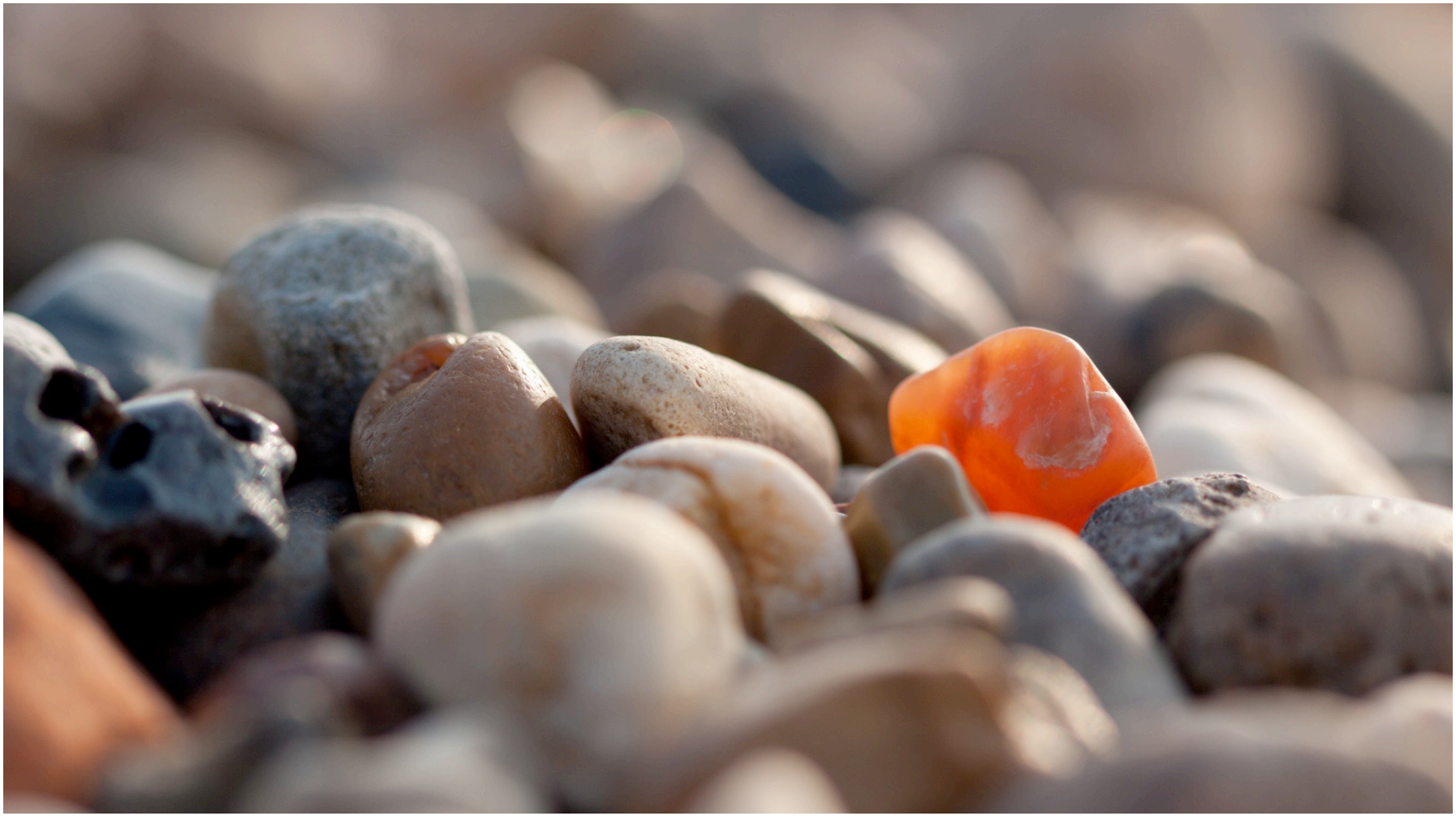

JaCkSecurity

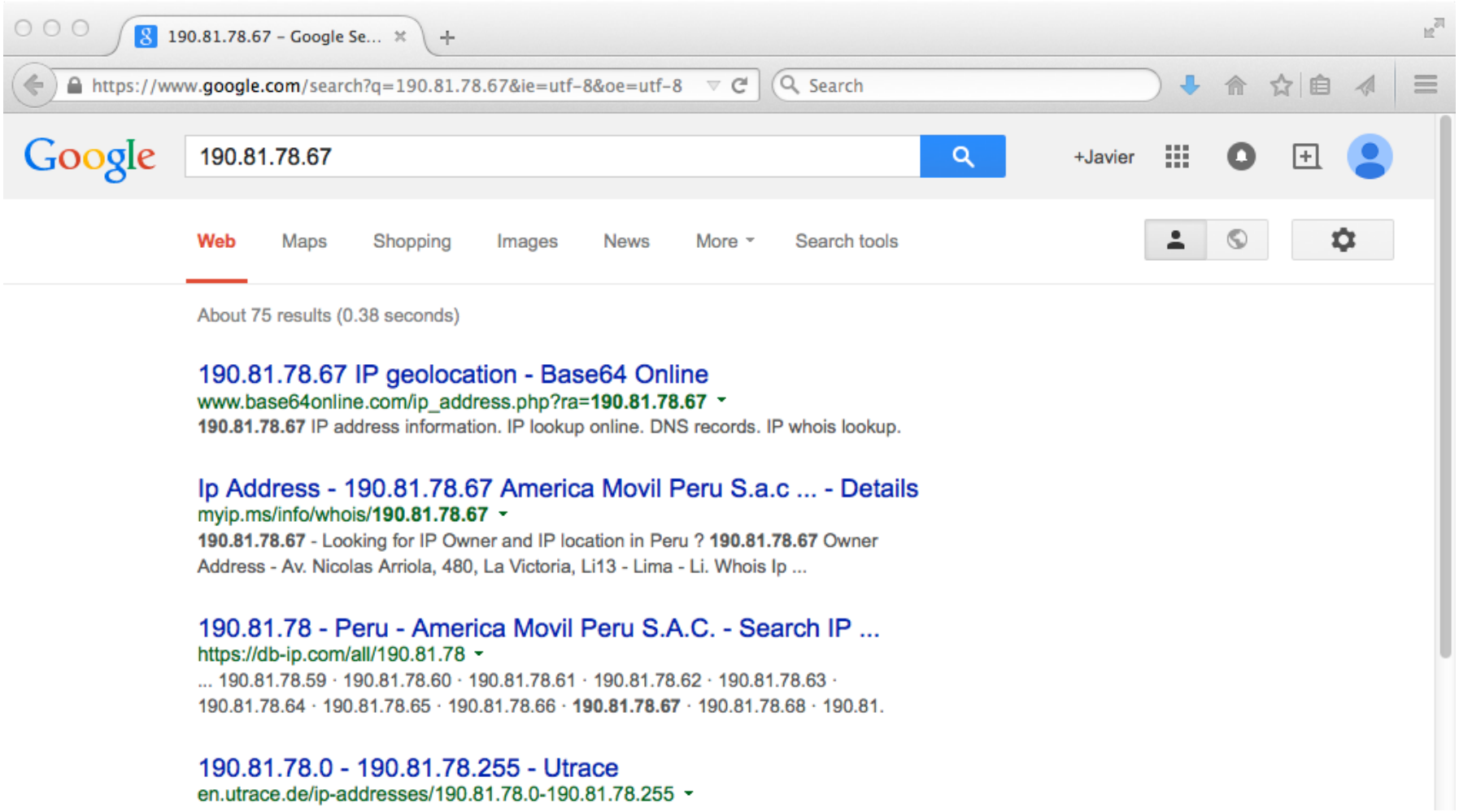
Aspectos requeridos en un incidente



Primeras básicas

- Algunas herramientas conocidas
  1. Googlear
  2. Whois
  3. DNS reverso
  4. Solicitar la identidad del propietario final al ISP
  5. Power searching de sitios web
  6. Power searching de hosts
  7. Power searching agresivo ¡PELIGRO!
  8. Vecinos Invasores ¡PELIGRO!

Googlear


190.81.78.67 - Google Se...
https://www.google.com/search?q=190.81.78.67&ie=utf-8&oe=utf-8
Search
Google
190.81.78.67
+Javier
Web
Maps
Shopping
Images
News
More
Search tools
About 75 results (0.38 seconds)
190.81.78.67 IP geolocation - Base64 Online
www.base64online.com/ip_address.php?ra=190.81.78.67
190.81.78.67 IP address information. IP lookup online. DNS records. IP whois lookup.
Ip Address - 190.81.78.67 America Movil Peru S.a.c ... - Details
myip.ms/info/whois/190.81.78.67
190.81.78.67 - Looking for IP Owner and IP location in Peru ? 190.81.78.67 Owner Address - Av. Nicolas Arriola, 480, La Victoria, Li13 - Lima - Li. Whois Ip ...
190.81.78 - Peru - America Movil Peru S.A.C. - Search IP ...
https://db-ip.com/all/190.81.78
... 190.81.78.59 · 190.81.78.60 · 190.81.78.61 · 190.81.78.62 · 190.81.78.63 · 190.81.78.64 · 190.81.78.65 · 190.81.78.66 · 190.81.78.67 · 190.81.78.68 · 190.81.
190.81.78.0 - 190.81.78.255 - Utrace
en.utrace.de/ip-addresses/190.81.78.0-190.81.78.255

1) Googlear

- For example, a request message could be sent from an HTTP/1.0 user agent to an internal proxy code-named "fred", which uses HTTP/1.1 to forward the request to a public proxy at nowhere.com, which completes the request by forwarding it to the origin server at www.ics.uci.edu. The request received by www.ics.uci.edu would then have the following Via header field:

```
Via: 1.0 fred, 1.1 nowhere.com (Apache/1.1)
```

1) Googlear

- For example, a request message could be sent from an HTTP/1.0 user agent to an internal proxy code-named ”ISACA", which uses HTTP/1.1 to forward the request to a public proxy at JACKSECURITY, which completes the request by forwarding it to the origin server at www.ics.uci.edu. The request received by www.ics.uci.edu would then have the following Via header field:

```
Via: 1.0 ISACA, 1.1 JACKSECURITY(Apache/1.1)
```

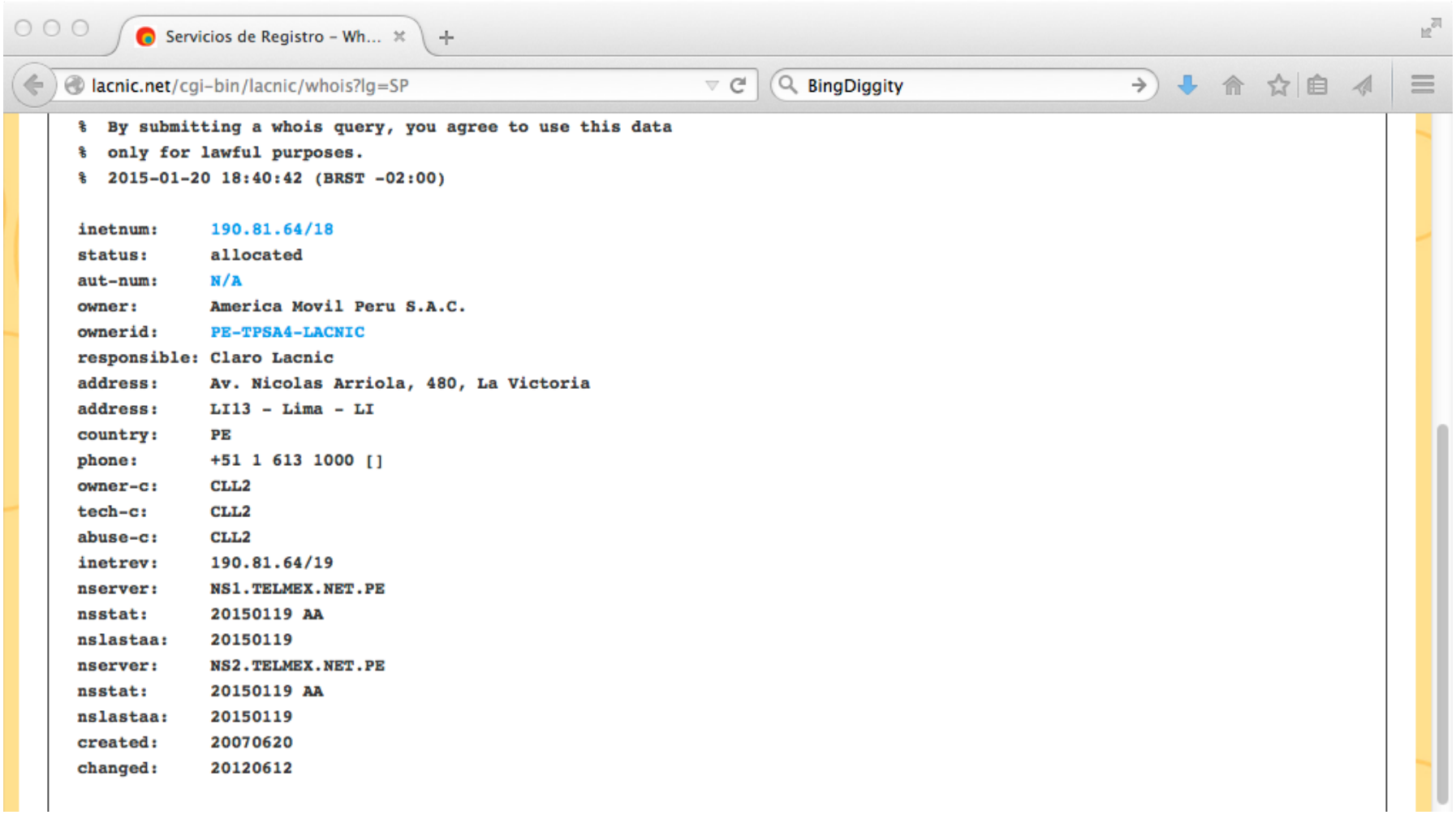
1) Googlear

- Pros:
  - Inmediato
- Cons:
  - Dependes de la suerte en extremo
    - La dir. IP puede pertenecer a un sitio web corporativo
      - **Recuerda:** la dir. IP que te agredió puede ser una víctima más
    - La dir. IP puede haber quedado registrado en un log de algún sistema de Internet, y dicho log estar disponible para ti
      - **Golazo:** si es un log de un web server, y logras visualizar la etiqueta VIA en la cabecera HTTP
        - » http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.45
- Source:
  - La base de datos de Google

2) Whois


Servicios de Registro - Wh...
lacnic.net/cgi-bin/lacnic/whois?lg=SP
owasp
lacnic
Servicios de Registro - Whois
es en pt
Whois
190.81.78.67
BUSCAR
Como buscar:
IDs: Llene el User ID. Los ID's se hacen con tres letras seguido o no por un cierto número.
Organizaciones: Llene el OrgID (owner-id) de la organización. El formato de los OrgIDs se componen con el código del país inicial de la organización y LACNIC.
ASN: Llene el número del sistema autónomo: 1251 o AS1251.
IP o bloque CIDR: Llene una dirección IP (200.200.200.200) o uno bloque CIDR (200.200/16).

2) Whois




```
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2015-01-20 18:40:42 (BRST -02:00)

inetnum:     190.81.64/18
status:      allocated
aut-num:     N/A
owner:       America Movil Peru S.A.C.
ownerid:     PE-TPSA4-LACNIC
responsible: Claro Lacnic
address:     Av. Nicolas Arriola, 480, La Victoria
address:     LI13 - Lima - LI
country:     PE
phone:       +51 1 613 1000 []
owner-c:     CLL2
tech-c:      CLL2
abuse-c:     CLL2
inetrev:     190.81.64/19
nserver:     NS1.TELMEX.NET.PE
nsstat:      20150119 AA
nslastaa:    20150119
nserver:     NS2.TELMEX.NET.PE
nsstat:      20150119 AA
nslastaa:    20150119
created:     20070620
changed:     20120612
```

2) Whois

- Pros:
  - Sólo si quieres contactarte con el ISP del agresor
- Cons:
  - La información ya no es específica
  - Si la hallas específica, de seguro es errada (por ser antiguo)
- Source:
  - La base de datos de ARIN/LACNIC/RIPE (desactualizada)

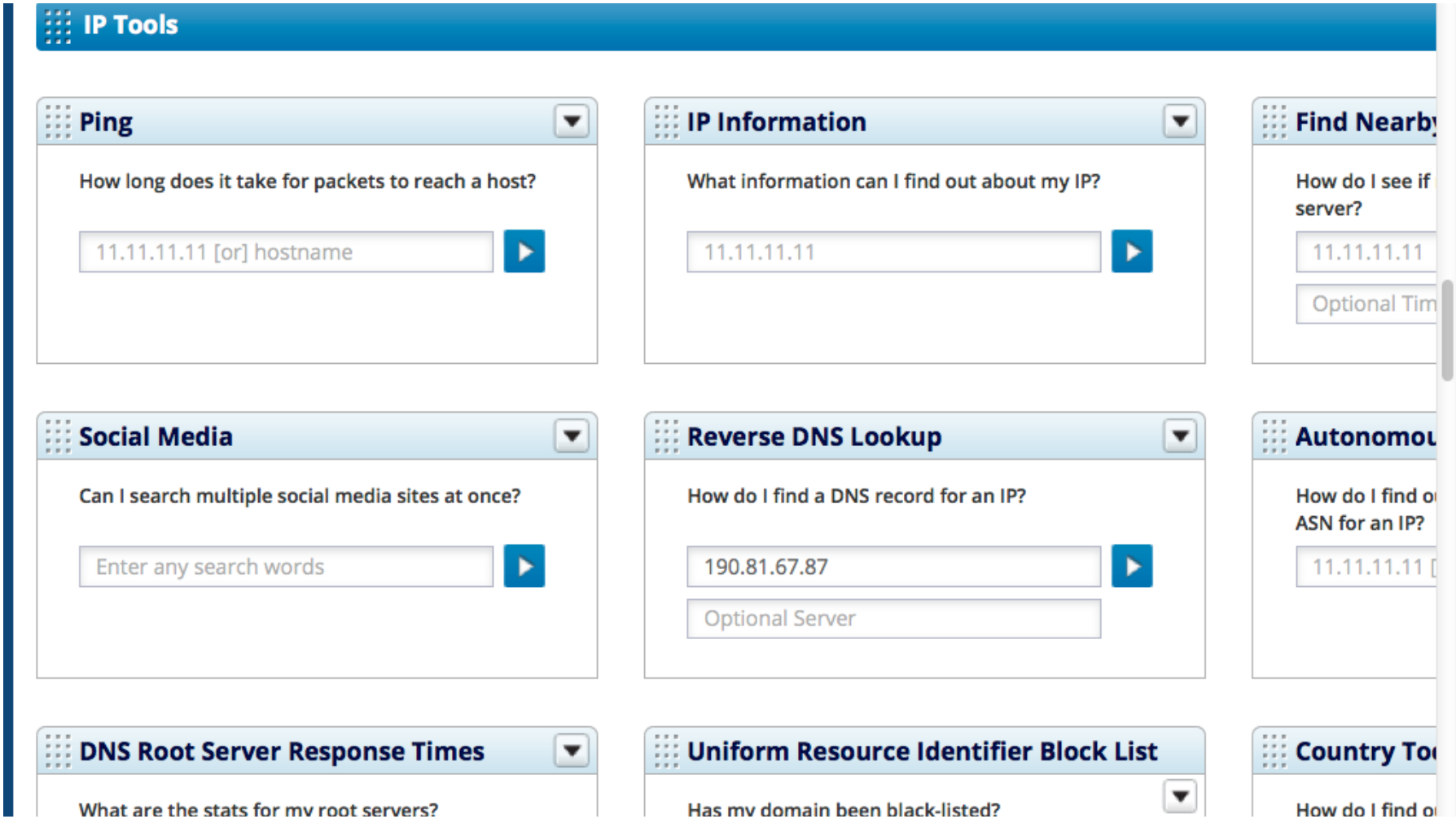
Intermediación

- Pros:
  - Es una buena estrategia
  - Usar al CSIRT del ISP (telco) como intermediario, para lanzar una seria advertencia al agresor
- Cons:
  - Supones que tu agresor tiene una dirección IP fija
  - Si lo usas para dirección IP dinámicas, el CSIRT del ISP (telco) tendrá un motivo más para hacerte esto:

3) DNS reverso (registro PTR del IP)

- This test will see if a reverse DNS entry exists for an IP address, and will also show you how the entry is found (the route of DNS servers that is taken), and who to contact to get a reverse DSN entry if none is found. The RFCs say that you should have a reverse DNS entry for every host on the Internet.

3) DNS reverso (registro PTR del IP)



3) DNS reverso (registro PTR del IP)

Nslookup

> set type=ptr

> 200.37.10.35

Server: dns2.unired.net.pe

Address: 200.37.10.35#53

35.10.37.200.in-addr.arpa name = dns2.unired.net.pe.

3) DNS reverso (registro PTR del IP)

- Pros:
  - Muy pocos
- Cons:
  - Requiere habilidad para identificar el DNS donde se alojan el PTR que buscas
  - Información no actualizada (muy descuidada por los DNS admins de los ISP)
  - Requieres tener acceso al DNS del ISP (ser cliente autorizado del servicio)
- Source:
  - Zona in-addr.arpa del DNS del ISP respectivo

4) Solicitar la ident. del propietario final al ISP

3.- ALCANCE

Los procedimientos de inspección y de requerimiento de información en relación al Secreto de las Telecomunicaciones y la Protección de Datos son aplicables a todas las empresas operadoras de Servicios Públicos de Telecomunicaciones.

4.- CONCEPTO

4.1 INVIOLABILIDAD Y SECRETO DE LAS TELECOMUNICACIONES

Se atenta contra la inviolabilidad y el secreto de las telecomunicaciones cuando deliberadamente una persona que no es quien cursa la comunicación, ni es el destinatario, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, utiliza, trata de conocer o facilitar que él mismo u otra persona conozca la existencia o el contenido de cualquier comunicación, de acuerdo a lo definido en el Artículo 10 del Reglamento General de la Ley de Telecomunicaciones.

4.2 PROTECCION DE DATOS E INFORMACION PERSONAL

Se atenta contra la protección de la información personal relativa a los abonados o usuarios cuando ésta es entregada a terceros i) sin el consentimiento previo, expreso y por escrito del abonado o usuario y además partes involucradas; o ii) sin una orden judicial específica motivada del Juez con las garantías previstas en la ley.

La obligación de protección de datos está referida única y exclusivamente a la información personal proporcionada por los abonados y usuarios a la empresa operadora en el curso de sus negocios . No se encuentra comprendida en los alcances de esta obligación la información personal que las empresas operadoras deben incluir en las guías de abonados que publiquen.

Reglamento del DS 020-2007-MTC

modificaciones a las definiciones de dichos términos se efectuarán mediante Decreto Supremo y previa audiencia pública cuando el Ministerio u Osiptel, en el caso de servicios públicos, consideren necesario recoger aportes de personas e instituciones especializadas.

Los términos no contenidos en dicho Glosario que se utilizan en el presente Reglamento tendrán el significado adoptado por el Convenio Internacional de la Unión Internacional de Telecomunicaciones.

SECCIÓN PRIMERA

DE LAS NORMAS GENERALES

Artículo 6º.- Régimen de libre competencia

Los servicios de telecomunicaciones se prestan en un régimen de libre competencia. A tal efecto están prohibidas las prácticas empresariales restrictivas de la leal competencia, entendiéndose por tales, entre otros, los acuerdos, actuaciones paralelas o prácticas concertadas entre empresas que produzcan o puedan producir el efecto de restringir, impedir o falsear la competencia.

Los titulares de concesiones y autorizaciones, en ningún caso podrán aplicar prácticas monopólicas restrictivas de la libre competencia, que impidan una competencia sobre bases equitativas con otros titulares de concesiones y autorizaciones de servicios de telecomunicaciones.

Artículo 7º.- Convergencia de servicios

El Estado ejerce una función promotora y facilitadora respecto al desarrollo de tecnologías de punta, propendiendo, en lo posible, a la convergencia de servicios y tecnologías, con la finalidad de otorgar mayores

El Ministerio elaborará el reglamento correspondiente.

Artículo 13º.- Inviolabilidad y secreto de las telecomunicaciones

Se atenta contra la inviolabilidad y el secreto de las telecomunicaciones, cuando deliberadamente una persona que no es quien origina ni es el destinatario de la comunicación, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, divulga, utiliza, trata de conocer o facilitar que él mismo u otra persona, conozca la existencia o el contenido de cualquier comunicación.

Las personas que en razón de su función tienen conocimiento o acceso al contenido de una comunicación cursada a través de los servicios públicos de telecomunicaciones, están obligadas a preservar la inviolabilidad y el secreto de la misma.

Los concesionarios de servicios públicos de telecomunicaciones están obligados a salvaguardar el secreto de las telecomunicaciones y la protección de datos personales, adoptar las medidas y procedimientos razonables para garantizar la inviolabilidad y el secreto de las comunicaciones cursadas a través de tales servicios, así como mantener la confidencialidad de la información personal relativa a sus usuarios que se obtenga en el curso de sus negocios, salvo consentimiento previo, expreso y por escrito de sus usuarios y demás partes involucradas o por mandato judicial.

Los titulares de servicios privados de telecomunicaciones deberán adoptar sus propias medidas de seguridad sobre inviolabilidad y secreto de las telecomunicaciones.

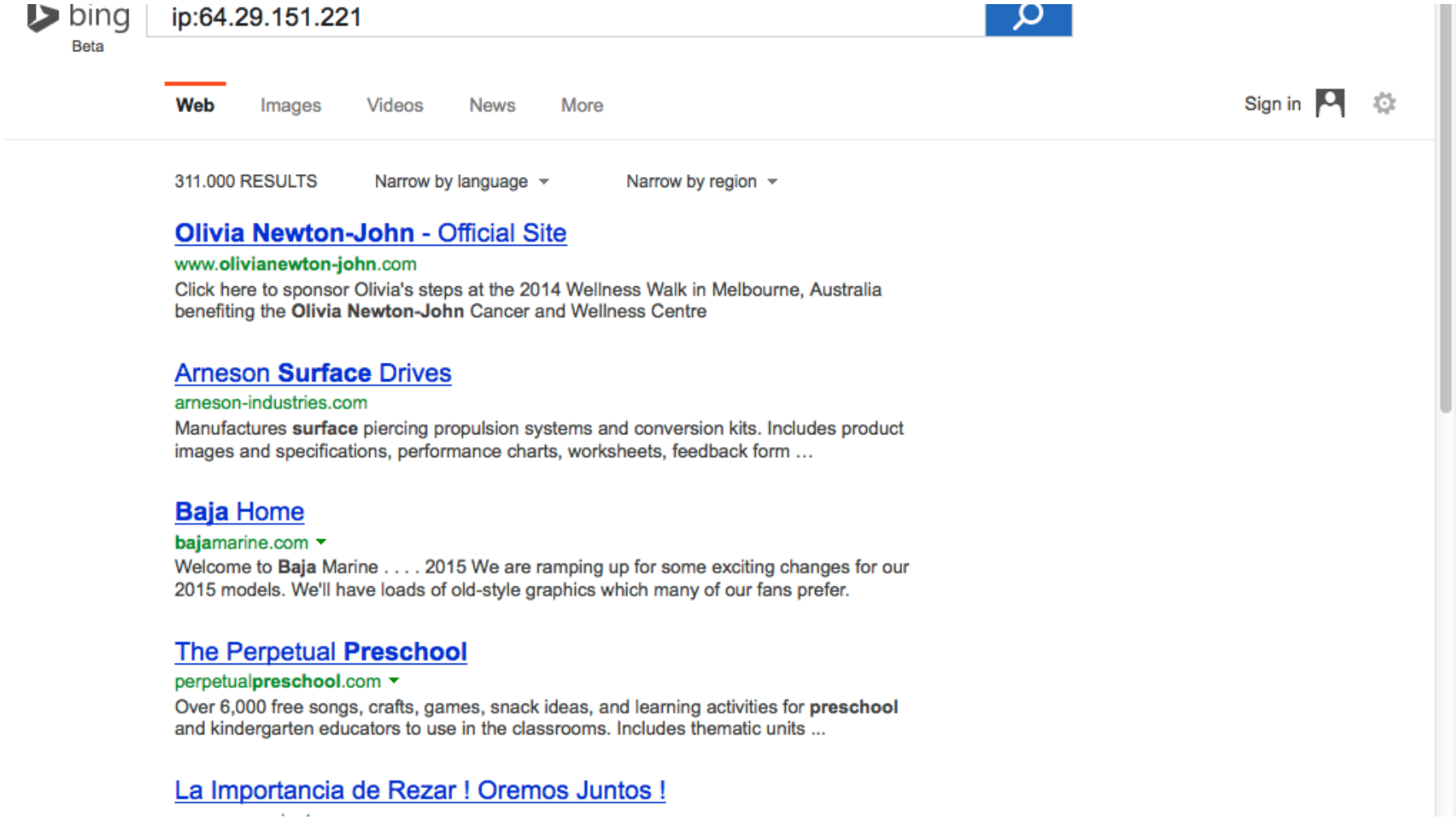
El Ministerio podrá emitir las disposiciones que sean necesarias para precisar los alcances del presente artículo.

4) Solicitar la ident. del propietario final al ISP

- Pros:
  - Ninguna.
- Cons:
  - Perder tiempo
  - Quedar en ridículo
- Source:
  - La base de datos del ISP

En resumen,...

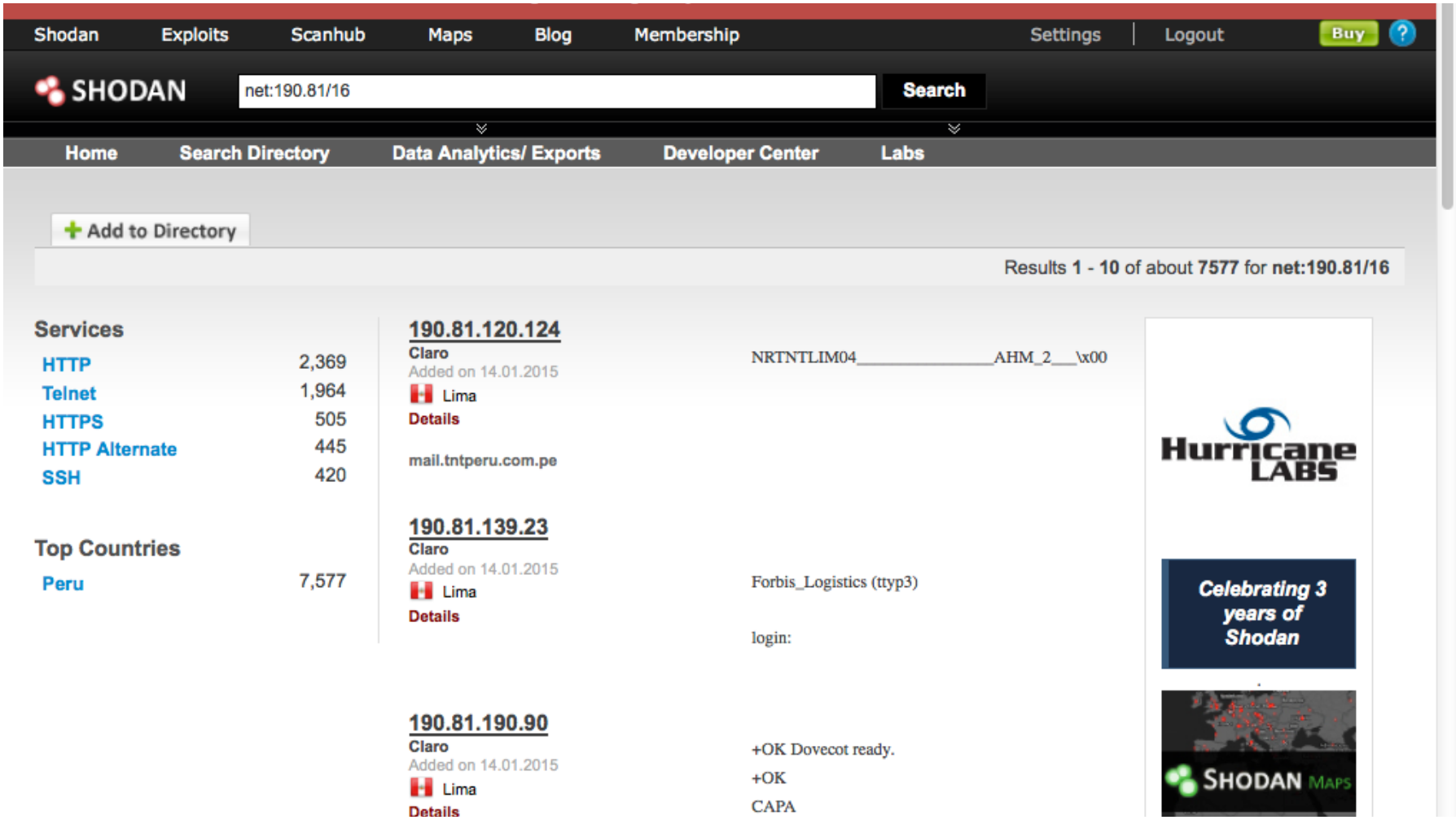
5) Power searching de sitios web



5) Power searching de sitios web

- Pros:
  - Primera forma básica de TRIANGULACIÓN legítima (sin agresión)
- Cons:
  - El vecindario de la dir. IP del agresor o el agresor puede no tener ningún sitio web publicado
- Source:
  - La base de datos de BING

6) Power searching de hosts



6) Power searching de hosts

- De acuerdo a un artículo de Forbes
  - *it's become a crucial tool for security researchers, academics, law enforcement and hackers looking for devices*

Web address	www.shodan.io
Type of site	search engine
Registration	Optional
Available in	English
Created by	John Matherly
Launched	2009
Current status	Active

6) Power searching de hosts

The 'country' filter is used to narrow results down by... country. It's useful for when you want to find computers running in a specific country.

Examples:
Apache servers located in Switzerland: **apache country:CH**
Nginx servers located in Germany: **nginx country:DE**

» geo

The 'geo' filter allows you to find devices that are within a certain radius of the given latitude and longitude. The filter accepts either 2 or 3 arguments. The optional third argument is the radius in kilometers within to search for computers (default: 5).

Examples:
Apache servers near 42.9693,-74.1224: **apache geo:42.9693,-74.1224**
Devices within a 50km radius of San Diego (32.8,-117): **geo:32.8,-117,50**

» hostname

The 'hostname' filter lets you search for hosts that contain the value in their hostname.

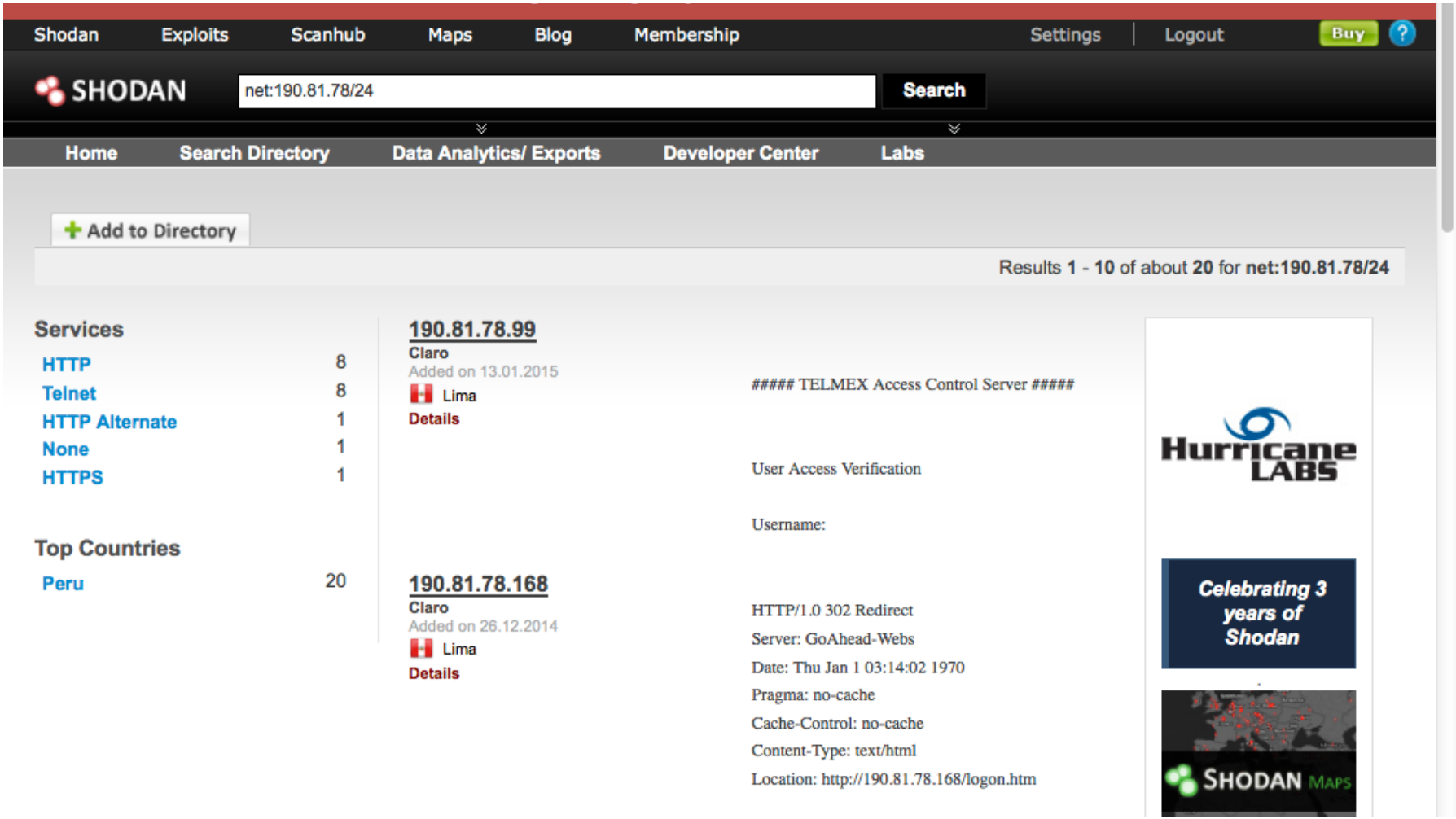
Examples:
GWS with 'google' in the hostname: **"Server: gws" hostname:google**
Nginx with '.de' in the hostname: **nginx hostname:.de**

» net

The 'net' filter provides a mechanism for limiting the search results to a specific IP or subnet. It uses CIDR notation to designate the subnet range. Here are a few examples:

Examples:
All data for IP 216.219.143.14: **net:216.219.143.14**
All data in the subnet 216.219.143.*: **net:216.219.143.0/24**
All data in the subnet 216.219.*: **net:216.219.0.0/16**

6) Power searching de hosts



6) Power searching de hosts

- Pros:
  - Primera forma básica de TRIANGULACIÓN legítima (sin agresión)
- Cons:
  - El vecindario de la dir. IP del agresor puede estar despoblado
- Source:
  - La base de datos de John Matherly
  - Otras base de datos (uffff!!! Ej. la de H.D. Moore)

¿Justificación?

- Datos del abonado obtenidos por la contratación de servicios de telecomunicaciones u otros, tales como:

  - Identificación del abonado, titularidad de la línea, código del cliente, servicios y equipos contratados, el número o dirección IP, titularidad de los nombres de usuario ("logins" o "users") y/o de las claves de acceso ("passwords") asociadas a un servicio determinado, la titularidad de las cuentas de correo electrónico y de cualesquiera servicios adicionales asociados a los servicios públicos de telecomunicaciones prestados por las Empresas del Grupo Telefónica.
  - Histórico de pedidos tales como traslados, cambio de número, averías, boletines de reparación y hojas de visita, etc.
  - Su ocupación, teléfonos de referencia, cuentas bancarias.
  - Modalidad y comportamiento de pago: pagos, pagos anticipados, pagos a plazos, notificación de recibos pendientes, recibos de servicios telefónicos, otros comprobantes de pagos, grabaciones por gestiones de deuda, entre otros.
  - Historial de suspensiones, cortes y reconexiones del servicio.
  - Origen de la suspensión del servicio distinto a la falta de pago, que hubiera motivado la conexión o desconexión del servicio.
  - Datos de reclamos, información del expediente y de los medios probatorios, el estado del reclamo (a un tercero ajeno al procedimiento), entrega del duplicado de recibo.
  - Resultado del control de llamadas maliciosas gestionado por el abonado debido a la

Excepción: se exceptúa la información que pueda obtenerse en guías telefónicas, en otros medios como páginas web de la Superintendencia Nacional de Administración Tributaria y de la Superintendencia Nacional de Registros Públicos o que, en general, tenga carácter de información pública.

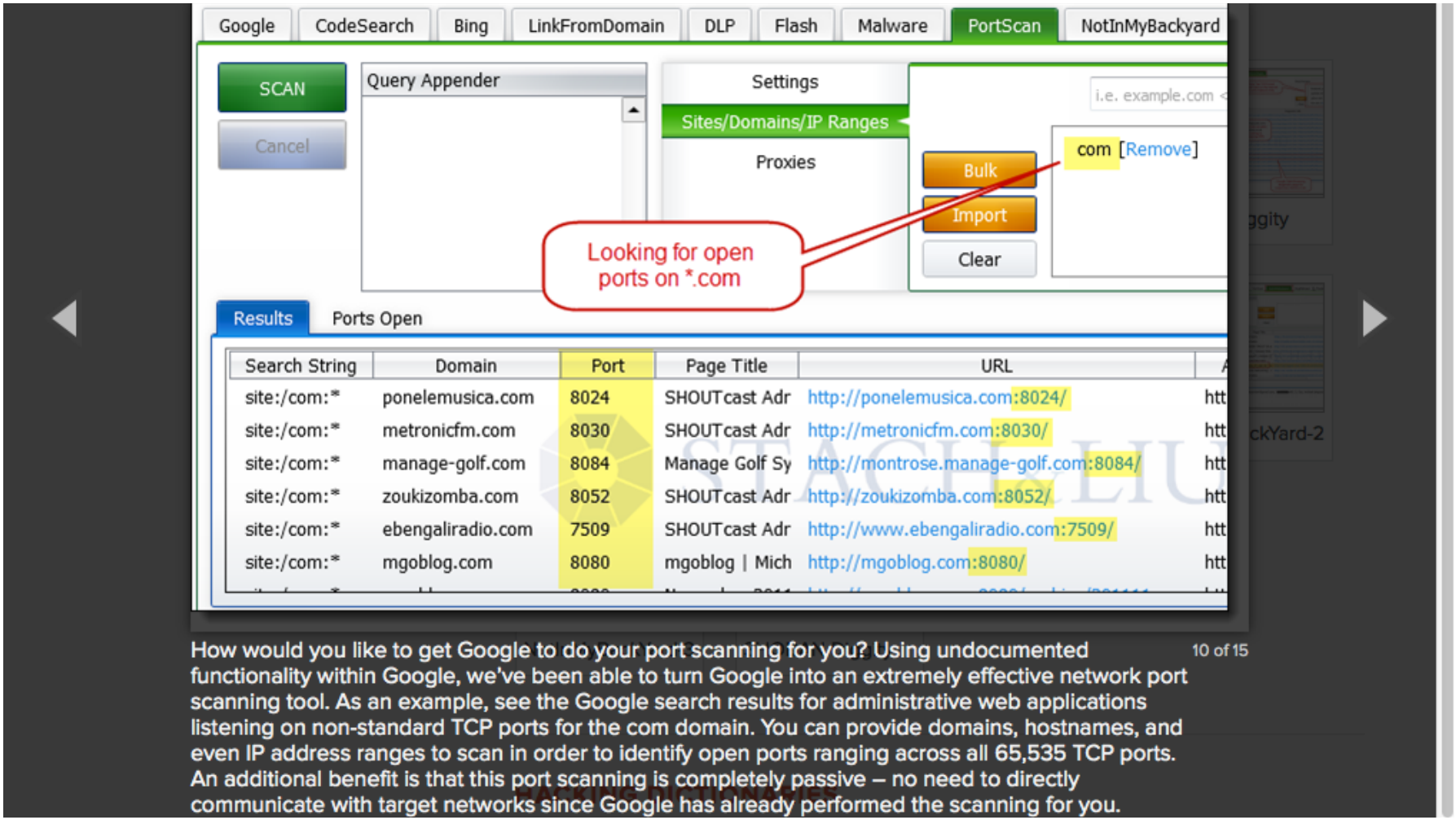
Excepción: se exceptúa la información que pueda obtenerse en guías telefónicas, en otros medios como páginas web de la Superintendencia Nacional de Administración Tributaria y de la Superintendencia Nacional de Registros Públicos o que, en general, tenga carácter de información pública.

La lista precedente no es exhaustiva ni limitativa. Frente a cualquier supuesto que origine duda debe solicitarse el apoyo correspondiente al área o gerencia de regulación del

excep | Highlight All | Match Case | 1 of 10 matches

¡DETENTE! estas a punto de cruzar la valla

6) Power searching agresivo



6) Power searching agresivo

- Pros:
  - Ninguna (en mi opinión)
- Cons:
  - Un motivo más para que sea visto poco ético
  - Un motivo para que el agresor te agreda más (una ciber guerra)
  - Un motivo para que no puedas nunca presentar cargos
- Source:
  - Online!

8) Vecinos invasores

escanear

hackear

ir a la reja

Cortesía de la Ley de Delitos Informáticos
Nº 30096


QuickTime Player Archivo Edición Visualización Ventana Ayuda
100% mar 07:25
Netflix
www.netflix.com/WiPlayer?movieid=70262504&trkid=13932984
Search
JACKSECURITY - JACK YOUR INCIDENTS NOW!
lacnic23
18/22 mayo - lima, perú
Estás viendo
The Good Wife
Temporada 1: Cap. 16
Moscas
Alicia y Will defienden a un abogado arrestado por asesinato. Peter planea estrategias con su equipo sobre cómo manejar su nuevo juicio y su rehabilitación pública.
Pausa

Importante

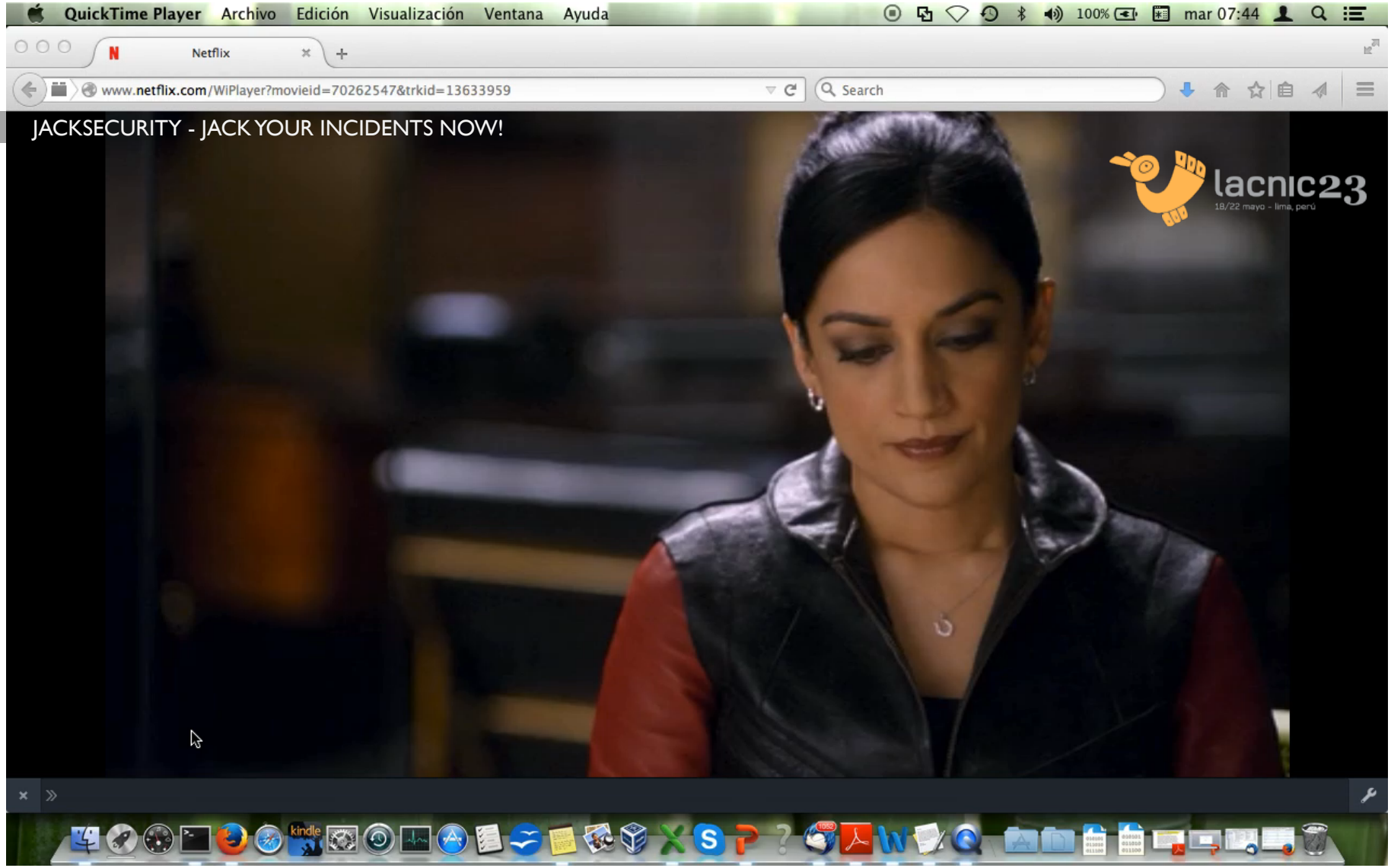
La siguiente presentación expresa los argumentos del presentador, y no deben ser interpretados como afirmaciones de la compañía. Asimismo, las técnicas mostradas aquí deben ser usadas bajo el balance ético profesional, y bajo algún tipo de consentimiento, y sin trasgredir la leyes existentes. Si Ud. no está deacuerdo con esto, no está obligado a quedarse en la sala, durante la presentación.

Advertencia ética

- *Ten cuidado con lo que deseas, porque es posible que se cumpla*

Significado del dicho

- Oyentes primerizos se confunden con su significado:
  - Dado que generalmente ellos desean que su deseo sea haga real
- El positivismo de esta frase puede confundirle, debido a la paradójica "advertencia" al inicio de la misma.
- Significado real:
  - Desear cosas y no percatarse de las consecuencias que podrían venir por lograr lo que desean


QuickTime Player Archivo Edición Visualización Ventana Ayuda
100% mar 07:44
Netflix
www.netflix.com/WiPlayer?movieid=70262547&trkid=13633959
Search
JACKSECURITY - JACK YOUR INCIDENTS NOW!
lacnic23
18/22 mayo - lima, perú

Antes de hacer triangulación

1. Ud. debe preguntarse qué:
    1. Qué hará cuando obtenga ese dato (no es información)
    2. Qué hará con esa dato (no es información)
2. Según esa respuesta, variará la técnica que elija.

El DATO

- Muchos routers responden (a Shodan o a estímulos TCP), muchos ISP emplean la misma posición y orden IP para sus routers o CPE (customer premise equipment)
- En Perú:
  - En países donde la penetración de Internet fue históricamente baja, los ISP crearon subnets desordenadas
- Extra-ventaja:
  - Nadie monitorea los routers, si reciben estímulos TCP, pues de hecho reciben miles de escaneos por semana.
- Nota:
  - Un estímulo TCP no es otra cosa que un paquete simple (sin flujo continuo)

Técnica: Triangular rango IP

- Sólo dos opciones conocidas
  - Asignado dir. IP por dir. IP
    - 192.168.100.1 Juan Pérez
    - 192.168.100.2 Juana Pérez
    - ...
  - Asignado en bloques (subnetting)
    - 192.168.100.0/24 Compañía Juan Pérez
    - 192.168.101.0/24 Compañía Juana Pérez
    - ...

Técnica: Triangular rango IP

- Secuencia:
  1. Alimentar datos con herramientas vistas antes
  2. ¿Es dinámica?
     - Determinar si la dir. IP es de un router doméstico
     - Determinar si la dir. IP siguiente es de otro router doméstico
  3. Ergo, es estática
     - Determinar el subnetting
       - Triangular información de herramientas vistas antes
       - Determinar dir. IP de los routers no-domésticos vecinos
         - » Lo más lejano a la dir. IP del agresor.

Técnica: Triangular rango IP

- Premisa:
  - La mayoría de ISP en el mundo asignan a los CPE (routers de última milla) una misma posición dentro de la subnet. P.E: xxx.xxx.106.0/29 (8 dir. IP)
    - xxx.xxx.106.0 (dir. ip de la red)
    - xxx.xxx.106.1 (router)
    - xxx.xxx.106.2
    - xxx.xxx.106.3
    - xxx.xxx.106.4
    - xxx.xxx.106.5
    - xxx.xxx.106.6
    - xxx.xxx.106.7 (dir. IP del broacast)

Técnica: Triangular rango IP

- Ergo:
  - Con cada router, determino, el inicio y fin de una subnet, al usar las calculadoras de subnets
    - xxx.xxx.106.1 (router)
    - xxx.xxx.106.9 (router)
    - xxx.xxx.106.17 (router)

Técnica: Triangular rango IP

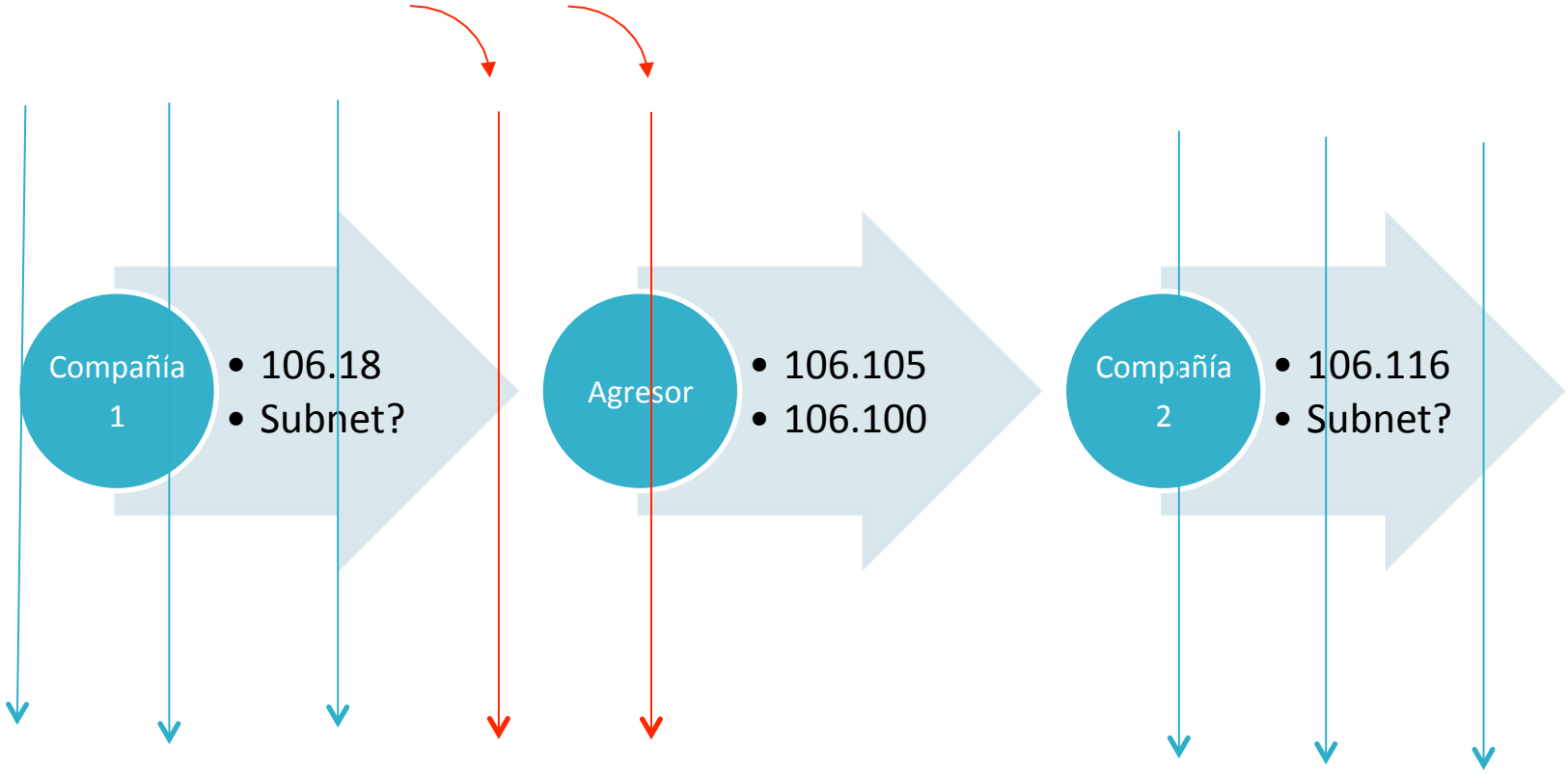
- Al ver un /28, un investigador sin conocimiento a lo indicado anteriormente asumirá erróneamente que todo el /24 (256 direcciones IP) tiene particiones de 16 dir. IP, es decir son 16 redes /28
  - 256 dir. IP / 16 dir. IP = 16 subnets
- A continuación, un ejemplo de *subnetting* desordenado

Técnica: Triangular rango IP

1. xxx.xxx.106.0/28
2. xxx.xxx.106.16/28
3. xxx.xxx.106.32/28
4. xxx.xxx.106.48/28
5. xxx.xxx.106.64/28
6. xxx.xxx.106.80/28
7. .
8. .
9. .
10. .
11. .
12. .
13. xxx.xxx.106.192/28
14. xxx.xxx.106.208/28
15. xxx.xxx.106.224/28
16. xxx.xxx.106.240/28

1. xxx.xxx.106.0/28
2. xxx.xxx.106.16/28
3. xxx.xxx.106.32/28
4. xxx.xxx.106.48/28
5. xxx.xxx.106.64/28
6. ***xxx.xxx.106.80/27***
7. xxx.xxx.106.112/28
8. .
9. .
10. .
11. xxx.xxx.106.192/28
12. xxx.xxx.106.208/28
13. xxx.xxx.106.224/28
14. xxx.xxx.106.240/28

Técnica: Triangular rango IP



Estímulos TCP

12:12:21.414949 IP 192.168.128.133.59409 > x.x.106.97.22: S 375561605:375561605(0) win 65535 <mss 1460,nop,wscale 3,nop,nop,timestamp[|tcp]>

12:12:21.474718 IP x.x.106.97.22 > 192.168.128.133.59409: R 0:0(0) ack 375561606 win 0

Estímulos TCP

12:13:19.637495 IP 192.168.128.133.59416 > x.x.106.113.22: S 75914324:75914324(0) win 65535 <mss 1460,nop,wscale 3,nop,nop,timestamp[|tcp]>

12:13:20.606500 IP 192.168.128.133.59416 > x.x.106.113.22: S 75914324:75914324(0) win 65535 <mss 1460,nop,wscale 3,nop,nop,timestamp[|tcp]>

12:13:21.607948 IP 192.168.128.133.59416 > x.x.106.113.22: S 75914324:75914324(0) win 65535 <mss 1460,nop,wscale 3,nop,nop,timestamp[|tcp]>

12:13:22.319747 IP x.x.106.113.22 > 192.168.128.133.59416: R 0:0(0) ack 75914325 win 0

12:13:22.440083 IP x.x.106.113.22 > 192.168.128.133.59416: R 0:0(0) ack 1 win 0

12:13:22.557948 IP x.x.106.113.22 > 192.168.128.133.59416: R 0:0(0) ack 1 win 0

Triangulando por la distancia (cuando no hay muchos routers)

12:29:38.823960 IP (tos 0x0, ttl 64, id 48573, offset 0, flags [DF], proto TCP (6), length 64) 192.168.128.133.59591 > x.x.106.81.22: S 4017224230:4017224230(0) win 65535 <mss 1460,nop,wscale 1,nop,nop,timestamp[|tcp]>

12:29:38.967264 IP (tos 0x0, ttl 243, id 50889, offset 0, flags [none], proto TCP (6), length 40) x.x.106.81.22 > 192.168.128.133.59591: R, cksum 0x699d (correct), 0:0(0) ack 4017224231 win 0

Metodología general

¿dinámica o estática?

perfilar al agresor, presentar cargos

Sentar precedente

Otras opciones

Dinámica

Identidad humana (estrategia corporativa)

A) Uso legal: presentar cargos

- Metodología general, pero sin escanear el rango IP del agresor
- Técnicas validas:
  1. Hallar el propietario vía:

ok 1. Googlear
ok 2. Whois
ok 3. DNS reverso (luego de verificar validez)
x 4. Solicitar la identidad del propietario final al ISP
ok 5. Power searching de sitios web
ok 6. Power searching de hosts

A) Uso legal: sentar un precedente

- Deberá seguir un proceso totalmente diferente a todos los descritos aquí, salvo que el dato que halló fue legítimamente público y tuvo toda la forma de información (un conjunto de datos que expresa una idea)
- Técnicas validas:
  1. Hallar el propietario vía

ok 1. Googlear
ok 2. Whois
ok 3. DNS reverso (luego de verificar validez)
ok 4. Solicitar la identidad del propietario final al ISP
ok 5. Power searching de sitios web
? 6. Power searching de hosts

B) Uso para información

- Podrías eventualmente "enviar estímulos TCP" (casi un escaneo, aventaja porque no es ruidoso)
- Técnicas válidas:

1. Hallar el propietario del bloque de direcciones IP

ok 1. Googlear
ok 2. Whois
ok 3. DNS reverso (luego de verificar validez)
x 4. Solicitar la identidad del propietario final al ISP
ok 5. Power searching de sitios web
ok 6. Power searching de hosts
ok 7. Estímulos TCP


Firefox File Edit View History Bookmarks Tools Window Help
mar 07:34
Netflix
www.netflix.com/WiPlayer?movieid=70262504&trkid=13932984
Search
JACKSECURITY - JACK YOUR INCIDENTS NOW!
lacnic23
18/22 mayo - lima, perú
Estás viendo
The Good Wife
Temporada 1: Cap. 16
Moscas
Alicia y Will defienden a un abogado arrestado por asesinato.
Peter planea estrategias con su equipo sobre cómo manejar
su nuevo juicio y su rehabilitación pública.
Los niños están acostados.
Los dejé ver algo de televisión.
Pausa

¿Cómo se hace esto?

- Centralizando datos
- Ejemplos:
  - Ser el dueño de la app (server)
  - Ser el dueño del DNS server
  - Ser el dueño de la red
  - Ser el dueño ...

El caso del centro del poder

- Se dice que Peter Peterson autor del libro para revisión del CCFP resolvió un caso en Perú hace decenas de años, al leer la dirección IP en la cabecera de correo.
- Cool! (eso ya no funciona ahora)

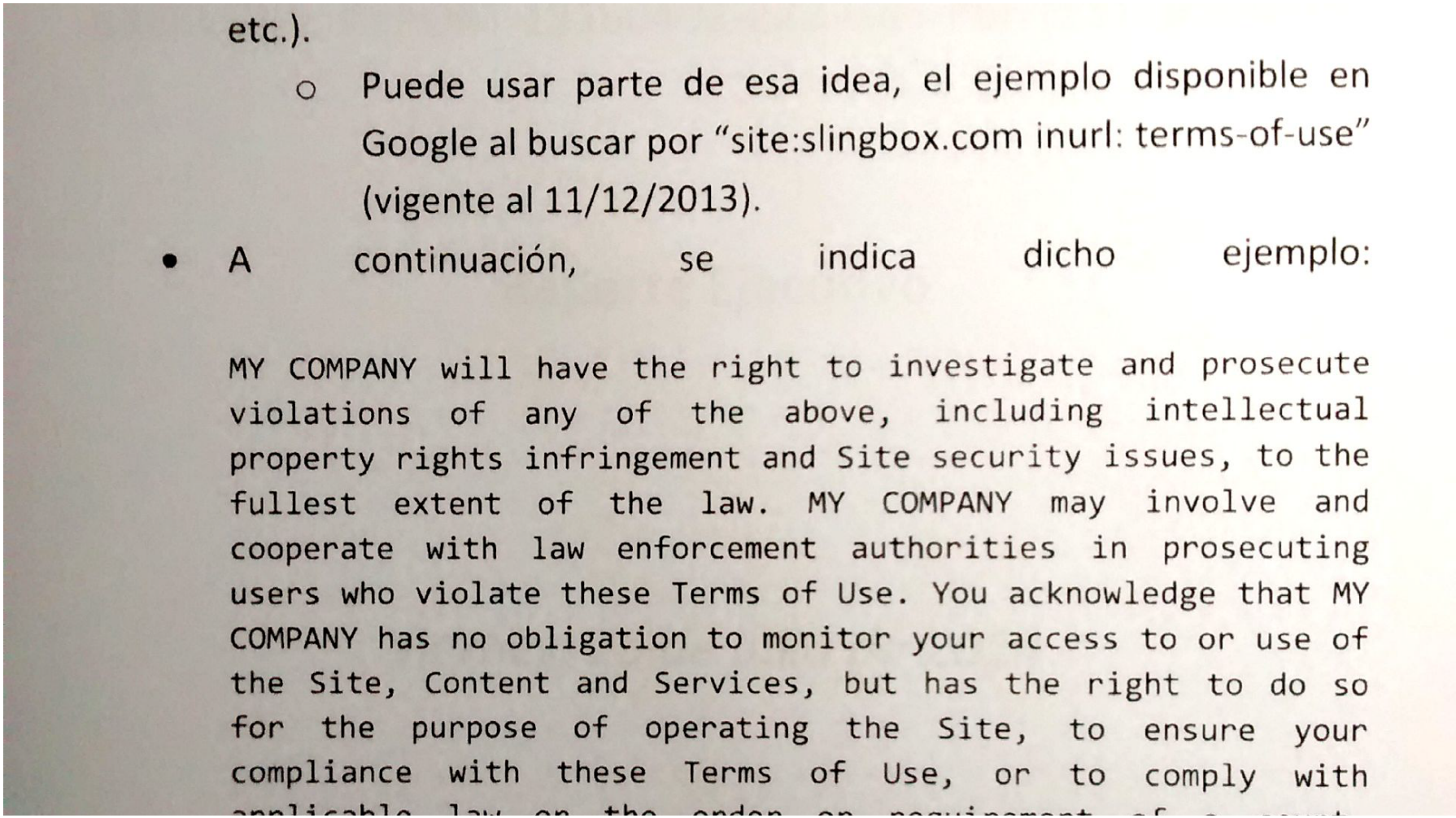
Incidentes

- La pregunta no es cómo, sino para qué lo necesitas!
- El mejor uso (sin consecuencias legales)
  - Establecer perfiles de campañas de ataque
  - Sin embargo, ...

Arma importante

- La página web no exhibe un banner o término de uso o término de servicio que –entre otras cosas:
  - Indique el tratamiento de conductas y acciones no permitidas, sospechosas o ilegales
  - Donde se exprese claramente que el usuario y/o visitante (sea o no legítimo de la aplicación y/o sitio web) consiente a la compañía el derecho a investigar y demandarlo por sospechas de violación y/o violaciones a cualquiera de los puntos tratados en los términos de uso (TOS).
  - Donde se exprese que la compañía se reserve el derecho a involucrarse o cooperar con las autoridades policiales por la violación de estos términos de uso (TOS).

Ejemplo del arma



etc.).

- Puede usar parte de esa idea, el ejemplo disponible en Google al buscar por "site:slingbox.com inurl: terms-of-use" (vigente al 11/12/2013).

- A continuación, se indica dicho ejemplo:

MY COMPANY will have the right to investigate and prosecute violations of any of the above, including intellectual property rights infringement and Site security issues, to the fullest extent of the law. MY COMPANY may involve and cooperate with law enforcement authorities in prosecuting users who violate these Terms of Use. You acknowledge that MY COMPANY has no obligation to monitor your access to or use of the Site, Content and Services, but has the right to do so for the purpose of operating the Site, to ensure your compliance with these Terms of Use, or to comply with

La respuesta que vale oro

- La dirección IP agresora le pertenece a...

Preguntas...

- Javier Romero, CTO, javier@jacksecurity.com