

FreeBSD-Security: "sh -i" My server was hacked. How can i found hole on my server?

## "sh -i" My server was hacked. How can i found hole on my server?

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-06/0017.html>

---

*From:* Oleg Rusanov ([frebsd-security\\_at\\_molecon.ru](mailto:frebsd-security_at_molecon.ru))

*Date:* 06/27/05

Date: Mon, 27 Jun 2005 14:21:10 +0400

To: frebsd-security <[frebsd-security@frebsd.org](mailto:frebsd-security@frebsd.org)>

Hello.

My server was hacked. The CPU has been loaded on 99 % by "sh -i" process.  
I found out that someone has started phpshell through a hole in one of phpbb forums.  
Also has filled in scripts for flud and spam and "vadim script" in  
"/tmp". I has made it noexec. Recently has found out the same process.  
May be i have left again /tmp opened, or other hole may be.  
What is better to do for clean my system?

```
amd64# ps aux -H
```

```
USER PID %CPU %MEM VSZ RSS TT STAT STARTED TIME COMMAND
nobody 60138 99.0 0.2 12796 4844 ?? RL 7:11AM 739:26.28 sh -i (perl5.8.6)
```

```
amd64# ps -lp 60138
```

```
UID PID PPID CPU PRI NI VSZ RSS MWCHAN STAT TT TIME COMMAND
65534 60138 1 291 114 0 12796 4844 - R ?? 762:55.06 sh -i (perl5.8.6)
```

```
amd64#
```

(i can not find info about parent process 65534)

```
amd64# sockstat| grep 60138
```

```
nobody perl5.8.6 60138 3 tcp4 my_ip:55000 161.53.178.240:9999
```

```
amd64#
```

```
amd64# lsof -p 60138
```

```
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
perl5.8.6 60138 nobody cwd VDIR 4,13 512 2 /
perl5.8.6 60138 nobody rtd VDIR 4,13 512 2 /
perl5.8.6 60138 nobody txt VREG 4,18 13144 6312845 /usr/local/bin/perl5.8.6
perl5.8.6 60138 nobody txt VREG 4,13 173264 616 /libexec/ld-elf.so.1
perl5.8.6 60138 nobody txt VREG 4,18 1272229 6524324 /usr/local/lib/perl5/5.8.6/mach/CORE/libperl.so
perl5.8.6 60138 nobody txt VREG 4,13 151160 576 /lib/libm.so.3
perl5.8.6 60138 nobody txt VREG 4,13 33024 339 /lib/libcrypt.so.2
perl5.8.6 60138 nobody txt VREG 4,13 52064 583 /lib/libutil.so.4
perl5.8.6 60138 nobody txt VREG 4,13 1055864 585 /lib/libc.so.5
```

"sh -i" My server was hacked. How can i found hole on my server?

## FreeBSD–Security: "sh -i" My server was hacked. How can i found hole on my server?

```
perl5.8.6 60138 nobody txt VREG 4,18 22226 6901089 /usr/local/lib/perl5/5.8.6/mach/auto/IO/IO.so
perl5.8.6 60138 nobody txt VREG 4,18 28921 6901280 /usr/local/lib/perl5/5.8.6/mach/auto/Socket/Socket.so
perl5.8.6 60138 nobody 0r VCHR 2,2 0t0 7 /dev/null
perl5.8.6 60138 nobody 1u PIPE 0x6f537410 0 ->0xfffff006f5372d0
perl5.8.6 60138 nobody 2w VREG 4,18 47856095 6407163 /usr/local/apache/logs/error_log
perl5.8.6 60138 nobody 3u IPv4 0xfffff00168142c0 0t0 TCP
my_hostname:55000->zagreb.hr.eu.undernet.org:9999 (ESTABLISHED)
perl5.8.6 60138 nobody 4u IPv4 0t0 TCP no PCB, CANTSENDMORE, CANTRCVMORE
perl5.8.6 60138 nobody 15w VREG 4,18 47856095 6407163 /usr/local/apache/logs/error_log
perl5.8.6 60138 nobody 18w VREG 4,18 84 6406351 /usr/local/apache/domlogs/my_site.ru-bytes_log
...
apache logs...
```

```
perl5.8.6 60138 nobody 61w VREG 4,18 847357 6407164 /usr/local/apache/logs/ssl_engine_log
perl5.8.6 60138 nobody 62w VREG 4,16 147300 8310 /var/log/my_site.ru
perl5.8.6 60138 nobody 63w VREG 4,18 0 6406441 /usr (/dev/ad4s1f)
perl5.8.6 60138 nobody 109w VREG 4,18 0 6406441 /usr (/dev/ad4s1f)
amd64#
```

```
amd64# fstat -p 60138
USER CMD PID FD MOUNT INUM MODE SZ|DV R/W
nobody perl5.8.6 60138 root / 2 drwxr-xr-x 512 r
nobody perl5.8.6 60138 wd / 2 drwxr-xr-x 512 r
nobody perl5.8.6 60138 text /usr 6312845 -rwxr-xr-x 13144 r
nobody perl5.8.6 60138 0 /dev 7 crw-rw-rw- null r
nobody perl5.8.6 60138 1* pipe ffffff006f537410 <-> ffffff006f5372d0 0 rw
nobody perl5.8.6 60138 2 /usr 6407163 -rw-r--r-- 47853541 w
nobody perl5.8.6 60138 3* internet stream tcp ffffff00168142c0
nobody perl5.8.6 60138 4* internet stream tcp
nobody perl5.8.6 60138 15 /usr 6407163 -rw-r--r-- 47853541 w
nobody perl5.8.6 60138 18 /usr 6406351 -rw-r--r-- 84 w
nobody perl5.8.6 60138 19 /usr 6406445 -rw-r--r-- 177196 w
nobody perl5.8.6 60138 20 /usr 6406367 -rw-r--r-- 273155 w
nobody perl5.8.6 60138 21 /usr 6406346 -rw-r--r-- 68 w
nobody perl5.8.6 60138 22 /usr 6406340 -rw-r--r-- 219769 w
nobody perl5.8.6 60138 23 /usr 6406152 -rw-r--r-- 61985 w
nobody perl5.8.6 60138 24 /usr 6406295 -rw-r--r-- 98621 w
nobody perl5.8.6 60138 25 /usr 6406287 -rw-r--r-- 2558162 w
nobody perl5.8.6 60138 26 /usr 6406284 -rw-r--r-- 32168 w
nobody perl5.8.6 60138 27 /usr 6406292 -rw-r--r-- 265964 w
nobody perl5.8.6 60138 28 /usr 6406213 -rw-r--r-- 1607 w
nobody perl5.8.6 60138 29 /usr 6407351 -rw-r--r-- 347197 w
nobody perl5.8.6 60138 30 /usr 6407377 -rw-r--r-- 140832 w
nobody perl5.8.6 60138 31 /usr 6407290 -rw-r--r-- 935975 w
nobody perl5.8.6 60138 32 /usr 6406393 -rw-r--r-- 5634 w
nobody perl5.8.6 60138 33 /usr 6407328 -rw-r--r-- 51239 w
nobody perl5.8.6 60138 34 /usr 6406252 -rw-r--r-- 12198 w
nobody perl5.8.6 60138 35 /usr 6407325 -rw-r--r-- 13538 w
nobody perl5.8.6 60138 36 /usr 6407319 -rw-r--r-- 23151 w
nobody perl5.8.6 60138 37 /usr 6407322 -rw-r--r-- 16184 w
nobody perl5.8.6 60138 38 /usr 6407341 -rw-r--r-- 146759 w
```

"sh -i" My server was hacked. How can i found hole on my server?

## FreeBSD-Security: "sh -i" My server was hacked. How can i found hole on my server?

```
nobody perl5.8.6 60138 39 /usr 6407329 -rw-r--r-- 36336 w
nobody perl5.8.6 60138 40 /usr 6406423 -rw-r--r-- 43747 w
nobody perl5.8.6 60138 41 /usr 6407330 -rw-r--r-- 95287 w
nobody perl5.8.6 60138 42 /usr 6406425 -rw-r--r-- 28586 w
nobody perl5.8.6 60138 43 /usr 6406223 -rw-r--r-- 210 w
nobody perl5.8.6 60138 44 /usr 6407166 -rw-r--r-- 613177 w
nobody perl5.8.6 60138 45 /usr 6406160 -rw-r--r-- 0 w
nobody perl5.8.6 60138 46 /usr 6406166 -rw-r--r-- 123158 w
nobody perl5.8.6 60138 47 /usr 6407974 -rw-r--r-- 272 w
nobody perl5.8.6 60138 48 /usr 6407952 -rw-r--r-- 196 w
nobody perl5.8.6 60138 49 /usr 6407915 -rw-r--r-- 49313 w
nobody perl5.8.6 60138 50 /usr 6407942 -rw-r--r-- 170924 w
nobody perl5.8.6 60138 51 /usr 6407933 -rw-r--r-- 1496129 w
nobody perl5.8.6 60138 52 /usr 6407931 -rw-r--r-- 202140 w
nobody perl5.8.6 60138 53 /usr 6407924 -rw-r--r-- 342351 w
nobody perl5.8.6 60138 54 /usr 6407913 -rw-r--r-- 23547 w
nobody perl5.8.6 60138 55 /usr 6407288 -rw-r--r-- 18729 w
nobody perl5.8.6 60138 56 /usr 6407289 -rw-r--r-- 377903 w
nobody perl5.8.6 60138 57 /usr 6407166 -rw-r--r-- 613177 w
nobody perl5.8.6 60138 58 /usr 6407175 -rw-r--r-- 4526 w
nobody perl5.8.6 60138 59 /usr 6407171 -rw-r--r-- 373516 w
nobody perl5.8.6 60138 60 /usr 6407181 -rw-r--r-- 49888 w
nobody perl5.8.6 60138 61 /usr 6407164 -rw-r--r-- 847357 w
nobody perl5.8.6 60138 62 /var 8310 -rw-r--r-- 147300 w
nobody perl5.8.6 60138 63 /usr 6406441 -rw----- 0 w
nobody perl5.8.6 60138 109 /usr 6406441 -rw----- 0 w
amd64#
```

then i kill -9 60138 process, its restart with other number - 86717, and i rebooted for kill him.

```
amd64# lsof -i -n | grep 86717
perl5.8.6 86717 nobody 3u IPv4 0xfffff004b465000 0t0 TCP my_ip:53650->161.53.178.240:9999
(ESTABLISHED)
perl5.8.6 86717 nobody 4u IPv4 0t0 TCP no PCB, CANTSENDMORE, CANTRCVMORE
amd64#
```

How can i found hole on my server?

--

Regards,

Oleg

mailto:freebsd-security@molecon.ru

---

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"