JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 2 September 2026
Hal: 1674-1680
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i2.1427

Penerapan Metode *Stateful Packet Filtering* Menggunakan Ufw di Poltekpar Medan dari Serangan *Port Scanning*

Riza Arivalva[1*], Hafni[2], Muhammad Zen[3]

[1,2,3]Sains Komputasi Dan Kecerdasan Digital, Sistem Komputer, Universitas Panca Budi, Medan, Indonesia
Email: [1*]arivalvariza@gmail.com, [2]hafni@dosen.pancabudi.ac.id, [3]muhammadzen@dosen.pancabudi.ac.id
(* Email Corresponding Author: arivalvariza@gmail.com)
Received: 1 Juli 2026 | Revision: 8 Juli 2026 | Accepted: 11 Juli 2026

Abstrak

Keamanan jaringan merupakan aspek krusial dalam menjaga integritas data dan keberlangsungan layanan sistem informasi, khususn ya di lingkungan institusi pendidikan seperti Poltekpar Medan. Salah satu ancaman awal yang sering terjadi dalam siklus serangan siber adalah *port scanning*, yang bertujuan untuk memetakan kerentanan sistem. Penelitian ini bertujuan untuk mengimplementasikan dan menganalisis efektivitas *Uncomplicated Firewall* (UFW) dengan metode *Stateful Packet Filtering* dalam memitigasi serangan tersebut. Metode penelitian menggunakan pendekatan eksperimental simulasi dengan topologi *host-guest*, di mana Ubuntu Server 22.04 bertindak sebagai target dan Windows 11 sebagai penyerang menggunakan Nmap. Pengujian dilakukan dengan membandingkan respons jaringan sebelum dan sesudah implementasi *firewall*. Hasil penelitian menunjukkan bahwa sebelum implementasi, seluruh *port* terbuka (22 dan 80) dapat dideteksi dengan status *Open*. Setelah UFW diaktifkan dengan konfigurasi *default deny incoming*, status *port* berubah menjadi *Filtered* dan sistem berhasil mencatat log aktivitas pemblokiran paket secara *real-time*. Analisis forensik log menunjukkan bahwa UFW mampu membedakan koneksi sah dan ilegal berdasarkan tabel status (*state table*), membuktikan bahwa metode *stateful* efektif menyembunyikan arsitektur jaringan dari pemindaian eksternal.

Kata Kunci: Keamanan Jaringan, Firewall, UFW, *Port Scanning*, *Stateful Inspection*

Abstract

Network security is a crucial aspect in maintaining data integrity and continuity of information system services, especially in educational institutions such as Poltekpar Medan. One of the initial threats that often occurs in the cyber attack cycle is port scanning, which aims to map system vulnerabilities. This study aims to implement and analyze the effectiveness of Uncomplicated Firewall (UFW) with Stateful Packet Filtering method in mitigating such attacks. The research method uses a simulation experimental approach with a host-guest topology, where Ubuntu Server 22.04 acts as the target and Windows 11 as the attacker using Nmap. Testing was carried out by comparing network responses before and after firewall implementation. The results showed that before implementation, all open ports (22 and 80) could be detected with Open status. After UFW was activated with default deny incoming configuration, the port status changed to Filtered and the system successfully logged packet blocking activities in real-time. Forensic log analysis shows that UFW is able to distinguish legitimate and illegal connections based on the state table, proving that the stateful method effectively hides the network architecture from external scanning..

Keywords*: Network Security, Firewall, UFW, Port Scanning, Stateful Inspection*

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini menuntut ketersediaan layanan jaringan yang handal, namun berbanding lurus dengan meningkatnya ancaman keamanan siber. Dalam era *big data*, keamanan jaringan komputer menjadi masalah yang harus diperhatikan karena banyaknya potensi bahaya di mana komputer terhubung dengan internet [1]. Serangan siber dapat merusak integritas, kerahasiaan, dan ketersediaan data, yang berpotensi menimbulkan kerugian besar bagi institusi pendidikan. Salah satu fase awal dari siklus serangan siber adalah *reconnaissance* atau pengumpulan informasi, yang sering dilakukan menggunakan teknik *port scanning*. Serangan ini bertujuan untuk mengidentifikasi layanan yang berjalan dan *port* yang terbuka pada server target untuk menemukan celah eksploitasi, sehingga memudahkan penyerang dalam merencanakan intrusi lebih lanjut [2].

Lingkungan Poltekpar Medan yang mengandalkan sistem informasi berbasis jaringan rentan terhadap ancaman ini jika tidak dilindungi dengan mekanisme pertahanan yang memadai. Tanpa adanya filter lalu lintas yang ketat, penyerang dapat dengan mudah memetakan arsitektur jaringan internal. Berbagai metode keamanan telah dikembangkan, salah satunya adalah *firewall*. Firewall didefinisikan sebagai sistem keamanan jaringan yang digunakan untuk mengatur dan membatasi lalu lintas data sesuai dengan kebijakan keamanan yang telah ditentukan [3].

Teknologi firewall telah berevolusi dari *packet filtering* statis menjadi metode yang lebih canggih seperti *stateful packet inspection* (SPI). Metode *stateful* tidak hanya memeriksa *header* paket, tetapi juga memantau status koneksi secara dinamis, sehingga mampu membedakan antara paket data yang sah dan paket yang mencurigakan

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 2 September 2026
Hal: 1674-1680
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i2.1427

[4]. Penelitian oleh Tarina et al. (2026) menekankan bahwa *firewall* modern harus mampu melakukan inspeksi mendalam untuk menghadapi ancaman yang kompleks [5]. Implementasi *stateful packet filtering* yang efisien pada sistem operasi linux dapat dilakukan menggunakan *uncomplicated firewall* (UFW), antarmuka manajemen *firewall* yang menyederhanakan konfigurasi *iptables* namun tetap mempertahankan kehandalan fitur keamanan *kernel Linux* [6].

Infrastruktur server memegang peranan vital dalam menyediakan layanan akses data bagi pengguna dalam sebuah organisasi. Sebagaimana dikemukakan oleh Rizal et al. [16], agar jaringan dapat dimanfaatkan secara optimal, diperlukan perancangan infrastruktur server yang efisien dan fleksibel untuk mengoptimalkan penggunaan sumber daya (*resources*) perangkat keras yang tersedia**.** Namun, optimalisasi server ini akan sia-sia jika tidak dibarengi dengan keamanan yang mumpuni, karena server yang terhubung ke jaringan tanpa perlindungan memadai sangat rentan terhadap serangan siber seperti *port scanning*.

Beberapa penelitian terdahulu telah membahas implementasi keamanan jaringan. Penelitian Vidya et al. (2020) menunjukkan bahwa metode *stateful inspection* lebih unggul dalam menyaring paket dibandingkan metode *gateway* statis karena kemampuannya memantau sesi koneksi [4R]. Sementara itu, penelitian Sabila et al. (2025) berfokus pada penggunaan s*nort* sebagai IDS untuk mendeteksi *port scanning* [2]. Namun, terdapat celah penelitian (*gap analysis*) di mana penggunaan UFW sebagai mekanisme pertahanan aktif (*active defense*) untuk memitigasi *port scanning* dengan analisis log forensik mendalam pada lingkungan server akademik masih perlu dikaji efektivitas teknisnya secara spesifik. Berbeda dengan penelitian Rusdianto (2025) yang menggabungkan *vulnerability scanning* [7], penelitian ini berfokus pada penguatan perimeter menggunakan firewall *stateful* untuk mencegah tahap awal serangan.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi efektivitas UFW menggunakan metode *stateful packet filtering* dalam memitigasi serangan *port scanning*. Penelitian ini diharapkan dapat memberikan kontribusi praktis dalam pengamanan infrastruktur jaringan di Poltekpar Medan dengan menghasilkan konfigurasi *firewall* yang optimal.

2. METODOLOGI PENELITIAN

2.1 Perancangan Lingkungan Simulasi

Penelitian ini menggunakan metode eksperimental dengan pendekatan simulasi jaringan *virtual*. Metode ini dipilih karena memungkinkan pengujian serangan siber yang aman tanpa mengganggu jaringan produksi yang sebenarnya. Perangkat lunak virtualisasi yang digunakan adalah *oracle virtualbox*. Topologi jaringan dikonfigurasi menggunakan mode *host-only adapter* untuk menciptakan saluran komunikasi privat yang terisolasi antara penyerang dan target.

Skema topologi terdiri dari dua *node* utama:

a. Sistem Target (*Victim*)
   Mesin virtual ubuntu server 22.04 LTS yang menjalankan layanan *apache web server* (*port* 80) dan SSH (*port* 22). Spesifikasi meliputi RAM 2GB dan penyimpanan 25GB. Ubuntu dipilih karena stabilitas dan performanya yang tinggi sebagai server [8].
b. Sistem Penyerang (*Attacker*)
   Komputer *Host* dengan sistem operasi windows 11 yang dilengkapi dengan *tools* pemindaian jaringan zenmap (GUI untuk Nmap) dan *command line* Nmap.

2.2 Tahapan Penelitian

Alur penelitian dilaksanakan mengikuti tahapan sistematis sebagai berikut:

a. Instalasi dan Konfigurasi Sistem
   Tahap awal melibatkan instalasi sistem operasi ubuntu server 22.04. Setelah instalasi dasar selesai, dilakukan instalasi paket layanan *apache2* untuk mensimulasikan layanan web server dan *nmap* untuk pengujian internal. Konfigurasi jaringan dilakukan secara statis dengan IP target 192.168.56.101 dan IP attacker 192.168.56.1.

b. Implementasi *Firewall*
   Pada tahap ini, UFW dikonfigurasi untuk menerapkan metode *stateful packet filtering*. Langkah-langkah konfigurasi meliputi:
   1. Mengaktifkan UFW dengan perintah *sudo ufw enable*.
   2. Menerapkan kebijakan *default deny incoming* untuk menolak semua koneksi masuk yang tidak diizinkan secara eksplisit.
   3. Membuka akses terbatas hanya pada *port* 22 (SSH) dan 80 (HTTP) menggunakan perintah *sudo ufw allow*.
   4. Mengaktifkan fitur pencatatan log dengan perintah *sudo ufw logging on*, level *high* untuk menangkap

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 2 September 2026
Hal: 1674-1680
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i2.1427

detail paket yang diblokir.

c. Konfigurasi Pengalamatan Jaringan

Untuk memastikan konektivitas yang stabil dan memudahkan analisis lalu lintas antara penyerang dan target, diterapkan pengalamatan IP statis pada segmen jaringan *Host-Only*. Pendekatan konfigurasi ini sejalan dengan penelitian Khairul et al [17]. yang menerapkan skema pengalamatan IP privat statis pada arsitektur server dan klien dalam satu subnet yang sama untuk menjamin jalur komunikasi yang jelas serta mempermudah proses pemantauan jaringan.

Konfigurasi IP yang diterapkan adalah:

1. IP Attacker: 192.168.56.1
2. IP Target: 192.168.56.101

d. Skenario Pengujian

Pengujian dilakukan menggunakan metode *black box testing* [9], di mana penyerang tidak mengetahui arsitektur keamanan target. Skenario dibagi menjadi dua fase yaitu:

Tabel 1. Fase Skenario

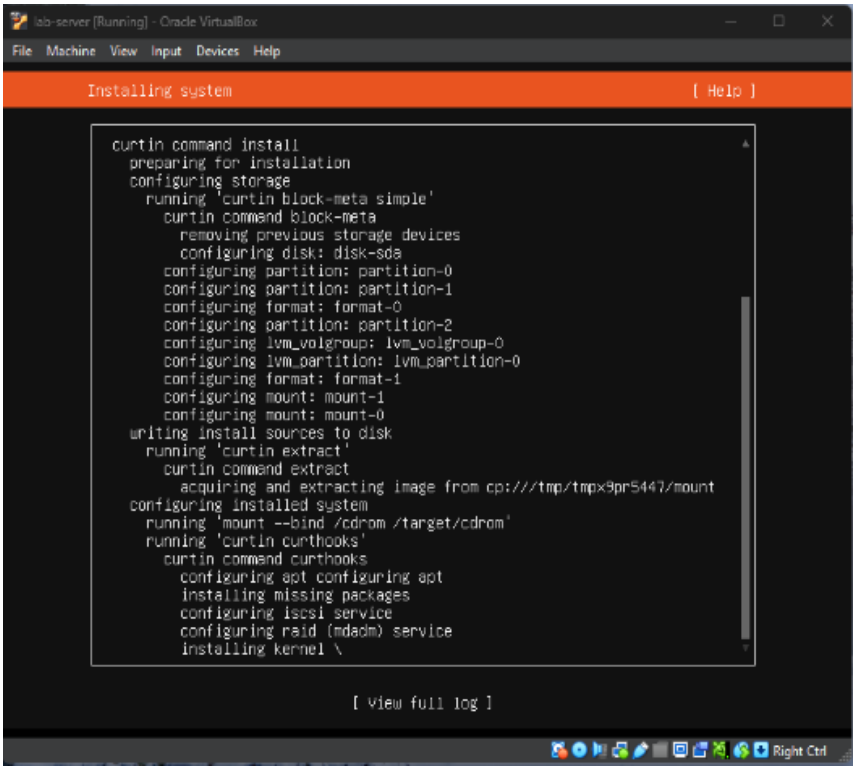
Fase	Keterangan
Tanpa *Firewall*	UFW dinonaktifkan. Penyerang melakukan pemindaian agresif terhadap target untuk mendapatkan *baseline* data
Dengan *Firewall*	UFW diaktifkan. Penyerang melakukan pemindaian ulang dengan parameter yang sama untuk melihat perubahan respons jaringan dan status *port*

3. HASIL DAN PEMBAHASAN

Bagian ini memaparkan hasil implementasi, pengujian serangan, dan analisis mendalam mengenai efektivitas UFW dalam memitigasi serangan *port scanning* berdasarkan data eksperimen yang diperoleh.

3.1 Implementasi Sistem Operasi Server

Proses pembangunan lingkungan uji coba diawali dengan instalasi sistem operasi server yang bertindak sebagai target.



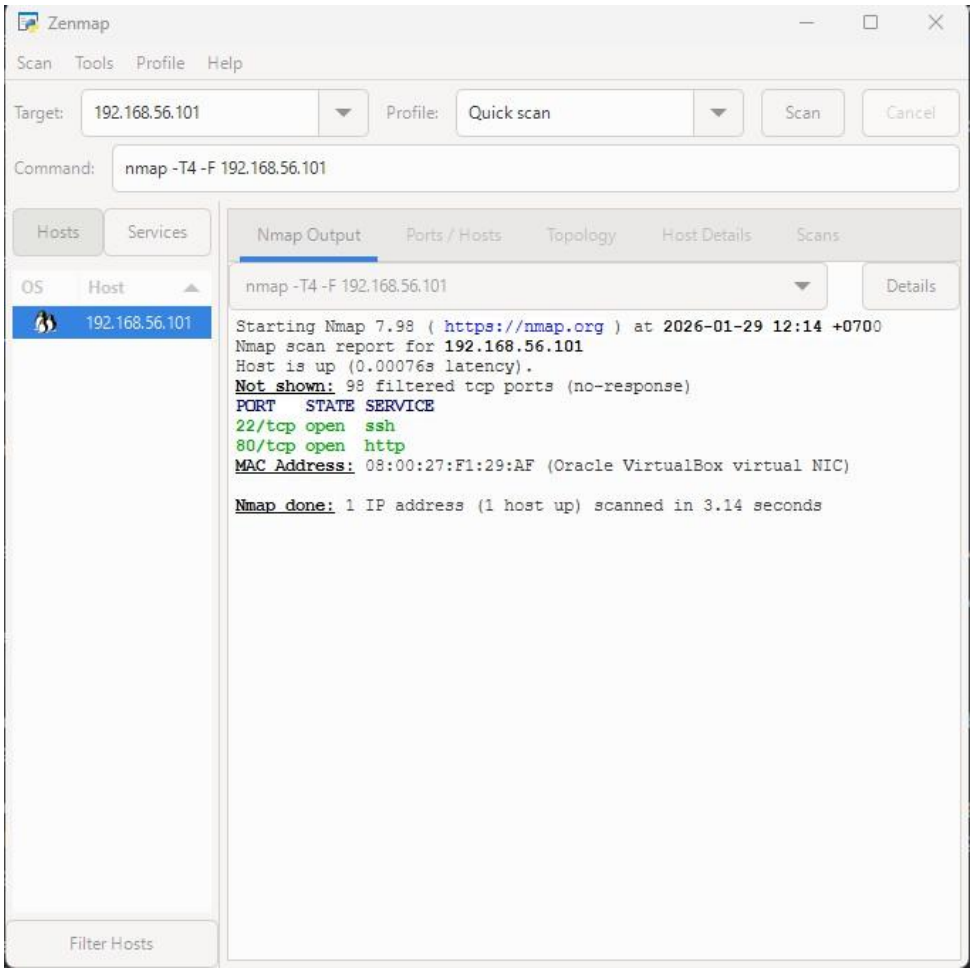
Gambar 1. Proses Instalasi Ubuntu Server 22.04

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 2 September 2026
Hal: 1674-1680
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i2.1427

Pada Gambar 1, terlihat proses instalasi sistem operasi ubuntu server yang sedang melakukan konfigurasi penyimpanan (*configuring storage*) dan ekstraksi paket sistem. Proses berjalan pada lingkungan virtual dengan alokasi sumber daya yang telah ditentukan. Keberhasilan instalasi ini ditandai dengan selesainya proses *curtin command install* yang membangun struktur direktori *root* dan kernel linux. Sistem ini menggunakan kernel versi 5.15 yang memiliki fitur *netfilter* bawaan, yang merupakan fondasi utama bagi UFW untuk melakukan manipulasi paket jaringan. Tanpa *kernel* yang terkonfigurasi dengan baik, modul *firewall* tidak dapat berinteraksi dengan *network stack*. Tahap ini merupakan implementasi dari desain topologi yang telah direncanakan. Server ini dipersiapkan untuk menjalankan layanan *apache2* yang nantinya akan menjadi objek perlindungan. Pemilihan ubuntu server 22.04 sejalan dengan penelitian Rahmadani etal. (2025) yang menyatakan bahwa ubuntu memberikan kinerja web server yang stabil dan efisien [8]. Stabilitas OS sangat penting agar hasil pengujian firewall tidak bias oleh kegagalan sistem operasi itu sendiri.

3.2 Pengujian *Firewall (Normal Traffic)*

Pada pengujian pertama setelah UFW diaktifkan, aturan *firewall* dikonfigurasi untuk mengizinkan lalu lintas HTTP pada *port* 80. Hal ini mensimulasikan kondisi operasional normal di mana layanan publik harus dapat diakses.



Gambar 2. Hasil Pemindaian Zenmap Saat *Port* 80 Diizinkan

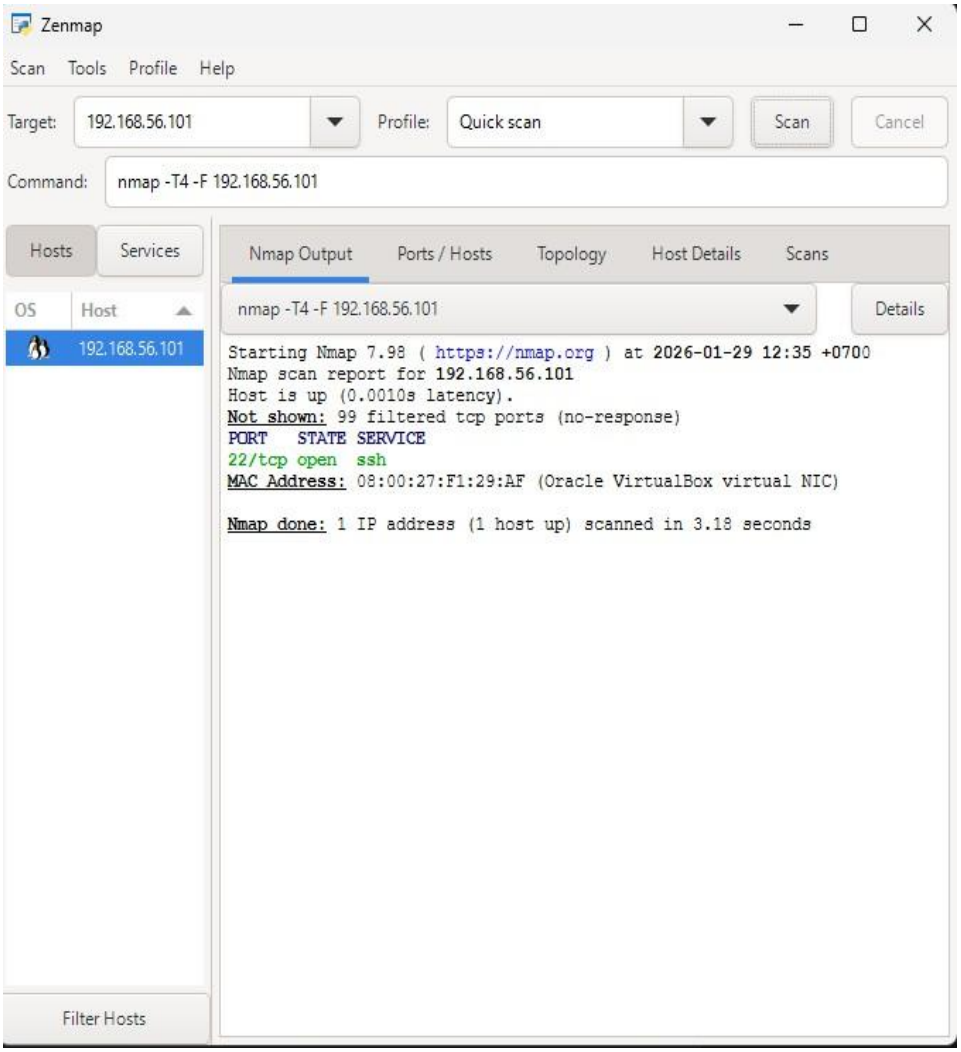
Pada Gambar 2, terlihat hasil pemindaian zenmap terhadap IP target 192.168.56.101. Output nmap menunjukkan "*PORT 80/tcp open http*" dan "*PORT 22/tcp open ssh*". Indikator berwarna hijau menandakan bahwa *port* tersebut dapat diakses sepenuhnya oleh penyerang. Status *OPEN* menunjukkan bahwa terjadi proses *three-way handshake* yang sukses antara penyerang dan target. Penyerang mengirimkan paket SYN, server membalas dengan SYN-ACK, dan penyerang membalas dengan ACK. Dalam konteks *firewall*, ini berarti aturan `ufw allow 80` telah berhasil dimuat ke dalam tabel *filter* di *iptables*, sehingga paket yang menuju *port* 80 melewati rantai INPUT tanpa hambatan. Hasil ini memvalidasi konfigurasi izin layanan terbatas pada metodologi. *Firewall* bekerja sesuai aturan yang ditetapkan *administrator* untuk mengizinkan lalu lintas legal. Kondisi ini, meskipun diinginkan untuk layanan publik, juga membawa risiko. Sebagaimana dijelaskan oleh Walidin et al. (2025), Nmap dapat memanfaatkan port terbuka untuk melakukan *fingerprinting* versi layanan Apache/2.4.41 yang terlihat pada detail *scan*, yang dapat digunakan untuk

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 2 September 2026
Hal: 1674-1680
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i2.1427

mencari kerentanan spesifik (CVE) pada layanan tersebut [10].

3.3 Pengujian *Firewall (Block Traffic)*

Pada skenario kedua, disimulasikan respons pertahanan ketika administrator mendeteksi anomali dan memutuskan untuk menutup akses ke *port* 80. Aturan *allow* dihapus dan kebijakan *default deny* mengambil alih.



Gambar 3. Hasil Pemindaian Zenmap Saat Port 80 Diblokir

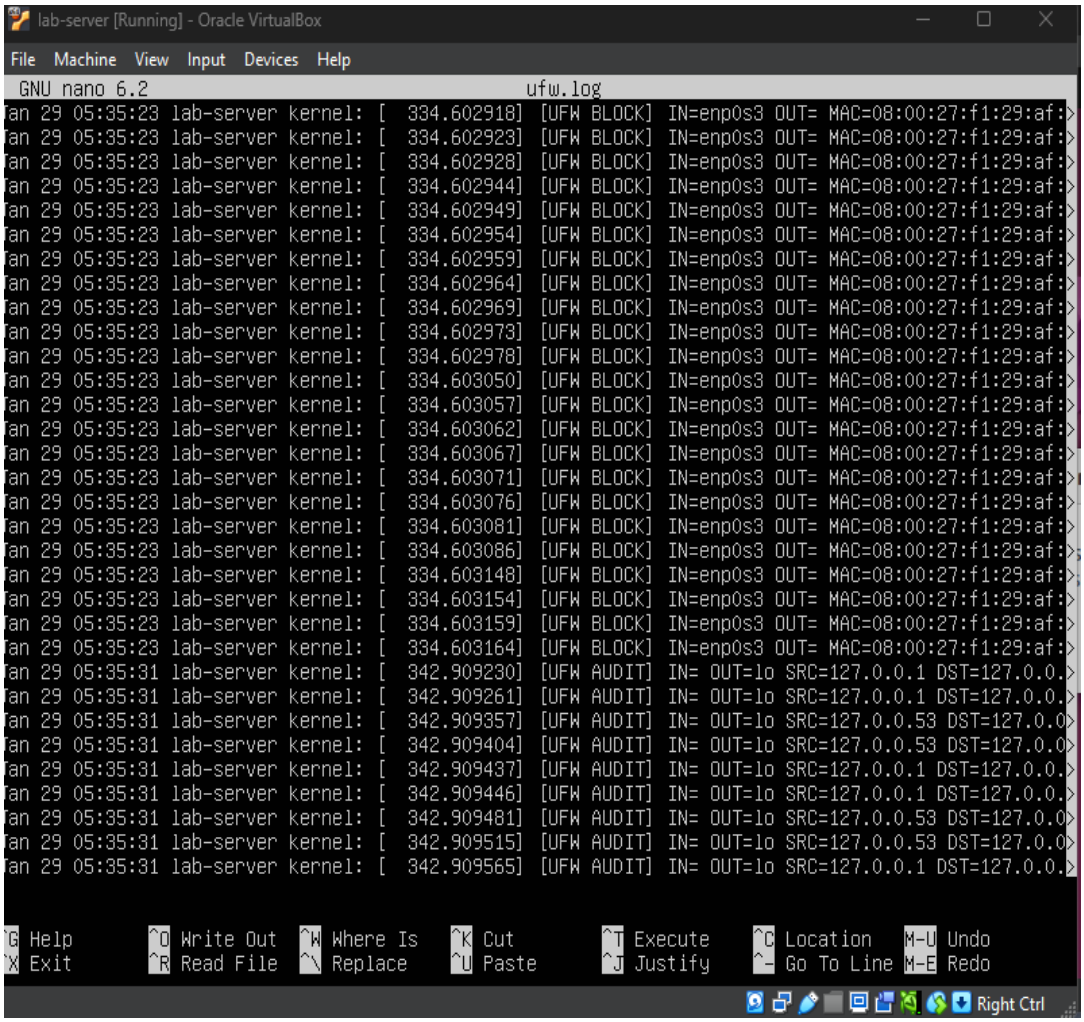
Pada Gambar 3, hasil pemindaian ulang menunjukkan perubahan drastis. *Port* 80 yang sebelumnya berstatus *Open*, kini tidak muncul dalam daftar *port* terbuka atau tertulis sebagai *99 filtered tcp ports* pada ringkasan. Hanya *port* 22 (SSH) yang tetap terbuka karena aturan izinnya tidak dihapus. Status *FILTERED* pada Nmap adalah indikator keberhasilan utama dari *packet filtering*. Secara teknis, ini terjadi karena UFW dikonfigurasi untuk melakukan aksi *DROP* alih-alih *REJECT*. Ketika nmap mengirimkan paket *SYN* ke *port* 80, *firewall* mencegat paket tersebut dan membuangnya diam-diam tanpa mengirimkan balasan ICMP *port unreachable* atau paket *RST* (Reset) ke penyerang. Akibatnya, Nmap harus menunggu hingga batas waktu *timeout* habis sebelum menyimpulkan bahwa *port* tersebut mungkin ada, tapi dilindungi *firewall*. Hasil ini membuktikan hipotesis penelitian bahwa UFW efektif mengubah visibilitas jaringan. Hal ini sesuai dengan tujuan mitigasi serangan port scanning di mana penyerang dipersulit untuk memetakan layanan. Berbeda dengan penelitian Wibowo Adi et al. (2024) yang menggunakan konfigurasi manual *iptables* yang kompleks [6], penggunaan UFW dalam penelitian ini membuktikan bahwa hasil *filtering* yang sama kuatnya status *Filtered* dapat dicapai dengan perintah yang lebih sederhana, meminimalkan *human error* dalam konfigurasi keamanan. Hal ini juga sejalan dengan teori *defense in depth* [5], di mana menyembunyikan port adalah lapisan pertahanan pertama.

3.4 Analisis Forensik *Log Firewall*

Salah satu fitur terpenting dari *stateful firewall* adalah kemampuannya mencatat aktivitas koneksi. Gambar 4

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 2 September 2026
Hal: 1674-1680
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i2.1427

menampilkan bukti *log* yang dihasilkan saat serangan *port scanning* terjadi.



Gambar 4. Log Aktivitas Pemblokiran Paket oleh UFW

Pada Gambar 4, terlihat baris-baris log dengan stempel waktu *timestamp* yang sangat rapat dalam detik yang sama. log didominasi oleh label [*UFW BLOCK*]. Informasi yang terekam meliputi antarmuka masuk (IN=enp0s3), alamat MAC pengirim (MAC=08:00:27...), alamat IP sumber (SRC=192.168.56.1), alamat IP tujuan (DST=192.168.56.101), dan protokol yang digunakan (PROTO=TCP). Data log ini berkorelasi langsung dengan hasil *filtered* pada zenmap. Ketiadaan respons dari server yang menyebabkan status *filtered* adalah akibat dari aksi blokir yang tercatat di log ini. Temuan ini mendukung teori Vidya et al. (2020) mengenai keunggulan *stateful inspection*. *Firewall* tidak hanya melihat alamat IP seperti *stateless*, tetapi memeriksa konteks paket. Jika dibandingkan dengan penelitian Sabila et al. (2025) yang menggunakan *snort* untuk deteksi [2], UFW memberikan pendekatan yang berbeda, *snort* mendeteksi *pola* serangan (*Signature Based*), sedangkan UFW memblokir berdasarkan *status koneksi* dan *kebijakan*. Kombinasi keduanya akan menghasilkan keamanan yang lebih robust, namun UFW sendiri terbukti cukup untuk memitigasi pemindaian dasar.

Keberadaan log ini juga memenuhi prinsip akuntabilitas dalam keamanan jaringan sebagaimana disebutkan dalam standar keamanan informasi. Status Blokir [*UFW BLOCK*] mengonfirmasi bahwa paket-paket tersebut cocok dengan aturan *default deny*. Pola serangan terlihat bahwa SRC adalah IP penyerang dan DST adalah IP server. Adanya banyak entri dalam waktu singkat mengindikasikan serangan *scanning* intensitas tinggi seperti parameter -T4 pada Nmap. *Stateful inspection* membuktikan mekanisme *stateful*. Paket-paket ini dianggap *INVALID* atau *NEW* yang tidak sesuai aturan. Karena tidak ada entri sesi yang sah di tabel koneksi *state table* untuk paket-paket *probe* nmap ini, *firewall* langsung memutusnya.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 5 No 2 September 2026
Hal: 1674-1680
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v5i2.1427

4. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan *stateful packet filtering* menggunakan UFW pada server ubuntu 22.04 di lingkungan Poltekpar Medan terbukti efektif dan efisien dalam memitigasi serangan *port scanning*. Secara spesifik, UFW mampu mengubah status *port* layanan yang tidak diizinkan dari *open* menjadi *filtered*. Hal ini menyulitkan penyerang dalam melakukan pemetaan jaringan karena tidak adanya respon balasan dari server. Mekanisme *drop* paket yang diterapkan UFW terbukti lebih aman dibandingkan mekanisme *reject*, karena tidak memberikan informasi balik kepada penyerang bahwa server tersebut aktif. Fitur *logging* pada UFW berhasil merekam atribut serangan secara rinci, yang sangat vital untuk keperluan analisis forensik pasca-insiden. Dibandingkan dengan konfigurasi iptables manual, UFW menawarkan kemudahan manajemen tanpa mengorbankan kemampuan keamanan *stateful* dari kernel linux. Disarankan bagi pengembangan selanjutnya untuk mengintegrasikan UFW dengan sistem deteksi intrusi seperti Snort atau Suricata serta menerapkan *port knocking* untuk meningkatkan lapisan keamanan pada layanan SSH.

REFERENCES

[1] Z. Munawar and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *Jurnal Sistem Informasi-J-SIKA*, vol. 2, no. 1, pp. 14–20, 2020.

[2] M. I. Sabila, M. Tahir, S. D. Mardania, and R. I. Arifin, "Implementasi Snort Sebagai IDS Dalam Mendeteksi Serangan Port Scanning Nmap Pada Simulasi Jaringan Virtual," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 4, 2025.

[3] F. A. Sihombing, N. N. Zuhra, L. Zahra, R. Alfarisyi, H. Nisa, and R. A. Astiyanto, "Implementasi Keamanan Jaringan Menggunakan Firewall dan Intrusion Detection System (IDS) pada Infrastruktur Jaringan Skala Kecil–Menengah," *Jurnal Ilmu Komputer (JIKUM)*, vol. 2, no. 1, 2025.

[4] V. Vidya, Surono, and G. Setiarso, "Application Gateway dan Stateful Inspection Method Pada Implementasi Firewall Untuk Optimasi Keamanan Jaringan Komputer," *Jurnal Pengembangan Rekayasa dan Teknologi*, vol. 4, no. 2, pp. 87–97, 2020.

[5] C. Tarina, N. Ismara, L. Mahara, Alysa, and N. Azimah, "Studi Literatur: Perkembangan Teknologi Firewall Dan Strategi Pertahanan Jaringan Pada Sistem Komputer," *Jurnal Ilmu Komputer (JIKUM)*, vol. 2, no. 1, 2025.

[6] D. W. Adi, F. Irawan, Z. R. Athallah, and S. N. Neyman, "Implementasi Firewall menggunakan Fitur dari IPTables pada Sistem Operasi Linux," *Journal of Internet and Software Engineering*, vol. 1, no. 2, pp. 1–7, 2024.

[7] Rusdianto and R. Yusuf, "Comparison of Port Scanning, Vulnerability Scanning, and Penetration Testing Combinations for Network Vulnerability Detection in GNS3 Testbed," *Jurnal Teknik Informatika (JUTIF)*, vol. 6, no. 5, pp. 3526–3542, 2025.

[8] D. S. Rahmadani, T. Ariyadi, E. Novitasari, and D. Pertiwiningsih, "Analisis Kinerja Web Server Berbasis Linux Ubuntu 22.04," *Jurnal Tera*, vol. 5, no. 1, pp. 35–44, 2025.

[9] W. L. Jaelani, Yanto, and F. Khoirunnisa, "Penetration Testing Website Dengan Metode Black Box Testing Untuk Meningkatkan Kea manan Website Pada Instansi (Redacted)," *NARATIF*, vol. 5, no. 1, 2023.

[10] A. P. Walidin, F. P. Putri, and D. Kiswanto, "Kali Linux Sebagai Alat Analisis Keamanan Jaringan Melalui Penggunaan Nmap, Wireshark, dan Metasploit," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 1, 2025.

[11] K. Aziz, S. Zakir, W. Aprison, and L. Efriyanti, "Implementasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik Di SMKN 3 Payakumbuh," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 3, 2024.

[12] R. Rahman, A. K. Hartono, and E. Tanduklangi, "Serangan dan Deteksi Port Scanning Menggunakan Wireshark dan Snort," *Jejak Digital: Jurnal Ilmiah Multidisiplin*, vol. 1, no. 4b, pp. 2138–2144, 2025.

[13] D. H. Gutama, A. K. A. Estetikha, and R. A. Setiawan, "Penanganan Serangan Brute Force dan Port Scanning Pada Router Mikrotik ," *Journal Sistem Informasi, dan Teknologi Informasi*, vol. 1, no. 2, 2022.

[14] R. Elfandiar and T. Sutabri, "Analisa Pengembangan Keamanan Menggunakan Stateful Inspection dan Metode Semi Deskriptif," *Digital Transformation Technology (Digitech)*, vol. 3, no. 1, 2023.

[15] I. Setiawan, "Penerapan Firewall Dan Iptables Untuk Keamanan Data Pada Jaringan Publik Berbasis Linux Server," Skripsi/Tesis, Universitas Persada Indonesia Y.A.I, Jakarta, 2025.

[16] C. Rizal, Supiyandi, M. Zen, and M. Eka, "Perancangan Server Kantor Desa Tomuan Holbung Berbasis Client Server," *Bulletin of Information Technology (BIT)*, vol. 3, no. 1, pp. 24–29, Jun. 2022

[17] Khairul, Z. Syahputra, R. F. Wijaya, and I. Purnama, "Pengembangan Video Streaming Server Menggunakan Emby Server untuk Layanan Konten Video pada Website," *Jurnal Komputer Teknologi Informasi dan Sistem Komputer (JUKTISI)*, vol. 4, no. 2, pp. 1503–1508, Sep. 2025