

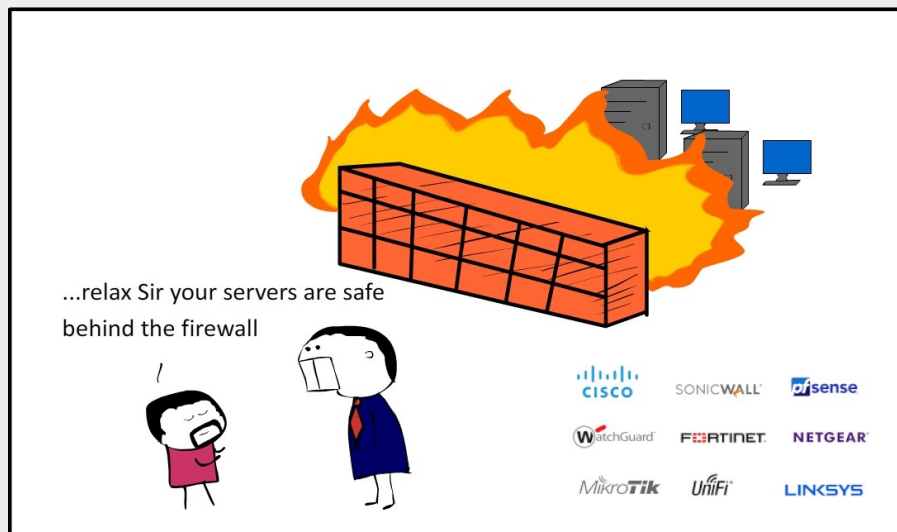
Ataques SIP, HoneyPots y otras hierbas



Ángel Elena Medina
craem@craem.net

:: Ataques SIP y otras hierbas ::

- Necesito que mi proxy SIP / pbx / webrtc esté abierto a internet.
- Colocar un firewall (appliance) delante, complica la señalización... nat y ALG no son tus amigos y tampoco hace magia.
- Firewall UTM → efecto placebo; creo que tengo todo asegurado, pero no



< - >



:: Ataques SIP y otras hierbas ::

Vale, ¿cómo puedo protegerme de los ataques ?

- Siempre por vpn (la más segura).
- Asegurando orígenes (todo siempre con ip's fijas).
- Capando las llamadas internacionales.
- Configurando rate-limits y pps (paquetes por segundo).
- Fail2ban (es un come recursos).

.....



- Configurando un honeyPot y alimentando el firewall del propio sip / proxy server con el detalle de los ataques.... ¿ pero cómo ?:
 - Usando software libre, como kamailio / rtpengine / asterisk



:: Ataques SIP y otras hierbas ::

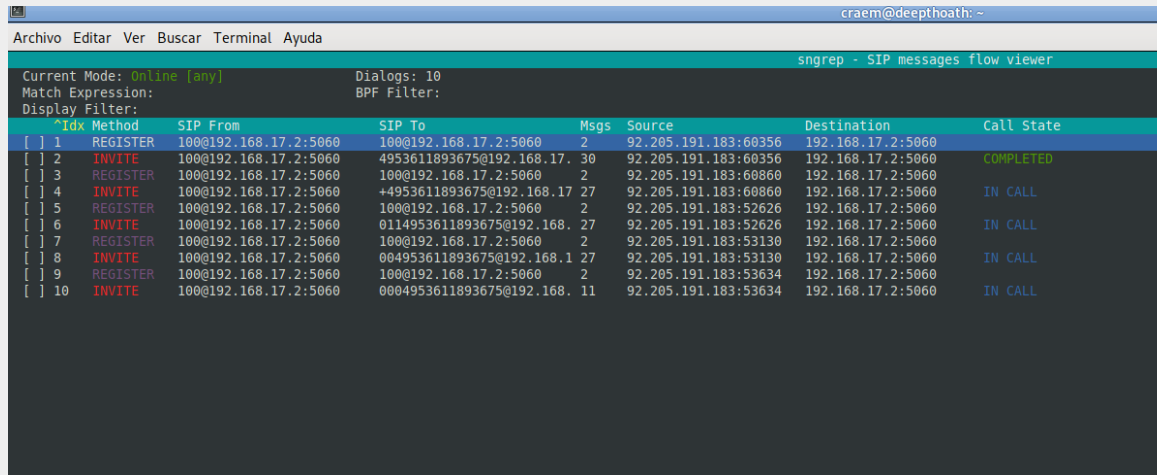
- Configuramos un honeypot en nuestra red y lo aislamos para que no puedan realizar “pivoting”.
- Intentamos que sea lo más transparente y parecido a un sistema “comprometido” / “desatendido”



- Aprovecharemos los ataques para:
 - Tener de primera mano los ataques en un sistema controlado
 - Recopilar mucha info
 - Analizar tráfico
 - Ser proactivos y crear nuestras defensas

:: Ataques SIP y otras hierbas ::

- Conectamos nuestro HoneyPot y lo dejamos abierto, a ver qué pasa !!!
- Abro la consola y veo los primeros intentos de invite's y registers.
- Ya tenemos la oportunidad de hacer algo más; inspección y bloqueo.



| Idx | Method | SIP From | SIP To | Msgs | Source | Destination | Call State |
|--------|----------|-----------------------|------------------------------------|------|----------------------|-------------------|------------|
| [] 1 | REGISTER | 100@192.168.17.2:5060 | 100@192.168.17.2:5060 | 2 | 92.205.191.183:60356 | 192.168.17.2:5060 | |
| [] 2 | INVITE | 100@192.168.17.2:5060 | 4953611893675@192.168.17.2:5060 | 30 | 92.205.191.183:60356 | 192.168.17.2:5060 | COMPLETED |
| [] 3 | REGISTER | 100@192.168.17.2:5060 | 100@192.168.17.2:5060 | 2 | 92.205.191.183:60860 | 192.168.17.2:5060 | |
| [] 4 | INVITE | 100@192.168.17.2:5060 | +4953611893675@192.168.17.2:5060 | 27 | 92.205.191.183:60860 | 192.168.17.2:5060 | IN CALL |
| [] 5 | REGISTER | 100@192.168.17.2:5060 | 100@192.168.17.2:5060 | 2 | 92.205.191.183:52626 | 192.168.17.2:5060 | |
| [] 6 | INVITE | 100@192.168.17.2:5060 | 0114953611893675@192.168.17.2:5060 | 27 | 92.205.191.183:52626 | 192.168.17.2:5060 | IN CALL |
| [] 7 | REGISTER | 100@192.168.17.2:5060 | 100@192.168.17.2:5060 | 2 | 92.205.191.183:53130 | 192.168.17.2:5060 | |
| [] 8 | INVITE | 100@192.168.17.2:5060 | 004953611893675@192.168.17.2:5060 | 27 | 92.205.191.183:53130 | 192.168.17.2:5060 | IN CALL |
| [] 9 | REGISTER | 100@192.168.17.2:5060 | 100@192.168.17.2:5060 | 2 | 92.205.191.183:53634 | 192.168.17.2:5060 | |
| [] 10 | INVITE | 100@192.168.17.2:5060 | 0004953611893675@192.168.17.2:5060 | 11 | 92.205.191.183:53634 | 192.168.17.2:5060 | IN CALL |

```
Oct 30 20:17:28 deepthoath /usr/local/sbin/kamailio[30796]: INFO: <script>: 92.205.191.183 sip:004953611893675@192.168.17.2:5060 sip:100@192.168.17.2:5060 OBIHAI/OBi477-1.3.0.2690
Oct 30 20:17:28 deepthoath /usr/local/sbin/kamailio[30796]: INFO: <script>: 100 (with IP:92.205.191.183) is trying to call to 004953611893675
```

:: Ataques SIP y otras hierbas ::

- Vamos a analizar los INVITE'S un poco más a fondo:

```
craem@deepthroat: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
Call flow for APvissAa2NkFXSP7utXNvgkWLuhg28g8uXLxNVRo (Color by Request/Response)  
51.161.13.200:5397 192.168.17.2:5060  
19:45:39.373646 INVITE (SDP) →  
+0.000005  
19:45:39.374251 200 PLEASE - Fuck me with ←  
+0.100009  
19:45:39.483320 ACK →  
INVITE sip:000026448303320@192.168.17.2:5060 SIP/2.0  
Via: SIP/2.0/UDP 51.161.13.200:5397;branch=z9hG4bK2f6f7ce6-331e-2161-otd3ft86njt03cfx;rport  
Max-Forwards: 70  
Contact: <sip:8890301053051.161.13.200:5397>  
To: <sip:000026448303320@192.168.17.2:5060>  
From: <sip:8890301053051.161.13.200:5397>;tag=ssn6258caa47z8zb  
Call-ID: APvissAa2NkFXSP7utXNvgkWLuhg28g8uXLxNVRo  
CSeq: 1 INVITE  
User-Agent: Cisco-SIPGateway/IOS-12.x  
Content-Type: application/sdp  
Content-Length: 741  
  
v=0  
o=- 1551542923 1551542924 IN IP4 51.161.13.200  
s=cisco-sipgateway/ios-12x  
c=IN IP4 51.161.13.200  
t=0 0  
m=audio 20002 RTP/AVP 9 104 98 3 8 0 101 97 100 108 15 4 105 106 107 103 103 103 18  
a=rtpmap:9 G722/8000  
a=fmtp:9 bitrate=64000  
a=rtpmap:104 G726-16/8000  
a=rtpmap:98 iLBC/8000  
a=fmtp:98 mode=20  
a=rtpmap:3 GSM/8000  
a=rtpmap:8 PCMA/8000  
a=rtpmap:0 PCMU/8000  
a=rtpmap:101 telephone-event/8000  
a=rtpmap:97 SPEEX/8000  
a=rtpmap:100 SPEEX/16000  
a=rtpmap:108 SPEEX/32000  
a=rtpmap:15 G728/8000  
a=rtpmap:4 G723/8000  
a=rtpmap:105 G726-24/8000  
a=rtpmap:106 G726-32/8000  
a=rtpmap:107 G726-40/8000  
a=rtpmap:103 L16/8000  
a=rtpmap:103 L16/44000  
a=rtpmap:103 L16/44000  
a=rtpmap:18 G729/8000  
a=fmtp:18 annexb=no  
a=sendrecv
```

:: Ataques SIP y otras hierbas ::

- **User Agent** : User-Agent: Cisco-SIPGateway/IOS-12.x

Puede ser totalmente inventado o de alguna lista que tenga el bot.

From: <sip:8890301053@51.161.13.200:5397>;tag=ssn6258caa47z8zb

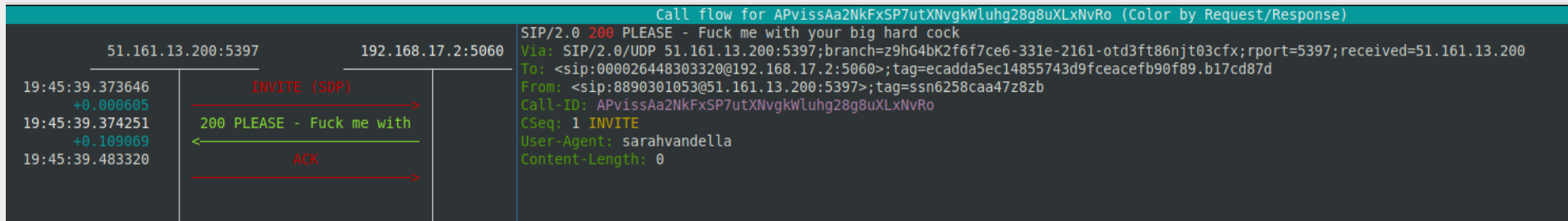
Es posible que sea inventado también, proceda de un ataque de diccionario de un sistema expuesto, o generada aleatoriamente.

To: <sip:000026448303320@192.168.17.2:5060>

El destino, en este caso es aleatorio y por norma general, lanzan bastantes invite's de este tipo para comprobar que el servidor responde y preparar el ataque más tarde.

Para hacerlo más creíble, le respondo un **200 Ok** con algo de gracia

Call flow for APvissAa2NkFxSP7utXNvgkwluhg28g8uXLxNvRo (Color by Request/Response)



:: Ataques SIP y otras hierbas ::

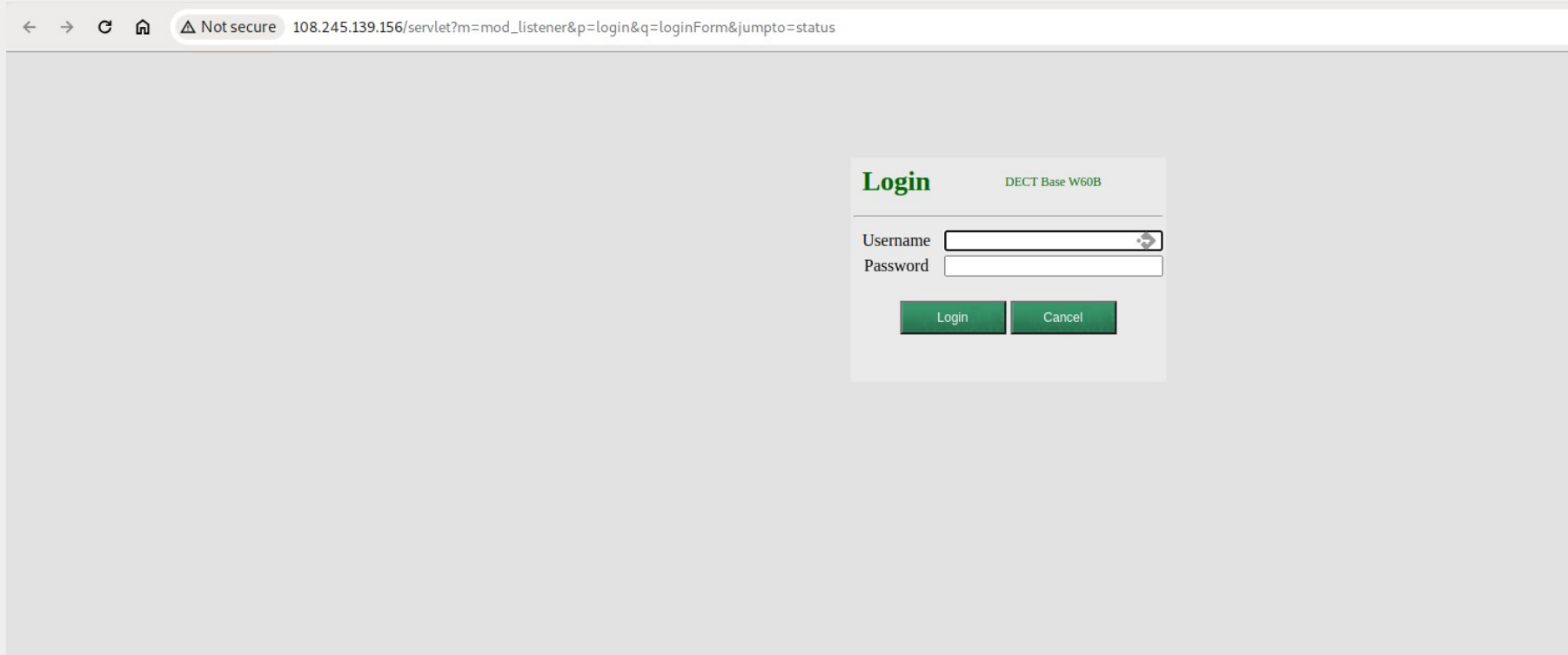
Vale bien... ¿pero cómo llegan a capturar estos sistemas expuestos ?. Hagamos una rápida búsqueda, de por ejemplo, Yealink, en la web de los amigos de **shodan.io**

The screenshot shows a web browser window with the address bar displaying `shodan.io/search?query=yealink&page=3`. The page content is a list of search results for the query 'yealink'. Each result includes an IP address, a brief description of the system, and a snippet of the captured data.

| IP Address | System Description | Captured Data Snippet |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 195.88.57.175 | Cloud Web Manage United States, Miami | HTTP/1.1 200 OK content-type: text/html; charset=UTF-8 content-length: 1 server: GoAhead-Webs/2.5.0 PeerSec-MatrixSSL/3.4.2-OPEN WebSockify Python/2.7.12 boss/1.0 (BOSS) BigIP Microsoft-IIS/7.5 bks400 PRTG/13.1.2.1462 Virtual Web 0.9 FC03-H |
| 108.245.139.156 | 108-245-139-156.lightspeed.irvnca.sbcglobal.net Private Customer - AT&T Internet Services United States, Los Angeles | SIP/2.0 200 OK Via: SIP/2.0/UDP nm;branch=fao;rport=26810 From: <sip:nm@nm>;tag=root To: <sip:nm2@nm2>;tag=2996606022 Call-ID: 50000 CSeq: 42 OPTIONS User-Agent: Yealink W608 77.83.0.85 Content-Length: 0 |
| 185.233.72.59 | ip-185-233-72-59.zipnet.pl ZIPnet sp. z o.o. Poland, Starogard Gdański | HTTP/1.1 200 OK Content-Type: text/html Accept-Ranges: bytes ETag: "-702809768" Last-Modified: Fri, 10 Apr 2020 03:24:04 GMT Content-Length: 127 Date: Sun, 07 Jan 2024 18:35:01 GMT Server: yealink embed httpd <html> <script type="text/javascript"> window.location = "/servlet?p=logi... |

:: Ataques SIP y otras hierbas ::

Ahora, intentamos abrir la web del dispositivo y.... SORPRESA !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!



The screenshot shows a web browser window with the address bar displaying "108.245.139.156/servlet?m=mod_listener&p=login&q=loginForm&jumpto=status". The page content is a login form titled "Login" for a "DECT Base W60B" device. The form includes fields for "Username" and "Password", and "Login" and "Cancel" buttons.

← → ↻ 🏠 ⚠ Not secure 108.245.139.156/servlet?m=mod_listener&p=login&q=loginForm&jumpto=status

Login

DECT Base W60B

Username

Password

Login Cancel

:: Ataques SIP y otras hierbas ::

Qué guai !!!!. ¿ Pero de qué sirve que entren al terminal ?; puuesssss vamos a hacer un mapa !!!!



Nota: Dora la exploradora, con su amigo, el MAPA

Yealink T46S Log Out English (English) ▼

Status **Account** **Network** **Dsskey** **Features** **Settings** **Directory** **Security**

Preference
Time&Date
Call Display
Upgrade
Auto Provision
Configuration

BIN Configuration

Export or Import Configuration ?

CFG Configuration

Export CFG Configuration File ?

Import CFG Configuration File ?

NOTE

Configuration
IP phones can provide feedback in a variety of forms such as log files, packets, status indicators and so on, which can help an administrator more easily find the system problem and fix it.

- Log Files
- Capturing Packets
- Configuration File (*.cfg/*.bin)

:: Ataques SIP y otras hierbas ::

De buenas a primeras, ya tenemos la config del dispositivo... user, password + Ip y luego, una sorpresita todavía mayor:

Nuestro amigo todopoderoso, el **Remote Control**

The screenshot shows a web interface for configuring a device. On the left is a sidebar with menu items: Forward&DND, General Information, Audio, Intercom, Transfer, Pick up & Park, Remote Control (highlighted), Phone Lock, and ACD. The main content area is titled 'Remote Control' and contains the following fields:

- Push XML Server IP Address:
- Username:
- Password:
- SIP Notify:
- Block XML in Calling:
- Action URI Allow IP List: (This field has a red dot to its left and a red dot to its right)
- CSTA Control:

Each field has a question mark icon to its right. At the bottom of the form are 'Confirm' and 'Cancel' buttons. On the right side of the interface is a 'NOTE' box with the following text:

Action URI
You can specify one or more trusted IP addresses on the IP phone, or allow the IP phone to receive and handle the URI from any IP address.

Click here to get more product documents.

Sólo SETeando el **Action URI Allow IP List** → any , ha tenemos un dialer remoto para hacer cientos de llamadas desde nuestro sistema.

:: Ataques SIP y otras hierbas ::

- No sirve de nada colocar un firewall delante ni que sea https.
- Un teléfono SIP no está pensado para colocarse directamente a internet y el servidor interno que lleva, tampoco.

Luego tenemos funciones mágicas que van muy bien, como el screen capture y alguna virguería más, como por ejemplo:

<https://support.yealink.com/en/portal/knowledge/show?id=a5c540089197a886a335af27>

How to get the screen capture of Yealink phones

Last Update Time : 2022-02-16 Pageviews : 26478

[Issue Description]

How to get the screen capture of Yealink phones?

[Resolution]

1. Login on the WEB interface and fill the 'Action URI allow IP List' (path: Features -- Remote Control -- Action URI allow IP List) with 'any' or 'IP address or your PC', then click 'Confirm'.

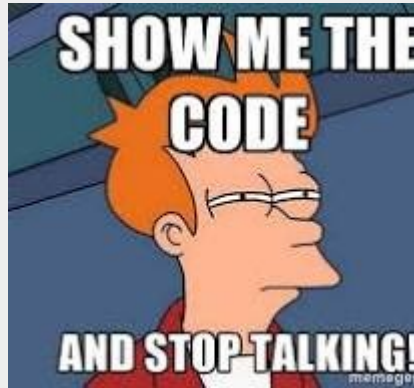
The screenshot shows the Yealink phone web interface. At the top, there are tabs for Status, Account, Network, Dsskey, and Features. The Features tab is selected. On the left, there is a sidebar with options: Forward&DND, General Information, Audio, Intercom, Transfer, Pick up & Park, and Remote Control. The Remote Control option is highlighted. In the main area, the 'Remote Control' section is expanded, showing fields for Push XML Server IP Address, Username, Password, SIP Notify, Block XML in Calling, Action URI Allow IP List, and CSTA Control. The 'Action URI Allow IP List' field is highlighted with a red box and contains the text 'any'. Below the fields are 'Confirm' and 'Cancel' buttons.

2. In the Browser, fill 'http://PhoneIP/screencapture' in the address bar (Phone IP is the IP address of your phone), then press 'Enter' key.

← → ↻ 10.81.56.16/screencapture

:: Ataques SIP y otras hierbas ::

Vale, que si.... Y el honeypot, cómo ?



:: Ataques SIP y otras hierbas ::

```
request_route {  
    # per request initial checks  
    route(REQINIT);  
  
    # NAT detection  
    route(NATDETECT);  
}
```

Como no va a tener que procesar llamadas, en el request route, la primera llamada que sea recoger los invite's para almacenar en la bbdd los datos que nos hagan falta. Luego, podemos diferenciar los ataques, por ejemplo, capturando los register e insertándolos en la bbdd:

```
# Al recibir un intento de registro, devolvemos siempre un OK  
if (is_method("REGISTER")) {  
    xlog("L_INFO", "Get Register for user $fU (IP: $si)\n");  
    xlog("L_INFO", "... afegim a ip blocades $si $tu $rU ... \n");  
    avp_db_query("INSERT into logs_ataque (ip,destino,src,method,userAgent) values ('$si','$tu','$fU','register','$ua')");  
  
    if ($fU != "100")  
        sl_send_reply("407", "Proxy Authentication Required::tonyina");  
}
```

:: Ataques SIP y otras hierbas ::

Aquí vemos el ejemplo con un paquete INVITE para realizar una llamada... en este caso la envío a un asterisk que está instalado en la misma máquina, descuelgo la llamada, envío un tono / pitido y se hace el HANGUP:

```
if (is_method("INVITE")) {  
    xlog("L_INFO", ".... afegim a ip blocades $si $tu $rU ... \n");  
    avp_db_query("INSERT into logs_ataque (ip,destino,src,method,userAgent) values ('$si','$tu','$fu','invite','$ua')");  
    xlog("L_INFO", "$si $tu $fu $ua \n");  
    xlog("L_INFO", "$fu (with IP:$si) is trying to call to $rU\n");  
    $rU = "6969";  
    $du = "sip:192.168.17.2:5061";  
    $rd = $dd;  
    $td = $dd;  
    record_route();  
    xlog("L_INFO", "enviem trucada a blackhole $rU\n");  
    route(RELAY);  
}
```


:: Ataques SIP y otras hierbas ::

Bueno, muy bien.... Y después, ¿ cómo lo podemos usar ?

```
mysql> select * from ips_ataques_extended order by hints_ataques desc limit 10;
```

| id | ip | as_number | inet_num | country | netname | description | hints_ataques | primer_ataque | ultimo_ataque |
|------|-----------------|-----------|------------------|---------|---------|---------------------------------|---------------|---------------------|---------------------|
| 2326 | 45.134.144.118 | 49870 | 45.134.144.0/24 | HK | 0 | AS49870-BV, NL | 2719639 | 2021-12-28 21:47:27 | 2022-01-27 14:31:24 |
| 1027 | 54.39.152.128 | 16276 | 54.39.0.0/16 | CA | 0 | OVH, FR | 2523898 | 2021-03-17 12:54:39 | 2021-03-18 15:29:03 |
| 783 | 62.210.9.51 | 12876 | 62.210.0.0/16 | FR | 0 | Online SAS, FR | 1684349 | 2021-01-22 15:17:13 | 2021-01-23 05:34:16 |
| 3457 | 45.134.144.223 | 47154 | 45.134.144.0/24 | HK | 0 | HUSAM-NETWORK, NL | 1199178 | 2022-08-29 17:02:26 | 2022-09-27 14:02:27 |
| 381 | 103.145.13.113 | 213371 | 103.145.13.0/24 | IN | 0 | SQUITTER-NETWORKS, NL | 927555 | 2020-11-09 01:41:22 | 2020-11-09 14:33:35 |
| 1392 | 193.107.216.182 | 201814 | 193.107.216.0/24 | HK | 0 | PL-SKYTECH-AS, PL | 922183 | 2021-05-05 16:25:38 | 2021-06-05 19:43:50 |
| 206 | 163.172.198.253 | 12876 | 163.172.0.0/16 | GB | 0 | Online SAS, FR | 585896 | 2020-10-08 19:18:01 | 2020-10-09 10:24:08 |
| 40 | 45.143.221.105 | 213371 | 45.143.221.0/24 | NL | 0 | SQUITTER-NETWORKS, NL | 366008 | 2020-09-22 15:07:27 | 2020-10-20 20:43:59 |
| 1312 | 193.46.255.98 | 47890 | 193.46.255.0/24 | RO | 0 | UNMANAGED-DEDICATED-SERVERS, GB | 336030 | 2021-04-18 21:44:59 | 2021-05-09 06:44:54 |
| 2186 | 212.83.189.43 | 12876 | 212.83.160.0/19 | FR | 0 | Online SAS, FR | 296158 | 2021-11-02 03:22:57 | 2021-11-06 01:32:16 |

10 rows in set (0,02 sec)

Esta es una tabla consolidada que se nutre de los logs de ataques que vamos registrando:

```
mysql> select * from ips_ataques_extended order by ultimo_ataque desc limit 10;
```

| id | ip | as_number | inet_num | country | netname | description | hints_ataques | primer_ataque | ultimo_ataque |
|------|----------------|-----------|-----------------|---------|---------|-----------------------|---------------|---------------------|---------------------|
| 9256 | 51.159.93.41 | 12876 | 51.158.0.0/15 | FR | 0 | Online SAS, FR | 60 | 2023-11-04 12:24:51 | 2024-01-10 09:43:35 |
| 9336 | 178.18.244.99 | 51167 | 178.18.240.0/20 | DE | 0 | CONTABO, DE | 3 | 2024-01-07 21:32:40 | 2024-01-10 05:15:53 |
| 9317 | 45.155.91.159 | 47154 | 45.155.91.0/24 | HK | 0 | HUSAM-NETWORK, PS | 24649 | 2023-12-27 09:42:58 | 2024-01-10 02:52:40 |
| 9285 | 78.153.140.222 | 202306 | 78.153.140.0/24 | RU | 0 | HOSTGLOBALPLUS-AS, GB | 90 | 2023-11-29 03:46:18 | 2024-01-10 02:22:19 |
| 9081 | 205.209.96.130 | 19318 | 205.209.96.0/19 | US | 0 | IS-AS-1, US | 36274 | 2023-08-16 01:48:08 | 2024-01-09 23:26:17 |
| 9296 | 87.98.243.61 | 16276 | 87.98.128.0/17 | FR | 0 | OVH, FR | 24 | 2023-12-03 18:11:47 | 2024-01-09 07:46:20 |
| 9310 | 205.209.104.2 | 19318 | 205.209.96.0/19 | US | 0 | IS-AS-1, US | 56369 | 2023-12-22 21:07:31 | 2024-01-08 22:06:42 |
| 9012 | 45.155.91.75 | 47154 | 45.155.91.0/24 | HK | 0 | HUSAM-NETWORK, PS | 45 | 2023-07-26 21:26:16 | 2024-01-08 14:06:11 |
| 9337 | 185.243.5.26 | 23470 | 185.243.5.0/24 | HK | 0 | RELIABLESITE, US | 1 | 2024-01-08 10:34:28 | 2024-01-08 10:34:28 |
| 9332 | 23.148.146.197 | 46664 | 23.148.146.0/24 | US | 0 | VDI-NETWORK, US | 1500 | 2024-01-06 06:24:38 | 2024-01-08 03:53:32 |

10 rows in set (0,02 sec)

:: Ataques SIP y otras hierbas ::

Ejemplo de cómo usarlo:

- Hacemos una pequeña API y mediante una sencilla consulta, tenemos las ip's de los bots, por ejemplo:

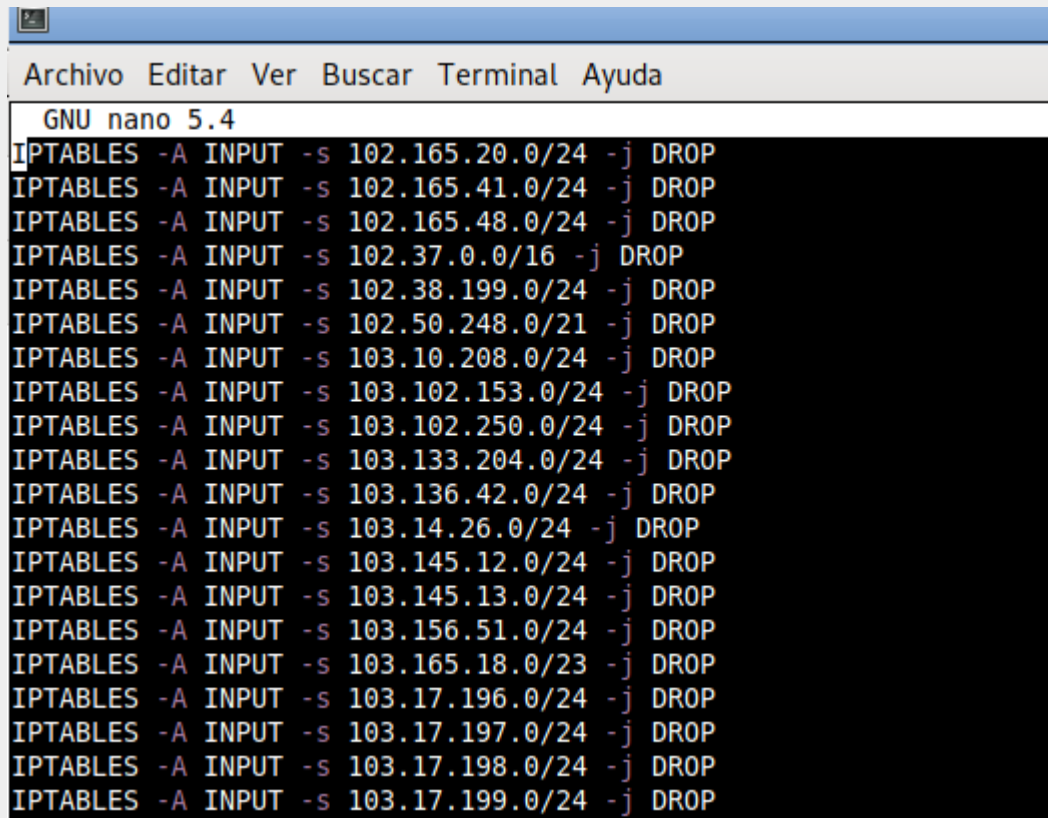


A screenshot of a web browser window. The address bar shows the URL `192.168.17.2:10000/listPREF?user_id=angel&token_id=2bXHytEI81lYn4ATuH9cpCp9LgsleJ` with a "Not secure" warning. The main content area displays a JSON response:

```
{
  "blocked-ips": [
    "102.165.20.0/24",
    "102.165.41.0/24",
    "102.165.48.0/24",
    "102.37.0.0/16",
    "102.38.199.0/24",
    "102.50.248.0/21",
    "103.10.208.0/24",
    "103.102.153.0/24",
    "103.102.250.0/24",
    "103.133.204.0/24",
    "103.136.42.0/24",
    "103.14.26.0/24",
    "103.145.12.0/24",
    "103.145.13.0/24",
    "103.156.51.0/24",
    "103.165.18.0/23",
    "103.17.196.0/24",
    "103.17.197.0/24",
    "103.17.198.0/24",
    "103.17.199.0/24",
    "103.204.223.0/24",
    "103.215.195.0/24",
    "103.225.136.0/24",
    "103.235.210.0/24",
    "103.25.59.0/24",
  ]
}
```

:: Ataques SIP y otras hierbas ::

Ejemplo para iptables / ipset:



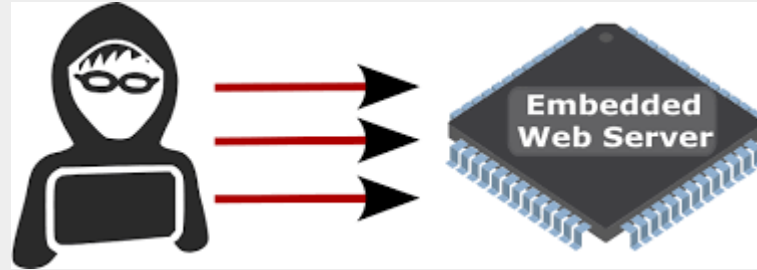
The image shows a terminal window with the GNU nano 5.4 editor. The menu bar at the top includes 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The editor contains a list of iptables rules, each starting with 'IPTABLES -A INPUT -s' followed by an IP address and subnet mask, and ending with '-j DROP'. The rules are for various IP ranges, including 102.165.20.0/24, 102.165.41.0/24, 102.165.48.0/24, 102.37.0.0/16, 102.38.199.0/24, 102.50.248.0/21, 103.10.208.0/24, 103.102.153.0/24, 103.102.250.0/24, 103.133.204.0/24, 103.136.42.0/24, 103.14.26.0/24, 103.145.12.0/24, 103.145.13.0/24, 103.156.51.0/24, 103.165.18.0/23, 103.17.196.0/24, 103.17.197.0/24, 103.17.198.0/24, and 103.17.199.0/24.

```
GNU nano 5.4
IPTABLES -A INPUT -s 102.165.20.0/24 -j DROP
IPTABLES -A INPUT -s 102.165.41.0/24 -j DROP
IPTABLES -A INPUT -s 102.165.48.0/24 -j DROP
IPTABLES -A INPUT -s 102.37.0.0/16 -j DROP
IPTABLES -A INPUT -s 102.38.199.0/24 -j DROP
IPTABLES -A INPUT -s 102.50.248.0/21 -j DROP
IPTABLES -A INPUT -s 103.10.208.0/24 -j DROP
IPTABLES -A INPUT -s 103.102.153.0/24 -j DROP
IPTABLES -A INPUT -s 103.102.250.0/24 -j DROP
IPTABLES -A INPUT -s 103.133.204.0/24 -j DROP
IPTABLES -A INPUT -s 103.136.42.0/24 -j DROP
IPTABLES -A INPUT -s 103.14.26.0/24 -j DROP
IPTABLES -A INPUT -s 103.145.12.0/24 -j DROP
IPTABLES -A INPUT -s 103.145.13.0/24 -j DROP
IPTABLES -A INPUT -s 103.156.51.0/24 -j DROP
IPTABLES -A INPUT -s 103.165.18.0/23 -j DROP
IPTABLES -A INPUT -s 103.17.196.0/24 -j DROP
IPTABLES -A INPUT -s 103.17.197.0/24 -j DROP
IPTABLES -A INPUT -s 103.17.198.0/24 -j DROP
IPTABLES -A INPUT -s 103.17.199.0/24 -j DROP
```

:: Ataques SIP y otras hierbas ::

¿ Cómo dar más funcionalidades a nuestro honeypot: ?

- Añadimos servicios interesantes como un servidor web y vulnerable, clonando al máximo el comportamiento



:: Ataques SIP y otras hierbas ::

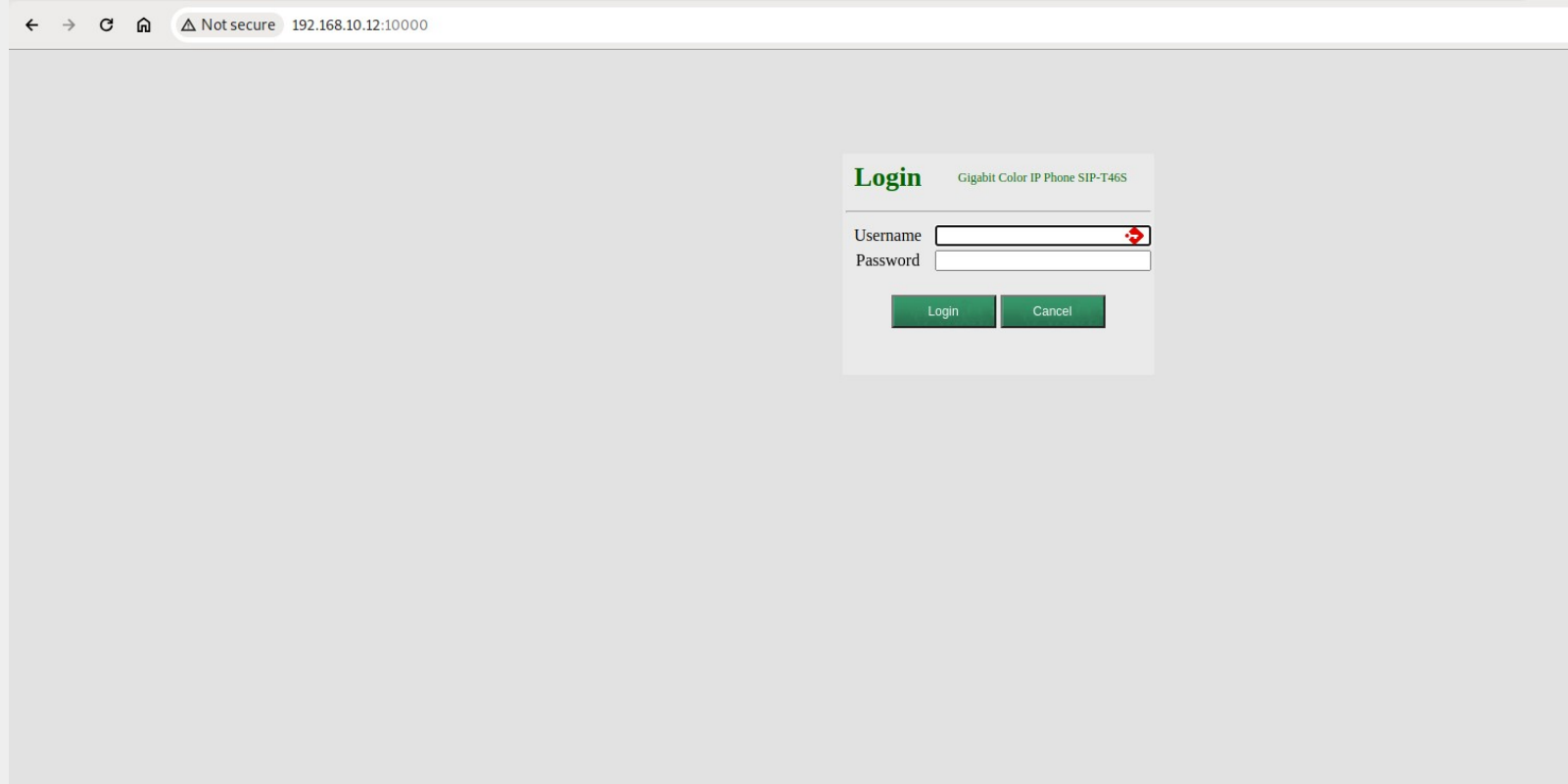
Seguimos con los HoynePot. Exponemos ahora un teléfono Yealink y recopilamos más datos para nuestra BBDD de atacantes:

The image shows a screenshot of the 'mc' (Midnight Commander) file manager interface. The title bar at the top indicates the current directory is '/usr/local/scripts/web-yealink' and the user is 'craem@bbs'. Below the title bar is a menu bar with options: 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The main window is split into two panes, 'Left' and 'Right', both showing the same directory listing. The 'Left' pane has a header with columns: '.n', 'Name', 'Size', 'Modify', and 'time'. The 'Right' pane has a similar header but includes an additional column for 'Options'. Both panes list the following files and directories: '..' (UP--DIR, Feb 5 08:23), '/custom' (4096, Feb 1 09:23), '/js' (4096, Feb 1 09:23), '/language' (4096, Feb 1 09:23), '/theme' (4096, Feb 1 09:23), and '*index.html' (3150, Jan 31 18:27). The 'Options' column in the 'Right' pane is currently empty.

Con un simple wget, podemos descargarla, corregimos los enlaces y en unos minutos, tenemos una web totalmente operativa.

:: Ataques SIP y otras hierbas ::

Ya tenemos la web operativa y lista para recopilar datos:



The screenshot shows a web browser window with the address bar displaying '192.168.10.12:10000' and a 'Not secure' warning. The main content area is a light gray background. In the center, there is a login form titled 'Login' for a 'Gigaset Color IP Phone SIP-T46S'. The form includes two input fields: 'Username' and 'Password'. The 'Username' field has a red error icon on the right. Below the input fields are two buttons: 'Login' and 'Cancel'.

← → ↻ 🏠 ⚠ Not secure 192.168.10.12:10000

Login Gigaset Color IP Phone SIP-T46S

Username

Password

Login Cancel

:: Ataques SIP y otras hierbas ::

Show me the code:

```
@app.route('/', methods=['GET'])
def home():
    ip_remote = request.remote_addr
    user_agent = request.user_agent
    miBBDD = mysql.connector.connect(host=server_honeypot, user=user_honeypot, password=passwd_honeypot, database=database_honeypot)
    mycursor = miBBDD.cursor()
    consulta = "insert into logs_ataque (ip,user) values (%s, %s)"
    values = (ip_remote,'none')
    print(consulta,values)
    mycursor.execute(consulta, values)
    miBBDD.commit()
    disconnectDB(miBBDD)
    return render_template('index.html')

@app.route('/servlet', methods=['GET','POST'])
def servlet():
    if request.method == 'POST':
        username = request.form['idUsername']
        password = request.form['idPassword']
        ip_remote = request.remote_addr
        user_agent = request.user_agent
        miBBDD = mysql.connector.connect(host=server_honeypot, user=user_honeypot, password=passwd_honeypot, database=database_honeypot)
        mycursor = miBBDD.cursor()
        consulta = "insert into logs_ataque (ip,user,password) values (%s, %s, %s)"
        values = (ip_remote,username,password)
        mycursor.execute(consulta, values)
        miBBDD.commit()
        disconnectDB(miBBDD)

        return render_template('index.html', message='Incorrect username or password!')
    return render_template('index.html')

if __name__ == '__main__':
    app.run(host='0.0.0.0',debug=False, port=10000, threaded=True)
```


:: Ataques SIP y otras hierbas ::

Y si dejamos unos días capturando.... Podremos seguir alimentando nuestra bbdd con ip's que "curiosean" nuestro honeyPot.

```
mysql> select * from logs_ataque;
```

| id_log_ataque | date_time | user_agent | ip | user | password |
|---------------|---------------------|------------|-----------------|-------|----------|
| 1 | 2024-02-02 22:47:29 | 0 | 192.168.7.80 | admin | admin |
| 2 | 2024-02-04 09:39:56 | 0 | 192.168.7.76 | none | NULL |
| 3 | 2024-02-04 09:55:03 | 0 | 83.97.73.245 | none | NULL |
| 4 | 2024-02-04 10:31:19 | 0 | 146.19.24.23 | none | NULL |
| 5 | 2024-02-04 10:31:28 | 0 | 147.78.103.13 | none | NULL |
| 6 | 2024-02-04 11:11:43 | 0 | 102.36.156.23 | none | NULL |
| 7 | 2024-02-04 12:01:00 | 0 | 195.170.172.128 | none | NULL |
| 8 | 2024-02-04 12:53:28 | 0 | 146.19.24.23 | none | NULL |
| 9 | 2024-02-04 14:08:50 | 0 | 146.19.24.23 | none | NULL |
| 10 | 2024-02-04 14:56:18 | 0 | 18.246.6.20 | none | NULL |
| 11 | 2024-02-04 15:31:03 | 0 | 146.19.24.23 | none | NULL |
| 12 | 2024-02-04 16:01:42 | 0 | 44.235.77.134 | none | NULL |
| 13 | 2024-02-04 16:06:25 | 0 | 147.78.103.13 | none | NULL |
| 14 | 2024-02-05 08:26:59 | 0 | 192.168.250.42 | none | NULL |

```
14 rows in set (0,00 sec)
```

:: Ataques SIP y otras hierbas ::

Conclusiones rápidas:

- La mayoría suelen ser equipos en clouds públicos, máquinas con firewall débil o con poco mantenimiento / monitorización.
- Muchos descuidos y exposiciones de puertos con servicios vulnerables, como rdp, ssh, ntp, dns y son sistemas usados para hacer de proxy.

```
mysql> select * from ips_ataques_extended where country='ES';
```

| id | ip | as_number | inet_num | country | netname | description | hints_ataques | primer_ataque | ultimo_ataque |
|------|----------------|-----------|------------------|---------|---------|------------------------------------------|---------------|---------------------|---------------------|
| 3 | 185.124.31.143 | 12479 | 185.124.31.0/24 | ES | 0 | UNI2-AS, ES | 1 | 2020-09-20 19:34:29 | 2020-09-20 19:34:29 |
| 853 | 91.126.70.139 | 35699 | 91.126.68.0/22 | ES | 0 | ADAMOEU-AS Adamo Telecom Iberia S.A., ES | 23 | 2021-02-07 11:30:55 | 2021-02-07 11:34:59 |
| 1022 | 185.118.188.58 | 203936 | 185.118.188.0/24 | ES | 0 | MismeNet Telecomunicaciones, ES | 4 | 2021-03-16 07:29:32 | 2021-03-16 07:30:32 |
| 1640 | 37.15.216.249 | 12479 | 37.15.216.0/22 | ES | 0 | UNI2-AS, ES | 2 | 2021-07-04 09:10:26 | 2021-07-04 09:10:29 |
| 1926 | 212.170.63.51 | 3352 | 212.170.0.0/16 | ES | 0 | TELEFONICA DE ESPANA, ES | 2 | 2021-08-30 08:14:49 | 2021-08-30 08:14:53 |
| 2312 | 185.59.66.98 | 56882 | 185.59.66.0/24 | ES | 0 | NET-LEAST-COST-ROUTING-TELECOM-SL, ES | 7 | 2021-12-25 23:37:44 | 2022-06-09 04:49:22 |
| 2683 | 188.65.89.140 | 15704 | 188.65.88.0/21 | ES | 0 | AS15704, ES | 1 | 2022-03-16 17:37:39 | 2022-03-16 17:37:39 |
| 3088 | 46.251.252.254 | 56882 | 46.251.252.0/23 | ES | 0 | NET-LEAST-COST-ROUTING-TELECOM-SL, ES | 5 | 2022-06-10 15:31:46 | 2022-06-11 03:51:01 |
| 7511 | 82.223.49.116 | 8560 | 82.223.0.0/16 | ES | 0 | IONOS-AS | 4 | 2022-10-07 22:41:17 | 2022-10-14 06:25:35 |
| 7629 | 88.12.35.164 | 3352 | 88.12.0.0/16 | ES | 0 | TELEFONICA DE ESPANA, ES | 1 | 2022-10-27 02:33:49 | 2022-10-27 02:33:49 |
| 8257 | 88.18.197.180 | 3352 | 88.18.0.0/16 | ES | 0 | TELEFONICA DE ESPANA, ES | 12 | 2023-02-16 05:07:23 | 2023-02-16 05:21:03 |
| 8563 | 78.136.83.179 | 29119 | 78.136.64.0/18 | ES | 0 | SERVIHOSTING-AS AireNetworks, ES | 243 | 2023-03-26 23:41:23 | 2023-04-03 15:50:16 |
| 8668 | 185.128.60.18 | 203614 | 185.128.60.0/22 | ES | 0 | WIFIIBERICA, ES | 1 | 2023-04-13 02:32:54 | 2023-04-13 02:32:54 |
| 8726 | 89.44.68.254 | 29119 | 89.44.64.0/21 | ES | 0 | SERVIHOSTING-AS AireNetworks, ES | 1 | 2023-04-26 23:36:42 | 2023-04-26 23:36:42 |
| 9158 | 83.54.118.112 | 3352 | 83.54.0.0/16 | ES | 0 | TELEFONICA DE ESPANA, ES | 7 | 2023-09-19 01:34:39 | 2023-09-19 01:39:06 |

15 rows in set (0,01 sec)

:: Ataques SIP y otras hierbas ::

En resumen, nos puede servir para:

- crear listas de reputación de ip's.
- crear listas para enviar blackhole's a los routers con communities o acl's.
- crear lista para ip's de iptables / ipset.
- Reportar a abuse.



:: Ataques SIP y otras hierbas ::

