Mata Kuliah	**: Pr. Keamanan Jaringan**
Program Studi	**: Teknologi Informasi**
SKS	**: 4 (2-2)**
Materi	**: Open VPN**
Alokasi Waktu	**: 2 X 120 menit**

Open VPN

Materi Virtual Private Network

A. Standar Kompetensi
   1. Mahasiswa mampu memahami dan mampu menjelaskan konsep dan landasan teori Keamanan Jaringan Komputer, serta pengujianya dalam sistem berbasis komputer.
   2. Mahasiswa merancang, mengkonfigurasi dan menguji penerapankeamanan jaringan dalam studi kasus tertentu.

B. Kompetensi Dasar
   1. Mahasiswa mampu menjelaskan cara kerja Opan VPN.
   2. Mahasiswa mampu melakukan instalasi dan konfigurasi Open VPN.

C. Teori

VPN atau Virtual Private Network adalah solusi koneksi private melalui jaringan public. Dengan VPN maka kita dapat membuat jaringan di dalam jaringan atau bisa disebut tunnel. VPN merupakan koneksi virtual yang bersifat private. Disebut private karena pada dasarnya jaringan ini merupakan jaringan yang sifatnya private yang tidak semua orang bisa mengaksesnya. VPN menghubungkan PC dengan jaringan public atau internet namun sifatnya private, karena bersifat private maka tidak semua orang bisa terkoneksi ke jaringan ini dan mengaksesnya.

Keamanan dengan konsep demikian maka jaringan VPN ini menawarkan kamanan dan untraceable, tidak dapat terdeteksi sehingga IP kita tidak diketahui, karena yang digunakan adalah IP public milik VPN server. Dengan adanya enkripsi dan dekripsi maka data yang lewat jaringan internet ini tidak dapat diakses oleh orang lain bahkan oleh client lain yang terhubung ke server VPN yang sama sekalipun. Karena kunci untuk membuka enkripsinya hanya diketahui oleh server VPN dan client yang terhubung. Enkripsi dan dekripsi menyebabkan data tidak dapat dimodifikasi dan dibaca sehingga keamanannya terjamin.

D. Alat dan Bahan

1. Modul praktek
2. Komputer/laptop
3. Virtual machine
4. Repositori

E. Pelaksanaan Praktek

1. Instal paket openvpn

   apt-get install openvpn
2. Salin direktori openvpn dari /usr ke /etc

   cp –R /usr/share/doc/openvpn/examples/easy-rsa/2.0 /etc/openvpn
3. Salin file server.conf.gz ke direktori /etc/openvpn

   cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn
4. Masuk ke direktori openvpn 2.0

   cd /etc/openvpn/2.0
5. Edit file vars

   nano vars
6. Ubah parameter country, province, city, org dan email menjadi

   export KEY_COUNTRY=”ID”

   export KEY_PROVINCE=”JT”

   export KEY_CITY=”Madiun”

   export KEY_ORG=”PNM”

   export KEY_EMAIL=pnm@gmail.com
7. Jalankan perintah berikut

   source vars

   ./clean-all

   ./build-dh

   ./pkitool - -initca

   ./pkitool - -server server

   ./pkitool client
8. Salin server.key ke direktori /etc/openvpn

   cp keys/server.key /etc/openvpn
9. Salin server.crt ke direktori /etc/openvpn

cp keys/server.crt /etc/openvpn

10. Salin file ca.crt ke direktori /etc/openvpn
    cp keys/ca.crt /etc/openvpn
11. Salin file dh1024.pem ke direktori /etc/openvpn
    cp keys/dh1024.pem /etc/openvpn
12. Salin file client.key ke direktori /etc/openvpn
    cp keys/client.key /etc/opnvpn
13. Salin file client.key ke direktori home
    cp keys/client.key /home/lulu
14. Salin file client.crt ke direktori home
    cp keys/client.crt /home/lulu
15. Salin file ca.crt ke direktori home
    cp keys/ca.crt /home/lulu
16. Buat user pada direktori bin
    useradd –m –s /bin/false lulu
17. Buat password untuk user lulu
    passwd lulu
18. Masuk ke direktori openvpn
    cd /etc/openvpn
19. Jalankan perintah berikut:
    gunzip server.conf.gz
    nano server.conf
20. Cari kata def1, ubah menjadi:
    push “redirect-gateway def1”
21. Hilangkan tanda semicolon di depan kata push “dhcp-option DNS 208.67.222.222”
22. Hilangkan tanda semicolon di depan kata push “dhcp-option DNS 208.67.220.220”
23. Hilangkan tanda semicolon di depan kata client to client
24. Hilangkan tanda semicolon di depan duplicate-cn
25. Simpan perubahan
26. Restart service opnvpn dengan perintah
    Service opnvpn restart

27. Install ssh

    apt-get install ssh
28. Pengaturan di server selesai selanjutnya pengaturan di client yang menggunakan sistem operasi Windows.
29. Download aplikasi openvpn client dan winscp.
30. Install keduanya.
31. Jalankan aplikasi winscp, menggunakan protokol SCP, port number 22, ip address 192.168.1.1 (server debian), username root dan passwordnya, klik login.
32. Jika ada peringatan pilih Yes.
33. Slain file client.key, client.crt dan ca.crt ke komputer windows.
34. Buka notepad dan masukkan berikut, simpan dengan nama client.ovpn

    client

    dev tun

    proto udp

    remote 192.168.1.1 1194

    key client.key

    cert client.crt

    ca ca.crt

    auth-user-pass

    persist-tun

    comp-lzo

    verb 3
35. Pindahkan ke-4 file ke direktori instalasi config openvpn.
36. Jalankan aplikasi openvpn client.