Honeypots, IDS y viceversa 😏

Estos viceversos no

Para qué tener estos sistemas

(Si aquí todos somos buenos □)

Para qué tener estos sistemas

- Detectar problemas en equipos de nuestra red.
- Detectar ataques desde y/o hacia nuestra red.
- Conocer los tipos de ataques y la sofisticación de ellos.

Qué hemos hecho

Qué hemos hecho

- Configurar un IDS (EasyIDS con Snort).
- Configurar un Honeypot (Honeydrive con Kippo).
- Generar ataques de prueba y ver qué nos mostraban.
- Analizar desde el punto de vista del atacante si estos sistemas se detectan fácilmente.

Kippo

Incluido en Honeydrive

Honeypot Kippo

- Honeypot altamente configurable
- Instalación y uso sencillo
- Específico para las conexiones ssh
- Desarrollado en Python y Twisted

Instalación y configuración de Kippo

- >git clone https://github.com/desaster/kippo.git
- Librerias: Twisted, PyCrypto y service_identity Zope
- Kippo.cfg

11

Kippo.cfg

*kippo.cfg [honeydrive@honeydrive: ~] [kippo - File Manager] Fri, 26 May 01:08 honeydrive

*kippo.cfg

File Edit Search Options Help

```
[honeypot]
ssh_port = 2222

hostname = PROServer

log_path = log

download_path = dl

contents_path = honeyfs

filesystem_file = fs.pickle

data_path = data

txtcmds_path = txtcmds

rsa_public_key = data/ssh_host_rsa_key.pub

rsa_private_key = data/ssh_host_rsa_key

dsa_public_key = data/ssh_host_dsa_key.pub

dsa_private_key = data/ssh_host_dsa_key

exec_enabled = true

fake_addr = 192.168.0.168

ssh_version_string = SSH-2.0-OpenSSH_5.5p1 Debian-6+squeeze2

interact_enabled = true
interact_port = 5000
```

Ctrl Derecho

```
honeydrive@honeydrive:~/Desktop/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 0.0.0.0:23              0.0.0.0:*               LISTEN
   -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
   -
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN
   2575/python
tcp        0      0 127.0.0.1:27017         0.0.0.0:*               LISTEN
   -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
   -
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN
   2575/python
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
   -
tcp        0      0 127.0.0.1:28017         0.0.0.0:*               LISTEN
   -
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
   -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
   -
tcp        0      0 192.168.0.175:2222      192.168.0.158:44516     ESTABLISH
ED 2575/python
tcp6       0      0 :::22                   :::*                    LISTEN
   -
honeydrive@honeydrive:~/Desktop/kippo$
```

- Start.sh
- netstat -antp

kippo.log [honeydrive@honeydrive: ~... log - File Manager

kippo.log

File Edit Search Options Help

```
2017-05-14 19:10:34+0100 [-] Log opened.
2017-05-14 19:10:34+0100 [-] twistd 11.1.0 (/usr/bin/python 2.7.3) starting up.
2017-05-14 19:10:34+0100 [-] reactor class: twisted.internet.pollreactor.PollReactor.
2017-05-14 19:10:34+0100 [-] HoneyPotSSHFactory starting on 2222
2017-05-14 19:10:34+0100 [-] Starting factory <kippo.core.ssh.HoneyPotSSHFactory
instance at 0xa2d828c>
2017-05-14 19:10:34+0100 [-] Factory starting on 5000
2017-05-14 19:10:34+0100 [-] Starting factory <twisted.internet.protocol.Factory
instance at 0xaa2f60c>
```

- sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-port 2222

```
root@PROServer:~# whoami
root
root@PROServer:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:4c:a8:ab:32:f4
          inet addr:10.98.55.4  Bcast:10.98.55.255  Mask:255.255.255.0
          inet6 addr: fe80::21f:c6ac:fd44:24d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84045991 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103776307 errors:0 dropped:0 overruns:0 carrier:2
          collisions:0 txqueuelen:1000
          RX bytes:50588302699 (47.1 GiB)  TX bytes:97318807157 (90.6 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:308297 errors:0 dropped:0 overruns:0 frame:0
          TX packets:308297 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:355278106 (338.8 MiB)  TX bytes:355278106 (338.8 MiB)
root@PROServer:~#
```

- ssh 192.168.0.175
- txtcmds_path

HoneyDrive 3 [Corriendo] - Oracle VM VirtualBox

honeydrive@honeydrive: ~... Mon, 29 May 11:22

honeydrive@honeydrive: ~/Desktop/kippo

honeydrive@honeydrive: ~/Desktop/kippo 77x22

```
honeydrive@honeydrive:~/Desktop/kippo$ telnet -e q localhost 5000
Telnet escape character is 'q'.
Trying 127.0.0.1...
Connected to localhost.
Escape character is 'q'.
*** kippo session management console ***
List of commands:
 list       - list all active sessions
 view       - attach to a session in read-only mode
 hijack     - attach to a session in interactive mode
 disconnect - disconnect a session
 help       - this help
 exit       - disconnect the console
```

```
list
ID   clientIP        clientVersion
3    192.168.0.158   SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8
```

- telnet -e q localhost 5000
- List
- View
- Hijack

patri@Ubuntu14: ~

```
-rw-r--r-- 1 root root  140 2013-04-05 12:52 .profile
drwx------ 1 root root 4096 2013-04-05 13:05 .ssh
drwx------ 1 root root 4096 2013-04-05 12:58 .aptitude
-rw-r--r-- 1 root root  570 2013-04-05 12:52 .bashrc
drwxr-xr-x 1 root root 4096 2017-05-28 18:22 gggfh
root@PROServer:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:4c:a8:ab:32:f4
          inet addr:10.98.55.4  Bcast:10.98.55.255  Mask:255.255.255.0
          inet6 addr: fe80::21f:c6ac:fd44:24d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84045991 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103776307 errors:0 dropped:0 overruns:0 carrier:2
          collisions:0 txqueuelen:1000
          RX bytes:50588302699 (47.1 GiB)  TX bytes:97318807157 (90.6 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:308297 errors:0 dropped:0 overruns:0 frame:0
          TX packets:308297 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:355278106 (338.8 MiB)  TX bytes:355278106 (338.8 MiB)
root@PROServer:~#
```

honeydri... [bin - File ... Sun, 28 May 18:30 honeydriv

honeydrive@honeydrive: /bin

honeydrive@honeydrive: /bin 77x22

```
drwx------ 1 root root 4096 2013-04-05 12:58 .aptitude
-rw-r--r-- 1 root root  570 2013-04-05 12:52 .bashrc
drwxr-xr-x 1 root root 4096 2017-05-28 18:22 gggfh
root@PROServer:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:4c:a8:ab:32:f4
          inet addr:10.98.55.4  Bcast:10.98.55.255  Mask:255.255.255.0
          inet6 addr: fe80::21f:c6ac:fd44:24d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84045991 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103776307 errors:0 dropped:0 overruns:0 carrier:2
          collisions:0 txqueuelen:1000
          RX bytes:50588302699 (47.1 GiB)  TX bytes:97318807157 (90.6 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:308297 errors:0 dropped:0 overruns:0 frame:0
          TX packets:308297 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:355278106 (338.8 MiB)  TX bytes:355278106 (338.8 MiB)
root@PROServer:~#
```

Ctrl Derecho

patri@Ubuntu14: ~

```
          inet6 addr: fe80::21f:c6ac:fd44:24d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84045991 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103776307 errors:0 dropped:0 overruns:0 carrier:
          collisions:0 txqueuelen:1000
          RX bytes:50588302699 (47.1 GiB)  TX bytes:97318807157 (90.6

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:308297 errors:0 dropped:0 overruns:0 frame:0
          TX packets:308297 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:355278106 (338.8 MiB)  TX bytes:355278106 (338.8 M
root@localhost:~# ls -l
drwxr-xr-x 1 root root 4096 2017-05-28 18:46 .
drwxr-xr-x 1 root root 4096 2017-05-28 18:46 ..
-rw-r--r-- 1 root root  140 2013-04-05 12:52 .profile
drwx------ 1 root root 4096 2013-04-05 13:05 .ssh
drwx------ 1 root root 4096 2013-04-05 12:58 .aptitude
-rw-r--r-- 1 root root  570 2013-04-05 12:52 .bashrc
drwxr-xr-x 1 root root 4096 2017-05-28 18:22 gggfh
root@localhost:~# te hemos pillado
```

HoneyDrive 3 [Corriendo] - Oracle VM VirtualBox

honeydri... [bin - File ... Sun, 28 May 18:47 honeydr

honeydrive@honeydrive: ~

honeydrive@honeydrive: ~ 77x22

```
honeydrive@honeydrive:~$ telnet -e q localhost 5000
Telnet escape character is 'q'.
Trying 127.0.0.1...
Connected to localhost.
Escape character is 'q'.
*** kippo session management console ***
List of commands:
 list       - list all active sessions
 view       - attach to a session in read-only mode
 hijack     - attach to a session in interactive mode
 disconnect - disconnect a session
 help       - this help
 exit       - disconnect the console
list
ID   clientIP        clientVersion
3    192.168.0.158   SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8
hijack 3
** Attaching to #3, hit ESC to return
te hemos pillado
```

EasyIDS

IDS con Snort

EasyIDS

https 192.168.1.9

Forense | Mac apps | Twitter | Wikipedia | Yahoo! | Noticias | Populares | AirDroid | Hipster things | Biz.nf | Save to Mendeley | URL Screenshot | La guía de lo... tele

EasyIDS

Analysis | Graphs | Settings | Status | Tools | Thanks

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- **Most recent 15 Unique Alerts**				
- **Most frequent 5 Unique Alerts**				

Sensors/Total: 1 / 1
Unique Alerts: 6
Categories: 3
Total Number of Alerts: 327

- Src IP addrs: 14
- Dest. IP addrs: 85
- Unique IP links 96

- Source Ports: 0
  - TCP (0) UDP (0)
- Dest Ports: 0
  - TCP (0) UDP (0)

Traffic Profile by Protocol

TCP (0%)

UDP (0%)

ICMP (6%)

Portscan Traffic (94%)

Alert Group Maintenance | Cache & Status | Administration

BASE 1.4.4 (dawn) (by **Kevin Johnson** and the **BASE Project Team**
Built on ACID by Roman Danyliw)

[Loaded in 2 seconds]

easyids [Running]

```
CentOS release 5.4 (Final)
Kernel 2.6.18-164.6.1.el5 on an i686

easyids login: jesus
Password:
Login incorrect

login: root
Password:
Last login: Sun May 28 14:49:21 on tty1

Welcome to EasyIDS
------------------------------------------------

For access to the EasyIDS web GUI use this URL
https://192.168.1.9

For help on EasyIDS commands you can use from this
command shell type help-easyids.

[root@easyids ~]# _
```

EasyIDS

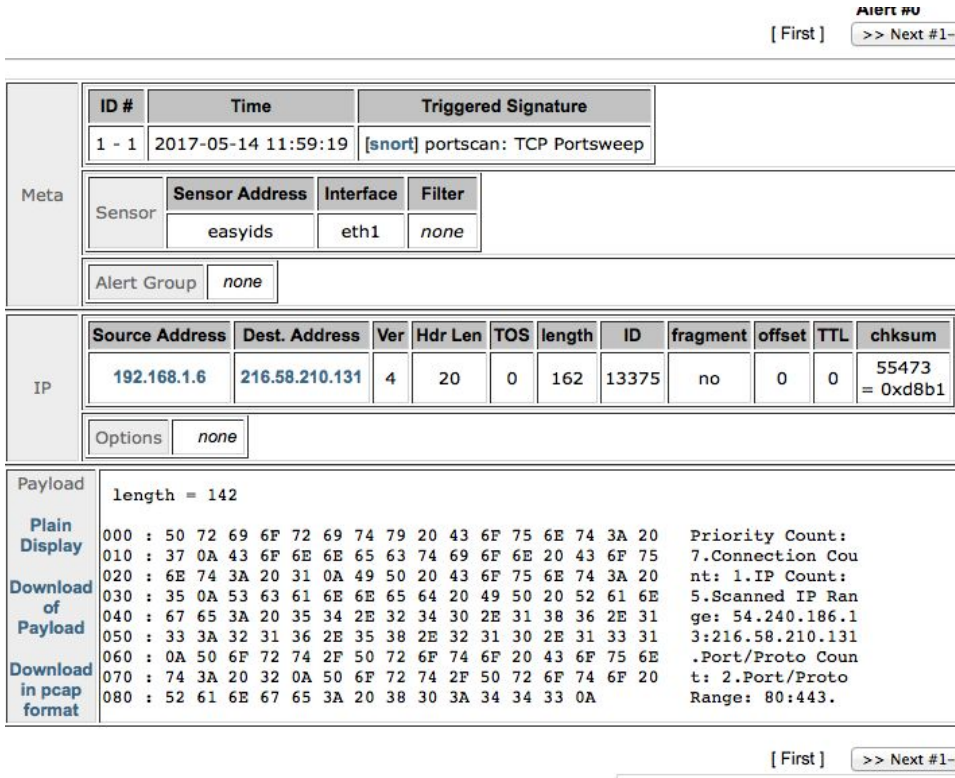
- IDS sencillo (supuestamente 😑) de configurar equipado con Snort y otras herramientas.
- Funcionamiento por interfaz gráfica a través de navegador.
- No se actualiza desde 2009 😟 (y hemos detectado algunos bugs importantes).

EasyIDS

Una vez configurado y funcionando, su uso es sencillo y amigable.

Snort funciona bien en él 👍 👌 y nos quita el engorro de manejarlo desde la terminal 😊.

Una pena que no siga el proyecto. 😞



Descubriendo un Honeypot

Descubriendo a un Honeypot

- TOP
- Acceso a archivos
- Archivos estáticos
- Exit

Descubriendo a un Honeypot

```
root@PROServer:~# top
E82: Cannot allocate any buffer, exiting...
```

No te permite usar el comando top

Descubriendo a un Honeypot

```
root@PROServer:~# cat /var/log/syslog
cat: /var/log/syslog: No such file or directory
root@PROServer:~# ls /var/log/
dmesg.0          installer        mail.log         kern.log         aptitude         news
wtmp             faillog          auth.log         lpr.log          user.log         fsck
syslog           dmesg            lastlog          mail.warn        mail.info        dpkg.log
daemon.log       alternatives.log mail.err         btmp             debug            apt
messages
root@PROServer:~#
```

No te permite acceso a ciertos archivos

Descubriendo a un Honeypot

```
root@PROServer:~#
dmesg.0          installer        mail.log
kern.log         aptitude         news
wtmp             faillog          auth.log
lpr.log          user.log         fsck
syslog           dmesg            lastlog
mail.warn        mail.info        dpkg.log
daemon.log       alternatives.log mail.err
btmp             debug            apt
messages
root@PROServer:~# rm /var/log/mail.log
root@PROServer:~# ls /var/log
dmesg.0          installer        kern.log
aptitude         news             wtmp
faillog          auth.log         lpr.log
user.log         fsck             syslog
dmesg            lastlog          mail.warn
mail.info        dpkg.log         daemon.log
alternatives.log mail.err         btmp
debug            apt              messages
root@PROServer:~#
```

```
root@PROServer:~# ls /var/log
dmesg.0          installer        mail.log
kern.log         aptitude         news
wtmp             faillog          auth.log
lpr.log          user.log         fsck
syslog           dmesg            lastlog
mail.warn        mail.info        dpkg.log
daemon.log       alternatives.log mail.err
btmp             debug            apt
messages
root@PROServer:~#
```

Archivos estáticos

Descubriendo a un Honeypot

```
Connection to server closed.
root@localhost:~#
```

No cierra conexión con el servidor

Descubriendo a un Honeypot

39	14.051684686	10.0.2.4	10.0.2.5	SSHv2	102	Client: Encrypted packet (le
40	14.052826291	10.0.2.5	10.0.2.4	SSHv2	102	Server: Encrypted packet (le
41	14.052892182	10.0.2.4	10.0.2.5	TCP	66	32790 → 22 [ACK] Seq=2398 Ac
42	14.405752477	10.0.2.4	10.0.2.5	SSHv2	102	Client: Encrypted packet (le
43	14.406826835	10.0.2.5	10.0.2.4	SSHv2	102	Server: Encrypted packet (le
44	14.406860899	10.0.2.4	10.0.2.5	TCP	66	32790 → 22 [ACK] Seq=2434 Ac
45	14.572534247	10.0.2.4	10.0.2.5	SSHv2	102	Client: Encrypted packet (le
46	14.573713872	10.0.2.5	10.0.2.4	SSHv2	102	Server: Encrypted packet (le
47	14.573757926	10.0.2.4	10.0.2.5	TCP	66	32790 → 22 [ACK] Seq=2470 Ac
48	14.786214713	10.0.2.4	10.0.2.5	SSHv2	102	Client: Encrypted packet (le
49	14.787157420	10.0.2.5	10.0.2.4	SSHv2	102	Server: Encrypted packet (le
50	14.787193527	10.0.2.4	10.0.2.5	TCP	66	32790 → 22 [ACK] Seq=2506 Ac
51	15.762766799	10.0.2.4	10.0.2.5	SSHv2	102	Client: Encrypted packet (le
52	15.764900160	10.0.2.5	10.0.2.4	SSHv2	214	Server: Encrypted packet (le
53	15.764950783	10.0.2.4	10.0.2.5	TCP	66	32790 → 22 [ACK] Seq=2542 Ac
54	15.764972017	10.0.2.5	10.0.2.4	SSHv2	138	Server: Encrypted packet (le
55	15.764975345	10.0.2.4	10.0.2.5	TCP	66	32790 → 22 [ACK] Seq=2542 Ac
56	15.765137513	10.0.2.4	10.0.2.5	SSHv2	102	Client: Encrypted packet (le
57	15.765202859	10.0.2.4	10.0.2.5	SSHv2	126	Client: Encrypted packet (le
58	15.765242995	10.0.2.4	10.0.2.5	TCP	66	32790 → 22 [FIN, ACK] Seq=26
59	15.765359233	10.0.2.5	10.0.2.4	TCP	66	22 → 32790 [ACK] Seq=3442 Ac
60	15.784509230	10.0.2.5	10.0.2.4	TCP	66	22 → 32790 [FIN, ACK] Seq=34
61	15.784544021	10.0.2.4	10.0.2.5	TCP	66	32790 → 22 [ACK] Seq=2639 Ac

Captura de cierre de sesión normal

Descubriendo a un Honeypot

55	47.777937458	10.0.2.4	10.0.2.15	SSHv2	118	Client: Encrypted packet (le
56	47.780366930	10.0.2.15	10.0.2.4	SSHv2	118	Server: Encrypted packet (le
57	47.780408230	10.0.2.4	10.0.2.15	TCP	66	48342 → 22 [ACK] Seq=3774 Ac
58	48.066775213	10.0.2.4	10.0.2.15	SSHv2	118	Client: Encrypted packet (le
59	48.069213622	10.0.2.15	10.0.2.4	SSHv2	118	Server: Encrypted packet (le
60	48.069256174	10.0.2.4	10.0.2.15	TCP	66	48342 → 22 [ACK] Seq=3826 Ac
61	48.183809661	10.0.2.4	10.0.2.15	SSHv2	118	Client: Encrypted packet (le
62	48.186099632	10.0.2.15	10.0.2.4	SSHv2	118	Server: Encrypted packet (le
63	48.186139130	10.0.2.4	10.0.2.15	TCP	66	48342 → 22 [ACK] Seq=3878 Ac
64	48.380207032	10.0.2.4	10.0.2.15	SSHv2	118	Client: Encrypted packet (le
65	48.383286490	10.0.2.15	10.0.2.4	SSHv2	118	Server: Encrypted packet (le
66	48.383329733	10.0.2.4	10.0.2.15	TCP	66	48342 → 22 [ACK] Seq=3930 Ac
67	48.983404597	10.0.2.4	10.0.2.15	SSHv2	118	Client: Encrypted packet (le
68	48.986218984	10.0.2.15	10.0.2.4	SSHv2	462	Server: Encrypted packet (le
69	48.986248937	10.0.2.4	10.0.2.15	TCP	66	48342 → 22 [ACK] Seq=3982 Ac
70	51.801318499	10.0.2.4	10.0.2.15	SSHv2	134	Client: Encrypted packet (le
71	51.801745099	10.0.2.4	10.0.2.15	TCP	66	48342 → 22 [FIN, ACK] Seq=40
72	51.802645921	10.0.2.15	10.0.2.4	TCP	66	22 → 48342 [FIN, ACK] Seq=48
73	51.802667601	10.0.2.4	10.0.2.15	TCP	66	48342 → 22 [ACK] Seq=4051 Ac

Captura de cierre de sesión honeypot

Conclusiones

Conclusiones

- Requiere bastante tiempo la implantación de estos sistemas.
- Además, deben estar muy bien configurados o no servirán de nada porque serán detectados.
- Siempre hay que intentar estar un paso por delante y para ello hay que conocer a tus enemigos. Con estas herramientas es fácil.

Honeypots, IDS y viceversa 😄