



MODERN HONEY NETWORK

PABLO VILCHEZ GARCIA

Honeypot



- **Un honeypot es un software o conjunto de maquinas que simulan vulnerabilidades.**
- **Con esto podremos sacar información de los atacantes, como qué tipo de ataques está desarrollando y avisar al administrador del sistema.**

Espacio Virtual de Trabajo

- **Tendremos una máquina como servidor MHN al que accederemos en una interfaz web y administraremos nuestros sensores**
- **Más máquinas desplegadas con otros sensores**
- **En todas instalaremos Ubuntu Server**

Instalación MHN

- **Para instalar MHN, desde su web en GitHub tenemos el repositorio y los comandos para la instalación.**
- **Clonamos el repositorio y ejecutamos los scripts de instalación**

```
sudo apt-get install git python gcc automake -y
```

```
git clone https://github.com/threatstream/mhn.git
```

```
cd mhn/scripts/
```

```
sudo ./install_hpfeeds.sh
```

```
sudo ./install_mnemosyne.sh
```

```
sudo ./install_honeymap.sh
```

Instalación MHN

- Finalmente ejecutamos el script de instalación de MHN

`sudo ./install_mhnserver.sh`

```
r/collector.json /opt/mhn/server/collector.json.example /opt/mhn/server/collecto
r.py /opt/mhn/server/collector_v2.py /opt/mhn/server/config.py /opt/mhn/server/c
onfig.pyc /opt/mhn/server/config.py.template /opt/mhn/server/generateconfig.py /
opt/mhn/server/initdatabase.py /opt/mhn/server/manage.py /opt/mhn/server/manual_
password_reset.py /opt/mhn/server/mhn /opt/mhn/server/mhn.db /opt/mhn/server/mhn
.log /opt/mhn/server/mhn.py /opt/mhn/server/migration_remove-hostname-and-name-u
niq-constraints.sql /opt/mhn/server/requirements.txt
+ supervisorctl update
mhn-celery-beat: added process group
mhn-celery-worker: added process group
mhn-collector: added process group
mhn-uwsgi: added process group
+ /etc/init.d/nginx restart
* Restarting nginx nginx [ OK ]
useras@m3:/opt/mhn/scripts$ sudo /etc/init.d/nginx status
[sudo] password for useras:
* nginx is running
useras@m3:/opt/mhn/scripts$ sudo /etc/init.d/supervisor status
is running
useras@m3:/opt/mhn/scripts$ sudo supervisorctl status
geoloc RUNNING pid 32697, uptime 0:53:05
honeymap RUNNING pid 32698, uptime 0:53:05
hpfeeds-broker RUNNING pid 13065, uptime 1:11:24
mhn-celery-beat RUNNING pid 1825, uptime 0:04:25
mhn-celery-worker FATAL Exited too quickly (process log may
have details)
mhn-collector RUNNING pid 1827, uptime 0:04:25
mhn-uwsgi RUNNING pid 1829, uptime 0:04:25
mnemosyne RUNNING pid 30928, uptime 0:58:05
useras@m3:/opt/mhn/scripts$
```

Corregir error en instalación

- Hay un error en la instalación, que se resuelve dando permisos a mhn.log

```
sudo chown www-data /var/log/mhn/mhn.log
```

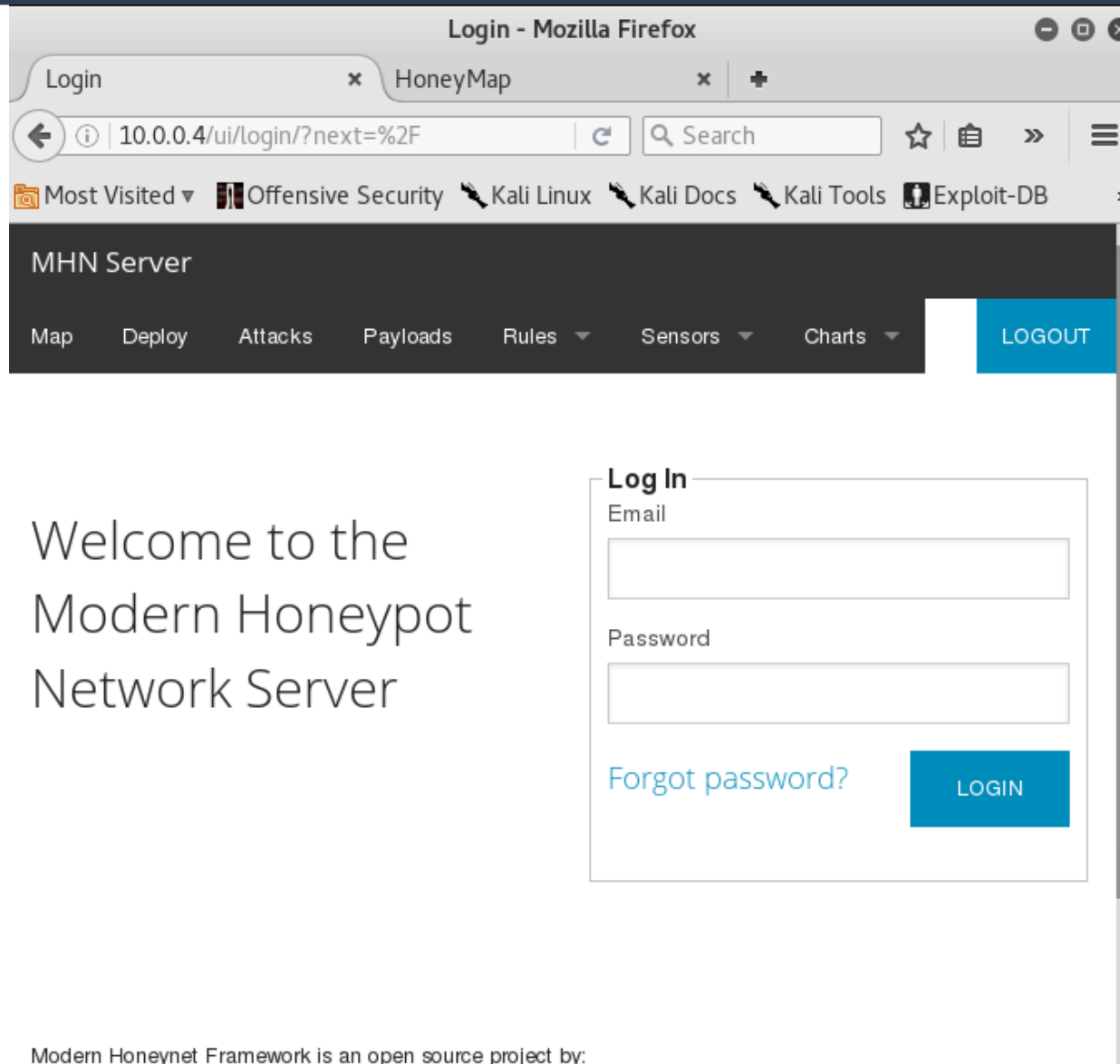
```
mhn-collector          RUNNING      pid 1243, uptime 0:01:50
mhn-uwsgi              RUNNING      pid 1061, uptime 0:02:33
mnemosyne              RUNNING      pid 1181, uptime 0:02:01
useras@m3:~$ sudo chown www-data /var/log/mhn/mhn.log
useras@m3:~$ sudo supervisorctl restart all
mhn-celery-beat: stopped
hpfeeds-broker: stopped
mnemosyne: stopped
geoloc: stopped
mhn-uwsgi: stopped
mhn-collector: stopped
honeymap: stopped
mhn-celery-beat: started
hpfeeds-broker: started
mnemosyne: started
geoloc: started
mhn-uwsgi: started
mhn-celery-worker: started
mhn-collector: started
honeymap: started
useras@m3:~$ sudo supervisorctl status
geoloc          RUNNING      pid 1341, uptime 0:00:32
honeymap        RUNNING      pid 1347, uptime 0:00:31
hpfeeds-broker  RUNNING      pid 1332, uptime 0:00:34
mhn-celery-beat RUNNING      pid 1331, uptime 0:00:34
mhn-celery-worker RUNNING      pid 1343, uptime 0:00:32
mhn-collector   RUNNING      pid 1346, uptime 0:00:31
mhn-uwsgi       RUNNING      pid 1342, uptime 0:00:32
mnemosyne       RUNNING      pid 1337, uptime 0:00:33
useras@m3:~$ _
```

Honeymap

- Tenemos el mapa donde se ven los ataques en 10.0.0.4:3000



Accesso a MHN



The screenshot shows a web browser window titled "Login - Mozilla Firefox". The address bar displays "10.0.0.4/ui/login/?next=%2F". The browser's bookmark bar includes "Most Visited", "Offensive Security", "Kali Linux", "Kali Docs", "Kali Tools", and "Exploit-DB". The page header, titled "MHN Server", contains navigation links: "Map", "Deploy", "Attacks", "Payloads", "Rules", "Sensors", "Charts", and a "LOGOUT" button. The main content area features a large welcome message and a login form.

MHN Server

Map Deploy Attacks Payloads Rules Sensors Charts LOGOUT

Welcome to the
Modern Honey
pot
Network Server

Log In

Email

Password

[Forgot password?](#)

Modern Honeynet Framework is an open source project by:

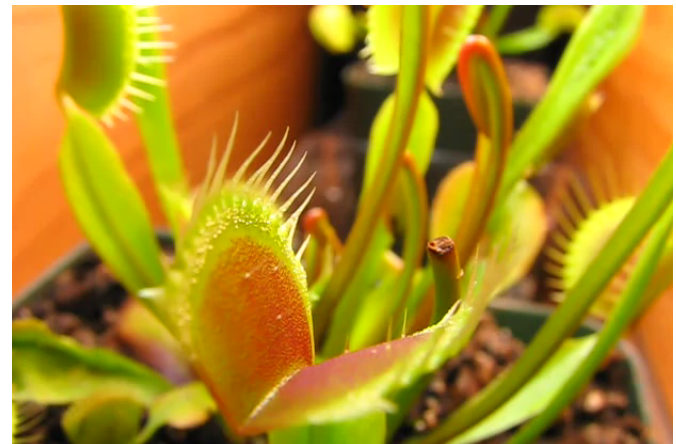
Sensores

- **Ya que MHN es el servidor honeypot, es posible replegar una red de sensores y monitorizarlos desde el servidor MHN**
- **MHN tiene un apartado con los scripts que automatizan la instalación de los sensores en diferentes dispositivos**

Dionaea

dionaea

- Es un honeypot capaz de capturar y analizar malware
- Levanta servicios y espera que los atacantes intenten hacerse con el control mediante payloads o peticiones maliciosas



Deploy MHN

- **En la pestaña deploy, MHN te da el script para instalar el sensor. Para dionaea tenemos que ejecutar el siguiente comando**

```
wget "http://10.0.0.4/api/script/?text=true&script_id=2" -O deploy.sh && sudo  
bash deploy.sh http://10.0.0.4 J865oGpA
```

Manage Deploy - Mozilla Firefox

Manage Deploy

10.0.0.4/ui/manage-deploy/?script_id=

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

MHN ServerMapDeployAttacksPayloadsRulesSensorsCharts

LOGOUT

Settings

Select Script

Ubuntu - Dionaea

Deploy Command

wget "http://150.214.205.65/api/script/?text=true&script_id=2" -O deploy.sh &&
sudo bash deploy.sh http://150.214.205.65 J865oGpA

Deploy Script

Name

Ubuntu - Dionaea

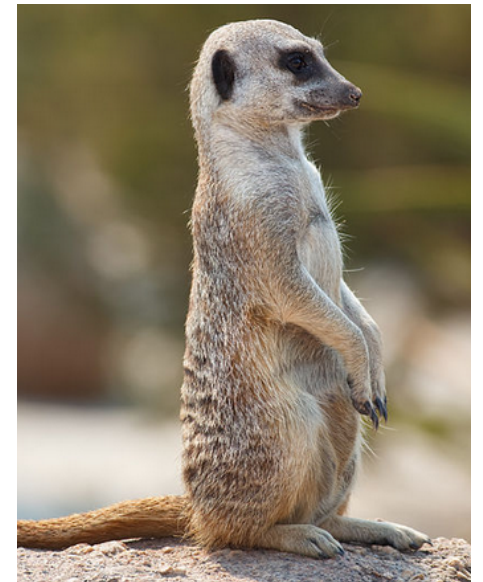
Script

yum -y install wget curl epel-release python-setuptools python-pip
easy_install supervisor
mkdir -p /etc/supervisor /etc/supervisor/conf.d

Suricata



- **Es un motor de supervisión de la seguridad en la red, muy escalable, multiproceso, etc.**
- **Reconoce automáticamente los protocolos más comunes y analiza el tráfico en busca de actividad sospechosa**



Suricata MHN

- **Para la instalación de Suricata en deploy elegimos**

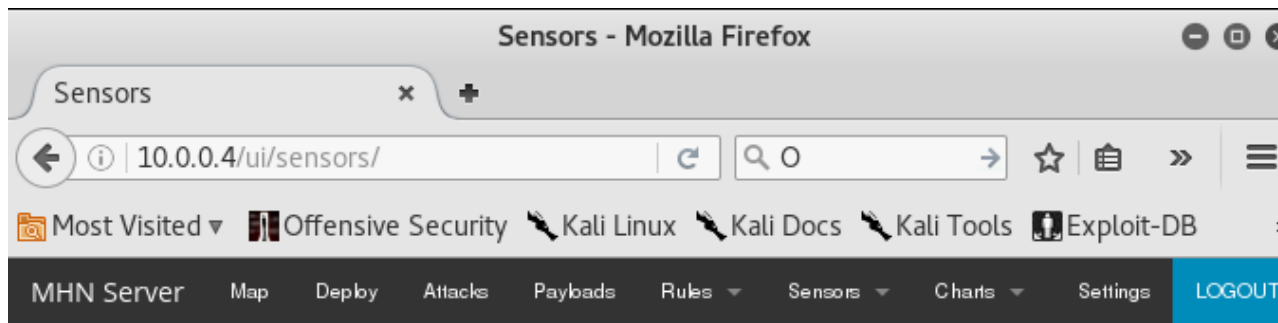
Ubuntu Server - Suricata

y nos devuelve el comando para ejecutar el script de instalación

```
wget "http://10.0.0.4/api/script/?text=true&script_id=13" -O deploy.sh && sudo  
bash deploy.sh http://10.0.0.4 J865oGpA
```

Sensors

- En la pestaña sensors podemos ver los sensores que tenemos instalados.



Sensors

	Name	Hostname	IP	Honeypot	UUID	Attacks
1- 	<input type="text" value="m3-dionaea"/>	m3	10.0.0.4	dionaea	1a813aee-2411-11e6-827e-0800278c6633	0
2- 	<input type="text" value="m2-suricata"/>	m2	10.0.0.3	suricata	42389d7a-2416-11e6-827e-0800278c6633	0

“Ataque”

- **Para ver el funcionamiento del Honeypot, vamos a hacer un escaneo de puertos en la IP del servidor MHN donde está instalado el sensor DIONAEA.**
- **Para esto, ejecutamos el siguiente comando:**

```
sudo nmap -A 10.0.0.4
```

```
userka@kali: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
userka@kali:~$ nmap -sP 10.0.0.4  
Starting Nmap 7.12 ( https://nmap.org ) at 2016-06-02 06:30 CEST  
Nmap scan report for 10.0.0.4  
Host is up (0.025s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds  
userka@kali:~$ nmap -A 10.0.0.4  
Starting Nmap 7.12 ( https://nmap.org ) at 2016-06-02 06:32 CEST  
[ ]
```

Sensors - Mozilla Firefox

Sensors

10.0.0.4/ui/sensors/

Search

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

MHN Server Map Deploy Attacks Payloads Rules Sensors Charts Settings LOGOUT

Sensors

	Name	Hostname	IP	Honeypot	UUID	Attacks
1- 🗑	m3-dionaea	m3	10.0.0.4	dionaea	1a813aee-2411-11e6-827e-0800278c6633	942
2- 🗑	m2-suricata	m2	10.0.0.3	suricata	42389d7a-2416-11e6-827e-0800278c6633	0

Modem Honeynet Framework is an open source project by:
THREATSTREAM.

```

userka@kali: ~
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
userka@kali:~$ sudo nmap -O 10.0.0.4
[sudo] password for userka:
Starting Nmap 7.12 ( https://nmap.org ) at 2016-06-02 06:37 CEST
Nmap scan report for 10.0.0.4
Host is up (0.0051s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
42/tcp    open  nameserver
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
3000/tcp  open  ppp
3306/tcp  open  mysql
5060/tcp  open  sip
5061/tcp  open  sip-tls
8181/tcp  open  unknown
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:DD:23:48 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.4
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https:
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.63 seconds
userka@kali:~$

```

Sensors - Mozilla Firefox

HoneyMap x Sensors x

10.0.0.4/ui/sensors/ Search

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

MHN Server Map Deploy Attacks Payloads Rules Sensors Charts Settings LOGOUT

Sensors

	Name	Hostname	IP	Honeypot	UUID	Attacks
1- 🗑️	m3-dionaea	m3	10.0.0.4	dionaea	1a813aee-2411-11e6-827e-0800278c6633	1029
2- 🗑️	m2-suricata	m2	10.0.0.3	suricata	42389d7a-2416-11e6-827e-0800278c6633	0

Modern HoneyNet Framework is an open source project by:

THREATSTREAM.

Ataques en MHN

- **Pagina para analizar ataques**

Attacks Report

Search Filters

Sensor

Honeypot

Date

Port

IP Address

GO

	Date	Sensor	Country	Src IP	Dst port	Protocol	Honeypot
1	2016-06-06 11:16:48	m3	<input data-bbox="889 895 927 924" type="text" value="?"/>	10.0.0.5	135	epmapper	dionaea
2	2016-06-06 11:16:40	m3	<input data-bbox="889 948 927 976" type="text" value="?"/>	10.0.0.5	135	epmapper	dionaea
3	2016-06-06 11:16:35	m3	<input data-bbox="889 1000 927 1029" type="text" value="?"/>	10.0.0.5	135	epmapper	dionaea
4	2016-06-06 11:16:30	m3	<input data-bbox="889 1053 927 1082" type="text" value="?"/>	10.0.0.5	135	epmapper	dionaea
5	2016-06-06 11:16:25	m3	<input data-bbox="889 1106 927 1134" type="text" value="?"/>	10.0.0.5	135	epmapper	dionaea
6	2016-06-06 11:16:20	m3	<input data-bbox="889 1158 927 1187" type="text" value="?"/>	10.0.0.5	135	epmapper	dionaea
7	2016-06-06 11:16:16	m3	<input data-bbox="889 1211 927 1240" type="text" value="?"/>	10.0.0.5	135	epmapper	dionaea
8	2016-06-06 11:16:16	m3	<input data-bbox="889 1264 927 1292" type="text" value="?"/>	10.0.0.5	4129	pcap	dionaea
9	2016-06-06 11:16:16	m3	<input data-bbox="889 1316 927 1345" type="text" value="?"/>	10.0.0.5	1037	pcap	dionaea
10	2016-06-06 11:16:16	m3	<input data-bbox="889 1369 927 1398" type="text" value="?"/>	10.0.0.5	1094	pcap	dionaea

Dashboard

Attack Stats

Attacks in the last 24 hours: **989**

TOP 5 Attacker IPs:

1.  **10.0.0.5 (989 attacks)**

TOP 5 Attacked ports:

1. **135 (17 times)**
2. **5060 (4 times)**
3. **5061 (3 times)**
4. **5101 (2 times)**
5. **49156 (2 times)**

TOP 5 Honey Pots:

1. **dionaea (989 attacks)**



FIN

