Accredited SINTA 5
72/E/KPT/2024

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 3, Juni 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

Impelementasi dan Perbandingan antara Adguardhome dan Pi-Hole sebagai Filtering Phising Menggunakan Metode Black Box

Asri Ansyah[1*], Aulia Syarif Aziz[2]
[1,2]Universitas Islam Negeri Ar-Raniry
[1,2]Jl. Syeikh Abdur Rauf, 0651-7776565 Banda Aceh
E-mail: 200212032@student.ar-raniry.ac.id[1*]

Submitted Date : 26 Mei 2025 ***Accepted Date : 01 Juni 2025***

Abstrak - Phishing merupakan salah satu bentuk kejahatan siber yang banyak terjadi dan mengancam keamanan data pribadi serta organisasi. Salah satu solusi teknis untuk mencegah akses ke situs phishing adalah penggunaan sistem penyaringan DNS (Domain Name System). Penelitian ini bertujuan untuk mengimplementasikan dan membandingkan dua perangkat lunak penyaring DNS, yaitu AdGuard Home dan Pi-hole, dalam memblokir situs phishing menggunakan metode Black Box Testing pada jaringan lokal. Metode penelitian yang digunakan adalah pendekatan kuantitatif dengan eksperimen langsung terhadap 313 URL yang terdiri dari 237 situs phishing dan 76 situs aman. Hasil pengujian menunjukkan bahwa AdGuard Home berhasil memblokir 91,56% situs phishing, dengan rata-rata waktu respons 280 ms dan tingkat akurasi 87,80%. Sementara itu, Pi-hole hanya memblokir 18,14% situs phishing, dengan waktu respons rata-rata 1106 ms dan akurasi 17,18%. Hasil penelitian menunjukkan bahwa AdGuard Home memiliki efektivitas dan akurasi yang lebih tinggi dibandingkan Pi-hole dalam memblokir situs phishing, meskipun keduanya masih memiliki kekurangan dalam hal kecepatan. Penelitian ini memberikan kontribusi dalam pemilihan solusi penyaring DNS yang optimal untuk perlindungan terhadap serangan phishing di jaringan lokal.
Kata kunci: Phishing; Penyaringan DNS; AdGuard Home; Pi-hole; Black Box Testing.

Abstract - *Phishing is one of the most common forms of cybercrime, posing a serious threat to both personal and organizational data security. One technical solution to prevent access to phishing websites is the use of Domain Name System (DNS) filtering systems. This study aims to implement and compare two DNS filtering software, AdGuard Home and Pi-hole, in blocking phishing websites using Black Box Testing within a local network. This research uses a quantitative experimental approach, testing 313 URLs consisting of 237 phishing sites and 76 safe sites. The results show that AdGuard Home successfully blocked 91.56% of phishing sites, with an average response time of 280 ms and an accuracy rate of 87.80%. In contrast, Pi-hole blocked only 18.14% of phishing sites, with an average response time of 1106 ms and an accuracy rate of 17.18%. The findings indicate that AdGuard Home outperforms Pi-hole in both effectiveness and accuracy in blocking phishing websites, although both systems show room for improvement in response speed. This study contributes to selecting the optimal DNS filtering solution for protection against phishing threats in local networks.*
Keywords: Phishing, DNS Filtering, AdGuard Home, Pi-hole, Black Box Testing
Keywords: Phishing; DNS Filtering; AdGuard Home; Pi-hole; Black Box Testing.

1. Pendahuluan

Perkembangan teknologi informasi yang pesat membawa dampak signifikan terhadap berbagai aspek kehidupan, termasuk dalam hal komunikasi, transaksi keuangan, serta akses informasi. Namun, seiring dengan manfaat tersebut, kejahatan siber turut berkembang, salah satunya adalah phishing. Phishing merupakan bentuk rekayasa sosial yang dilakukan dengan cara menyamar sebagai entitas terpercaya guna memperoleh informasi pribadi dan sensitif pengguna, seperti kata sandi dan data keuangan.

Di Indonesia, ancaman phishing telah menjadi perhatian serius. Regulasi terkait telah diatur dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) [1] dan perubahannya melalui Undang-Undang No. 19 Tahun 2016, serta diperkuat dengan Peraturan Pemerintah No. 71 Tahun 2019 [2]. Regulasi ini menegaskan pentingnya perlindungan terhadap data pribadi dan kewajiban penyelenggara sistem elektronik untuk mengamankan sistem dari ancaman siber.

Salah satu solusi teknis yang dapat digunakan untuk menangkal serangan phishing adalah dengan menerapkan teknologi penyaring DNS (Domain Name System Filtering). Penyaring DNS bekerja dengan mencegah akses pengguna ke situs berbahaya sebelum situs tersebut dimuat di perangkat. Dua aplikasi populer yang mendukung fungsi ini adalah AdGuard Home dan Pi-hole. Keduanya bersifat open-source dan dapat diimplementasikan secara lokal untuk memblokir domain berbahaya termasuk phishing dan iklan.

Meskipun kedua aplikasi tersebut memiliki fungsi utama yang serupa, penelitian yang secara langsung membandingkan efektivitas AdGuard Home dan Pi-hole dalam memblokir situs phishing masih sangat terbatas.

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 3, Juni 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

Oleh karena itu, penelitian ini bertujuan untuk mengisi kesenjangan tersebut dengan melakukan pengujian menggunakan metode Black Box Testing dalam lingkungan jaringan lokal. Penelitian ini mengukur efektivitas, kecepatan respons, dan akurasi pemblokiran dari kedua sistem sebagai dasar rekomendasi pemanfaatan teknologi DNS Filtering dalam meningkatkan keamanan jaringan dari ancaman phishing.

2. Tinjauan Pustaka

2.1. *Phishing*

Phishing merupakan salah satu bentuk serangan rekayasa sosial yang dirancang untuk mencuri informasi sensitif seperti nama pengguna, kata sandi, dan data keuangan dengan menyamar sebagai entitas terpercaya [3]. Teknik ini umumnya dilakukan melalui email, situs palsu, atau pesan instan yang tampak sah. Seiring dengan meningkatnya akses internet, phishing menjadi salah satu ancaman yang paling sering ditemui oleh pengguna, baik individu maupun institusi.

Menurut Wirachmi [4], phishing telah berkembang menjadi bentuk kejahatan siber yang semakin canggih dengan memanfaatkan kemiripan tampilan situs resmi untuk menipu pengguna. Oleh karena itu, dibutuhkan sistem keamanan yang dapat memblokir akses ke situs-situs berbahaya tersebut sebelum pengguna sempat mengaksesnya.

DNS *Filtering* adalah metode untuk membatasi akses ke situs web tertentu berdasarkan daftar domain yang telah ditentukan, dengan tujuan utama meningkatkan keamanan jaringan [5]. Saat pengguna mencoba mengakses domain yang termasuk dalam daftar blokir, server DNS akan mencegah permintaan tersebut diteruskan, sehingga situs tidak dapat dibuka.

Teknologi ini efektif dalam mencegah akses ke situs phishing, malware, iklan berbahaya, dan konten yang tidak diinginkan lainnya. DNS Filtering dapat diterapkan secara lokal menggunakan perangkat lunak seperti AdGuard Home dan Pi-hole, yang memungkinkan administrator jaringan untuk melindungi seluruh perangkat dalam jaringan tanpa harus menginstal perangkat lunak di setiap klien [6].

2.3. AdGuard Home dan Pi-hole

AdGuard Home adalah sistem penyaring DNS berbasis open-source yang dirancang untuk memblokir iklan, pelacak, dan situs berbahaya secara langsung di tingkat jaringan [7]. AdGuard Home dapat diakses melalui antarmuka web, memudahkan pengguna dalam melakukan konfigurasi dan pemantauan aktivitas DNS.

Pi-hole juga merupakan solusi penyaring DNS yang populer dan bersifat open-source. Dirancang awalnya untuk Raspberry Pi, Pi-hole berfungsi sebagai DNS sinkhole yang mampu memblokir permintaan ke domain tertentu berdasarkan daftar blokir yang ditentukan [8]. Meski memiliki fungsi serupa, perbedaan konfigurasi dan basis daftar blokir membuat efektivitas masing-masing perangkat dapat bervariasi dalam menangani phishing.

Metode Black Box Testing adalah pendekatan pengujian perangkat lunak yang berfokus pada pengamatan hasil keluaran dari serangkaian masukan tanpa mengetahui struktur internal sistem yang diuji [9]. Dalam konteks penelitian ini, metode ini digunakan untuk menguji efektivitas penyaring DNS dalam memblokir situs phishing dengan melihat hasil dari URL yang diuji apakah berhasil diblokir atau tidak. Metode ini cocok digunakan untuk membandingkan performa dari dua sistem yang berbeda tanpa memerlukan pengetahuan teknis mendalam tentang arsitektur internal perangkat lunak.

3. Metode Penelitian

3.1. Pendekatan Penelitian

Penelitian ini menggunakan metode eksperimen dengan pendekatan kuantitatif untuk membandingkan performa dua sistem penyaring DNS, yaitu AdGuard Home dan Pi-hole, dalam memblokir situs phishing pada jaringan lokal. Metode ini dipilih karena mampu memberikan data terukur berdasarkan pengujian langsung terhadap masing-masing sistem.

3.2. Lingkungan Pengujian

Pengujian dilakukan dalam jaringan lokal dengan dua skenario: DNS klien diarahkan ke server AdGuard Home dan ke server Pi-hole secara bergantian. Sistem dijalankan pada Ubuntu Server melalui VirtualBox di komputer host. Komputer klien dan smartphone digunakan sebagai perangkat uji akses situs phishing.

3.3. Prosedur Implementasi

Langkah-langkah implementasi meliputi:

1. Instalasi dan konfigurasi AdGuard Home dan Pi-hole pada server Ubuntu.
2. Pengaturan DNS komputer klien menuju IP masing-masing server filtering.
3. Akses terhadap 313 situs (237 situs phishing dan 76 situs aman) menggunakan browser secara manual.
4. Pemantauan dan pencatatan hasil akses (berhasil diblokir atau tidak) menggunakan Wireshark dan log sistem.

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 3, Juni 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

3.4. Parameter Evaluasi

Tiga indikator utama yang digunakan dalam pengujian:

a. Efektivitas: Persentase situs phishing yang berhasil diblokir.
b. Kecepatan Respon: Waktu rata-rata pemrosesan DNS saat akses situs.
c. Akurasi: Tingkat kesalahan sistem dalam memblokir situs aman (false positive) dan tidak memblokir situs phishing (false negative).

Rumus evaluasi yang digunakan antara lain [10] :

a. $\text{Efektivitas (\%)} = \frac{\text{Jumlah situs phishing yang diblokir}}{\text{Total situs phishing}} \times 100\%$
b. $\text{Rata-rata Waktu Respon (ms)} = \frac{\text{Total waktu respon}}{\text{Jumlah permintaan situs phishing}}$
c. $\text{Akurasi (\%)} = \frac{TP+TN}{TP+TN+FP+FN} \times 100\%$

Dengan keterangan:

a. TP: True Positive (phishing diblokir),
b. TN: True Negative (aman tidak diblokir),
c. FP: False Positive,
d. FN: False Negative.

3.5. Alat dan Bahan

Table 1. alat dan bahan

No	Alat/Bahan	Spesifikasi/Keterangan
1.	Server	Ubuntu Server 24.04 LTS di VirtualBox
2.	Klien	Laptop dan DNS diarahkan ke server filtering
3.	AdGuard Home	Versi 0.107.53
4.	Pi-hole	Versi v5.18.3
5.	Wireshark	Versi 4.4.1
6.	Daftar situs phishing	Diambil dari URLHaus
7.	Putty	Remote SSH

4. Hasil dan Pembahasan

Implementasi dilakukan dengan menginstal AdGuard Home dan Pi-hole secara bergantian pada satu server Ubuntu di VirtualBox. IP server dikonfigurasi statis agar dapat diakses oleh klien. Pengujian dilakukan dengan mengarahkan DNS perangkat klien ke IP server filtering, lalu mengakses 313 URL yang terdiri dari 237 situs phishing dan 76 situs aman. Hasil akses, waktu respon DNS, dan status blokir dicatat menggunakan log aplikasi dan Wireshark.

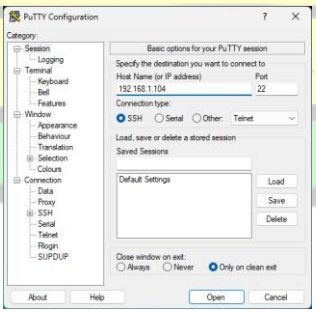
4.1. Hasil Implementasi

Pada tahap ini dilakukan instalasi dan konfigurasi AdGuardHome dan Pi-hole pada perangkat ubuntu server yang berada di VirtualBox yang terinstall di komputer host. Berikut adalah tahapan-tahapan cara pengimplementasinya.

4.1.1 Implementasi AdGuard Home

1. Login Putty

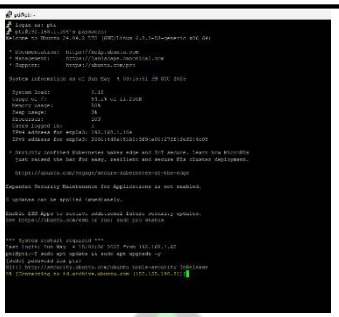
Putty digunakan untuk login ubuntu server via SSH caranya login putty dengan alamat IP ubuntu server, untuk mengetahui IP nya ketikkan perintah (ip a), lalu buka putty dan masukkan IP ubuntu servernya 192.168.1.104, port 22, lalu tekan *open*.



Gambar 1. Putty

2. Perbarui sistem

Setelah berhasil masuk ke ubuntu server via SSH Putty, perbarui sistem perangkat lunak ubuntu dengan perintah "sudo apt update && sudo apt upgrade -y" lalu enter.

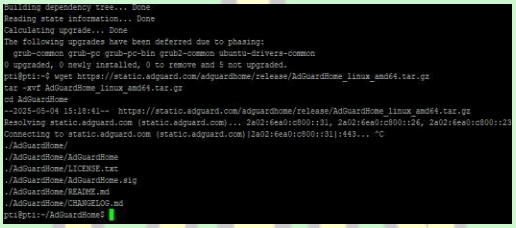


Gambar 2. Perbarui system

3. Unduh Adguardhome

Untuk mengunduh Adguardhome gunakan perintah sebagai berikut pada ubuntu server lalu ubuntu akan mengunduh, dan mengekstrak *AdGuard Home* secara otomastis.

Wget https://static.adguard.com/adguardhome/release/AdGuardHome_linux_amd64.tar.gz
tar -xvf AdGuardHome_linux_amd64.tar.gz
cd AdGuardHome

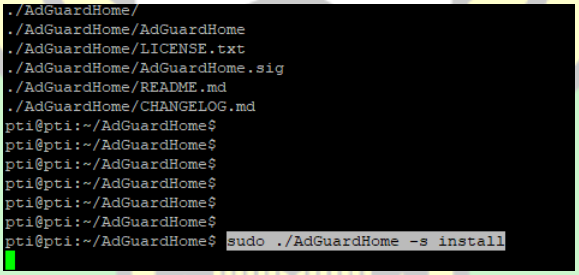


Gambar 3. Unduh dan Ekstrak AdGuardHome

4. Pemasangan *AdguardHome*

Setelah mengunduh *AdguardHome* perlu dilakukan pemasangan atau penginstallan, Untuk pemasang *AdguardHome* masukkan perintah berikut.

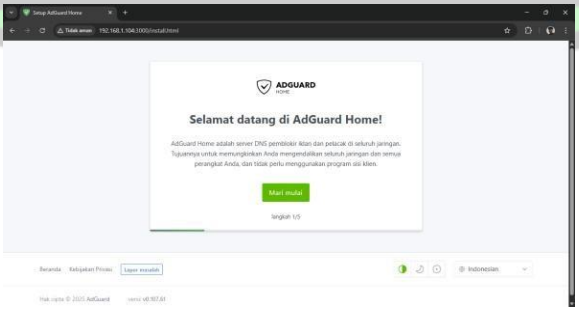
Sudo ./AdGuardHome -s install



Gambar 4. Pemasangan AdguardHome

5. Antarmuka *AdguardHome*

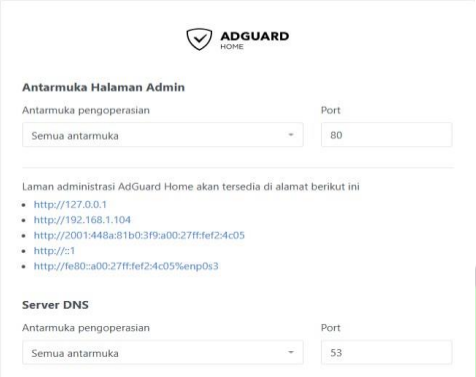
Untuk pengaturan lanjutan *AdguardHome*, perlu untuk mengakses *Web Interface AdguardHome* dengan menggunakan *Browser* pada perangkat komputer penguji, dengan memasukkan alamat IP dan port bawaan *AdguardHome* seperti berikut. http://192.168.1.104:3000



Gambar 5. Antarmuka awal AdguardHome

6. Pengaturan *AdguardHome*

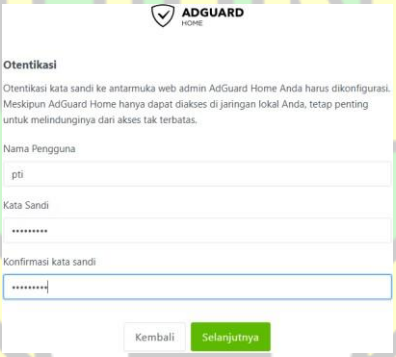
Setelah masuk pada antarmuka halaman admin dilanjutkan dengan mengatur IP dan port yang akan digunakan sebagai alamat akses nya, dengan memilih interface dan port (DNS: 53, UI: 3000).



Gambar 6. IP dan port AdguardHome

7. Nama pengguna dan kata sandi

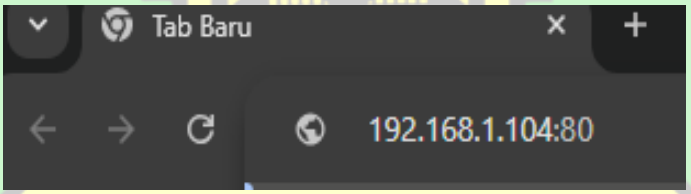
Buat nama pengguna dan kata sandi yang akan digunakan untuk login admin, lalu dilanjutkan dengan mengkonfirmasi kata sandi, lalu tekan tombol selanjutnya.



Gambar 7. Atur kata sandi *Adguardhome*

8. Akses antarmuka *AdguardHome*

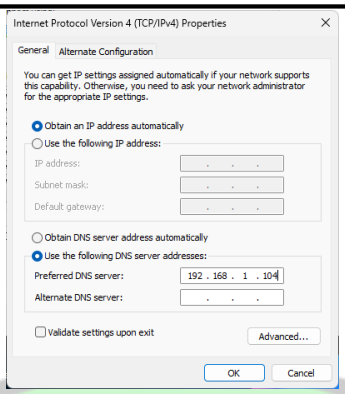
Untuk melihat antarmuka Adguardhome harus memasukkan alamat IP server tempat pemasangan, dan diikuti dengan port yang dipisahkan dengan titikdua (:).



Gambar 8. IP dan Port Adguardhome

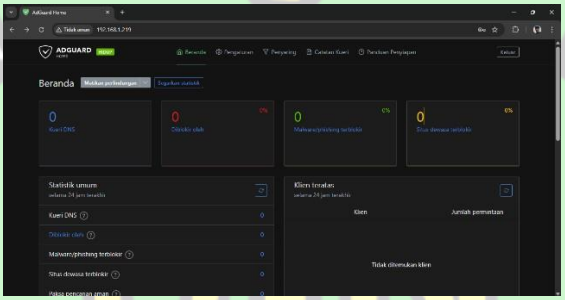
9. Menambah klien

Untuk menambah klien pada AdguardHome maka harus merubah DNS pada *"Internet Protocol Version 4 (TCP/Ipv4)"* bawaan menjadi IP Adguardhome, pilih baris yang bertuliskan *"use the following DNS server addresses"* lalu isi IP *AdguardHome* pada menu *"preferred DNS server:"*



Gambar 9. *Internet Protocol Version 4*

10. Antarmuka AdguardHome

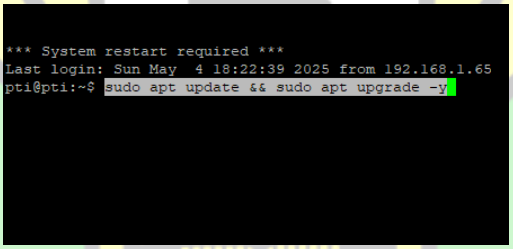


Gambar 10. Antarmuka adguardhome

4.1.2 Implementasi Pi-hole

1. Perbarui sistem

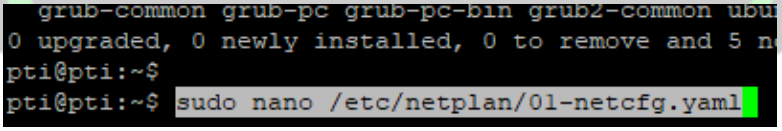
Seperti pada AdguardHome sebelum menginstall Pihole juga harus memperbarui sistem pada ubuntu server, dengan perintah yang sama sudo apt update && sudo apt upgrade -y



Gambar 11.Update Ubuntu Server

2. IP Statis

Alamat IP statis digunakan karena komputer memerlukan DNS yang tetap dan tidak berubah-ubah, untuk menetapkan IP statis diperlukan sedikit perubahan pada file konfigurasi jaringan, gunakan perintah "sudo nano /etc/netplan/01-netcfg.yaml" untuk membuka file konfigurasi jaringan.



Gambar 12. Membuka file konfigurasi jaringan

3. Edit file konfigurasi jaringan

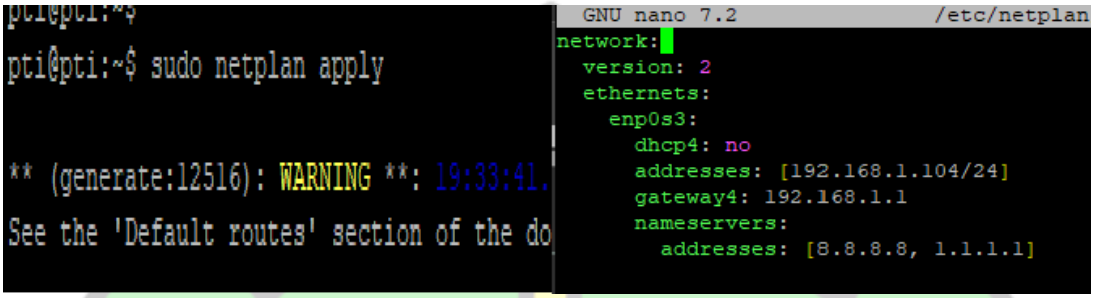
Setelah membuka file konfigurasi jaringan masukkan pengaturan IP statis pada file tersebut, lalu simpan dan keluar, setelah keluar jalankan dengan perintah sudo netplan apply

Contoh konfigurasi:

network:

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 3, Juni 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

```
version: 2
ethernets:
  enp0s3:
    dhcp4: no
    addresses: [192.168.1.104/24]
    gateway4: 192.168.1.1
    nameservers:
      addresses: [8.8.8. 8, 1.1.1.1]
```

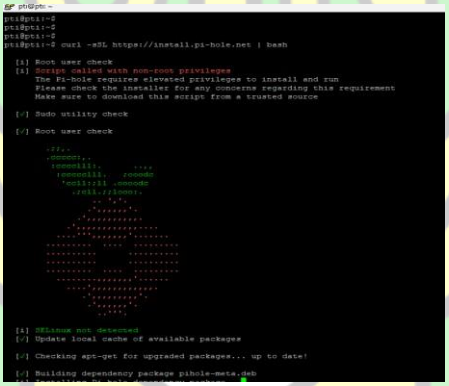


Gambar 13. Konfigurasi IP Statis

4. Instalasi Pi-hole

Pemasangan Pihole pada ubuntu server juga menggunakan perintah atau *command* yang di ketikkan pada halaman ubuntu server, masukkan perintah dan jalankan dengan tombol *enter*, pihole akan mengunduh secara otomatis.

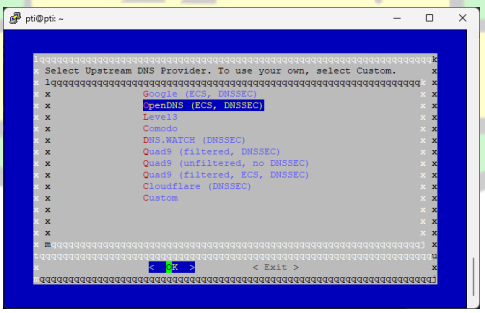
curl -sSL https://install.pi-hole.net | bash



Gambar 14. Instalasi awal *Pi-hole*

5. Memilih DNS upstream

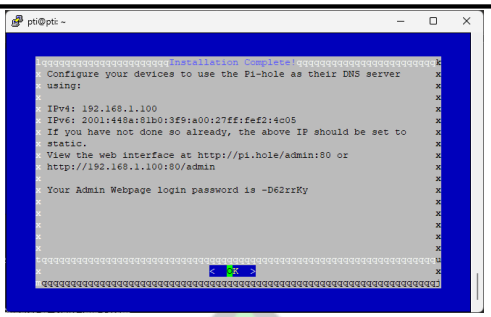
Pilih google kemudian tekan *enter*.



Gambar 15. DNS upstream

6. Kata sandi Pihole

Pi-hole menampilkan kata sandi *default* antarmuka admin yang akan digunakan untuk masuk ke antarmuka Pi-hole nantinya.

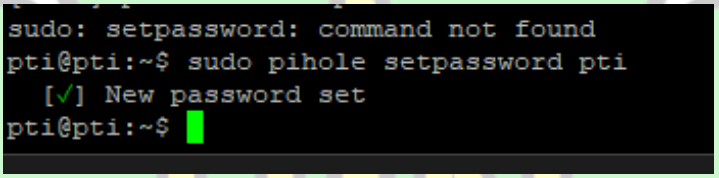


Gambar 16. Kata sandi default pihole

7. Ganti kata sandi pihole

Ganti kata sandi Pihole menggunakan sandi yang mudah user ingat menggunakan perintah *Sudo pihole setpassword* (isi sandi) misalnya

Sudo pihole setpassword pti



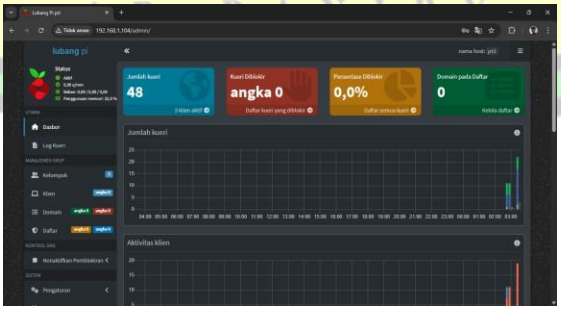
Gambar 17. ganti sandi Pi-hole

8. Akses antarmuka pihole

Buka peramban internet pada komputer klien lalu masukkan alamat IP pihole dan garis miring (/) admin untuk mengakses antarmuka web dari Pi-hole (http://192.168.1.104/admin), masuk menggunakan kata sandi yang sudah diperbarui.

Gambar 18. antarmuka login Pihole

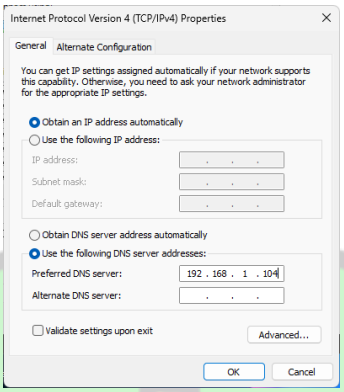
9. Antarmuka Pihole



Gambar 19. antarmuka web admin Pi-hole

10. Ubah DNS perangkat klien

Mengganti DNS server komputer klien menjadi DNS pihole (192.168.1.104), dapat juga mengubah manual diperangkat Atau diatur di router seperti *AdguardHome* agar semua perangkat menggunakan Pi-hole.



Gambar 20. Ganti DNS

4.2. Hasil Pengujian Black Box

Penelitian dilakukan untuk mengetahui seberapa baik dua alat, yaitu AdGuard Home dan Pi-hole, dalam memblokir situs berbahaya (phishing) dan memastikan situs yang aman tetap bisa diakses. Pengujian dilakukan dengan mencoba 313 tautan, yang terdiri dari 237 tautan phishing (situs berbahaya) dan 76 tautan aman. Kedua alat diuji di jaringan lokal yang sama agar hasilnya adil. Sebelum penerapan AdGuard Home dan Pi-hole, seluruh tautan dalam daftar, baik yang termasuk situs aman maupun situs phishing, dapat diakses tanpa hambatan. Ini berarti bahwa tidak ada sistem pemblokiran yang aktif sebelumnya. Data ini menjadi tolak ukur awal (baseline) yang penting untuk membandingkan kinerja pemblokiran setelah sistem DNS filtering diaktifkan. Pengujian dilakukan dengan cara mengakses sejumlah situs phishing dari komputer client yang DNS-nya diarahkan ke IP server (yang menjalankan AdGuard Home atau Pi-hole). Pengujian menggunakan daftar situs phishing yang aktif berdasarkan URLHaus.

4.2.1 Hasil Pengujian dengan AdGuard Home

AdGuard Home menunjukkan hasil yang sangat baik. Dari 237 situs phishing yang diuji, 217 berhasil diblokir, sedangkan 26 masih lolos dan bisa diakses. Untuk situs yang seharusnya aman, dari 76 tautan, 70 bisa dibuka dengan benar, tapi 6 situs aman salah diblokir. Rata-rata waktu yang dibutuhkan AdGuard Home untuk merespons adalah 280 milidetik, yang tergolong lambat menurut kriteria dalam penelitian (di atas 200 ms). Secara keseluruhan, tingkat keberhasilan AdGuard Home dalam memblokir situs phishing adalah 91,56%, dan tingkat ketepatannya dalam mengenali situs berbahaya dan aman adalah 87,80%.

Tabel 1. Hasil Pengujian AdGuard Home

No.	Alamat Website	Label	Status Akses	Hasil Evaluasi
1	https://facebook.com	Aman	Bisa diakses	Benar - Akses Aman
2	https://instagram.com	Aman	Bisa diakses	Benar - Akses Aman
3	https://telegram.org	Aman	Bisa diakses	Benar - Akses Aman
4	https://tiktok.com	Aman	Bisa diakses	Benar - Akses Aman
5	https://twitter.com	Aman	Tidak bisa diakses (Kode 400)	Salah - Website Aman Diblokir
…	...	...	...	...
309	http://booking.hotel-id2046.com	Phishing	Diblokir	Benar - Phishing Diblokir
310	http://mateusz.rkusidlos.pl	Phishing	Diblokir	Benar - Phishing Diblokir
311	http://olx-pl.numerid045439702478.click	Phishing	Diblokir	Benar - Phishing Diblokir
312	http://olx-pl.alsde.lol	Phishing	Diblokir	Benar - Phishing Diblokir
313	http://gridveil.online	Phishing	Diblokir	Benar - Phishing Diblokir

Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)
Vol. 8 No. 3, Juni 2025
P-ISSN 2620-8342
E-ISSN 2621-3052

4.2.2 Hasil Pengujian dengan Pi-hole

Hasil yang diperoleh dari Pi-hole menunjukkan bahwa kinerjanya masih berada di bawah AdGuard Home dalam hal efektivitas pemblokiran dan identifikasi situs phishing. Dari 237 situs phishing, hanya 43 yang berhasil diblokir, dan 194 situs berbahaya lolos. Untuk situs yang aman, 72 bisa diakses dengan benar, sementara 4 salah diblokir. Waktu rata-rata untuk merespons dari Pi-hole adalah 1106 milidetik, yang juga termasuk kategori lambat. Tingkat keberhasilan Pi-hole dalam memblokir situs phishing hanya 18,14%, dan tingkat ketepatannya hanya 17,18%.

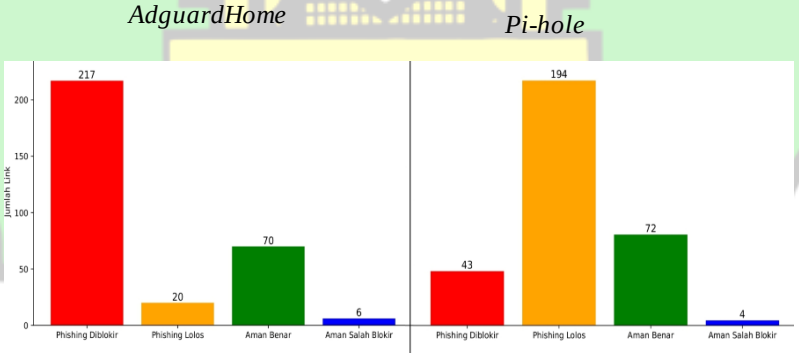
Tabel 2. Hasil Pengujian dengan Pi-hole

No.	Alamat Website	Label	Status Akses	Hasil Evaluasi
1	https://facebook.com	Aman	Bisa diakses	Benar - Akses Aman
2	https://instagram.com	Aman	Bisa diakses	Benar - Akses Aman
3	https://telegram.org	Aman	Bisa diakses	Benar - Akses Aman
4	https://tiktok.com	Aman	Bisa diakses	Benar - Akses Aman
5	https://twitter.com	Aman	Tidak bisa diakses (Kode 400)	Salah - Website Aman Diblokir
…	...	...	...	...
309	http://booking.hotel-id2046.com	Phishing	Bisa diakses	Salah - Phishing Tidak Diblokir
310	http://mateusz.rkusidlos.pl	Phishing	Bisa diakses	Salah - Phishing Tidak Diblokir
311	http://olx-pl.numerid045439702478.click	Phishing	Bisa diakses	Salah - Phishing Tidak Diblokir
312	http://olx-pl.alsde.lol	Phishing	diblokir	Benar - Phishing Diblokir
313	http://gridveil.online	Phishing	Bisa diakses	Salah - Phishing Tidak Diblokir

4.3. Pembahasan

Berdasarkan hasil pengujian, AdGuard Home terbukti memiliki kinerja yang secara signifikan lebih unggul dibandingkan Pi-hole dalam hal memblokir situs phishing serta mengidentifikasi situs yang aman. Dari 237 situs phishing, AdGuard Home berhasil memblokir 217 situs (91,56%) dan hanya salah memblokir 6 dari 76 situs aman (akurasi 87,80%). Meskipun memiliki waktu respons 280 ms yang sedikit lambat menurut standar penelitian, performanya masih dapat diterima dalam penggunaan sehari-hari. Sebaliknya, Pi-hole hanya mampu memblokir 43 dari 237 situs phishing (18,14%), dan salah memblokir 4 dari 76 situs aman (akurasi 17,18%). Waktu responsnya jauh lebih lambat, yaitu 1106 ms, yang mengindikasikan kinerja yang kurang optimal baik dari sisi efektivitas maupun efisiensi. Secara umum, AdGuard Home menunjukkan performa yang lebih baik dan layak direkomendasikan sebagai solusi penyaringan DNS untuk melindungi jaringan dari ancaman phishing, baik bagi pengguna individu maupun organisasi. Namun, masih terdapat kebutuhan untuk meningkatkan kecepatan responsnya.

Tabel 2. Hasil Pengujian Pihole



Gambar 21. Grafik perbandingan adguardhome dan pihole

5. Kesimpulan

Temuan-temuan dari penelitian ini menunjukkan bahwa AdGuard Home memiliki tingkat efektivitas yang tinggi dalam memblokir situs phishing, dengan persentase keberhasilan sebesar 91,56%, akurasi 87,80%, dan waktu respon rata-rata 280 ms. Pi-hole menunjukkan performa yang jauh lebih rendah, hanya mampu memblokir 18,14% situs phishing dengan akurasi 17,18% dan waktu respon rata-rata 1106 ms. AdGuard Home

lebih direkomendasikan sebagai solusi penyaring DNS untuk keperluan perlindungan jaringan lokal dari serangan phishing, terutama di lingkungan rumah, kantor kecil, atau institusi pendidikan. Kelemahan utama pada kedua sistem terletak pada waktu respon DNS yang belum memenuhi kategori ideal (<200 ms), sehingga perlu dilakukan optimasi lebih lanjut. Penelitian ini memberikan dasar evaluatif dalam memilih perangkat lunak penyaring DNS dan membuka peluang untuk pengembangan studi lanjutan terkait integrasi daftar blokir pihak ketiga, serta pengujian pada infrastruktur jaringan yang lebih kompleks.

Daftar Pustaka

[1] Republik Indonesia, "Undang-Undang tentang Informasi dan Transaksi Elektronik," *Bi.Go.Id*, no. September, pp. 1–2, 2008, [Online]. Available: https://peraturan.bpk.go.id/Home/Details/37589/uu-no-11-tahun-2008

[2] I. Firdaus, "Implementasi Kebijakan E-KTP di Kecamatan Jiput Kabupaten Pandeglang," pp. 1–162, 2019, [Online]. Available: http://eprints.untirta.ac.id/1438/

[3] M. Yazid, "Cyber Crime Dengan Metode Phising," Sitkom. Accessed: Dec. 03, 2023. [Online]. Available: https://www.scribd.com/doc/293156943/Cyber-Crime-Dengan-Metode-Phising

[4] L. M. Ajeng Wirachmi, "Mengenal Sejarah Phising yang Lahir Sejak 1996." Accessed: Dec. 05, 2023. [Online]. Available: https://ekbis.sindonews.com/read/831919/178/mengenal-sejarah-phising-yang-lahir-sejak-1996-1658311647

[5] R. Mujiastuti and I. Prasetyo, "Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE," *J. Tek. Inform.*, no. November 2021, pp. 1–10, 2021, [Online]. Available: www.google.com

[6] Adguard, "AdGuard Home," Adguard.com. Accessed: Oct. 29, 2024. [Online]. Available: https://adguard.com/en/welcome.html

[7] idcloudhost.com, "Mengenal Pi-hole: Pengertian, Cara Kerja, dan Fungsinya," idcloudhost. Accessed: Oct. 15, 2024. [Online]. Available: https://idcloudhost.com/blog/apa-itu-pi-hole/?form=MG0AV3

[8] Pi-hole, "Pi-hole," pi-hole.net. Accessed: Oct. 29, 2024. [Online]. Available: https://pi-hole.net/landing/blog/

[9] R. B. Trengginaz, A. Yusup, D. S. Sunyoto, M. R. Jihad, and Y. Yulianti, "Pengujian Aplikasi Pemesanan Tiket Kereta berbasis Website Menggunakan Metode Black Box dengan Teknik Equivalence Partitioning," *J. Teknol. Sist. Inf. dan Apl.*, vol. 3, no. 3, p. 144, 2020, doi: 10.32493/jtsi.v3i3.5349.

[10] A. Setiawan *et al.*, "ANALISIS DISTRIBUSI RATA-RATA WAKTU RESPON APLIKASI BERBASIS WEB MENGGUNAKAN KURVA NORMAL DAN SIMPANGAN BAKU," vol. 9, no. 1, pp. 211–216, 2025.