

## Cara jitu perangi spam menggunakan SpamAssassin

Written by ari

Monday, 27 December 2004 06:27 - Last Updated Tuesday, 28 December 2004 02:10

---



Spam.. sebuah kata yang mengesalkan bagi semua pengguna email. Betapa tidak, setiap hari ketika kita membuka email pasti ada beberapa atau bahkan belasan email spam. Mulai dari penawaran jam rolex, obat kuat viagra, sampai software warez. Artikel ini akan membahas cara jitu

perangi spam menggunakan SpamAssassin

. Mail server saya yang dilengkapi dengan SpamAssassin (selanjutnya saya singkat SA

) dan clamav tiap bulan rata-rata berhasil menangkap 20.000

spam dan virus. Saya perkirakan jumlah yang tak berhasil ditangkap sekitar 30%. Jadi masih ada 6.000 email spam/virus yang berhasil lolos ke mailbox para user.

Baiklah, kita mulai... Berikut ini adalah hal2 yang dapat kita lakukan untuk memerangi spam menggunakan SA secara efektif:

1. Gunakan daftar rules filter SA tambahan. Secara default SA telah memiliki kemampuan untuk mengenali banyak spam, namun alangkah baiknya bila kita lengkapi juga dengan generic rules yang lebih variatif dan lengkap. Rules2 ini dapat kita peroleh dari

<http://www.rulesemporium.com/> Letakkan rules2 tersebut di folder

/etc/mail/spamassassin

dan kemudian restart SA. Patut diperhatikan bahwa rules bigevil.cf sebaiknya tidak dipakai lagi, sebab sangat berat. Ketika saya mencobanya, free swapfile saya langsung drop dari 700MB ke 40MB, dan pemakaian resource CPU lompat ke 400%!

2a. Testlah efek dari penggunaan rules2 tersebut di atas, dan kamu akan mulai merasakan bahwa spam yang masuk ke mailbox mulai berkurang. Namun kamu akan melihat bahwa tetap ada beberapa spam yang berhasil lolos, sebab memang spammer2 sangat kreatif dan pintar di dalam usahanya masuk ke dalam mailbox kita. Misalnya dengan menuliskan kata2

'viagra'

menjadi

'viiii aaaa gggraaa'

Oleh karena itu langkah selanjutnya adalah dengan

**MENGAJARI SA**

untuk mengenali spam2 tersebut. Caranya adalah sebagai berikut:

- masukkan email2 spam tersebut ke dalam folder trash, atau lebih baik lagi bila kita buat folder sendiri, misalnya 'Tempat-SPAM'

- login ke dalam server, dan jalankan perintah berikut (ini asumsi kita menggunakan vpopmail, dan menggunakan format Maildir):

```
sa-learn --showdots --spam
```

```
/home/vpopmail/domains/domainkita/mailboxkita/Maildir/namafolderygisinyaspam/cur/*
```

- setelah kita jalankan, maka akan muncul titik2 yang menunjukkan progressnya. Tunggulah beberapa saat, tergantung banyaknya email spam di dalam folder tersebut. Nanti kalau sudah selesai akan muncul pesan &quot;Learned from 3 message(s) (3 message(s) examined).&quot;

2b. Langkah selanjutnya yang juga penting adalah **MENGAJARI SA** untuk mengenali email2

## Cara jitu perangi spam menggunakan SpamAssassin

Written by ari

Monday, 27 December 2004 06:27 - Last Updated Tuesday, 28 December 2004 02:10

---

mana yang bukan spam, atau disebut juga 'ham'. Caranya adalah sebagai berikut:

- masukkan email2 ham atau YANG BUKAN spam tersebut ke dalam folder tersendiri, atau lebih baik lagi bila kita buat folder sendiri, misalnya 'BUKAN-SPAM'
- login ke dalam server, dan jalankan perintah berikut (ini asumsi kita menggunakan vpopmail, dan menggunakan format Maildir):  
sa-learn --showdots --ham  
/home/vpopmail/domains/domainkita/mailboxkita/Maildir/namafolderygisinyaBUKANspam/cur/\*
- setelah kita jalankan, maka akan muncul titik2 yang menunjukkan progressnya. Tunggulah beberapa saat, tergantung banyaknya email BUKAN spam di dalam folder tersebut.

### PERHATIAN!!

Pastikan bahwa ketika kamu menjalankan command2 di atas, folder yang kamu maksud **MEMANG BERISI**

email2 yang kamu maksudkan! Sebabnya misalkan kalau ternyata ada email yang bukan spam tapi kamu ajari SA sebagai spam, maka email2 tersebut akan dianggap spam oleh SA! Kalau sampai, misalkan email dari

pacar

kita ngga sengaja ter-mark sebagai spam.. wah.. bahaya besar.. hehe..!

3. Turunkan treshold/ambang batas scoring SA di dalam mengenali spam. Biasanya standar yang dipakai adalah angka 5. Jadi email yang memiliki score di atas 5 baru kita anggap spam. Marilah kita turunkan score ini ke 1.0. Langkah ini memang cukup agresif dan belum tentu semua admin setuju. Tapi dari hasil pengamatan saya, bila SA telah kita ajari, maka ia akan memberikan score negatif bagi email2 yang 'bersih'. Dengan menurunkan score ke level 1.0 ini, maka efektivitas SA menjadi lebih baik. Tapi tentu saja ini terserah masing2 kamu.

4. Langkah keempat ini tidak berhubungan langsung dengan menangkal spam yang masuk ke server kita, tapi **MEMBANTU** di dalam 'menggangu' aktivitas spammer. Spammer biasanya mendapatkan daftar2 email dari orang2 yang dikenal dengan sebutan 'Harvester'. Para harvester ini menggunakan program otomatis (bot/crawler) untuk menjelajahi internet mencari alamat2 email di dalam website. Nah, kita bisa mengganggu efektifitas bot/crawler ini dengan memasang ratusan bahkan ribuan alamat email palsu di dalam web kita. Teknik ini disebut sebagai 'spambait' atau pengumpan spam. Dengan terjaringnya ribuan alamat email palsu ini, maka para harvester tersebut menjadi sulit memisahkan mana email yang benar dan mana yang palsu.

Kamu pasti bertanya, &quot;Bagaimana caranya saya membuat email2 palsu sampai berjumlah ribuan? Capek dong!&quot; Tidak perlu khawatir, banyak tersedia website yang menyediakan fasilitas untuk me-generate email2 palsu ini, salah satunya adalah di <http://www.theworldofstuff.com/spam/email.html> Disitu kamu akan bisa menghasilkan 100 email palsu per halaman. Tinggal kita ketik More saja untuk membuat 100 email palsu lainnya.

Lalu selanjutnya kamu juga pasti bertanya2, &quot;Tapi masak saya membuat sebuah halaman web yang isinya email2 palsu tersebut? Ngga asik banget!&quot; Oh, tidak perlu begitu... kita bisa 'menyembunyikan' alamat2 email palsu ini dari pandangan pengunjung website kita, sambil tetap 'terlihat' oleh program bot/crawler tersebut. Caranya adalah menggunakan CSS

## Cara jitu perangi spam menggunakan SpamAssassin

Written by ari

Monday, 27 December 2004 06:27 - Last Updated Tuesday, 28 December 2004 02:10

---

(cascading Style Sheet). Dari website di atas kita mendapatkan tricknya tersebut yaitu:

1. Masukkan kode ini di antara tag <HEAD> dan </HEAD>

```
<STYLE TYPE="text/css">
```

```
<!--
```

```
#body {z-index:1;}
```

```
#body a:link {color:0000FF;}
```

```
#body a:active {color:FF0000;}
```

```
#body a:visited {color:800080;}
```

```
#bait {font-size:1pt; font-weight:extra-light; color:FFFFFF; position: absolute; left:0px; top:0px; visibility:visible; line-height:1px; z-index:-1;}
```

```
#bait a:link, a:active, a:visited {color: FFFFFFFF;}
```

```
-->
```

```
</STYLE>
```

2. Selanjutnya, BAGI isi website yang sesungguhnya, selalu kita awali dengan tag <div id="body">

dan kita akhiri dengan </div> Setelah itu, kita buat layer yang akan berisi alamat2 email palsu itu, dimana kita awali dengan tag

```
<div id="bait">
```

Kita masukkan email2 palsu ini ke dalam layer ini. Dan kemudian kita akhiri dengan tag </div>.

Bila bingung, kamu bisa melihat contoh source page htmlnya yang

<http://www.theworldofstuff.com/spam/>

Ok, semoga artikel ini dapat bermanfaat di dalam meningkatkan efektivitas penangkalan spam dan juga 'menggangu' aktivitas spammer. Hehe... Dari hasil pengamatan saya selama 48 jam ini, belum ada 1 pun spam yang berhasil masuk ke dalam mailbox saya lagi. Tapi memang harus disadari sangat sulit memerangi spam, dan cepat atau lambat para spammer akan menemukan cara alternatif di dalam meloloskan spamnya, tapi sebagai kita harus tetap berusaha. Seperti kata pepatah, &quot;I won't die without a fight!&quot; Hehe..

Bahan2 referensi:

<http://wiki.apache.org/spamassassin/BayesInSpamAssassin>

<http://www.theworldofstuff.com/spam/>

<http://www.rulesemporium.com/>



v.1.0 by ari\_stress a.k.a tiger74

Jakarta, 27 Desember 2004. fajarpri at arinet.org

Penulis adalah Microsoft Certified Professional, yang jatuh cinta kepada Linux. Bekerja di sebuah lembaga pendidikan di Jakarta