Materi Workshop Admin Jaringan

1. Telnet dan SSH server
2. FTP server, anonymous FTP & Secure FTP
3. File Sharing using Samba
4. DNS Server
5. Web Server
6. Web hosting & Virtual Domain
7. Project 1
8. Demo Project 1 (UTS)
9. Mail Server : SMTP & POP
10. Webmail
11. DHCP Server
12. Proxy Server
13. Proxy Server : Content Filtering
14. Network Monitoring
15. Project 2
16. Demo Project 2 (UAS)

Pertemuan 1

Telnet Server dan SSH Server

A. Pengecekan Sistem

Sebelum memulai praktikum, pastikan komputer anda terhubung ke jaringan.

1. Catat IP address dan netmask dari komputer yang anda gunakan.
   Gunakan perintah **ifconfig**.
   $ sudo ifconfig eth0
   Catat IP address dan netmask komputer anda

2. Coba ping ke komputer di sekitar anda, pastikan komputer anda bisa saling terhubung
   Gunakan perintah **ping.**
   $ ping 10.252.108.xxx (pilih komputer di sebelah kiri dan kanan anda)

3. Pastikan anda terhubung ke default gateway
   Gunakan perintah ping ke default gateway lab jarkom 10.252.108.1
   $ ping 10.252.108.1

4. Pastikan bahwa komputer anda sudah terhubung ke DNS server PENS
   $ cat /etc/resolv.conf
   Catatlah, berapa IP dari DNS server PENS.

5. Pastikan bahwa komputer anda sudah terhubung ke Debian repositories
   $ cat `/etc/apt/sources.list`

6. Periksa apakah Debian anda bisa melakukan proses update langsung ke Debian repositories
   $ sudo apt-get update

Untuk memulai praktikum, anda harus memastikan bahwa langkah nomer 1-6 di atas semuanya sudah sukses. Jika tidak, maka anda tidak bisa melanjutkan praktikum di bawah ini.

B. Instalasi dan Konfigurasi Telnet Server

Telnet atau (**Tel**ecommunication **net**work) adalah sebuah protokol jaringan yang digunakan pada Internet atau Local Area Network untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal. TELNET dikembangkan pada

1969 dan distandarisasi sebagai IETF STD 8, salah satu standar Internet pertama. TELNET memiliki beberapa keterbatasan yang dianggap sebagai risiko keamanan. Telnet merupakan sebuah protocol yang memungkinkan penggunanya dapat login dan bekerja pada sistem jarak jauh.

7. Instalasi telnet server
   $ sudo apt-get install telnetd

8. Mengaktifkan layanan telnet server
   Telnet dianggap service yang tidak aman sehingga hampir semua distro Linux secara defalut men-disable layanan ini. Agar layanan telnet server dapat berhasil, edit file /etc/inetd.conf. Anda dapat menggunakan ediot vi, vim, nano, gedit atau yang lainnya.

   $ vi /etc/inetd.conf

   Hapuslah komen (tanda #) pada baris ini.

```
#telnet         stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
```

   Setelah simpan dan keluar dari editor.

9. Agar perubahan file konfigurasi tersebut dapat langsung dirasakan, silahkan restart service inetd dengan perintah berikut
   $ sudo /etc/init.d/openbsd-inetd restart

10. Membuat user baru untuk uji coba telnet serber
    Buatlah 2 user baru untuk keperluan uji coba telnet server dan SSH server. Gunakan
    $ sudo adduser user1
    $ passwd user1

    $ sudo adduser user2
    $ passwd user2

11. Uji coba telnet server dari localhost
    $ telnet localhost
    Masukkan username dan password, jika berhasil ketik exit untuk keluar dari telnet server.

12. Uji coba telnet server dari host lain.
    Bekerjasamalah dengan teman anda, minta teman anda untuk telnet ke telnet server yang anda gunakan. Gunakan user1 dan user2 untuk login ke telnet server.
    $ telnet ip_address_telnet_server

13. Gunakan perintah who atau finger (dari telnet server) untuk melihat siapa saja user yang sedang login
    $ who
    $ finger

C. Memahami Kelemahan layanan Telnet

Username dan password di layanan telnet dikirimkan secara plaintext (tidak di-enkripsi). Oleh karena itu, telnet dianggap layanan yang tidak aman. Percobaan berikut ini bertujuan untuk membuktikan bahwa telnet adalah layanan yang tidak aman

14. Jalakan wireshark pada komputer server (telnet server). Jika belum ada wireshark, install dulu software ini dengan perintah apt-get install
    Dari komputer client, lakukan koneksi telnet ke telnet server.
    Jika client sudah sukses login ke telnet server, hentikan program wireshark.
15. Analisa paket TCP khususnya saat program telnet di layer aplikasi. Letakkan kursor pada paket awal aplikasi telnet sudah tersambung, lalu klik kanan dan pilih 'follow TCP stream'. Analisa trafik tersebut dan coba temukan nama password yang digunakan.
16. Setelah anda sekarang memahami bahwa telnet adalah aplikasi yang tidak aman, maka lakukan :
    - Uninstall aplikasi telnet server
    - Kembalikan file **/etc/inetd.conf** seperti semula (disable layanan telnet)

Secure Shell (SSH)

SSH adalah akronim dari Secure Shell. SSH adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan.Contoh penggunaan SSH di kalangan administrator adalah untuk me-remote server.

Fungsi SSH Server:

1. Menggantikan telnet, rlogin, ftp, dan rsh, salah satu fungsi utamanya adalah untuk menjamin keamanan dalam melakukan transmisi data pada suatu jaringan.
2. Melakukan enkripsi terhadap data yang dikirim.
3. Protokol untuk pertukaran data dalam suatu jaringan.
4. Otentifikasi, mekanisme untuk memastikan pengirim dan penerima adalah benar dan aman.
5. Kerahasiaan, memastikan kerahasiaan data yang dikirim agar hanya diketahui oleh penerima dan pengirim.

Cara Kerja SSH Server

Pada saat suatu client mencoba mengakses suatu linux server melalui SSH. SH daemon yang berjalan baik pada linux server maupun SSH client telah mempunyai pasangan public/private key yang masing-masing menjadi identitas SSH bagi keduanya.

Konfigurasi SSH Server

Perrtama Instal dulu paket untuk SSH server

 # apt-get install ssh

Setelah aplikasi terinstall, layanan SSH Server sudah langsung bisa kita gunakan melalui port default 22.
Kalau kita hendak merubah port default, maka kita edit file konfigurasinya :
 # nano /etc/ssh/sshd_config

Cari baris berikut dan ubah sesuai dengan keinginan :
 # What ports, IPs and protocols we listen for
Port 354

Setelah itu restart SSH server anda
 # /etc/init.d/ssh restart

Uji layanan ssh anda.
Kalau port SSH masih standart :
 # ssh root@localhost

Kalau port SSH sudah diganti (misal 354)
 # ssh root@localhost –p 354

Masukkan password root.
Apabila bisa login maka SSH berhasil.
Untuk logout ketikkan exit.