Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 2 (2026) pp: 20667- 20677
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Analisis Risiko Roundcube Debian dengan CVSS dan Random Forest

Evaldo Manurung[1], Christin Sigiro[2], Lotar Mateus Sinaga[3]
[1,2,3]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas
[1]evaldomanurung31@gmail.com, [2]christinsigiro@gmail.com, [3]lotarmateus88@gmail.com

Abstrak

Penelitian ini menganalisis risiko keamanan Roundcube Mail Server pada Debian 12 melalui perbandingan kondisi sebelum dan sesudah penerapan keamanan dasar. Lingkungan pengujian dibangun pada jaringan lokal menggunakan domain evaldo.com agar konfigurasi server, client, dan koneksi dapat dikendalikan. Data dikumpulkan melalui validasi akses webmail, uji pengiriman dan penerimaan email, pemindaian port menggunakan Nmap, audit sistem menggunakan Lynis, pengujian web server menggunakan Nikto, serta pencatatan status UFW, Fail2Ban, dan Zabbix Agent. Setiap temuan teknis dinilai menggunakan Common Vulnerability Scoring System (CVSS), kemudian disusun menjadi dataset awal untuk rancangan klasifikasi risiko berbasis Random Forest. Hasil penelitian menunjukkan bahwa Roundcube tetap dapat diakses dan digunakan untuk aktivitas email pada kedua skenario pengujian. Meskipun UFW telah diaktifkan, Nmap masih mendeteksi port FTP, SSH, SMTP, DNS, HTTP, POP3, IMAP, IMAPS, dan POP3S dalam kondisi terbuka. Temuan tersebut menunjukkan bahwa aktivasi firewall belum secara langsung mengurangi eksposur layanan apabila rule yang diterapkan masih terlalu longgar dan belum disesuaikan dengan kebutuhan sistem. Risiko tertinggi ditemukan pada penggunaan HTTP tanpa HTTPS karena webmail memproses kredensial pengguna dan isi komunikasi melalui kanal yang tidak terenkripsi. Sebagian besar temuan lain berada pada kategori risiko sedang karena layanan masih terbatas pada jaringan lokal. Penelitian ini menyimpulkan bahwa keamanan dasar perlu dilanjutkan dengan hardening yang lebih spesifik, meliputi pembatasan rule firewall, penerapan HTTPS, penonaktifan service yang tidak diperlukan, penguatan autentikasi SSH, konfigurasi Fail2Ban, serta pemantauan log secara berkala. Dataset awal yang dihasilkan dapat menjadi dasar pengembangan dan pengujian kuantitatif model Random Forest pada penelitian selanjutnya dengan jumlah sampel yang lebih besar.

Kata Kunci: *Roundcube, Debian 12, CVSS, Random Forest, Keamanan Mail Server*

1. Latar Belakang

Mail server tetap menjadi layanan inti dalam komunikasi digital karena menangani pengiriman, penerimaan, penyimpanan, dan pengelolaan email. Layanan email tidak berdiri sebagai satu komponen tunggal. Di dalamnya terdapat SMTP untuk pengiriman pesan, IMAP atau POP3 untuk pengambilan pesan, DNS untuk pemetaan nama domain, web server untuk akses webmail, serta mekanisme autentikasi pengguna. Kompleksitas ini membuat administrator perlu memeriksa konfigurasi setiap service secara konsisten. Studi terbaru menunjukkan bahwa keamanan email masih menghadapi masalah konfigurasi pada SPF, MTA-STS, DANE, BIMI, TLS, auto-detect client, dan infrastruktur domain email (Liu et al., 2021; Czybik et al., 2023; Tatang et al., 2021; Yajima et al., 2023; Li et al., 2023; Tang et al., 2025; Ashiq et al., 2025; Lee et al., 2022; Bartoli, 2023).

Roundcube memberi akses email melalui browser. Fitur ini memudahkan pengguna kampus, laboratorium, organisasi kecil, dan jaringan lokal. Namun, webmail juga menambah permukaan serangan karena kredensial pengguna masuk melalui aplikasi berbasis web. Karena itu, akses HTTPS, validitas sertifikat, dukungan TLS, dan konfigurasi server harus dikelola dengan tepat. Kajian webmail menunjukkan bahwa konfigurasi HTTPS yang tidak konsisten dapat menimbulkan kerugian pada proses pengiriman dan akses email (Li et al., 2023). Temuan TLS dan auto-detect pada ekosistem email juga menunjukkan bahwa konfigurasi transport layer perlu diuji dari sisi server dan client (Tang et al., 2025).

Debian 12 sering dipakai sebagai sistem operasi server karena stabil, ringan, dan memiliki dukungan paket yang luas. Namun, keamanan server tidak cukup dinilai dari pilihan sistem operasi. Administrator juga perlu memeriksa service aktif, rule firewall, pembaruan paket, proteksi login, dan pemantauan log. Penelitian tentang hardening dan vulnerability management menegaskan bahwa pengurangan attack surface, pembatasan service, pengujian penetrasi, dan otomasi deteksi kerentanan dapat membantu mengurangi risiko teknis pada infrastruktur server (Sotiropoulos et al., 2023; Seara & Serrão, 2024; Akhilesh et al., 2022; Tudosi et al., 2023; Sarker et al., 2023; Echeverría et al., 2021).

Penelitian ini menggunakan Common Vulnerability Scoring System untuk memberi nilai awal pada setiap temuan. CVSS membantu peneliti menyusun prioritas perbaikan, tetapi skor tersebut tidak boleh dibaca sebagai ukuran risiko tunggal. Literatur terbaru menunjukkan bahwa CVSS memiliki keterbatasan ketika konteks sistem, eksposur service, dan potensi eksploitasi tidak dihitung secara memadai (Walkowski et al., 2021; Howland, 2021; Costa et al., 2022; Elder et al., 2024). Karena itu, penelitian ini membaca skor CVSS bersama status firewall, jenis service, dan kebutuhan fungsi mail server.

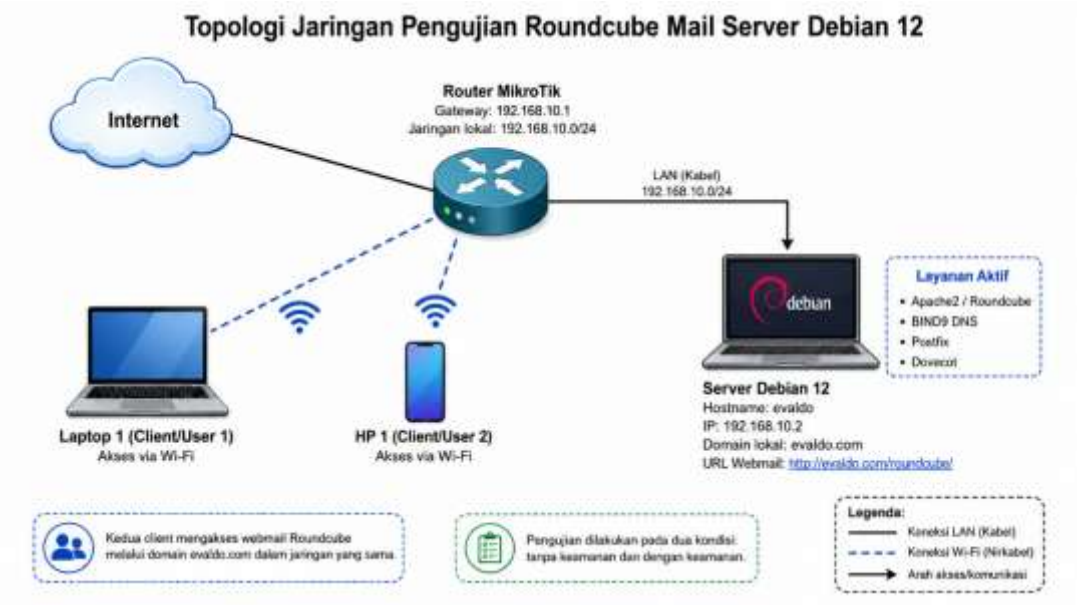
Penelitian ini juga merancang klasifikasi risiko menggunakan Random Forest. Pendekatan berbasis data dalam vulnerability assessment mulai banyak digunakan karena jumlah temuan keamanan terus bertambah. Dataset CVE, deskripsi kerentanan, fitur service, dan skor severity dapat mendukung proses klasifikasi risiko dan prioritas mitigasi (Costa et al., 2022; Elder et al., 2024; Bhandari et al., 2021; Kuppa et al., 2021; Silvestri et al., 2023; Fu et al., 2023; Cheimonidis & Rantos, 2023; Sun et al., 2023). Berdasarkan masalah tersebut, penelitian ini menganalisis keamanan Roundcube Mail Server Debian 12 sebelum dan sesudah keamanan dasar diterapkan, lalu menyusun dataset awal dari hasil Nmap, Lynis, Nikto, status firewall, skor CVSS, dan level risiko.

2. Metode Penelitian

Penelitian menggunakan eksperimen komparatif. Server Roundcube Mail Server Debian 12 diuji dalam dua skenario, yaitu kondisi tanpa keamanan dasar dan kondisi dengan keamanan dasar. Pengujian dilakukan pada laboratorium jaringan lokal agar konfigurasi server, client, dan koneksi dapat dikendalikan. Data dianalisis secara deskriptif, lalu disusun kembali menjadi data terstruktur untuk rancangan klasifikasi risiko. Tahapan penelitian meliputi perancangan topologi, pembangunan server, pengujian skenario pertama, penerapan keamanan dasar, pengujian skenario kedua, penilaian CVSS, penyusunan dataset, dan rancangan model Random Forest. Desain ini mengikuti prinsip vulnerability assessment yang menilai service, konfigurasi, dan bukti teknis secara berurutan (Seara & Serrão, 2024; Akhilesh et al., 2022; Tudosi et al., 2023; Sarker et al., 2023).

2.1. Lingkungan Pengujian

Objek penelitian adalah Roundcube Mail Server pada Debian GNU/Linux 12 Bookworm. Server dijalankan melalui VirtualBox dengan hostname evaldo dan alamat IP 192.168.10.2/24. Router menggunakan MikroTik dengan gateway 192.168.10.1. Domain lokal yang dipakai adalah evaldo.com, sedangkan akses webmail dilakukan melalui http://evaldo.com/roundcube/. Client uji terdiri atas laptop dan perangkat seluler dalam jaringan lokal yang sama. Lingkungan ini dipilih karena dekat dengan praktik pembelajaran administrasi mail server pada jaringan kecil dan memungkinkan bukti pengujian dikumpulkan secara langsung.



Gambar 1. Topologi jaringan pengujian Roundcube Mail Server Debian 12.

Tabel 1. Spesifikasi perangkat dan konfigurasi pengujian

Komponen	Keterangan
Objek penelitian	Roundcube Mail Server pada Debian GNU/Linux 12
Hostname server	evaldo
Virtualisasi	Oracle VM VirtualBox
IP server	192.168.10.2/24
Gateway	192.168.10.1
DNS server	192.168.10.2

DOI: https://doi.org/10.31004/riggs.v5i2.11597

Komponen	Keterangan
Domain lokal	evaldo.com
URL webmail	http://evaldo.com/roundcube/
Router	MikroTik
Jaringan pengujian	Jaringan lokal 192.168.10.0/24
Client uji	HP 1 dan HP 2 pada jaringan lokal
Akun pengguna uji	laptop1@evaldo.com dan hp1@evaldo.com
Perangkat scanner	Terminal Debian 12 pada server pengujian
Tools pengujian	Nmap, Lynis, Nikto, UFW, Fail2Ban, Zabbix Agent
Kondisi pengujian	Kondisi 1 tanpa keamanan dan kondisi 2 dengan keamanan

2.2. Skenario dan Teknik Pengumpulan Data

Pengujian dilakukan dalam dua skenario. Pada skenario pertama, keamanan dasar belum diterapkan dan UFW masih tidak aktif. Pada skenario kedua, keamanan dasar sudah diaktifkan. Status UFW, Fail2Ban, dan Zabbix Agent dicatat untuk melihat perubahan kontrol keamanan. Pada setiap skenario, Roundcube diakses melalui browser, lalu diuji dengan pengiriman dan penerimaan email antar-akun. Pengujian teknis memakai Nmap untuk melihat port dan service terbuka, Lynis untuk memeriksa konfigurasi sistem, dan Nikto untuk mengamati potensi kelemahan web server. Kombinasi alat ini mengikuti praktik penetration testing dan vulnerability assessment yang menggabungkan pemindaian service, audit konfigurasi, dan pengujian aplikasi web (Akhilesh et al., 2022; Tudosi et al., 2023; Sarker et al., 2023).

Gambar 2. Status UFW pada kondisi tanpa keamanan.

```
root@evaldo:~# cat /root/jurnal-roundcube/kondisi-2-dengan-keamanan/01-status-ufw.txt
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
80/tcp                     ALLOW IN    192.168.10.0/24
53/udp                     ALLOW IN    192.168.10.0/24
53/tcp                     ALLOW IN    192.168.10.0/24
25/tcp                     ALLOW IN    192.168.10.0/24
110/tcp                    ALLOW IN    192.168.10.0/24
143/tcp                    ALLOW IN    192.168.10.0/24
993/tcp                    ALLOW IN    192.168.10.0/24
995/tcp                    ALLOW IN    192.168.10.0/24
22/tcp                     ALLOW IN    192.168.10.0/24
10050/tcp                  ALLOW IN    192.168.10.0/24

root@evaldo:~#
```

Gambar 3. Status UFW pada kondisi dengan keamanan dasar.

2.3. Penilaian Risiko dan Rancangan Klasifikasi

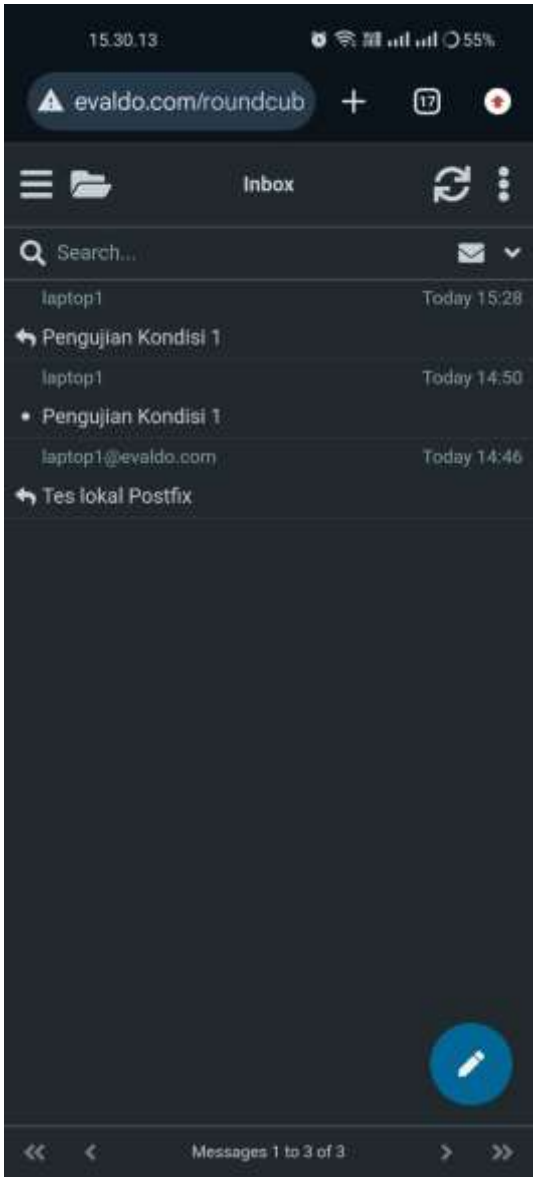
Setiap temuan dinilai dengan CVSS berdasarkan dampaknya terhadap kerahasiaan, integritas, dan ketersediaan layanan. Skor tersebut digunakan untuk mengelompokkan temuan ke dalam kategori Low, Medium, High, atau Critical. Karena CVSS memiliki batasan, hasil penilaian tetap dibaca bersama konteks server, status firewall, dan kebutuhan layanan (Walkowski et al., 2021; Howland, 2021; Costa et al., 2022; Elder et al., 2024). Setelah itu, temuan disusun menjadi dataset awal dengan atribut port, service, tool, status firewall, CVSS score, dan risk level. Dataset ini menjadi masukan awal untuk Random Forest. Pemilihan Random Forest didasarkan pada kebutuhan mengolah atribut kategorikal dan numerik secara bersamaan, serta pada penelitian terdahulu tentang prediksi, klasifikasi, dan perbaikan kerentanan perangkat lunak (Silvestri et al., 2023; Fu et al., 2023; Cheimonidis & Rantos, 2023; Sun et al., 2023).

DOI: https://doi.org/10.31004/riggs.v5i2.11597

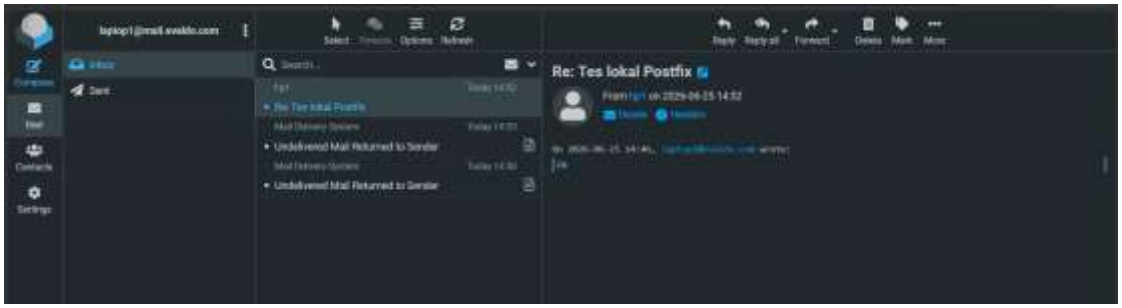
3. Hasil dan Diskusi

3.1. Validasi Layanan Roundcube

Pengujian awal memastikan bahwa Roundcube dapat diakses dari client pada jaringan lokal. Halaman login tampil melalui domain evaldo.com. Setelah login, pengguna berhasil mengirim dan menerima email. Hasil ini menunjukkan bahwa layanan utama webmail, seperti Apache2, Postfix, Dovecot, dan DNS lokal, sudah berjalan sesuai kebutuhan pengujian. Akses yang tetap berhasil pada kedua skenario juga menunjukkan bahwa penerapan UFW tidak memutus fungsi utama webmail.

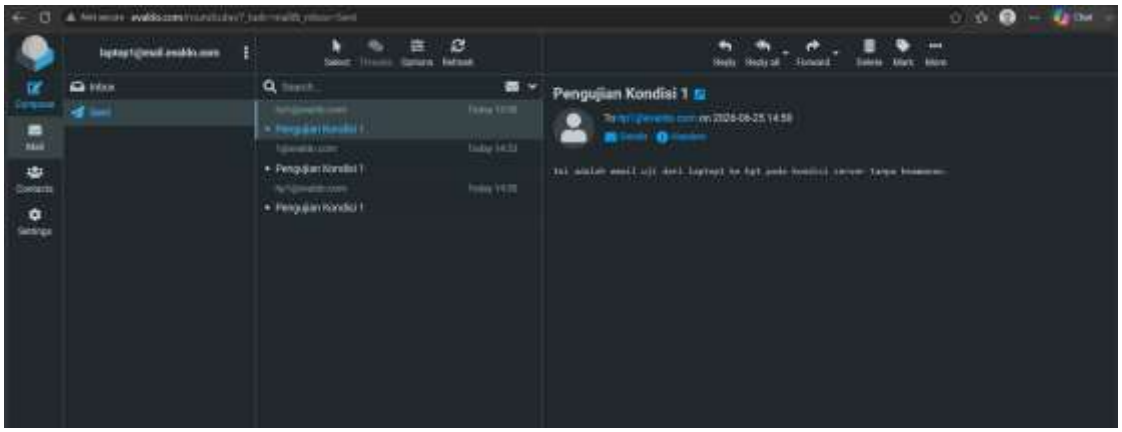


Gambar 4. Tampilan Roundcube pada client kondisi tanpa keamanan.



Gambar 5. Aktivitas email pada kondisi tanpa keamanan.

DOI: https://doi.org/10.31004/riggs.v5i2.11597



Gambar 6. Aktivitas email pada kondisi dengan keamanan dasar.

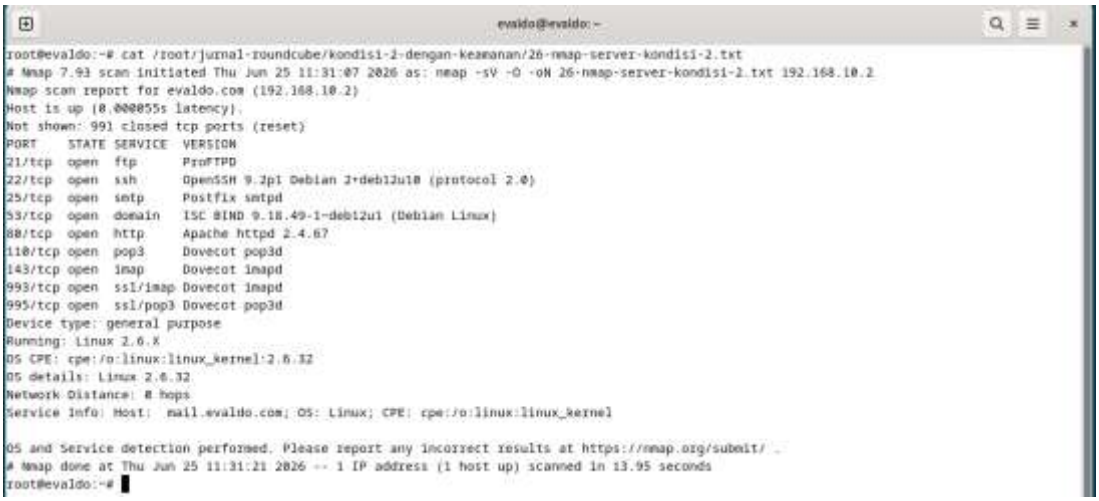
3.2. Hasil Pemindaian Port

Pemindaian Nmap dilakukan untuk memeriksa service yang terbuka pada server. Pada kondisi tanpa keamanan, Nmap mendeteksi FTP, SSH, SMTP, DNS, HTTP, POP3, IMAP, IMAPS, dan POP3S. Setelah UFW diaktifkan, daftar port yang terdeteksi tetap sama. Temuan ini penting karena firewall yang aktif belum tentu mengurangi eksposur apabila rule masih mengizinkan port tersebut dari jaringan client. Dalam pengelolaan server, port terbuka perlu disesuaikan dengan kebutuhan layanan agar permukaan serangan tidak lebih luas dari fungsi yang benar-benar diperlukan (Sotiropoulos et al., 2023; Seara & Serrão, 2024; Akhilesh et al., 2022; Tudosi et al., 2023; Sarker et al., 2023; Echeverría et al., 2021).

```
root@evaldo:~# cat /root/jurnal-roundcube/kondisi-1-tanpa-keamanan/19-nmap-server-kondisi-1.txt
# Nmap 7.93 scan initiated Thu Jun 25 11:07:09 2026 as: nmap -sV -O -oN 19-nmap-server-kondisi-1.txt 192.168.10.2
Nmap scan report for evaldo.com (192.168.10.2)
Host is up (0.000043s latency).
Not shown: 991 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      ProFTPD
22/tcp  open  ssh      OpenSSH 9.2p1 Debian 2+deb12u10 (protocol 2.0)
25/tcp  open  smtp     Postfix smtpd
53/tcp  open  domain   ISC BIND 9.18.49-1~deb12u1 (Debian Linux)
80/tcp  open  http     Apache httpd 2.4.67
110/tcp open  pop3     Dovecot pop3d
143/tcp open  imap     Dovecot imapd
993/tcp open  ssl/imap Dovecot imapd
995/tcp open  ssl/pop3 Dovecot pop3d
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: Host:  mail.evaldo.com; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jun 25 11:07:23 2026 -- 1 IP address (1 host up) scanned in 13.94 seconds
root@evaldo:~#
```

Gambar 7. Hasil pemindaian Nmap pada kondisi tanpa keamanan.



DOI: https://doi.org/10.31004/riggs.v5i2.11597

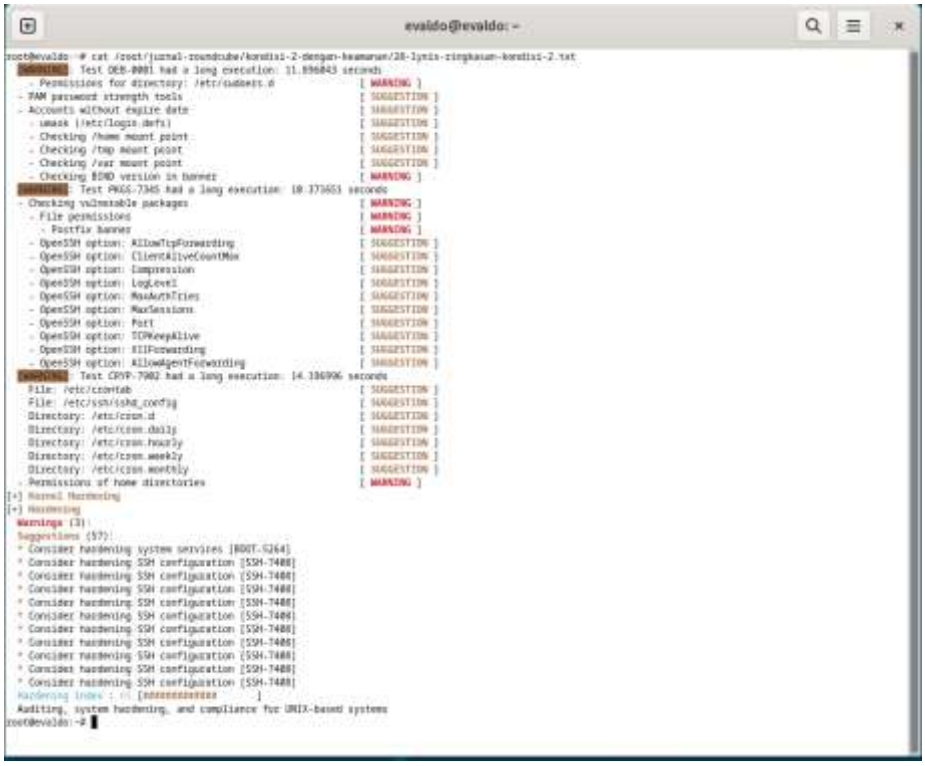
Gambar 8. Hasil pemindaian Nmap pada kondisi dengan keamanan dasar.

Tabel 2. Perbandingan port terbuka berdasarkan Nmap

Port	Service	Kondisi 1	Kondisi 2	Keterangan
21/tcp	FTP	Open	Open	Masih terbuka
22/tcp	SSH	Open	Open	Masih terbuka
25/tcp	SMTP	Open	Open	Masih terbuka
53/tcp	DNS	Open	Open	Masih terbuka
80/tcp	HTTP	Open	Open	Masih terbuka
110/tcp	POP3	Open	Open	Masih terbuka
143/tcp	IMAP	Open	Open	Masih terbuka
993/tcp	IMAPS	Open	Open	Masih terbuka
995/tcp	POP3S	Open	Open	Masih terbuka

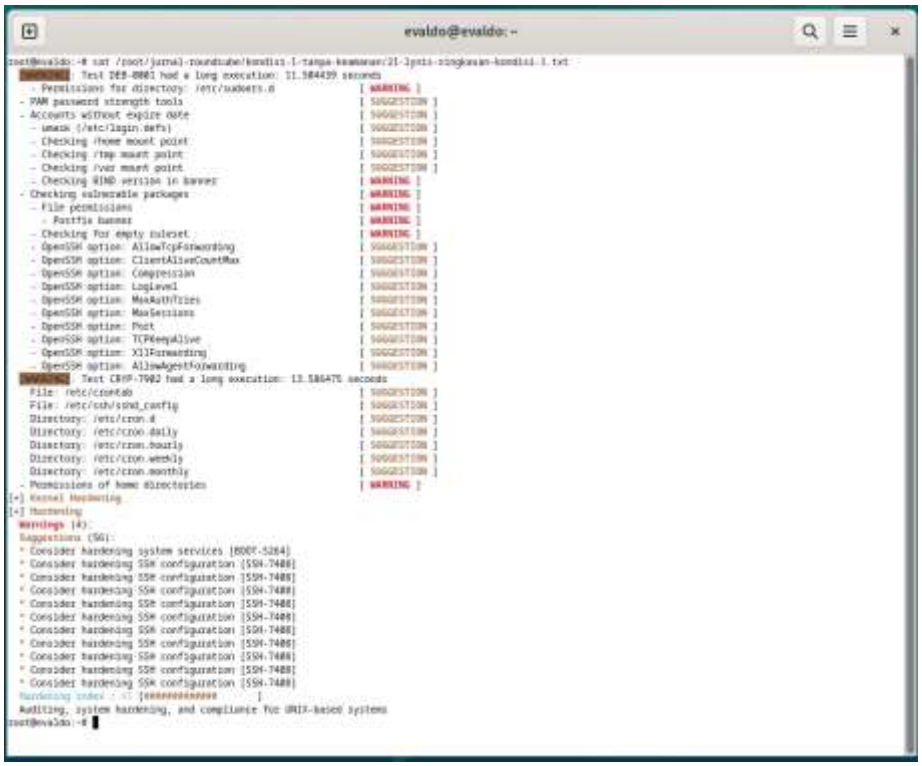
3.3. Audit Sistem dan Pengujian Web Server

Audit Lynis digunakan untuk membaca rekomendasi hardening sistem. Nikto digunakan untuk menguji sisi web server. Hasil audit memperlihatkan bahwa firewall aktif belum cukup untuk menyatakan server aman. Server masih memerlukan penguatan konfigurasi. Penilaian keamanan perlu menggabungkan beberapa sumber, seperti hasil pemindaian port, audit konfigurasi, dan log aktivitas. Literatur threat intelligence dan otomasi deteksi kerentanan juga menekankan bahwa risiko teknis lebih mudah diprioritaskan ketika data keamanan dari beberapa sumber digabungkan (Seara & Serrão, 2024; Silvestri et al., 2023; Sun et al., 2023).



Gambar 9. Ringkasan audit Lynis pada kondisi tanpa keamanan.

DOI: https://doi.org/10.31004/riggs.v5i2.11597



Gambar 10. Ringkasan audit Lynis pada kondisi dengan keamanan dasar.

Gambar 11. Hasil pengujian Nikto pada kondisi tanpa keamanan.

Gambar 12. Hasil pengujian Nikto pada kondisi dengan keamanan dasar.

Tabel 3. Perbandingan kontrol keamanan

Aspek	Kondisi 1	Kondisi 2	Analisis
UFW	Tidak aktif	Aktif	Kontrol firewall meningkat
Fail2Ban	Belum menjadi fokus	Dicatat/aktif jika tersedia	Ada tambahan proteksi login
Zabbix Agent	Belum menjadi fokus	Dicatat/aktif jika tersedia	Ada dukungan monitoring
Roundcube	Dapat diakses	Dapat diakses	Fungsi webmail tetap berjalan
Nmap	9 port terbuka	9 port terbuka	Belum ada penurunan eksposur port
Lynis	Ada rekomendasi	Ada rekomendasi	Hardening lanjutan masih dibutuhkan
Nikto	Ada temuan web	Ada temuan web	Konfigurasi web perlu diperkuat

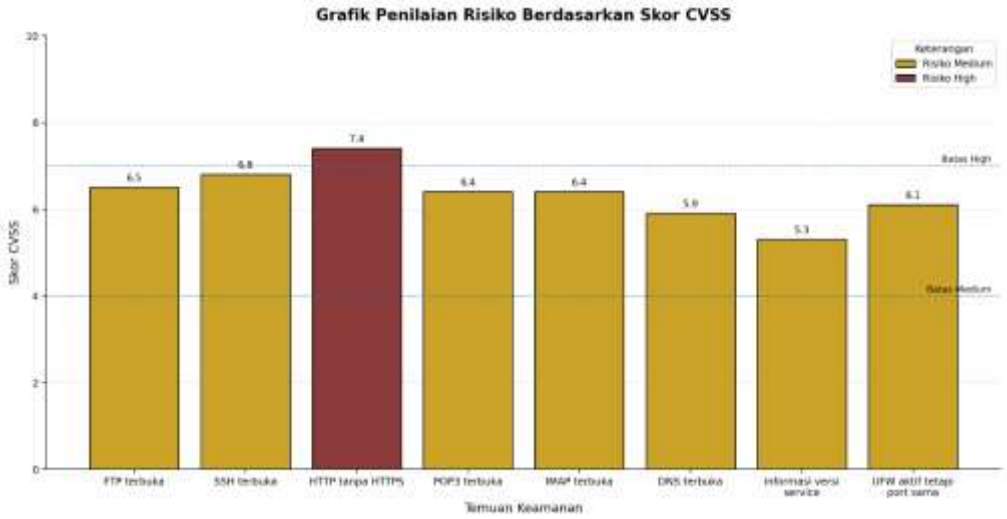
DOI: https://doi.org/10.31004/riggs.v5i2.11597

3.4. Analisis CVSS

CVSS digunakan untuk memberi prioritas awal pada temuan. Sebagian besar temuan masuk kategori Medium karena service terbuka masih berada di jaringan lokal. Namun, peluang penyalahgunaan tetap ada jika autentikasi lemah, konfigurasi tidak dibatasi, atau monitoring tidak aktif. Temuan HTTP tanpa HTTPS diberi kategori High karena webmail membawa kredensial pengguna dan isi komunikasi. Hasil ini mendukung penelitian webmail yang menekankan pentingnya konfigurasi HTTPS pada layanan berbasis browser (Li et al., 2023).

Tabel 4. Penilaian risiko berdasarkan CVSS

No	Temuan	Sumber	Dampak	Skor	Risiko
1	FTP terbuka	Nmap	Potensi penyalahgunaan akses file	6.5	Medium
2	SSH terbuka	Nmap	Potensi akses tidak sah	6.8	Medium
3	HTTP tanpa HTTPS	Nmap/Nikto	Risiko pencurian kredensial	7.4	High
4	POP3 terbuka	Nmap	Eksposur layanan email	6.4	Medium
5	IMAP terbuka	Nmap	Eksposur layanan email	6.4	Medium
6	DNS terbuka	Nmap/Lynis	Risiko penyalahgunaan DNS	5.9	Medium
7	Informasi versi service	Nmap/Lynis	Memudahkan fingerprinting	5.3	Medium
8	UFW aktif tetapi port sama	UFW/Nmap	Hardening belum optimal	6.1	Medium



Gambar 13. Grafik penilaian risiko berdasarkan skor CVSS

3.5. Dataset dan Rancangan Random Forest

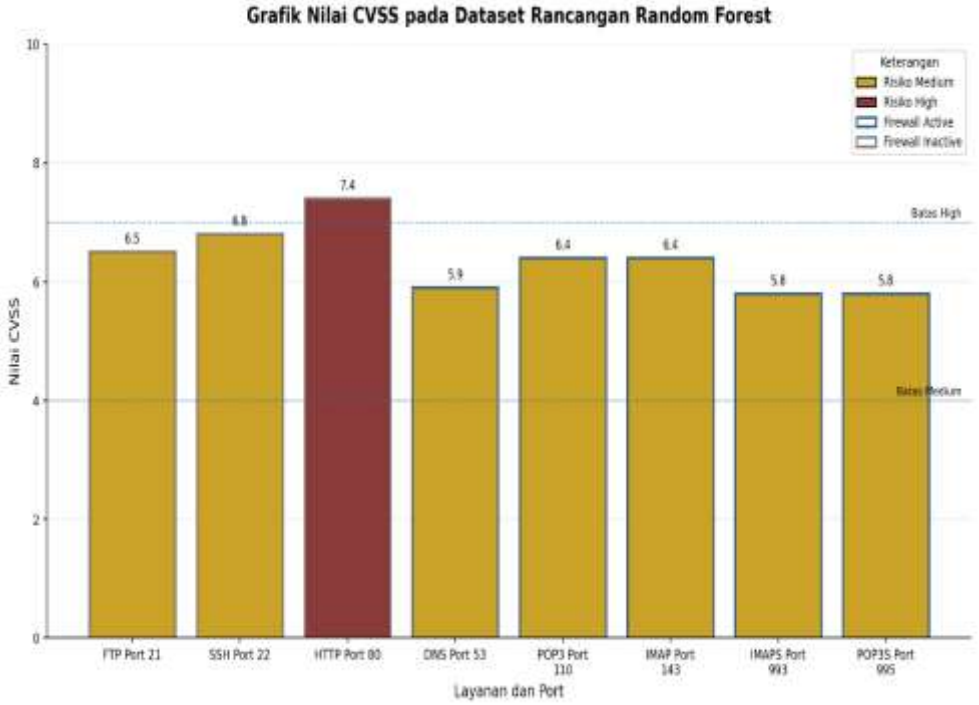
Hasil pengujian kemudian disusun sebagai dataset awal. Dataset ini belum menjadi model final karena jumlah data masih terbatas. Namun, struktur atributnya sudah memperlihatkan kebutuhan dasar untuk pengembangan klasifikasi risiko. Atribut port dan service menjelaskan objek temuan. Tool menunjukkan sumber deteksi. Status firewall menjelaskan konteks kontrol keamanan. CVSS score dan risk level digunakan sebagai dasar label. Pada penelitian berikutnya, dataset dapat diperluas dengan status enkripsi, jenis protokol, jumlah percobaan login gagal, hasil audit Lynis, hasil Nikto, dan log autentikasi. Pendekatan ini sejalan dengan penelitian klasifikasi kerentanan yang memanfaatkan fitur teknis, deskripsi, dan metrik severity (Costa et al., 2022; Bhandari et al., 2021; Kuppa et al., 2021; Silvestri et al., 2023; Fu et al., 2023; Cheimonidis & Rantos, 2023; Sun et al., 2023).

DOI: https://doi.org/10.31004/riggs.v5i2.11597

Gambar 14. Alur rancangan klasifikasi risiko menggunakan Random Forest

Tabel 5. Dataset rancangan Random Forest

No	Port	Service	Tool	Firewall	CVSS	Risk
1	21	FTP	Nmap	Inactive	6.5	Medium
2	22	SSH	Nmap	Inactive	6.8	Medium
3	80	HTTP	Nmap/Nikto	Inactive	7.4	High
4	53	DNS	Nmap/Lynis	Active	5.9	Medium
5	110	POP3	Nmap	Active	6.4	Medium
6	143	IMAP	Nmap	Active	6.4	Medium
7	993	IMAPS	Nmap	Active	5.8	Medium
8	995	POP3S	Nmap	Active	5.8	Medium



Gambar 15. Grafik penilaian risiko berdasarkan skor CVSS

3.6. Diskusi

Hasil penelitian memperlihatkan dua temuan utama. Pertama, Roundcube Mail Server Debian 12 dapat berjalan dan digunakan untuk aktivitas email pada jaringan lokal. Bukti pengujian terlihat dari akses login, pengiriman email, penerimaan email, dan balasan email pada kedua skenario. Kedua, keamanan dasar belum otomatis menurunkan jumlah port terbuka. UFW yang aktif memang menambah kontrol, tetapi rule yang masih mengizinkan seluruh service dari jaringan lokal membuat hasil Nmap tidak berubah. Karena itu, evaluasi firewall perlu melihat status layanan dan ketepatan rule secara bersamaan (Tudosi et al., 2023; Echeverría et al., 2021).

DOI: https://doi.org/10.31004/riggs.v5i2.11597

Dari sisi risiko, port FTP, SSH, POP3, IMAP, IMAPS, POP3S, DNS, dan HTTP perlu diperiksa kembali sesuai kebutuhan layanan. Dalam jaringan lokal, beberapa port memang dibutuhkan agar pengujian email dapat berjalan. Namun, pada penerapan nyata, setiap port sebaiknya dibatasi menurut kebutuhan pengguna, subnet yang diizinkan, dan protokol yang dipakai. FTP lebih aman jika diganti dengan mekanisme transfer yang lebih terlindungi atau dibatasi hanya untuk administrator. SSH perlu memakai autentikasi kuat, pembatasan alamat sumber, dan proteksi percobaan login. Akses webmail juga perlu menggunakan HTTPS agar kredensial tidak dikirim melalui kanal tidak terenkripsi (Li et al., 2023; Tang et al., 2025).

CVSS membantu menentukan prioritas temuan dalam penelitian ini. Namun, skor CVSS tidak dipakai sebagai ukuran risiko mutlak. Dua temuan dengan skor yang sama dapat memiliki prioritas berbeda jika berada pada layanan yang berbeda atau memiliki konteks akses yang berbeda. Kritik terhadap CVSS dan penelitian vulnerability management menunjukkan bahwa konteks lingkungan, potensi eksploitasi, dan karakteristik sistem tetap perlu dihitung ketika peneliti menyusun prioritas perbaikan (Walkowski et al., 2021; Howland, 2021; Costa et al., 2022; Elder et al., 2024; Sotiropoulos et al., 2023).

Rancangan Random Forest digunakan sebagai langkah awal untuk mengubah temuan teknis menjadi dataset yang lebih mudah dianalisis. Pada tahap ini, Random Forest belum digunakan untuk menghitung akurasi model karena jumlah sampel masih kecil. Meski demikian, rancangan dataset sudah menunjukkan arah pengembangan penelitian. Data scan, log, dan audit perlu dikumpulkan lebih banyak agar model dapat belajar dari variasi kondisi server. Arah ini sejalan dengan perkembangan vulnerability assessment modern yang menggabungkan severity score, fitur teknis, threat intelligence, dan machine learning untuk membantu prioritas perbaikan (Silvestri et al., 2023; Fu et al., 2023; Cheimonidis & Rantos, 2023; Sun et al., 2023).

4. Kesimpulan

Penelitian ini menyimpulkan bahwa Roundcube Mail Server Debian 12 berhasil berjalan pada jaringan lokal dan dapat diakses melalui domain evaldo.com maupun alamat IP server. Aktivitas pengiriman dan penerimaan email berjalan pada kondisi tanpa keamanan dan kondisi dengan keamanan dasar. Penerapan UFW pada skenario kedua menambah kontrol keamanan, tetapi belum menurunkan jumlah port terbuka berdasarkan pemindaian Nmap. Port FTP, SSH, SMTP, DNS, HTTP, POP3, IMAP, IMAPS, dan POP3S masih terbuka pada dua kondisi pengujian. Temuan dengan prioritas tertinggi adalah HTTP tanpa HTTPS karena berhubungan langsung dengan keamanan kredensial webmail. Dataset awal untuk rancangan Random Forest telah disusun dengan atribut port, service, tool pengujian, status firewall, skor CVSS, dan level risiko. Hasil ini menunjukkan bahwa keamanan dasar perlu dilanjutkan dengan hardening yang lebih spesifik, terutama pembatasan rule firewall, penggunaan HTTPS, evaluasi service yang tidak diperlukan, penguatan SSH, konfigurasi Fail2Ban, dan monitoring log berkala. Penelitian berikutnya dapat memperluas dataset dengan hasil scan, log autentikasi, percobaan akses gagal, dan fitur konfigurasi agar model klasifikasi risiko dapat diuji secara kuantitatif.

Referensi

1. Akhilesh, R., Bills, O., Chilamkurti, N., & Chowdhury, M. J. M. (2022). Automated penetration testing framework for smart-home-based IoT devices. Future Internet, 14(10), Article 276. https://doi.org/10.3390/fi14100276
2. Ashiq, M. I., Fiebig, T., & Chung, T. (2025). Unraveling the complexities of MTA-STS deployment and management in securing email. Proceedings of the ACM Internet Measurement Conference. https://doi.org/10.1145/3730567.3732916
3. Bartoli, A. (2023). Network architecture and ROA protection of government mail domains: A case study. Computer Communications. https://doi.org/10.1016/j.comcom.2023.02.004
4. Bhandari, G. P., Naseer, A., & Moonen, L. (2021). CVEfixes: Automated collection of vulnerabilities and their fixes from open-source software. Proceedings of the International Conference on Predictive Models and Data Analytics in Software Engineering. https://doi.org/10.1145/3475960.3475985
5. Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. Future Internet, 15(10), Article 324. https://doi.org/10.3390/fi15100324
6. Costa, J. C., Roxo, T., Sequeiros, J. B. F., Proenca, H., & Inacio, P. R. M. (2022). Predicting CVSS metric via description interpretation. IEEE Access. https://doi.org/10.1109/ACCESS.2022.3179692
7. Czybik, S., Horlboge, M., & Rieck, K. (2023). Lazy gatekeepers: A large-scale study on SPF configuration in the wild. Proceedings of the ACM Internet Measurement Conference. https://doi.org/10.1145/3618257.3624827
8. Echeverría, A. D., Cevallos, C., Ortiz-Garcés, I., & Andrade, R. (2021). Cybersecurity model based on hardening for secure Internet of Things implementation. Applied Sciences, 11(7), Article 3260. https://doi.org/10.3390/app11073260
9. Elder, S., Rahman, M. R., Fringer, G., Kapoor, K., & Williams, L. (2024). A survey on software vulnerability exploitability assessment. ACM Computing Surveys. https://doi.org/10.1145/3648610
10. Fu, M. C., Tantithamthavorn, C., Le, T., Kume, Y., Nguyen, V., Phung, D., & Grundy, J. (2023). AIBugHunter: A practical tool for predicting, classifying and repairing software vulnerabilities. Empirical Software Engineering. https://doi.org/10.1007/s10664-023-10346-3
11. Howland, H. (2021). CVSS: Ubiquitous and broken. Communications of the ACM. https://doi.org/10.1145/3491263
12. Kuppa, A., Aouad, L. M., & Le-Khac, N.-A. (2021). Linking CVE's to MITRE ATT&CK techniques. Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment. https://doi.org/10.1145/3465481.3465758
13. Lee, H., Ashiq, M. I., Muller, M., van Rijswijk-Deij, R., Kwon, T., & Chung, T. (2022). Under the hood of DANE mismanagement in SMTP. Zenodo. https://doi.org/10.5281/zenodo.7696293

DOI: https://doi.org/10.31004/riggs.v5i2.11597

14. Li, R., Zhang, Z., Shao, J., Lu, R., Jia, X., & Wei, G. (2023). The potential harm of email delivery: Investigating the HTTPS configurations of webmail services. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2023.3246600
15. Liu, E., Akiwate, G., Jonker, M., Mirian, A., Savage, S., & Voelker, G. M. (2021). Who's got your mail? Proceedings of the ACM Internet Measurement Conference. https://doi.org/10.1145/3487552.3487820
16. Sarker, K. U., Yunus, F., & Deraman, A. (2023). Penetration taxonomy: A systematic review on the penetration process, framework, standards, tools, and scoring methods. Sustainability, 15(13), Article 10471. https://doi.org/10.3390/su151310471
17. Seara, J. P., & Serrão, C. (2024). Automation of system security vulnerabilities detection using open-source software. Electronics, 13(5), Article 873. https://doi.org/10.3390/electronics13050873
18. Silvestri, S., Islam, S., Papastergiou, S., Tzagkarakis, C., & Ciampi, M. (2023). A machine learning approach for the NLP-based analysis of cyber threats and vulnerabilities of the healthcare ecosystem. Sensors, 23(2), Article 651. https://doi.org/10.3390/s23020651
19. Sotiropoulos, P., Mathas, C.-M., Vassilakis, C., & Kolokotronis, N. (2023). A software vulnerability management framework for the minimization of system attack surface and risk. Electronics, 12(10), Article 2278. https://doi.org/10.3390/electronics12102278
20. Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2023.3273282
21. Tang, K., Tu, C., Mak, S. L. A., & Chau, S. Y. (2025). A multifaceted study on the use of TLS and auto-detect in email ecosystems. Proceedings of the Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2025.240532
22. Tatang, D., Flume, R., & Holz, T. (2021). Extended abstract: A first large-scale analysis on usage of MTA-STS. Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-030-80825-9_18
23. Tudosi, A.-D., Graur, A., Balan, D., & Potorac, A. D. (2023). Research on security weakness using penetration testing in a distributed firewall. Sensors, 23(5), Article 2683. https://doi.org/10.3390/s23052683
24. Walkowski, M., Oko, J., & Sujecki, S. (2021). Vulnerability management models using a common vulnerability scoring system. Applied Sciences, 11(18), Article 8735. https://doi.org/10.3390/app11188735
25. Yajima, M., Chiba, D., Yoneya, Y., & Mori, T. (2023). A first look at brand indicators for message identification (BIMI). Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-031-28486-1_20

DOI: https://doi.org/10.31004/riggs.v5i2.11597