Penggunaan Secure Shell (SSH) Sebagai Sistem Komunikasi Aman Pada Web Ujian Online

Heni Jusuf [1,*]

[1] Program Studi Teknik Elektro Fakultas Teknik dan Sains; Universitas Nasional; Jl. Sawo Manila, Pejaten, Pasar Minggu Jakarta Selatan; e-mail: heni.jusuf@civitas.unas.ac.id

* Penulis yang menangani Korespondensi:
E-mailheni.jusuf@civitas.unas.ac.id

Abstract: *Network security becomes a critical need for the administrator to manage the website. One example is the online test web. Security is needed in order to take precautions against system attacks that could harm certain parties. The use of SSH (secure shell) can minimize the risk of attack on the computer network. With encryption and decryption techniques that work automatically in the connection, SSH provides confidentiality and integrity of data across a network. Support of SSH port forwarding can be used to establish a secure communication tunnel to the web administrator to online exams. Support SSH port forwarding function proved to be able to secure the communication that occurs when accessing web administrator exams online, through dynamic port forwarding and local port forwarding in the local network.*

Keywords*: Network security, secure shell (SSH), Port forwading, Private network.*

Abstrak*: Keamanan jaringan menjadi kebutuhan penting bagi administrator dalam mengatur website. Salah satu contohnya adalah web ujian online. Keamanan dibutuhkan sebagai upaya untuk melakukan pencegahan terhadap penyerangan sistem yang dapat merugikan pihak tertentu. Penggunaan SSH (secure shell) dapat meminimalisir resiko terjadinya serangan di dalam jaringan komputer. Dengan teknik enkripsi dan dekripsi yang bekerja secara otomatis di dalam koneksinya, SSH menyediakan kerahasiaan dan integritas data di dalam jaringan. Dukungan port forwarding dari SSH dapat dimanfaatkan untuk membentuk sebuah tunnel yang dapat mengamankan komunikasi administrator ke dalam web ujian online. Dukungan SSH terhadap fungsi port forwarding terbukti dapat mengamankan komunikasi yang terjadi saat*

ISSN: 2355-3421, 75 - 84

administrator mengakses web ujian online, melaui dynamic port forwarding maupun local port forwarding di dalam jaringan lokal (private network).

***Kata kunci**: Keamanan jaringan, SSH, Port forwading, Private network.*

1. Pendahuluan

SSH (*secure shell*) adalah protokol jaringan yang berada di lapisan aplikasi pada protokol TCP/IP, memfasilitasi sistem komunikasi yang aman diantara dua sistem yang menggunakan arsitektur klien server dengan menyediakan kerahasiaan dan integritas data melalui teknik enkripsi dan dekripsi yang dilakukan secara otomatis didalam koneksinya, untuk menggunakan SSH dibutuhkan otentifikasi user berupa kunci umum dan password yang terenkripsi.

SSH digunakan untuk mengendalikan komputer jarak jauh (*remote*), mengirim file, membuat terowongan yang terenkripsi (*tunneling/port forwarding*) dan lain-lain. Port forwarding menyediakan kemampuan untuk mengkonversi koneksi TCP tidak aman ke koneksi SSH aman untuk pengalihan koneksi dari suatu IP ke IP lain sehingga seolah-olah klien menghubungi IP tujuan secara langsung, port forwarding melalui SSH akan membentuk sambungan yang aman antara komputer lokal dengan komputer remote melalui layanan yang disampaikan.

Pada penelitian ini akan dibuat sebuah server SSH sebagai *gateway* menggunakan aplikasi Open SSH, yang dapat melewatkan komunikasi administrator ke web ujian online melalui sambungan yang aman dengan menggunakan fungsi port forwarding, diterapkan pada jaringan lokal BINA INSANI. Dengan menggunakan password untuk mengotentikasi administrator/klien SSH ke dalam SSH server.

Permasalahan dalam penelitian ini yaitu:

1. Bagaimana administrator web ujian online dapat mengakses langsung ke localhost website secara remote (local port forwarding).
2. Bagaimana mencegah SSH dari serangan oleh pihak lain di dalam jaringan local.

Keamanan Jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut “penyusup” untuk mengakses setiap bagian dari sistem jaringan komputer.Tujuan dari Keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan dari ancaman berupa serangan secara langsung ataupun tidak langsung sehingga mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

Terdapat 2 serangan keamanan yaitu serangan pasif dan serangan aktif. Serangan pasif mencoba mempelajari atau memanfaatkan informasi dari sistem tapi tidak mempengaruhi sumberdaya sistem sedangkan serangan aktif berusaha mengubah sumber daya sistem atau mempengaruhi kegiatan system.

Terdapat 2 hal yang dapat mengamankan lalu lintas dalam sebuah jaringan komputer,

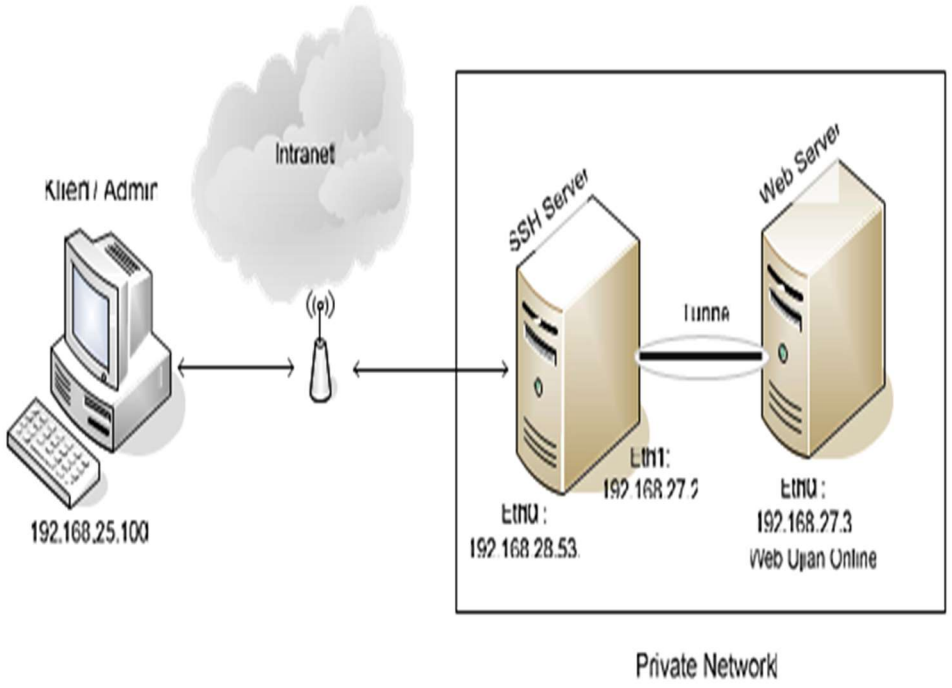
yaitu otentikasi dan enkripsi.

2. Metode Penelitian

Meliputi instalasi aplikasi, konfigurasi, pembuatan identifikasi untuk klien/user, dan konfigurasi jaringan antara SSH server dan web server. Tahapan selanjutnya adalah klien akan mencoba me-remote SSH server setelah SSH berhasil di-remote, klien mengubah pengaturan pada web browser untuk melakukan port forwarding, dan klien SSH dapat mengakses web untuk melakukan pengaturan web ujian online. Setelah semuanya selesai, klien keluar dari SSH dengan melakukan logout.Sementara proses tersebut berlangsung, proses dipantau dan dimonitor dengan aplikasi manajemen jaringan yang dapat menampilkan keterangan saat lalu lintas jaringan berlangsung, sehingga dapat dilihat apakah keterangan tersebut dapat dibaca dengan mudah dan menjadikan SSH tidak aman, atau sulit, jika tidak berhasil maka akan di lakukan koreksi terhadap konfigurasi SSH, identifikasi saat pendaftaran user, dan konfigurasi jaringan.

3. Hasil dan Analisis

Topologi pada gambar 1 menggambarkan klien dengan IP address 192.168.25.100 me-remote SSH pada IP address 192.168.28.53 melalui jaringan, SSH yang digunakan klien sebagai sistem keamanan untuk komunikasi dalam jaringan sebelum mengakses web ujian online pada IP address 192.168.27.3.



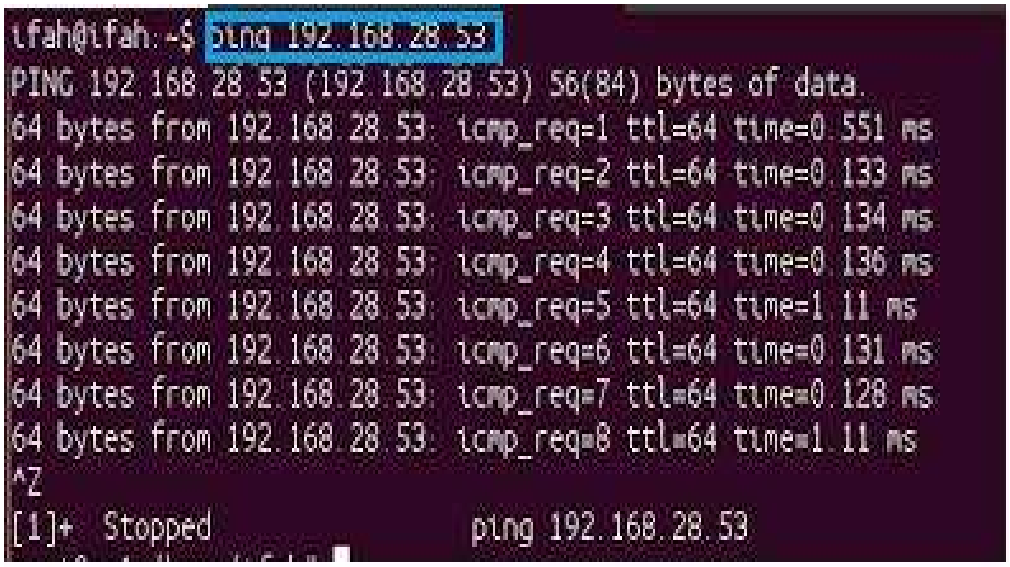
Gambar 1. Topologi Sistem Keamanan SSH

ISSN: 2355-3421, 75 - 84

SSH menyediakan proteksi terhadap komunikasi dalam jaringan dengan membentuk sebuah tunnel atau terowongan yang berfungsi untuk menjaga keamanan data yang mengalir dalam jaringan. Sehingga ketika klien mengakses web ujian online maka klien tidak mengakses secara langsung web ujian online, tetapi melalui tunnel yang telah terbentuk saat klien pertama kali melakukan akses login ke SSH, dengan demikian aktivitas klien dalam jaringan akan terenkripsi oleh SSH selama klien tetap tehubung dengan SSH server.

Dengan konfigurasi secara default, SSH sudah dapat digunakan. Namun untuk menambah keamanan SSH server dan mengoptimalkan penggunaannya, konfigurasi tersebut dapat diubah sesuai dengan kebutuhan SSH server.

Pengujian dimulai dengan melakuan test koneksi ke SSH server, yaitu dengan melakukan ping ke alamat IP SSH server yaitu 192.168.28.53 melalui PC klien, pengujian dilakukan seperti pada gambar 2.



Gambar 2. Ping SSH Server

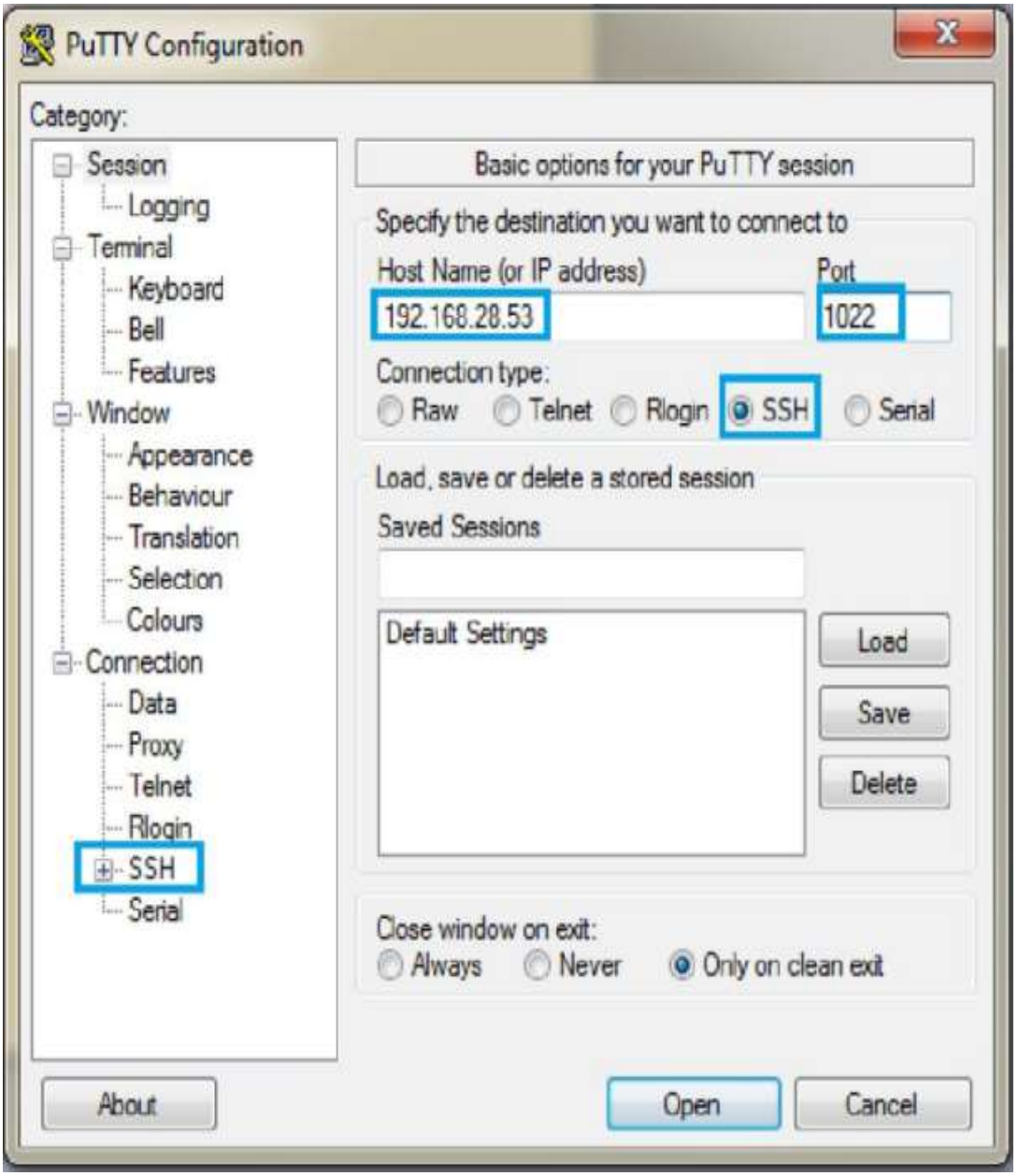
Dari gambar 2. terlihat bahwa test koneksi yang dilakukan dari PC klien dengan alamat IP 192.168.25.100 ke alamat IP SSH server yaitu 192.168.28.53 berhasil dilakukan hal ini terlihat dari replay yang terjadi dari hasil test koneksi PING yang dilakukan klien.

Untuk dapat me-remote SSH server pada klien windows gunakan aplikasi putty, klik 2 kali aplikasi putty, pilih Connection type SSH masukan alamat IP SSH server beserta port SSH, dan klik Open masukan username dan password dari akun aktif anda untuk dapat terkoneksi dengan ssh server, pastikan bahwa username dan password yang anda gunakan benar.

3.1. Akses Web Ujian Online dengan DPF (*dynamic port forwarding*)

Klien akan mencoba mengakses web ujian online melalui SSH yang mendukung fungsi Dinamic Port Forwarding. Dalam melakukan dynamic port forwarding dibutuhkan SOCKS dan

port. SOCKS merupakan protokol kecil yang dijadikan sebagai proxy untuk transmisi data melalui jaringan dan port yang dibentuk ketika melakukan login ke remote SSH server, keduanya diatur pada setiap web browser yang akan gunakan.



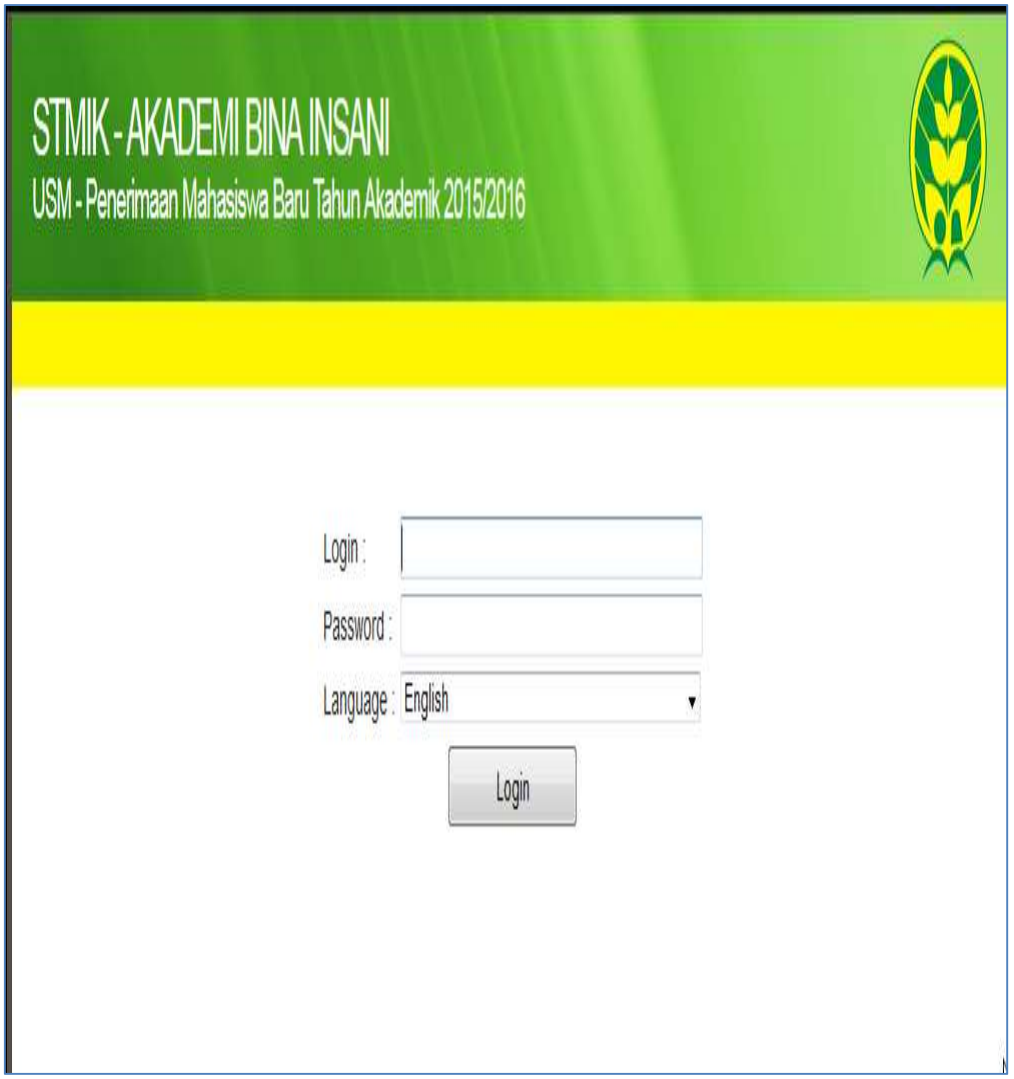
Gambar 3. Konfigurasi Putty untuk Remote SSH

Buka aplikasi putty dengan klik 2 kali, maka akan muncul tampilan seperti gambar 4.3. Pilih Connection type SSH, masukan IP SSH server beserta port SSH Kemudian klik SSH pada Category di sebelah kiri dan pilih Tunnels, pilih Dynamic dan masukan source port 2000 setelah itu klik Add maka akan muncul D2000, lalu tekan Open.

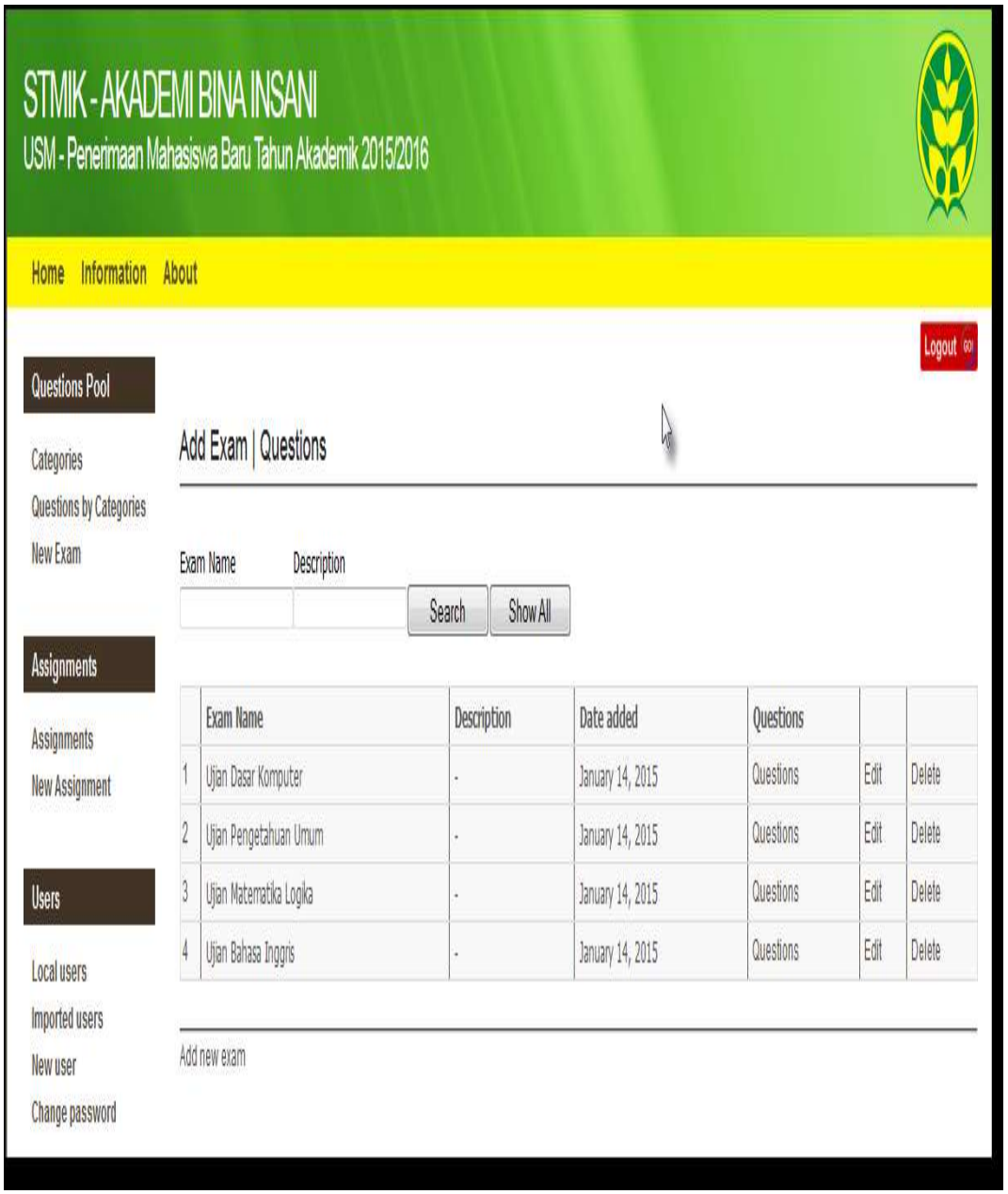
ISSN: 2355-3421, 75 - 84

Setelah tekan Open maka akan muncul tampilan, gunakan username dan password, untuk dapat terhubung dengan SSH server. Kemudian buka terminal dengan klik tombol start lalu ketik cmd, gunakan perintah netstat –a lalu tekan enter untuk mengetahui apakah port 2000 telah terbentuk. Jika port 2000 telah terbentuk, gunakan IP lokal 127.0.0.1 dan port 2000 yang telah terbentuk untuk dijadikan sebagai proxy. Dengan cara buka browser pada PC klien windows, jika menggunakan Mozilla sebagai web browser pilih Tools >> Options, kemudian pilih Advanced >> Network >> Settings maka akan muncul jendela Connections Settings, pilih Manual proxy configuration, masukan IP lokal 127.0.0.1 pada bagian SOCKS dan port 2000 pada bagian port dan klik Ok.

Konfigurasi berfungsi untuk membentuk tunnel atau terowongan yang akan mengamankan lalu lintas jaringan SSH klien dari pihak lain selama terhubung dengan SSH server. Selanjutnya pada web browser yang sudah di-setting, masukan alamat http://192.168.27.3 maka akan muncul gambar 4. yang merupakan tampilan awal web ujian online.



Gambar 4. Tampilan Web Ujian Online



Gambar 5. Tampilan menu ujian

3.2. Analisis Keamanan DPF (*Dynamic Port Forwarding*)

Analisis ini dilakukan untuk membuktikan apakah DPF benar dapat mengamankan komunikasi klien dengan web ujian online, dengan memonitor saat akses berlangsung menggunakan aplikasi wireshark. Diasumsikan proses monitor telah dilakukan, keamanan dari penggunaan DPF ssh, yaitu klien dialihkan terlebih dahulu ke ssh kemudian saat klien mengakses web ujian online maka klien tidak secara langsung terhubung dengan web ujian online tapi melalui ssh server. Terlihat pada hasil monitoring IP asal adalah 192.168.25.100 dan IP tujuan adalah 192.168.28.53. Protokol yang digunakan adalah protokol TCP, dari hasil

ISSN: 2355-3421, 75 - 84

monitoring juga tidak memperlihatkan adanya informasi berupa username dan password, semua informasi yang mengalir di jaringan akan langsung dienkripsi ssh secara transparan.

3.3. Akses Localhost Web ujian online dengan LPF (*local port forwarding*)

Klien akan mencoba mengakses web ujian online melalui SSH yang mendukung fungsi local port forwarding. Pada *local port forwarding* SSH dikonfigurasi untuk listen pada port yang dipilih. SSH membawa semua lalu lintas menggunakan port yang dipilih dan mengirimkannya melalui sebuah terowongan SSH. Buka aplikasi putty dengan klik 2 kali, maka akan muncul tampilan. Pilih Connection type SSH, masukan IP SSH server beserta port SSH Kemudian klik SSH pada Category di sebelah kiri dan pilih Tunnels maka akan tampil menu, pilih Local masukan Source port 8000 dan masukan Destination 192.168.27.3:80 setelah itu klik Add maka akan muncul L8000 192.168.27.3:80, lalu tekan Open, Maka akan muncul tampilan menu, gunakan username dan password untuk dapat terhubung dengan SSH server.

Kemudian buka terminal dengan klik tombol start lalu ketik cmd, gunakan perintah netstat –a lalu tekan enter untuk mengetahui apakah port 8000 telah terbuka. Untuk dapat mengunakan port tersebut lakukan dengan cara buka web browser, masukan alamat http://localhost:8000 lokasi hosting web ujian online.

3.4. Analisis Keamanan LPF (*Local Port Forwarding*)

Analisis ini dilakukan untuk membuktikan apakah LPF benar dapat mengamankan komunikasi klien dengan web ujian online melalui lokal, dengan memonitor saat akses berlangsung menggunakan aplikasi wireshark. Diasumsikan proses monitor telah dilakukan. memperlihatkan keamanan penggunaan LPF dengan ssh, yaitu klien dialihkan terlebih dahulu ke ssh kemudian saat klien mengakses web server (lokasi hosting web ujian online) maka klien tidak secara langsung terhubung dengan web ujian online tapi melalui ssh server. Terlihat pada hasil monitoring IP asal adalah 192.168.25.100 dan IP tujuan adalah 192.168.28.53. Protokol yang digunakan adalah protocol TCP. Akses langsung ke web server (lokasi hosting web ujian online) tidak dapat dilakukan, bila dilakukan maka kita akan mendapat pesan error.

3.5. Pengujian Keamanan SSH

Pengujian ini dilakukan dengan membandingkan protokol telnet dengan ssh, keduanya adalah protokol yang digunakan untuk remote login. Diasumsikan proses monitoring telah dilakukan dengan menghasilkan analisis, bahwa ssh menggunakan enkripsi saat melakukan remote sehingga informasi berupa username dan password tidak dapat terlihat, berbeda dengan telnet, pada telnet tidak digunakan enkripsi saat melakukan remote sehingga mudah bagi pihak lain untuk mengetahui informasi berupa username dan password hal ini memperlihatkan keamanan ssh dengan telnet yang merupakan protocol untuk remote login.

3.6. Pengujian Serangan

Pengujian ini dilakukan dengan brute force ke ssh server, brute force adalah serangan langsung ke dalam sistem komputer dengan menggunakan kombinasi password berupa angka, huruf maupun simbol secara acak, sehingga memungkinkan dari kombinasi password tersebut ada, password yang dapat digunakan untuk menembus sistem komputer.

Pengujian ini dilakukan oleh penyerang dengan sistem operasi backtrack dan aplikasi ncrack, diasumsikan bahwa penyerang telah mengetahui IP ssh server, port ssh dan ip pada jaringan diizinkan untuk mengakses ssh. Pengujian ini dilakukan dengan mencoba sejumlah password untuk masuk ke dalam ssh server. Hal ini terjadi karena password yang digunakan client1 tidak mudah untuk ditebak, penggunaan password yang kuat, unik dan sulit ditebak dapat menghindari pengguna dari serangan brute force tersebut. Kemudian setelah mengetahui adanya percobaan penyerangan yang dilakukan pihak lain dan tercatat didalam log SSH, kita dapat memblock IP dari jaringan mana yang melakukan penyerangan. Sehingga IP tersebut tidak lagi diizinkan untuk mencoba mengakses SSH, hal ini dilakukan untuk meningkatkan keamanan SSH.

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, penggunaan SSH sebagai sistem komunikasi aman ke dalam web ujian online berbasis private network maka diperoleh beberapa hal yaitu:

1. Dengan menggunakan fungsi SSH dynamic port forwarding, kita dapat mencegah pihak lain untuk mengetahui username dan password yang digunakan administrator saat mengakses web ujian online di dalam jaringan local, namun bila tanpa menggunakan fungsi SSH dynamic port forwarding, maka username dan password akan terlihat oleh pihak lain ketika pihak tersebut menggunakan aplikasi wireshark untuk menganalisa jaringan local yang administrator gunakan.
2. Dengan menggunakan fungsi SSH local port forwarding, administrator web ujian online dapat mengakses langsung localhot website secara remote, namun bila tanpa menggunakan fungsi SSH local port forwarding, maka administrator tidak dapat mengakses langsung localhost website.
3. SSH terbukti lebih aman bila dibandingkan dengan protokol sejenisnya yaitu telnet yang keduanya merupakan protokol aplikasi untuk melakukan remote. Hal ini disebabkan karena SSH menggunakan teknik enkripsi dan dekripsi sedangkan telnet tidak menggunakan teknik enkripsi dan dekripsi sehingga kode atau
4. Command yang dituliskan dapat terbaca dengan jelas tanpa adanya enkripsi.
5. Dengan mengoptimalkan konfigurasi SSHd_Config pada SSH server, menutup kemungkinan serangan dengan membatasi hak akses, dan melakukan maintenance pada SSH server secara berkala kita dapat mencegah dan menghindari SSH dari serangan

ISSN: 2355-3421, 75 - 84

khususnya serangan brute force.

Dari penelitian ini, untuk pengembangan sistem komunikasi keamanan dengan SSH berbasis private network, yaitu :

Penggunaan username dan password dapat dirubah menjadi public dan private key atau karberos untuk menambah keamanan penggunanya.

Referensi

[1] Albaab, Andi Zainul. Sistem Pengatur Keamanan Mikrotik dengan SSH berbasis website. Yogyakarta : UIN Sunan Kalijaga. 2012.

[2] Baret, Daniel J, dkk. SSH The Secure Shell The Definite Guide 2nd Edition, O'Reilly Media, California. 2005.

[3] Cahyani, Ika Dwi. Sistem Keamanan Enkripsi Secure Shell (SSH) untuk Keamanan Data. Semarang : Universitas Pandanaran. 2010.

[4] Rahardjo, Budi. Keamanan Sistem Informasi Berbasis Intranet, PT.Instan Informatika, Bandung. 2002.

[5] Ramadhan, Karunia. Studi Keamanan pada Protokol SSH.Bandung: ITB. 2011.

[6] Starlings, William. Cryptography and Network Security. Prentice Hall. New York. 2006.

[7] Hidayat, Syarif & Agung Priyamanto. Manajemen Jaringan Menggunakan Remote Server Administrator, Yogyakarta : Universitas Islam Indonesia. 2006.

[8] Tung, Khoe Yao.Teknologi Jaringan Intranet, Andi, Yogyakarta. 2001.