MENCARI ALAMAT TARGET IN ONE HOSTING !!!

Author : #kartubeben crew @ Dalnet
Thanks : someonet who tech me about it
E-mail : m_beben@gawab.com
Website : www.kartubeben.org

Assalamu'alaikum all, pa khabar nih ???

Penulis doain ente semua tetap berada dalam lindungan Allah SWT yang telah memberikan kite hidayah sehingga kite semua dapat berkumpul bersama-sama di tempat yang sederhana ini, tidak lupa pula sha... ups, kok jadi macam ceramah ya ??? Wekekeke... ya sudah lah ☺☺☺ :P~

OK, sekarang kite serius ya, ingat... jangan ada lagi yang maen-maen apalagi becanda. Se... Ri... Us... !!! ... OK !!!

Oh iya, sebelum penulis memulai tulisan ini, maka ada baiknya ente memperhatikan peringatan penulis berikut ini :

TULISAN INI HANYALAH DI PERUNTUKKAN UNTUK PARA NEWBIES, JADI KALO ENTE MERASA UDAH EXPERT, MERASA UDAH PINTER, KALO MERASA... AH POKOKE KALO ENTE ITU UDAH HEBAT, MAKA DILARANG DAN SANGAT TERLARANG MEMBACA TULISAN INI DEMI KEBAIKAN ENTE SENDIRI. PENULIS TIDAK MENJAMIN JIKA ENTE KELAK BAKAL MATI KEBOSANAN KARENA MEMBACA TULISAN INI.

TERIMA KASIH.

TTD

ORANG KEREN

Hmm... bila ente semua udah pada baca artikel penulis sebelumnya tentang "*php-bugs dan permisi file*" sehingga dapat mendeface dalam satu hosting walau target yang aslinya gak sempet kita deface. Nah, mungkin timbul pertanyaan dibenak ente pada... Gimana seh caranya kita tahu and liat nama situs target yang kita deface dalam satu hosting itu.

Hmmmm..... ngerti enggak (-_-) ???

Gini loh, misalnya kita mendapatkan target www.contoh.com trus kita dapatin id yang kita jalankan di target adalah nobody (ini enggak mutlak lho, bisa aja id user yang kita jalankan adalah apache ato www-

data pokoke prinsipnya kite memiliki hak menulis di target). Nah setelah kite cek dan ricek, eh..... kita bisa melakukan mass defacing di sana :P~ (slurpp.....) (ini kalo memang permisi file di target memungkinkan kita untuk melakukan mass defacing tapi kale ente gak bisa ngelakuin mass defacing di target ente, gak ada salahnya buat baca terus ini artikel, sapa tau di sana ente dapatin web jualan misalnya, walo gak bisa deface, paling enggak bisa lah sekedar liat-liat suasana, wakakaka..... ☺☺☺)

Hehehe..... kembali ke pokok masalah, langkah selanjutnya adalah melihat directori aktif kita saat ini. Bukan apa-apa, tujuan sebenarnya dari tindakan ini adalah untuk melihat dimana kita berpijak saat ini, soalnya kebanyakan (bahkan hampir semua target) nyatuin semua directory web dalam satu directory untuk memudahkan administrasi.

```
$pwd

/home/recompil/public_html
```

Lalu kita melihat di sana bahwa directory aktif saat ini adalah /home/recompil/public_html. Jika kita melihat directory aktif target tersebut, maka kita berasumsi bahwa admin menyatukan semua directory web usernya ada di bagian /home.

Lho, kok di bagian /home seeh ??? Bukannya di /home/recompil ???

OK... kita simpan dulu pertanyaan tersebut. Entar kita membahasnya OK.

Lalu langkah kedua adalah melihat daftar user-user web yang berada di bagian directory /home dengan menggunakan command ls –la.

```
$ls -la /home

total 4620
drwxr-xr-x  273 root     root         8192 Aug  4 13:00 .
drwxr-xr-x   16 root     root         4096 Nov 30  2003 ..
drwx--x--x    7 abbeydis abbeydis     4096 Jun 22 07:39 abbeydis
drwxrwxrwx    7 acebroth acebroth     4096 Jun 22 02:28 acebroth
drwxrwxrwx    7 rattanwa rattanwa     4096 Jun 22 05:24 rattanwa
drwx--x--x    7 raygiubi raygiubi     4096 Jun 22 02:28 raygiubi
drwx--x--x   14 recompil recompil     4096 Jun 22 07:09 recompil
```

Nah, itu adalah hasil dari command ls –la di directory /home trus langkah selanjutnya adalah menentukan name site target yang bakal kite deface dalam 1 hosting dengan target asli kite ☺☺☺ Oh iya, tadi ada

yang tanya khan kenape directory web usernya ada di bagian /home dan bukan di bagian /home/recompil. Nah, sebenarnya di bagian /home/recompil ada folder /public_html, file itu memang bawaan yang menjadi ciri khas apache, jadi sebenarnya letak web user itu ada di /home bukannya di /home/recompile. Hmm... belom ngerti juga ya apa yang dimaksud penulis ☹☹☹ memang penulis gak bisa begitu jelas menjelaskan yang penulis maksud, berbelit-belit khan ☹☹☹

OK..... next, kita gak perlu berhenti di sini. Langkah selanjutnya adalah melihat dimana letak httpd.conf target kita. Guna httpd.conf adalah sebagai configurasi apache dalam mengatur server. Lalu tujuan kita mencari httpd.conf itu adalah untuk melihat vhost name server target kita (sebenarnya dari sana langsung bisa juga seh tanpa perlu gunain command pwd ama ls –la segala ☺, tapi kayaknya gak menarik, soalnya entar tulisan ini gak penuh, wekekeke ☺☺☺).

Ada beberapa cara dalam mencari httpd.conf target. Salah satunya adalah :

```
$locate httpd.conf

/etc/httpd/conf/httpd.conf
/etc/httpd/conf/httpd.conf.bak
/etc/httpd/conf/httpd.conf.old
/etc/httpd/conf/httpd.conf.new
```

Jika kita melihat fila hasil output dari command locate, maka jangan dulu bingung file mana yang harus dilihat. Kita ambil file httpd.conf tanpa embel-embel segala sebagi patokan, jadi bukan httpd.conf.bak ato httpd.conf.old. Ingat httpd.conf tanpa embel-embel yah.

Trus, kita liat deh tuh httpd.conf dengan perintah cat, caranya

```
$cat /etc/httpd/conf/httpd.conf

..........
<VirtualHost 66.45.242.178>
ServerAlias www.abbeydistribution.com abbeydistribution.com
ServerAdmin webmaster@abbeydistribution.com
DocumentRoot /home/abbeydis/public_html
BytesLog domlogs/abbeydistribution.com-bytes_log
ServerName www.abbeydistribution.com
User abbeydis
Group abbeydis
CustomLog domlogs/abbeydistribution.com combined
ScriptAlias /cgi-bin/ /home/abbeydis/public_html/cgi-bin/
</VirtualHost>
..........
```

Sebenarnya tampilan file httpd.conf bukan seperti yang ente lihat itu, itu hanya sekedar contoh pada bagian vhost user abbeydis yang memiliki site www.abbeydistribution.com yang meletakkan file-file webnya di directory /home/abbeydis/public_html.

Seep, gimana... udah ngerti khan apa yang penulis maksudkan ☺☺☺

Kalo belom juga ngerti ya wees, cari diri perngertian sendiri, wekekeke... memang penulis terkadang suka banget ngambek ya :P~

Namun, nah ini namun yah... terkadang di beberapa target, command locate malah gak mau jalan, entah itu dikatain bahwa command locate gak ada dalam daftar command-command yang bisa mereka handle-lah ato... pokoke yang jelas mereka ngatain bahwa yang namanya locate itu gak ada, udah digusur kali ama adminnya :P~

Nah, gimana neh kalo seandainya itu yang terjadi ???

Pengalaman penulis sendiri seeh penulis gunain command whereis dengan argumen ke httpd sebagai binnary-nya ato file executenya apache. Jadi command yang penulis jalankan adalah whereis httpd kemudian setelah dapat hasilnya penulis lakukan command cat /<hasil dari command whereis httpd> ditambah dengan /conf/httpd.conf. jadi intinya begini loh :

```
$whereis httpd

/etc/httpd/httpd
```

```
$cat /ect/httpd/conf/httpd.conf

..........
<VirtualHost 66.45.242.178>
ServerAlias www.abbeydistribution.com abbeydistribution.com
ServerAdmin webmaster@abbeydistribution.com
DocumentRoot /home/abbeydis/public_html
BytesLog domlogs/abbeydistribution.com-bytes_log
ServerName www.abbeydistribution.com
User abbeydis
Group abbeydis
CustomLog domlogs/abbeydistribution.com combined
ScriptAlias /cgi-bin/ /home/abbeydis/public_html/cgi-bin/
</VirtualHost>
..........
```

Nah, mungkin ada beberapa teknik lain yang belom penulis kuasai, seperti melihatnya melalui file-file configurasi DNS di target misalnya :P~ tetapi menurut penulis ini sudahlah cukup. Selamat berkarya terus

para newbies..... eh penulis boleh ngiklan dikit gak ??? kalo boleh, penulis mo ngiklanin #kartubeben neh :

gabung-gabung donk ke komunitas kita di channel #kartubeben di server dalnet :P~ wekekekeke.....

OK, See you next time !!!

Greatz : #kartubeben crew @ irc.dal.net
K-159 and all of #aikmel crew and staff
the_day, y3dips and all of #e-c-h-o crew and staff
kevin yang udah banyak membantu penulis
Nixell yang udah berbaik hati kenapa penulis
sam_stradlin , pArMin , CupiD^ , pakcik dan semua yang udah bantu-bantu di #kartubeben
Special : bang mus di Mina Net yang udah ngajarin penulis tentang cara membuat router dan konsep dns di dunia internet walo sekarang penulis udah lupa lagi ☹☹☹

#kartubeben
@ irc.dal.net