32. HASIL CEK_60960140

by 60960140 Te

Submission date: 08-Aug-2022 11:51AM (UTC+0700)
Submission ID: 1880114987
File name: 32. TE-60960140-Analisis Keamanan Webserver Menggunakan Penetration Test.pdf (305.57K)
Word count: 3241
Character count: 20133

JURNAL INFORMATIKA, Vol. 8 No. 2 September 2021, Halaman 183~190
ISSN: 2355-6579 I E-ISSN: 2528-2247

Analisis Keamanan *Webserver* Menggunakan Penetration Test

Fahmi Fachri [1], Abdul Fadlil[2], Imam Riadi[3]

[1]Program Studi Informatika, Universitas Ahmad Dahlan, Yogyakarta
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
[3]Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta
Jln. Prof. Dr. Soepomo, Janturan, Yogyakarta, 55164.

e-mail: [1]fahmi2007048017@webmail.uad.ac.id, [2]fadlil@mti.uad.ac.id, [3]imam.riadi@is.uad.ac.id.

Informasi Artikel	Diterima: 28-06-2021	Direvisi: 28-07-2021	Disetujui: 25-08-2021

Abstrak

Keamanan adalah faktor penting yang harus diperhatikan dalam membangun sebuah *web server*. Pengujian Penetrasi didefinisikan sebagai upaya legal dan resmi untuk mengekploitasi sistem komputer dengan tujuan mencari kerentanan pada *web server* serta meningkatkan keamanan sistem. Pengujian penetrasi ini dilakukan pada *web server* yang merupakan Sistem Informasi Akademik pada perguruan tinggi. Metode yang digunakan dalam penelitian ini mencakup *Information Gathering, Vullnerability Assessmant, gaining acces, maintaining acces, Clearing Track*. Hasil penelitian menampilkan bahwa terdapat empat kelemahan pada *web server* yaitu level high, empat kelemahan level medium, dan dua kerentanan dengan level low. Ditemukannya beberapa port yang masih terbuka dalam *web server* yang menyebabkan peretas dengan mudah masuk kedalam sistem untuk mengekploitasi informasi yang terdapat dalam Sistem Informasi Akademik. Hasil ujicoba simulasi serangan terhadap sistem berhasil masuk dengan mendapatkan *username* dan *password*.

Kata Kunci: *Web server, Penetration test, log*

Abstract

Security is one of the important factors that must be considered in building a web server. Penetration test is defined as a legal and official effort to exploit computer systems with the aim of finding vulnerabilities in webservers and improving system security. Penetration test is carried out on a web server which is an academic information system at a university. The methods used in this research include Information Gathering, Vullnerability Assessmant, gaining access, maintaining access, Clearing Track. The results of the study show that there are four vulnerabilities on the website with a high level, four vulnerabilities with a medium level, and two vulnerabilities with a low level. Dhe discovery of several ports that are still open on the webserver that causes hackers to easily enter the system to exploit the information contained in the academic information system. The results of the simulation trial of the attack on the system successfully entered by getting a username and password.

Keywords: *Web server, Penetration test, log*

1. Pendahuluan

Keamanan jaringan menjadi aspek yang sangat penting seiring dengan peningkatan volume data yang dipertukarkan di internet. Setiap organsiasi maupun perusahaan dituntut untuk selalu menjaga kerahasiaan, integritas dan otentikasi data pada sebuah *web server* sesuai standar keamanan internasional. Hal ini salah satunya disebabkan oleh meningkatnya ketergantungan masyarakat pada sistem informasi jaringan sehingga keamanan keseluruhan dari sistem harus selalu diukur dan ditingkatkan. Selain itu resiko kurangnya kemanan dalam system menjadikan potensi masuknya *hacker* kedalam *system* yang berdampak pada kerusakan atau beralihnya fungsi *system* yang telah dibuat.

Beberapa penelitian telah melakukan pengujian keamanan *web server* dengan berbagai metode diantaranya dengan metode suricata (Nazwita, 2017); SSE-CMM ISO 27002: 2013 (Kurniawan & Riadi, 2018) dan Bot telegram (Rheno Widianto & Abdullah Azzam, 2018). Selain itu terdapat pula riset yang menggunakan metode penetatrion testing (Stiawan et al., 2016)

JURNAL INFORMATIKA, Vol. 8 No. 2 September 2021
ISSN: 2355-6579 I E-ISSN: 2528-2247

Penelitian ini akan menguji kelemahan dan kerentanan *web server* dengan objek perguruan tinggi. Setiap perguruan tinggi pasti pernah mengalami permasalahan pada *web server.* Salah satu kasus yang sering terjadi adalah terkait Sistem Infromasi Akademik (SIA). Sistem Informasi Akademik dibuat dengan tujuan untuk memberikan layanan akademik kepada dosen, karyawan dan mahasiswa. Beberapa permasalahan yang sering dihadapi adalah *hacking system*, dirubah *file index* hingga meng *injectkan file backdoor* dalam sistem, dan ini akan menjadi bahaya jika ada seseorang dan tidak bertanggung jawab mencoba untuk melakukan *attack website* secara terus menerus maka Sistem Informasi Akademik tidak bisa berjalan sebagaimana mestinya. Oleh karena itu penting untuk diteliti bagaimana keamanan sistem informasi akademik tetap terjaga informasi dan semua data yang ada didalamnya.

Cara paling akurat untuk mengevaluasi sikap keamanan informasi organisasi adalah dengan mengamati bagaimana organisasi tersebut berdiri melawan serangan, cara terbaik untuk memastikan bahwa sistem aman adalah dengan mencoba pengujian penetrasi, pengujian penetrasi sering kali memungkinkan analisis keamanan menemukan kerentanan baru (Zeebaree et al., 2020)

Beberapa Negara yang *Web server* nya terkena serangan oleh *hacker.*

Sumber : (Jofie yordan, 2019)

Gambar 1. Data Negara yang servernya dibobol *hacker*

Terdapat lima negara paling tinggi yang terkena serangan para hacker , adalah :

- China
- Malaysia
- Indonesia
- India
- Vietnam

Indonesia menduduki peringkat ke-2 dengan jumlah serangan 39.957 *server* dalam laporan survey BSSN (Badan Siber dan Sandi Negara).

Data Skala Nasional Indonesia serangan *Webserver* oleh para *Hacker*

Sumber : (Salsabila, 2020)

Gambar 2. Data skala Nasional serangan Web Server

Menurut data diatas yang telah dihimpun oleh Badan Siber dan Sandi Negara (BSSN), menjelaskan bahwa dari mulai bulan Januari sampai bulan Agustus 2020, menghasilkan sebanyak 190 juta dalam upaya serangan terhadap *web server* yang ada di Indonesia, data ini menunjukan bahwa ada kenaikan lebih dari lima kali lipat dibanding jumlah data yang sama pada tahun lalu yang tercatat di kisaran 39 juta.

Angka paling banyak tercatat pada bulan Agustus 2020, bahwa Badan Siber dan Sandi Negara (BSSN) mencatat jumlah serangan siber di kisaran 63 juta, jauh lebih tinggi dibandingkan Agustus 2019 yang hanya di kisaran 5 juta.

Data diatas menunjukan bahwa keadaan *web server* yang ada di indonesia masih jauh dari keadaan aman dari ancaman dan serangan.

Penelitian ini menggunakan *Penetration Test* atau mencari kerentanan yang ada pada *Web server.* Hasil dari pengujian ini diharapkan dapat dicermati pola serangan yang dilakukan oleh para *Hacker*, dan tindakan yang dapat dilakukan dalam mengamankan sebuah *Web Server.*

1.1 Pengertian Penetrasi *Testing*

Pengujian penetrasi (juga dikenal sebagai pentesting atau PT) adalah praktik umum untuk secara aktif menilai pertahanan jaringan komputer atau *(Web Server)* dengan merencanakan dan mengeksekusi semua kemungkinan serangan untuk menemukan dan mengeksploitasi kerentanan yang ada. (Ghanem & Chen, 2020).

Pengujian penetrasi menggunakan metode dan cara yang digunakan oleh penjahat dunia maya untuk menemukan kerentanan ini, tetapi diizinkan untuk melakukannya. Ini berarti tidak seperti penjahat dunia maya penguji penetrasi memiliki persetujuan / izin dari organisasi yang sedang diuji (Kelrey & Muzaki, 2019)

Pengujian penetrasi adalah bagian penting dari penilaian keamanan dunia maya, dengan fokus pada potensi kerentanan yang terkait sistem yang ada . Sebelum sistem TI

diterapkan, praktik terbaik pengamanatkan penetrasi yang lengkap pengujian harus dilakukan dan diulang secara teratur, baik secara rutin maupun saat sistem dikonfigurasi ulang, untuk memastikan perlindungan dari kerentanan baru.

1.2 *WebServer*

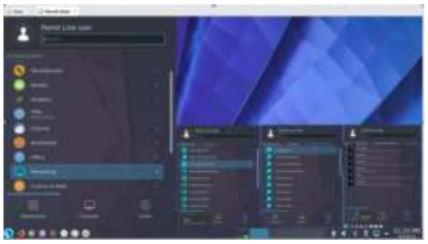
Web Server adalah sebuah *Software* dalam sebuah *Server* yang berfungsi menerima permintaan *(Request)* berupa halaman *Website* melalui HTTP atau HTTPs dari *Client* (*Browser*) dan mengirimkan kembali (*Response*) dalam bentuk halaman – halaman *Website* yang umumnya berbentuk HTML (Nurkamiden et al., 2017).

Web Server juga memilki fungsi tidak hanya mengolah data tapi dapat juga mengirimkan data berupa file foto dan video berdasarkan permintaan *Client*. *Web Server* dapat berjalan secara *Online*.

1.3 Sistem Operasi *Parrot Linux*

Parrot OS, produk unggulan dari *Parrot Security* adalah distribusi *GNU / Linux* berbasis Debian dan dirancang dengan mengutamakan Keamanan dan Privasi. Mencakup laboratorium *portable* lengkap untuk semua jenis operasi keamanan dunia maya, mulai dari pentesting hingga forensik digital dan rekayasa balik, tetapi juga mencakup semua yang diperlukan untuk mengembangkan perangkat lunak dan menjaga keamanan data.

Parrot adalah komunitas pengembang dan pakar keamanan di seluruh dunia yang bekerja sama untuk membangun kerangka alat bersama untuk membuat pekerjaan mereka lebih mudah, terstandarisasi, dan lebih dapat diandalkan serta aman.



Sumber : Hasil Penelitian *Home Screen Parrot OS*

Gambar 3. *Operating System Parrot Linux*

Parrot OS memiliki *tools* dan fitur lengkap yang dapat dimanfaatkan untuk penetrasi test seperti pada table dibawah ini, yaitu

Tabel 1. Fitur *Penetrasi Test Parrot OS*

Tools Penetrasi Test	Fitur Penetrasi
- Information Gathering - Vulnerability Assessment - Exploitation Tools - Privilege Escalation - Maintaining Access - Reverse Engineering - RFID Tools - Stress Testing - Reporting Tools - Services - Miscellaneous	- Fresh & lightweight pentest environment!-- Easy to use automation tools for beginners Must have professional tools for Pro Pentesters. - External tools developed by our community. - Only a selected set of tools is preinstalled out of the box

Sumber : (KOMINFO UBP, 2021)

2. Metode Penelitian

Tahapan penetration testing merupakan tahapan pengujian berupa serangan beruntun pada *website* Sistem Informasi Akadmik (I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, 2020).

Penetration testing pada penelitian diawali dengan studi literatur mengenai pengujian yang dilakukan dan melakukan diskusi dan wawancara terhadap pihak pengelola *website*. Penelitian ini menggunakan laptop dengan sistem operasi *Parrot OS* dan beberapa tools untuk simulasi serangan sistem dalam melakukan *Penetration Test*.

Tabel 2. Hardware

No	Alat	Keterangan Spesifikasi
1	Laptop Acer Aspire E5-475G	- Processor i5-7200u - Ram 16gb - SSD 240gb - Nvdia 940mx

Sumber : Hasil Penelitian

Tabel 3. Software

No	Nama Tools	Fungsi
1	Parrot	*Operating System*
2	Nmap	*Information Gathering*
3	Vega / Netparker	*Vullnerability*
4	Medusa	*Gaining Access*

Sumber : Hasil Penelitian

Teknik Pengujian Penetration Testing

Teknik yang digunakan dalam demo simulasi serangan yaitu :

Sumber : (Bin Ibrahim & Kant, 2018)

Gambar 4. Teknik Pengujian Penetrasi Test

3. Hasil dan Pembahasan

1. Information Gathering

Pengumpulan informasi dalam penelitian ini menggunakan 2 cara scanning yang terdapat dalam sistem operasi Parrot Security yaitu *network exploration or security auditing* (Nmap) dan *Whois Lookup.*

Sumber : Hasil Penelitian *Parrot OS*

Gambar 5. Tampilan hasil pemindaian NMAP

Sumber : Hasil Penelitian *Parrot OS*

Gambar 6. Tampilan hasil pemindaian NMAP

Gambar 5 dan 6 yaitu pemindaian menggunakan NMAP yang dihasilkan dari *Parrot OS* sebagai *attacker*, menunjukan beberapa port terbuka, salah satunya port 22 dan service yang berjalan pada ip 36.92.50.26 terdapat informasi, status dan versi lainnya.

a. Informasi bagian depan

Informasi bagian depan yang dihasilkan dari panggilan ip 36.92.50.26 menggunakan browser terdapat bagian yang langsung diperlihatkan kepada pengguna. Pengguna dapat secara langsung berinterkasi pada bagian depan ini.

Gambar 7. Tampilan halaman Front-end Login

b. Informasi bagian belakang

Informasi bagian belakang yaitu bagian belakang layar dari sebuah *website*. Informasi back-end berhubungan dengan *Domain Name Server* dan hal lain yang berkaitan dengan *website* dari *back-end*.

Hasil Scanning dan pengecekan yang didapat dari laman https://whois.domaintools.com/ menghasilkan informasi sebagai berikut

Sumber : (Who Is, n.d.)

Gambar 8. Tampilan informasi who is

Informasi *Whois* menjelaskan informasi mengenai server. *Created Dates* adalah tanggal DNS didaftarkan, tanggal DNS *update* dan tanggal domain hangus;

Name Servers adalah server nama otoritatif yang mengasuh zona nama domain dari nama domain yang digunakan pada server (Fauzan, 2019).

Sumber : (Who Is, n.d.)

Gambar 9. Tampilan informasi DNS

Domain Name System (DNS) adalah salah satu komponen terpenting dari Internet saat ini, sebuah sistem yang menyimpan informasi tentang nama *host* ataupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam server, merupakan standar penamaan konvensi antara nama domain yang

dapat dibaca manusia dan alamat Internet Protocol (IP) yang dapat dirutekan mesin dari sumber daya Internet (Khormali et al., 2021).

Sumber : (Who Is, n.d.)

Gambar 10. Tampilan informasi diagnosa

Gambar 10 adalah sebuah permintaan yang dilakukan pada *server* baik *ping* dan *traceroute* berstatus normal dan berjalan dengan baik.

2. Vullnerability Assessmant

Vulnerability assessments yaitu strategi yang mengikuti pendekatan sistematis dan proaktif untuk menemukan sebuah kerentanan (Shinde & Ardhapurkar, 2016).
Penilaian kerentanan pada tahap ini menggunakan 2 *tools* yaitu Netparker dan Vega.

Sumber : Hasil Penelitian *Tools Netparker*

Gambar 11. Tampilan vunerability Assessmant

Gambar 11 menunjukan hasil scanning vulnerability Assessmant menggunakan Netparker yang menghasilkan kerentanan tingkat *Hight* yaitu "*Password Transmitted over HTTP*".

Sumber : Hasil Penelitian *Tools Vega*

Gambar 12. Tampilan vunerability Assessmant

Pada gambar 12, hasil pemindaian *tool* Vega *Vulnerability Scanner* menunjukkan empat kelemahan pada *website* dengan *level high*, empat kelemahan dengan *level medium*, dan dua kelamahan dengan *level low*. Pada informasi diatas perrlu diperhatikan agar terhindar dari serangan oleh pihak yang tidak bertanggungjawab.

3. Gaining Acces

Gaining Access adalah bagian ketiga dari pengujian penetrasi testing. pada bagian ini, akan terhubung ke jaringan yang memungkinkan untuk meluncurkan serangan dan mendapatkan informasi yang lebih akurat kedalam system website target (Ismail & Pramudita, 2020).

Sumber : Hasil Penelitian *Parrot OS*

Gambar 13. Tampilan pemberian password

Berdasarkan gambar 13 yang dihasilkan dari *Parrot OS* sebagai *attacker* , dapat dilihat bahwa pengujian akses kedalam *system web server* dimulai dengan diberikan asumsi berbagai password secara acak untuk dilakukan *session* pencarian

Sumber : Hasil Penelitian *Parrot OS*

Gambar 14. Tampilan pemberian username

Gambar 14, yaitu tahapan selanjutnya pengujian akses kedalam *system web server* dengan diberikan asumsi berbagai username

secara acak untuk dilakukan *session* pencarian terhadap *webserver*

Pada tahapan ini peneliti mendapatkan *wordlist* dan *username* dengan cara obervasi, riset pada objek penelitian, pengujian hanya diberikan nama organisasinya saja dan informasi lainnya harus dicari sendiri oleh penguji (Krishnan & Wei, 2019).

Sumber : Hasil Penelitian *Parrot OS*

Gambar 15. pencarian *username* dan *password*

Pada Gambar 15 adalah pencarian *username* dan *password* dengan melakukan *scanning* secara bergantian terhadap beberapa asumsi *user* yang telah diberikan, tahap ini menggunakan perintah medusa yang ada pada *Parrot OS*.

Sumber : Hasil Penelitian *Parrot OS*

Gambar 16. Ditemukan *username* dan *password*

Gambar 16 adalah tampilan ditemukannya mengenai *username* dan *password* yang berhasil diperoleh dari *system target*.

Sumber : Hasil Penelitian *Parrot OS*

Gambar 17. Login ssh ke *system target*

Gambar 17 menampilkan bahwa berhasil masuk ke dalam *system* dengan memasukan *username* dan *password* yang telah ditemukan pada *operating system Parrot*.

4. Maintening Acces

Maintaining Access adalah fase dari siklus *penetration test* yang memiliki tujuan untuk memungkinkan pentester berlama-lama di sistem yang ditargetkan sampai dia memperoleh informasi apa yang dia anggap berharga dan kemudian berhasil mengekstraknya dari sistem (Li et al., 2018).

Sumber : Hasil Penelitian *Parrot OS*

Gambar 18. Mendapatkan akses system

Gambar 18 Menampilkan informasi apa saja yang terdapat dalam system target, dalam tahap ini peretas dapat mengambil atau mengubah informasi yang ada pada system web server tersebut (I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, 2020).

5. Clearing Track

Tahap *clearing tracks* merupakan tahap terakhir dari *penetration test*. Pengujian pada tahap ini dilakukan dengan menghapus seluruh *log file* serangan yang telah dilakukan pada tahapan sebelumnya, tujuannya agar tidak bisa terlacak oleh bagian *IT Security* (Yunanri et al., 2016).

4. Kesimpulan

Berdasarkan penelitian yang dilakukan mengenai keamanan *web server* maka kesimpulan yang didapat adalah terdapat kelemahan pada Sistem Informasi Akademik. Jenis kelemahan pada Sistem Informasi Akademik didapatkan tiga kategori adalah level high, level medium dan level low. Bagian yang dilakukan penyerangan terhadap system yaitu pada port 22 mengenai ssh. Simulasi serangan menggunakan *Parrot OS* menghasilkan keberhasilan masuk kedalam system, dengan ditemukannya *username* dan *password* maka dapat *Login* ke target. Saran dan masukan terhadap Perguruan tinggi agar segera mengambil tindakan penutupan *port* TCP yang

terbuka, serta perbaikan *bug* pada sistem yang dapat dimanfaatkan penyerang sebagai celah keamanan mengenai Sistem Informasi Akademik . Kedepannya, penelitian mengenai *penetration testing* pada *webserver* dapat dilakukan setelah dilakukan perbaikan berdasarkan rekomedasi yang diberikan, serta penggunaan *framework penetration testing* lainnya dapat digunakan sebagai perbandingan hasil pengujian.

Referensi

Bin Ibrahim, A., & Kant, S. (2018). Penetration Testing Using SQL Injection to Recognize the Vulnerable Point on Web Pages. *International Journal of Applied Engineering Research*, *13*(8), 5935–5942. http://www.ripublication.com

Fauzan, R. H. (2019). Pengujian Keamanan Sistem Informasi Akademik Menggunakan Metode Penetration Testing. *Studi Kasus: Institut Pertanian Stiper Yogyakarta*.

Ghanem, M. C., & Chen, T. M. (2020). Reinforcement learning for efficient network penetration testing. *Information (Switzerland)*, *11*(1), 1–23. https://doi.org/10.3390/info11010006

I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, D. M. S. A. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati*, *Vol. 8*, *No*(2), 113–124.

Ismail, R. W., & Pramudita, R. (2020). Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi. *Jurnal Mahasiswa Bina Insani*, *5*(1), 53–62.

Jofie yordan, muhammad fikrie. (2019, February 17). *BSSN Bikin Website Pemantau Serangan Siber di Indonesia*. https://kumparan.com/kumparantech/bssn-bikin-website-pemantau-serangan-siber-di-indonesia-1549535309181754057/full

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *CyberSeccurity Dan Forensik Digital*, *2*(2), 77–81.

Khormali, A., Park, J., Alasmary, H., Anwar, A., Saad, M., & Mohaisen, D. (2021). Domain name system security and privacy: A contemporary survey. *Computer Networks*, *185*, 107699. https://doi.org/10.1016/j.comnet.2020.107699

KOMINFO UBP. (2021, April 8). *MENGULAS DISTRO LINUX PARROT OS*. 1. http://himatif.ubpkarawang.ac.id/2021/04/mengulas-distro-linux-parrot-os/

Krishnan, S., & Wei, M. (2019). SCADA testbed for vulnerability assessments, penetration testing and incident forensics. *7th International Symposium on Digital Forensics and Security, ISDFS 2019*, 1–6. https://doi.org/10.1109/ISDFS.2019.8757543

Kurniawan, E., & Riadi, I. (2018). Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *2*(1), 12. https://doi.org/10.29407/intensif.v2i1.11830

Li, S., Jiang, H., & Shi, M. (2018). Redis-based web server cluster session maintaining technology. *ICNC-FSKD 2017 - 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery*, 3065–3069. https://doi.org/10.1109/FSKD.2017.8393274

Nazwita, S. R. (2017). Analisis Sistem Keamanan Web Server dan Database Server Menggunakan Suricata. *Seminar Nasional Teknologi Informasi Komunikasi Dan Industri*, *0*(0), 2579–5406. http://ejournal.uin-suska.ac.id/index.php/SNTIKI/article/view/3368

Nurkamiden, M. R., Najoan, M. E. I., & Putro, M. D. (2017). Rancang Bangun Sistem Pengendalian Perangkat Listrik Berbasis Web Server Menggunakan Mini PC Raspberry Pi Studi Kasus Gedung Fakultas Teknik Universitas Sam Ratulangi. *Jurnal Teknik Informatika*, *11*(1). https://doi.org/10.35793/jti.11.1.2017.15980

Rheno Widianto, S., & Abdullah Azzam, I. (2018). Analisis Upaya Peretasan Web Application Firewall dan Notifikasi Serangan Menggunakan Bot Telegram pada Layanan Web Server. *Elektra*, *3*(2), 19–28.

Salsabila, P. Z. (2020, October 12). Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi. *Kompas.Com*, 1. https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi

Shinde, P. S., & Ardhapurkar, S. B. (2016). Cyber security analysis using vulnerability assessment and penetration testing. *IEEE WCTFTR 2016 - Proceedings of 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare*.

https://doi.org/10.1109/STARTUP.2016.7583912

Shravan, K., Neha, B., & Pawan, B. (2014). Penetration Testing : A Review. *Compusoft*, *3*(Iv), 752–757.

Stiawan, D., Idris, M. Y., Abdullah, A. H., AlQurashi, M., & Budiarto, R. (2016). Penetration testing and mitigation of vulnerabilities windows server. *International Journal of Network Security*, *18*(3), 501–513. http://joiv.org/index.php/joiv/article/view/190

Who Is. (n.d.). *Who Is*. https://who.is/

Yunanri, Riadi, I., & Yudhana, A. (2016). Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST). *Annual Research Seminar*, *2*(1), 300–304.

Zeebaree, S. R. M., Jacksi, K., & Zebari, R. R. (2020). Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers. *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(1), 505–512. https://doi.org/10.11591/ijeecs.v19.i1.pp505-512

32. HASIL CEK_60960140

ORIGINALITY REPORT

11%	13%	5%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.sciencegate.app Internet Source	6%
2	Submitted to Universitas Bina Sarana Informatika Student Paper	5%

Exclude quotes	On	Exclude matches	< 5%
Exclude bibliography	On		