

Lama juga tidak menulis tentang server. Kali ini saya akan memberikan sedikit tips untuk mengamankan VPS server dari malware dan virus menggunakan Linux Malware Detect (Maldet) dan ClamAV.

Jadi kita menginstal terlebih dahulu Maldet, kemudian dipadukan dengan ClamAV supaya proses scan lebih cepat dan efektif.

Instalasi Linux Malware Detect

Ketika artikel ini ditulis versi terakhirnya adalah **maldetect-1.5** jadi ketika melakukan perintah `cd` ganti dengan versi yang kamu download (akan kelihatan ketika kita melakukan perintah `tar -xvf maldetect-current.tar.gz`).

```
wget http://www.rfxn.com/downloads/maldetect-current.tar.gz tar -xvf maldetect-current.tar.gz  
cd maldetect-1.5 ./install.sh
```

Setelah Maldet terinstal secara otomatis akan membuat cron job harian kapan proses scan akan dilakukan secara rutin.

Konfigurasi Linux Malware Detect

Buka file yang menyimpan konfigurasi dari Maldet:

```
vi /usr/local/maldetect/conf.maldet
```

Nilai 1=true dan nilai 0=false.

Jika ingin menerima notifikasi email.

```
email_alert=1 email_addr=youremail@example.com email_subj="Malware alerts for  
$HOSTNAME - $(date +%Y-%m-%d)"
```

Pindahkan malware ke folder karantina.

Cara Scan Malware dan Virus di VPS Linux (CentOS)

Written by BiRU

Tuesday, 31 May 2016 20:58 -

```
quar_hits=1
```

Hapus malware yang terdeteksi.

```
quar_clean=1
```

Instalasi ClamAV

Dengan menginstall ClamAV maka Madet akan menjadi sangat powerful.

```
yum install epel-release yum update && yum install clamd
```

Cara Scan Malware dan Virus

Untuk scan folder gunakan perintah berikut:

```
maldet --scan-all /var/www/html
```

Jika kita ingin melakukan scan untuk file type tertentu misal .php:

```
maldet --scan-all /var/www/html/*.php
```

Untuk melihat hasil scanning yang sudah dilakukan bisa melakukan perintah berikut, ganti 12345-1234.1234 dengan ID-nya.

```
maldet --report 12345-1234.1234
```

Untuk mengupdate Linux Malware Detect:

```
maldet -u
```

Menghapus semua file di folder karantina:

```
rm -rf /usr/local/maldetect/quarantine/*
```

Nah itulah cara mengamankan VPS server kita dari malware dan virus dengan menggunakan Linux Malware Detect dan ClamAV.