P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 4 No. 1, Maret, 2023, Hal. 1-9

IMPLEMENTASI TWO-FACTOR AUTHENTICATION (2FA) DAN FIREWALL POLICIES DALAM MENGAMANKAN WEBSITE

Hero Raka Herdiantoro [1)], M Reza Redo Islami [2)]
[1,2)] Teknik Informatika, STMIK Dharma Wacana Metro

Jl. Kenanga No.3, Mulyojati, Kec. Metro Bar., Kota Metro
[1]herorakahrh@gmail.com , [2]rzredo@gmail.com

Abstrak *:* Era industri 4.0 menuntut segala aspek kehidupan masyarakat untuk memanfaatkan teknologi guna mempermudah dalam menyelesaikan suatu masalah, salah satu teknologi yang sangat populer adalah *website, website* menjadi populer karena dapat di akses melalui berbagai *platforms,* dengan populernya *website* menyebabkan meningkatnya serangan pada *website.* Pelaku kejahatan *cyber (cyber criminals)* biasanya mencuri akun dari *administrator website* guna memanipulasi *data* dan informasi, untuk itu perlu adanya metode keamanan untuk melindungi *website* dari serangan. Berbagai metode pengamanan akun telah banyak di kembangkan, salah satunya adalah metode *two-factor authentication (2FA),* metode ini digunakan untuk mengantisipasi apabila akun *administrator* di curi oleh *cyber criminals,* apabila akun tersebut di dapatkan orang lain, pelaku harus mendapatkan *password* ke dua yang di kirimkan sistem ke *email* maupun nomor *handphone* korban, sehingga untuk dapat masuk ke dalam *website* di perlukan dua langkah autentikasi. Selain dengan *2FA* penelitian ini akan memanfaatkan *firewall* untuk mengizinkan beberapa alamat *(IP Address)* yang dapat mengakses halaman *administrator,* sehingga apabila pelaku berada di luar alamat yang di izinkan, pelaku tetap tidak dapat masuk ke dalam website. Dengan memanfaatkan *2FA* dan *firewall policies,website* akan memiliki proteksi lebih dari ancaman keamanan *cyber.*

Kata Kunci : 2FA, Kebijakan *firewall, website,* Keamanan *cyber*.

Abstrac t: *The industrial era 4.0 requires all aspects of people's lives to take advantage of technology to make it easier to solve a problem, one of the very popular technologies is the website, websites are becoming popular because they can be accessed through various platforms, the popularity of websites causes increased attacks on websites. Cyber criminals usually steal accounts from website administrators to manipulate data and information, for this reason, it is necessary to have a security method to protect websites from attacks. Various account security methods have been developed, one of which is the two-factor authentication (2FA) method, this method is used to anticipate if the administrator's account is stolen by a cybercriminal, if someone else gets the account, the perpetrator must get the second password sent. system to the victim's email or cellphone number, so to be able to enter the website, two authentication steps are needed. In addition to 2FA, this research will utilize a firewall to allow multiple addresses (IP addresses) to access administrator pages, so that if the perpetrator is outside the permitted address, the perpetrator still cannot enter the website. By utilizing 2FA and firewall policies, websites will have more protection from cyber security threats.*

Keywords: *2FA*, *Firewall policy, website, Cyber security*

PENDAHULUAN

Teknologi informasi yang semakin berkembang, dapat di akses dengan mudah kapan saja dan di mana saja menimbulkan kecemasan bagi pengelola sistem karena tidak sedikit pelaku kejahatan memanfaatkan situasi ini untuk kepentingan diri sendiri (Huwaidi, 2022, 107). Website merupakan platform yang menjadi tulang punggung teknologi informasi, dapat di akses kapan saja dan di mana saja sehingga dapat meningkatkan resiko website dari kejahatan cyber (Saputra, 2022, 1). Website perlu di lindungi sepanjang waktu untuk meningkatkan keamanan pasa website. kebutuhan mekanisme pengaman secara realtime untuk mengurangi resiko terjadinya serangan sangat di perlukan (Risqiwati, et al., 2018).

Website sebagian besar menggunakan metode otentikasi tunggal guna mengamankan akses halaman tertentu, proses otentikasi ini berfungsi untuk membuktikan kebenaran, ke aslian maupun validitas data kunci yang di inputkan guna masuk ke dalam sistem (Mustaqim, 2019, 1). Dalam prakteknya proses otentikasi tunggal masih memiliki kelemahan, salah satu kelemahan dari otentikasi tunggal adalah serangan *phising*. Menurut Sharma (2022) *phising* mampu mendapatkan data guna masuk ke dalam sebuah sistem dan melakukan serangan lanjutan dengan masuk ke dalam sistem menggunakan data *sensitive* (*username* dan *password*) yang telah di dapatkan. Untuk itu perlu mekanisme pengamanan lebih untuk meningkatkan keamanan pada website.

Metode pengamanan pada website telah banyak di kembangkan oleh pakar sebelumnya, salah satu metode pengamanan proses otentikasi adalah *two-factor authentication (2FA)* yaitu proses otentikasi yang menggunakan dua atau lebih metode otentikasi guna meningkatkan keamanan dan meminimalisir serangan pengalihan akun (Setiawan, 2020, 63). Selain menggunakan 2FA guna mengamankan halaman tertentu, salah satunya yaitu dengan memanfaatkan *firewall, menurut Anwar (2021,2) firewall* memainkan peranan penting dalam mengamankan sebuah sistem. Hidayat (2018) mengamankan sebuah halaman admin router menggunakan fitur *whitelist* pada *firewall*, sehingga hanya alamat internet *(IP Address)* tertentu yang dapat mengakses halaman tersebut.

Beberapa penelitian berkaitan 2FA telah di lakukan, Fitriyansyah (2020, 8) mengembangkan *OTP* (*one time password*) yaitu proses otentikasi ganda melalui *SMS (short message service),* namun memiliki kelemahan apabila nomor handphone pengguna telah di salahgunakan maka proses *OTP* menjadi tidak efektif. Selain itu Mahardhika (2020, 361) berhasil membangun mekanisme 2FA menggunakan *OTP* yang di kirimkan melalui layanan *SMS* dan menjelaskan bahwa *SMS* membutuhkan biaya berupa pulsa guna mengirimkan kode *OTP* kepada pengguna, perlu adanya proses OTP yang dapat memanfaatkan layanan gratis seperti whatsapp, telegram maupun *E-mail*.

Berdasarkan penelitian sebelumnya penelitian ini berfokus untuk membangun mekanisme *2FA* memanfaatkan layanan *E-mail* guna mengurangi resiko keamanan apabila data pengguna di salah gunakan orang lain, selain itu penelitian ini

P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 4 No. 1, Maret, 2023, Hal. 1-9

bertujuan untuk mengamankan halaman administrator website internal yang di gunakan untuk mencatat aktivitas pekerjaan, dengan memanfaatkan *whitelist* pada *firewall*, sehingga halaman administrator hanya dapat di akses melalui *IP Address* tertentu, hal ini bertujuan mengantisipasi apabila akun dan *OTP* di curi maka pengguna tidak akan dapat mengakses halaman apabila di luar dari jaringan yang di ijinkan. dengan mekanisme tersebut di harapkan *confidentiality, integrity dan availability (CIA)* data dan informasi yang terkandung pada website dapat terjaga dan aman dari berbagai ancaman kemanan *cyber*

KAJIAN PUSTAKA DAN LANDASAN TEORI

Beberapa kajian pustaka tentang meknisme pengamanan website telah di kumpulkan dan di pelajari, hal ini bertujuan untuk mendapatkan kesimpulan dari berbagai teori guna membangun mekanisme pengamanan otentikasi sebuah website, beberapa kajian dan landasan teori diantaranya 2FA, *Firewall,* website dan beberapa sumber yang berkaitan dengan penelitian.

Two-Factor Authentication (2FA)

Authentication atau otentikasi adalah proses pemeriksaan suatu identitas guna melakukan validasi ke aslian identitas tersebut guna masuk ke dalam sistem (Saputra, 2021, 3). Terdapat beberapa metode dalam melakukan otentikasi yaitu *something you know* yaitu menggunakan sesuatu yang kita ketahui contohnya *username* dan *password*. *something you have* contohnya menggunakan sesuatu yang sifatnya unik misalnya *simcard* pada *handphone*. *something you are* yaitu otentikasi menggunakan sidik jari, retina mata atau *face detector.* proses otentikasi pada aplikasi yang sangat sensitive seperti proses transaksi keuangan, penilaian dan aplikasi penting lainya tidak cukup hanya menggunakan otentikasi tunggal, maka muncul istilah *2FA* yaitu proses otentikasi dengan menggabungkan dua metode yang berbeda (Fitriyansyah, 2020, 5).

Firewall

Firewall merupakan sebuah perangkat lunak maupun keras yang terpasang pada sistem guna mengamankan jaringan maupun aplikasi dari ancaman pada data, *firewall* di tuntut untuk mampu melidungi sistem dari ancaman kemanan pada data baik dari luar maupun dalam jaringan (Anwar, 2021). *Firewall policies* (kebijakan *firewall*) terdapat dua macam yaitu *allow all deny any* memperbolehkan semua trafik yang masuk maupun keluar dari jaringan dan memblokir beberapa trafik, sedangkan kebijakan yang ke dua adalah *deny all allow any* yaitu memblokir semua trafik dan hanya mengizinkan trafik tertentu saja (Saputra, 2022).

Keamanan Komputer

Keamanan komputer merupakan sebuah studi yang dilakukan guna mempelajari pola suatu serangan terhadap jaringan komputer (Muhammad, 2021). Keamanan komputer sendiri memiliki tujuan yaitu memastikan *confidentiality, integrity* dan *availability* pada data, artinya keamanan komputer bertujuan untuk memastikan data menjadi rahasia, tidak di modifikasi atau di rusak serta selalu tersedia ketika di butuhkan (Brinkley,1995).

Website

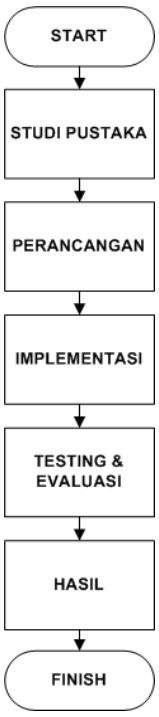
Website merupakan sebuah sarana yang di gunakan sebagai media memasarkan produk, menyampaikan informasi dan dapat digunakan untuk mempresentasikan citra perusahaan (Fariadi, 2022). Menurut Mastan (2019) berdasarkan tujuannya

P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 4 No. 1, Maret, 2023, Hal. 1-9

website terbagi menjadi beberapa jenis yaitu, *personal website*, *corporate website*, *portal website* dan *forum website,* masing-masing jenis website di buat berdasarkan tujuanya, *personal* digunakan untuk kebutuhan pribadi, *corporate* di gunakan untuk menunjang kebutuhan perusahaan, *portal* digunakan untuk layanan berita, *email* dan jasa sedangkan forum digunakan untuk tujuan media diskusi.

METODE

Penelitian ini terdiri dari beberapa proses yang di lakukan guna mencapai tujuan dari penelitian, proses tersebut berjalan ber urutan dari awal hingga akhir, beberapa proses yang di lakukan pada penelitian ini dapat di lihat pada gambar alur penelitian di bawah ini.



Gambar 1. Alur penelitian

Penelitian di awali dengan proses studi literatur guna mengetahui cara kerja dan jenis *2FA*, serta cara mengamankan halaman administrator website melalui mekanisme pengamanan menggunakan *firewall*, selanjutnya proses perancangan adalah tindak lanjut dari proses studi literatur sehingga mekanisme yang akan di bangun sesuai dengan studi yang mutakhir dan relevan, setelah proses perancangan hal yang dilakukan adalah melakukan implementasi mekanisme pengamanan *2FA* dan implementasi *firewall,* setelah mekanisme di implementasi maka akan di lakukan proses testing dan evaluasi untuk mengetahui apakah mekanisme telah berhasil meningkatkan keamanan pada website.

HASIL DAN PEMBAHASAN

Tahap studi pustaka

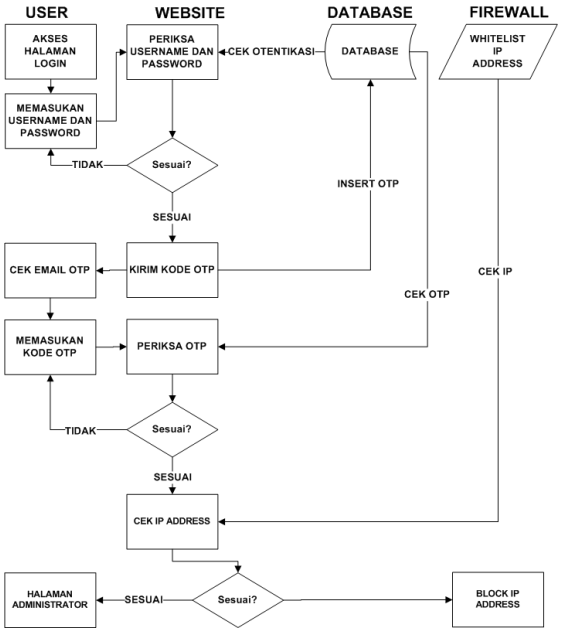
Pada tahap studi pustaka telah di dapatkan beberapa kelebihan dan kelemahan dari metode *2FA* dalam mengamankan sebuah website, beberapa penelitian sebelumnya di antaranya yang di lakukan oleh Mahardhika (2020), menjelaskan bahwa proses pengiriman kode otentikasi ganda menggunakan SMS sangat tergantung pada pulsa. Kemungkinan gagalnya kode terkirim karena pulsa habis sangat mungkin terjadi, maka pada penelitian ini akan memanfaatkan *E-mail* guna mengirimkan kode otentikasi tanpa terhalang pulsa dan hemat biaya.

Selain itu untuk meningkatkan keamanan pada halaman admin website pelu adanya proteksi *whitelist* pada *IP* tertentu, hal ini guna mengamankan halaman sensitif apabila website yang di kelola memang hanya untuk kepentingan internal, misal aplikasi transaksi, pencatatan logistik, input penilaian dan sebagainya, sehingga apabila *2FA* telah di kuasai penyerang, penyerang hanya dapat mengakses halaman dengan alamat *IP* tertentu, yang pastinya akan menambah sulit penyerang untuk mengakses halaman administrator website.

P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 4 No. 1, Maret, 2023, Hal. 1-9

Tahap perancangan

Pada tahap perancangan yang merupakan proses design sistem yang akan di bangun. Berikut ini gambar design mekanisme *2FA* dan kebijakan *firewall* yang akan di bangun

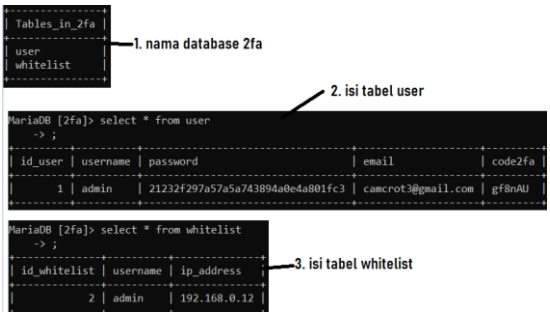


Gambar 2. Design mekanisme

Dalam memberikan proteski lebih pada halaman website, objek penelitian adalah pada website yang di gunakan untuk mencatat inventaris pemasangan alat jaringan internet, dimana website ini hanya digunakan pada internal perusahaan dalam mencatat penggunaan alat, namun website tetap harus *online* untuk memberikan informasi pemasangan alat dan status ke aktifan alat kepada seluruh *staff* dan pengguna internet pada perusahaan. Proses *login* ke dalam halaman administrator di lakukan dengan memasukan *username* dan *password*, selanjutnya pengguna akan menerima *email* berupa kode acak yang telah di simpan ke *database*, sehingga kode yang diterima pengguna akan di masukan ke form otentikasi ke dua apabila kode tersebut cocok dengan kode yang ada pada *database* maka sistem akan mencocokan *IP address* pengguna dengan *IP Address* yang ada pada *firewall,* apabila alamat *IP* pengguna terdaftar pada *whitelist firewall* maka pengguna akan di arahkan ke halaman administrator. *Firewall* pada penelitian ini menggunakan konsep *Web Application Firewall (WAF)* yaitu *firewall* yang akan melakukan *filter* pada lapisan aplikasi *(layer 7)* sehingga mekanisme yang di butuhkan tidak memerlukan *hardware* tambahan mekanisme ini akan membaca *IP* pengguna dan mencocokan *IP* tersebut dengan daftar *whitelist* yang ada pada tabel *firewall.*

Tahap implementasi, Testing dan evaluasi

Tahap implementasi di awali dengan proses pembuatan database MySQLyang terdiri dari 2 buah tabel, tabel pertama memiliki nama user dan tabel kedua memiliki nama whitelist. Berikut ini gambar 3 yang merupakan isi database yang telah di buat.

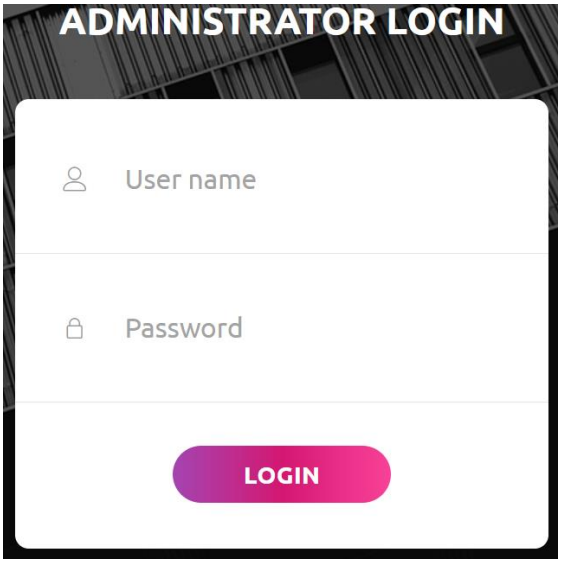


Gambar 3. Database 2FA

Pada gambar 3 terdapat dua table pada database 2FA yaitu table user dan whitelist.

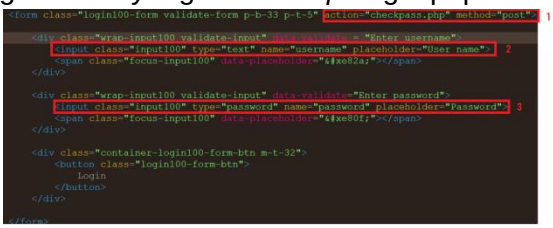
Sebelum memasuki halaman administrator pengguna akan di arahkan ke halaman login.php, dimana halaman ini digunakan untuk memasukan *username* dan *password*, berikut ini gambar 4 tampilan halaman login.php

P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 4 No. 1, Maret, 2023, Hal. 1-9



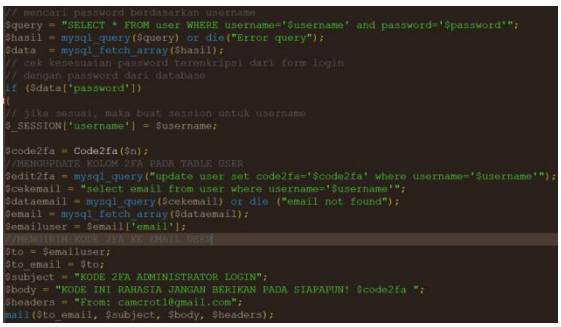
Gambar 4. Tampilan halaman login.php

Script login.php menggunakan *hypertext processor (PHP)* berikut ini merupakan gambar 5 yang berisi *script* login.php



Gambar 5. *Script* login.php

Script akan melakukan *post* data *username* dan *password*, data tersebut akan di arahkan ke *script* checkpass.php, berikut ini gambar 6 isi dari script checkpass.php.

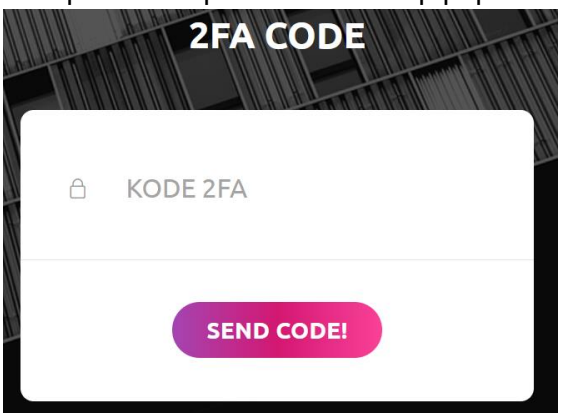


Gambar 6. *Script* checkpass.php

checkpass.php berfungsi untuk mencocokan *username* dan *password* dari pengguna, apabila inputan pengguna cocok dengan *username* dan *password* pada tabel user maka *script* checkpass.php akan melakukan *generate random string* dengan panjang 6 karakter, lalu checkpass.php akan melakukan update code2fa yang ada pada tabel user, selain itu kode 2FA akan di kirim ke *email user*, berikut ini gambar 7 menunjukan email yang masuk ke pengguna setelah menjalankan checkpass.php

Gambar 7. Tampilan email

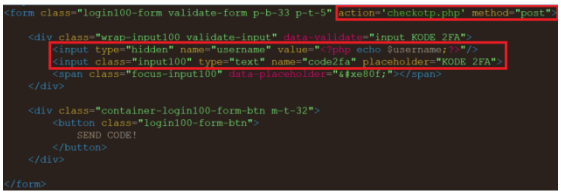
Email yang di terima *user* yang ber isi kode *2FA* cocok dengan kolom code2fa pada tabel user, kode ini yang akan di *input user* ke otp.php, checkpass.php akan mengarahkan pengguna ke halaman otp.php. berikut ini gambar 8 yang merupakan tampilan halaman otp.php



Gambar 8. Tampilan halaman otp.php

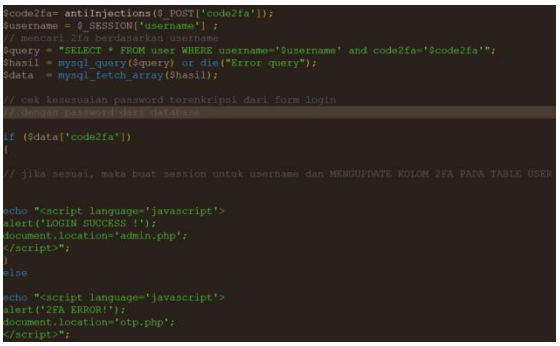
Script otp.php ini berfungsi untuk menyediakan inputan kode 2FA yang telah di kirimkan ke *email*, otp.php akan mengarahkan inputan pengguna ke *script* checkotp.php guna dilakukan validasi kode 2FA yang di inputkan pengguna. Berikut ini gambar 9 isi *script* otp.php

P_ISNN: 2721-3501 e-ISSN 2721-3978
JMIK (JURNAL MAHASISWA ILMU KOMPUTER)
Vol. 4 No. 1, Maret, 2023, Hal. 1-9



Gambar 9. Isi *script* otp.php

Setelah pengguna menginputkan kode 2FA maka otp.php akan melakukan *post* data menuju script checkotp.php *script* ini berfungsi untuk melakukan otentikasi ke dua yaitu mencocokan username dan code2fa yang ada pada table user. berikut ini gambar 10 yang merupakan isi dari *scrip*t checkotp.php

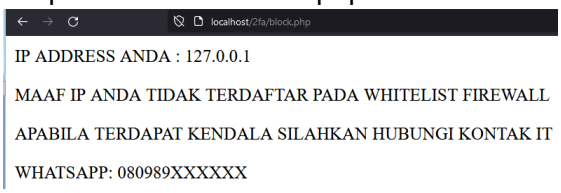


Gambar 10. *Script* checkout.php

Apabila *username* dan kode *2FA* yang di inputkan *user* sesuai dengan table user yang ada pada database, maka selanjutnya pengguna akan masuk ke halaman administrator yaitu pada *script* admin.php, *script* admin merupakan halaman dashboard administrator, pada admin.php terdapat script yang melakukan pencocokan *username* dan pembacaan *IP address* user, berikut ini gambar 11 yaitu isi script admin.php

Gambar 11. *Script* admin.php

Setelah *IP user* terbaca, *IP* ini akan di cocokan dengan *IP* yang ada pada tabel *whitelist*, apabila *IP address user* tidak cocok dengan *IP address* pada table *whitelist* maka pengguna akan di arahkan ke halaman block.php, berikut gambar 12 tampilan halaman block.php



Gambar 12. Tampilan halaman block.php

Namun apabila *IP Address user* cocok dengan *IP Address* yang ada pada *database, user* akan masuk ke halaman *dashboard* administrator, berikut ini gambar 13 tampilan dari halaman administrator

Gambar 13. Tampilan halaman administrator

KESIMPULAN

Hasil penelitian Implementasi *Two-Factor Authentication (2FA)* dan *Firewall Policies* Dalam Mengamankan Website mendapatkan hasil dan kesimpulan sebagai berikut.

1. Penelitian ini telah berhasil mengimplementasikan *2FA* dan *Firewall policy* guna meningkatkan keamanan halaman administrator website.
2. Dengan adanya mekanisme otentikasi ganda *2FA* kemanan website menjadi meningkat, apabila akun pengguna di dapatkan oleh pelaku kejahatan *cyber (cybercriminals)* maka pelaku tidak akan dapat masuk ke

dalam sistem karena harus memasukan kode *2FA* yang di kirim ke *email* korban, secara tidak langsung untuk mendapatkan kode *2FA,* pelaku harus mendapatkan akun *email* dari korban.

3. Apabila pelaku berhasil membajak *email* korban, masih terdapat mekanisme *whitelist* yang akan memblokir pelaku, apabila *IP Address* pelaku tidak sesuai dengan *IP address* pada table whitelist.
4. Namun akibat adanya whitelist dapat menimbulkan permasalahan baru yaitu apabila pengguna otentik tidak menggunakan jaringan yang sudah terdaftar pada whitelist maka pengguna tidak akan bisa mengakses halaman administrator.
5. Saran dari penelitian ini yaitu perlu adanya *tunneling virtual private network* (VPN) yang dapat membuat jaringan *private* untuk memfasilitasi user yang berada di luar jaringan, sehingga apabila user sedang *work from home (WFH)* dapat menggunakan *VPN* yang telah di *whitelist*, sehingga jaringan user terhindar dari pemblokiran dan jaringan tetap aman.

REFERENSI

[1] Saputra, I. P., Utami, E., & Muhammad, A. H. (2022, October). Comparison of anomaly based and signature based methods in detection of scanning vulnerability. In 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 221-225). IEEE.

[2] Rahman, M. A. (2020). PENGEMBANGAN SISTEM OTENTIKASI PADA SEBUAH APLIKASI YANG BERBASISKAN WEB. Syntax: Journal of Software Engineering, Computer Science and Information Technology, 1(1), 1-9.

[3] Heriyanto, Y., Qalban, A. A., & Mukaromah, I. A. (2022). Pengembangan Metode Login Two Factor Authentication (2FA) untuk Keamanan Sistem Informasi Akademik. Journal of Innovation Information Technology and Application (JINITA), 4(2), 142-150.

[4] Choirul Mustaqim, A. H. M. A. D. Implementasi Two factor authentication Dan Algoritma Rsa Sebagai Metode Otentikasi Login Pada Si-Abka (Sistem Amal Bakti Kementerian Agama) (Doctoral dissertation, Fakultas Ilmu Komputer).

[5] Mahardhika, G. C., & David, F. Implementasi Two Factor Authentication (2FA) pada Sistem Keamanan Otentikasi User di Aplikasi Kasir Legends Barbershop. JUSTIN (Jurnal Sistem dan Teknologi Informasi), 8(4), 357-361.

[6] Setiawan, H., Sartika, D., & Ramadhan, B. G. (2020). IMPLEMENTASI TIME-BASED ONE TIME PASSWORD (TOTP) PADA SISTEM TWO FACTOR AUTHENTICATION (2FA). Jurnal Teknologi, 13(1), 63-68.

[7] Mastan, I. A. (2019). Perancangan Website Aplikasi Penjualan Restoran Ayam Keprabon. JBASE-Journal of Business and Audit Information Systems, 2(2).

[8] Huwaidi, M. Z., & Destya, S. Mencegah Serangan Rekayasa Sosial dengan Human Firewall. JUSTIN (Jurnal Sistem dan Teknologi Informasi), 10(1), 107-112.

[9] Mihalos, M. G., Nalmpantis, S. I., & Ovaliadis, K. (2019). Design and Implementation of Firewall Security Policies using Linux Iptables. Journal of Engineering Science & Technology Review, 12(1).

[10] Islami, M. R. R. (2022). DETEKSI DINI SERANGAN PADA WEBSITE MENGGUNAKAN METODE ANOMALI

BASED. JIKO (Jurnal Informatika dan Komputer), 5(3), 224-229.
[11] Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. Applied Sciences, 11(19), 9183.
[12] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques–a review of Cyber Defense Mechanisms. IJARCCE, 11(7), 153-160.
[13] Fitriyansyah, A. Y., & Hazri, M. (2020). Analisis Security Web Login Mahasiswa Menggunakan Algoritma Two-Factor Time-Based One Time Password. SAINSTECH: JURNAL PENELITIAN DAN PENGKAJIAN SAINS DAN TEKNOLOGI, 30(1).
[14] NUGROHO, I. S. STUDI LITERATUR: ANALISIS KEBUTUHAN PERANCANGAN SECURE MULTI-FACTOR AUTHENTICATION STUDI KASUS REGISTRASI ONLINE UKDW.
[15] Musu, W., Muhtamar, S., Palullu, A., & Patendean, W. (2022). Analisis Pola Penggunaan Fitur Autentikasi Dua Faktor oleh para Remaja di Media Sosial. E-JURNAL JUSITI: Jurnal Sistem Informasi dan Teknologi Informasi, 11(2), 212-222.
[16] Saputra, I. P., Yusuf, R., & Saprudin, U. (2021). IMPLEMENTASI CLOUD COMPUTING SEBAGAI RADIUS SERVER PADA JARINGAN INTERNET ROUTER MIKROTIK. *Journal Computer Science and Information Systems: J-Cosys*, *1*(2), 81-86.
[17] Hidayat, A., & Saputra, I. P. (2018). Analisa Dan Problem Solving Keamanan Router Mikrotik Rb750Ra Dan Rb750Gr3 Dengan Metode Penetration Testing (Studi Kasus: Warnet Aulia. Net, Tanjung Harapan Lampung Timur). Jurnal RESISTOR (Rekayasa Sistem Komputer), 1(2), 118-124.
[18] Gollmann, D. (2010). Computer security. Wiley Interdisciplinary Reviews: Computational Statistics, 2(5), 544-554.
[19] Brinkley, D. L., & Schell, R. R. (1995). Concepts and terminology for computer security. Information security: An integrated collection of essays, 40-97.
[20] Risqiwati, D., & Irawan, E. A. (2018). Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server. *Techno. Com*, *17*(4), 347-354.

.