

SSH蜜罐 :kippo

2012-10-24 20:58:54 By admin

前言

蜜罐好比是情报收集系统。蜜罐好像是故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后，你就可以知道他是如何得逞的

蜜网是指另外采用了技术的蜜罐，从而以合理方式记录下黑客的行动，同时尽量减小或排除对因特网上其它系统造成的风险。建立在反向防火墙后面的蜜罐就是一个例子。防火墙的目的不是防止入站连接，而是防止蜜罐建立出站连接。不过，虽然这种方法使蜜罐不会破坏其它系统，但同时很容易被黑客发现。

数据收集是设置蜜罐的另一项技术挑战。蜜罐监控者只要记录下进出系统的每个数据包，就能够对黑客的所作所为了一清二楚。蜜罐本身上面的日志文件也是很好的数据来源。但日志文件很容易被攻击者删除，所以通常的办法就是让蜜罐向在同一网络上但防御机制较完善的远程系统日志服务器发送日志备份。（务必同时监控日志服务器。如果攻击者用新手法闯入了服务器，那么蜜罐无疑会证明其价值。）

蜜罐系统的优点之一就是它们大大减少了所要分析的数据。对于通常的网站或邮件服务器，攻击流量通常会被合法流量所淹没。而蜜罐进出的数据大部分是攻击流量。因而，浏览数据、查明攻击者的实际行为也就容易多了。

自1999年启动以来，蜜网计划已经收集到了大量信息。部分发现结果包括：攻击率在过去一年增加了一倍；攻击者越来越多地使用能够堵住漏洞的自动点击工具（如果发现新漏洞，工具很容易更新）；尽管虚张声势，但很少有黑客采用新的攻击手法。

打开SERVER

安装

```
root@ubuntu:~# mkdir kippo
root@ubuntu:~# apt-get install python-dev openssl python-openssl python-pyasn1 python-twisted python-mysqldb
```

获得源代码

```
root@ubuntu:~# cd kippo/
root@ubuntu:~/kippo# svn checkout http://kippo.googlecode.com/svn/trunk/ .
```

添加一个独立的用户组给KIPPO

```
root@ubuntu:~/kippo# useradd -s /bin/bash -d /home/kippo -m kippo
```

添加一个独立的MYSQL用户给KIPPO

```
root@ubuntu:~/kippo# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 34
Server version: 5.1.61-0ubuntu0.10.10.1-log (Ubuntu)
```

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
mysql> CREATE DATABASE kippo;
Query OK, 1 row affected (0.00 sec)
mysql> GRANT ALL ON kippo.* to 'kippo'@'localhost' identified by '123456';
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> show databases;
```

```
+-----+
| Database |
+-----+
| information_schema |
| kippo          |
| mysql          |
| pentest        |
+-----+
4 rows in set (0.01 sec)
```

```
mysql>
```

帐号和数据库一样 密码123456

导入默认数据库 #本文地址http://fuzzexp.org/ssh_honeypot_kippo.html

```
root@ubuntu:~/kippo# cd doc/sql/
root@ubuntu:~/kippo/doc/sql# ls
mysql.sql update2.sql update3.sql update4.sql update5.sql update6.sql
root@ubuntu:~/kippo/doc/sql# mysql -ukippo -p123456 kippo < mysql.sql
```

编辑配置

kippo.cfg.dist

```
root@ubuntu:~/kippo# mv kippo.cfg.dist kippo.cfg
```

编辑他 我的如下 :

```
root@ubuntu:~/kippo# cat kippo.cfg
#
# Kippo configuration file (kippo.cfg)
#
```

```
[honeypot]
```

```
# IP addresses to listen for incoming SSH connections.
#
# (default: 0.0.0.0) = any address
ssh_addr = 0.0.0.0
```

```
# Port to listen for incoming SSH connections.
#
# (default: 2222)
ssh_port = 2222
```

```
# Hostname for the honeypot. Displayed by the shell prompt of the virtual
# environment.
#
# (default: sales)
hostname = ubuntu
```

```
# Directory where to save log files in.
#http://fuzzexp.org/?p=5571
# (default: log)
log_path = log
```

```
# Directory where to save downloaded (malware) files in.
#
# (default: dl)
download_path = dl
```

```
# Directory where virtual file contents are kept in.
#
# This is only used by commands like 'cat' to display the contents of files.
# Adding files here is not enough for them to appear in the honeypot - the
# actual virtual filesystem is kept in filesystem_file (see below)
#
# (default: honeyfs)
contents_path = honeyfs
```

```
# File in the python pickle format containing the virtual filesystem.
#
```

```
# This includes the filenames, paths, permissions for the whole filesystem,
# but not the file contents. This is created by the createfs.py utility from
# a real template linux installation.
#
# (default: fs.pickle)
filesystem_file = fs.pickle

# Directory for miscellaneous data files, such as the password database.
#
# (default: data_path)
data_path = data

# Directory for creating simple commands that only output text.
#
# The command must be placed under this directory with the proper path, such
# as:
#   txtcmds/usr/bin/vi
# The contents of the file will be the output of the command when run inside
# the honeypot.
#
# In addition to this, the file must exist in the virtual
# filesystem {filesystem_file}
# 本文地址http://fuzzexp.org/ssh\_honeypot\_kippo.html
# (default: txtcmds)
txtcmds_path = txtcmds

# Public and private SSH key files. If these don't exist, they are created
# automatically.
#
# (defaults: public.key and private.key)
public_key = public.key
private_key = private.key

# Initial root password. NO LONGER USED!
# Instead, see {data_path}/userdb.txt
password = 123456

# IP address to bind to when opening outgoing connections. Used exclusively by
# the wget command.
#
# (default: not specified)
out_addr = 0.0.0.0

# Sensor name use to identify this honeypot instance. Used by the database
# logging modules such as mysql.
#
# If not specified, the logging modules will instead use the IP address of the
# connection as the sensor name.
#
# (default: not specified)
```

```
#sensor_name=myhostname

# Fake address displayed as the address of the incoming connection.
# This doesn't affect logging, and is only used by honeypot commands such as
# 'w' and 'last'
#
# If not specified, the actual IP address is displayed instead (default
# behaviour).
#
# (default: not specified)
#fake_addr = 192.168.66.254

# Banner file to be displayed before the first login attempt.
#
# (default: not specified)
#banner_file =

# Session management interface.
#
# This is a telnet based service that can be used to interact with active
# sessions. Disabled by default.
#
# (default: false)
interact_enabled = false
# (default: 5123)
interact_port = 5123

# MySQL logging module
#
# Database structure for this module is supplied in doc/sql/mysql.sql
#
# To enable this module, remove the comments below, including the
# [database_mysql] line.

[database_mysql]
host = localhost
database = kippo
username = kippo
password = 123456

# XMPP Logging
#
# Log to an xmpp server.
# For a detailed explanation on how this works, see:
#
# To enable this module, remove the comments below, including the
# [database_xmpp] line.

#[database_xmpp]
#server = sensors.carnivore.it
```

```
#user = anonymous@sensors.carnivore.it
#password = anonymous
#muc = dionaea.sensors.carnivore.it
#signal_createsession = kippo-events
#signal_connectionlost = kippo-events
#signal_loginfailed = kippo-events
#signal_loginsucceeded = kippo-events
#signal_command = kippo-events
#signal_clientversion = kippo-events
#debug=true
root@ubuntu:~/kippo#
```

安装监听工具

```
root@ubuntu:~/kippo# apt-get install authbind
```

配置

```
root@ubuntu:~/kippo# chown kippo:kippo /etc/authbind/byport/22
root@ubuntu:~/kippo# chmod 777 /etc/authbind/byport/22
root@ubuntu:~/kippo# chown -R kippo:kippo /root/kippo/
```

创建一个启动脚本

```
root@ubuntu:~/kippo# echo "twistd -y kippo.tac -l log/kippo.log --pidfile kippo.pid" > 1.sh
root@ubuntu:~/kippo# cat 1.sh
twistd -y kippo.tac -l log/kippo.log --pidfile kippo.pid
root@ubuntu:~/kippo#
```

移动工具位置

```
root@ubuntu:~# mv kippo/ /opt/
root@ubuntu:~# cd /opt/
root@ubuntu:/opt# ls
kippo
root@ubuntu:/opt# cd kippo/
```

更改下KIPPO用户密码 切换到[KIPPO](#)

```
root@ubuntu:~/kippo# passwd kippo
```

```
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
root@ubuntu:~/kippo# su kippo  
kippo@ubuntu:/root/kippo$ id  
uid=1002(kippo) gid=1002(kippo) groups=1002(kippo)  
kippo@ubuntu:/root/kippo$
```

启动

```
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:25 cervical sshd[27066]: Invalid user julia from 85.62.8.13
Sep 17 22:37:25 cervical sshd[27066]: error: Could not get shadow information for NOUSER
Sep 17 22:37:25 cervical sshd[27066]: Failed password for invalid user julia from 85.62.8.13 port 33067 ssh2
Sep 17 22:37:26 cervical sshd[27068]: reverse mapping checking getaddrinfo for 85.62.8.13.static.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:26 cervical sshd[27068]: Invalid user julial23 from 85.62.8.13
Sep 17 22:37:26 cervical sshd[27068]: error: Could not get shadow information for NOUSER
Sep 17 22:37:26 cervical sshd[27068]: Failed password for invalid user julial23 from 85.62.8.13 port 33222 ssh2
Sep 17 22:37:27 cervical sshd[27070]: reverse mapping checking getaddrinfo for 85.62.8.13.static.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:27 cervical sshd[27070]: Invalid user a from 85.62.8.13
Sep 17 22:37:27 cervical sshd[27070]: error: Could not get shadow information for NOUSER
Sep 17 22:37:27 cervical sshd[27070]: Failed password for invalid user a from 85.62.8.13 port 33365 ssh2
Sep 17 22:37:30 cervical sshd[27072]: reverse mapping checking getaddrinfo for 85.62.8.13.static.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:30 cervical sshd[27072]: Invalid user julie from 85.62.8.13
Sep 17 22:37:30 cervical sshd[27072]: error: Could not get shadow information for NOUSER
Sep 17 22:37:30 cervical sshd[27072]: Failed password for invalid user julie from 85.62.8.13 port 33488 ssh2
Sep 17 22:37:31 cervical sshd[27074]: reverse mapping checking getaddrinfo for 85.62.8.13.static.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:31 cervical sshd[27074]: Invalid user juliel23 from 85.62.8.13
Sep 17 22:37:31 cervical sshd[27074]: error: Could not get shadow information for NOUSER
Sep 17 22:37:31 cervical sshd[27074]: Failed password for invalid user juliel23 from 85.62.8.13 port 35041 ssh2
Sep 17 22:37:32 cervical sshd[27076]: reverse mapping checking getaddrinfo for 85.62.8.13.static.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:32 cervical sshd[27076]: Invalid user a from 85.62.8.13
Sep 17 22:37:32 cervical sshd[27076]: error: Could not get shadow information for NOUSER
Sep 17 22:37:32 cervical sshd[27076]: Failed password for invalid user a from 85.62.8.13 port 35757 ssh2
Sep 17 22:37:32 cervical sshd[27078]: reverse mapping checking getaddrinfo for 85.62.8.13.static.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:32 cervical sshd[27078]: Invalid user june from 85.62.8.13
Sep 17 22:37:32 cervical sshd[27078]: error: Could not get shadow information for NOUSER
Sep 17 22:37:32 cervical sshd[27078]: Failed password for invalid user june from 85.62.8.13 port 35930 ssh2
Sep 17 22:37:33 cervical sshd[27080]: reverse mapping checking getaddrinfo for 85.62.8.13.static.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:33 cervical sshd[27080]: Invalid user junel23 from 85.62.8.13
Sep 17 22:37:33 cervical sshd[27080]: error: Could not get shadow information for NOUSER
Sep 17 22:37:33 cervical sshd[27080]: Failed password for invalid user junel23 from 85.62.8.13 port 36297 ssh2
Sep 17 22:37:34 cervical sshd[27082]: reverse mapping checking getaddrinfo for 85.62.8.13.static.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:34 cervical sshd[27082]: Invalid user a from 85.62.8.13
Sep 17 22:37:34 cervical sshd[27082]: error: Could not get shadow information for NOUSER
Sep 17 22:37:34 cervical sshd[27082]: Failed password for invalid user a from 85.62.8.13 port 36423 ssh2
Sep 17 22:37:35 cervical sshd[27084]: reverse mapping checking getaddrinfo for 85.62.8.13.static.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
```

```
kippo@ubuntu:/opt/kippo$ pwd
```

```
/opt/kippo
```

```
kippo@ubuntu:/opt/kippo$ ./start.sh
```

```
Starting kippo in background...Loading dblog engine: mysql
```

```
Generating RSA keypair...
```


done.

查看监听

```

2011-03-20 17:26:03-0700 [SSHSservice ssh-userauth on HoneyPotTransport,2,202 116.8.64] root trying auth password
2011-03-20 17:26:04-0700 [SSHSservice ssh-userauth on HoneyPotTransport,2,202 116.8.64] login attempt [root/P@ssw0rd] failed
2011-03-20 17:26:05-0700 [HoneyPotTransport,2,202 116.8.64] Got remote error, code 11
2011-03-20 17:26:05-0700 [HoneyPotTransport,2,202 116.8.64] connection lost [Kippo, I have run Kippo for couple of days. Its
2011-03-20 17:26:05-0700 [Kippo.core.honeypot.HoneyPotSSHFactory] New connection: 202.116.8.64:57507 (192.168.0.105:2222) [session: 3]
2011-03-20 17:26:06-0700 [HoneyPotTransport,3,202 116.8.64] Remote SSH version: SSH-2.0-libssh-0.1
2011-03-20 17:26:06-0700 [HoneyPotTransport,3,202 116.8.64] kex alg, key alg: diffie-hellman-group1-sha1 ssh-rsa
2011-03-20 17:26:06-0700 [HoneyPotTransport,3,202 116.8.64] outgoing: aes256-cbc hmac-sha1 none has been use for that malicious
2011-03-20 17:26:06-0700 [HoneyPotTransport,3,202 116.8.64] incoming: aes256-cbc hmac-sha1 none
2011-03-20 17:26:06-0700 [HoneyPotTransport,3,202 116.8.64] NEW KEYS
2011-03-20 17:26:06-0700 [HoneyPotTransport,3,202 116.8.64] starting service ssh-userauth
2011-03-20 17:26:07-0700 [SSHSservice ssh-userauth on HoneyPotTransport,3,202 116.8.64] root trying auth password
2011-03-20 17:26:07-0700 [SSHSservice ssh-userauth on HoneyPotTransport,3,202 116.8.64] login attempt [root/password] failed
2011-03-20 17:26:08-0700 [HoneyPotTransport,3,202 116.8.64] Got remote error, code 11
2011-03-20 17:26:08-0700 [HoneyPotTransport,3,202 116.8.64] connection lost
2011-03-20 17:26:08-0700 [Kippo.core.honeypot.HoneyPotSSHFactory] New connection: 202.116.8.64:57646 (192.168.0.105:2222) [session: 4]
2011-03-20 17:26:09-0700 [HoneyPotTransport,4,202 116.8.64] Remote SSH version: SSH-2.0-libssh-0.1
2011-03-20 17:26:09-0700 [HoneyPotTransport,4,202 116.8.64] kex alg, key alg: diffie-hellman-group1-sha1 ssh-rsa
2011-03-20 17:26:09-0700 [HoneyPotTransport,4,202 116.8.64] outgoing: aes256-cbc hmac-sha1 none
2011-03-20 17:26:09-0700 [HoneyPotTransport,4,202 116.8.64] incoming: aes256-cbc hmac-sha1 none
2011-03-20 17:26:09-0700 [HoneyPotTransport,4,202 116.8.64] NEW KEYS
2011-03-20 17:26:09-0700 [HoneyPotTransport,4,202 116.8.64] starting service ssh-userauth
2011-03-20 17:26:09-0700 [SSHSservice ssh-userauth on HoneyPotTransport,4,202 116.8.64] root trying auth password
2011-03-20 17:26:09-0700 [SSHSservice ssh-userauth on HoneyPotTransport,4,202 116.8.64] login attempt [root/1qaz2wsx] failed

```

kippo@ubuntu:/opt/kippo\$ netstat -antp

(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:587	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:2222	0.0.0.0:*	LISTEN	4615/python
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN	-
tcp	0	0	192.168.71.130:22	192.168.71.129:44874	ESTABLISHED	-
tcp6	0	0	:::22	:::*	LISTEN	-

kippo@ubuntu:/opt/kippo\$

tcp 0 0 0.0.0.0:2222 0.0.0.0:* LISTEN 4615/python

查找进程

kippo@ubuntu:/opt/kippo\$ ps -ef | grep 4615

```

kippo 4615 1 0 13:47 ? 00:00:00 /usr/bin/python /usr/bin/twistd -y kippo.tac -l log/kippo.log -
-pidfile kippo.pid
kippo 4626 4588 0 13:48 pts/0 00:00:00 grep --color=auto 4615
kippo@ubuntu:/opt/kippo$

```

扫描下UB kippo的配置文件端口定义为2222

```
root@Dis9Team:~# nmap -sV 192.168.71.130 -p 2222
```

```
Starting Nmap 5.51 ( http://nmap.org ) at 2012-10-11 22:51 PDT
```

```
Nmap scan report for 192.168.71.130
```

```
Host is up (0.00024s latency).
```

```
PORT      STATE SERVICE VERSION
```

```
2222/tcp open  ssh      OpenSSH 5.1p1 Debian 5 (protocol 2.0)
```

```
MAC Address: 00:0C:29:9E:3F:14 (VMware)
```

```
Service Info: OS: Linux
```

```
Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

```
root@Dis9Team:~#
```

OPENSSH服务出现了.

kippo的配置文件的密码定义为123456 测试一下

#本文地址http://fuzzexp.org/ssh_honeypot_kippo.html

```
root@Dis9Team:~# ssh root@192.168.71.130 -p2222
```

```
The authenticity of host '[192.168.71.130]:2222 ([192.168.71.130]:2222)' can't be established.
```

```
RSA key fingerprint is d9:f0:74:99:58:5e:32:74:a1:7b:27:78:2e:b1:83:a8.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added '[192.168.71.130]:2222' (RSA) to the list of known hosts.
```

```
Password:
```

```
Password:
```

```
ubuntu:~# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
ubuntu:~#
```

邪恶的操作

```
ubuntu:~# ls /
```

```
sys    bin    mnt     media  vmlinuz  opt      cdrom  selinux  tmp     proc    sbin  
etc    dev    srv     initrd.img  lib      home    var    usr      boot   root    lost+found
```

```
ubuntu:~# ls -la /
```

```
drwxr-xr-x 1 root root 4096 2012-10-12 13:53 .
```

```
drwxr-xr-x 1 root root 4096 2012-10-12 13:53 ..
```

```
drwxr-xr-x 1 root root  0 2009-11-20 16:19 sys
```

```
drwxr-xr-x 1 root root 4096 2009-11-08 23:42 bin
```

```
drwxr-xr-x 1 root root 4096 2009-11-06 19:08 mnt
```

```
drwxr-xr-x 1 root root 4096 2009-11-06 19:08 media
lrwxrwxrwx 1 root root 25 2009-11-06 19:16 vmlinuz -> /boot/vmlinuz-2.6.26-2-686
drwxr-xr-x 1 root root 4096 2009-11-06 19:09 opt
lrwxrwxrwx 1 root root 11 2009-11-06 19:08 cdrom -> /media/cdrom0
drwxr-xr-x 1 root root 4096 2009-11-06 19:08 selinux
drwxrwxrwx 1 root root 4096 2009-11-20 16:19 tmp
dr-xr-xr-x 1 root root 0 2009-11-20 16:19 proc
drwxr-xr-x 1 root root 4096 2009-11-08 23:41 sbin
drwxr-xr-x 1 root root 4096 2009-11-20 16:20 etc
drwxr-xr-x 1 root root 3200 2009-11-20 16:20 dev
drwxr-xr-x 1 root root 4096 2009-11-06 19:09 srv
lrwxrwxrwx 1 root root 28 2009-11-06 19:16 initrd.img -> /boot/initrd.img-2.6.26-2-686
drwxr-xr-x 1 root root 4096 2009-11-08 23:46 lib
drwxr-xr-x 1 root root 4096 2009-11-06 19:22 home
drwxr-xr-x 1 root root 4096 2009-11-06 19:09 var
drwxr-xr-x 1 root root 4096 2009-11-08 23:46 usr
drwxr-xr-x 1 root root 4096 2009-11-08 23:39 boot
drwxr-xr-x 1 root root 4096 2009-11-20 17:08 root
drwx----- 1 root root 16384 2009-11-06 19:08 lost+found
ubuntu:~#
```

删除全部文件

```
ubuntu:~# rm -rf /
ubuntu:~# ls -ls /
drwxr-xr-x 1 root root 4096 2012-10-12 13:53 .
drwxr-xr-x 1 root root 4096 2012-10-12 13:53 ..
drwxr-xr-x 1 root root 0 2009-11-20 16:19 sys
drwxr-xr-x 1 root root 4096 2009-11-08 23:42 bin
drwxr-xr-x 1 root root 4096 2009-11-06 19:08 mnt
drwxr-xr-x 1 root root 4096 2009-11-06 19:08 media
lrwxrwxrwx 1 root root 25 2009-11-06 19:16 vmlinuz -> /boot/vmlinuz-2.6.26-2-686
drwxr-xr-x 1 root root 4096 2009-11-06 19:09 opt
lrwxrwxrwx 1 root root 11 2009-11-06 19:08 cdrom -> /media/cdrom0
drwxr-xr-x 1 root root 4096 2009-11-06 19:08 selinux
drwxrwxrwx 1 root root 4096 2009-11-20 16:19 tmp
dr-xr-xr-x 1 root root 0 2009-11-20 16:19 proc
drwxr-xr-x 1 root root 4096 2009-11-08 23:41 sbin
drwxr-xr-x 1 root root 4096 2009-11-20 16:20 etc
drwxr-xr-x 1 root root 3200 2009-11-20 16:20 dev
drwxr-xr-x 1 root root 4096 2009-11-06 19:09 srv
lrwxrwxrwx 1 root root 28 2009-11-06 19:16 initrd.img -> /boot/initrd.img-2.6.26-2-686
drwxr-xr-x 1 root root 4096 2009-11-08 23:46 lib
drwxr-xr-x 1 root root 4096 2009-11-06 19:22 home
drwxr-xr-x 1 root root 4096 2009-11-06 19:09 var
drwxr-xr-x 1 root root 4096 2009-11-08 23:46 usr
drwxr-xr-x 1 root root 4096 2009-11-08 23:39 boot
drwxr-xr-x 1 root root 4096 2009-11-20 17:08 root
```

```
drwx----- 1 root root 16384 2009-11-06 19:08 lost+found
ubuntu:~#
```

删除不了 读下默认文件

```
ubuntu:~# cat /etc/shadow
cat: /etc/shadow: No such file or directory
ubuntu:~# cat /etc/shadow-
cat: /etc/shadow-: No such file or directory
ubuntu:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
richard:x:1000:1000:richard,,,:/home/richard:/bin/bash
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
ubuntu:~#
```

不是系统的 估计是伪造的

一些操作都记录到MYSQL数据库里面 [链接看看](#)

```
mysql> select * from sessions;
```

id	starttime	endtime	sensor	ip	termsize	client
04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:01:41	NULL	1	192.168.211.128	161x34	1

```
1 row in set (0.00 sec)
```



```
mysql> select * from input;
```

id	session	timestamp	realm	success	input
1	8223fe4c6f1d11e0b61f000c29fbd3ab	2011-04-25 10:01:13	NULL	1	exit
2	8223fe4c6f1d11e0b61f000c29fbd3ab	2011-04-25 10:01:15	NULL	1	exit
3	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:01:54	NULL	0	hello
4	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:01:55	NULL	0	sadf
5	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:01:56	NULL	0	sdag
6	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:01:58	NULL	0	df -l
7	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:02:01	NULL	0	halt
8	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:02:03	NULL	1	pwd
9	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:02:04	NULL	1	cd
10	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:02:05	NULL	1	cd
11	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:02:07	NULL	1	ls
12	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:02:09	NULL	1	touch haha
13	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:02:11	NULL	1	ls
14	04cc194c6f2311e0b61f000c29fbd3ab	2011-04-25 10:02:13	NULL	0	ll

```
kippo@ubuntu:/opt/kippo$ mysql -u kippo -p
```

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 41

Server version: 5.1.61-0ubuntu0.10.10.1-log (Ubuntu)

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
mysql>
```

查下破解记录 #本文地址http://fuzzexp.org/ssh_honeypot_kippo.html

```
mysql> use kippo;
```

Reading table information for completion of table and column names

You can turn off this feature to get a quicker startup with -A

Database changed

```
mysql> select * from auth;
```

id	session	success	username	password	timestamp
1	0c592448143111e287c0000c299e3f14	0	root	dfsdfds	2012-10-12 05:52:51

```
| 2 | 0c592448143111e287c0000c299e3f14 | 1 | root | 123456 | 2012-10-12 05:52:54 |
+---+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

mysql>

操作记录

mysql> select * from input;

```
+---+-----+-----+-----+-----+-----+
| id | session                | timestamp      | realm | success | input              |
+---+-----+-----+-----+-----+-----+
| 1 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:52:56 | NULL | 1 | id
|
| 2 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:53:28 | NULL | 1 | ls /
|
| 3 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:53:34 | NULL | 1 | ls -la /
|
| 4 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:53:47 | NULL | 1 | rm -rf /
|
| 5 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:53:50 | NULL | 1 | ls -ls /
|
| 6 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:54:23 | NULL | 1 | echo "hacked by
helen" > 1 |
| 7 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:54:25 | NULL | 1 | cat 1
|
| 8 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:54:31 | NULL | 1 | echo "hacked by
helen" > > 1 |
| 9 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:54:37 | NULL | 1 | ls
|
| 10 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:54:39 | NULL | 1 | ls
|
| 11 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:54:40 | NULL | 1 | ls -la
|
| 12 | 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:54:41 | NULL | 1 | pwd
|
+---+-----+-----+-----+-----+-----+
12 rows in set (0.00 sec)
```

mysql>

会话记录

mysql> select * from sessions;

```
+-----+-----+-----+-----+-----+-----+
| id          | starttime      | endtime        | sensor | ip          | termsize | client |
+-----+-----+-----+-----+-----+-----+
```

```
+-----+-----+-----+-----+-----+-----+
| cb9ef50e143011e287c0000c299e3f14 | 2012-10-12 05:50:58 | NULL          | 1 | 192.168.71.12
9 | NULL | NULL |
| df36bce6143011e287c0000c299e3f14 | 2012-10-12 05:51:31 | 2012-10-12 05:51:31 | 1 | 192.168
.71.129 | NULL | NULL |
| ec4e7748143011e287c0000c299e3f14 | 2012-10-12 05:51:53 | NULL          | 1 | 192.168.71.1
29 | NULL | NULL |
| 0c592448143111e287c0000c299e3f14 | 2012-10-12 05:52:46 | NULL          | 1 | 192.168.71.1
29 | 124x37 | 1 |
+-----+-----+-----+-----+-----+-----+
4 rows in set (0.00 sec)
```

mysql>

参考

<http://fuzzexp.org/Wiki/notepad/a-virtual-honeypot-framework>

<http://fuzzexp.org/Wiki/notepad/honeypot>

版权声明：

本站遵循 [署名-非商业性使用-相同方式共享 2.5](#) 共享协议。

转载请注明转自[Dis9 Team](#)并标明URL。

本文链接 <http://fuzzexp.org/?p=5571>