# Analisis Keamanan Jaringan Wirelessmenggunakan Metode Penetration Testing Execution Standard (PTES)

*By* Bita Parga Zen

WORD COUNT 2825 TIME SUBMITTED 08-AUG-2023 05:02PM

PAPER ID 101844093

JURNAL SISTEM INFORMASI GALUH
Volume 1, Nomor 2, Juli 2023
(Satria Galang Saputra, S.Kom)
ISSN 2964-7740
https://ojs.unigal.ac.id/index.php/jsig/index

# Analisis Keamanan Jaringan *Wireless* menggunakan Metode *Penetration Testing Execution Standard* (PTES)

**Satria Galang Saputra[1], Bita Parga Zen[2], Abdurahman[3]**
[1,2]Institut Teknologi Telkom Purwokerto
[3]Universitas Sriwijaya
E-mail: [1]18102249@ittelkom-pwt.ac.id, [2]bita@ittelkom-pwt.ac.id, [3]abdurahman@unsri.ac.id

***Abstract***

*Network security has become a very important aspect along with the increase in the number of internet users. The Kalisapu Village Office, is a public service area located in Slawi District, Tegal Regency which currently uses Wireless Local Area Network (WLAN) network technology as a means of internet access and for various purposes, both administrative and other services to meet community needs. which only uses one wireless access point to access the internet network. Wireless networks must have good security to avoid various threats of crime, therefore it is necessary to analyze network security using the Penetration Testing Execution Standard (PTES) method, which is a framework or guide used as a reference for implementing network penetration. From the results of testing five times using the Kali Linux operating system virtual machine with the type of MAC authentication bypassing attack, each arp spoofing has a successful status while encryption cracking has three failures and two successes. Based on test results, it can be interpreted that the wireless network security system is quite safe, but it is necessary to make some improvements to the system configuration and network topology to strengthen the security system and minimize the threat of crime.*

***Keywords*** : *Network Security, WLAN, Penetration Testing Execution Standar.*

***Abstrak***

*Keamanan jaringan menjadi aspek yang sangat penting seiring dengan peningkatan jumlah pengguna internet, Dalam aspek kehidupan hampir semua dipengaruhi oleh internet termasuk dalam lingkup pekerjaan. Kantor Balai Desa Kalisapu Kecamatan Slawi Kabupaten Tegal merupakan tempat layanan publik yang berada di Kecamatan Slawi Kabupaten Tegal yang saat ini menggunakan teknologi jaringan Wireless Local Area Network (WLAN) sebagai sarana akses internet dan untuk berbagai keperluan baik bersifat administrasi maupun layanan lainnya untuk memenuhi kebutuhan masyarakat yang hanya menggunakan satu wireless access point untuk mengakses jaringan internet. Jaringan wireless harus memiliki keamanan yang baik untuk menghindari berbagai ancaman kejahatan, maka dari itu diperlukan analisis kemanan jaringan dengan metode Penetration Testing Execution Standard (PTES) yaitu suatu kerangka kerja atau panduan yang digunakan sebagai acuan melaksanakan penetrasi jaringan. Dari hasil pengujian sebanyak lima kali menggunakan virtual machine sistem operasi kali linux dengan jenis serangan bypassing mac authentication, arp spoofing masing-masing berstatus berhasil sedangkan cracking the encryption berstatus mengalami tiga kegagalan dan dua berhasil. Berdasarkan hasil pengujian tersebut dapat disimpulkan sistem keamanan jaringan wireless cukup aman namun perlu dilakukan beberapa perbaikan pada sistem konfigurasi serta topologi jaringannya untuk memperkuat sistem keamanan serta menimimalisir ancaman kejahatan.*

***Kata Kunci*** *: Keamanan Jaringan, WLAN, Penetration Testing Execution Standar.*

## I. PENDAHULUAN

Kemajuan teknologi informasi dan sistem pertahanan siber saat ini berkembang begitu pesat dengan kemajuan teknologi dalam bidang siber khususnya webserver dan database dapat menjadi ancaman pencurian data dan informasi sehingga diperlukan penilaian

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

keamanan untuk mencegah pencurian data[1]. Hasil survey dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dengan Indonesia Survey Center pada tahun 2019-2020 triwulan ke-2 menunjukkan peningkatan jumlah pengguna internet sebesar 73,7%, dari total 266,91 juta orang di Indonesia sebanyak 196,71 juta orang merupakan pengguna internet[2].

Tingginya jumlah pengguna internet di Indonesia tentu perlu dilakukan sebuah pengawasan dan pengamanan pada sistem agar terhindar dari serangan kejahatan siber. Menurut laporan Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Adminisrasi ruang Badan Siber dan Sandi Negara (BSSN) mencatat bahwa 88.414.926 serangan siber telah terjadi antara 1 Januari hingga 12 April 2020, pola serangan yang paling umum adalah *trojan activity* dengan sebesar 56% dan aktivitas Information gathering (pengumpulan informasi) hingga 43%[3].

Menurut laporan Badan Pusat Statistik pada tahun 2020 jumlah pengguna internet di Indonesia khususnya pedesaan pada lingkup pekerjaan mencatat 51,3 % yang artinya internet sekarang sudah banyak digunakan baik di pedesaan untuk urusan pekerjaan[4]. Seiring dengan kemajuan teknologi tersebut kemampuan sistem keamanan jaringan mutlak menjadi sangat penting untuk menjaga kenyamanan berselancar di internet. Sistem keamanan jaringan selayaknya harus selalu diukur dan ditingkatkan untuk mengurangi potensi kejahatan siber yang berdampak pada kerusakan atau terganggunya sistem jaringan komputer yang telah ada.

Kantor Balai Desa Kalisapu merupakan tempat layanan publik yang berada di Kecamatan Slawi Kabupaten Tegal yang saat ini menggunakan teknologi jaringan *Wireless Local Area Network* (WLAN) sebagai sarana akses internet untuk berbagai keperluan baik bersifat administrasi, menyimpan data-data warga pada *server* komputer lokal maupun layanan lainnya untuk memenuhi kebutuhan masyarakat. Oleh karena itu, analisis keamanan jaringan diperlukan untuk mengevaluasi kerentanan dalam sistem keamanan jaringan nirkabel.

Salah satu metode yang digunakan untuk menganalisis keamanan jaringan adalah uji penetrasi yang merupakan metode penilaian dan analisis pada sebuah sistem jaringan komputer. Dalam

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

analisis keamanan jaringan ini akan menggunakan penetration testing execution standard (PTES) sebagai acuan dalam pelaksanaanya. (PTES) adalah salah satu standar atau acuan yang digunakan sebagai panduan pengujian penetrasi yang berisi saran terperinci terkait metode dan teknik yang digunakan pada setiap tahap pengujian[5].

## II. METODE PENELITIAN

Sistem Jaringan Komputer

Jaringan komputer adalah jaringan telekomunikasi antara dua atau lebih perangkat yang saling terhubung sehingga dapat saling bertukar data atau informasi. Suatu jaringan komputer dapat terhubung jika perangkat dalam jaringan memiliki sebuah perangkat kartu jaringan yang dapat dihubungkan secara *wired* (kabel) atau *wireless* (nirkabel) sehingga dapat bertukar data/informasi dan berbagi sumber daya[6].

Jaringan *Wireless LAN*

*Wireless Local Area Network* adalah jaringan komputer yang menggunakan frekuensi radio dan infra merah sebagai media transmisi data. WLAN sering disebut sebagai jaringan nirkabel[7]. Proses komunikasi nirkabel ini dimulai dengan munculnya peralatan berbasis radio, seperti walkie-talkie, remote control, ponsel, dan peralatan radio lain, kebutuhan untuk menjadikan komputer sebagai barang yang mudah dibawa (mobile) dan mudah terintegrasi dengan jaringan yang ada mendorong pengembangan teknologi nirkabel.

Sistem Keamanan Jaringan Komputer

Keamanan jaringan adalah konfigurasi yang memiliki fungsi melindungi data, menjaga kerahasiaan, integritas, serta menjamin ketersediaan akses jaringan komputer, dalam keamanan jaringan terdiri beberapa aspek apabila sebuah jaringan komputer disebut aman jika memenuhi kategori berikut ini[8]:

1. *Confidentiality* (Kerahasiaan)
   Aspek untuk melindungi suatu informasi dengan membatasi pihak ketiga yang akan mengakses ke informasi tersebut hanya pengirim dan penerima yang mengetahuinya.
2. *Integrity* (Integritas)
   Aspek menjamin informasi atau data bisa konsisten, akurat, dan terjaga tidak dapat diubah oleh pihak lain dan hanya bisa diubah oleh pengirim dan penerima.
3. *Authentication*
   Mengutamakan validitas dari pengguna informasi atau data yang

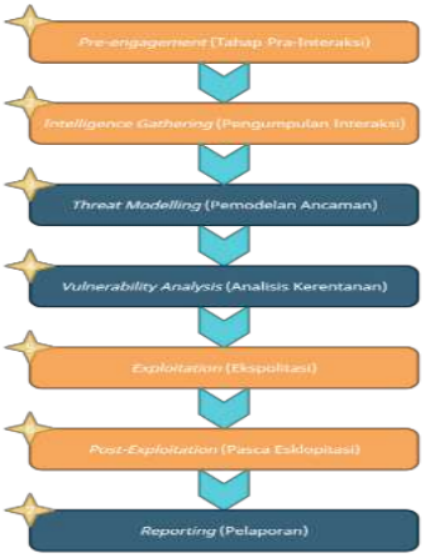
ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

valid berasal dari server asli yang diakses.

4. *Availability*
   Layanan informasi atau data dapat diakses kapanpun dan terjamin ketersediannya ketika akan digunakan.
5. *Non Repudiation*
   Aspek yang berkaitan dengan pencataan pengguna, ketika melakukan akses ke sistem atau jaringan pengguna tidak dapat menyangkal telah masuk ke sistem atau jaringan tersebut.

Penetration Testing

Penetration testing merupakan bagian dari jenis *ethical hacking* yaitu metode serta prosedur pengujian keamanan informasi. Penetration testing adalah aktivitas untuk mengevaluasi sebuah sistem dengan melakukan serangan untuk mengetahui celah keamanan pada sistem tersebut[9]. Dalam keamanan jaringan wireless, penetration testing digunakan untuk menambahkan firewall pada router yang dapat mengurangi resiko kerentanan sistem atau data yang terdapat didalamnya. Penetration testing memiliki standar atau pedoman yang dapat digunakan sebagai acuannya atau biasa disebut Penetration Testing Execution Standard (PTES). Standar ini memungkinkan seorang pentester dapat fokus mengeksploitasi area yang rentan dan memilih teknik serangan yang sesuai[10] [11].



Gambar 2. 1 Tahapan PTES

1. Pre-engagement (Pra Interaksi)
   Tahap persiapan atau kesepakatan yang dilakukan pentester kepada pemilik layanan agar tidak terjadi permasalahan pelanggaran hukum dan kebijakan.
2. Intelligence Gathering (Pengumpulan Informasi)
   Tahap pengumpulan informasi yang dapat membantu proses penetration testing yang dapat diambil dari beberapa metode yang pada penelitian ini berfokus penetration test keamanan jaringan wireless.
3. Threat Modelling (Pemodelan Ancaman)
   Tahap untuk melakasanakn penetration test yang benar dengan

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

melakukan pendekatan pemodelan ancaman agar lebih mudah menentukan serangan ke pemilik layanan yang dalam penelitian ini adalah serangan ke sistem jaringan wireless.

4. Vulnerability Analysis (Analisis Kerentanan)

   Tahap mencari dan menganalisa informasi kerentanan sistem jaringan wireless guna mempermudah dalam proses pentest yang diperloleh berdasarkan informasi yang didapatkan dari metode yang digunakan sebelumnya.

5. Exploitation (Eksploitasi)

   Tahap melakukan penetrasi test masuk ke sistem jaringan wireless untuk mengetahui celah keamanan jaringan dengan metode yang digunakan namun dilakukan setelah mengetahui celah keamanan yang bisa digunakan serta serangan yang dilakukan akan berhasil atau gagal.

6. Post Exploitation (Pasca Ekspoitasi)

   Tahap menyusun rencana setelah proses eksploitasi serta melakukan analisis bagian yang paling rentan dan menjelaksan bagian yang terkena resiko serta dampaknya dan memastikan prosedur yang disepakati sebelumnya dapat digunakan selama tahap pasca eksploitasi.

7. Reporting (Pelaporan)

   Tahap menyajikan laporan hasil setelah dilakukan uji penetrasi dengan melaporkan resiko yang ditemukan dan bagaimana rekomendasi penanggulangan resiko pada celah yang ditemukan [12].

## III. HASIL DAN PEMBAHASAN

***Pre-engagement* (Pra-Interaksi)**

Pada tahap ini penulis memberikan beberapa pertanyaan umum untuk mempermudah proses wawancara mengenai *network penetration test*, *wireless network penetration test*, *physical penetration test* dan *system administrator*.

***Intelligence gathering* (Pengumpulan informasi)**

Melakukan pengumpulan informasi sebanyak mungkin untuk membantu proses pengujian penetrasi jaringan *wireless* dengan metode pengumpulan data yang sudah dijelaskan diatas.

***Threat Modelling* (Pemodelan Ancaman)**

Mengidentifikasi ancaman (threat) pada celah keamanan yang mungkin terjadi untuk mempermudah penentuan serangan.

Tabel 3. 1 Pemodelan Ancaman(*Threat*)

| No | Identifikasi Ancaman (*threat*) |
|---|---|
| 1 | Enkripsi WPA2-PSK yang rentan terhadap serangan *bruto force* |

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

| | |
|---|---|
| 2 | Tidak mengaktifkan fitur *mac filtering* pada jaringan *wireless* |
| 3 | Siapa saja dapat langsung terhubung dengan mengetahui *password* yang diterapkan |
| 4 | Hanya menggunakan satu *router* dan *ssid* untuk akses internet dan berbagi data. |
| 5 | Tidak ada pembatasan akses |
| 6 | Pegawai kantor balai desa kalisapu belum mengerti sepenuhnya tentang keamanan sistem jaringan *wireless* |

***Vulnerability Analysis* (Analisis Kerentanan)**

Mencari dan mengidentifikasi beberapa celah keamanan jaringan wireless yang nantinya akan digunakan dalam pengujian keamanan jaringan wireless di kantor balai desa kalisapu.

Tabel 3. 2 Analisis Kerentanan

| No | Analisis Kerentanan |
|---|---|
| 1 | Enkripsi WPA2-PSK memiliki celah keamanan yang dapat diserang dengan teknik *cracking the encryption* dengan metode *bruto force* |
| 2 | Tidak menerapkan pembatasan *mac address* sehingga bisa ditiru, celah keamanan pada *mac filtering* yang tidak aktif dapat diserang melalui uji coba dengan teknik *bypassing mac address* dengan memodifikasi *mac address* yang sama dengan yang sudah terhubung. |
| 3 | Fitur *ARP binding* yang tidak aktif dapat di manfaatkan untuk memanipulasi *traffic data* dengan menonaktifkan koneksi jaringan sehingga *user* tidak dapat terhubung, celah ini dapat di uji coba melalui serangan *ARP Spoofing*. |

***Exploitasi* (Uji Simulasi Serangan)**

*Cracking the encryption*

Pada simulasi serangan ini menggunakan tools aircrack-ng untuk mengetahui ketahanan sistem keamanan jaringan wireless menggunakan keamanan *WPA2-PSK* yang terpasang di Kantor Balai Desa Kalisapu, pada tools aircrack-ng ini menggunakan metode *brute force* yaitu dengan menebak sebuah password yang sedang digunakan, metode ini membutuhkan sebuah kumpulan kata atau *wordlist* yang berisi kata-kata yang memungkinkan digunakan sebagai password yang akan membantu proses pemecahan sebuah password serta paket handshake yaitu proses sebuah perangkat ketika terhubung dengan jaringan tersebut, pengumpulan kata ini dilakukan dengan cara pengamatan serta eksperimen di lingkungan sekitar kantor balai desa, implementasi ini dilakukan sebanyak 5 kali dengan menggunakan wordlist yang berbeda pada setiap percobaan yang kemudian dilakukan pencocokan kata dengan paket handshake, percobaan keempat dan kelima berhasil dengan menemukan

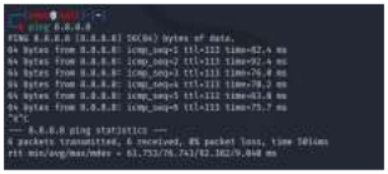
ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

password yang digunakan yaitu "lu*******if".

Gambar 3.1 Enkripsi Password Ditemukan

*Bypassing Mac Authentication*

*Bypassing MAC Address* merupakan pengujian dengan merubah suatu MAC perangkat untuk menguji penerapan *MAC address filtering*. Dalam pengujian ini penulis menggunakan tools Macchanger, yaitu sebuah tools yang tersedia pada sistem operasi kali linux, penulis melakukan perubahan nilai MAC pada kartu jaringan yang digunakan untuk mengakses jaringan internet yang pada percobaan kali ini dilakukan sebanyak 5 kali. Setelah proses perubahan nilai MAC, dalam pengujian akses internet penulis berhasil terhubung kedalam jaringan internet dan dipastikan jaringan *wireless* tidak menerapkan pembatasan *MAC Address*.



Gambar 3.2 Pengujian koneksi internet

*ARP Spoofing*

ARP Spoofing memanfaatkan celah keamanan pengiriman ARP secara broadcast dengan melakukan penyadapan terhadap perangkat yang sedang terhubung. pengujian ini dilakukan sebanyak 5 kali serta menggunakan tools Murder Death Kill 3 (mdk3) untuk memanipulasi pengguna dengan memutus koneksi jaringan sehingga pengguna seolah masih terhubung dalam jaringan internet akan tetapi sebenarnya koneksi jaringan sudah tidak dapat terhubung.

Gambar 3.3 Pengujian akses internet

**Report Pengujian Dengan Metode PTES**

Berikut penyampaian hasil dari seluruh tahap pengujian penetration testing yang dilakukan penulis menggunakan metode PTES yang dilakukan pada jaringan wireless Kantor Balai Desa Kalispu Kecamatan Slawi Kabupaten Tegal

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

| Jenis Serangan | Data yang dibutuhkan | Batasan Pengujian | Tools | Status Pengujian |
|---|---|---|---|---|
| *Cracking The Encryption* | *Handshake*, *wordlist*, SSID target | *Crack password* wifi | Aircrack-ng | Gagal<br>Gagal<br>Gagal<br>Berhsil<br>Berhsil |
| *Bypassing Mac Address* | Daftar alamat MAC yang terhubung | Merubah alamat MAC untuk masuk kedalam jaringan | Macchanger | Berhasil<br>Berhasil<br>Berhasil<br>Berhasil<br>Berhasil |
| *ARP Spoofing* | Daftar perangkat yang terhubung | Memutus koneksi jaringan (*offline*) | Murder Death Kill 3 (MDK 3) | Berhasil<br>Berhasil<br>Berhasil<br>Berhasil<br>Berhasil |

## IV. KESIMPULAN

Berdasarkan tahap uji penetrasi yang dilakukan, sistem keamanan jaringan wireless di Kantor Balai Desa Kalisapu cukup aman dengan sudah menerapkan sistem enkripsi WPA2-PSK akan tetapi masih rentan terhadap serangan, berdasarkan uji serangan cracking the encryption keamanann tersebut masih bisa diekspolitasi dengan teknik brute force untuk mencari kata sandi berdasarkan paket handshake dan wordlist yang telah dibuat. Konfigurasi dan topologi jaringan yang digunakan perlu dilakukan beberapa perbaikan seperti dalam tahap uji serangan yang lainnya menggunkan teknik Bypassing MAC Address serta ARP Spoofing pengujian ini berstatus berhasil selama lima kali pengujian, perlu diperbaiki konfigurasi sistem keamanan jaringan wireless serta topologi jaringan yang dipakai untuk menghindari serangan jaringan wireless seperti cracking the encryption, Bypassing MAC Authentiaction, ARP Spoofing.

## V. SARAN

Gunakan kombinasi password berupa huruf kapital atau kecil, angka, dan karakter dengan ukuran minimal 8 yang bertujuan meminimalisir serangan cracking the encryption.

Mengaktifkan sistem MAC Filtering berfungsi mencegah serangan Bypassing Mac Authentication dengan mendaftarkan perangkat yang digunakan di kantor balai desa kalisapu.

## DAFTAR PUSTAKA

[1] B. P. Zen, R. A. G. Gultom, A. H. S. Reksoprodjo, P. T. Penginderaan, T. Pertahanan, and U. Pertahanan, "ANALISIS SECURITY ASSESSMENT MENGGUNAKAN METODE PENETRATION TESTING DALAM MENJAGA KAPABILITAS KEAMANAN TEKNOLOGI INFORMASI PERTAHANAN NEGARA SECURITY ASSESSMENT

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

ANALYSIS USING PENETRATION TESTING METHODS IN MAINTAINING THE SECURITY CAPABILITY OF NATIONAL DEFENSE INFORMATION TECHNOLOGY," 2020.

[2] Humas APJII, "Laporan Survei Internet APJII 2019-2020 (Q2)," 2020. https://apjii.or.id/survei. (accessed Nov. 10, 2021).

[3] B. H. dan K.-B. Bagian Komunikasi Publik, "Rekap Serangan Siber (Januari – April 2020)," *Badan Siber dan Sandi Negara*, Apr. 20, 2020.

[4] Badan Pusat Statistik Indonesia, "Pengguna Internet di Indonesia," 2020.

[5] D.M. Sari, M. Yamin, and LM.B. Aksara, "Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration Testing," *J. semanTIK*, vol. 3, pp. 203–208, 2017.

[6] Iqsyahiro, "Modul Mata Kuliah Jaringan Komputer," 2019.

[7] Zawiyah and Rini, "Desain Jaringan WLAN Berdasarkan Cakupan Area dan Kapasitas," *J.Infotel*, vol. 8, pp. 115–123, 2016.

[8] A. Kholiq and D. Khoirunnisa, "ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) DENGAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES) (STUDI KASUS : PT. WIN PRIMA LOGISTIK)," 2019.

[9] Ec-Council, *Modul CEH v8 Penetration Test*.

[10] Admin, "High level organization of the standard," 2014. http://www.pentest-standard.org/ (accessed Jan. 11, 2022).

[11] P. P. Anggraeni and Z. Pertahanan, "SECURITY ANALYSIS ON WEBSITES USING THE INFORMATION SYSTEM ASSESSMENT FRAMEWORK (ISSAF) AND OPEN WEB APPLICATION SECURITY VERSION 4 (OWASPv4) USING THE PENETRATION TESTING METHOD," vol. 8, no. 3, pp. 2549–9459, 2022, doi: 10.33172/jp.v8.

[12] S. Andriyani, M. Fajar Sidiq, and B. Parga Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar," 2023.

[13] Firdaus, E. A., & Maulani, S. (2023). Perencanaan Kerangka Kerja Menggunakan The Open Group Architecture Framework-Architecture Development Method (TOGAF-ADM) pada Puskesmas Sukatani. *Jurnal Sistem Informasi Galuh*, *1*(1), 32–37.

# Analisis Keamanan Jaringan Wirelessmenggunakan Metode Penetration Testing Execution Standard (PTES)

ORIGINALITY REPORT

10%
SIMILARITY INDEX

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | repository.usd.ac.id<br>Internet | 37 words — 1% |
| 2 | masturah.com<br>Internet | 23 words — 1% |
| 3 | www.coursehero.com<br>Internet | 22 words — 1% |
| 4 | blitarjay.blogspot.com<br>Internet | 20 words — 1% |
| 5 | journal.uib.ac.id<br>Internet | 20 words — 1% |
| 6 | repository.ub.ac.id<br>Internet | 20 words — 1% |
| 7 | Amiruddin Amiruddin, Hafizh Ghozie Afiansyah, Hernowo Adi Nugroho. "Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8", 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS, 2021<br>Crossref | 10 words — < 1% |
| 8 | Fahmi Fachri, Abdul Fadlil, Imam Riadi. "Analisis Keamanan Webserver menggunakan Penetration | 10 words — < 1% |

Test", Jurnal Informatika, 2021
Crossref

| | | |
|---|---|---|
| 9 | Submitted to Telkom University<br>Your Indexed Documents | 10 words — < 1% |
| 10 | jurnal.untan.ac.id<br>Internet | 10 words — < 1% |
| 11 | koreascience.or.kr<br>Internet | 10 words — < 1% |
| 12 | core.ac.uk<br>Internet | 9 words — < 1% |
| 13 | www.tutorialspoint.com<br>Internet | 9 words — < 1% |
| 14 | 123dok.com<br>Internet | 8 words — < 1% |
| 15 | Adams Pratama Yanuar. "Cyber war : Ancaman Baru Keamanan Nasional dan Internasional", Jurnal Keamanan Nasional, 2021<br>Crossref | 8 words — < 1% |
| 16 | teknik.usni.ac.id<br>Internet | 8 words — < 1% |
| 17 | ukitoraja.ac.id<br>Internet | 8 words — < 1% |

| | | | |
|---|---|---|---|
| EXCLUDE QUOTES | ON | EXCLUDE SOURCES | OFF |
| EXCLUDE BIBLIOGRAPHY | ON | EXCLUDE MATCHES | OFF |