p-ISSN: 2301-5373
e-ISSN: 2654-5101

Implementasi Port Knocking Dalam Mengamankan Jaringan VPN Pada Sistem E-Learning

I Ketut Prawira Adhisastra[1], I Komang Ari Mogi[2], Cokorda Rai Adi Pramartha[3], I Gede Santi Astawa[4], Made Agung Raharja[5], Ngurah Agus Sanjaya ER[6]

[a]Informatics departement, Faculty of Math and Science, University of Udayana
South Kuta, Badung, Bali, Indonesia
[1]prawira.adhisastra@yahoo.com
[2]arimogi@unud.ac.id
[3]cokorda@unud.ac.id
[4]santi.astawa@unud.ac.id
[5]made.agung@unud.ac.id
[6]agus_sanjaya@unud.ac.id

Abstract

universities that have started using e-learning as a learning medium. However, the system on e-learning is vulnerable to attacks such as identity theft, and authentication on e-learning systems. One way to secure data on a network is to implement a Virtual Private Network (VPN) on the network which can make a network private. That way, the security on the port on the E-learning server will be guaranteed. But attacks on servers more often occur on port 23 (telnet) because telnet does not encrypt the connection process. One of the attacks that is often used is a brute force attack. Based on these problems, research has been carried out to secure port 23 (telnet) and port 80 (e-learning website) on the e-learning server from brute force attacks by implementing the port knocking method. Port 23 and port 80 on the e-learning server that uses the port knocking method are always closed so that the client must do port knocking before being able to use port 23 and port 80 on the e-learning server. By implementing port knocking on the e-learning server, brute force attacks can be avoided because the attacked port is closed.

Keywords: *VPN, Port Knocking, E-Learning, Security, Digital*

1. Pendahuluan

E-Learning adalah sistem pendidikan yang menggunakan aplikasi elektronik untuk mendukung pengembangan kegiatan belajar mengajar dengan media internet[1]. E-learning memungkinkan perolehan pengetahuan dan informasi melalui perangkat yang terhubung dengan internet seperti handphone, komputer, tablet, dain lain-lainnya, Namun, karena sistem e-learning merupakan jaringan yang terbuka pasti rentan terhadap berbagai serangan keamanan. Sistem e-learning rentan terhadap serangan seperti pencurian identitas, dan otentikasi pada sistem e-learning[2].Peretas merupakan ancaman besar bagi kehidupan di jaman sekarang, dengan segala jenis kecanggihan teknologi yang ada, peretas dapat menggunakan metode tertentu untuk menyerang suatu jaringan internet. Salah satu cara untuk dapat mengamankan suatu data pada jaringan tertentu adalah dengan menggunakan Virtual Private Network (VPN). Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan local[3].

Dengan menggunakan VPN pada sistem e-learning maka keamanan untuk sistem e-learning akan terjamin. Virtual Private Network (VPN) merupakan sebuah teknologi komunikasi yang dapat memungkinkan untuk terkoneksi ke jaringan publik dan dapat menggunakannya untuk bergabung dengan jaringan lokal. Dengan menggunakan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti menggunakan koneksi atau jaringan LAN, walaupun sebenarnya menggunakan jaringan publik. Dengan begitu, keamanan pada bagian port-nya pada server E-learning akan terjamin. Karena port adalah sebuah mekanisme komunikasi perangkat satu dengan

perangkat lainnya. Oleh karena itu port 23 (telnet) juga sangat perlu diamankan, telnet berfungsi untuk seorang network administrator untuk bisa melakukan remote untuk login ke dalam suatu komputer. Jika port ini terus terbuka maka peretas akan menemukan celah untuk mencuri informasi dan data yang ada. Maka dari itu port yang terbuka tersebut perlu di tutup jika tidak ada komunikasi agar peretas tidak dapat masuk ke dalam port tersebut.

Maka dari itu penelitian ini menambahkan sebuah metode untuk mengamankan suatu jaringan VPN dengan menggunakan metode Port knocking. Metode port knocking merupakan sebuah teknik pertahanan yang digunakan untuk mencegah penyerang melakukan scanning untuk mendapatkan suatu informasi tentang kelemahan servis yang berpotensi dieksploitasi. Port knocking merupakan sebuah metode yang memberikan kekuasaan kepada user berdasarkan firewall untuk melakukan suatu komunikasi melalui port yang tertutup[4]. Port knocking bekerja seperti halnya brankas dengan kunci kombinasi angka putar. pada brankas tersebut, Anda diharuskan memutar kunci kombinasi beberapa kali hingga tepat seperti yang ditentukan[5]. Menggunakan metode port knocking dalam mengamankan suatu jaringan yang memiliki tujuan untuk memberikan tambahan lapisan keamanan yang ringan pada jaringan komputer yang berjalan melalui port yang tertutup.

Pada penelitian ini, penulis ingin meningkatkan keamanan jaringan virtual private network pada sistem E-learning dengan mengimplementasikan metode port knocking. Metode port knocking akan digunakan untuk menutup dan membuka akses masuk kedalam port tertentu dan metode ini terintegrasi bersama firewall. Untuk mendapatkan akses penuh ke dalam port, hanya *user* yang sudah memiliki akses kedalam port knocking yang dapat mengakses langsung, seperti admin atau client.

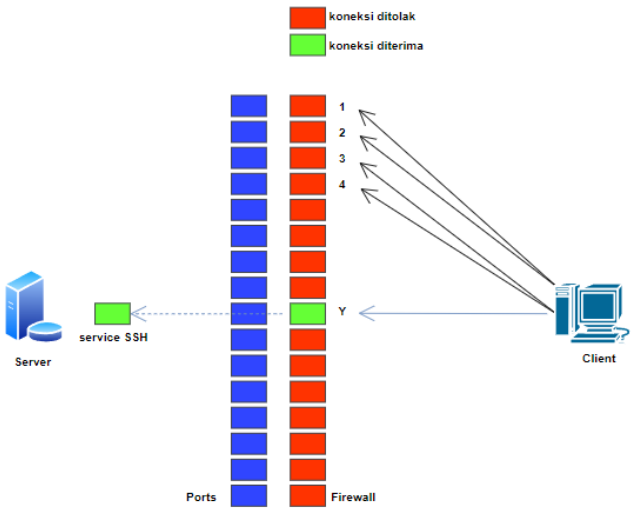
2. Metode Penelitian

Metode port knocking akan menggunakan algoritma PCG-XSH-RR untuk melakukan pengacakan pada jumlah dan nomor port yang berfungsi untuk membangkitkan sebuah deretan nomor *port* yang harus diketuk oleh client untuk melakukan koneksi terhadap sistem e-learning. Saringan VPN pada sistem E-Learning akan diamankan dengan menggunakan metode port knocking untuk mengatasi serangan brute force.

2.1. Port Knocking

Port knocking merupakan metode yang digunakan untuk dapat mengamankan jaringan internet agar tidak mudah diretas atau diserang. Cara kerja *port knocking* ini adalah dengan membuka dan menutup akses ke port tertentu dan metode ini terintegrasi Bersama dengan firewall. Untuk dapat memperoleh akses penuh ke dalam port, hanya hanya *user* yang sudah memiliki akses yang dapat mengakses langsung, seperti admin atau client.

.



Gambar 2.1 Proses Port Knocking

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Metode *Port knocking* dapat diilustrasikan seperti pada gambar 2.1 di atas. Apabila *client* ingin mengakses service SSH pada server melui port Y, maka *client* terlebih dahulu harus mengirimkan paket SYN menujut port 1,2,3,4 agar dapat mengakses port Y[7]. Namun metode ini masih memiliki beberapa kelemahan dalam mengatasi *port.* Penelitian ini menambahkan algoritma PCG-XSH-RR untuk melakukan pengacakan bilangan pada port.

2.2. PCG-XSH-RR

Permuted Congruential Generator-Xorshift-Random Rotation (PCG-XSH-RR merupakan salah satu algoritma pengacakan bilangan yang dikembangkan oleh Melissa E. O'Neill pada tahun 2014[8]. PCG memiliki keunggulan dari algoritma random lainnya, yaitu lebih cepat dalam waktu komputasi,banyak memiliki variasi, menggunakan memori yang kecil, seragam, sederhana, mudah dipahami dan sulit untuk di prediksi. Algoritma PCG-XSH-RR adalah varian yang paling disarankan dalam penggunaan algoritma PCG karena mempunyai state 64-bit dan output 32-bit selain itu algoritma ini juga memiliki tujuan untuk dapat membuat pembangkit bilangan acak yang baik untuk dapat digunakan dalam berbagai hal[7].

Permuted Congruential Generator-Xorshift-Random Rotation (PCG-XSH-RR) yang berfungsi untuk membangkitkan bilangan acak sebagai jumlah port dan nomor port yang harus diketuk untuk melakukan pengetukan pada metode port knocking. Pembangkitan bilangan acak ini dilakakan pada komputer server yang kemudian akan dikirimkan ke client untuk melakukan pengetukan. Bilangan acak ini dilakukan dengan menghasilkan 2 objek yang berupa jumlah port dan nomor port. Pengacakan terhadap jumlah port memiliki range 1 sampai 100, kemudian untuk nomor port memiliki range 1 sampai 65000.Berdasarkan penjelasan diatas objek dari algoritma ini adalah jumlah port dan nomor port yang akan dgunakan sebagi rule untuk melakukan port knocking dari komputer client ke server.

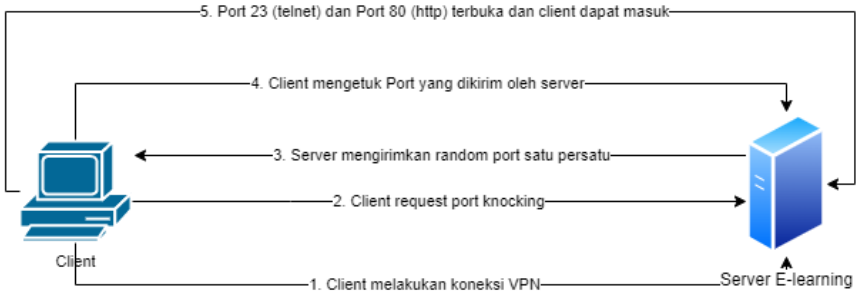
Table 1. Ilustrasi port nomor yang digunakan

190	394	874	8740	543

Table 1. adalah ilustrasi dari pembangkitan bilangan acak untuk port yang menggunakan algoritma PCG-XSH-RR, pembangkitan bilangan acak ini dilakukan sebanyak dua kali untuk menentukan jumlah port dan port berapa yang digunakan sebagai rule untuk melakukan pengetukan pada metode port knocking. Berdasarkan tabel 1 didapatkan port sejumlah 5 dengan hasil port yang random. Port tersebut nantinya akan digunakan untuk smelakukan pengetukan sebelum port tujuan (23 & 80) dapat terbuka. Sebelumnya port 23 & 80 dalam keadaan tertutup sebelum dilakukan pengetukan dan akan terbuka setelah dilakukan pengetukan yang sesuai dengan rule port dari hasil pembangkitan bilangan acak.

2.3. Bagan Rancangan Sistem

Berikut adalah bagan dari rancangan sistem pada penelitian ini



Gambar 2.2 Bagan dari Rancangan Sistem

Gambar 2.2 merupakan bagan dari rancangan sistem pada penelitian ini yang terdapat dua komputer yaitu, komputer server e-learning dan komputer client. Kedua komputer tersebut memiliki fungsi dan tugas yang berbeda, berikut adalah fungsi dan tugas dari kedua komputer :

1. Server

Komputer server e-learning memiliki fungsi untuk melakukan pembangkitan bilangan acak dengan algoritma PCG-XSH-RR dan untuk menerima request dari client. Request yang dikirim oleh client beruba request untuk membuka port 23 (telnet) dan port 80 yang akan menampilkan halaman website e-learning jika client menginputkan IP dari server e-learning pada browser. Kemudian server akan mengirimkan nomor port dari hasil pembangkitan bilangan acak yang telah dilakukan secara bertahap untuk di ketuk oleh client.

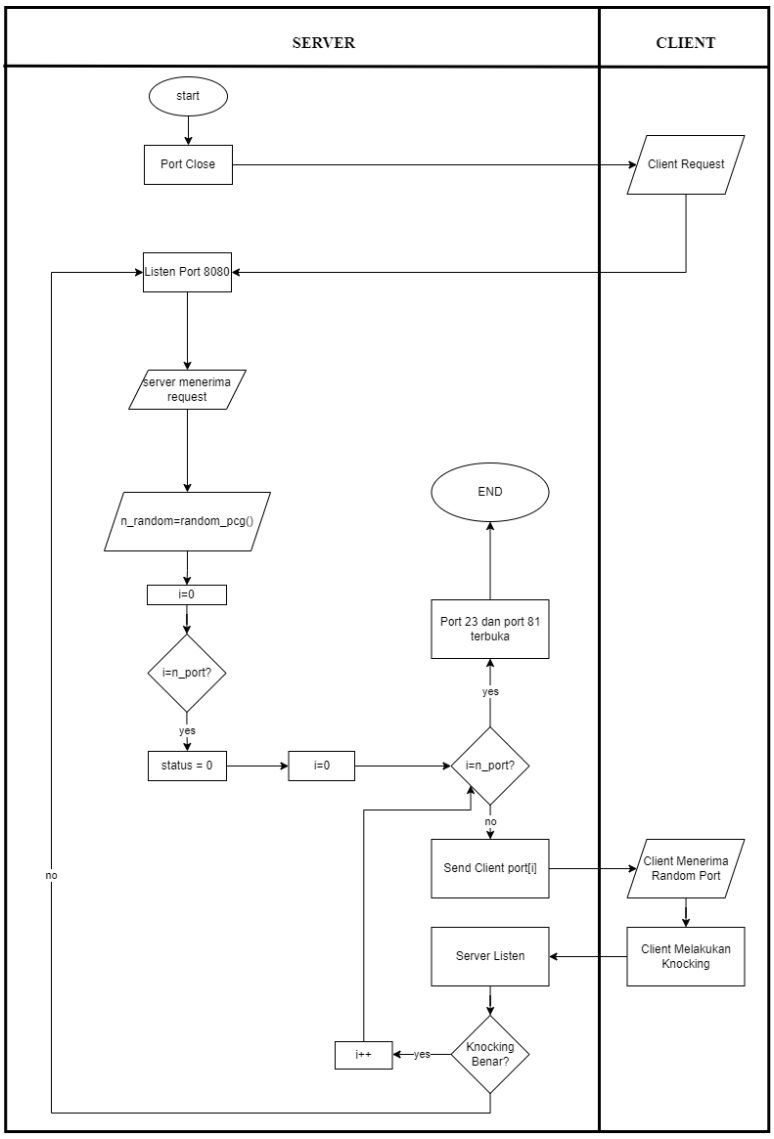
2. Client

Komputer client memiliki fungsi melakukan request ke komputer server untuk dapat membuka port 23 dan port 80. Sebelum dapat membuka port 23 dan 80 client harus melakukan request untuk mendapatkan nomor port dari server, kemudian client akan melakukan pengetukan apabila sudah mendapatkan nomor port yang diacak oleh server secara bertahap. Setelah proses pengetukan selesai dilakukan dengan benar, maka port 23 dan 80 dapat terbuka dan dapat diakses oleh client.

2.7. Flowchart Proses Open Port dan Close Port

Pada proses ini akan dijelaskan bagaimana client dapat membuka port yang tertutup pada server dan client penutup port pada server apabila sudah selesai melakukan koneksi.

1. Proses open port



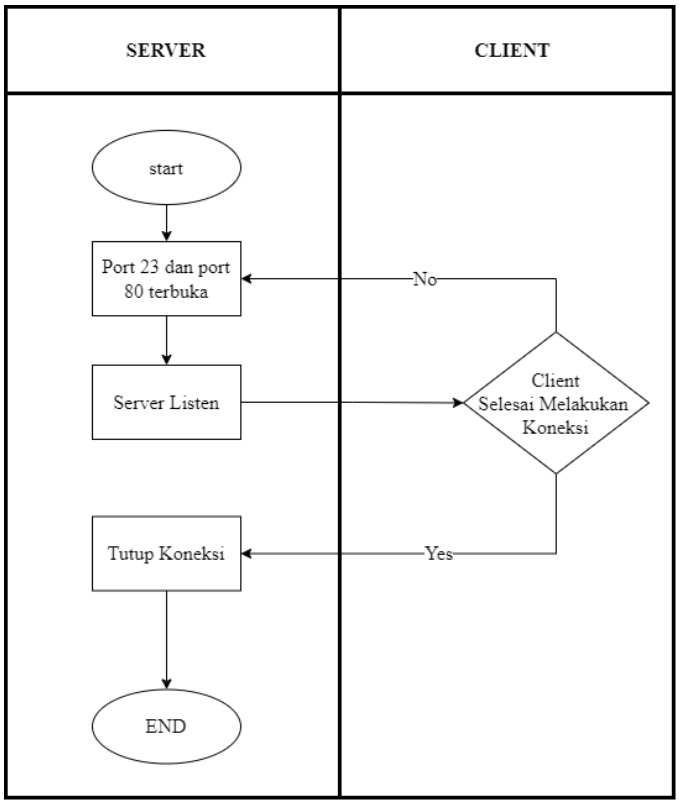
Gambar 2.3 Flowchart Proses Open Port

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Berikut penjelasan untuk gambar 2.3 Flowchart Proses Open Port :

1. Pada proses pertama keadaan *port* masih tertutup untuk koneksi terhadap *client* baru.
2. *Client* melakukan *request* dan akan didengar oleh *port* 8080, dimana keadaan *port* 8080 selalu dalam keadaan *listen*. Fungsi dari *port* 8080 disini adalah untuk selalu *listening* terhadap *request* dari *client* yang berupa *request port knocking*.
3. *Server* menerima *request* dari *client* dan akan dilakukan pengujian terhadap *request* tersebut.
4. *request* dari *client* merupakan *port knocking* maka akan dilakukan pengacakan dengan algoritma PCG-XSH-RR.
5. Variabel n_*port* digunakan untuk menampung nilai terhadap *port* yang telah diacak.
6. Variabel i akan bernilai 0.
7. Diuji apakah i bernilai sama dengan n_*port* atau tidak.
8. Apabila tidak maka akan dilakukan proses terhadap variabel *port*[i] yang menampung *port* yang diacak. Kemudian nilai i akan selalu ditambah 1, kemudian pengujian kembali dilakukan terhadap nilai i.
9. Apabila iya maka variabel status akan bernilai 0 atau false.
10. Kemudian i bernilai 0.
11. Dilakukan pengujian kembali apakah i sama dengan *port* yang telah di*random*.
12. Apabila tidak maka *port* yang telah diacak akan dikirim satu per satu ke *client*. *Client* akan menerima *port* dan melakukan pengetukan. Dalam keadaan tersebut *server* dalam keadaan listen untuk menerima ketukan. Kemudian akan dilakukan pengujian apakah pengetukan sudah benar atau tidak. Apa bila iya maka nillai i akan bertambah 1 dan pengujian terhadap nilai i apakah sama dengan *port* yang diacak akan dilakukan kembali. Apabila tidak maka proses akan kambali menuju keadaan dimana *port* 8080 hanya dalam keadaan listen untuk menerima *request* kembali dari *client* berupa *request port knocking*.
13. Apabila iya maka *port telnet* akan terbuka dan proses selesai.

2. Proses close port



Gambar 2.4 Flowchart Proses Close port

Berikut penjelasan untuk gambar 2.4 *flowchart* proses *close port*:

1. Pada proses pertama *port* 23 dan *port* 80 sudah dalam keadaan terbuka dan *server* masih dalam keadaan listen.
2. Kemudian dilakukan pengujian apakah *client* sudah selesai melakukan koneksi atau tidak.
3. Apabila tidak maka *port* 23 dan *port* 80 masih dalam keadaan terbuka dan apabila iya maka koneksi akan ditutup.
4. Proses selesai

3. Hasil dan Pembahasan

Pada bagian hasil dan pembahasan ini, penuilis melakukan pengujian serangan brute force terhadap jaringan pada sistem e-learning dengan menggunakan metode port knocking dan tidak menggunakan metode port knocking. Dengan tujuan seberapa pengaruh penggunaan metode port knocking untuk mengamankan jaringan vpn pada system e-learning.

pada penelitian ini menggunakan tools Ncrack 0.4ALPHA. pengujian ini akan mencoba untuk masuk ke server melalui port 23 (telnet) dengan menggunakan ncrack. Pada proses serangn brute force attack ini akan digunakan wordlist yang berisi username dan password. Pada wordlist ini berisikan list kata – kata yang berbeda pada masing-masing file.

```
root@client-VirtualBox:/home/client/Documents/wordlist# ncrack -U username2.lis
t -P password2.list 192.168.1.11:23

Starting Ncrack 0.7 ( http://ncrack.org ) at 2022-04-12 11:41 WITA

Discovered credentials for telnet on 192.168.1.11 23/tcp:
192.168.1.11 23/tcp telnet: 'server' '12345'

Ncrack done: 1 service scanned in 45.01 seconds.

Ncrack finished.
root@client-VirtualBox:/home/client/Documents/wordlist#
```

Gambar 3.1 Brute Force Attack pada Server

Pada gambar 3.1 telah dilakukan brute force attack menuju ke server e-learning yang tidak menggunakan metode port knocking, brute force attack menyerang melalui port 23 untuk mendapatkan username dan password. Serangan berhasil dilakukan dan ncrack berhasil di mendapatkan username dan password melalui port 23 (telnet).

```
root@client-VirtualBox:/home/client/Documents/wordlist# ncrack -U username2.lis
t -P password2.list 192.168.1.11:23

Starting Ncrack 0.7 ( http://ncrack.org ) at 2022-04-12 11:54 WITA


Ncrack done: 1 service scanned in 3.00 seconds.

Ncrack finished.
root@client-VirtualBox:/home/client/Documents/wordlist#
```

Gambar 3.2 Brute Force Attack Pada Server Dengan Port knocking

Pada gambar 3.2 telah dilakukan brute force attack menuju ke server e-learning yang menggunakan metode port knocking, brute force attack menyerang melalui port 23 untuk mendapatkan username dan password. Serangan tidak berhasil dilakukan dan ncrack gagal mendapatkan username dan password melalui port 23 (telnet). Hal tersebut dapat terjadi karena metode port knocking membuat port 23 yang awalnya terbuka menjadi tertutup, sehingga hanya client yang sudah memiliki akses saja yang dapat membuka port 23.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Tabel 3.1 Pengujian Brute Force Attack

JUMLAH WORDLIST	TANPA METODE PORT KNOCKING		DENGAN METODE PORT KNOCKING	
	WAKTU (DALAM DETIK)	HASIL BRUTE FORCE ATTACK	WAKTU (DALAM DETIK)	HASIL BRUTE FORCE ATTACK
1	33	SUKSES	3	TIDAK SUKSES
2	45	SUKSES	3	TIDAK SUKSES
3	51	SUKSES	3	TIDAK SUKSES
4	66	SUKSES	3	TIDAK SUKSES
5	69	SUKSES	3	TIDAK SUKSES
6	75	SUKSES	3	TIDAK SUKSES
7	81	SUKSES	3	TIDAK SUKSES
8	90	SUKSES	3	TIDAK SUKSES
9	144	SUKSES	3	TIDAK SUKSES
10	146	SUKSES	3	TIDAK SUKSES

Pada Tabel 3.1 merupakan hasil dari pengujian untuk Brute Force Attack yang dilakukan sebanyak 10 kali dengan wordlist yang di dalamnya terdapat kata-kata yang berbeda di setiap file wordlist. Dilakukan 10 kali pengujian berdasarkan pada perhitungan confidence interval yang didapatkan yaitu dengan nilai kepercayaan 95% bahwa 10 kali sudah mampu memberikan hasil yang valid.

4. Kesimpulan

Berdasarkan pada penelitian yang telah dilakukan, metode port knocking dapat mengatasi serangan pada jaringan VPN dengan membuat port 23 (telnet) dan port 80 (web e-learning) dalam keadaan filtered atau tertutup, sehingga hanya client atau admin yang telah memiliki akses yang dapat mengakses port tersebut. Port 23 (telnet) dan port 80 (web e-learning) dapat terjamin keamanannya dari serangan brute force yang menggunakan tool ncrack.

Referensi

[1] I. G. So and F. Kurniawan, “Perancangan E-Learning Berbasis Internet pada Sekolah SMK Negeri 13 Jakarta,” *Binus Bus. Rev.*, vol. 1, no. 2, p. 394, 2010, doi: 10.21512/bbr.v1i2.1085.

[2] S. K. Chung, O. C. Yee, M. M. Singh, and R. Hassan, “SQL injections attack and session hijacking on e-learning systems,” *I4CT 2014 - 1st Int. Conf. Comput. Commun. Control Technol. Proc.*, no. I4ct, pp. 338–342, 2014, doi: 10.1109/I4CT.2014.6914201.

[3] I. Afrianto and E. B. Setiawan, “Kajian virtual private network (vpn) sebagai sistem pengamanan data pada jaringan komputer (studi kasus jaringan komputer unikom),” *Maj. Ilm. UNIKOM*, vol. 12, no. 1, pp. 43–52, 2015, doi: 10.34010/miu.v12i1.34.

[4] Edy Haryanto1), Widyawan2), dan Dani Adhipta 3) 1, “Meningkatkan keamanan port knocking dengan kombinasi special features icmp, source port, dan tunneling,” pp. 187–194, 2016.

[5] E. Sutanta, “Analisis Keamanan Sistem Aplikasi (Study Kasus Pada Aplikasi E-Learning Di IST AKPRIND Yogyakarta),” *Pros. Semin. Nas. SNAST 2008, IST AKPRIND Yogyakarta, ISSN 1979-911X*, pp. 243–253, 2008, [Online]. Available: http://snast.akprind.ac.id/.

[6] P. Riska, P. Sugiartawan, and I. Wiratama, “Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking,” *J. Sist. Inf. dan Komput. Terap. Indones.*, vol. 1, no. 2, pp. 53–64, 2018, doi: 10.33173/jsikti.12.

[7] I. M. A. D. Putra and I. K. Ari Mogi, “The Data Communication Security Design on IoT Based Systems with the Port Knocking Method,” *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 8, no. 4, p. 387, 2020, doi: 10.24843/jlk.2020.v08.i04.p04.

[8] M. E. O’neill, “A PCG: A Family of Simple Fast Space-Efficient Statistically Good Algorithms for Random Number Generation,” *ACM Trans. Math. Softw. V*, vol. V, no. 212, pp. 1–46, 2017, [Online]. Available: http://www.pcg-random.org/pdf/toms-oneill-pcg-family.pdf.