware pada router menggunakan metode root shell exploit secara remote. Metode ini diharapkan memberikan solusi efisien dan aman dalam meningkatkan kinerja router. Penelitian ini diharapkan memberikan pemahaman mendalam tentang teknologi wireless dan solusi inovatif dalam mengoptimalkan perangkat router.

2. BAHAN DAN METODE

Dalam penelitian ini, terdapat dua jenis bahan yang digunakan untuk mencapai tujuan penelitian. Pertama, digunakan bahan berbentuk perangkat lunak yang meliputi file OpenWRTInvation, firmware OpenWRT versi 22.03.0-rc4, dan koneksi internet. File OpenWRTInvation merupakan program khusus yang dikembangkan untuk mendukung proses instalasi OpenWRT pada perangkat router Xiaomi MI Router 4A. Firmware OpenWRT versi 22.03.0-rc4 digunakan sebagai versi firmware terbaru yang kompatibel dengan perangkat tersebut. Koneksi internet menjadi penting dalam memfasilitasi akses ke berbagai sumber daya yang diperlukan selama proses instalasi, seperti unduhan firmware OpenWRT dan akses ke server yang menyediakan sumber daya tambahan [6].

Kedua, dalam penelitian ini juga digunakan bahan perangkat keras, yaitu Router Xiaomi MI Router 4A. Pemilihan router ini didasarkan pada popularitasnya di pasaran dan kompatibilitasnya dengan firmware OpenWRT. Router Xiaomi MI Router 4A menyediakan platform yang memadai untuk mengimplementasikan Teknik Root Exploit dalam proses instalasi OpenWRT. Dengan menggunakan bahan perangkat keras ini, penelitian ini bertujuan untuk mengeksplorasi dan menguji kemungkinan instalasi firmware OpenWRT pada perangkat router Xiaomi MI Router 4A.

Penelitian ini juga melibatkan penggabungan teori-teori yang diperoleh dari informasi-forum OpenWrt dan dokumentasi web resmi. Tahap analisis terdiri dari dua aspek, yaitu analisis sistem yang sudah ada dan analisis kebutuhan sistem. Pada analisis sistem yang sudah ada, dilakukan studi literatur melalui buku, jurnal ilmiah, dan informasi yang ditemukan di internet untuk memahami sistem yang sudah ada, termasuk spesifikasi dan fitur dari firmware OpenWRT. Sementara itu, pada analisis kebutuhan sistem, dilakukan analisis terhadap kebutuhan pengguna dan sistem, termasuk mempertimbangkan perangkat keras seperti Router Xiaomi MI Router 4A dan perangkat lunak seperti OpenWrt 22.03.0-rc4 dan OpenWRTInvation.

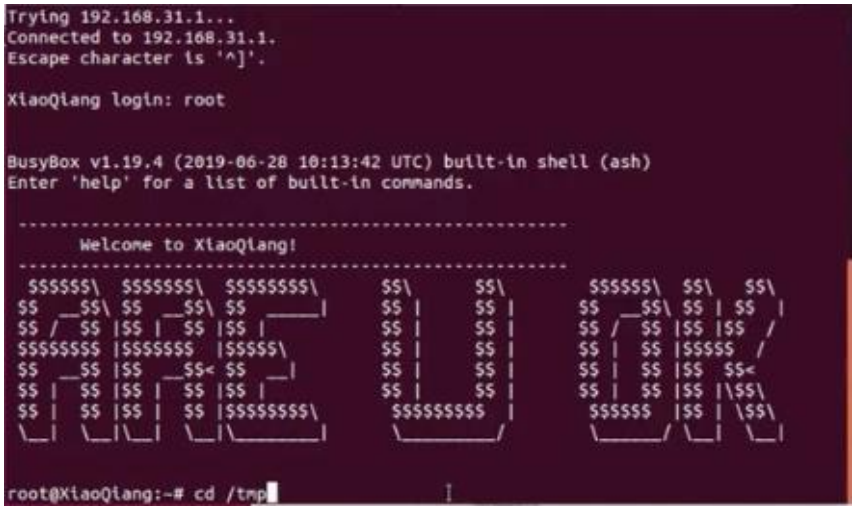
Setelah tahap analisis, penelitian dilanjutkan dengan tahap pengujian. Pengujian dilakukan menggunakan metode pengujian blackbox, di mana peneliti menguji fungsionalitas sistem yang telah dirancang dan dibuat tanpa mengetahui detail implementasinya. Pengujian blackbox bertujuan untuk memverifikasi apakah OpenwrtInvasion berjalan lancar dan memenuhi persyaratan fungsional yang telah ditetapkan sebelumnya. Pengujian ini melibatkan serangkaian skenario dan pengujian fungsional yang dilakukan secara sistematis untuk memastikan keberhasilan instalasi firmware OpenWRT menggunakan Teknik Root Exploit pada perangkat router Xiaomi MI Router 4A [7].

3. HASIL dan PEMBAHASAN

3.1. Hasil

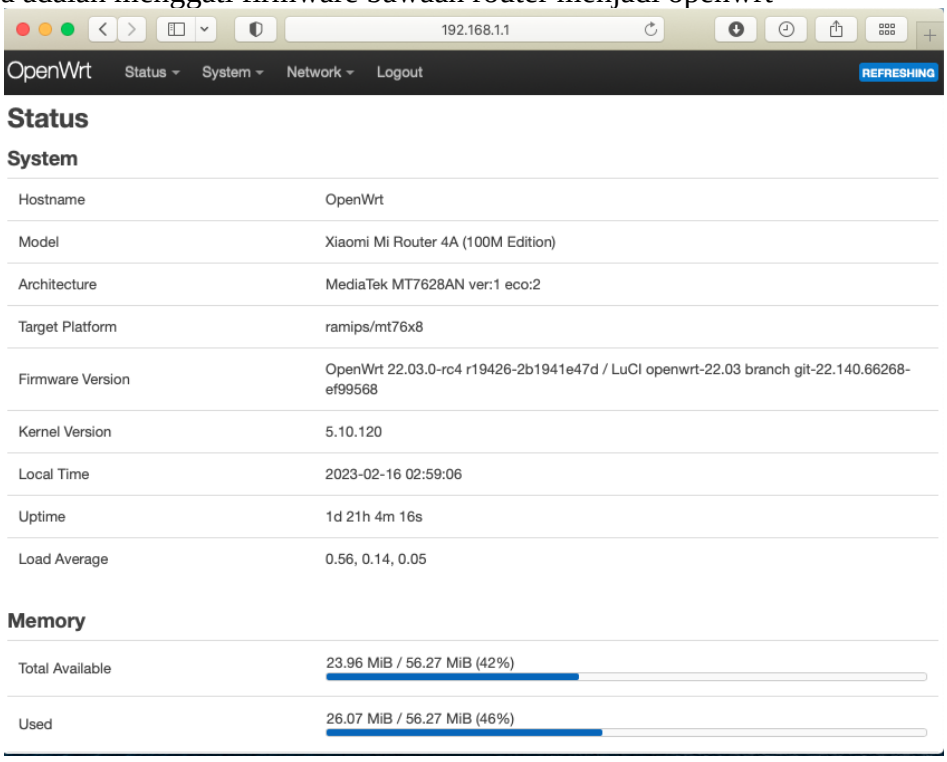
OpenWRTInvation bekerja dengan cara mengupload backup file yang berisi arbitrary code yang dapat disimpan pada directori manapaun pada router. Ketika file tersebut dikalankan OpenWRTInvation dapat mereset password pada sistem dan membuka jalur akses melalui

Telnet atau SSH dengan hak akses sebagai root, sesuai dengan yang ditunjukkan pada Gambar 1.



Gambar 1. Hak akses root pada router.

Setelah berhasil mendapatkan hak akses sebagi root pada sistem router, Langkah selanjutnya adalah menggati firmware bawaan router menjadi openwrt



Gambar 2. Halaman utama luci web admin

Gambar 2 yang ditampilkan di atas menunjukkan halaman utama luci web admin yang mengindikasikan bahwa router Xiaomi MI Router 4A telah berhasil menginstal dan menjalankan firmware OpenWRT. Dalam gambar tersebut, terlihat antarmuka pengguna luci yang memperlihatkan konfigurasi dan fitur yang tersedia pada firmware OpenWRT yang berjalan di router Xiaomi MI Router 4A. Hal ini menegaskan bahwa proses instalasi firmware OpenWRT pada perangkat router telah berhasil dan pengguna sekarang dapat mengakses berbagai pengaturan dan fungsi yang disediakan oleh OpenWRT melalui antarmuka luci web

admin. Gambar 2 merupakan bukti visual yang menunjukkan keberhasilan migrasi firmware pada router Xiaomi MI Router 4A ke OpenWRT.

3.2. Pembahasan

Implementasi root shell exploit ini memiliki beberapa langkah yang harus diikuti. Langkah-langkah tersebut meliputi konfigurasi jaringan, penemuan Stock Code, eksploitasi menggunakan OpenWRTInvation, dan akhirnya instalasi firmware OpenWRT.

Untuk mengkonfigurasi jaringan, sambungkan router Xiaomi ke internet melalui port WAN. Secara default, router akan mendapatkan subnet 192.168.31.x dan dapat diakses melalui alamat IP 192.168.31.1. Selanjutnya, sambungkan komputer atau laptop dengan sistem operasi Linux ke router Xiaomi melalui port LAN atau jaringan nirkabel untuk melakukan proses eksploitasi.

Untuk menemukan Stock Code yang diperlukan dalam proses invasi, login ke router melalui web browser menggunakan alamat IP 192.168.31.1. Pada bar alamat URL, terdapat string yang disebut Stock Code yang akan digunakan dalam proses eksploitasi. Untuk mendapatkan akses root pada router menggunakan OpenWRTInvation, clone skrip OpenWRTInvation ke komputer dengan perintah

```
git clone https://github.com/acecilia/OpenWRTInvasion.git
```

Setelah itu, install dependensi yang diperlukan dan jalankan eksploitasi. Jika eksploitasi berhasil, Anda akan mendapatkan hak akses root pada router dan dapat login melalui telnet.

```
sudo pip3 install -r requirements.txt # Install requirements

sudo python3 remote_command_execution_vulnerability.py
```

Setelah berhasil memperoleh hak akses root pada sistem router, langkah selanjutnya adalah mengganti firmware bawaan router dengan OpenWRT. Untuk melakukannya, pindah ke direktori yang sesuai dan jalankan perintah yang diperlukan. Proses instalasi akan memakan waktu sekitar 15 menit atau lebih, dan selama proses ini, lampu indikator router akan berkedip cepat berwarna oranye. Setelah instalasi selesai, router akan restart dan menjalankan firmware OpenWRT. Untuk memastikan keberhasilan instalasi, akses alamat IP 192.168.1.1 melalui web browser.

4. KESIMPULAN

Proses instalasi OpenWRT pada router umumnya melibatkan penggunaan perangkat programmer SPI yang langsung terhubung secara fisik ke memori router. Dalam proses ini, router perlu dibongkar agar dapat terhubung antara programmer SPI dan memori router. Pembongkaran perangkat menjadi langkah penting untuk mengakses memori dan memungkinkan proses instalasi OpenWRT dilakukan.

Namun, hasil dari penelitian ini menunjukkan bahwa terdapat alternatif yang dapat digunakan untuk menginstal firmware OpenWRT pada perangkat router Xiaomi Mi Router 4A, yaitu dengan menggunakan Teknik Root Exploit. Teknik ini menawarkan solusi yang lebih sederhana tanpa perlu melakukan pembongkaran fisik pada router. Dalam Teknik Root Exploit, proses instalasi firmware dapat dilakukan melalui koneksi internet dan menggunakan akses Telnet atau SSH pada perangkat router. Dengan demikian, pengguna dapat menginstal

OpenWRT tanpa perlu melibatkan langkah tambahan yang kompleks, seperti pembongkaran fisik pada perangkat.

DAFTAR PUSTAKA

[1] Fietkau, Felix. 2005. *567-Paper-OpenWrt hacking*.

[2] Lowe, D. 2008. *Networking All-in-One Desk Reference for Dummie* (4th edition). Hoboken : Wiley Publishing

[3] Purbo, Onno W, Protus Tanuhandaru dkk. 2011. *Jaringan Wireless di Dunia Berkembang. Panduan Praktis Perencanaan dan Pembangunan Infrastruktur Komunikasi yang Rendah*. Yogyakarta : Andi.

[4] Raharja , R. Anton, Afri Yunianto, Wisesa Widyantoro. 2001. *Modul Pelatihan Pengenalan Linux*.

[5] Setiawan, Arif. 2013. *Skripsi: Rancang Bangun Sistem Monitoring Ruangan Menggunakan Webcam Berbasis OpenWrt. Yogyakarta*: UIN Sunan Kalijaga

[6] Openwrt, "Techdata: Xiaomi Mi Router 4A (MIR4A) 100M," *openwrt.org* https://openwrt.org/toh/hwdata/xiaomi/xiaomi_mi_router_4a_100m (acsessed jun, 2023)

[7] Github.com "OpenWRTInvasion," *acecilia*, https://github.com/acecilia/OpenWRTInvasion (acsessed jun, 2023)