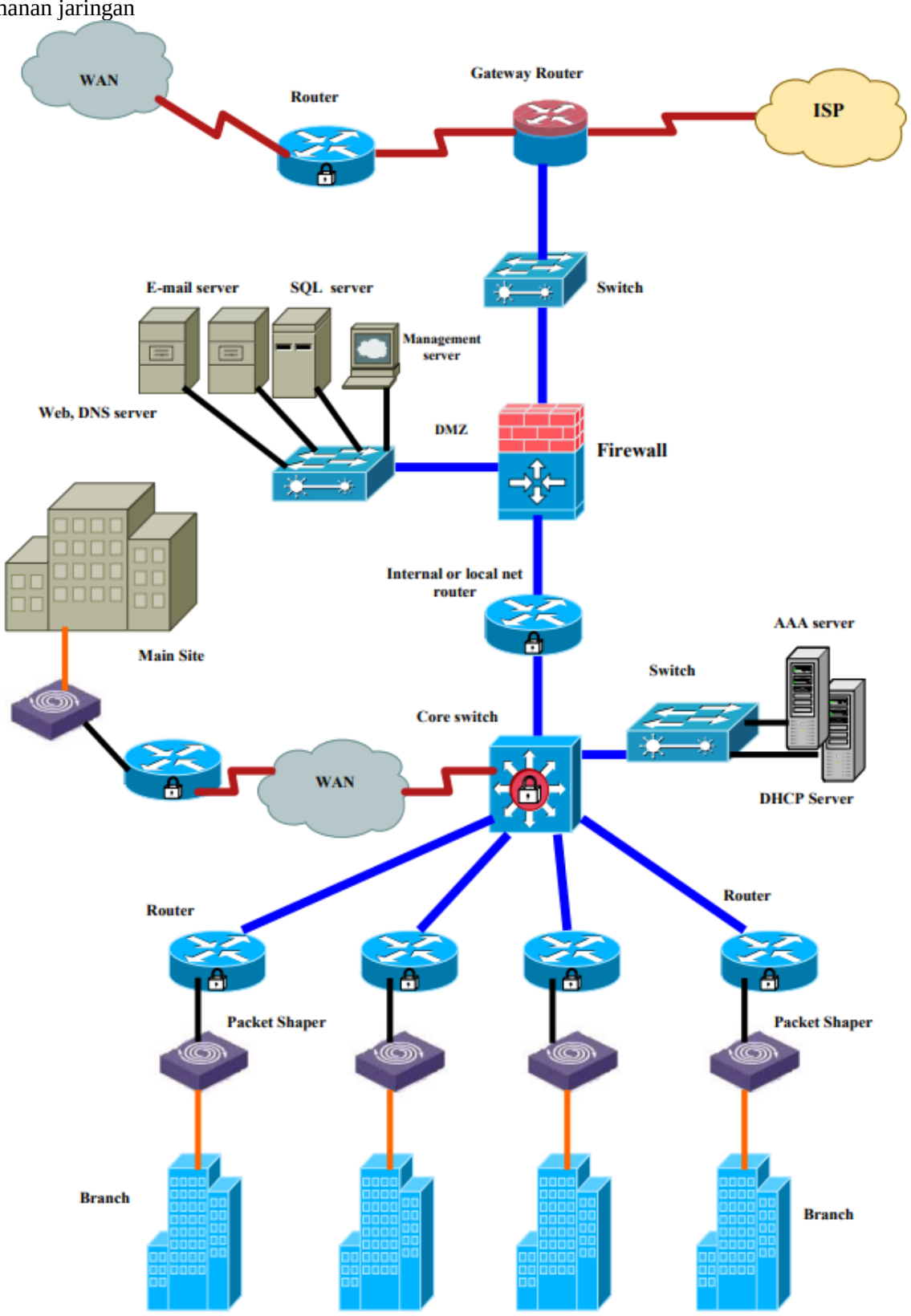
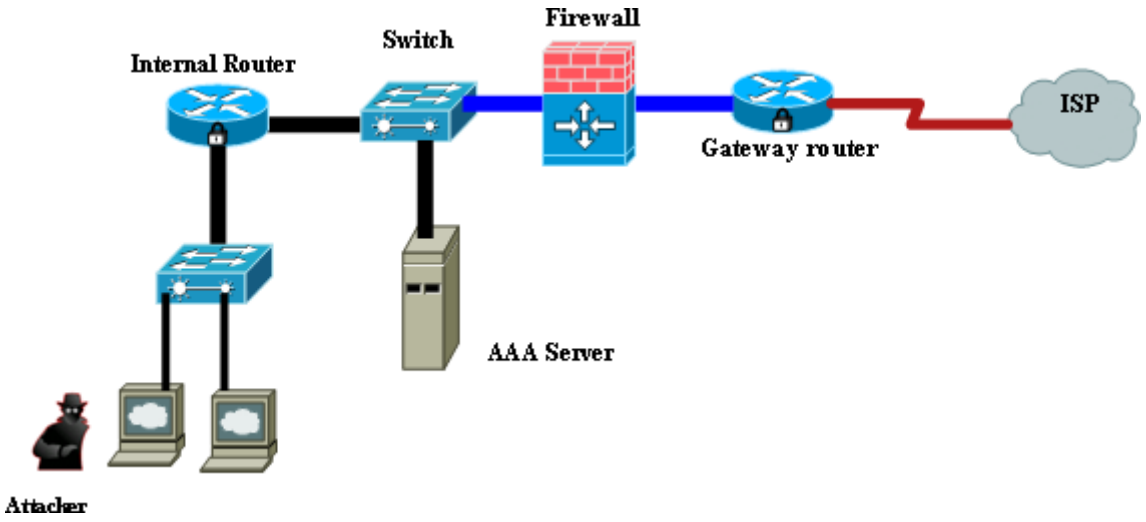
A.) Desain keamanan jaringan



Gambar 1. Struktur model keamanan jaringan



Gambar 2. Router dengan konfigurasi firewall untuk test bed jaringan

Router melakukan banyak pekerjaan berbeda di jaringan modern, meneruskan lalu lintas antara dua atau lebih jaringan lokal dalam rute organisasi atau perusahaan. Router interior mungkin memberlakukan beberapa batasan pada lalu lintas yang mereka teruskan antar jaringan. Meneruskan lalu lintas antara perusahaan yang berbeda (kadang-kadang disebut 'sistem otonom' yang berbeda). Lalu lintas antara jaringan berbeda yang membentuk Internet diarahkan oleh router tulang punggung.

Tingkat kepercayaan antara jaringan yang terhubung oleh router backbone biasanya sangat rendah. Biasanya, router backbone dirancang dan dikonfigurasi untuk meneruskan lalu lintas secepat mungkin, tanpa memaksakan batasan apa pun padanya. Tujuan keamanan utama untuk router backbone adalah untuk memastikan bahwa manajemen dan operasi router dilakukan hanya oleh pihak yang berwenang, dan untuk melindungi integritas informasi perutean yang digunakan untuk meneruskan lalu lintas. Router backbone biasanya menggunakan Exterior Gateway Protocols untuk mengelola rute [5].

Mengkonfigurasi router backbone adalah tugas yang sangat khusus. Router perbatasan meneruskan lalu lintas antara perusahaan dan jaringan luar. Aspek kunci dari router perbatasan adalah bahwa ia membentuk bagian dari batas antara jaringan internal yang terpercaya dari suatu perusahaan,

dan jaringan eksternal yang tidak tepercaya (misalnya Internet). Ini dapat membantu mengamankan perimeter jaringan perusahaan dengan memberlakukan pembatasan pada lalu lintas yang dikontrolnya. Router perbatasan dapat menggunakan protokol perutean, atau mungkin sepenuhnya bergantung pada rute statis.

Kebijakan keamanan adalah definisi fungsi keamanan terhadap intrusi jaringan. Mesin keamanan menyediakan fungsi keamanan penyaringan paket, otentikasi, kontrol akses, analisis intrusi dan jejak audit di wilayah kernel router [10, 12]. Router adalah komponen kunci dari Internet, dan bagian penting dari jaringan yang mengontrol aliran paket data dalam jaringan dan menentukan jalur yang optimal untuk mencapai tujuan, dan keamanannya merupakan bagian penting dari keamanan keseluruhan untuk jaringan yang mereka layani . Kesalahan router atau serangan terhadap router dapat merusak seluruh jaringan. Karena router terhubung ke setidaknya dua jaringan dan mengelola lalu lintas jaringan, keamanan diperlukan untuk mengontrol akses router yang tidak sah dan intrusi jaringan ilegal. Teknologi router aman memiliki fungsi keamanan, seperti deteksi intrusi, IPsec dan kontrol akses, diterapkan ke router lama untuk jaringan yang aman. Router mungkin bertanggung jawab untuk menyaring lalu lintas, memungkinkan beberapa paket melewati dan menolak yang lain [13]. Penyaringan bisa menjadi fungsi yang sangat penting dari router; memungkinkan mereka untuk membantu melindungi komputer dan komponen jaringan lainnya. Mungkin juga di ujung tujuan, router mungkin harus memecah paket besar untuk mengakomodasi batas ukuran LAN tujuan. Router modern tidak hanya melakukan fungsi relay, tetapi juga penyaringan, pemisahan, enkripsi dan pemantauan aliran data. Selain itu, mereka menyediakan berbagai antarmuka manajemen untuk konfigurasi, pemeliharaan (jarak jauh), dan pemantauan. Semua fungsi ini berpotensi mempengaruhi ketersediaan, integritas, dan kerahasiaan koneksi data, sehingga membuat router menjadi komponen jaringan yang sangat kritis terhadap keamanan. Namun, mengkonfigurasi router adalah tugas yang sulit dan rawan kesalahan.

Firewall dapat melindungi jaringan dari serangan eksternal dengan memeriksa semua paket pesan yang mencoba melewati jaringan dan menolak paket yang tidak memenuhi batasan keamanan. Namun, itu tidak melindungi data karena ditransmisikan dari satu jaringan ke jaringan lain. Data yang ditransmisikan dari satu jaringan ke jaringan lain melalui Internet rentan untuk diakses di banyak titik antara sumber dan tujuan. Secure socket layer (SSL) adalah salah satu sarana untuk menyediakan komunikasi yang aman antara titik-titik yang terhubung melalui Internet.

Router dan firewall mendukung sejumlah besar layanan jaringan pada lapisan 2, 3, 4, dan 7 [14]. Beberapa dari layanan ini adalah protokol lapisan aplikasi yang memungkinkan pengguna dan proses host untuk terhubung ke router, firewall, dan perangkat jaringan lainnya. Lainnya adalah proses dan pengaturan otomatis yang dimaksudkan untuk mendukung

warisan atau konfigurasi khusus, yang merugikan keamanan. Beberapa dari layanan ini dapat dibatasi atau dinonaktifkan untuk meningkatkan keamanan tanpa menurunkan penggunaan operasional router dan kinerja jaringan. Juga serangan dan peretas dapat memanfaatkan layanan ini untuk menemukan titik kelemahan dalam jaringan. Praktik keamanan umum untuk router dan firewall harus hanya mendukung lalu lintas dan protokol yang dibutuhkan jaringan. Contoh untuk layanan ini adalah:

1. CDP, Cisco Discovery Protocol adalah protokol berpemilik yang digunakan router Cisco untuk mengidentifikasi satu sama lain pada segmen LAN. Ini hanya berguna dalam situasi khusus, dan dianggap merusak keamanan.
2. Server Kecil TCP dan UDP, standar protokol TCP dan UDP menyertakan daftar layanan sederhana yang direkomendasikan yang harus disediakan oleh host. Dalam hampir semua kasus, router tidak perlu mendukung layanan ini, dan mereka harus dinonaktifkan.
3. Finger Server, server jari IOS mendukung protokol 'jari' Unix, yang digunakan untuk menanyakan host tentang pengguna yang masuk.
4. Server HTTP, sebagian besar router dan firewall mendukung administrasi jarak jauh berbasis web menggunakan protokol HTTP. Sementara fitur akses web cukup mendasar di sebagian besar router, mereka adalah mekanisme yang layak untuk memantau, mengonfigurasi, dan menyerang router. Jika administrasi jarak jauh berbasis web tidak diperlukan, maka itu harus dinonaktifkan seperti yang ditunjukkan di bawah ini. Administrasi jarak jauh berbasis web berguna terutama ketika mengintervensi router atau firewall yang mencegah penggunaan Telnet untuk tujuan itu. Namun, penting untuk dicatat bahwa baik Telnet dan administrasi jarak jauh berbasis web mengungkapkan kata sandi penting secara jelas. Oleh karena itu, administrasi jarak jauh berbasis web harus dihindari.
5. Bootp Server, Bootp adalah protokol datagram yang digunakan oleh beberapa host untuk memuat sistem operasi mereka melalui jaringan. Router Cisco mampu bertindak sebagai server bootp, terutama untuk perangkat keras Cisco lainnya. Fasilitas ini dimaksudkan untuk mendukung strategi penyebaran di mana satu router Cisco bertindak sebagai repositori pusat perangkat lunak IOS untuk kumpulan router tersebut. Dalam praktiknya, bootp sangat jarang digunakan, dan menawarkan penyerang kemampuan untuk mengunduh salinan perangkat lunak iOS router.
6. Configuration Auto-Loading, beberapa router seperti router Cisco dan router Linksys, mampu memuat konfigurasi startup mereka dari memori lokal atau dari jaringan. Memuat dari jaringan tidak aman, dan harus dipertimbangkan.
7. Perutean sumber IP, perutean sumber adalah fitur IP dimana paket individu dapat menentukan rute. Fitur ini digunakan dalam beberapa jenis serangan. Router Cisco biasanya menerima dan memproses rute sumber. Kecuali jaringan bergantung pada perutean sumber, itu harus dinonaktifkan di semua perute jaringan.

8. Proxy ARP, host jaringan menggunakan Address Resolution Protocol (ARP) untuk menerjemahkan alamat jaringan menjadi alamat media. Router dapat bertindak sebagai perantara untuk ARP, menanggapi permintaan ARP pada antarmuka yang dipilih dan dengan demikian memungkinkan akses transparan antara beberapa segmen LAN. Layanan ini disebut proxy ARP. Karena melanggar perimeter keamanan LAN, secara efektif memperluas LAN pada lapisan 2 di beberapa segmen, ARP proxy harus digunakan hanya antara dua segmen LAN pada tingkat kepercayaan yang sama, dan hanya jika benar-benar diperlukan untuk mendukung arsitektur jaringan lama.
9. IP Directed Broadcast, siaran langsung mengizinkan host pada satu segmen LAN untuk memulai siaran fisik pada segmen LAN yang berbeda. Teknik ini digunakan dalam beberapa serangan penolakan layanan lama. Oleh karena itu harus menonaktifkan fungsi ini.
10. IP Unreachable, Redirects, dan Mask Replies: Internet Control Message Protocol (ICMP) mendukung lalu lintas IP dengan menyampaikan informasi tentang jalur, rute, dan kondisi jaringan. Router Cisco secara otomatis mengirim pesan ICMP dalam berbagai kondisi. Tiga pesan ICMP biasanya digunakan oleh penyerang untuk pemetaan dan diagnosis jaringan: 'Host unreachable', 'Redirect', dan 'Mask Reply'. Pembuatan otomatis pesan-pesan ini penting untuk dinonaktifkan di semua antarmuka, terutama antarmuka yang terhubung ke jaringan yang tidak tepercaya.
11. Layanan SNMP, Simple Network Management Protocol (SNMP) adalah protokol Internet standar untuk pemantauan dan administrasi jarak jauh otomatis. Ada beberapa versi SNMP yang berbeda, dengan properti keamanan yang berbeda. Jika jaringan memiliki infrastruktur SNMP yang digunakan untuk administrasi, maka semua router di jaringan itu harus dikonfigurasi untuk berpartisipasi secara aman di dalamnya. Sebagai contoh router Cisco dapat dikonfigurasi untuk bertindak sebagai klien untuk SNMP. Ketika layanan SNMP diaktifkan pada router, alat manajemen jaringan dapat menggunakannya untuk mengumpulkan informasi tentang konfigurasi router, tabel rute, beban lalu lintas, dan banyak lagi. Dengan tidak adanya skema SNMP yang diterapkan, semua fasilitas SNMP di semua router harus dinonaktifkan menggunakan langkah-langkah ini:

1. Hapus semua string komunitas yang ada.
2. Nonaktifkan fitur penonaktifan dan perangkap sistem SNMP.
3. Nonaktifkan pemrosesan sistem SNMP.

B) Injeksi SQL berdasarkan input pengguna

Serangan injeksi SQL dasar menggunakan input pengguna. Aplikasi web menerima input melalui formulir, yang meneruskan input pengguna ke database untuk diproses. Jika aplikasi web menerima input ini tanpa membersihkannya, penyerang dapat menyuntikkan pernyataan SQL melalui bidang formulir dan menghapus, menyalin, atau memodifikasi konten database.

Injeksi SQL berdasarkan cookie

Pendekatan lain untuk injeksi SQL adalah memodifikasi cookie menjadi kueri database "meracuni". Aplikasi web sering memuat cookie dan menggunakan datanya sebagai bagian dari operasi basis data. Pengguna jahat, atau malware yang disebarkan pada perangkat pengguna, dapat memodifikasi cookie, untuk menyuntikkan SQL dengan cara yang tidak terduga ke dalam database backend.

Injeksi SQL berdasarkan header HTTP

Variabel server seperti header HTTP juga dapat digunakan untuk injeksi SQL. Jika aplikasi web menerima input dari header HTTP, header palsu yang berisi SQL arbitrer dapat menyuntikkan kode ke dalam database.

Injeksi SQL orde kedua

Ini mungkin serangan injeksi SQL yang paling kompleks, karena mereka mungkin tertidur untuk jangka waktu yang lama. Serangan injeksi SQL orde kedua mengirimkan data beracun, yang mungkin dianggap jinak dalam satu konteks, tetapi berbahaya dalam konteks lain. Bahkan jika pengembang membersihkan semua input aplikasi, mereka masih rentan terhadap jenis serangan ini.

Dampak Serangan Injeksi SQL

Berikut adalah beberapa contoh kerusakan yang dapat ditimbulkan oleh serangan injeksi SQL pada organisasi, jika berhasil:

- **Mencuri kredensial**—Injeksi SQL dapat digunakan untuk menemukan kredensial pengguna. Penyerang kemudian dapat menyamar sebagai pengguna ini dan menggunakan hak istimewa mereka.
- **Akses database**—penyerang dapat menggunakan injeksi SQL untuk mendapatkan akses ke informasi yang disimpan di server database.
- **Ubah data**—penyerang dapat menggunakan injeksi SQL untuk mengubah atau menambahkan data baru ke database yang diakses.
- **Hapus data**—penyerang dapat menggunakan injeksi SQL untuk menghapus catatan database, termasuk tabel drop.
- **Akses jaringan**—penyerang dapat menggunakan injeksi SQL untuk mengakses server database dengan hak istimewa sistem operasi. Penyerang kemudian dapat mencoba mengakses jaringan.

Sniped code :

```
String firstname = req.getParameter("firstname");String lastname =
req.getParameter("lastname");String query = "SELECT id, firstname, lastname FROM author
WHERE firstname = ? and lastname = ?";// Menggunakan a PreparedStatement untuk
mengambil kueri pengguna dan membersihkannya // dengan menyetelnya sebagai string,
alih-alih langsung meneruskannya ke DB
PreparedStatement pstmt = koneksi.prepareStatement( query );
pstmt.setString( 1, nama depan );
pstmt.setString( 2, nama belakang );try{ Hasil Set Hasil = pstmt.execute();}
```

C.) pengujian

Ini adalah serangan injeksi SQL sederhana berdasarkan input pengguna. Penyerang menggunakan formulir yang membutuhkan nama depan dan nama belakang sebagai input. Penyerang memasukkan:

- Nama depan:sendihot
- Nama keluarga:Sihole

Pernyataan SQL yang memproses input formulir terlihat seperti ini:

```
pilih id, nama depan, nama belakang dari penulis
```

Setelah penyerang menyuntikkan ekspresi jahat ke dalam nama depan, pernyataannya terlihat seperti ini:

```
pilih id, firstname, lastname dari penulis di mana firstname = 'malicious'ex' dan lastname
='newman'
```

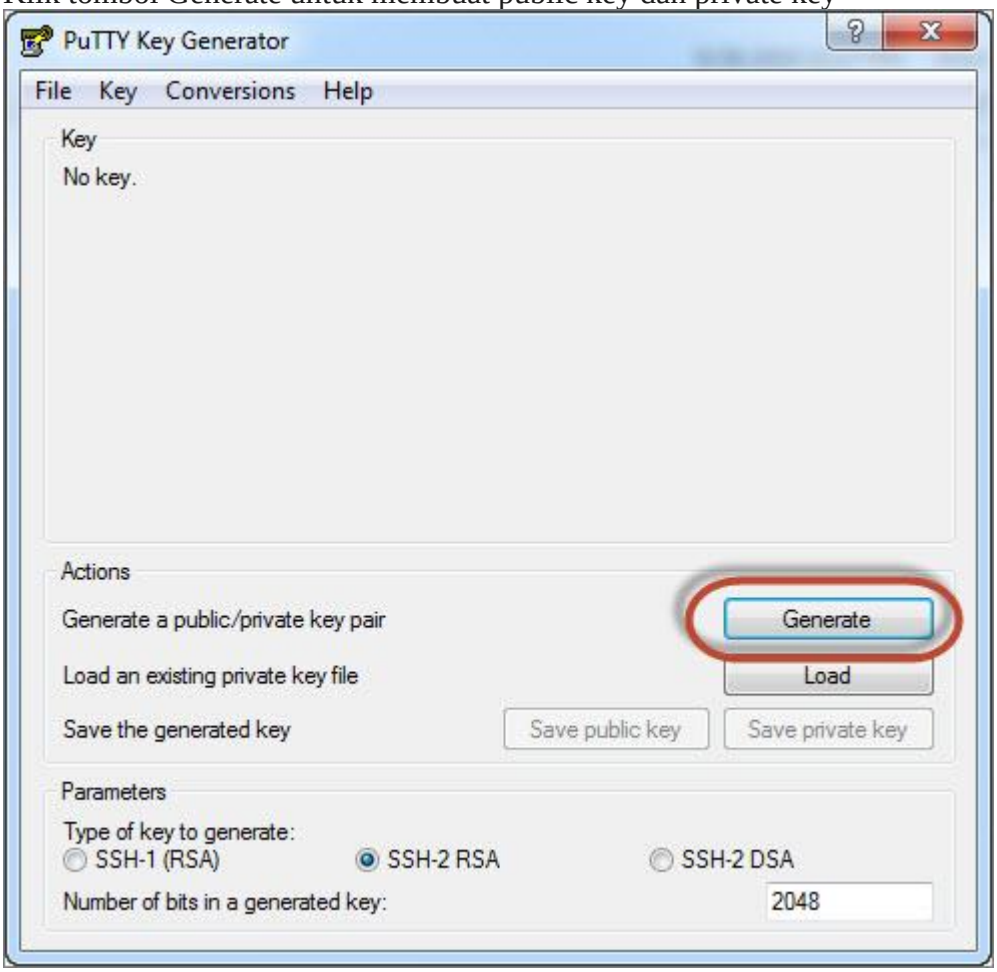
Basis data mengidentifikasi sintaks yang salah karena tanda kutip tunggal, dan mencoba mengeksekusi pernyataan jahat.

Berikut adalah kode dari OWASP yang menunjukkan cara mencegah serangan ini, dengan membersihkan input.

```
String firstname = req.getParameter("firstname");String lastname =
req.getParameter("lastname");String query = "SELECT id, firstname, lastname FROM author
WHERE firstname = ? and lastname = ?";// Menggunakan a PreparedStatement untuk
mengambil kueri pengguna dan membersihkannya // dengan menyetelnya sebagai string,
alih-alih langsung meneruskannya ke DB
PreparedStatement pstmt = koneksi.prepareStatement( query );
pstmt.setString( 1, nama depan );
pstmt.setString( 2, nama belakang );try{ Hasil Set Hasil = pstmt.execute();}
```

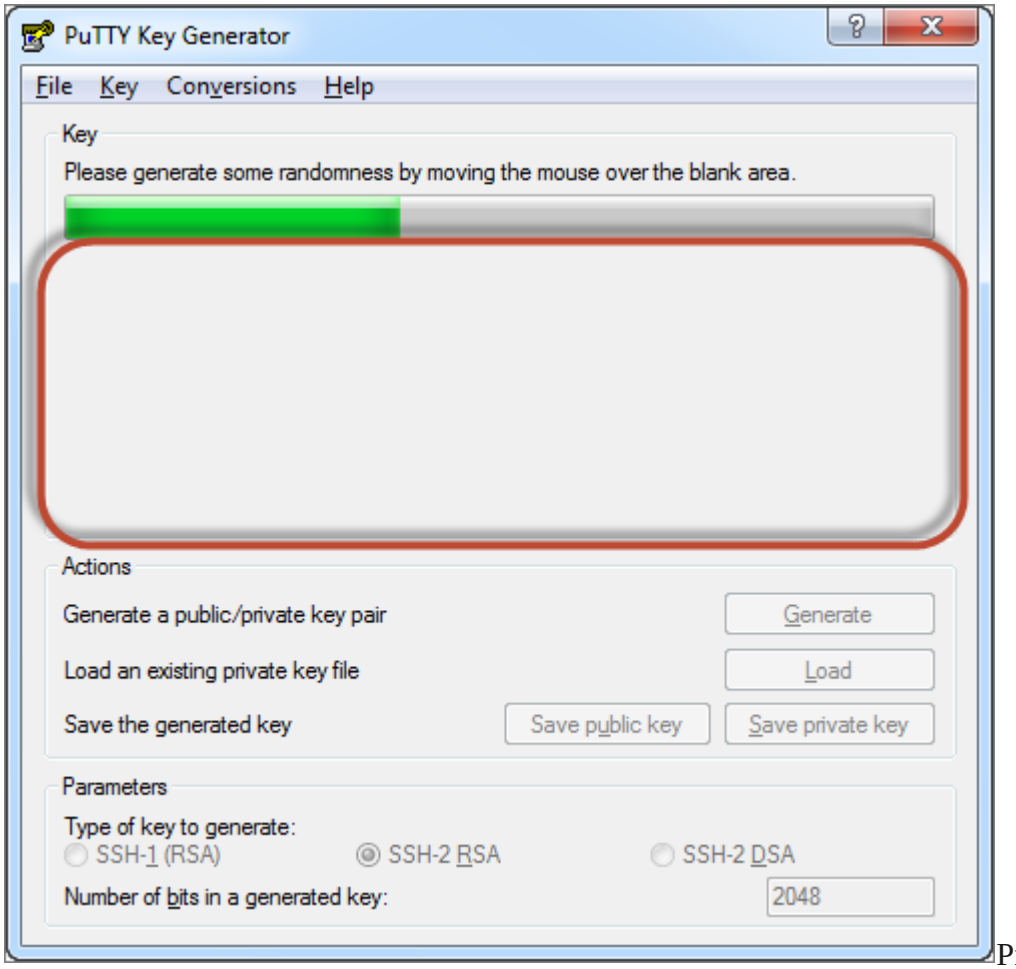
D.) *public private key (PPK*)di Komputer Windows

1. Install Putty sebagai SSH Client.
2. Jalankan PuTTYgen untuk membuat key. PuTTYgen adalah aplikasi khusus dari PuTTY untuk membuat public key dan private key
3. Klik tombol Generate untuk membuat public key dan private key



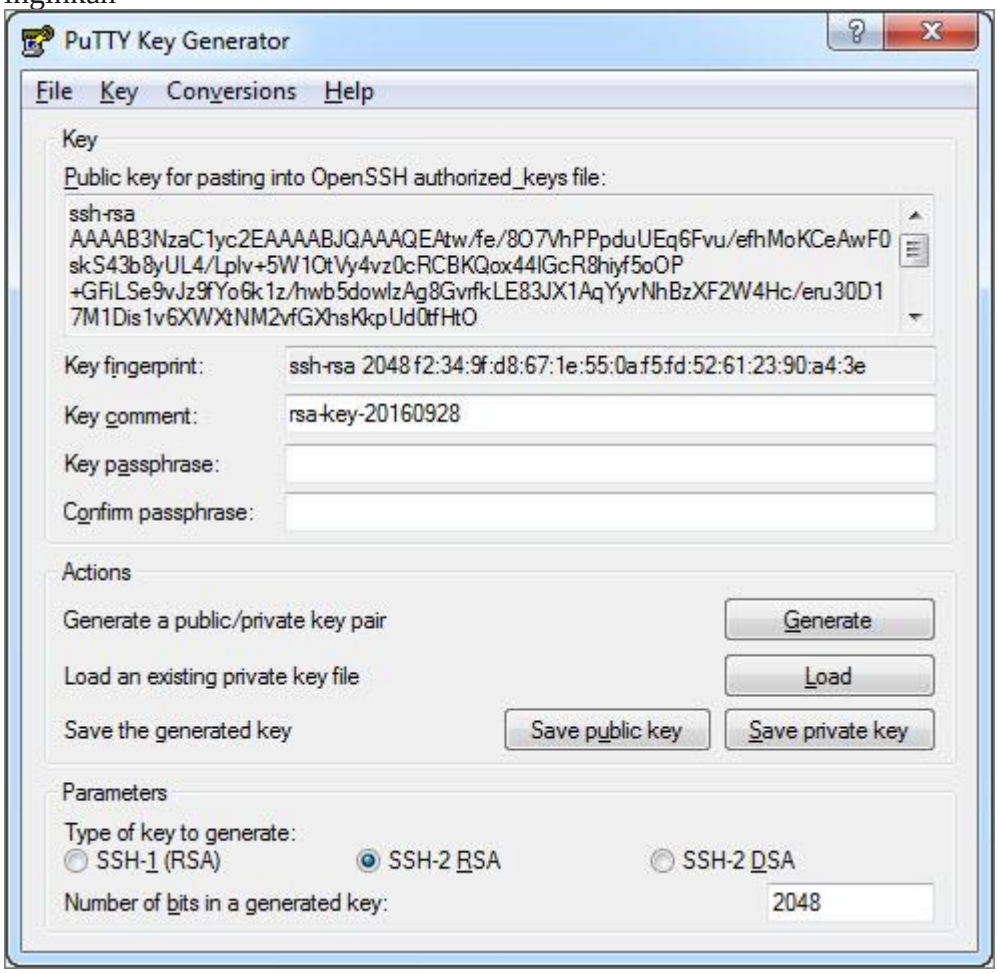
Membuat SSH KeyUntuk parameter, pilih settingan default yang diberikan oleh PuTTY.

4. Gerakkan mouse di bagian kotak merah agar PuTTY bisa membuat key. Gerakkan terus sampai progress bar terisi penuh.



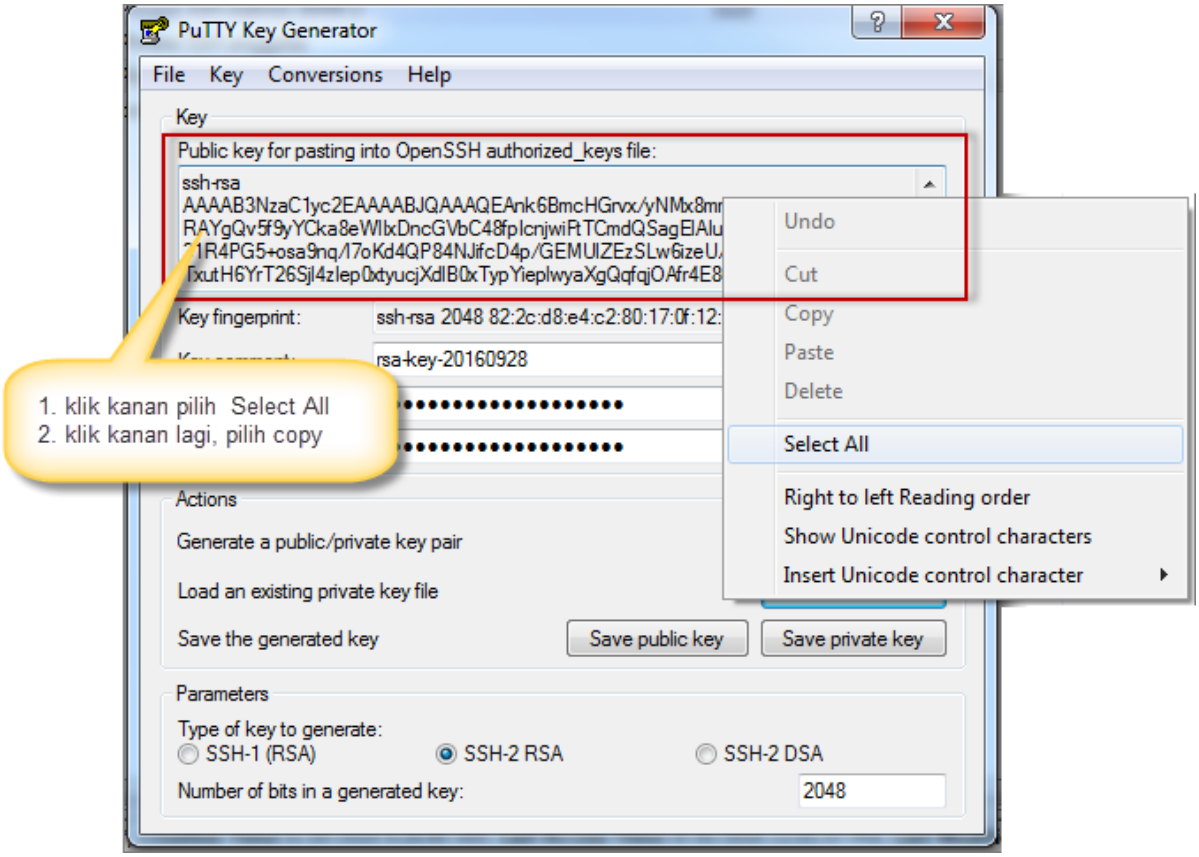
Progress membuat SSH Key

5. Jika sudah selesai, maka simpanlah public key dan private key di folder yang kamu inginkan



SSH Key selesai dibuat

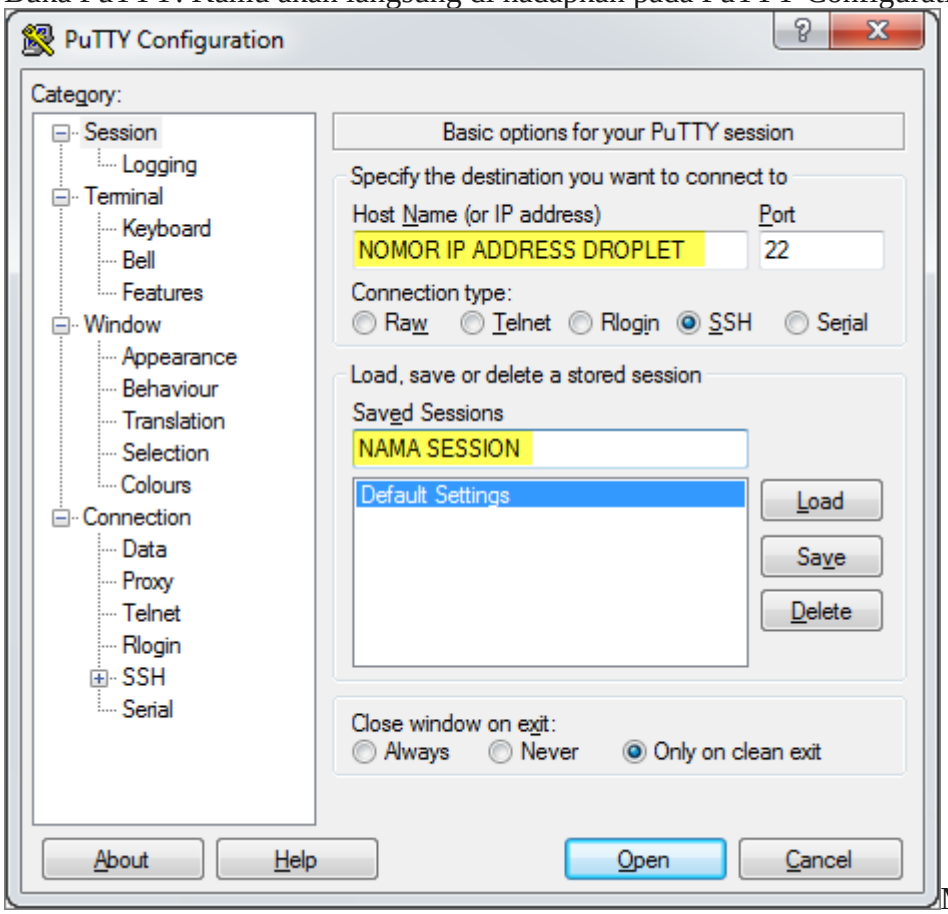
6. Pada bagian yang diberi kotak merah, copy mulai dari ssh-rsa sampai ke bagian bawah.



Copy Public Key

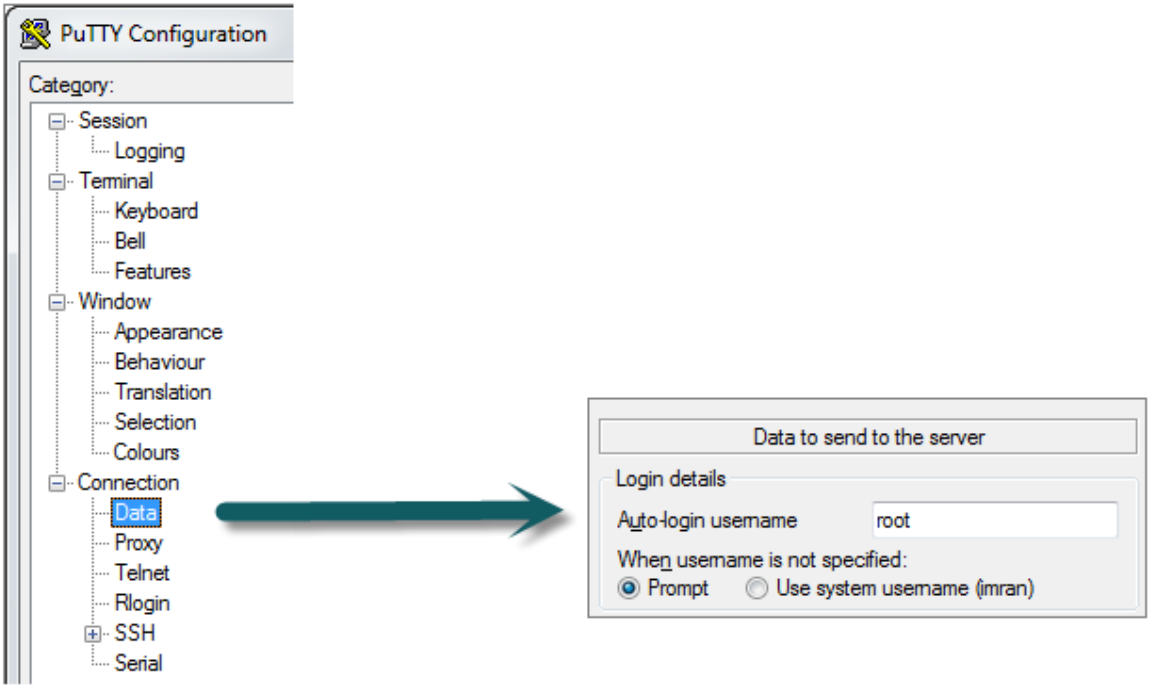
7. Buka notepad, dan paste kedalam notepad. Simpan dalam bentuk file text. Kemudian pindahkan file notepad ke komputer yang biasa digunakan untuk mengakses server VPS.
8. Pada komputer yang biasa digunakan untuk akses server VPS, buka file tersebut dengan editor text biasa. Bisa menggunakan notepad atau Text Edit jika komputer Mac. Select All semua isi file tersebut kemudian copy.
9. Paste kedalam file authorized_keys di server VPS. Tentu saja kamu harus sudah menambah user baru ssh di server VPS.
10. Setelah public key tersimpan di server VPS, maka kamu bisa mencoba melakukan koneksi dengan PuTTY ke server VPS

11. Buka PuTTY. Kamu akan langsung di hadapkan pada PuTTY Configuration.



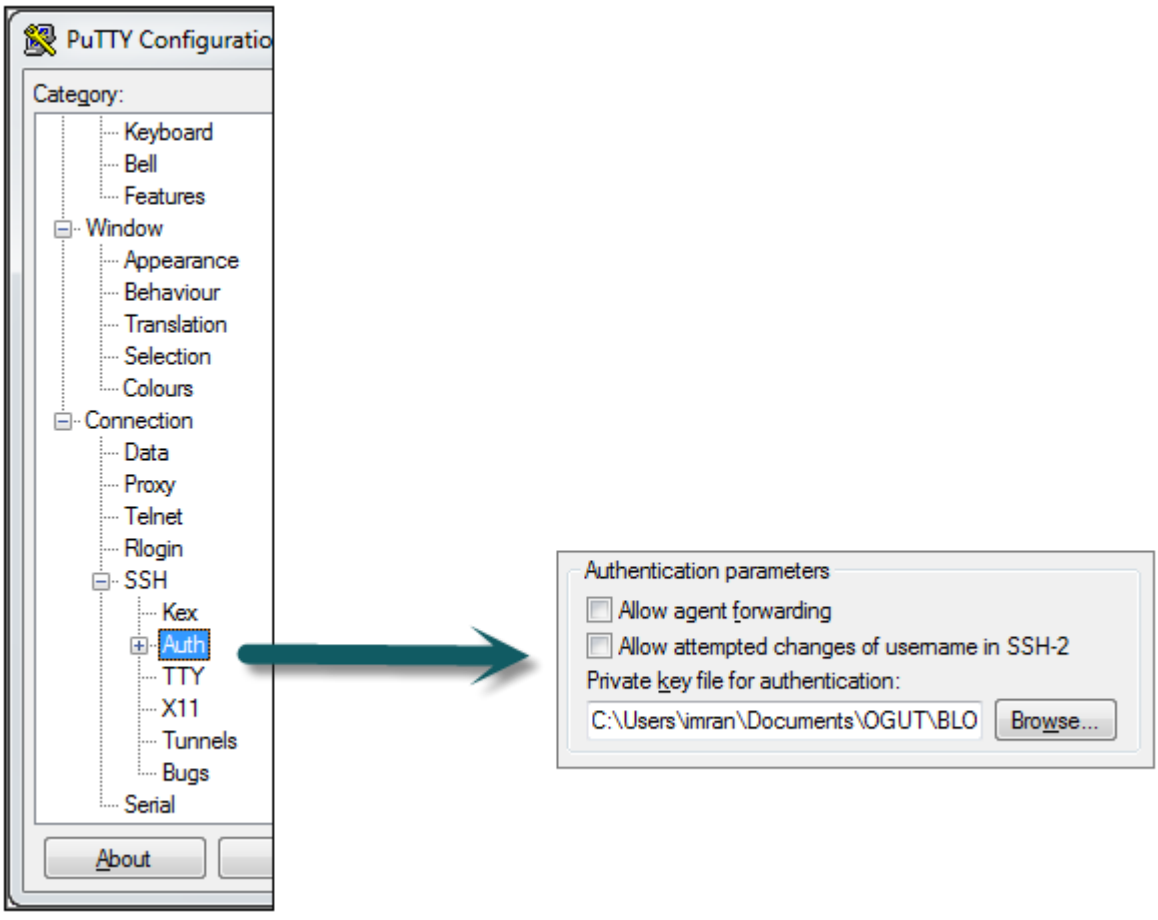
Membuat PuTTY session yang baru

12. Masukkan nomor IP server dan port untuk mengakses server. Secara default port ssh adalah port 22. Tapi port itu bisa dirubah di file /etc/ssh/sshd_config
13. Pada bagian Category > Connection > Data, masukkan autologin username pada VPS



PuTTY data configuration

14. Kemudian beralih pada Category > Connection > SSH > Auth



PuTTY Data ConfigurationKlik tombol Browse dan arahkan pada folder file private key disimpan.

15. Kembali ke Category > Session, masukkan name session pada bagian “Saved Sessions” dan klik Save untuk menyimpan.