

# HONEYPOTS



Jorge Gutiérrez Segobia  
Manuel López Aceituno  
Cristian Vélez Ruiz

# ¿Que es un Honeypot?

- Herramienta usada seguridad informática
- Ser el objetivo de un posible ataque informático
- Básicamente se trata de dejar que te ataquen para luego ver quién y cómo te ha atacado
- Si el sistema dispuesto para ser atacado forma toda una red de herramientas y computadoras se le denomina honeynet

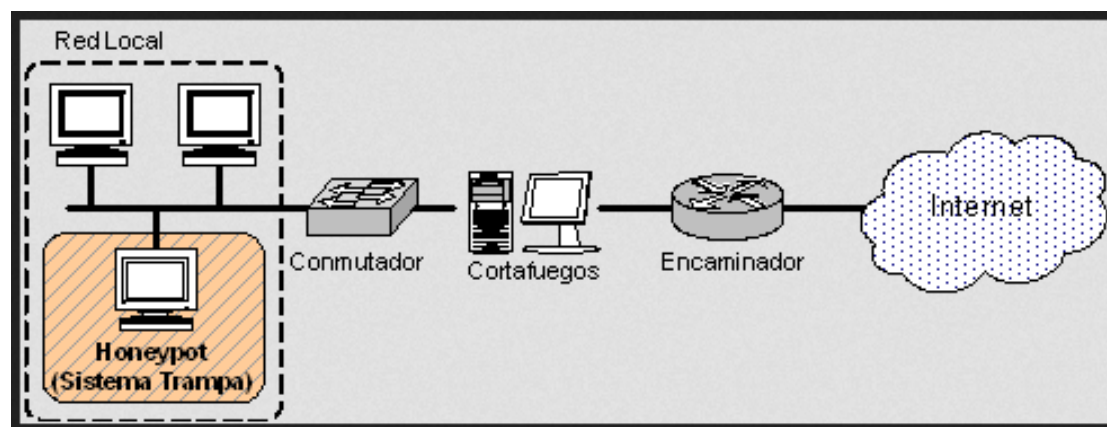
# ¿Que es un Honeypot?

- Baja interacción: se limitan a simular sistemas operativos y/o aplicaciones con vulnerabilidades
- Alta interacción: trabajan sobre sistemas operativos reales y son capaces de reunir mucha más información

# Donde colocar el Honeypot

- En un entrono cerrado, aislado y separado de cualquier sistema de producción
- Dentro de una red o entrono real de producción. (Tendremos que reforzar y afinar las medidas de seguridad del sistema donde se encuentre)

# Donde colocar el Honeypot



# Como funciona el Honeypot

- Según su alta o baja interacción
- Tiene como función atraer a los "hackers" para conocer e investigar los comportamientos
- Supongamos que tenemos un servidor ofreciendo servicios tales como SSH, FTP, WEB, et...

# Como funciona el Honeypot

- Podríamos emular esos servicios en los puertos estándares (22, 21, 80) y distraer a los atacantes para que pierdan el tiempo y de paso ver qué hacen, qué exploits utilizan, si explotan alguna vulnerabilidad nueva, etc

# ¿Qué vamos a hacer nosotros?

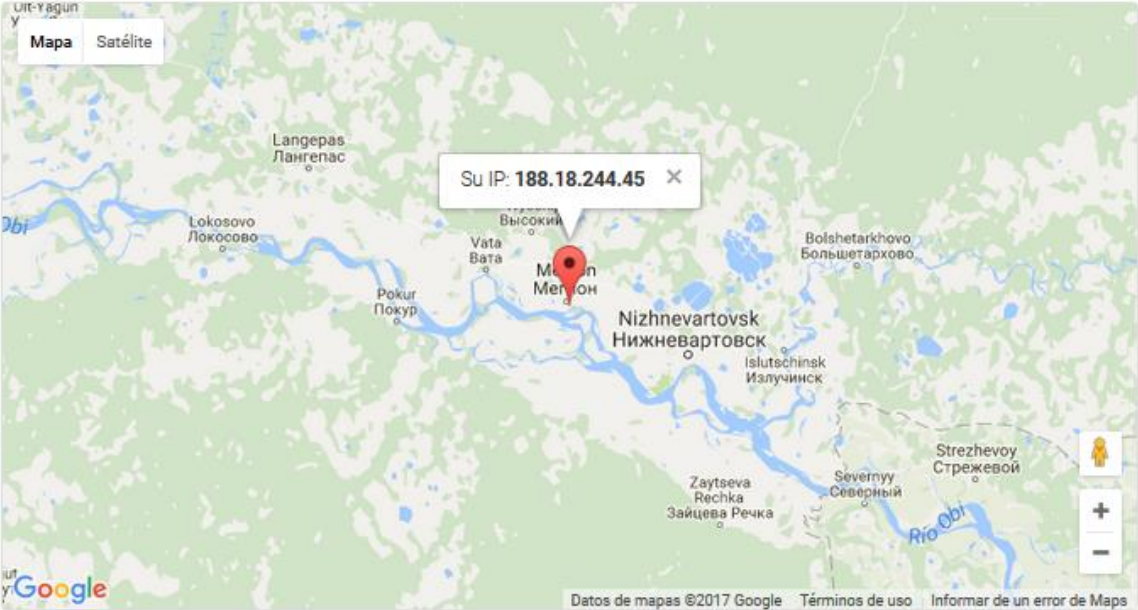
- Probaremos a dejar que nos ataquen habilitando SSH con una IP pública
- Usaremos software específico para Honeypot
- Analizaremos de donde provienen las IP's presuntamente atacantes



# Abrir SSH

```
pi@honeeepi: ~  
20-May 14:06:22 User: invalid IP: admin  
20-May 14:06:24 User: invalid IP: admin  
20-May 14:06:26 User: invalid IP: admin  
pi@honeeepi:~ $ zgrep -hi "Failed password for " /var/log/aut* | sed "s/invalid  
user //" | tr -s " " | awk '{print $11" "$9}' | sort | uniq -c | sort -rn | head  
-2000  
18 190.179.172.225 root  
18 186.57.51.75 root  
18 140.255.97.103 root  
12 179.37.47.69 root  
8 133.123.42.74 root  
6 211.81.48.67 admin  
6 188.18.244.45 root  
6 179.37.47.69 admin  
4 192.168.0.11 root  
3 60.28.118.2 oracle  
3 60.28.118.2 admin  
1 46.182.18.46 admin  
1 192.168.0.15 pi  
1 178.20.55.18 admin  
1 171.25.193.131 admin  
1 103.207.36.117 support  
1 103.207.36.117 1234  
pi@honeeepi:~ $
```

# Abrir SSH



País	Russian Federation
Ciudad	Meion
Latitud	61.029598236084
Longitud	76.11360168457
ISP	Rostelecom

# Artillery

```
root@kali:~# nmap velezruiz.ddns.net

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-20 13:19 EDT
Nmap scan report for velezruiz.ddns.net (217.216.51.132)
Host is up (0.91s latency).
rDNS record for 217.216.51.132: 217.216.51.132.dyn.user.ono.com
Not shown: 973 closed ports
PORT      STATE      SERVICE
1/tcp     filtered  tcpmux
3/tcp     filtered  compressnet
4/tcp     filtered  unknown
6/tcp     filtered  unknown
7/tcp     filtered  echo
9/tcp     filtered  discard
21/tcp    open      ftp
22/tcp    open      ssh
25/tcp    open      smtp
53/tcp    open      domain
110/tcp   open      pop3
111/tcp   open      rpcbind
135/tcp   open      msrpc
445/tcp   open      microsoft-ds
1433/tcp  open      ms-sql-s
1723/tcp  open      pptp
3389/tcp  open      ms-wbt-server
5800/tcp  open      vnc-http
5900/tcp  open      vnc
8080/tcp  filtered  http-proxy
8082/tcp  filtered  blackice-alerts
10000/tcp open      snet-sensor-mgmt
16992/tcp open      amt-soap-http
```

# Artillery


```
pi@raspberrypi:/var/artillery $ cat /var/artillery/banlist.txt
#
#
#
# Binary Defense Systems Artillery Threat Intelligence Feed and Banlist Feed
# https://www.binarydefense.com
#
# Note that this is for public use only.
# The ATIF feed may not be used for commercial resale or in products that are
# charging fees for such services.
# Use of these feeds for commerical (having others pay for a service) use is s
# ictly prohibited.
#
#
#
114.107.30.128
216.218.206.67
pi@raspberrypi:/var/artillery $
```

# Artillery

**CUALESMI IP** Geolocalizar IP Whois ADSLZone MovilZona Android RedesZone TabletZona Test de Velocidad

114.107.30.128

Mapa Satélite



Google


País	China
Ciudad	Hefei
Latitud	31.863899230957
Longitud	117.28079986572
ISP	China Telecom Anhui

# Artillery

**CUALESMI IP** Geolocalizar IP Whois ADSLZone MovilZona Android RedesZone TabletZona Test de Velocidad

216.218.206.67

Mapa Satélite



Google

Datos de mapas ©2017 Google Términos de uso

País	United States
Ciudad	Fremont
Latitud	37.549701690674
Longitud	-121.96209716797
ISP	Hurricane Electric



# Artillery

Kali-Linux [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda


Applications Places Firefox ESR Sat 13:37

The Shadowserver Foundation - Mozilla Firefox

The Shadowserver Fo... x

216.218.206.67 Search

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



Recorte de ventana

## The Shadowserver Foundation

If you are looking at this page, then more than likely, you noticed a scan coming from this server across your network and/or poking at a service that you have running.

The Shadowserver Foundation is currently undertaking a project to search for publicly accessible devices that have services running that should not be exposed because they are trivial to exploit or abuse. The goal of this project is to identify hosts that have these types of services exposed and [report](#) them back to the network owners for remediation.

Further details on this scanning project can be found on our blog at: <http://blog.shadowserver.org/2014/03/28/the-scannings-will-continue-until-the-internet-improves/>

Statistics on these scans can be found at: <http://blog.shadowserver.org/2014/08/22/of-scannings-and-statistics/>

If you would like to sign up for reports on any data that we have collected on your network, you can request them from here: <https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork>

All of the probes that are used in our tests are benign and do not ( and will **never** ) contain exploit code. Scans with these types of tools are off-limits for us.

All the data that we collect is visible to anyone who connects to a particular host with on the proper port using the proper commands.

If you have any more questions please feel free to send us an email at: [dnssec \[at\] shadowserver \[dot\] org](mailto:dnssec[at]shadowserver[dot]org)

[The Shadowserver Foundation](#)

CTRL DERECHA

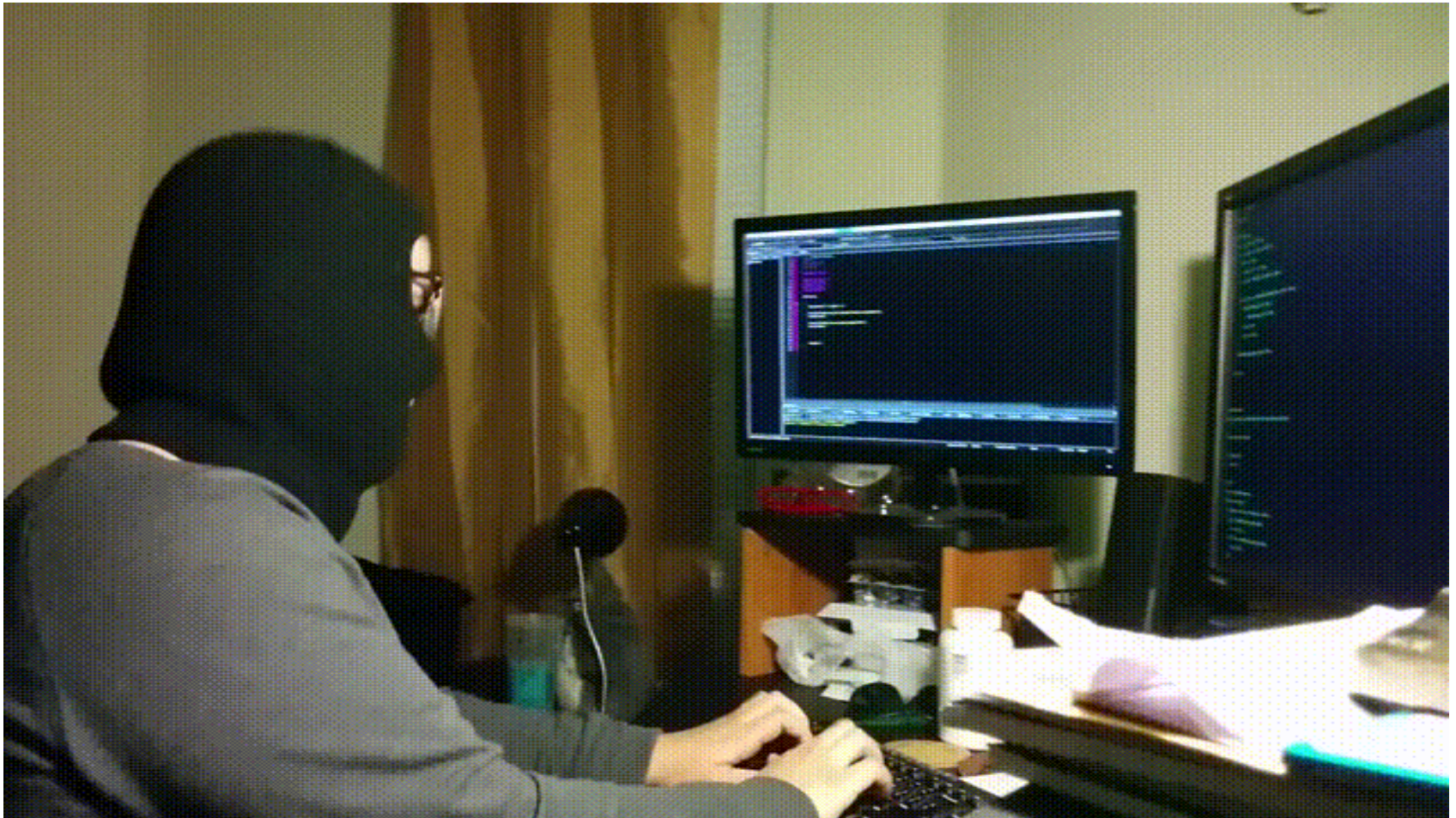
# ¿Qué hacemos con estas IP?

- Obtener su país, organización, y posición GPS.
- ¿Cómo?
  - <http://ipinfo.io/>
- ¿Problemas?
  - Solo 1000 request al día.
- Automatización

**I ❤️ #!/bin/bash**



# Automatización



# Automatización

- curl
- Grep, cat y cut.
- Generamos un .csv

	A	B	C	D	E	F
1	IP	<u>Country</u>	<u>Region</u>	<u>Org</u>	<u>Lat</u>	<u>Lon</u>
2	93.99.128.230	<u>CZ</u>	<u>Jihomoravsky kraj</u>	<u>AS6830 Liberty Global Operations B.V.</u>	48,9227	17,1043
3	221.162.125.32	<u>KR</u>	<u>Busan</u>	<u>AS4766 Korea Telecom"</u>	35,1028	129,0403
4	175.121.89.7	<u>KR</u>		<u>AS9318 SK Broadband Co Ltd"</u>	37,5112	126,9741
5	113.124.140.21	<u>CN</u>	<u>Shandong</u>	<u>AS4134 CHINANET-BACKBONE"</u>	36,6683	116,9972
6	78.31.67.2	<u>DE</u>		<u>AS24961 myLoc managed IT AG"</u>	51,2993	9,491

# Mostrando la información

- My maps, Google Inc
- Enlace de acceso publico:
  - [goo.gl/o6Yrh1](https://goo.gl/o6Yrh1)

# Resultado

