NETWORK MONITORING DAN LOG ANALYSIS

3.1. ALOKASI WAKTU DAN PERSIAPAN

Praktikum ini terdiri dari 3 percobaan, untuk menyelesaikan semua percobaan pada modul ini membutuhkan waktu 100 menit atau satu kali pertemuan.

Untuk kelancaran praktikum, asisten praktikum sebaiknya sudah menyiapkan software-software dan meng-*install*-nya pada komputer yang digunakan sebagai praktikum. Asisten juga harus memantau kondisi jaringan pada semua komputer dan memastikan komputer server dan client terhubung dengan baik.

3.2. DASAR TEORI

3.2.1. Footprinting

Footprinting adalah fase persiapan ketika penyerang mengumpulkan/ mencari sebanyak mungking informasi yang mungkin tentang target sebelum dilakukan penyerangan. Metode yang tepat sangat beragam. Di lab ini kita akan mempelajari teknik mengumpulkan informasi non-intrusive (tanpa mengganggu). Disini tidak ada sistem yang dilanggar atau diakses. Informasi datang dari sumber public terpecaya.

Pada umumnya penggunaan tool untuk footprinting adalah tool whois. Tool whois akan mengumpulkan semua informasi tentang perusahaan target dari beberapa database yang terdistribusi di dunia.

Bila alamat IP target telah diperoleh, penyerang bisa melacak rute antara sistem dan sistem target. Kebanyakan sistem operasi menyediakan sebuah utilitas 'traceroute' pada detail jalur perjalanan

IP paket antara dua sistem. Alat traceroute visual seperti Neotrace dan VisualRoute bahkan memberikan informasi cukup rinci pada setiap 'hop' pada rute, seperti informasi kemana pemilik dan jaringan tersebut terdaftar.

3.2.2. Logging

Logging merupakan prosedur di mana sebuah sistem operasi atau aplikasi merekam setiap kejadian dan menyimpan rekaman tersebut untuk dapat dianalisa di kemudian hari. Kejadian yang direkam ini bisa saja menyangkut sistem operasi, atau khusus program-program tertentu saja. Linux memiliki fasilitas logging yang sangat komprehensif.

Semua file log di Linux disimpan dalam direktori /var/log. Beberapa program/file log yang penting adalah :

a. lastlog

   Berisi rekaman kapan user login terakhir kali. Yang ditampilkan adalah nama login, port dan waktu login terakhir kali. Untuk memanggilnya cukup ketikkan lastlog.

b. xferlog (vsftpd.log)

   Mencatat semua informasi yang pernah login di ftp daemon. Data yang ditampilkan berupa waktu saat ini, durasi transfer file, host yang mengakses (baik nomor IP maupun nama host), jumlah file yang ditransfer, nama file, tipe transfer (Binary atau ASCII), perintah khusus yang diberikan (jika file dikompres atau tar), arah transfer (incoming, outgoing), modus akses (anonymous, guest, atau user resmi), nama user, layanan, metode otentikasi, dan user ID.

c. access_log

   Berisi rekaman untuk layanan http (HyperText Transfer Protocol) atau layanan web server. Access_log biasanya terdiri dari Nomor IP dari pengakses, jam dan tanggal akses, printah atau permintaan, dan kode status.

d. error_log

   Berisi rekaman pesan kesalahan atas service http atau web server. Error_log terdiri dari jam dan waktu, tipe kesalahan, alasan kesalahan, layanan, dan perintah yang dijalankan berikutnya (kadang-kadang).

e. messages

Rekaman kejadian sistem dan kernel, ditangani oleh dua daemon, syslogd merekam semua program yang dijalankan. Untuk mengkonfigurasikannya dapat mempergunakan syslog.conf. klogd, menerima dan merekam pesan kernel File messages dapat dilihat di / var/log/messages.

f. Host

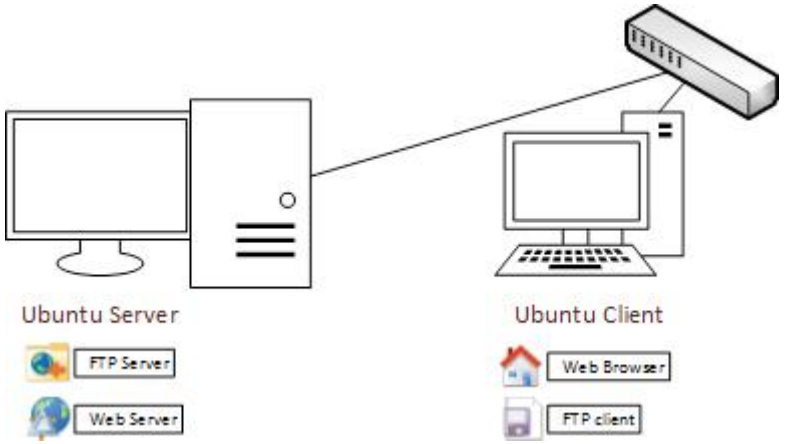
Merupakan sebuah utiliti yang sederhana yang dapat digunakan untuk melihat ip suatu host dengan memanfaatkan DNS.

3.3. TUJUAN

1. Mengenalkan konsep Manajemen Log di linux
2. Mengetahui berbagai macam file log yang ada di linux
3. Melakukan analisa terhadap file log yang ada di linux
4. Melakukan monitoring terhadap file log di linux

3.4. BAHAN DAN ALAT

1. Siapkan dua buah komputer dengan sistem operasi Ubuntu Linux yang terhubung dalam sebuah jaringan
2. Komputer pertama menggunakan sebagai server yang memiliki layanan WEB (menggunkan Apache2) dan FTP (menggunakan vsftpd)
3. Komputer kedua digunakan sebagai clien yang mengakses layanan pada server, komputer ini dilengkapi dengan Firefox sebagai web browser dan aplika Filezila sebagai FTP *client*



3.5. LANGKAH PERCOBAAN

3.5.1. Percobaan 1: Menggunakan perintah lastlog

1. Pada komputer server jalankan perintah lastlog

```
root@fki-ums:/# lastlog
```

contoh hasil:

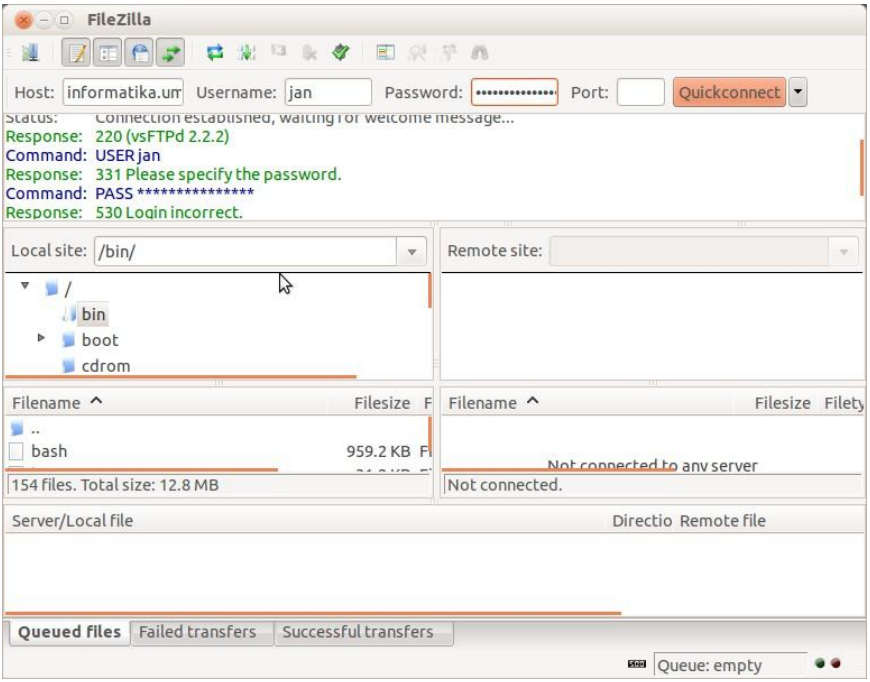
```
Username    Port   From   Latest
root                      **Never logged in**
daemon                    **Never logged in**
…
…
andi        pts/2         Mon Dec 20 11:03:14 +0700 2010
joko        pts/1         Mon Dec 20 11:01:45 +0700 2010
```

2. Amati hasil percobaan dan lakukan analisis terhadap hasil tersebut kemudian simpulkan mengapa hasilnya seperti itu.

3.5.2. Percobaan 2: Informasi yang pernah login di ftp daemon

1. Pastikan ftp server telah di-*install* (vsftpd), gunakan komputer klien untuk melakukan proses *download* sebuah

file pada komputer server menggunakan protokol ftp (anda dapat menggunakan program FileZilla pada komputer klien untuk melakukan upload dan download).



2. Setelah klient melakukan download, masuk ke server dan baca file vsftpd.log pada server dengan perintah:

```
$ sudo cat /var/log/vsftpd.log
```

contoh hasil:

```
Mon Dec 20 12:37:57 2010 [pid 2] CONNECT: Client
"192.168.56.1"
Mon Dec 20 12:37:58 2010 [pid 1] [joko] OK LOGIN:
Client "192.168.56.1"
Mon Dec 20 12:39:10 2010 [pid 2] CONNECT: Client
"192.168.56.1"
Mon Dec 20 12:39:10 2010 [pid 1] [joko] OK LOGIN:
Client "192.168.56.1"
Mon Dec 20 12:41:13 2010 [pid 2] CONNECT: Client
```

```
"192.168.56.1"
Mon Dec 20 12:41:13 2010 [pid 1] [joko] OK LOGIN:
Client "192.168.56.1"
Mon Dec 20 12:41:14 2010 [pid 3] [joko] OK
DOWNLOAD: Client "192.168.56.1", "/home/joko/
examples.desktop", 179 bytes, 5.39Kbyte/sec
```

3. Gunakan komputer klien untuk melakukan proses upload sebuah file ke server. Setelah client melakukan upload, baca file vsftpd.log pada server.

```
root@fki-ums:/# cat /var/log/vsftpd.log
```

4. Amati hasil percobaan dan lakukan analisis terhadap hasil tersebut kemudian simpulkan mengapa hasilnya seperti itu.

3.5.3. Percobaan 3: Mengamati log pengaksesan sebuah halaman web

1. Pastikan paket http server sudah terinstal (apache web server), gunakan komputer clien untuk mengakses halaman web dari server tersebut menggunkan web browser.

2. Baca file error.log dan access.log pada komputer server.

```
# cat /var/log/apache2/error.log
# cat /var/log/apache2/access.log
```

3. Amati dan pelajari hasilnya, kemudian simpulkan!
4. Baca file log system pada komputer server.

```
# tail -f /var/log/syslog
# tail -f /var/log/messages
```

5. Amati hasil percobaan dan lakukan analisis terhadap hasil tersebut kemudian simpulkan mengapa hasilnya seperti itu.