PROSIDING Seminar Nasional SISFOTEK ISSN 2597-3584 (Media Online)
Sistem Informasi dan Teknologi
website : www.seminar.iaii.or.id | email : seminar@iaii.or.id

Implementasi Port Forwarding Untuk Keamanan Data Server (Studi Kasus: Dinas Pendidikan Kab. Pasuruan)

Siska Dea[1], Dian Wahyuningsih[2], Mahmud Yunus[3]
[1,2,3]Teknologi Informasi, STMIK PPKIA Pradnya Paramita
siskhadhea@gmail.com

Abstract

District Education Office. Pasuruan has a windows-based website application that uses Windows server 2008. The server was hijacked by hackers by changing the database configuration and changing the website display script. Hijacking occurs because of the large number of open ports that are not used on Windows Server 2008. The more open ports, the more vulnerable the server is to penetrate. Even after installing a firewall on Windows Server 2008, hackers can still penetrate it. This can be overcome by migrating to a new server, but it cannot be done because the server is connected to the Windows-based Central Ministry server for the sake of data decentralization. To overcome this problem, Windows Server 2008 is paired with a Linux server as a firewall router that is configured using the port forwarding method. The results of the study show that port forwarding can provide security on Windows Server 2008. Clients from outside networks cannot access Windows Server 2008 directly, so clients cannot find out the original IP address or open ports which can be a gap to penetrate the network. Windows server 2008. Clients from the network can access website applications on Windows server 2008 through an intermediary router.

Keywords: *dinas pendidikan kab. pasuruan, port forwarding, server security, windows server 2008, linux server*

Abstrak

Dinas Pendidikan Kab. Pasuruan memiliki aplikasi *website* berbasis windows yang menggunakan Windows server 2008. Server tersebut dibajak oleh *hacker* dengan mengganti konfigurasi database serta mengganti *script* tampilan *website*. Pembajakan terjadi karena banyaknya *port* terbuka yang tidak digunakan pada Windows server 2008. Semakin banyak *port* yang terbuka semakin rentan dilakukan penetrasi server. Meskipun sudah melakukan pemasangan *firewall* pada Windows server 2008, *hacker* masih dapat menembusnya. Hal tersebut bisa diatasi dengan melakukan migrasi ke server baru, namun tidak dapat dilakukan karena server tersebut terhubung dengan server Kementrian Pusat yang berbasis windows untuk kepentingan desentralisasi data. Untuk mengatasi permasalahan tersebut Windows server 2008 disandingkan dengan server linux sebagai router *firewall* yang dikonfigurasi menggunakan metode *port forwarding*. Hasil dari penelitian diperoleh bahwa dengan melakukan *port forwarding* dapat memberi keamanan pada Windows server 2008. *Client* dari jaringan luar tidak dapat mengakses Windows server 2008 secara langsung, sehingga *client* tidak dapat mengetahui alamat IP asli maupun *port* yang terbuka yang dapat menjadi celah untuk melakukan penetrasi pada Windows server 2008. *Client* dari jaringan dapat mengakses aplikasi website yang ada di Windows server 2008 melalui perantara router.

Kata kunci: *dinas pendidikan kab. pasuruan, port forwarding, keamanan server, windows server 2008, server linux*

1. Pendahuluan

Guna menjamin keberlangsungan sebuah aplikasi berbasis *website* dibutuhkan server yang tangguh. Pemerintahan banyak membuat aplikasi dengan menggunakan server Windows sebagai wadah aplikasinya. Salah satunya adalah aplikasi data pokok pendidikan (dapodik) milik Dinas Pendidikan Kab. Pasuruan yang menggunakan Windows Server 2008. Aplikasi tersebut terhubung dengan aplikasi kementrian pusat melalui ip publik untuk desentralisasi data.

Windows server 2008 memiliki banyak port yang terbuka yang menyebabkan server lebih mudah dipenetrasi. Banyak serangan yang dilakukan oleh orang-orang yang tidak bertanggung jawab melakukan serangan terhadap server. Serangan-serangan tersebut sering dilakukan pada suatu *port–port* yang dalam

keadaan terbuka, sehingga nantinya akan membuat orang–orang yang tidak mempunyai hak akses maupun yang tidak berkepentingan dapat dengan mudah mengendalikan *port–port* yang telah dimasuki [1].

Salah satu insiden pernah terjadi pada server milik Dinas Pendidikan Kab. Pasuruan yang dibajak oleh pihak tidak bertanggung jawab dengan mengubah konfigurasi koneksi *database* sehingga aplikasi tidak dapat menampilkan data dari *database* serta mengubah *script* tampilan. Usaha yang pernah dilakukan adalah melakukan pemasangan *firewall* di server tetapi masih dapat ditembus oleh *hacker*.

Salah satu cara mengatasi permasalahan tersebut adalah dengan melakukan migrasi server dari Windows server 2008 ke server baru. Namun migrasi server tidak dapat dilakukan karena aplikasi Kementrian Pusat untuk kebutuhan sinkronisasi data berbasis Windows. Pada penelitian ini diusulkan untuk menyandingkan server Windows dengan server linux guna menambah keamanan. Sebelum mengakses aplikasi yang ada di server Windows 2008 akan ditahan terlebih dahulu oleh keamanan linux. Server linux berperan sebagai router dengan menggunakan metode *port forwarding*.

Berdasarkan latar belakang permasalahan tersebut, maka fokus dari penelitian ini adalah mengimplementasikan metode *port forwarding* untuk mengamankan data yang ada di Windows server 2008. Metode *port forwarding* ini akan membatasi akses ke Windows server 2008, sehingga Windows server 2008 hanya dapat dihubungi oleh router. *Request* dari *client* diterima oleh router, kemudian diteruskan ke server Windows 2008, sehingga server Windows 2008 lebih aman karena tidak dapat diakses langsung dari jaringan luar dan untuk berkomunikasi dengan server Windows 2008 harus melalui perantara router terlebih dahulu.

Keamanan server sangat penting untuk menjaga data yang ada di dalamnya beserta menjaga kinerjanya. Ada beberapa cara untuk menjaga keamanan server, salah satunya melakukan konfigurasi *firewall*. *Firewall* adalah sebuah sistem aplikasi di dalam sistem komputer yang berfungsi untuk melindungi komputer yang terkoneksi dalam jaringan komputer dari berbagai macam ancaman atau gangguan dari user yang tidak bertanggung jawab. Penggunan *firewall* merupakan suatu cara untuk memastikan informasi yang bersifat pribadi atau data yang terhubung dengan internet tidak dapat diakses oleh pihak yang tidak bersangkutan [2]. Untuk melakukan konfigurasi firewall salah satunya dapat menggunakan *port forwarding*. Settingan router yang perlu dirubah adalah fungsi *Port Forwarding* yang harus diaktifkan, karena pada kebanyakan router suatu fungsi *Port Forwarding* biasanya telah dimatikan secara *default* [3].

Windows Server 2008 merupakan pengembangan dari versi sebelumnya yaitu Windows Server 2003 dan Windows Vista. Windows Server 2008 memiliki sistem *tools* virtualisasi dan web *resources* diantaranya IIS 7, Windows Server Manager, dan Windows PowerShell. Windows server 2008 memiliki celah keamanan sehingga rentan dilakukan pembajakan pada server. Celah tersebut diantaranya kemanan pad IIS kurang terjamin, banyak port yang terbuka secara defaut. Hasil yang telah dicapai dari penelitian tentang eksploitasi system keamanan RPC (*Remote Procedure Call*) pada jaringan Windows Server 2008 diantaranya adalah pengubahan terhadap password administrator, proses reboot, dan pengambilan file yang ada pada direktori Windows Server 2008 [4], hal tersebut menambah celah untuk melakukan pembajakan.

Ubuntu merupakan salah satu distro linux debian yang saat ini banyak digunakan. Ubuntu memiliki sebuah *tools firewall* yang disebut iptables. IPTables adalah program aplikasi (berbasis linux) yang memungkinkan administrator sistem untuk mengkonfigurasi tabel yang disediakan oleh firewall kernel linux (diimplementasikan sebagai modul Netfilter yang berbeda) dan rantai dan aturan di tempat itu [5]. IPTables berfungsi untuk mengatur lalu lintas jaringan dengan mengizinkan atau memblokir koneksi masuk, keluar, atau sekedar melewati server. Beberapa tabel yang ada di IPTables adalah tabel filter, Network Address Translation (NAT), dan *mangle*. Yang digunakan pada penelitian ini adalah tabel NAT untuk konfigurasi *port forwarding* dan tabel filter untuk pemblokiran port yang tidak digunakan.

Port Forwarding bertugas sebagai penerjemah alamat atau nomor *port* dari sebuah paket ke tujuan baru dan meneruskan paket sesuai dengan tabel *routing* yang telah dibuat [6]. *Port forwarding* merupakan bagian dari iptables. Untuk melakukan *port forwarding*, tabel NAT menggunakan fitur *Destination* NAT dalam *chain* PREROUTING. Untuk menambah keamanan, setelah dilakukan *port forwarding* dilakukan penambahan konfigurasi *port blocking* untuk memblokir *port-port* yang tidak digunakan. *Port blocking* dapat digunakan untuk mengatur hak akses jaringan pada setiap port LAN (Local Area Network) [7].

Jaringan komputer merupakan kumpulan dari beberapa *host* dan konektivitasnya. *Host* bisa berupa komputer (PC), laptop, atau jenis lainnya, sedangkan konektivitas adalah media penghubung yang bisa berupa kabel (*wire*) atau tanpa kabel (*wireless*) [8]. Jaringan komputer ada yang bersifat publik yang artinya dapat diakses oleh semua orang yang memiliki jaringan internet. Sedangkan jaringan lokal merupakan jaringan yang hanya dapat diakses oleh orang yang berada pada area dengan menggunakan koneksi pada alamat tertentu.

Penelitian ini dilakukan untuk mengamankan data pada Windows 2008 agar terhindar dari *hacker* dengan proses desentralisasi data dengan Kementrian Pusat tetap dapat dilakukan, serta menyediakan perantara agar jaringan luar dapat mengakses aplikasi website dapodik yang ada di Windows server 2008 dengan normal dan aman.

2. Metode Penelitian

Metode yang digunakan pada penelitian ini adalah metode *port forwarding*. Fungsi *port forwarding* adalah membuka akses terhadap perangkat pada jaringan lokal untuk dapat diakses melalui jaringan publik [9]. Untuk menambah keamanan, setelah dilakukan *port forwarding* dilakukan penambahan konfigurasi *port blocking* untuk memblokir *port-port* yang tidak digunakan. Konfigurasi *port blocking* berguna untuk menghalangi akses pihak yang dikenal maupun tidak dikenal untuk mencegah terjadinya pencurian data. Konfigurasi *port forwarding* dan *port blocking* dilakukan menggunakan menggunakan *prototype* dengan linux ubuntu yang difungsikan sebagai router.

2.1. Alat Penelitian

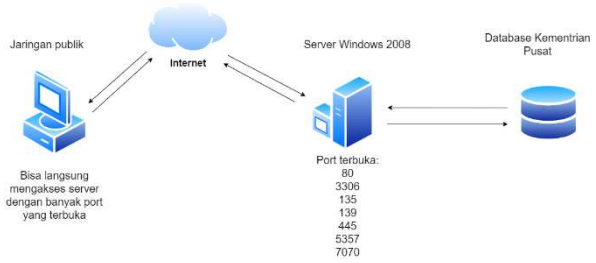
Pada penelitian ini, untuk mensimulasikan topologi yang ada di Dinas Pendidikan Kab. Pasuruan dibangun *prototype* dengan spesifikasi sebagai berikut:

Tabel 1. Spesifikasi alat penelitian

No	Spesifikasi Hardware	Spesifikasi Software	Fungsi
1.	Virtual Box	Sistem operasi Windows server 2008 Web server IIS	Sebagai web server dan server sinkronisasi
2.	Dynabook laptop: Intel Core i5 (3rd Gen) 3437U Memory DDR3 SDRAM 4Gb Hardisk SSD 128Gb	Sistem operasi linux ubuntu	Sebagai router *port forwarding*
3.	IP Privat server linux	192.168.43.19	Sebagai pengganti IP publik
4.	Jaringan Internet		Untuk akses internet menggunakan *tethering*

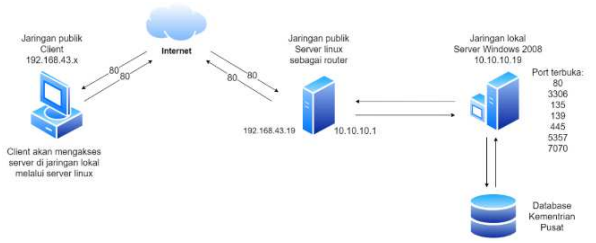
2.2 Topologi Jaringan

Topologi jaringan dibagi menjadi topologi jaringan sebelum dan sesudah dilakukan *port forwarding*.



Gambar 1. Topologi jaringan sebelum *port forwarding*

Gambar 1 merupakan topologi jaringan sebelum dilakukan port forwarding. Pada topologi tersebut *client* dari jaringan publik terhubung satu jaringan dengan server, sehingga dapat mengakses server secara langsung dan dapat melihat banyaknya port yang terbuka. Hal tersebut menyebabkan server lebih rentan dipenetrasi. Server Windows 2008 terhubung dengan aplikasi Kementrian Pusat untuk melakukan sinkronisasi data melalui jaringan internet.



Gambar 2. Topologi jaringan sesudah *port forwarding*

Gambar 2 merupakan topologi sesudah dilakukan *port forwarding*. Jaringan publik yang akan mengakses server Windows 2008 atau jaringan lokal menggunakan ip publik yang ada di router server linux. *Port* yang dibuka hanya port 80, kemudian router server linux meneruskan *request* tersebut ke ip server Windows 2008 menggunakan ip lokal antara router server linux dan server Windows 2008. Server Windows 2008 dapat melakukan sinkronisasi dengan server Kementrian Pusat dengan memanfaatkan jaringan *Network Address Translation* (NAT) yang dikonfigurasi di router linux server.

Topologi sesudah dilakukan port forwarding terdiri dari jaringan publik dan jaringan lokal, yang IP *address*, netmask dan *gateway* diatur seperti tabel berikut:

Tabel 2. IP *address*, netmask, *gateway* jaringan publik

Perangkat	IP	Netmask	*Gateway*
Internet	192.168.43.x	255.255.255.0	192.168.43.x
Server Linux	192.168.43.19	255.255.255.0	192.168.43.x
Client	192.168.43.56	255.255.255.0	192.168.43.x

Tabel 3. IP *address*, netmask, *gateway* jaringan lokal

Perangkat	IP	Netmask	Gateway
Server Linux	10.10.10.1	255.255.255.0	10.10.10.1
Windows server 2008	10.10.10.19	255.255.255.0	10.10.10.1

2.2. Konfigurasi

Sebelum konfigurasi *port forwarding* dilakukan *setting* ipv4 dan aktivasi fungsi ip forward terlebih dahulu. Kemudian dilakukan konfigurasi iptables.

```
luqman@luqman-dynabook-R632-F:~$ sudo iptables \
> -t nat \
> -A PREROUTING \
> -p tcp \
> -d 192.168.43.19 \
> --dport 80 \
> -j DNAT \
> --to-destination 10.10.10.19:80
[sudo] password for luqman:
luqman@luqman-dynabook-R632-F:~$ sudo iptables \
> -t nat \
> -A POSTROUTING \
> -o wlp2s0 \
> -j MASQUERADE
```

Gambar 3. Konfigurasi *port forwarding*

Gambar 3 merupakan konfigurasi port forwarding pada server linux yang dilakukan dengan 2 langkah yaitu PREROUTING dan POSTROUTING. PREROUTING merupakan koneksi yang masuk ke dalam router dan melewati router. Pada proses PREROUTING dilakukan pengalamatan paket dari IP server linux diarahkan ke IP Windows server 2008. POSTROUTING merupakan koneksi yang akan keluar dari router. Pada proses ini dilakukan dengan masquerade untuk menyamarkan IP Windows server 2008 seolah paket yang dikembalikan ke jaringan luar berasal dari IP server linux. Pada proses POSTROUTING juga bertujuan agar Windows server 2008 tetap dapat mengakses internet.

```
sudo iptables -A INPUT -s 0/0 -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -s 0/0 -p tcp --dport 22 -j DROP
sudo iptables -A INPUT -s 0/0 -p tcp --dport 7070 -j DROP
sudo iptables -A INPUT -s 0/0 -j DROP
```

Gambar 4. Konfigurasi *port blocking*

Gambar 4 merupakan konfigurasi *port blocking* untuk memblokir *port-port* yang tidak digunakan untuk menambah keamanan. Perintah yang pertama digunakan untuk mengizinkan mengakses *port* 80, dimana request yang masuk diteruskan ke Windows server 2008 menggunakan *port forwarding* yang telah dikonfigurasi sebelumnya. Perintah selanjutnya digunakan untuk memblokir port 22,7070 dan semua *port* yang terbuka sehingga tidak ada request yang bisa masuk selain melalui *port* 80.

3. Hasil dan Pembahasan

3.1. Pengujian Topologi Jaringan

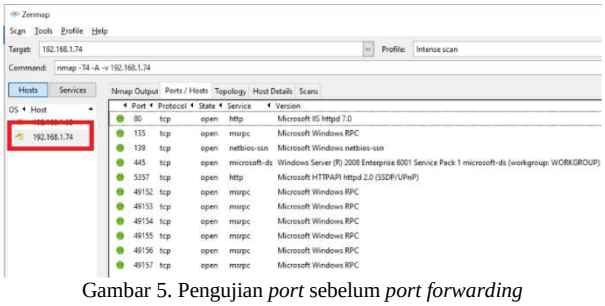
Untuk mengetahui hasil berdasarkan topologi jaringan yang telah dibuat, dilakukan pengujian ping antar perangkat di jaringan sebelum dan sesudah dilakukan *port forwarding*. Berikut ini hasil dari pengujian topologi jaringan yang telah dilakukan:

Tabel 4. Hasil pengujian topologi jaringan sebelum dan sesudah *port forwarding*

No.	Pengujian	Hasil Sebelum	Hasil Sesudah	Keterangan
1.	Client ping ke IP internet	Berhasil	Berhasil	Client dapat mengakses internet
2.	Client ping ke IP Windows Server 2008	Berhasil	Tidak berhasil	Sesudah dilakukan port forwarding client tidak mengetahui IP asli Windows server 2008 dan hanya dapat menghubungi melalui IP server linux
3.	Client ping ke server linux	-	Berhasil	Sebelum dilakukan port forwarding hasil ping kosong, karena server linux belum ada di topologi jaringan publik
4.	Server linux ping ke internet	-	Berhasil	Sebelum dilakukan port forwarding hasil ping kosong, karena server linux belum ada di topologi jaringan lokal
5.	Server linux ping ke Windows Server 2008	-	Berhasil	Sebelum dilakukan port forwarding hasil ping kosong, karena server linux belum ada di topologi jaringan lokal
6.	Windows server 2008 ping ke server linux	-	Berhasil	Sebelum dilakukan port forwarding hasil ping kosong, karena server linux belum ada di topologi jaringan lokal

3.2. Pengujian Konfigurasi *Port*

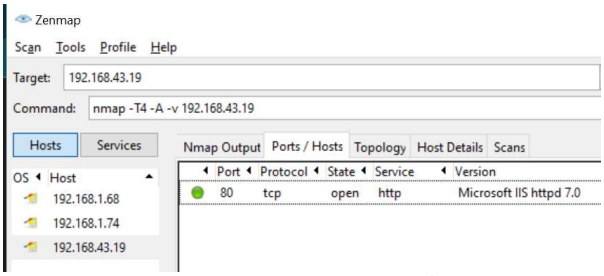
Untuk mengetahui hasil dari *port* yang dibuka maupun diblokir sebelum dan sesudah dilakukan *port forwarding*, dilakukan pengujian *scanning port* menggunakan aplikasi zenmap dengan hasil sebagai berikut:



Gambar 5. Pengujian *port* sebelum *port forwarding*

Gambar 5 merupakan hasil *scanning port* sebelum dilakukan *port forwarding*. *Client* dari jaringan luar dapat melakukan *scan port* secara langsung pada Windows server 2008. Pada gambar tersebut terlihat banyak *port* dengan status *open*. *Security-minded people know that each open port is an avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users*

[10]. Jika diartikan secara bebas *port* yang berstatus *open* rentan dilakukan eksploitasi dan pembajakan oleh pihak yang tidak bertanggung jawab.



Gambar 6. Pengujian *port* sesudah *port forwarding*

Gambar 6 merupakan hasil pengujian *port* menggunakan zenmap pada server linux yang telah dikonfigurasi port forwarding. Berdasarkan pengujian tersebut hanya port 80 saja yang terbuka. Port yang tidak diperlukan telah ditutup sehingga mengurangi celah untuk melakukan penetrasi pada Windows server 2008 melalui port yang terbuka.

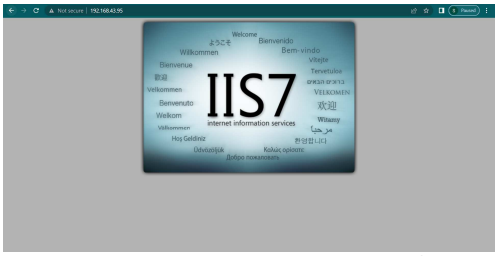
Hasil pengujian port sebelum dan sesudah *port forwarding* ditunjukkan dengan tabel berikut:

Tabel 5. Hasil pengujian konfigurasi *port* sebelum dan sesudah *port forwarding*

No	Pengujian	Hasil Sebelum	Hasil Sesudah	Keterangan
1.	Port yang terbuka	80, 135, 139, 445, 5357, 49152, 49153, 49154, 49155, 49156, 49157	80	Scanning port yang terbuka sebelum port forwarding dilakukan langsung pada Windows server 2008
2.	Port yang diblokit	-	Semua port kecuali port 80	Sebelum dilakukan port forwarding tidak ada port yang diblokir pada Windows server 2008, sedangkan sesudah dilakukan port forwarding dilakukan pemblokiran semua port kecuali port 80

3.3. Pengujian Akses Aplikasi

Untuk mengetahui hasil akses aplikasi sebelum dan sesudah dilakukan *port forwarding*, dilakukan pengujian dengan hasil sebagai berikut:

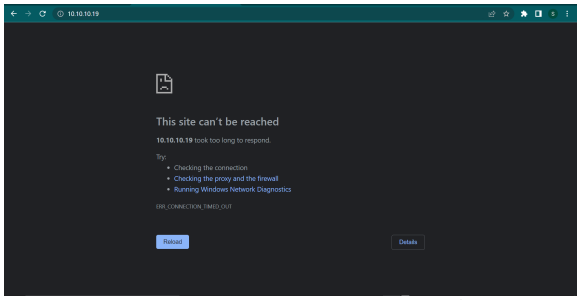


Gambar 7. Pengujian akses aplikasi sebelum *port forwarding*

Gambar 7 merupakan hasil pengujian akses aplikasi sebelum dilakukan *port forwarding* yang menampilkan halaman aplikasi yang ada di Windows server 2008. Pengujian diakses menggunakan IP 192.168.43.95 milik Windows server 2008.

Gambar 8. Pengujian akses aplikasi sesudah *port forwarding*

Gambar 8 merupakan hasil pengujian akses aplikasi sesudah dilakukan *port forwarding* yang menampilkan halaman aplikasi yang ada di Windows server 2008 melalui perantara server linux. Pengujian diakses menggunakan IP 192.168.43.19 milik server linux.



Gambar 9. Pengujian akses aplikasi sesudah *port forwarding*

Gambar 9 merupakan hasil pengujian akses aplikasi sesudah dilakukan *port forwarding* yang menampilkan halaman aplikasi yang ada di Windows server 2008 gagal dimuat menggunakan IP Windows server 10.10.10.19. Hal tersebut karena Windows server 2008 berbeda jaringan dengan client. Untuk mengaksesnya harus melalui perantara server linux.

Hasil pengujian port sebelum dan sesudah *port forwarding* ditunjukkan dengan tabel berikut:

Tabel 5. Hasil pengujian konfigurasi *port* sebelum dan sesudah *port forwarding*

No	Pengujian	Hasil Sebelum	Hasil Sesudah	Keterangan
1.	Client akses aplikasi langsung ke Windows server 2008	Berhasil	Tidak Berhasil	Setelah dilakukan port forwarding client tidak dapat mengakses Windows server 2008 secara langsung, melainkan harus melalui perantara server linux karena sudah berbeda jaringan

No	Pengujian	Hasil Sebelum	Hasil Sesudah	Keterangan
2.	Client akses aplikasi melalui router server linux	-	Berhasil	Sebelum dilakukan port forwarding hasil akes aplikasi kosong, karena server linux belum ditambahkan di topologi. Sesudah port forwarding berhasil akses aplikasi karena berada dalam satu jaringan publik
3	Router server linux akses aplikasi langsung ke Windows server 2008	-	Berhasil	Sebelum dilakukan port forwarding hasil akes aplikasi kosong, karena server linux belum ditambahkan di topologi. Sesudah port forwarding berhasil akses aplikasi karena berada dalam satu jaringan lokal

4. Kesimpulan

Berdasarkan pengujian konfigurasi yang telah dilakukan, *port forwarding* dapat memberi keamanan pada Windows server 2008. *Client* dari jaringan luar tidak dapat mengakses windows server 2008 secara langsung, sehingga *client* tidak dapat mengetahui IP maupun *port* yang terbuka. *Client* dari jaringan luar hanya berhubungan dengan router server linux. Selain itu *port* yang terbuka hanya yang dibutuhkan sehingga mempersempit celah untuk melakukan penetrasi pada Windows server 2008. Dengan penerapan *port forwarding* jaringan luar dapat mengakses aplikasi *website* dapodik yang ada di Windows server 2008 dengan normal dan aman melalui perantara router server linux.

Ucapan Terimakasih

Terimakasih kepada Dinas Pendidikan Kabupaten Pasuruan yang sudah bersedia menjadi tempat melakukan penelitian. Serta STMIK PPKIA Pradnya Paramita yang telah memberikan pendanaan prosiding penelitian ini.

Daftar Rujukan

[1] P. Riska, P. Sugiartawan dan I. Wiratama, "Sistem Keamanan Jaringan Komputer dan Data Dengan Menggunakan Metode Port Knocking," *Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI)*, p. 53, 2018.

[2] S. Khadafi, S. Nurmuslimah dan F. K. Anggakusuma, "IMPLEMENTASI FIREWALL DAN PORT KNOCKING SEBAGAI KEAMANAN DATA TRANSFER PADA FTP SERVER BERBASISKAN LINUX UBUNTU SERVER," *Jurnal Ilmiah NERO Vol. 4 No. 3*, p. 182, 2019.

[3] F. A. Purwaningrum, A. Purwanto dan E. A. Darmadi, "OPTIMALISASI JARINGAN MENGGUNAKAN FIREWALL," *Jurnal IKRA-ITH Informatika*, p. 21, 2018.

[4] A. Nugroho dan M. Kusban, "Eksploitasi Sistem Keamanan RPC (Remote Procedure Call) pada Jaringan Windows Server 2008," Universitas Muhammadiyah Surakarta, Surakarta, 2015.

[5] E. S. Jullev A dan B. M. Susanto, "Pemanfaatan Iptables Sebagai Intrusion Detection System (IDS) pada Linux Server," *Seminar Nasional Hasil Penelitian*, p. 349, 2017.

[6] L. S. Dry dan Z. Munir, "Rancang Bangun IP PUBLIC Berbasis VPN Server dan Port Forwarding Untuk Mail Server Pada CV Pacific Computer Batam," *Jurnal Sistem Informasi dan Manajemen STMIK GICI*, p. 1, 2017.

[7] S. dan W. Sulistyo, "Model Keamanan Jaringan Menggunakan Firewall Port Blocking," *Krea-TIF: Jurnal Teknik Informatika*, p. 10, 2022.

[8] S. Sumardi dan M. T. Asri Zaen, "PERANCANGAN JARINGAN KOMPUTER BERBASIS MIKROTIK ROUTER OS PADA SMAN 4 PRAYA," *JIRE (Jurnal Informatika & Rekayasa Elektronika)*, p. 52, 2018.

[9] H. Pratama dan N. F. Puspitasari, "Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP," *Citec Journal*, p. 52, 2020.

[10] nmap, "Port Scanning Basics," nmap.org, 20 07 2022. [Online]. Available: https://nmap.org/book/man-port-scanning-basics.html. [Diakses 27 07 2022].