IJINF (Internal Journal of Informatics)

Evaluasi Efektivitas Hardening dalam Meningkatkan Keamanan Sistem Operasi Windows dan Linux

Supriyanto[1], Ahmad Rafi Kannajmi[2], Dicky Saputra[3]
[1,2,3]Department of Informatics, Universitas Sultan Ageng Tirtayasa

Article Info

Article history:

Received June 21, 2025
Revised August 13, 2025
Accepted August 17, 2025

Keywords:

Hardening
Sistem Operasi
Keamanan Jaringan
Linux
Windows

ABSTRAK

Perkembangan ancaman siber menuntut penerapan strategi keamanan yang proaktif, khususnya pada sistem operasi sebagai target utama eksploitasi. Penelitian ini bertujuan mengevaluasi efektivitas teknik hardening pada sistem operasi Windows dan Linux melalui pendekatan eksperimental. Pada sistem Linux, teknik hardening dilakukan dengan konfigurasi SSH, implementasi Fail2Ban, dan pengaturan IPTables sebagai firewall. Sementara pada Windows, diterapkan fitur Controlled Folder Access dan konfigurasi Windows Defender Firewall. Evaluasi dilakukan dengan simulasi serangan untuk mengukur tingkat keamanan sebelum dan sesudah hardening. Hasil penelitian menunjukkan bahwa hardening mampu menurunkan tingkat kerentanan sistem secara signifikan. Linux berhasil memblokir akses tidak sah melalui SSH dan lalu lintas IP yang mencurigakan, sedangkan Windows mampu mendeteksi dan mengkarantina malware serta memblokir akses ke situs tertentu. Temuan ini menegaskan bahwa penerapan hardening yang tepat dapat meningkatkan ketahanan sistem terhadap ancaman siber, serta menjadi acuan dalam penguatan kebijakan keamanan TI di berbagai lingkungan operasional.

Corresponding Author:

Czidni Sika Azkia,
Informatics Department, Faculty of tehnik, Universitas Sultan Ageng Tirtayasa

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mengubah berbagai aspek kehidupan manusia, mulai dari aktivitas sehari-hari hingga operasional bisnis dan pemerintahan. Di balik kemudahan yang ditawarkan oleh digitalisasi, terdapat tantangan besar yang mengintai, yakni risiko keamanan siber. Ancaman seperti *malware*, *ransomware*, *brute-force attack*, *privilege escalation*, hingga *Distributed Denial of Service (DDoS)* semakin meningkat dari waktu ke waktu. Laporan dari berbagai lembaga keamanan menunjukkan bahwa sistem operasi merupakan salah satu titik kritis yang paling sering dieksploitasi oleh pelaku serangan siber. Sistem operasi (Operating System/OS) adalah perangkat lunak fundamental yang mengelola perangkat keras dan perangkat lunak lain dalam suatu sistem komputer. Sebagai inti dari pengelolaan sistem, OS menjadi target utama bagi serangan siber. Sistem operasi yang tidak dikonfigurasi dengan benar atau masih menggunakan pengaturan default sangat rentan terhadap eksploitasi. Oleh karena itu, pendekatan proaktif dalam penguatan sistem operasi merupakan kebutuhan mendesak dalam upaya mempertahankan integritas dan ketersediaan data serta sistem.

Salah satu strategi penting dalam menjaga keamanan sistem operasi adalah dengan menerapkan teknik *system hardening*. Hardening merujuk pada serangkaian tindakan yang bertujuan untuk memperkuat sistem terhadap berbagai jenis ancaman siber, dengan cara mengurangi permukaan serangan. Ini dilakukan melalui berbagai metode, seperti menonaktifkan layanan yang tidak

diperlukan, membatasi akses pengguna, mengatur firewall, memperketat otentikasi, serta memperbarui sistem secara berkala. Implementasi hardening sangat bergantung pada jenis sistem operasi yang digunakan. Windows dan Linux adalah dua sistem operasi yang dominan digunakan dalam infrastruktur teknologi informasi. Keduanya memiliki arsitektur dan pendekatan keamanan yang berbeda. Windows, dengan GUI yang terintegrasi dan pengelolaan terpusat melalui Group Policy, banyak digunakan dalam lingkungan korporasi. Di sisi lain, Linux dengan sifat open-source dan fleksibilitas konfigurasinya lebih umum digunakan pada server dan sistem kritis. Meskipun keduanya memiliki keunggulan masing-masing, keduanya tetap memerlukan proses hardening agar dapat beroperasi dengan aman di tengah meningkatnya ancaman digital.

Beberapa penelitian terdahulu telah menunjukkan bahwa penerapan *hardening* secara signifikan dapat meningkatkan postur keamanan suatu sistem. Dalam konteks Linux, implementasi firewall seperti IPTables, penguatan akses SSH, dan penggunaan tools seperti Fail2Ban telah terbukti mengurangi risiko serangan. Begitu pula dengan Windows, pengaturan kebijakan keamanan lokal dan grup, serta konfigurasi port dan layanan dapat memperkuat sistem dari dalam. Namun, masih diperlukan studi komparatif yang mengevaluasi efektivitas hardening pada kedua sistem ini secara sistematis dan berdasarkan pendekatan eksperimen yang valid. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengevaluasi efektivitas implementasi teknik hardening pada sistem operasi Windows dan Linux. Evaluasi dilakukan dengan membandingkan kondisi keamanan sistem sebelum dan sesudah dilakukan hardening, menggunakan parameter seperti jumlah port terbuka, jumlah layanan aktif, serta tingkat kerentanan yang terdeteksi melalui alat audit keamanan. Dengan pendekatan eksperimen, penelitian ini diharapkan dapat memberikan kontribusi dalam pemahaman strategi keamanan sistem operasi serta menjadi rujukan dalam penerapan kebijakan keamanan yang lebih baik di masa depan. Tujuan khusus dari penelitian ini adalah untuk menganalisis proses hardening yang sesuai pada sistem operasi Windows dan Linux, mengukur efektivitas hardening melalui pengujian dan simulasi serangan, membandingkan tingkat keamanan sistem sebelum dan sesudah proses hardening, serta memberikan rekomendasi praktik terbaik dalam implementasi hardening pada kedua platform tersebut. Penelitian ini memiliki urgensi yang tinggi di tengah meningkatnya digitalisasi layanan dan kebutuhan akan sistem yang tahan terhadap serangan. Hasil dari penelitian ini diharapkan dapat memperkaya literatur keamanan siber serta membantu praktisi TI dalam menyusun strategi penguatan sistem yang tepat dan kontekstual.

2. TINJAUAN PUSTAKA

2.1. Keamanan Sistem Operasi

Keamanan sistem operasi merupakan aspek mendasar dalam menjaga kestabilan dan integritas sistem teknologi informasi. Sistem operasi, baik Windows maupun Linux, menjadi sasaran utama serangan karena perannya yang sangat sentral dalam mengelola seluruh proses komputasi. Oleh karena itu, penguatan keamanan sistem operasi mutlak diperlukan sebagai upaya preventif terhadap potensi eksploitasi. Keamanan sistem operasi mencakup berbagai lapisan, mulai dari manajemen pengguna, kontrol akses file, pengaturan layanan jaringan, hingga mekanisme enkripsi dan autentikasi. Dalam konteks modern, pendekatan terhadap keamanan sistem harus bersifat menyeluruh, tidak hanya berbasis teknologi, tetapi juga melibatkan prosedur administratif dan audit berkala guna memastikan sistem tetap dalam kondisi optimal dan minim kerentanan.

2.2. Hardening Sistem Operasi

Hardening merupakan proses penguatan sistem operasi dengan cara menonaktifkan layanan yang tidak diperlukan, membatasi akses, serta menerapkan konfigurasi keamanan yang ketat. Tujuan utama hardening adalah mengurangi permukaan serangan dengan meminimalkan celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Proses ini melibatkan identifikasi terhadap komponen yang rentan, analisis risiko, implementasi solusi keamanan, dan pemantauan berkelanjutan. Dalam praktiknya, hardening dapat dilakukan melalui berbagai teknik seperti

pembatasan akses root, penerapan otentikasi berbasis kunci, penghapusan aplikasi yang tidak digunakan, serta konfigurasi firewall dan sistem deteksi intrusi.

2.3. Perbandingan Keamanan Windows dan Linux

Linux merupakan sistem operasi berbasis open-source yang banyak digunakan untuk server dan infrastruktur TI berskala besar. Kelebihan Linux terletak pada kestabilan, efisiensi sumber daya, serta kemampuan kustomisasi yang tinggi. Linux menyediakan kontrol penuh terhadap sistem, mulai dari pengelolaan layanan, file sistem, hingga keamanan jaringan. Salah satu distribusi yang umum digunakan dalam penelitian dan industri adalah Ubuntu, yang menawarkan kemudahan dalam instalasi dan penggunaan, namun tetap mempertahankan fleksibilitas pengaturan. Di sisi lain, Windows adalah sistem operasi komersial yang banyak digunakan dalam lingkungan desktop dan enterprise. Windows menawarkan antarmuka grafis yang ramah pengguna serta dukungan luas terhadap berbagai aplikasi bisnis. Namun, dari sisi keamanan, Windows memiliki tantangan tersendiri karena secara default banyak layanan berjalan secara otomatis dan membuka port yang tidak selalu dibutuhkan. Oleh karena itu, hardening sistem Windows memerlukan pendekatan berbeda, khususnya melalui pengaturan Group Policy, kontrol firewall bawaan, dan pembatasan user access control.

2.4. VirtualBox

Virtualisasi merupakan teknologi inovatif yang memungkinkan penggunaan sumber daya komputasi secara lebih efisien [1]. Konsep dari virtualisasi sendiri berkembang untuk meminimalisir penggunaan server fisik dengan cara melakukan konversi sumber daya komputasi menjadi bentuk virtual [2]. secara fundamental, virtualisasi memungkinkan pengguna untuk menjalankan beberapa sistem operasi pada waktu yang bersamaan, serta dapat meningkatkan efisiensi penggunaan perangkat keras dan sumber daya komputasi [3]. Oracle VM VirtualBox merupakan perangkat lunak virtualisasi terkemuka yang memungkinkan pengguna untuk mengeksekusi sistem operasi tambahan di dalam sistem operasi utama [1]. Sebagai hypervisor tipe 2, VirtualBox dirancang untuk berbagai keperluan, termasuk server, desktop, dan sistem embedded [2]. Teknologi ini memungkinkan pengguna untuk menjalankan sistem operasi seperti Windows, Mac OS, Linux, atau Oracle Solaris dalam lingkungan virtual tanpa perlu menginstall ulang sistem operasi tersebut di komputer [3]. Manfaat utama virtualisasi mencakup sentralisasi tugas administratif, peningkatan skalabilitas, dan kemampuan dalam melakukan pengujian jaringan secara aman sebelum melakukan implementasi fisik. VirtualBox menawarkan keunggulan seperti kemampuan menjalankan beberapa sistem operasi bersamaan, fitur snapshot, dan mendukung riset teknologi dengan risiko minimal [4]. Teknologi ini secara signifikan membantu profesional IT dalam merancan, menguji, dan mengoptimalkan infrastruktur jaringan komputer.

2.5. Secure Shell (SSH)

Secure Shell (SSH) adalah protokol jaringan kunci yang dirancang untuk menghadirkan komunikasi terenkripsi dan aman antara dua sistem komputer [5]. Berbeda dengan protokol tradisional seperti telnet yang hanya menggunakan plain text, SSH menyediakan mekanisme enkripsi yang cukup komprehensif untuk melindungi pertukaran data. Protokol SSH ini secara khusus dikembangkan untuk menggantikan layanan sistem berbasis Unix/Linux yang rentan terhadap intersepsi data [6]. Fungsi utama Secure Shell mencakup hal seperti akses remote, pengendalian, dan manajemen perangkat jaringan secara aman. Implementasi dari Secure Shell ini biasanya menggunakan arsitektur client/server dengan enkripsi kunci publik dan privat, mirip seperti konsep pengiriman surat rahasia melalui pos-pos. Mekanisme keamanan ini dapat memastikan bahwa hanya penerima yang memiliki kunci yang dapat mengakses informasi yang dikirimkan [6]. Secure Shell menawarkan keunggulan signifikan dalam keamanan jaringan, dengan enkripsi menyeluruh selama komunikasi, autentikasi aman untuk akses remote, dan perlindungan data sensitif dari intersepsi. Implementasi Secure Shell yang paling populer adalah OpenSSH, yang mana akan digunakan pada penelitian kali ini sebagai salah satu teknik dalam proses hardening server. OpenSSH sendiri biasanya telah terintegrasi dalam berbagai distribusi Linux.

2.6. Fail2Ban

Fail2Ban merupakan aplikasi atau tools keamanan jaringan yang dirancang untuk mencegah upaya bruteforce atau login yang berulang dan mencurigakan pada sistem server Linux [7][8]. Fail2Ban

ini bekerja dengan melakukan monitor berbagai protokol-protokol seperti SSH, HTTP, dan SMTP, dengan fokus utamanya pada pengamanan daemon SSH yang biasanya berjalan secara terus-menerus [8]. Mekanisme cara kerja dari Fail2Ban sendiri yaitu, melibatkan pemantauan login gagal dan pemberian sanksi berupa pemblokiran alamat IP yang melakukan percobaan brute force atau melakukan banyaknya login secara berulang kali. Secara teknis, Fail2Ban mengubah aturan konfigurasi firewall berdasarkan pola dari deteksi intrusi (IDS) yang telah ditentukan, sehingga mampu meminimalisir potensi serangan dari luar jaringan [7]. Salah satu fitur utamanya adalah Fail2Ban akan melakukan identifikasi dan memblokir alamat IP dicurigai melakukan percobaan login yang tidak sah, dengan batasan default yaitu tidak lebih dari 3 kali percobaan login.

2.7. IPTables

IPTables merupakan suatu modul keamanan sistem dalam sistem operasi Linux yang berfungsi sebagai firewall dan pengatur lalu lintas jaringan [9][10]. Sebagai tools filter jaringan, IPTables mampu mengontrol lalu lintas data yang masuk, keluar dan melewati komputer dengan dukungan pada OSI Layer 7 Application Layer, Layer 4 Transport Layer, dan Layer 3 Network Layer [9]. Sistem IPTables ini memiliki tiga chain utama yaitu, proses masuk (INPUT), proses keluar (OUTPUT), dan proses routing paket jaringan (FORWARD), serta memungkinkan pembentukan kebijakan keamanan berdasarkan sekumpulan peraturan yang spesifik [9][10]. Lebih lanjut lagi, IPTables dapat dimanfaatkan dalam mencegah serangan DDoS, memantau aktivitas keluar masuknya jaringan yang mencurigakan, serta melindungi infrastruktur sistem server dari potensi ancaman keamanan siber [9][11].

2.7. Firewall

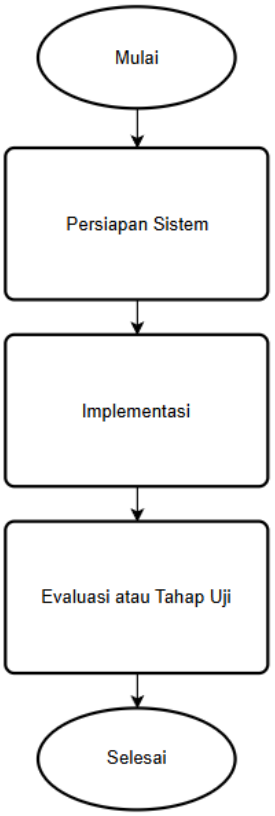
Firewall ialah sistem atau perangkat keamanan jaringan komputer yang berperan sangat kritis dalam mengontrol dan memfilter lalu lintas data jaringan [9][10]. Fungsi utama dari firewall sendiri yaitu untuk mengizinkan lalu lintas jaringan yang dianggap aman dan mencegah akses dari sumber yang tidak terpercaya [10]. Secara arsitektural, firewall dapat ditempatkan pada berbagai titik jaringan, seperti di antara internet dan router, di antara jaringan lokal dan server, atau bahkan pada komputer pribadi [9].

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental dengan tahapan utama: perancangan, implementasi, dan evaluasi teknik hardening pada sistem operasi Windows dan Linux. Pada sistem Linux, teknik yang diterapkan meliputi konfigurasi Fail2Ban dan IPTables, sedangkan pada sistem Windows dilakukan aktivasi fitur keamanan seperti Ransomware Protection dan Controlled Folder Access. Evaluasi dilakukan dengan cara melakukan simulasi uji keamanan untuk mengukur efektivitas dari masing-masing konfigurasi hardening. Tujuannya adalah untuk menilai peningkatan tingkat keamanan setelah penerapan hardening serta memberikan rekomendasi praktik terbaik berdasarkan hasil pengujian.

3.1. Diagram Alir

Diagram alir metodologi penelitian ini menggambarkan tahapan yang tersusun secara logis untuk mengevaluasi efektivitas hardening pada sistem operasi Windows dan Linux. Pada sistem Linux, tahapan dimulai dari identifikasi port dan layanan aktif, konfigurasi keamanan SSH, implementasi Fail2Ban untuk mitigasi serangan brute force, hingga penerapan IPTables sebagai firewall untuk pengendalian lalu lintas jaringan. Sementara pada sistem Windows, proses meliputi aktivasi fitur Ransomware Protection dan Controlled Folder Access. Setiap tahapan dirancang untuk memastikan proses perancangan, penerapan, dan evaluasi berjalan sistematis, sehingga efektivitas teknik hardening dapat diukur secara terstruktur dan objektif.



Gambar 1. Diagram Alir

3.2. Persiapan Sistem

Pada tahap ini, peneliti akan menyiapkan lingkungan virtualisasi menggunakan Oracle VM VirtualBox untuk menginstal sistem operasi Windows dan Linux. Peneliti juga akan melakukan identifikasi terhadap komponen dan layanan yang diperlukan sebagai dasar penerapan hardening. Untuk Linux, peneliti akan mempersiapkan konfigurasi awal seperti pengaktifan layanan SSH, serta instalasi Fail2Ban dan IPTables. Sementara itu, pada Windows akan dilakukan aktivasi fitur keamanan seperti Controlled Folder Access dan Windows Defender Firewall.

3.3. Implementasi

Pada tahap ini, peneliti akan menerapkan teknik-teknik hardening sesuai sistem operasi masing-masing. Di sistem Linux, peneliti akan mengonfigurasi Fail2Ban untuk membatasi akses SSH dan mengatur IPTables untuk mengontrol lalu lintas jaringan. Di sistem Windows, peneliti akan mengaktifkan perlindungan akses folder dan menambahkan aturan khusus dalam Windows Firewall untuk memblokir koneksi ke IP atau situs tertentu.

3.4. Evaluasi atau Tahap Uji

Pada tahap ini, peneliti akan melakukan pengujian terhadap sistem yang telah di-hardening. Pengujian akan dilakukan dengan simulasi serangan atau akses yang tidak sah, seperti mencoba login SSH secara berulang di Linux, atau mengakses file berbahaya dan situs terblokir di Windows. Tujuannya adalah untuk menilai apakah konfigurasi hardening berhasil mencegah potensi ancaman sesuai dengan skenario uji yang telah direncanakan.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Penerapan Hardening

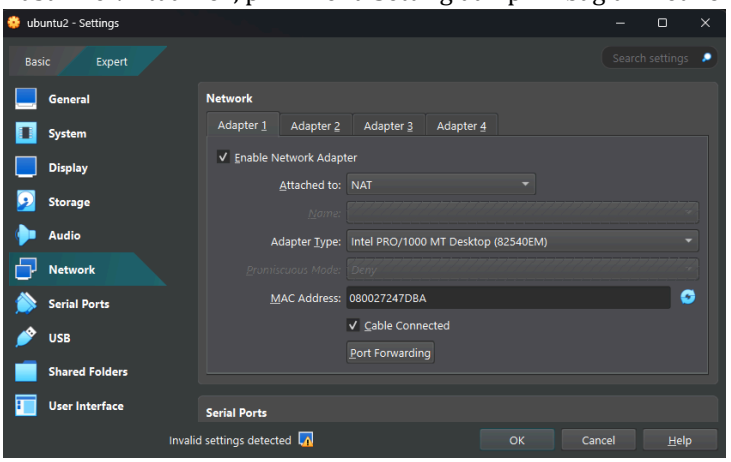
4.1.1. Sistem Operasi Linux

a. Persiapan Sistem

- Identifikasi Port

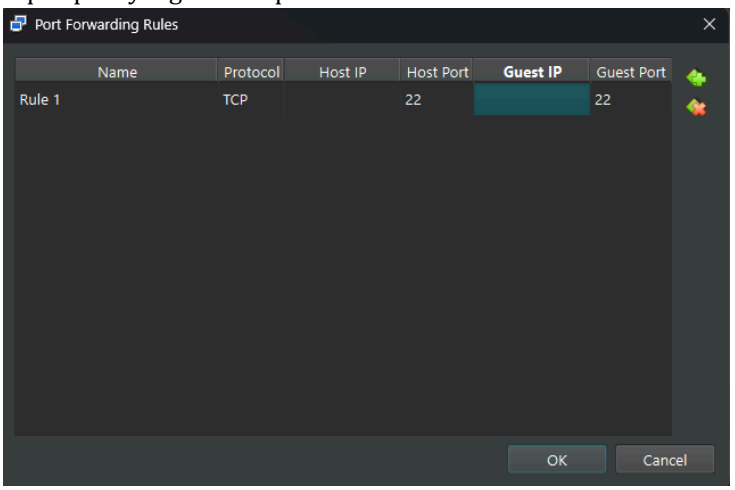
merupakan langkah penting dalam proses hardening server Linux untuk meningkatkan keamanan dan efisiensi sistem. Setiap layanan yang berjalan di server dapat menjadi pintu masuk potensial bagi penyerang, terutama jika memiliki kerentanan. Dengan menonaktifkan layanan yang tidak digunakan, permukaan serangan dapat diminimalkan, sehingga mengurangi risiko eksploitasi. Langkah-langkah yang dapat dilakukan dalam proses ini adalah:

➔ Masuk ke VirtualBox, pilih menu Setting dan pilih bagian Network.



Gambar 2. Menu Settings VirtualBox

➔ Klik tombol Port Forwarding, lalu tambahkan port yang diinginkan atau hapus port yang tidak diperlukan.



Gambar 3. Menu Tambah Rules Port

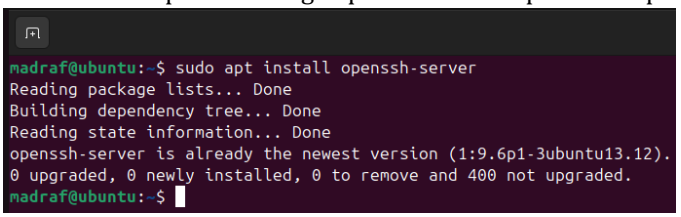
- Konfigurasi SSH

Konfigurasi SSH (Secure Shell) dalam proses hardening server Linux berfungsi untuk meningkatkan keamanan akses jarak jauh ke server dengan mencegah potensi serangan atau akses tidak sah. SSH adalah protokol yang digunakan

untuk manajemen server secara aman, sehingga pengaturan yang tepat menjadi langkah penting dalam melindungi sistem. Langkah-langkah yang perlu dilakukan dalam proses ini adalah sebagai berikut:

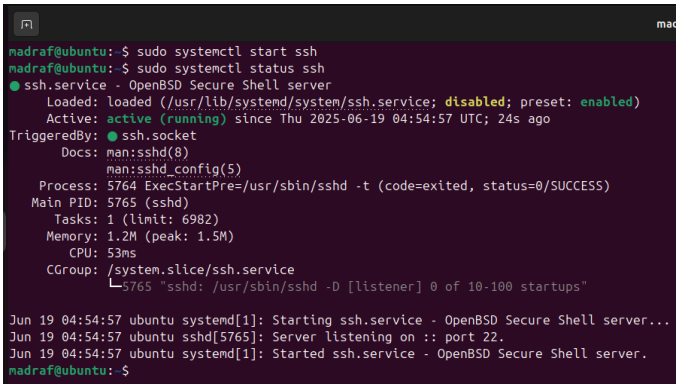
➔ Mulai mesin ubuntu dalam VirtualBox, dan buka terminal

➔ install OpenSSH dengan perintah sudo apt install openssh-server.



Gambar 4. Install OpenSSH di terminal linux

➔ Aktifkan SSH dengan perintah sudo systemctl start ssh, dan periksa apakah SSH sudah aktif atau belum dengan menjalankan perintah sudo systemctl status ssh.



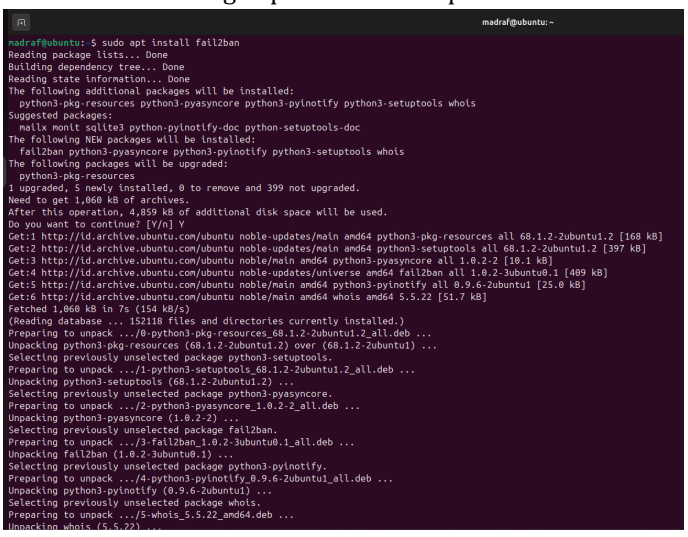
Gambar 5. Aktifkan SSH dan Cek Status SSH

➔ jika sudah aktif, maka SSH sudah siap untuk digunakan

b. Implementasi

- Implementasi Fail2ban

➔ Install Fail2ban dengan perintah sudo apt install fail2ban



Gambar 6. Install Fail2Ban di terminal Linux

➔ Setelah selesai terinstall, masuk ke dalam folder fail2ban dengan perintah cd /etc/fail2ban/. Lalu periksa file apa saja yang ada didalam folder fail2ban dengan menjalankan perintah ls

```
madraf@ubuntu2:~$ cd /etc/fail2ban/
madraf@ubuntu2:/etc/fail2ban$ ls
action.d         jail.conf           paths-debian.con
f
fail2ban.conf    jail.d              paths-opensuse.c
onf
fail2ban.d       paths-arch.conf
filter.d         paths-common.conf
madraf@ubuntu2:/etc/fail2ban$ sudo cp fail2ban.con
f fail2ban.local
madraf@ubuntu2:/etc/fail2ban$ sudo cp jail.conf ja
il.local
madraf@ubuntu2:/etc/fail2ban$
```

Gambar 7. Buka Folder Fail2Ban

➔ Copy file jail.conf dan fail2ban.conf

```
root@ubuntu: /etc/fail2ban
madraf@ubuntu:/etc/fail2ban$ sudo su
root@ubuntu:/etc/fail2ban# ls
action.d  fail2ban.conf  fail2ban.d  filter.d  jail.conf  jail.d  paths-arch.conf  paths-common.conf  paths-debian.conf  paths-opensuse.conf
root@ubuntu:/etc/fail2ban# cp fail2ban.conf fail2ban.local
root@ubuntu:/etc/fail2ban# cp jail.conf jail.local
root@ubuntu:/etc/fail2ban#
```

Gambar 8. Copy File

➔ Buka file jail.local dan ubah maxentry menjadi 2 atau 3 (sesuai kebutuhan)

```
root@ubuntu: /etc/fail2ban
  GNU nano 7.2                                                    /etc/fail2ban/jail.lc
# can be defined using space (and/or comma) separator.
#ignoreip = 127.0.0.1/8 ::1

# External command that will take an tagged arguments to ignore, e.g. <ip>,
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
bantime  = 10m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 10m

# "maxretry" is the number of failures before a host get banned.
maxretry = 3

# "maxmatches" is the number of matches stored in ticket (resolvable via tag <matches> in actions).
maxmatches = %(maxretry)s

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#
# pyinotify: requires pyinotify (a file alteration monitor) to be installed.
#              If pyinotify is not installed, Fail2ban will use auto.
# gamin:     requires Gamin (a file alteration monitor) to be installed.
#              If Gamin is not installed, Fail2ban will use auto.
# polling:   uses a polling algorithm which does not require external libraries.
# systemd:   uses systemd python library to access the systemd journal.
#              Specifying "logpath" is not valid for this backend.
#              See "journalmatch" in the jails associated filter config
# auto:      will try to use the following backends, in order:
#              pyinotify, gamin, polling.
#
```

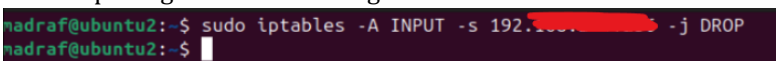
Gambar 9. Ubah maxentry pada file jail.local

- Implementasi Iptables
  - ➔ Install iptables

```
madraf@ubuntu2:~$ sudo apt install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.10-3ubuntu2).
iptables set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 225 not upgraded.
madraf@ubuntu2:~$
```

Gambar 10. Install iptables di terminal Linux

➔ Dalam percobaan ini, peneliti mencoba untuk memblokir akses dari IP address perangkat windows dengan membuat rules khusus



Gambar 11. Membuat rules baru

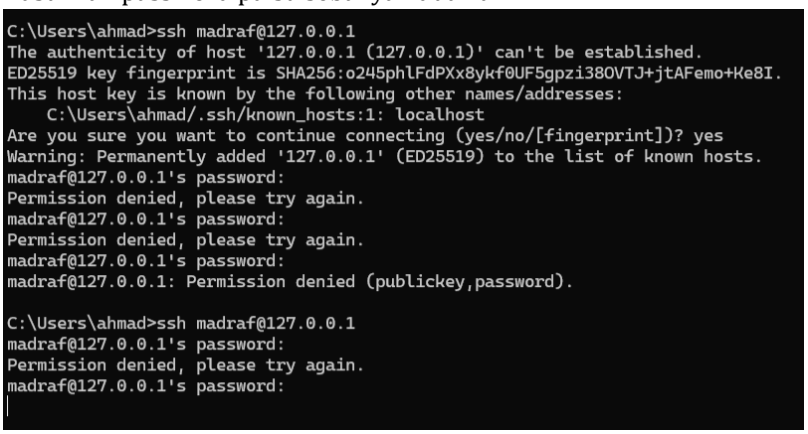
➔ Periksa apakah rules tersebut berhasil masuk kedalam rules iptables

Gambar 12. Cek rules sudah diperbarui atau belum

c. Evaluasi atau Tahap Uji

- Uji Fail2ban

➔ Buka command prompt windows dan coba login kedalam server ubuntu dengan menggunakan ssh yang sudah dikonfigurasi sebelumnya, dan Masukkan password palsu sebanyak dua kali



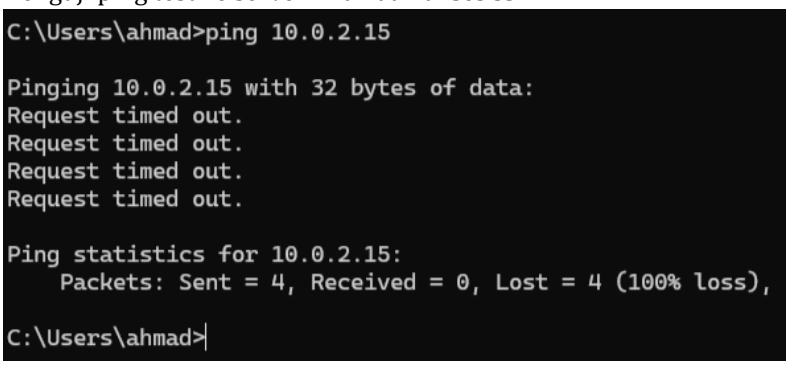
Gambar 13. Melakukan test iptables

➔ Berdasarkan gambar diatas, terlihat bahwa fail2ban sudah aktif dan menutup koneksi dari IP address segera setelah 2 kali percobaan login gagal. Untuk melihat buktinya jalankan perintah sudo fail2ban-client status sshd

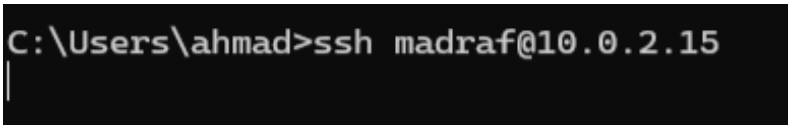
Gambar 14. Cek Status Ban

➔ Dapat dilihat dari status, bahwa ip yang digunakan untuk mengakses ssh tadi sudah di banned.

- Uji Iptables
  - ➔ Setelah rules telah berhasil masuk kedalam rules iptables langkah selanjutnya menguji ping test ke server linux dan akses ssh



Gambar 15. Uji ping



Gambar 16. Uji akses SSH

  - ➔ Gambar diatas menunjukkan bahwa firewall telah aktif dan memblokir IP address sehingga membuatnya tidak bisa mengakses server serta jaringan ubuntu yang dituju.

4.1.2. Sistem Operasi Windows

a. Controlled Folder Access (CFA)

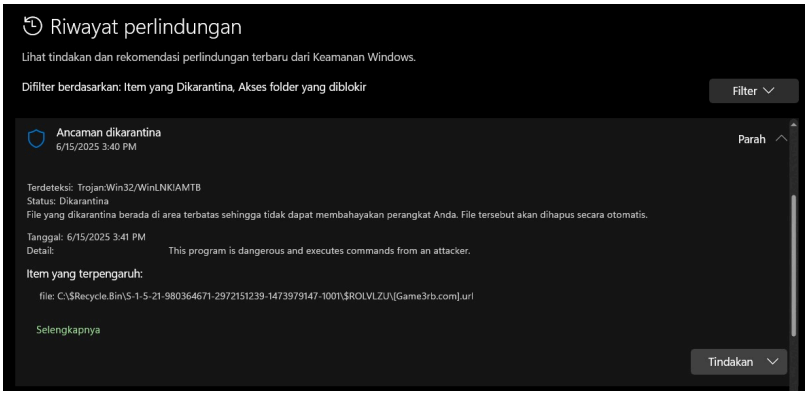
Pada sistem operasi Windows, teknik hardening dilakukan dengan mengaktifkan fitur Controlled Folder Access (CFA) yang terdapat dalam Windows Security. Langkah implementasinya merujuk pada tahapan berikut:

1. Masuk ke Windows Security > Virus & Threat Protection.
2. Pilih menu Kelola Proteksi Ransomware.
3. Aktifkan opsi Controlled Folder Access.
4. Tambahkan folder penting seperti Documents, Downloads, dan Pictures ke daftar folder yang dilindungi.

Gambar 17. Menu Kelola Proteksi Ransomware pada Sistem Operasi Windows

Setelah fitur aktif, peneliti melakukan simulasi ancaman dengan mencoba mengunduh dan menjalankan shortcut file dari situs mencurigakan (Game3rb.com). Hasilnya, sistem secara otomatis:

- Mendeteksi file sebagai Trojan:Win32/WinLNK.AMTB,
- Mengkarantina file, dan
- Menampilkan deskripsi bahwa file tersebut "berbahaya dan mengeksekusi perintah dari penyerang".



Gambar 18. Tampilan Riwayat Perlindungan dari File Berbahaya

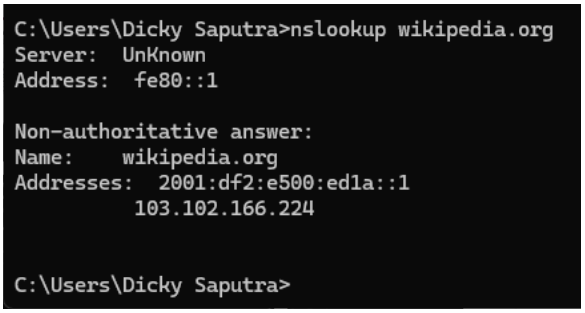
Ini membuktikan bahwa Controlled Folder Access tidak hanya mencegah akses ilegal ke folder yang dilindungi, tetapi juga dapat mengenali file shortcut berbahaya yang biasa digunakan dalam penyebaran malware seperti ransomware dan spyware.

b. Windows Defender Firewall

Pada sistem operasi Windows, teknik hardening juga dilakukan dengan memanfaatkan fitur Windows Defender Firewall. Fitur ini digunakan untuk membatasi lalu lintas jaringan keluar menuju alamat IP tertentu yang dianggap berisiko atau tidak diizinkan.

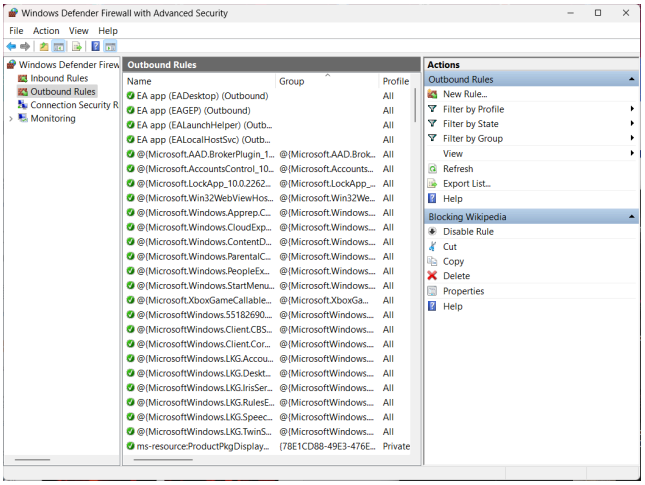
Langkah implementasinya merujuk pada tahapan berikut:

1. Cek alamat IP tujuan menggunakan nslookup di Terminal yang terkoneksi dengan internet. Tujuan yang akan dilakukan pengujian adalah website wikipedia.org.



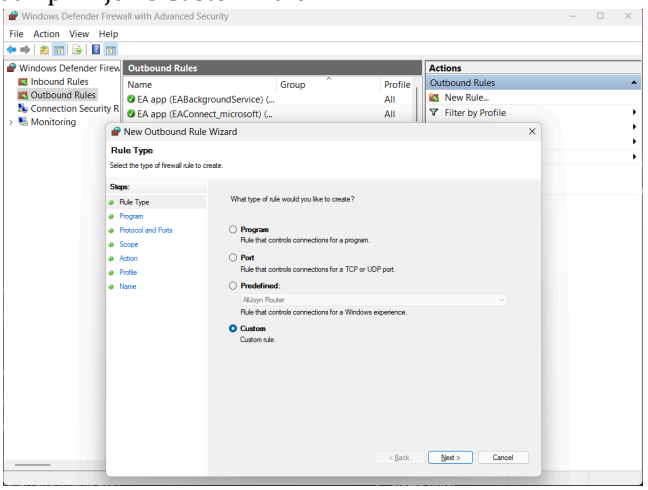
Gambar 19. Mencari Alamat IP wikipedia.org menggunakan nslookup di Terminal

2. Buka Windows Defender Firewall with Advanced Security



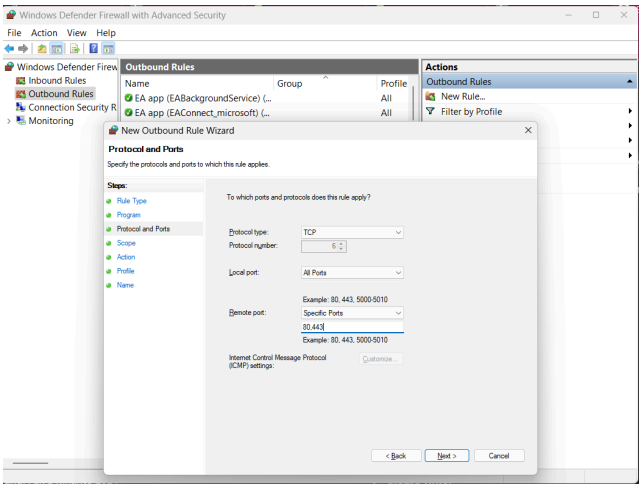
Gambar 20. Tampilan Windows Defender Firewall with Advanced Security

3. Masuk ke menu Outbound Rules
4. Klik New Rule dan pilih jenis Custom Rule



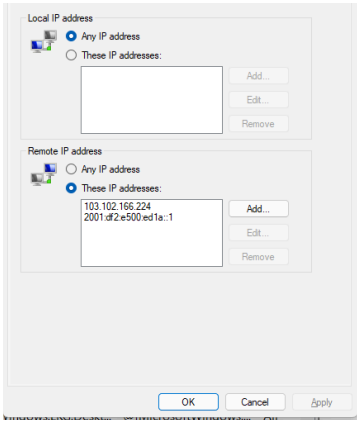
Gambar 21. Tampilan Rule Type pada New Outbound Rules

5. Atur protokol ke TCP, dan tentukan remote port yaitu 80, 443



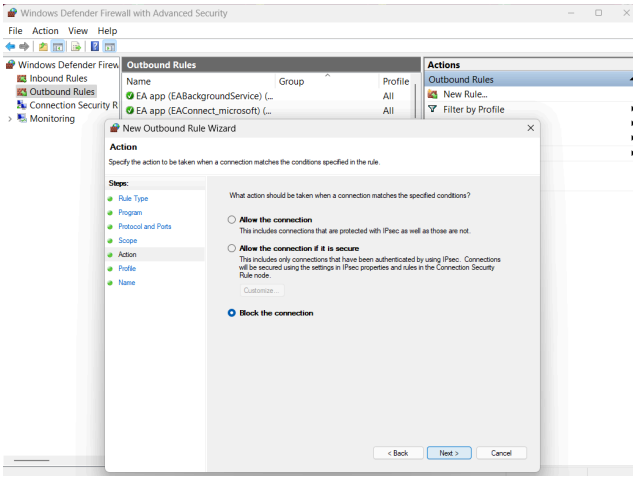
Gambar 22. Tampilan Konfigurasi Remote Port

6. Masukkan alamat IP target 103.102.166.224 dan 2001:df2:e500:cd1a::1 (IPv4 dan IPv6 hasil dari nslookup wikipedia.org) ke dalam kolom Remote IP Address



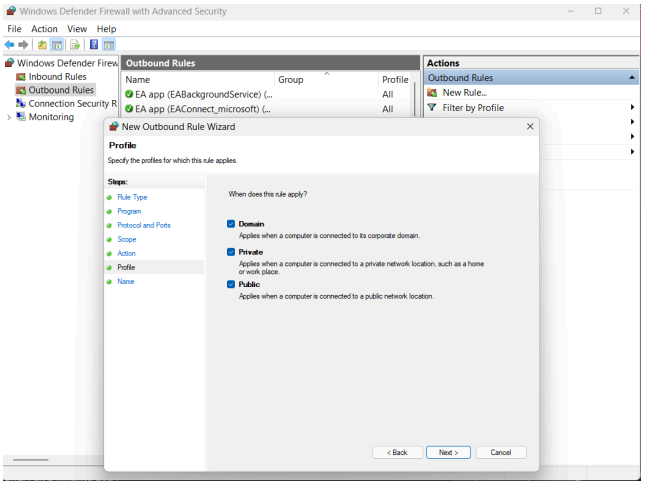
Gambar 23. Tampilan Remote IP Adress

7. Pilih opsi Block the connection



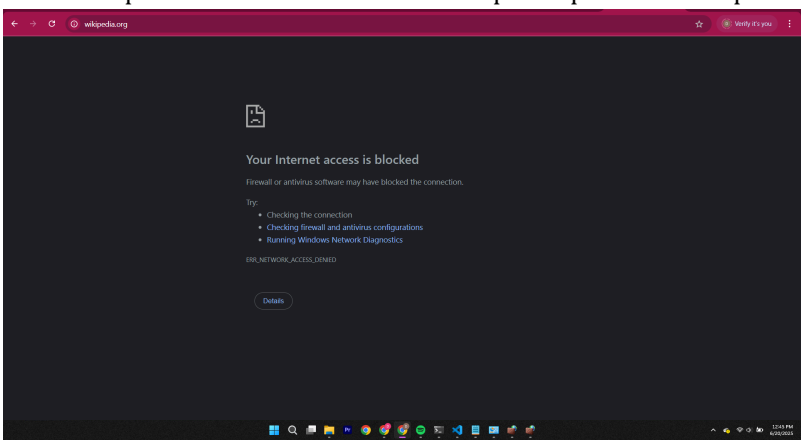
Gambar 24. Tampilan Action untuk Blokir Koneksi

8. Terapkan untuk semua profil (Domain, Private, Public)



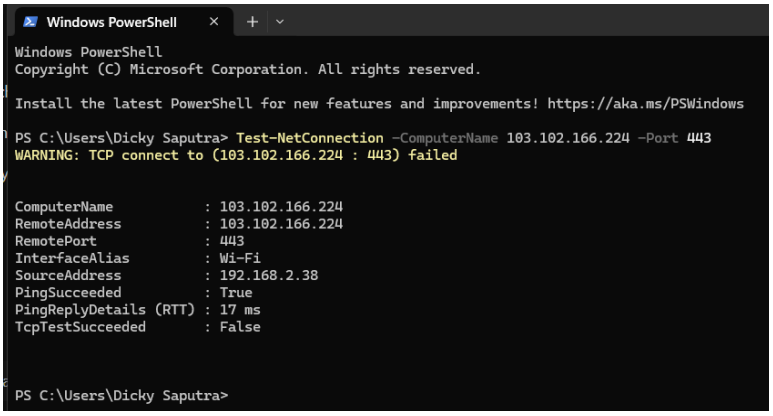
Gambar 25. TampilanPenerapan ke Semua Profil

Setelah rule firewall diterapkan, peneliti melakukan pengujian dengan mencoba mengakses situs https://wikipedia.org melalui browser yang sebelumnya bisa diakses. Hasilnya, situs tidak dapat diakses dan browser menampilkan pesan error seperti:

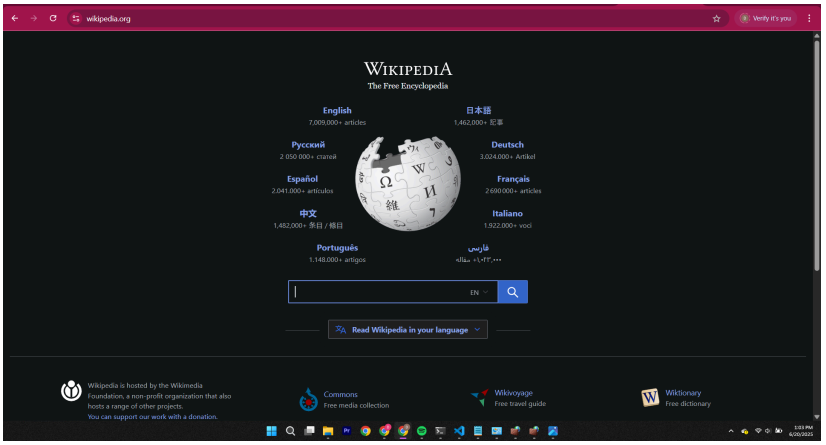


Gambar 26. Tampilan Website wikipedia.org setelah penerapan rule firewall

Sebagai verifikasi tambahan, pengujian dilakukan melalui perintah PowerShell:



Gambar 27. Verifikasi tambahan pada Powershell dengan Test-NetConnection



Gambar 28. Tampilan Website wikipedia.org ketika rule firewall dimatikan

Hal ini membuktikan bahwa Windows Defender Firewall dapat digunakan secara efektif sebagai teknik hardening sistem operasi Windows untuk membatasi koneksi ke server yang tidak diizinkan, dan mencegah akses aplikasi terhadap layanan eksternal tertentu berdasarkan IP dan port.

5. KESIMPULAN

Penelitian ini menunjukkan bahwa implementasi teknik hardening pada sistem operasi Windows dan Linux dapat secara efektif meningkatkan keamanan sistem (khususnya di jaringan). Pada sistem Linux, konfigurasi Fail2Ban berhasil mencegah upaya login SSH setelah dua kali percobaan (sesuai dengan parameter maxentry yang diberikan), dan IPTables mampu memblokir koneksi dari IP perangkat Windows, ditunjukkan dengan hasil ping yang request timeout dan gagalnya akses SSH ke server. Di sisi lain, pada sistem Windows, aktivasi Controlled Folder Access berhasil mendeteksi dan mengkarantina file trojan saat dilakukan simulasi pengunduhan game bajakan. Selain itu, penambahan aturan baru pada Windows Defender Firewall untuk memblokir akses ke IP sebuah situs web juga berhasil dilakukan, menunjukkan bahwa firewall mampu bekerja sesuai konfigurasi yang diterapkan. Secara keseluruhan, hasil ini membuktikan bahwa kombinasi berbagai teknik hardening yang tepat mampu meningkatkan ketahanan sistem terhadap berbagai ancaman keamanan, baik dalam bentuk serangan jaringan maupun potensi infeksi malware. Selain meningkatkan keamanan, teknik hardening juga menjadi sebuah langkah pencegahan akan adanya serangan yang tak terduga.

Ucapan Terimakasih

Penulis menyampaikan terima kasih kepada dosen pengampu mata kuliah yang telah memberikan arahan dan bimbingan selama penyusunan jurnal ini. Ucapan terima kasih juga disampaikan kepada seluruh pihak yang telah membantu, baik secara langsung maupun tidak langsung, dalam proses penelitian dan pengembangan sistem peningkatan kontras citra ini. Dukungan fasilitas laboratorium, perangkat lunak, serta referensi akademik turut berperan besar dalam kelancaran pelaksanaan penelitian ini.

REFERENCES (10 PT)

[1] Anam, M. K., Sudyana, D., Ulfah, A. N., Lizarti, N., & Agustin. (2020). Optimalisasi Penggunaan VirtualBox Sebagai Virtual Computer Laboratory untuk Simulasi Jaringan dan Praktikum pada SMK Taruna Mandiri Pekanbaru. J-PEMAS - Jurnal Pengabdian Masyarakat, 1(2), 39–44.

[2] Benufinit, Y. A., & Enstein, J. (2021). ANALISA SIKAP RESPONSIF TERHADAP VIRTUALBOX SIMULASI PADA MAHASISWA ORACLE MATAKULIAH SISTEM OPERASI. Jurnal Pendidikan Teknologi Informasi (JUKANTI), 4(2), 11–18. https://doi.org/https://doi.org/10.37792/jukanti.v4 i2.258

[3] Farida, T., & Hariadi, E. (2019). Pengembangan Media Pembelajaran Virtual Box Untuk Mengukur Kelayakan Modul Pada Mata Pelajaran Komputer Dan Jaringan Dasar Di Smkn 7 Surabaya. IT-Edu : Jurnal Information Technology and Education, 4(1).

[4] Santoso, N. A., Zakaria, Z., & Kurniawan, R. D. (2022). Analisis Jaringan Komputer Menggunakan Teknologi Virtualisasi. Jurnal Minfo Polgan, 11(2), 52–58. https://doi.org/10.33395/jmp.v11i2.11652

[5] Desmira, D., & Wiryadinata, R. (2022). Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knocking. Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI), 5(1), 28–33. https://doi.org/10.55338/jikomsi.v5i1.242

[6] Christopher, W., & Hermawan, R. Z. (2024). Pemantauan dan Pengawasan Serangan Siber SSH Brute Force di Indonesia dengan IBM QRadar Community Edition. Jurnal Ilmiah Teknik Informatika (TEKINFO), 25(2), 120–127.

[7] Ramadhani, Y., & Sholeh, M. (2022). Penerapan Tools Fail2Ban Untuk Mencegah Serangan Brute Force Pada Web Server Online Learning Uhamka (OLU). Jurnal Teknik Informatika Dan Komputer, 1(2), 41–45. https://doi.org/10.22236/jutikom.v1i2.10447

[8] Wicaksono, A. (2023). PERANCANGAN DAN IMPLEMENTASI IDS SURICATA, SNORT, DAN FAIL2BAN PADA RASPBERRY PI. [Sekolah Tinggi Teknologi Terpadu Nurul]. https://repository.nurulfikri.ac.id/id/eprint/213

[9] Adi, D. W., Athallah, Z. R., Irawan, F., & Neyman, S. N. (2024). Implementasi Firewall menggunakan Fitur dari IPTables pada Sistem Operasi Linux. Journal of Internet and Software Engineering, 1(2), 7. https://doi.org/10.47134/pjise.v1i2.2671

[10] Akbar, A. S. I., & Suksmadana, I. M. B. (2019). Implementasi Iptables untuk Packet Filtering Firewall pada Raspberry Pi. Jurnal Ilmiah Kajian Teori Dan Aplikasi Teknik Elektro, 6(1).

[11] Rahmadaniar, I., Tondang, D. A. A., Fernando, B. S., & Setiawan, A. (2024). Implementasi Firewall Menggunakan Iptables untuk Melindungi Server dari Serangan DDoS. Journal of Internet and Software Engineering, 1(3), 10. https://doi.org/10.47134/pjise.v1i3.2564