

---

## PENGONTROLAN KEAMANAN SISTEM KOMPUTER CLIENT DARI SERANGAN HACKER DAN VIRUS KOMPUTER SECARA JARAK JAUH (*REMOTE SERVER*) DENGAN MENGGUNAKAN SSH

Jamaluddin, Rimbun Siringoringo, El Rahmat Jaya Hulu<sup>✉</sup>

Universitas Methodist Indonesia, Medan, Indonesia

Email: [elrahmathulu28@gmail.com](mailto:elrahmathulu28@gmail.com)

DOI: <https://doi.org/10.46880/jmika.Vol7No1.pp123-127>

### ABSTRACT

*Computer system security is very important to be considered by computer users to protect their computers from attacks such as hackers and computer viruses that can take data and damage the user's computer system. Hacker is a person or party who has the skill in breaking through and sneaking to access a computer without the user's permission and can take data and even damage the system on the user's computer. And a Computer Virus is a computer program that copies and inserts copies into the program and can damage the computer system. So that by using SSH (Secure Shell) can control and check computer security from hacker attacks and computer viruses without having to come to the location where there is a client computer or done remotely (Remote Server).*

**Keywords:** *Security, Hackers, Virus, Secure Shell, Remote Server.*

### ABSTRAK

*Keamanan sistem komputer sangat penting diperhatikan oleh pengguna komputer untuk melindungi komputernya dari serangan seperti hacker dan adanya virus komputer yang dapat mengambil data serta merusak sistem komputer si pengguna. Hacker adalah seseorang atau pihak yang memiliki keahlian dalam menerobos dan menyelipkan untuk mengakses komputer tanpa seizin pengguna dan dapat mengambil data bahkan merusak sistem pada komputer si pengguna. Dan Virus Komputer merupakan program komputer yang melakukan penyalinan dan menyisipkan salinan ke dalam program tersebut dan dapat merusak sistem komputer. Sehingga dengan menggunakan SSH (Secure Shell) dapat melakukan pengontrolan dan melakukan pengecekan keamanan komputer dari serangan hacker dan virus komputer tanpa harus datang ke lokasi tempat adanya komputer client atau dilakukan secara jarak jauh (Remote Server).*

**Kata Kunci:** *Keamanan, Hecker, Virus, Secure Shell, Remote Server.*

---

### PENDAHULUAN

Dengan perkembangan zaman era digital saat ini semakin banyak teknologi berkembang serta banyak pihak yang ahli untuk memanfaatkan teknologi tersebut dalam hal mengganggu kenyamanan pengguna komputer khususnya keamanan sistem komputer dan server yang selalu terhubung dalam jaringan ataupun internet yang akan menjadi sasaran pihak atau orang yang tidak bertanggung jawab untuk mengganggu data bahkan melakukan peretasan sistem dari komputer pengguna (Farizy & Eriana, 2022).

Virus komputer juga dapat mengganggu kenyamanan dan keamanan sistem komputer si pengguna karena dapat merusak sistem perangkat komputer dengan cara melakukan penyalinan dan menyisipkan salinan ke dalam program komputer. Untuk mengatasi hal tersebut harus dibutuhkan keamanan sistem komputer. Karena, keamanan sistem komputer dapat diartikan sebagai cara dan upaya untuk

mencegah dan mengamankan sistem komputer dari ancaman serangan hacker dan virus komputer tersebut (Stiawan, 2005).

Seseorang yang mempunyai perangkat komputer lebih dari satu, sangat bagus untuk menggunakan SSH (Secure Shell). Karena dengan menggunakan SSH pengguna dapat mengontrol keamanan sistem komputernya secara jarak jauh (Remote Server) tanpa harus datang ke lokasi adanya komputer client yang akan dikontrol (Jubilee Enterprise, 2013).

### LANDASAN TEORI

#### Keamanan Sistem Komputer

Keamanan sistem komputer dapat didefinisikan sebagai cara dan upaya yang dilakukan untuk mencegah dan mengamankan sistem komputer dari segala ancaman dan serangan yang dapat mengganggu kinerja sistem komputer (Russell & Gangemi, 1991).

Jadi, dalam hal ini keamanan sistem komputer sangat penting di terapkan pengguna di dalam sistem perangkat komputernya agar sistem komputernya dapat terlindungi dan tetap aman.

Yang harus dilakukan untuk mencegah dan mengamankan sistem komputer adalah (Stiawan, 2005):

1. Membuat dan penggunaan Password yang sulit,
2. memastikan data terenkripsi,
3. Memasang program Anti Virus untuk melindungi sistem komputer,
4. Perlu berhati-hati saat menggunakan jaringan Wifi atau jangan asal tersambung di dalam jaringan Wifi,
5. Jangan asal mengklik link yang dibagikan, karena link itu bisa saja digunakan Hacker untuk melakukan peretasan.

### SSH (Secure Shell)

SSH merupakan protokol transfer yang penguanya memungkinkan untuk mengontrol perangkat lain dengan cara remote atau mengontrol secara jarak jauh dan terkoneksi didalam jaringan atau internet. Di dalam SSH melibatkan 2 atau lebih komputer, yang mana satu komputer dijadikan sebagai komputer server dan komputer lainnya dijadikan sebagai komputer client. disini komputer server dan komputer client harus saling terhubung di dalam satu jaringan yang sama, dalam hal ini komputer server dapat mengendalikan bahkan mengontrol keamanan sistem komputer client secara jarak jauh (Ylonen & Lonvick, 2006).

### Hacker (Peretas)

Hacker adalah seseorang atau pihak yang memiliki keahlian di bidang komputer dan jaringan yang mampu menerobos dan menyelip untuk mengakses komputer tanpa seizin pengguna dan dapat mengambil data bahkan melakukan peretasan merusak sistem pada komputer si pengguna (Stiawan, 2005).

### Virus

Virus Komputer merupakan program komputer yang melakukan penyalinan dan menyisipkan salinan ke dalam program tersebut dan dapat merusak sistem komputer (Pamungkas, 2018).

Jenis-jenis virus komputer yang perlu diwaspadai dan bisa merusak sistem komputer diantaranya Worm, Trojan, Backdoor, Spyware, Rogue, Rookit, Multipartite Virus, Memory Resident Virus, FAT Virus, Directory Virus, Companion Virus dan jenis virus lainnya (Pamungkas, 2018).

## METODE PENELITIAN

### Pengumpulan Data

Pengumpulan data dilakukan dengan mencari bahan dari jurnal yang sudah publish dan dari situs web yang mendukung dan mengembangkan judul jurnal ini.

### Desain Sistem

Didalam desain sistem ada berupa gambar topologi jaringan yang menghubungkan komputer server dan komputer client. Sehingga, komputer server dapat mengontrol keamanan dari komputer client secara jarak jauh (Remote Server) dari serangan hacker serta adanya virus komputer pada sistem komputer client.

### Mengimplementasikan Sistem

Sistem yang telah didesain kemudian diimplementasikan dengan membuat pengujian SSH (Secure Shell) didalam sistem komputer agar komputer server dapat mengontrol sistem komputer client secara jarak jauh (Remote Server) dari serangan hacker dan adanya virus komputer pada sistem komputer client.

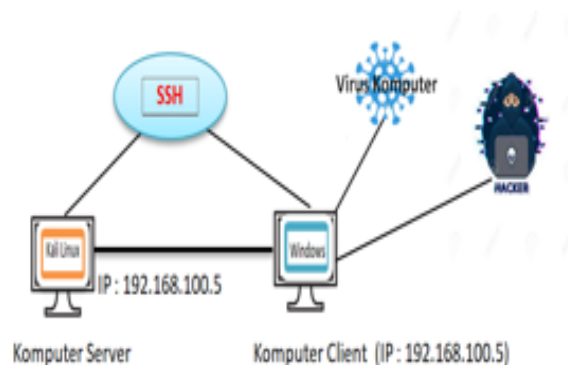
### Menguji Sistem

Mengecek keberhasilan SSH dalam menghubungkan komputer server dan komputer client secara jarak jauh (Remote Server).

## HASIL DAN PEMBAHASAN

### Desain Sistem

Desain sistem berupa topologi jaringan seperti yang ada di gambar 1. Pada gambar tersebut terlihat komputer server dan komputer client yang saling terhubung. Untuk menghubungkan komputer server dan komputer client diperlukan IP dari komputer client untuk dimasukkan ke komputer server dan diatur didalam SSH agar komputer server dapat mengontrol keamanan sistem komputer client secara jarak jauh (Remote Server) dari serangan hacker dan adanya virus komputer pada sistem komputer client.



Sumber: (Pratama, Orisa, & Ariwibisono, 2020)

**Gambar 1.** Topologi Jaringan Menggunakan SSH

Desain sistem berupa teknologi yang dipakai pada sistem komputer server dan komputer client adalah seperti pada tabel berikut.

**Tabel 1.** Teknologi Sistem

Komputer Server	Kali Linux
Komputer Client	Windows 10

**Implementasi dan Pengujian Sistem**

Untuk implementasi sistem dilakukan di dalam sistem operasi utama dan juga menggunakan virtual box. Virtual Box adalah perangkat lunak virtualisasi yang digunakan untuk menginstal dan mengeksekusi sistem operasi di dalam sistem operasi utama. Untuk tahap implementasi sistem maka sistem operasi kali linux diinstal di dalam virtual box sedangkan sistem operasi windows tetap di sistem operasi utama.

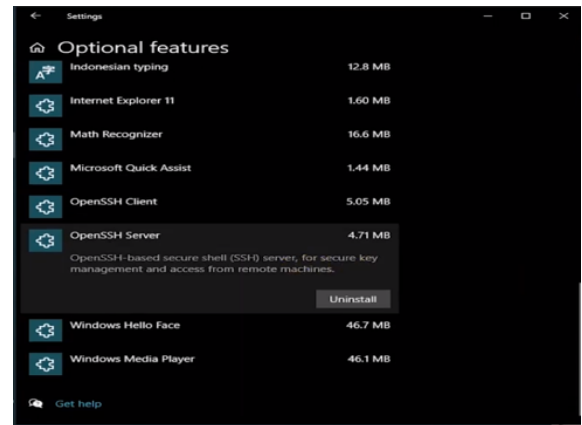
Selanjutnya melakukan pengujian sistem dengan menggunakan SSH (Secure Shell) untuk mengontrol secara jarak jauh (Remote Server) dapat dilakukan dengan mengaktifkan Firewall pada windows sebagai komputer client sedangkan di Kali Linux Firewall di nonaktifkan.

Selanjutnya meginstall open SSH Server dengan melakukannya pada menu settings seperti yang ditunjukkan pada gambar berikut:



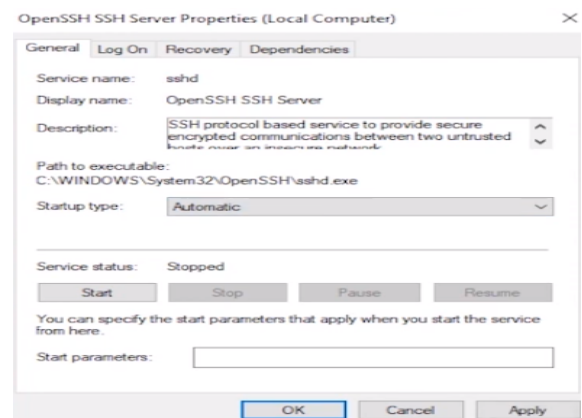
**Gambar 2.** Tampilan Menu Setting

Setelah berhasil menginstall OpenSSH Server maka muncul tampilan seperti gambar berikut:



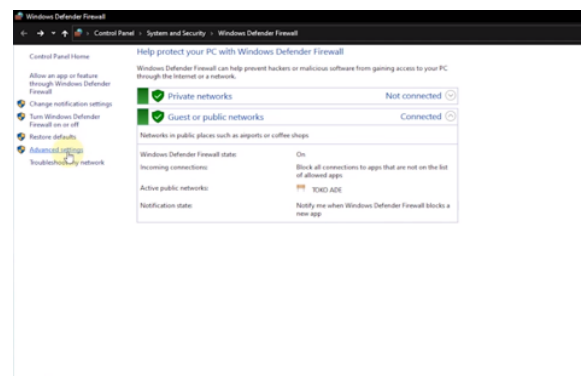
**Gambar 3.** Tampilan Menu Open Features

Selanjutnya masuk ke menu services dan pilih OpenSSH Server, maka muncul tampilan seperti di bawah ini, pilih Automatic, setelah itu klik Start, lalu pilih OK seperti ditampilkan pada gambar berikut:



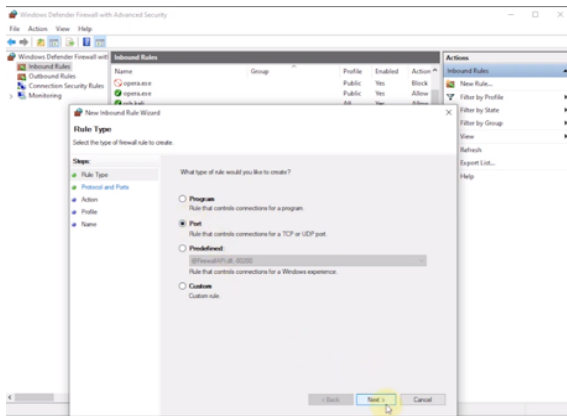
**Gambar 4.** Setting Open SSH

Selanjutnya masuk ke Windows Defender Firewall, lalu pilih Advanced settings



**Gambar 5.** Advanced Setting Windows Defender Firewall

Selanjutnya pilih Inbound Rules, lalu pilih New Rule, kemudian pilih Port lalu klik Next

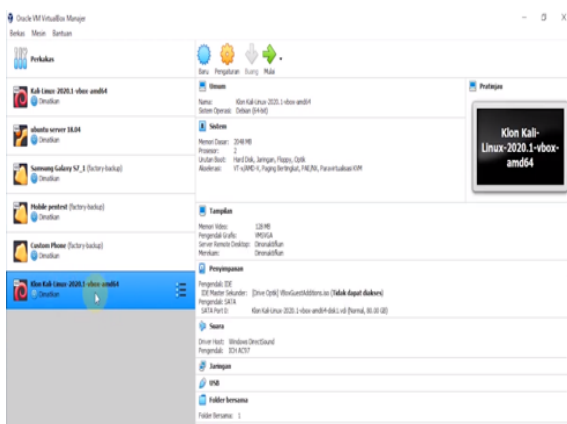


Gambar 6. Tampilan Inbound Rules dan memilih Port

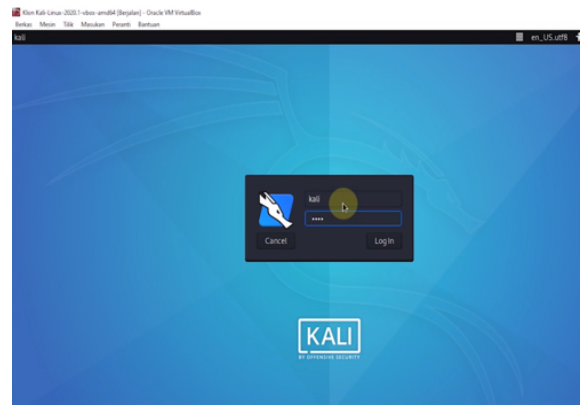
Setelah itu muncul tampilan seperti ini, pilih TCP dan pilih Specific local ports dengan ports 22, Selanjutnya setting SSH Port dan digunakan untuk keamanan ketika menggunakan SSH karena cuman pengguna komputer itu yang tau berapa IP dan berapa Port pada komputernya Selanjutnya berikan username dan password pada komputeryang akan direote seperti ditunjukkan gambar berikut:



Gambar 7. Pemberian Username dan pssword pada Komputer Client

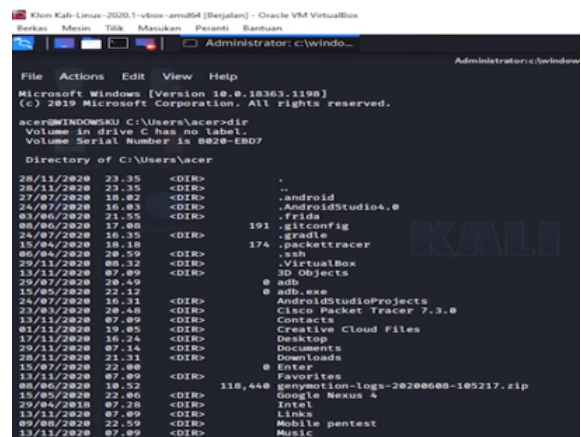


Gambar 8. Tampilan Virtual Box dan Kali Linux



Gambar 9. Pengaksesan Kali Linux pada Virtual Box

Local disk C yang ada di Komputer Client (Sistem Operasi Windows) sudah ada di dalam Sistem Komputer Server (Sistem Operasi Kali Linux). Untuk mengetesnya input perintah dir, maka muncul file atau data-data dari Komputer Client di dalam sistem Komputer Server. Selanjutnya Komputer Server bisa mengontrol dan mengendalikan sistem Komputer Client.



Gambar 10. Tampilan Mengontrol Komputer Client

Dengan berhasilnya pengujian sistem dengan menggunakan SSH ini komputer server dapat mengontrol atau mengendalikan keamanan sistem komputer client dan mengetahui jika ada serangan Hacker dan adanya virus komputer pada sistem komputer client menggunakan SSH secara jarak jauh (Remote Server).

## KESIMPULAN

Dari pemaparan secara keseluruhan maka dapat diambil beberapa kesimpulan, yakni keamanan pada sistem komputer harus perlu di perhatikan si pengguna komputer agar data dan sistem komputernya tetap aman dari serangan Hacker dan Virus Komputer, terutama pada pengguna komputer yang memiliki lebih dari satu

perangkat komputer, sangat bagus menggunakan SSH agar dapat mengontrol atau mengendalikan keamanan sistem komputernya.

SSH (Secure Shell) merupakan protokol transfer yang memungkinkan penguanya untuk mengontrol perangkat lain dengan cara remote atau mengontrol secara jarak jauh dan terkoneksi di dalam jaringan atau internet.

#### **DAFTAR PUSTAKA**

- Farizy, S., & Eriana, E. S. (2022). *Keamanan Sistem Informasi*. Pamulang: Unpam Press.
- Jubilee Enterprise. (2013). *Teknik Mengendalikan PC dari Jarak Jauh*. Jakarta: Elex Media Komputindo.
- Pamungkas, P. D. A. (2018). Analisis Cara Kerja Sistem Infeksi Virus Komputer. *Bina Insani ICT Journal*, 1(1), 15–40.
- Pratama, R., Orisa, M., & Ariwibisono, F. X. (2020). Aplikasi monitoring dan controlling server menggunakan protocol icmp (internet control message protocol) dan ssh (secure shell) berbasis website. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 4(1), 397–403.
- Russell, D., & Gangemi, G. T. (1991). *Computer Security Basics*. California: O'Reilly Media, Inc.
- Stiawan, D. (2005). *Sistem Keamanan Komputer*. Jakarta: Elex Media Komputindo.
- Ylonen, T., & Lonvick, C. (2006). *The secure shell (SSH) protocol architecture*.