

Pruebas de penetración y hacking ético

1. TERMINOLOGÍA

Flujo de trabajo del tema 1



Introducción

- 50's, 60's



- La palabra “Hacker”, era utilizada por grupos de entusiastas para describir genialidad en un individuo, en aquellos capaces de modificar el comportamiento de un mecanismo o de su entorno basándose solo en dicha genialidad.

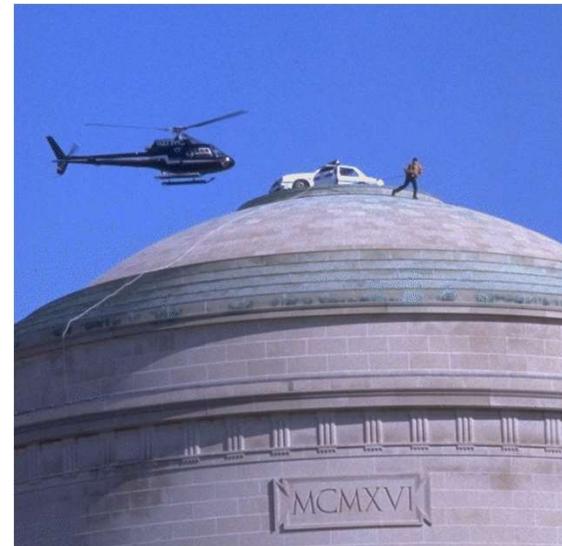


Legado

Los “Hackers” y los grupos que estos formaron contribuyeron en gran medida al avance del computo, ya que al aumentar el interés en estos temas, lo hicieron las contribuciones ajenas al campo científico.

De estos grupos se derivó algo llamado “ética hacker”, que hasta nuestros días es objeto de inspiración para desarrolladores de proyectos de código libre y profesionales de la seguridad informática.

- La importante para este curso:
 - ***Los hackers deben ser juzgados por su hacking, sin importar sus títulos, edad, raza o posición.***



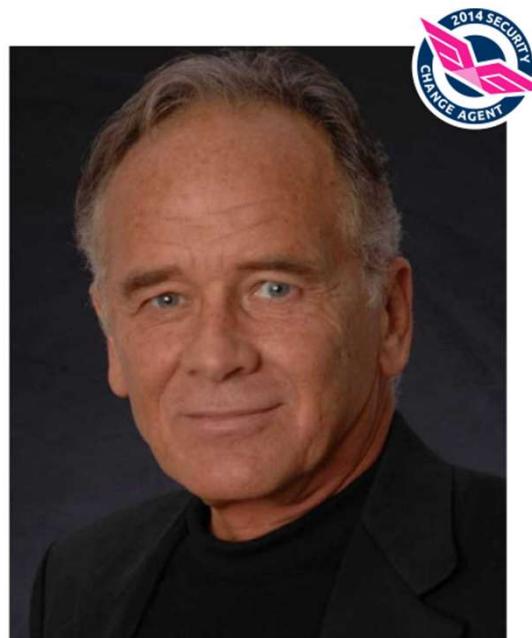
Historia

- El concepto de pruebas de penetración no existía propiamente hasta años recientes, sin embargo debido al creciente uso que tuvieron las computadoras en las universidades y por partes de los gobiernos, se vio la necesidad de tener equipos dedicados a probar la resistencia a fallos de dichas computadoras.
- A estos equipos de pruebas se le llamaba Tiger Team.



Historia(continuación)

- En el año 1972, James P. Anderson publicó un documento en el que se hacia referencia a pruebas de seguridad orientadas a los sistemas de información. Este [documento](#) se considera como la base para lo que hoy se conoce como pruebas de penetración o hacking ético.



Historia(continuación)



--= HACKEANDO PRESIDENCIA.GOB.MX =--
www.presidencia.gob.mx
por alt3kx!

Desafortunadamente, la supercomputadora Cray de la UNAM ya sufrió uno de estos incidentes, en su nivel mayor de gravedad, es decir, obtención de privilegios de superusuario por parte del intruso. Es necesario reconocer que fue este incidente el que efectivamente “disparó” el proyecto de seguridad. A continuación se describe este incidente.

Al hacer una revisión detallada de la cuenta, se vio que pertenecía a todos los grupos y tenía activados todos los permisos, situación en la que ningún usuario de la Cray (ni siquiera **root**) se encuentra.

12. Se procedió a identificar a los responsables del ataque, que resultaron ser estudiantes de la Facultad de Ciencias de la UNAM.

usuario *God*, que accedía desde el Instituto de Investigaciones en Ciencias Nucleares. Fue detectado y se reportó a su vez al FBI. Para sorpresa de todos, llegó la policía investigadora estadounidense porque justamente se estaba violando el principio de que la supercomputadora no podía utilizarse para investigaciones nucleares.⁵



Cuando identifican a De Icaza y lo llevan al Instituto, se dan cuenta que se trata de un muchacho de 19 años que tenía una granja de PC para descifrar *passwords*. Mandan llamar a su padre y ambos se presentan en la oficina de Víctor Guerra, entonces responsable de la DGSCA. Ahí confiesa De Icaza que sólo quería demostrarle a la funcionaria que él podía poner su clave en la *Cray*.⁶

Evaluación de seguridad

- Proceso para determinar la eficacia de la seguridad en una entidad que se evalúa (host, sistema, red, etc.).
- Los hallazgos identificados se documentan.
- Se genera un reporte final que refleja la postura de seguridad.

Documentos

Políticas de seguridad

Bitácoras

Configuraciones de seguridad

Conjunto de reglas

Pruebas de penetración

Ethical Hacking

Hacking

- Manipulación de la tecnología para que realice algo para lo cual no fue diseñada.

Ethical Hacking

- Técnicas de ataque para encontrar fallos en los sistemas con el permiso del dueño del activo, con el objetivo de mejorar su seguridad.

Pruebas de penetración

SANS

- Proceso enfocado en la penetración de las defensas de la organización, para comprometer los sistemas y obtener el acceso a la información.

NIST

- Prueba de seguridad técnica en donde un evaluador simula ataques reales para identificar los métodos para eludir las características de seguridad de una aplicación, un sistema o la red.

EC-
Council

- Pruebas de penetración son un método que evalúa los niveles de seguridad de un sistema o red en particular.

Pruebas de penetración

Proceso intrusivo, donde se evalúan mecanismos y configuraciones de seguridad de una organización.

Utiliza métodos de ataque comunes para vulnerar la seguridad y comprometer los sistemas.

Busca obtener información sensible de la organización.

Diferencias entre conceptos

Evaluación de seguridad

Ethical hacking

Pruebas de penetración

Amenaza, Vulnerabilidad y Riesgo

Amenaza

Todo aquello que puede causar daño, modificación o pérdida en los activos de una organización.

Delincuencia organizada, compañías de software espías, empleados descontentos, malware, fenómenos naturales.

Vulnerabilidad

Es un defecto o falla de seguridad.

Las vulnerabilidades suelen corregirse con parches o actualizaciones de versión.

Riesgo

Es la probabilidad de que determinada amenaza logre explotar una vulnerabilidad presentando un evento no deseado.

Se debe tomar en cuenta que el riesgo estará presente mientras no se elimine la amenaza que lo genera.

Exploit y Ataque

- Medio que un atacante utiliza para aprovechar una vulnerabilidad y penetrar sistemas.
- Permite alterar un activo de información.

Exploit



- Acciones que se aprovechan de las vulnerabilidades de un sistema.
- Puede resultar en la pérdida de las distintas propiedades de seguridad.

Ataque



Hackers

- “*Persona que disfruta tener un intimo entendimiento del trabajo interno de un sistema, computadora o redes de computadoras...”***
- El término se utiliza incorrectamente en los medios de comunicación para referirse a crackers.



OFFENSIVE
security

(Offensive security, 2017)

**IETF (1983). Internet Users' Glossary. Recuperado el 5 de junio de 2017, de <https://tools.ietf.org/html/rfc1392#appendix-H>

Crackers



(Kiuwan, 2017)

- “*Individuos quienes intentan acceder a sistemas de computo sin autorización.”***
- Buscan obtener algún beneficio (reconocimiento personal o económico), a través de la defraudación de usuarios u organizaciones.

**IETF (1983). Internet Users' Glossary. Recuperado el 5 de junio de 2017, de <https://tools.ietf.org/html/rfc1392#appendix-C>

Script Kiddies

- Usuarios con pocos conocimientos de cómputo y tecnologías.
- Utilizan herramientas creadas por otras personas para causar daño, sin entender realmente el funcionamiento.



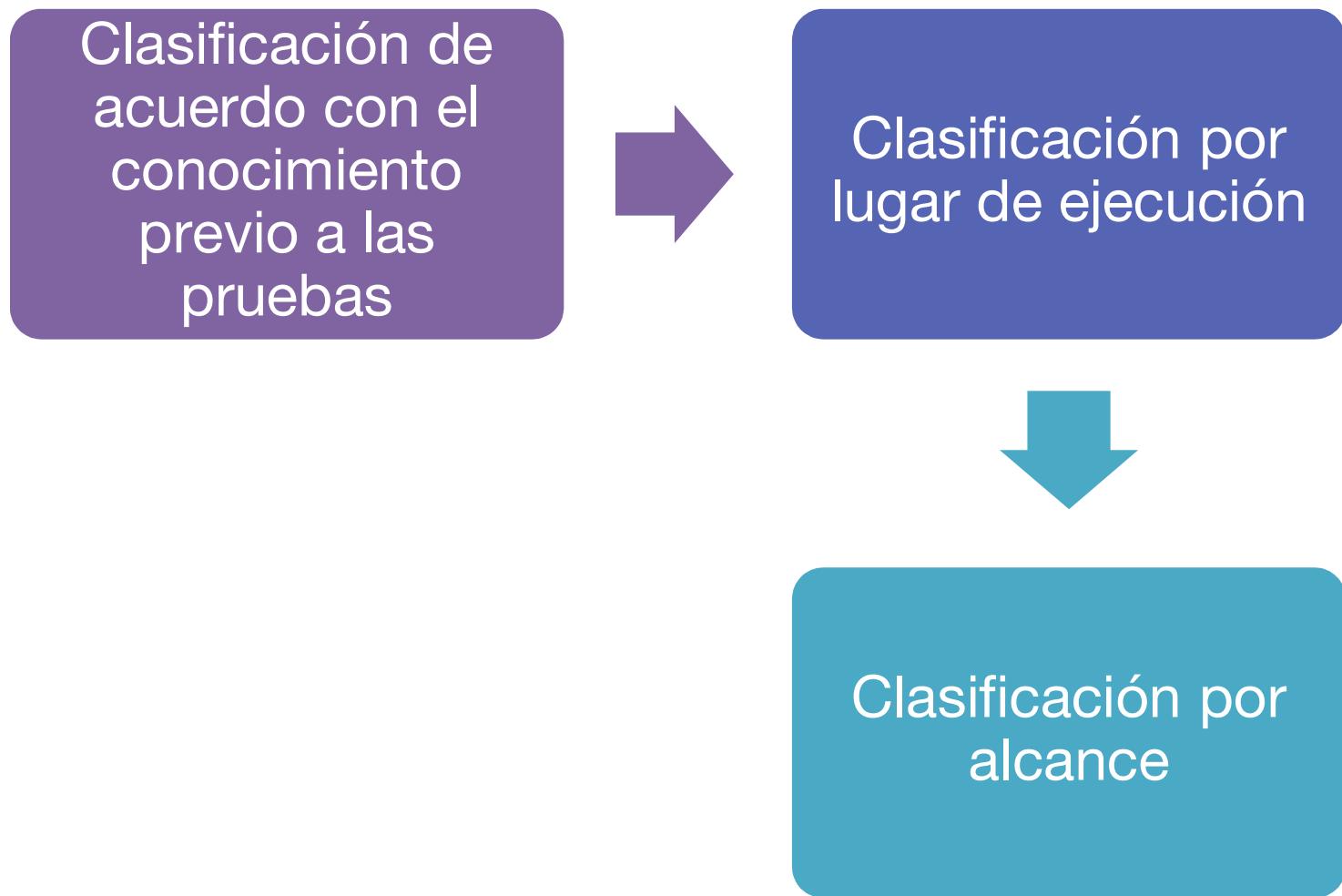
(rinconinformatec, 2016)



Hackers are free people, just like artists who wake up in the morning in a good mood and start painting.

2. TIPOS DE PRUEBAS DE PENETRACIÓN

Flujo de trabajo del tema 2



Clasificación por conocimiento previo

- Depende de la información proporcionada al *pentester* antes del inicio de las pruebas.
- A menor información proporcionada por el cliente, el reto es mayor para el especialista.
- El desempeño es parecido al de un atacante ajeno a la organización.

Caja negra

Caja Blanca

Caja Gris

Caja negra

Consiste en intentar penetrar el objeto de evaluación sin tener conocimientos del sistema para generar una situación real.

Se recolecta información divulgada por la institución en sitios web, en repositorios públicos, etc.



El evaluador, parte de cero y construye el escenario, obteniendo información de distintos sitios y personas.

Es una representación de un atacante externo a la organización.

Caja Blanca



Consiste en realizar una prueba de seguridad teniendo acceso al código fuente de alguna aplicación o las configuraciones de seguridad de algún servidor.

Tiene como objetivo identificar malas configuraciones o errores de programación.

Caja Gris



Enfoque parecido a las pruebas de caja negra, pero en este tipo de prueba se cuenta con más información del objeto de evaluación.

Puede ser un mapa de la arquitectura de red, la ubicación física de los dispositivos u otros elementos.

Clasificación por lugar de ejecución

Externas

- Se realizan fuera del perímetro de seguridad de la organización.
- Permite conocer la postura de seguridad desde Internet.
- Muestra vulnerabilidades que podrían ser explotadas por un atacante externo.

Internas

- Los especialistas en pentest trabajan en la red de la organización.
- Asumen el rol de una persona de confianza o el de un atacante que ha penetrado las defensas del perímetro.

Clasificación por alcance

- La evaluación de seguridad se realiza por partes.
- Se realiza una clasificación según la parte que se va a probar o evaluar.
- Las pruebas se enfocan en los elementos indicados por el cliente.

Pruebas de Servicios de Red

Pruebas de aplicaciones Web

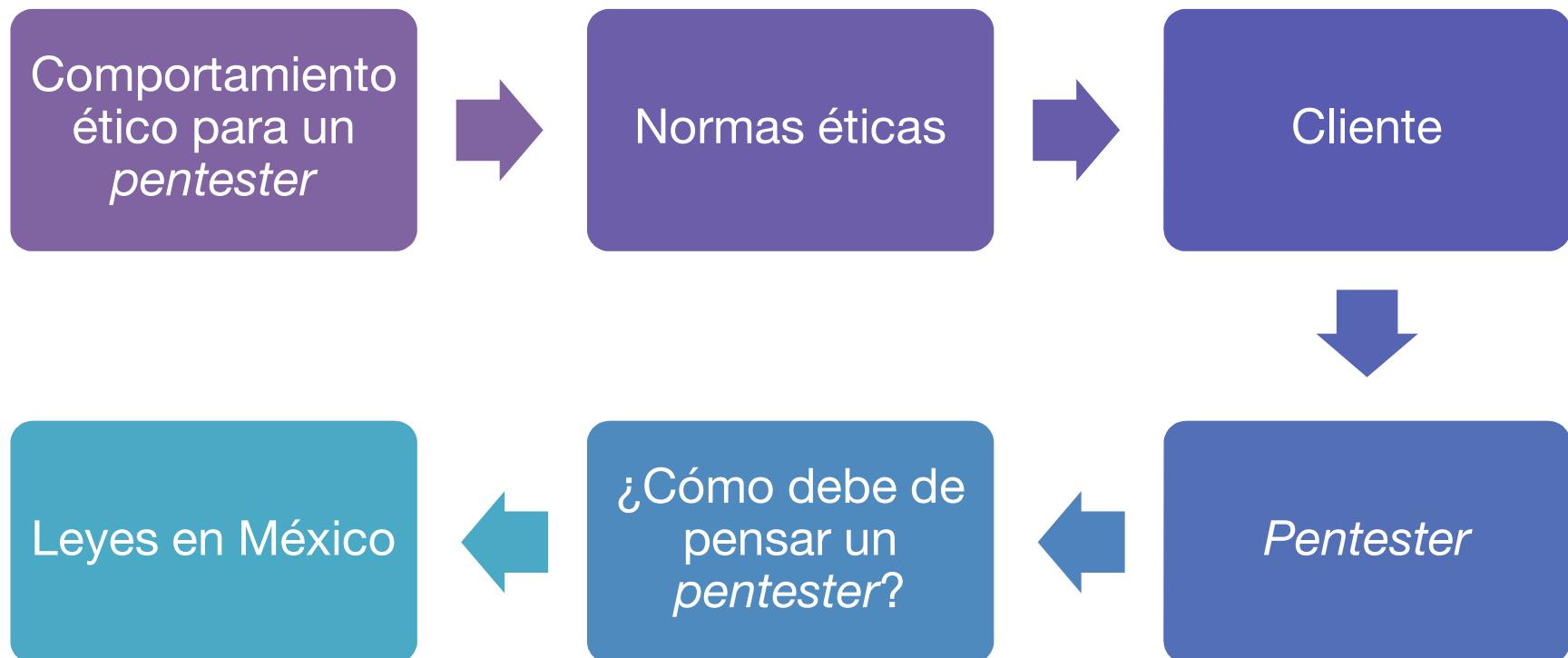
Pruebas de seguridad inalámbrica

Pruebas de ingeniería social

Pruebas de seguridad física

3. RESPONSABILIDAD ÉTICA Y LEGAL

Flujo de trabajo del tema 3



Comportamiento ético para un pentester

Ética

- Conjunto de normas morales que rigen la conducta humana.

Clasificación de hackers de acuerdo a su comportamiento

- Emplean técnicas de penetración sin autorización contra sistemas de información.
- Su motivación es la curiosidad y obtener ganancias económicas.
- Sus acciones son condenadas por el hecho de hacerlas sin

Sombrero
Negro



- Llevan a cabo la evaluación de seguridad con un contrato establecido con un cliente.
- Trabajan para mejorar la postura de seguridad de las organizaciones.
- Tienen como objetivo encontrar vulnerabilidades de la organización. Al concluir, entregan un informe de resultados.

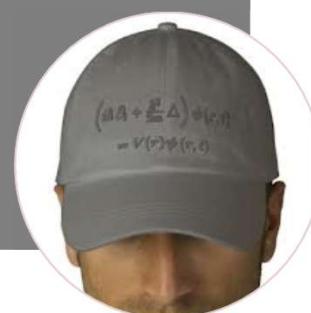
Sombrero
Blanco



Clasificación de hackers de acuerdo a su comportamiento

- Incluye a los especialistas que por lo general se rigen bajo la ley, pero podrían estar bajo los límites de la misma.
- Quienes realizan ingeniería inversa de software propietario, sin obtención de ganancias financieras, pueden incluirse en esta categoría.

Sombrero Gris



Normas éticas



(ISSA , 2017)

- Promover ética a los profesionales de seguridad

- Definir normas a seguir

- Impulsar certificaciones



(IEEE , 2017)

Normas éticas (continuación)

Information System
Security Association
(ISSA)

- Organización internacional sin fines de lucro que proporciona foros educativos y publicaciones que mejoran el conocimiento y habilidad de sus miembros en temas de seguridad.

Internet Activities
Board (IAB)

- Reconoce el comportamiento poco ético en Internet mediante el RFC 1087.

Institute of Electrical
and Electronics
Engineers (IEEE)

- Organización internacional enfocada en el avance e innovación tecnológica para el beneficio humano. Realizan conferencias, publicaciones y estándares de tecnología.

Normas éticas (continuación)

- Certificación Profesional de Sistemas de Seguridad de la Información (CISSP)
- Propuesta por el Consorcio Internacional de Certificación de Seguridad de Sistemas de Información o (ISC)2
- Contiene una sección enfocada en leyes, investigaciones y ética

Normas éticas (continuación)

El código ético manejado por (ISC)² es:

- a) Proteger a la sociedad, a la comunidad y a la infraestructura
- b) Actuar de forma honorable, honesta, justa, responsable y legal
- c) Proporcionar servicio de forma diligente y competente a sus superiores
- d) Proteger y promover el crecimiento de la profesión

Comportamientos no éticos en Internet RFC 1087

Tratar de obtener acceso no autorizado a los recursos de Internet

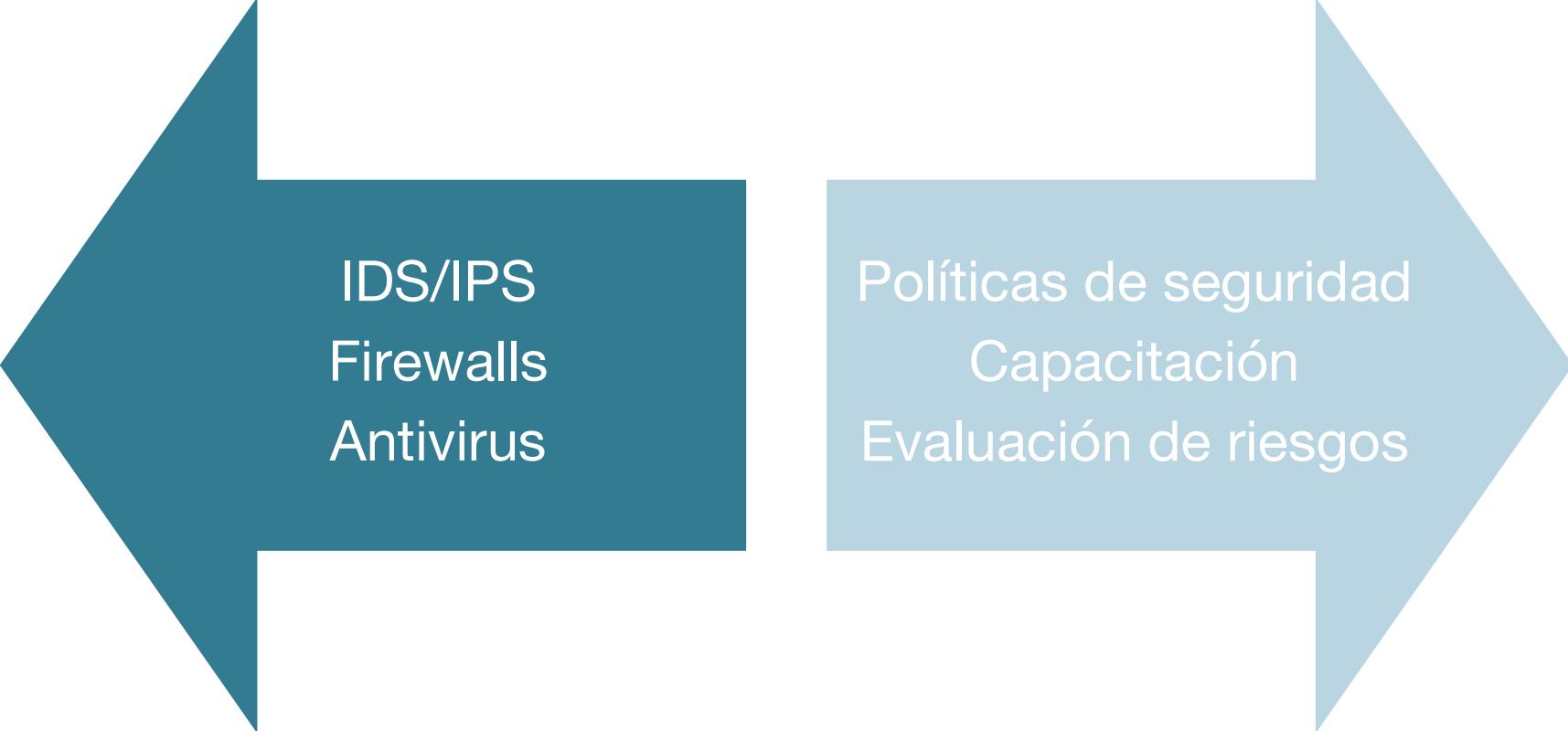
Interrumpir el uso previsto de Internet

Desperdiciar los recursos (personas, capacidad, equipos)

Destruir la integridad de la información digital

Comprometer la privacidad de los usuarios

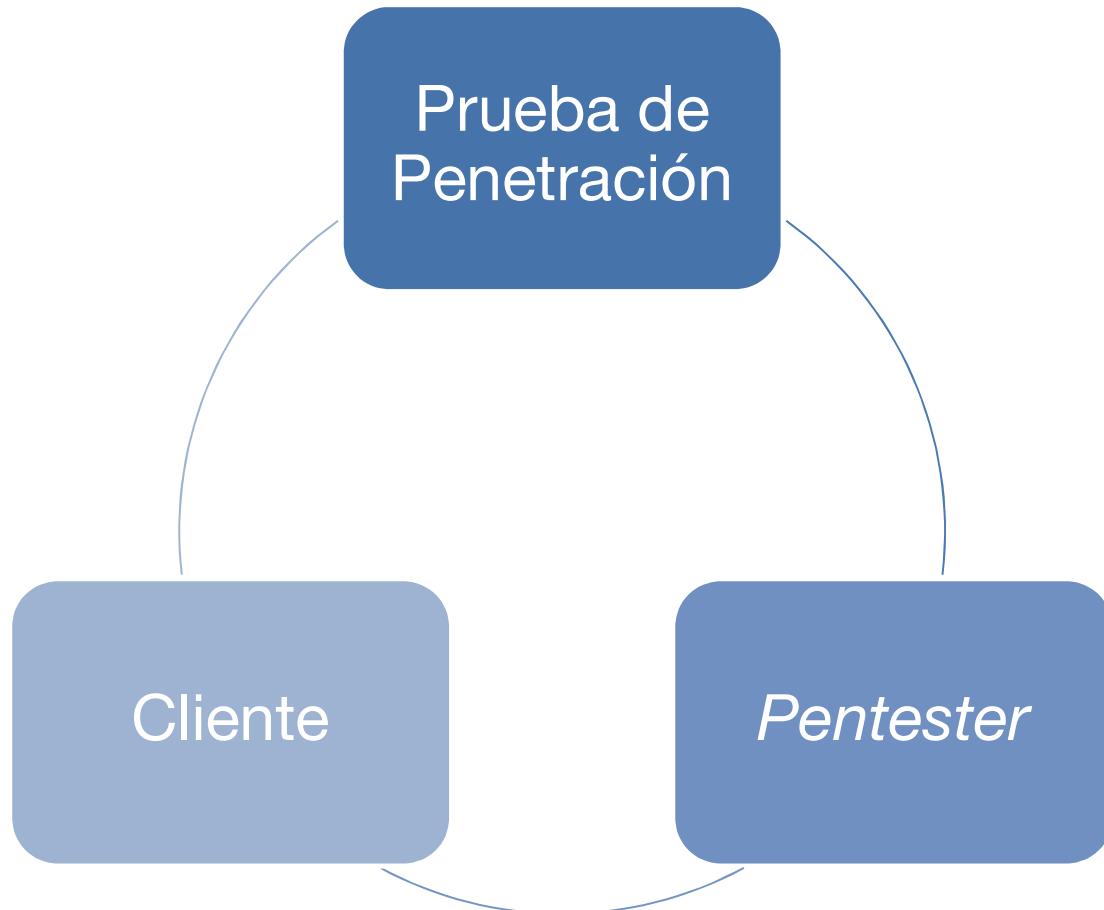
Normas éticas (continuación)



IDS/IPS
Firewalls
Antivirus

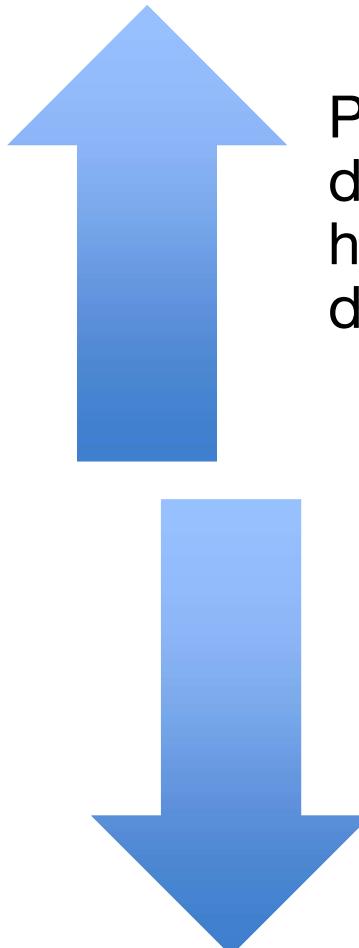
Políticas de seguridad
Capacitación
Evaluación de riesgos

Relación cliente - pentester



¿Cómo debe de pensar un pentester?

- De acuerdo con SANS Institute, un *pentester* dijo:
- “Nosotros nos entrometemos en las computadoras y hacemos que lo que realizan los diseñadores, implementadores, desarrolladores y administradores de sistemas hagan cosas para lo cual no fueron diseñados.”



Pensar fuera
de la caja y
hacer cosas
diferentes.

Pero al mismo
tiempo ser
minucioso,
metódico y
cuidadoso.

Leyes en México

Con la evolución de la tecnología, los delincuentes encontraron nuevos medios para realizar actividades criminales.

Esto obligó a trabajar en leyes para dichos crímenes y las sanciones establecidas.

En México se ha trabajado desde hace unos años en delitos informáticos, siendo Sinaloa el primer estado que creó leyes para este tipo de crímenes.

Delitos informáticos

Denegación de servicio (Dos)

- Dejar sin servicio temporal o permanentemente un sistema de información.

Destrucción o alteración de información

- Atentar contra la integridad de la información.

Dumpster diving

- Buscar información en la basura.

Espionaje

- Por lo regular se presenta entre naciones o empresas competidoras.

Fraude

- A menudo se relaciona con falsas subastas. Se puede incluir en esta categoría *phishing*, *cross-site scripting* y ataques de redirección.

Delitos informáticos

Contenido ilegal de material

- En algunos casos, se utiliza un equipo comprometido como un sitio de descarga o almacenamiento de contenidos ilegales, como software pirata, música o películas.

Software malicioso

- Conocido también como *malware*, los virus y los gusanos cuestan a las empresas miles de millones de dólares cada año.

Suplantación de identidad

- Hacerse pasar por una persona.

Ingeniería social

- Es el acto de manipular a una persona mediante técnicas psicológicas y habilidades sociales para revelar información confidencial.

Piratería de software

- Busca tener un beneficio de software licenciado y es ilegal en muchos países.

Delitos informáticos

Suplantación de direcciones IP

- Se utiliza a menudo para evitar la detección o punto de origen de los ataques.

Terrorismo

- Ataques contra la infraestructura de comunicación, por ejemplo dejar a un país sin comunicación.

Robo de contraseñas

- Esto se logra usando técnicas simples como el *sniffing* o con técnicas más invasivas como ataques de fuerza bruta.

Intrusiones de red

- Obtener acceso no autorizado, en la red hay muchas formas de comunicación que pueden representar un blanco atractivo para los crackers.

Leyes en México (continuación)

- El marco legal mexicano considera delitos informáticos, comercio electrónico, responsabilidad de personal de TI, entre otros. Las leyes que las regulan son principalmente:
 - Código Penal Federal
 - Códigos penales estatales
 - Código Civil
 - Código de Comercio
 - Código Federal de procedimientos Civiles
 - Ley Federal de Telecomunicaciones
 - Ley de Seguridad Nacional
 - Ley Federal del Derecho de Autor
 - Ley de Propiedad Industrial
 - LFPDPPP

Leyes en México (continuación)

Código penal federal

Libro segundo, título noveno.

Capítulo II

Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1. .- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

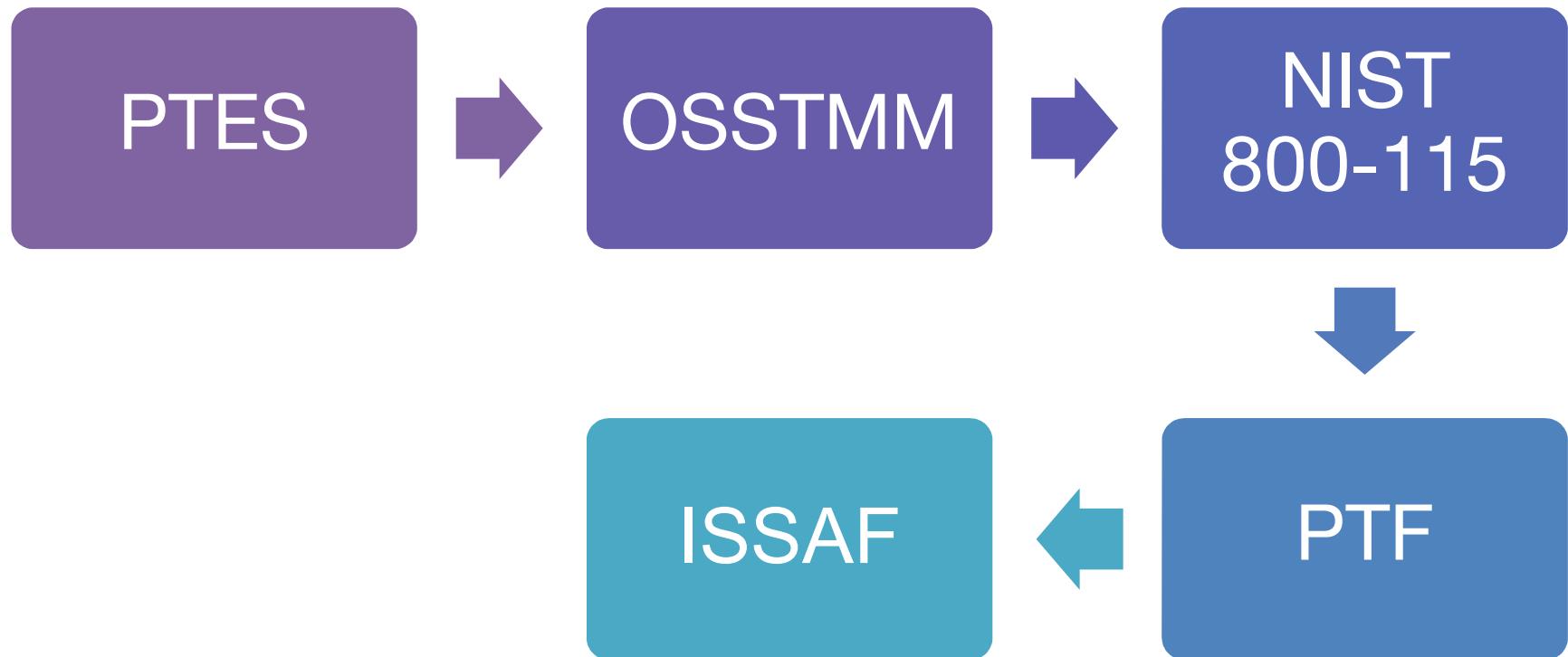
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

4. METODOLOGÍAS PARA REALIZAR PRUEBAS DE PENETRACIÓN

Metodología probada y repetible



Flujo de trabajo del tema 4



PTES (Penetration Testing Execution Standard)

Proyecto diseñado para proporcionar a las empresas y proveedores de servicios de seguridad un enfoque común de pruebas de penetración.

Inició en noviembre de 2010 y ha tenido alrededor de 1800 revisiones. Su contenido es abierto y se encuentra en versión BETA.

PTES busca elevar la calidad general de las pruebas y ayudar a las empresas a definir qué es lo que necesitan y esperan de una prueba de penetración.



(pentest-standard.org, 2015)

OSSTMM (Open Source Security Testing Methodology)

Metodología abierta, para probar la seguridad operacional de locaciones físicas, iteraciones humanas y todas las formas de comunicación.

Los ravs no miden el riesgo para una superficie de ataque pero mejoran la medición de la misma.

Un rav es la medida operativa para calificar una superficie de ataque.

Pruebas de seguridad:

- Humanos
- Físicos
- Redes inalámbricas
- Telecomunicaciones
- Redes de datos

NIST 800-115 (National Institute Standards and Technology 800-115)

Guía técnica de pruebas y evaluación de seguridad de la información.

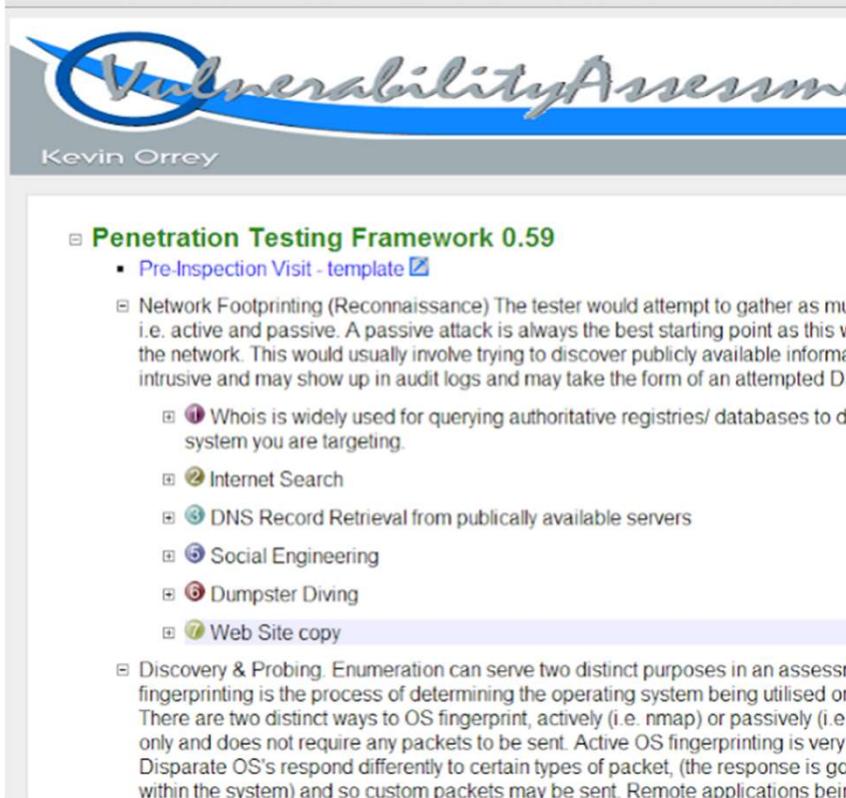
Publicada por NIST, la última versión se encuentra disponible desde septiembre de 2008.

Proporciona metodologías, técnicas y herramientas para realizar la evaluación de procesos, servicios, pruebas de penetración y revisión de políticas de seguridad.

Está dividida en tres fases principales:

- Planeación
- Ejecución
- Post-ejecución

PTF (Penetration Test Framework)



The screenshot shows a software application window titled "VulnerabilityAssessment" with a logo featuring a blue circle and a stylized arrow. Below the title, it says "Kevin Orrey". The main content area has a green header "Penetration Testing Framework 0.59". Under this, there is a list of steps:

- Pre-Inspection Visit - template ↗
- Network Footprinting (Reconnaissance) The tester would attempt to gather as much information as possible, i.e. active and passive. A passive attack is always the best starting point as this will not affect the network. This would usually involve trying to discover publicly available information about the target system, which may show up in audit logs and may take the form of an attempted DNS query.
 - ① Whois is widely used for querying authoritative registries/ databases to determine the domain name and IP address of the system you are targeting.
 - ② Internet Search
 - ③ DNS Record Retrieval from publicly available servers
 - ④ Social Engineering
 - ⑤ Dumpster Diving
 - ⑥ Web Site copy
- Discovery & Probing. Enumeration can serve two distinct purposes in an assessment. Fingerprinting is the process of determining the operating system being utilised on a target system. There are two distinct ways to OS fingerprint, actively (i.e. nmap) or passively (i.e. OS fingerprinting). Active OS fingerprinting is very noisy and does not require any packets to be sent. Active OS fingerprinting is very noisy and does not require any packets to be sent. Disparate OS's respond differently to certain types of packet, (the response is governed by the operating system) and so custom packets may be sent. Remote applications being tested will respond differently to different types of packet, (the response is governed by the application).

(Vulnerabilityassessment, 2015)

- Marco creado para la ejecución de pruebas de penetración en forma de lista.
- Propone una metodología con técnicas y herramientas, que se definen en modo pasivo o activo sobre el sistema.
- Fue diseñado por Kevin Orrey, se encuentra en la versión 0.59.

ISSAF (Information Systems Security Assessment Framework)

Es fuente de referencia en pruebas de penetración, aunque ISSAF no es una comunidad activa. Proporciona orientación técnica en pruebas de penetraciones extensas. Algunas áreas que cubre son:

- Metodología de pruebas de penetración
- Fases de pruebas de penetración
- Pruebas de seguridad en contraseñas
- Evaluación de seguridad en routers y switches
- Evaluación de seguridad en IDS



5. PLANEACIÓN

Planeación

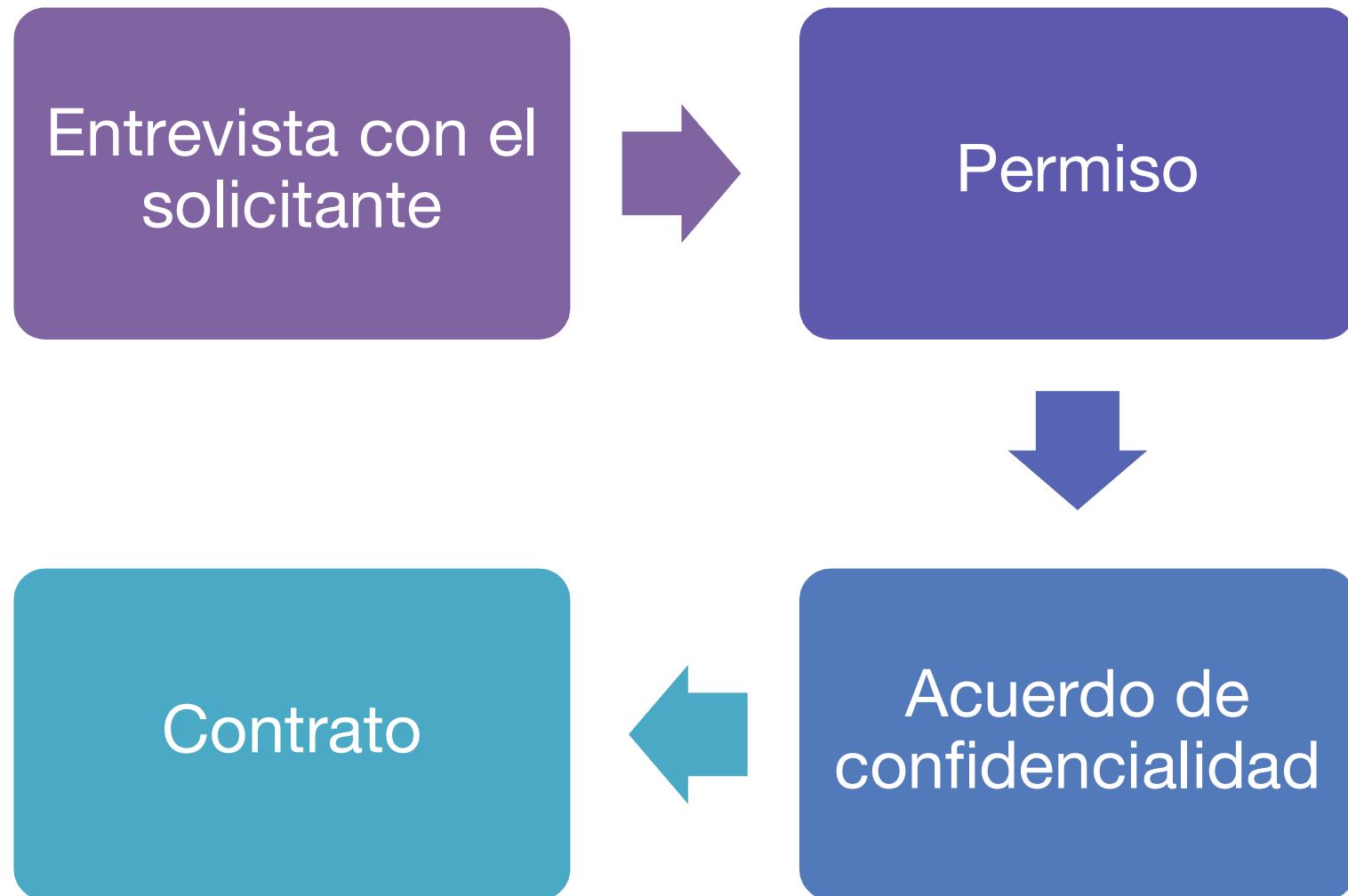
Primera fase

- -Límites
- -Elementos a evaluar
- -Autorización

Elementos en la etapa de preparación

- Entrevista con el solicitante
- Información de consecuencias de las pruebas
- Integración de equipo de trabajo
- Permiso
- Acuerdo de confidencialidad

Flujo de trabajo del tema 5



Entrevista con el solicitante

Explicar en qué
consisten las
pruebas

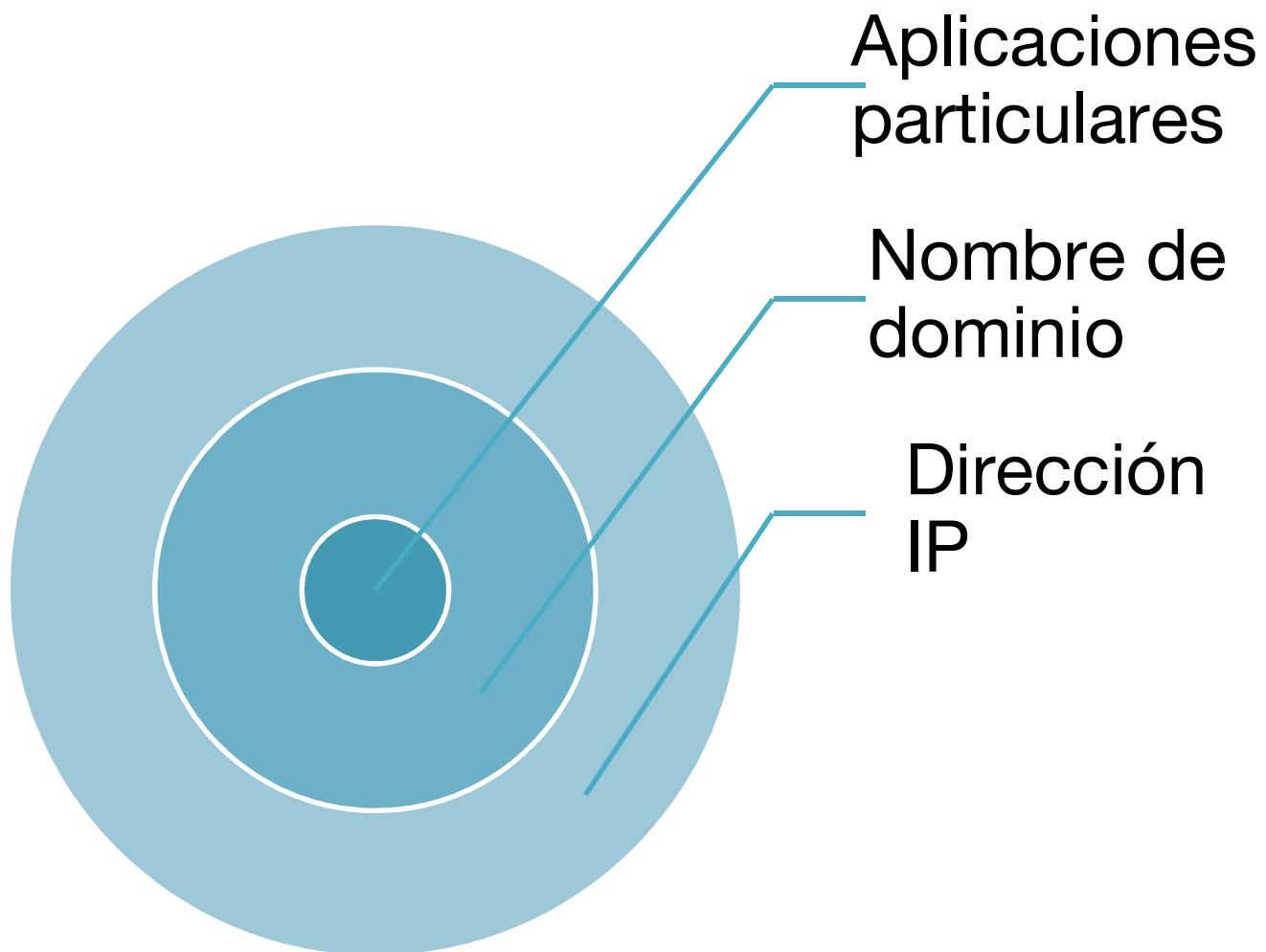
Cómo serán
realizadas

Identificar activos
importantes para el
negocio

Entrevista con el solicitante



Entrevista con el solicitante



Entrevista con el solicitante

Especificar las pruebas aplicadas a los objetivos:

- Escaneo de puertos
- Escaneo de vulnerabilidades
- Penetración en los objetivos
- DoS
- Ingeniería social
- *Lock Picking*
- Manipulación en la capa de aplicación

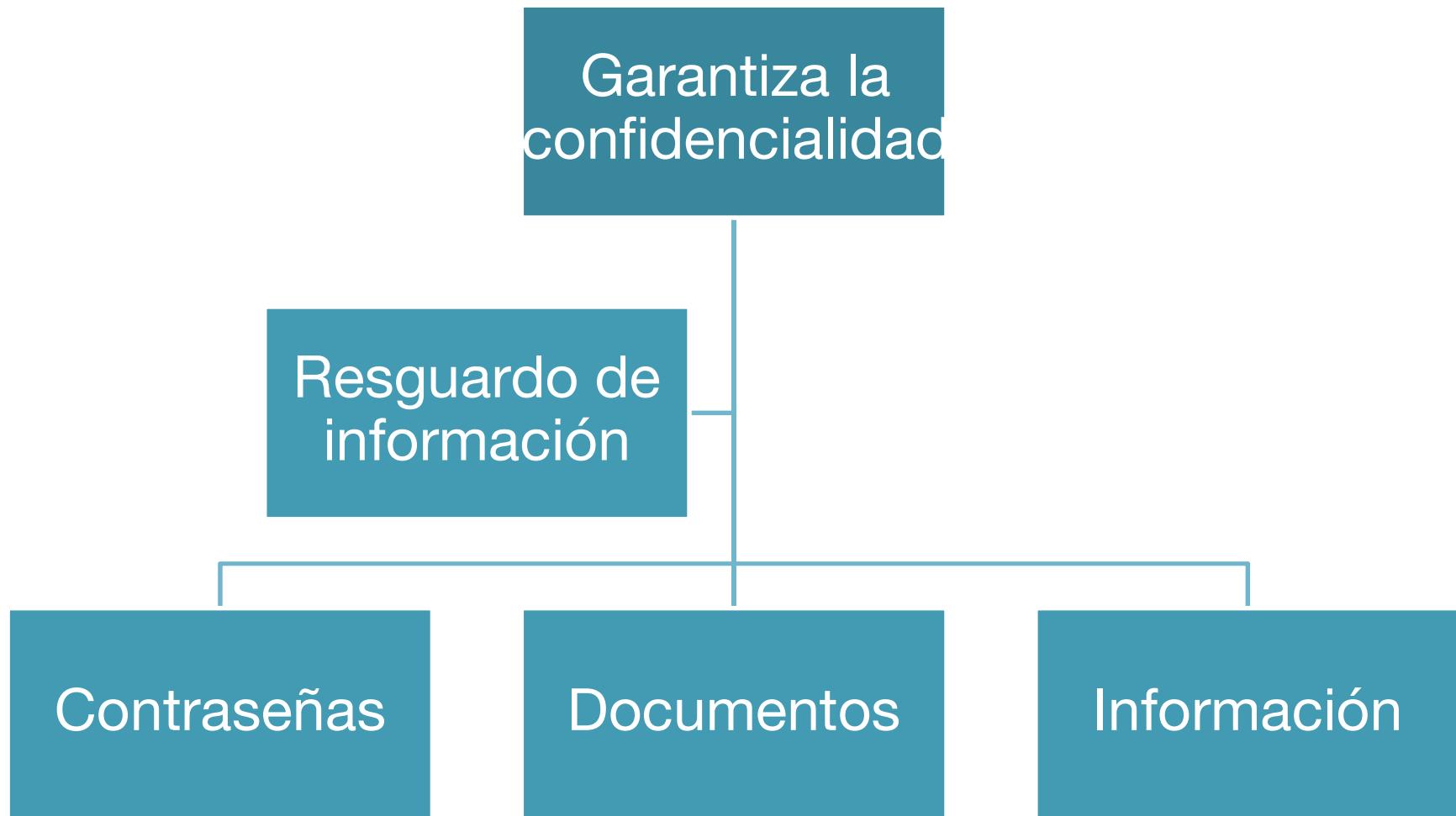
Permiso

- Un *pentester* debe tener un permiso para comenzar cualquier tipo de pruebas.

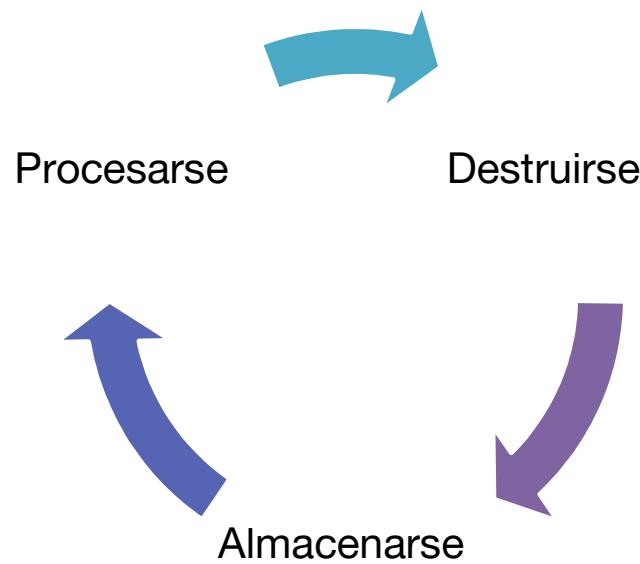
No hay un formato estándar para elaborar la autorización

- Equipo que realizará las pruebas
- Ventana de tiempo
- Nombre y firma de la persona que autoriza
- Direcciones IP de los objetivos de evaluación

Acuerdo de confidencialidad



Acuerdo de confidencialidad



Las pruebas de penetración se deben hacer desde un equipo dedicado para evitar que la información sea comprometida.

- El acuerdo de confidencialidad debe ser firmado por cada elemento del equipo de evaluación.

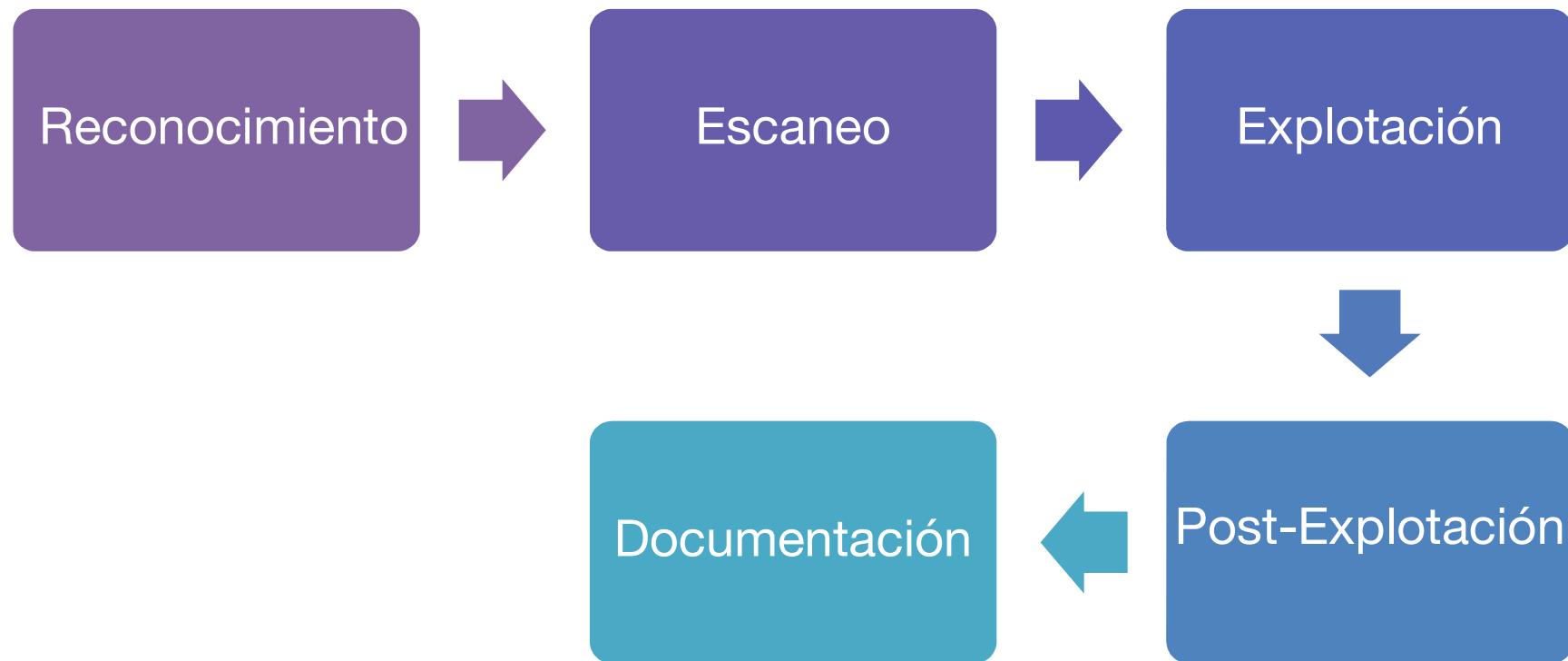
- De acuerdo al nivel de confidencialidad de la información manejada en el proyecto, es la cantidad de tiempo que no se puede revelar algún tipo detalle.

Contrato



FASES DE LAS PRUEBAS DE PENETRACIÓN

Flujo de trabajo del tema 6



6. RECONOCIMIENTO

Reconocimiento

Reunir la mayor cantidad de información sobre el objetivo de evaluación.



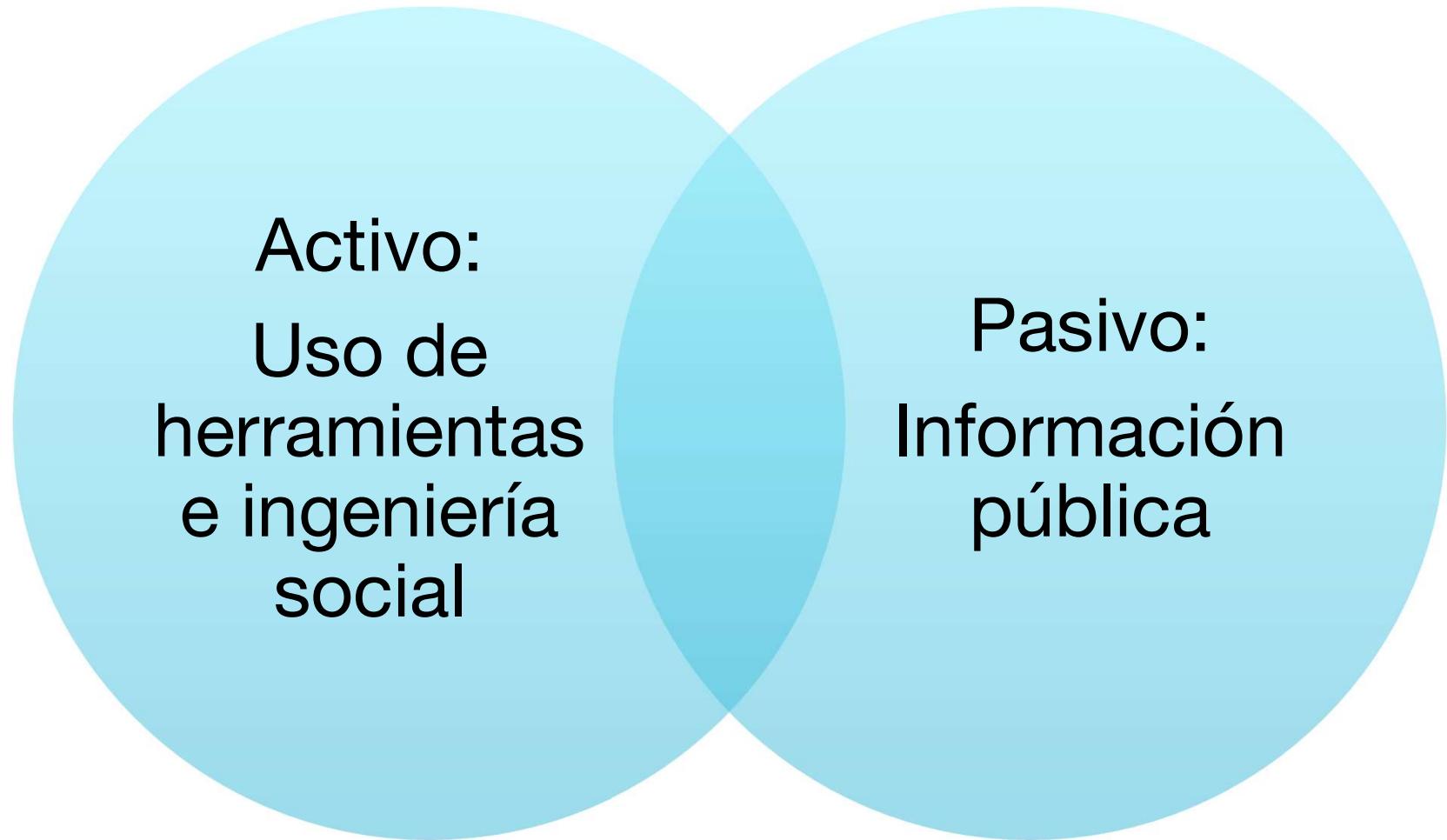
(miriadaxglennpereira.blogspot.mx, 2017)

Se requiere mucho tiempo.



(tunegociocorrecto, 2017)

Reconocimiento (continuación)



Reconocimiento (continuación)

Internet

Google Hacking

Técnicas y
herramientas

whois

nslookup

Whois

- Base de datos pública para consultar detalles y datos personales de los dominios registrados e información almacenada.
- Permite corroborar la disponibilidad del dominio.

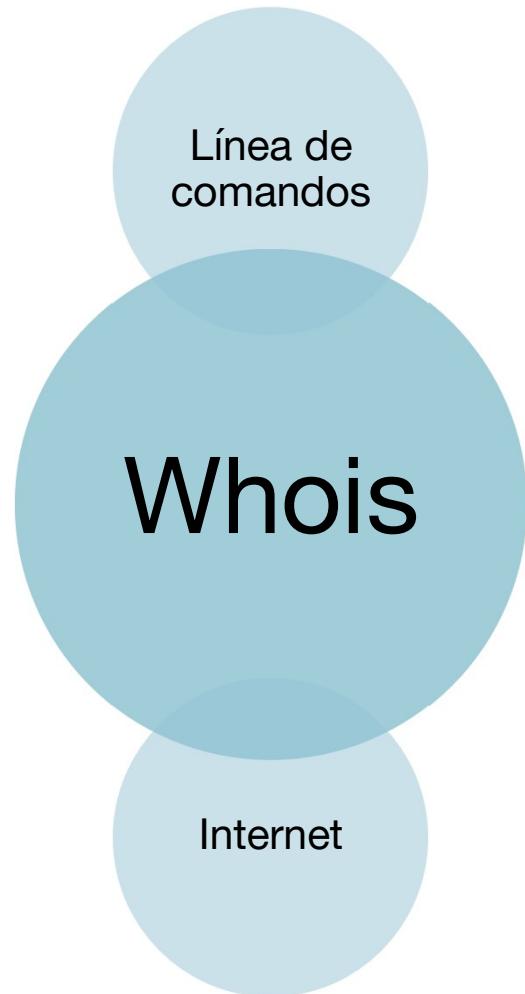
Fecha de registro

Fecha de expiración

Datos de contacto del administrador

Direcciones IP de los servidores DNS

Whois (continuación)



- Direcciones URL que ofrecen el servicio son:
 - <http://www.whois.net>
 - <http://whois.domaintools.com>
 - <http://www.geektools.com/tools.php>
 - <http://who.is>

Registros Regionales de Internet

RIR

Gestión de recursos
numéricos de Internet

IPv4, IPv6

Números de Sistemas
Autónomos



(RIR, 2017)

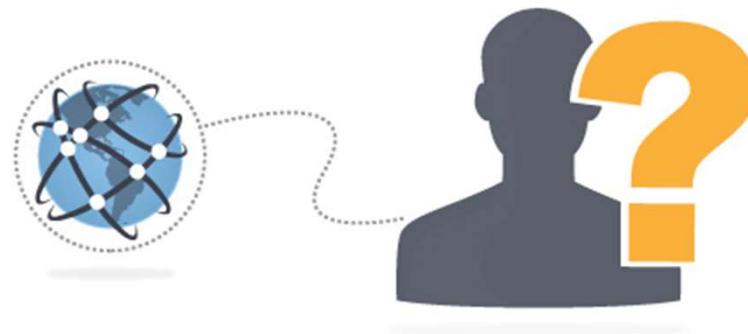
Registros Regionales de Internet (continuación)

AFRINIC	African Network Information Center	Continente de África	http://www.afrinic.net
APNIC	Asia Pacific Network Information Center	Asia y la región del Pacífico	http://www.apnic.net
ARIN	American Registry for Internet Numbers	América anglosajona : de Canadá, algunas islas del Caribe, Atlántico Norte y de los Estados Unidos	https://www.arin.net
LACNIC	Latin America & Caribbean Network Information Center	América Latina y parte del Caribe	http://www.lacnic.net/ es/web/lacnic/inicio
RIPE NCC	Réseaux IP Européens Network Coordination Center	Europa, el Oriente medio y Asia central	http://www.ripe.net

PRÁCTICA #1: WHOIS

Práctica #1 whois

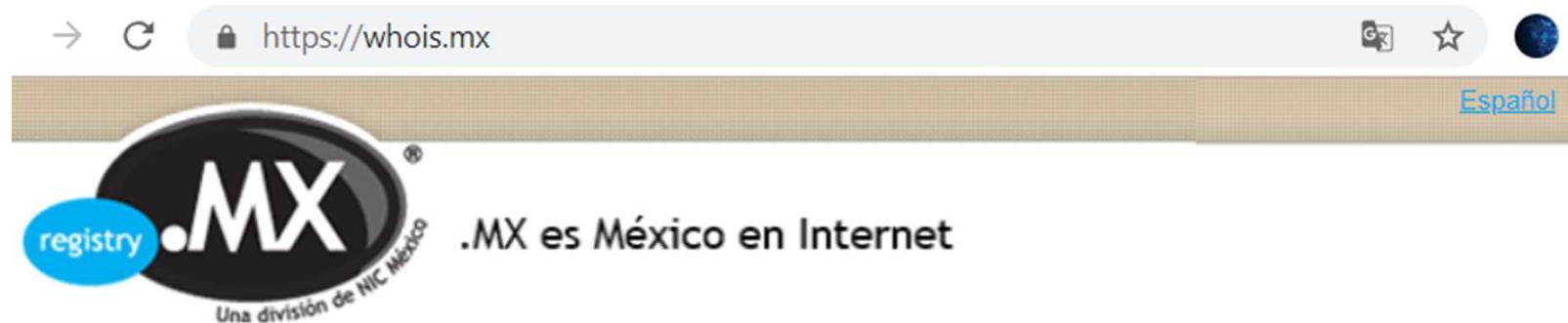
Herramientas que permiten consultar mediante el protocolo Whois, una base de datos pública, la cual contiene información detallada sobre los dominios registrados.



(2015)

Práctica #1: Desarrollo

En el formulario se ingresará el dominio unam.mx



La herramienta "WHOIS" buscará en la base de datos del Registry .MX, el nombre proporcionado correspondiente al tipo de objeto seleccionado:

› **Nombre del objeto:**

(WHOIS, 2017)

Práctica #1: Desarrollo

Una vez realizada la consulta, se despliega información referente al dominio:

- Nombre de dominio
- Fecha de creación y expiración
- Contacto administrativo
- Servidores de nombres de dominio

Registrar Data

Domain Name: unam.mx

Created On: 1989-03-31
Expiration Date: 2018-03-30
Last Updated On: 2017-03-27
Registrar: Akky (Una division de NIC Mexico)
URL: http://www.akky.mx
Whois TCP URI: whois.akky.mx
Whois Web URL: http://www.akky.mx/jsf/whois/whois.jsf

Registrant:
Name: UNAM
City: Mexico
State: Distrito Federal
Country: Mexico

Administrative Contact:
Name: ALEJANDRO CRUZ SANTOS
City: Mexico
State: Distrito Federal
Country: Mexico

Technical Contact:
Name: ALEJANDRO CRUZ SANTOS
City: Mexico
State: Distrito Federal
Country: Mexico

Billing Contact:
Name: ALEJANDRO CRUZ SANTOS
City: Mexico
State: Distrito Federal
Country: Mexico

Name Servers:
DNS: ns3.unam.mx 132.248.108.215, 2001:1218:100:10a:108:0:0:215
DNS: ns4.unam.mx 132.248.204.32, 2001:1218:403:203:204:0:0:32

(*who.is*, 2017)

Práctica #1: Conclusiones

- La información obtenida del dominio es pública
- Se obtienen nombres de responsables, fechas de expedición y expiración.
- Direcciones de servidores DNS de la organización.
- Información útil para realizar técnicas de ingeniería social.
- Se conoce, desde el anonimato, un poco de la infraestructura tecnológica de la organización.

Servidores DNS

Traducción de nombres de dominio a direcciones IP.

Ejemplo:

- unam.mx
- 132.247.70.37

Registros DNS

NS	A	HINFO	MX
<ul style="list-style-type: none">• Indica el nombre de los servidores asociados a un dominio.	<ul style="list-style-type: none">• Asocia nombres de dominio a una dirección IP.	<ul style="list-style-type: none">• Campo descriptivo de hardware:<ul style="list-style-type: none">• SO• Procesador	<ul style="list-style-type: none">• Identifica los servidores de correo.

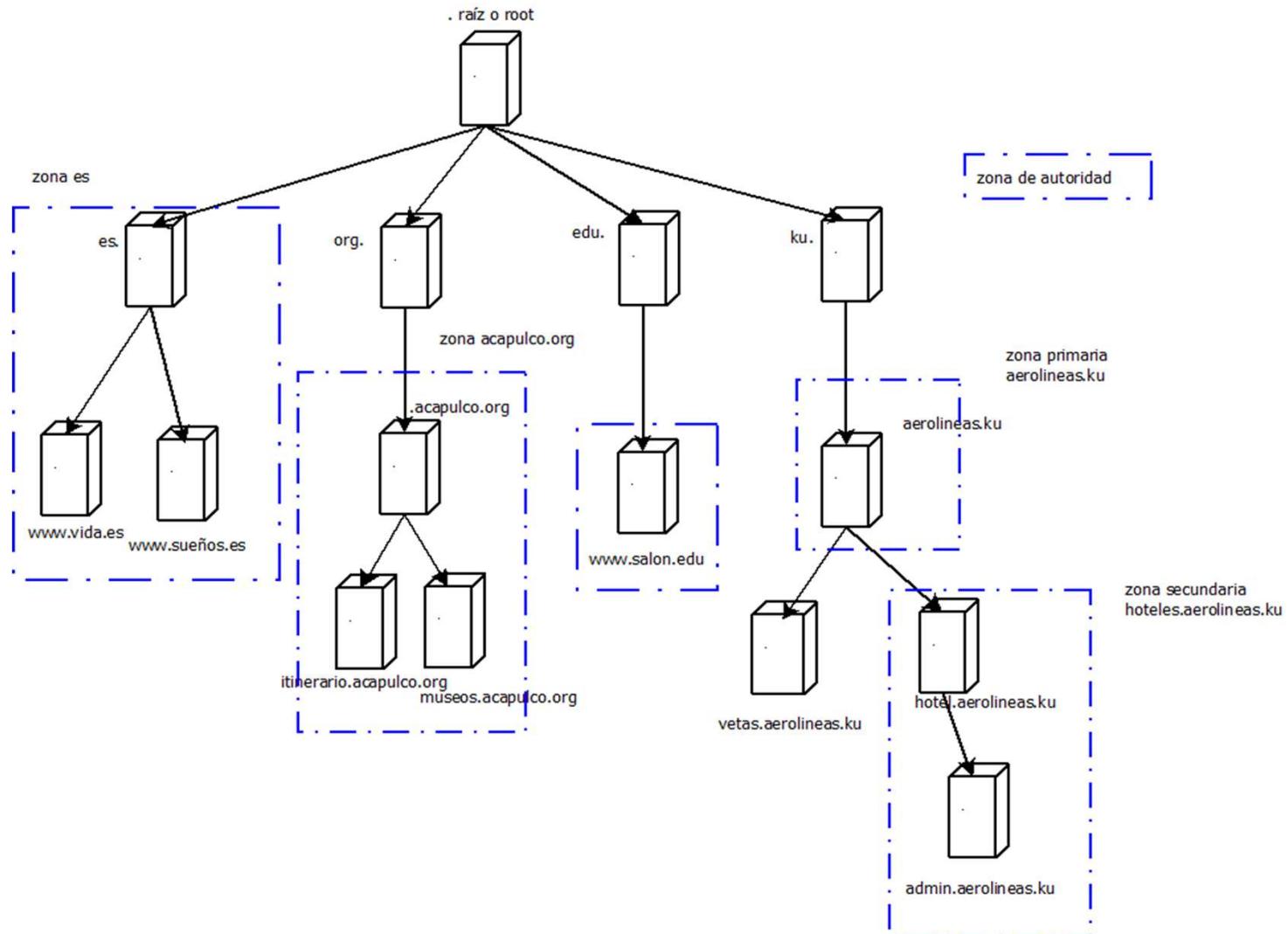
Zonas DNS



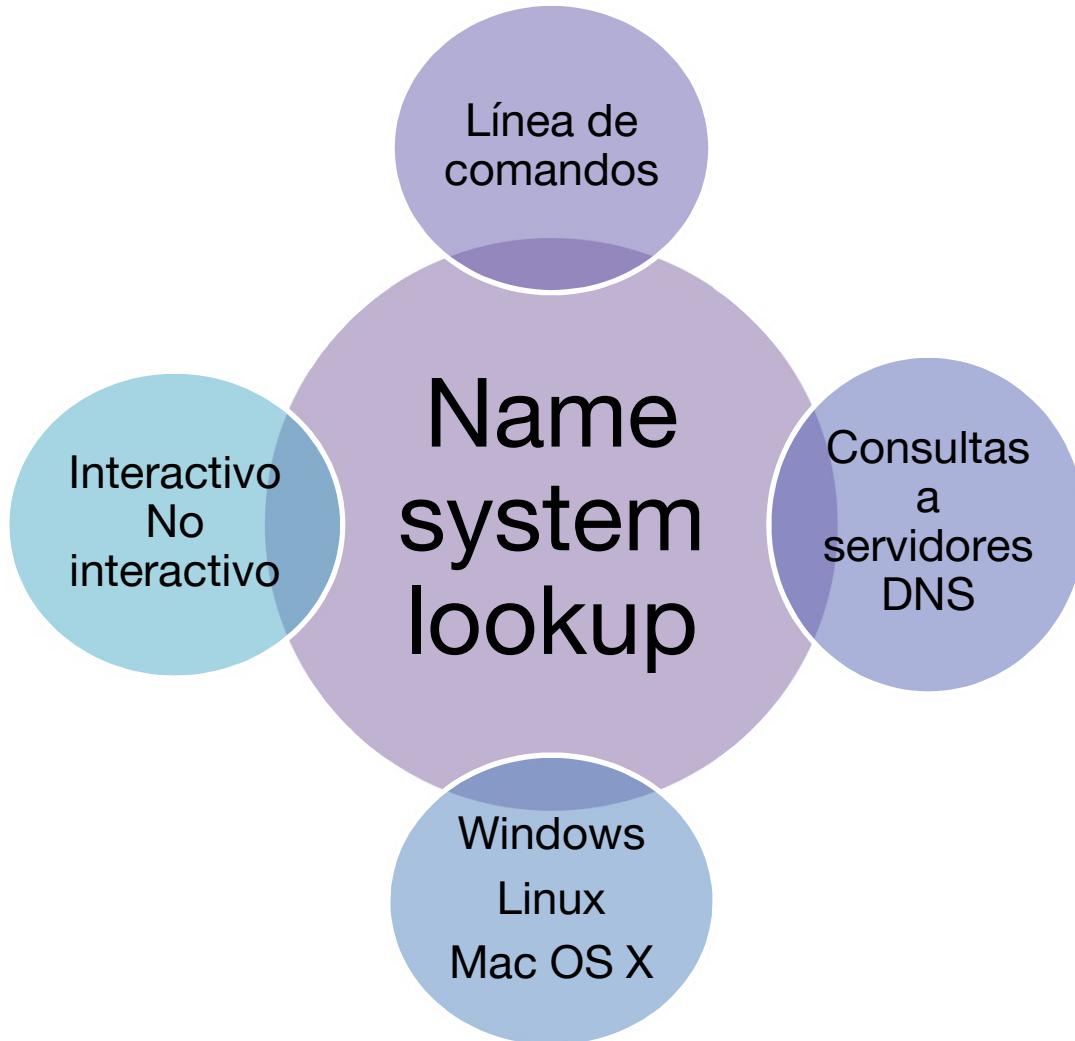
Zonas
DNS

- Conjunto de dominios
- Gestión de dominios

Zonas DNS (continuación)



Nslookup



Nslookup (continuación)

Respuesta autoritativa

El DNS está autorizado hacer consultas a una zona DNS

Respuesta no autoritativa

El DNS no está autorizado hacer consultas a una zona DNS

Nslookup (continuación)

set

- all, muestra las opciones del servidor actual y host.
- type, define el tipo de registro a consultar.
- d2, muestra exhaustivamente información para depuración.

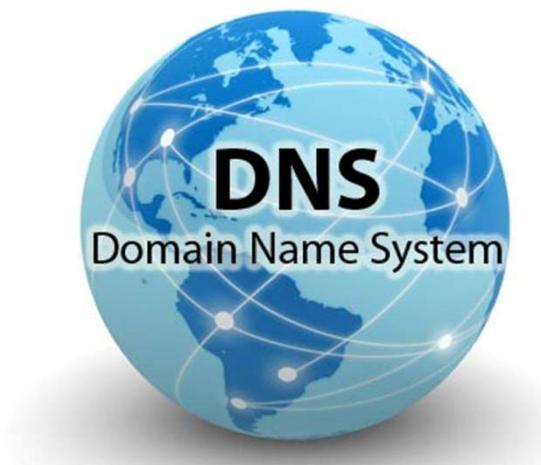
Server

- server, establecer un servidor DNS específico para realizar consultas de nombres de dominio

PRÁCTICA #2: CONSULTAS A SERVIDORES DE NOMBRES DE DOMINIO (DNS)

Práctica #2: DNS

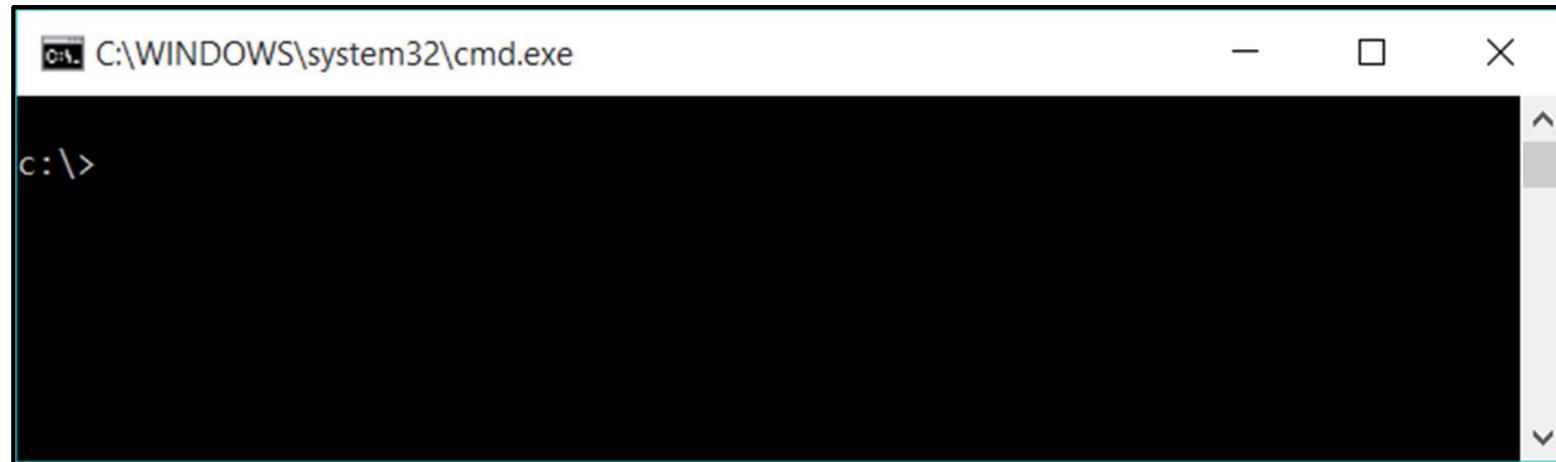
La consulta a los servidores de nombres de dominio (DNS) es una técnica de recolección de información sobre un dominio.



(2017)

Práctica #2: Consultas DNS

Iniciar el intérprete de comandos de Windows (CMD).



Práctica #2: Consultas DNS

En el intérprete de comandos se hará una consulta de información del dominio gmail.com mediante el comando:

```
nslookup -type=any gmail.com
```

```
C:\>nslookup -type=any gmail.com
Server: dns2.unam.mx
Address: 132.248.10.2

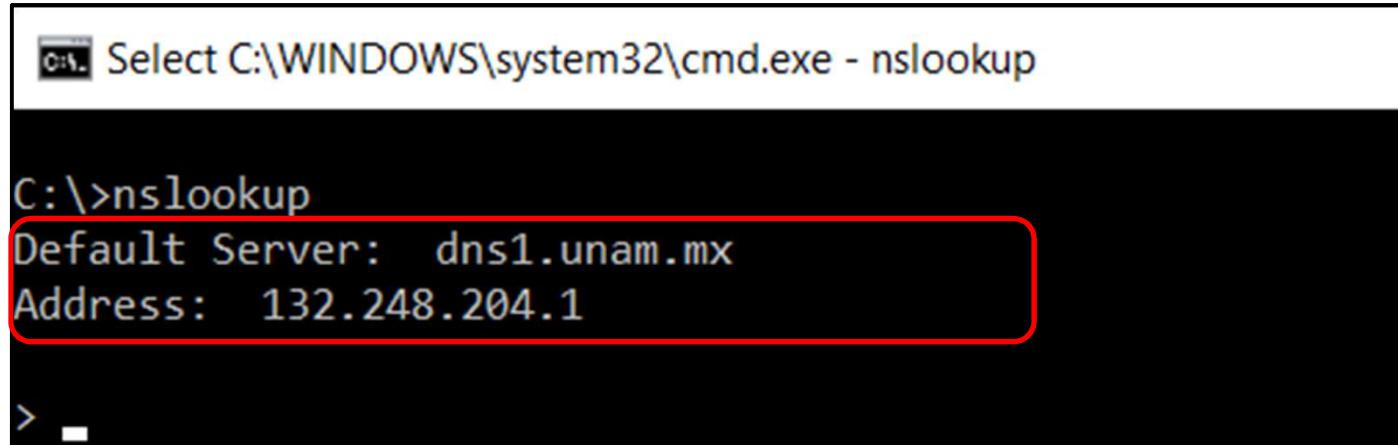
Non-authoritative answer:
gmail.com
    primary name server = ns2.google.com
    responsible mail addr = dns-admin.google.com
    serial = 159412591
    refresh = 900 (15 mins)
    retry = 900 (15 mins)
    expire = 1800 (30 mins)
    default TTL = 60 (1 min)
gmail.com      text =
                "v=spf1 redirect=_spf.google.com"
gmail.com      internet address = 216.58.193.37
gmail.com      AAAA IPv6 address = 2607:f8b0:4012:805::2005
gmail.com      MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
gmail.com      MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com      MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com
gmail.com      MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com      MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
gmail.com      nameserver = ns2.google.com
```

Registros de tipo:
A, MX, NS

Práctica #2: Consultas DNS

Una forma alterna de operación de nslookup es el modo interactivo, para acceder se ingresa en el CMD

nslookup



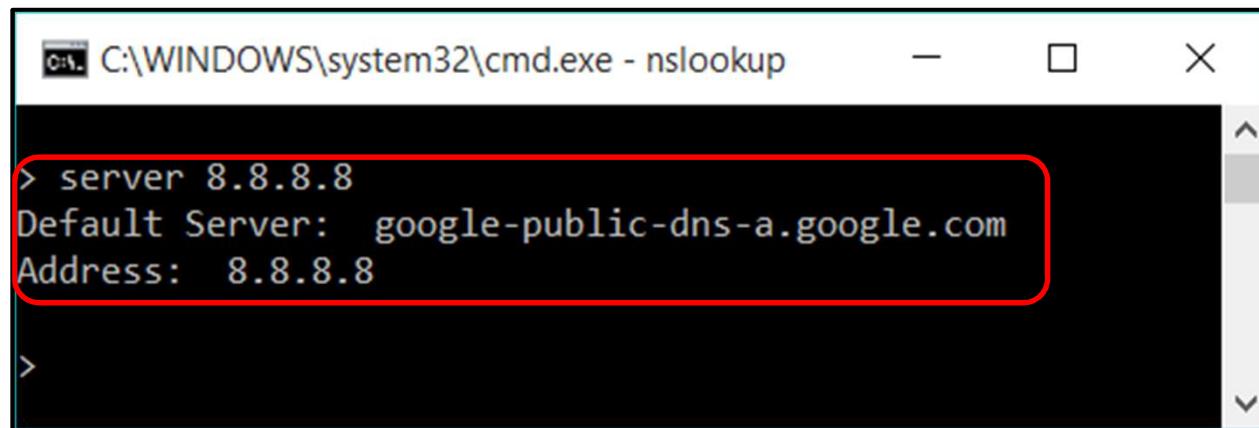
The screenshot shows a Windows Command Prompt window with the title "Select C:\WINDOWS\system32\cmd.exe - nslookup". The command "nslookup" is entered at the prompt, followed by "Default Server: dns1.unam.mx" and "Address: 132.248.204.1". The text from "Default Server:" to "Address:" is highlighted with a red rectangle.

```
C:\>nslookup
Default Server: dns1.unam.mx
Address: 132.248.204.1
```

Práctica #2: Consultas DNS

Con el parámetro server, se configura el servidor DNS al cual se le harán las consultas de nombres de dominio, en este caso utilizaremos un DNS publico de Google con:

server 8.8.8.8

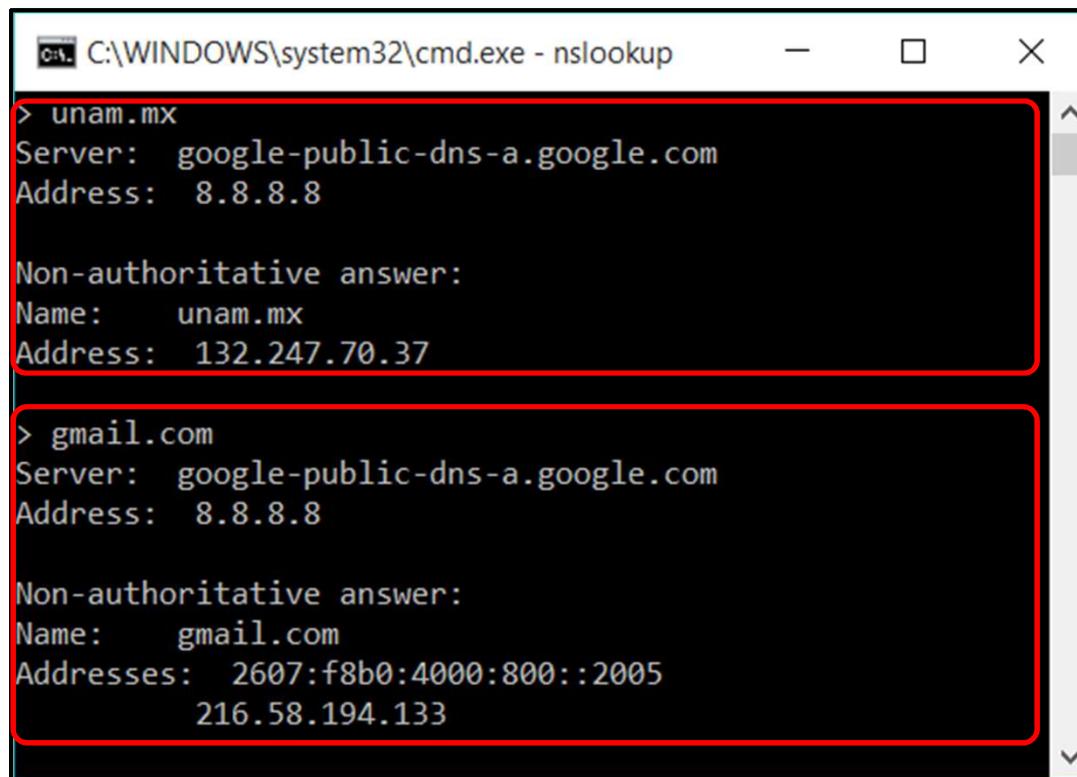


A screenshot of a Windows Command Prompt window titled "C:\WINDOWS\system32\cmd.exe - nslookup". The window contains the following text:
> server 8.8.8.8
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

The line starting with "> server 8.8.8.8" is highlighted with a red rectangle.

Práctica #2: Consultas DNS

Después de haber realizado la configuración del servidor DNS, se indica el nombre de dominio que se desea consultar



```
C:\WINDOWS\system32\cmd.exe - nslookup
> unam.mx
Server: google-public-dns-a.google.com
Address: 8.8.8.8

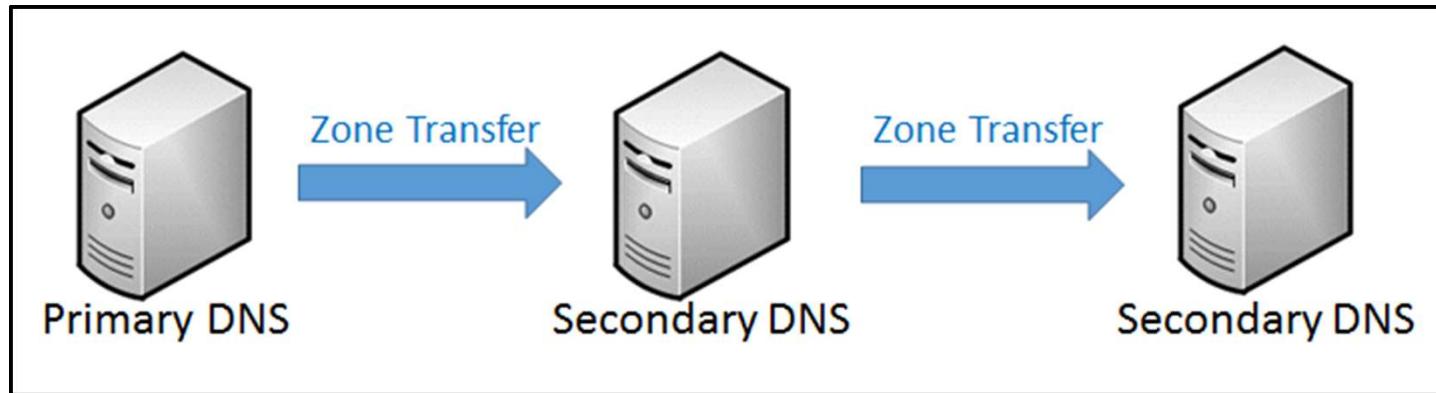
Non-authoritative answer:
Name: unam.mx
Address: 132.247.70.37

> gmail.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: gmail.com
Addresses: 2607:f8b0:4000:800::2005
           216.58.194.133
```

Práctica #2: Transferencia de Zona

Las transferencias de zona son empleadas usualmente entre servidores DNS primarios y secundarios para la sincronización de registros.



(gitlearning.wordpress.com 2017)

Práctica #2: Transferencia de Zona

Realizar una consulta con **whois** sobre un dominio para identificar los servidores DNS

```
root@kali:~# whois zonettransfer.me
Domain Name: ZONETRANSFER.ME
Registry Domain ID: D108500000003513097-AGRS
Registrar WHOIS Server:
Registrar URL: http://www.meshdigital.com
Updated Date: 2015-12-20T07:03:18Z
Creation Date: 2011-12-27T15:34:08Z
Registry Expiry Date: 2017-12-27T15:34:08Z
```

```
Tech Country: GB
Tech Phone: +44.8712309525
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: services@123-reg.co.uk
Name Server: NSZTM1.DIGI.NINJA
Name Server: NSZTM2.DIGI.NINJA
```

Para este ejemplo se usará el servidor DNS
NSZTM1.DIGI.NINJA

Práctica #2: Transferencia de Zona

Para probar si se encuentra habilitada la transferencia de zona ejecutar lo siguiente:

```
# dig axfr @nsztm1.digi.ninja zonetransfer.me
```

Donde

axfr – Representa el protocolo de transferencia autoritativa

@nsztm1.digi.ninja – Servidor DNS al que se realiza la consulta

zonetransfer.me – Nombre de dominio relacionado

Práctica #2: Transferencia de Zona

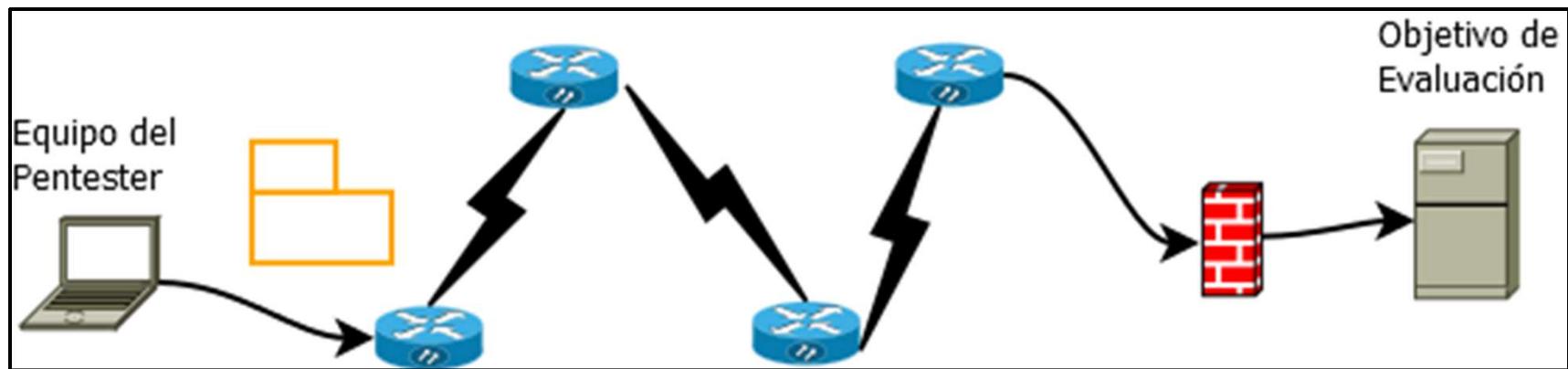
Salida del comando anterior...

```
; <>> DiG 9.10.3-P4-Debian <>> axfr @nsztm1.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.    7200   IN      SOA    nsztm1.digi.ninja. robin.digi.ninja. 2014101603 172800 9
00 1209600 3600
zonetransfer.me.    7200   IN      RRSIG   SOA 8 2 7200 20160330133700 20160229123700 44244 zonetransfer.me. GzQojkYAP8zuT0B9UAx66mTDiEGJ26hVIIP2ifk2DpbQLrEAPg4M77i4 M0yFWHpNfMJIuuJ8nMxQgFVCU3yT0eT/EMbN98FYC8lVYwEZewHtbMmS 88jVlF+c0z2WarjCdyV0+UJCTdGtBJriIczC52EXKw2RCkv3gtdKKVa fBE=
zonetransfer.me.    7200   IN      NS     nsztm1.digi.ninja.
zonetransfer.me.    7200   IN      NS     nsztm2.digi.ninja.
zonetransfer.me.    7200   IN      RRSIG   NS 8 2 7200 20160330133700 20160229123700 44244 zonetransfer.me. TyFngBk2PMWxgJc6RtgCE/RhE0kqeWfhYSBxFxezupFLeiDjHeVXo+S WZxP54Xvfk7jlFClnZ9lRNkL5qHyxRElhH1JJl1hvod0fycqLqCnx XIqkOzUCkm2Mxr80cGf2jVNDUcLPD05XjHg0XCK9tRbVKIpB92f4Qal ulw=
zonetransfer.me.    7200   IN      A      217.147.177.157
zonetransfer.me.    7200   IN      RRSIG   A 8 2 7200 20160330133700 20160229123700 44244 zonetransfer.me. unoMaEPiyoAr0yAWg/coPbAFNznaAlUJW3/QrvJleer50VvGLW/cK+VE DcZLfCu6paQhgJHVddG4p145vVQe3QRvp7EJpUh+SU7dX0I3gnqm0a4H k190S4utcXY5FhaN7xBKHvwBlavQaSHTq61q/iuLSB0lSlqp/DAMUpC+ WzE=
zonetransfer.me.    300   IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.    300   IN      RRSIG   HINFO 8 2 300 20160330133700 20160229123700 44244 zonetransfer.me. Xebvrpv8nCGn/+iHqok1rcItTPqcskv6jpJ1pCo4WYbnqByLultzygWx JlyVzz+wJHEqRQYDjqGbl0dyUgKn2FFnqb1092kKghchHHvoMEh+Jf5i7 0trtucpRs3AtlneLj2vauOCIEdbjma4IxgdwPahKIhgtgWcUInVFh3Rr SwM=
zonetransfer.me.    7200   IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.    7200   IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.    7200   IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.    7200   IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.    7200   IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.    7200   IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.    7200   IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
```

Práctica #2: Conclusiones

- Direcciones IP y nombres canónicos de los servidores.
- Consulta de registros DNS.
 - A
 - MX
 - HINFO
 - PTR
- Pudiese encontrarse información para identificar nuevos objetivos en servidores incorrectamente configurados.

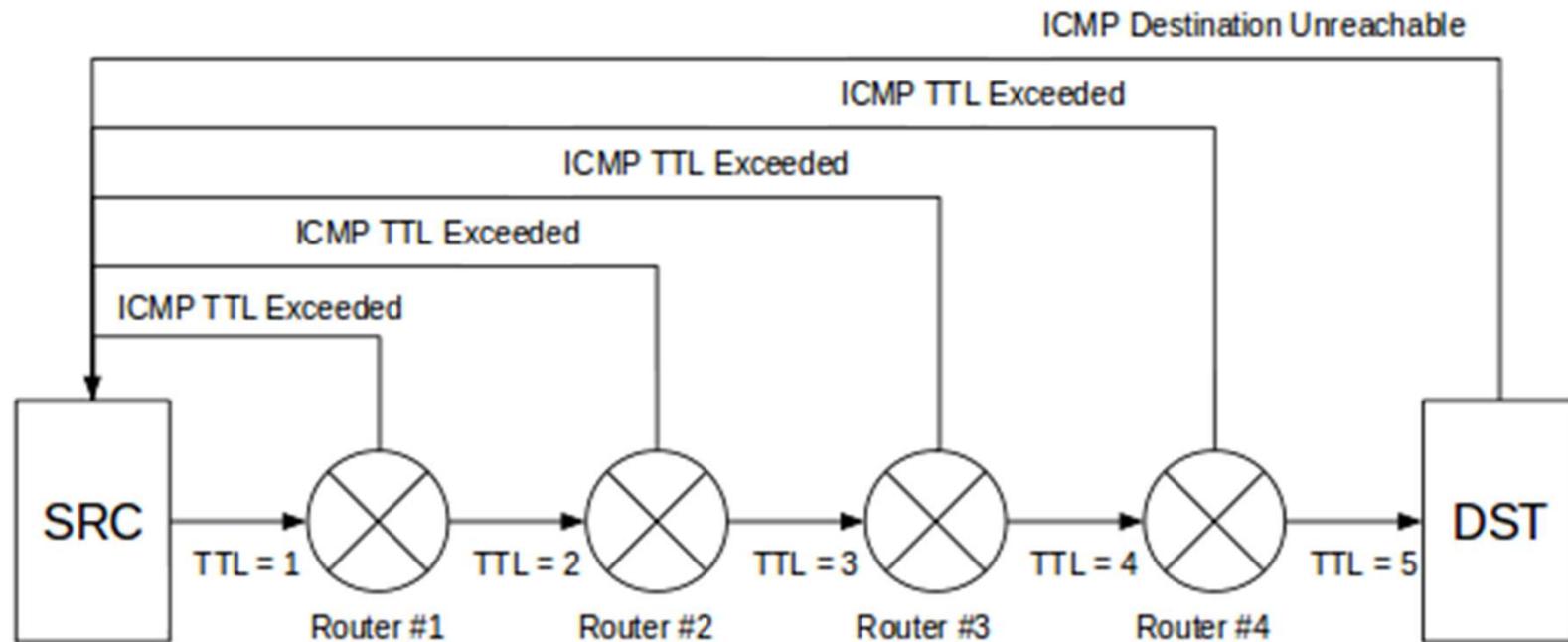
Trazado de ruta de red



Existen herramientas de línea de comandos que se encuentran incluidas en sistemas Windows, Unix/Linux:

- Tracert (Windows)
- Traceroute (Unix/Linux)
- Ping

Trazado de ruta de red



```
tcpdump host 8.8.8.8 -i any -v
```

Traceroute y Tracert



Herramientas dedicadas a la identificación de la ruta de red de un paquete

- Herramientas en línea:
 - <http://hackertarget.com/ip-trace/>
 - <http://www.dnsstuff.com>
 - <http://network-tools.com>

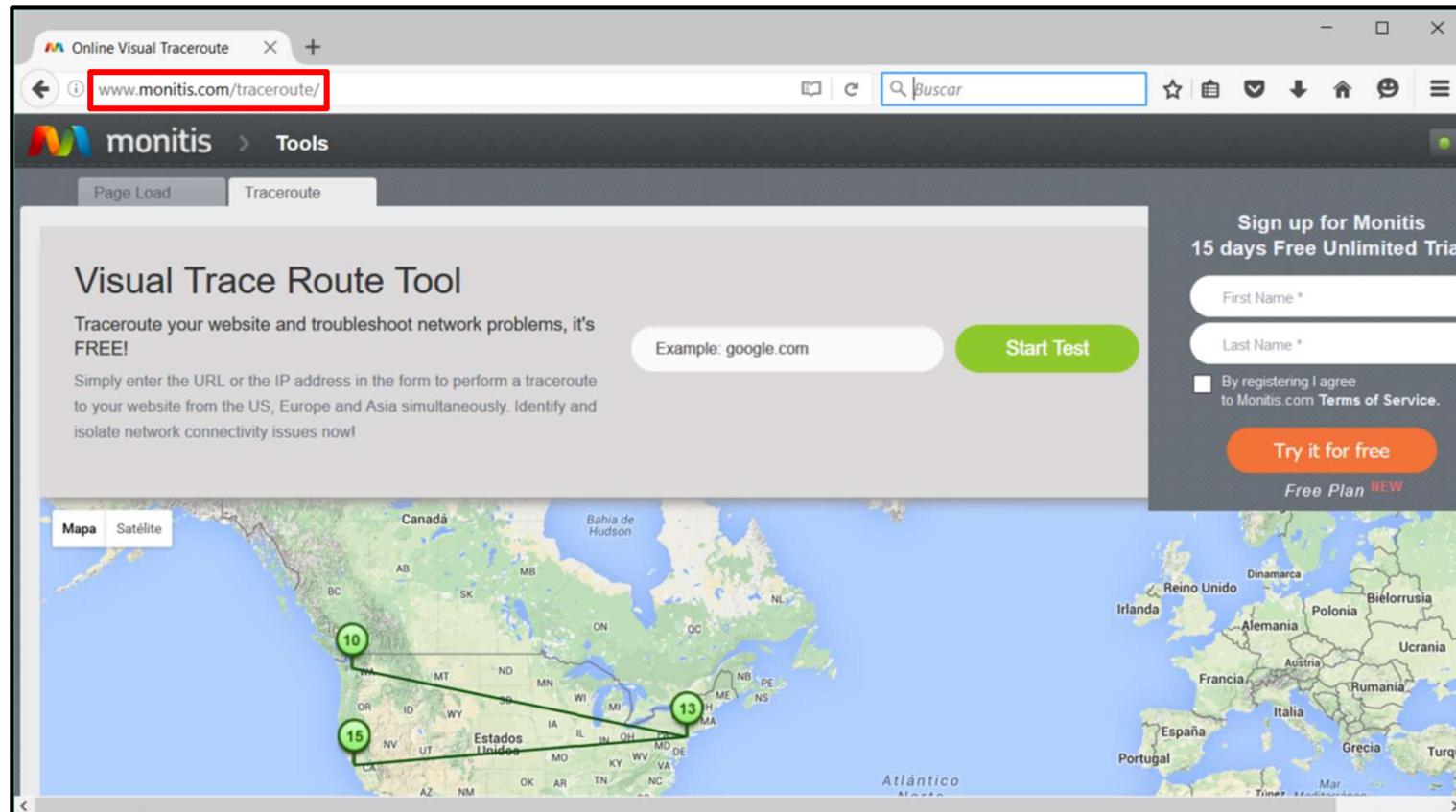
PRÁCTICA #3: TRACEROUTE Y TRACERT

Práctica #3: traceroute y tracert

Mediante las herramientas Tracert y Traceroute se obtiene una traza (ruta) de un paquete IP desde el equipo fuente hasta el destino.

Práctica #3:

Iniciar el navegador e introducir la siguiente URL:
<http://www.monitis.com/traceroute/>



(monitis.com, 2017)

Práctica #3: Desarrollo

Ingresar en el formulario una dirección IP o un nombre de dominio, y dar clic en el botón “*Start Test*”.

Traceroute your website and troubleshoot network problems, it's FREE!

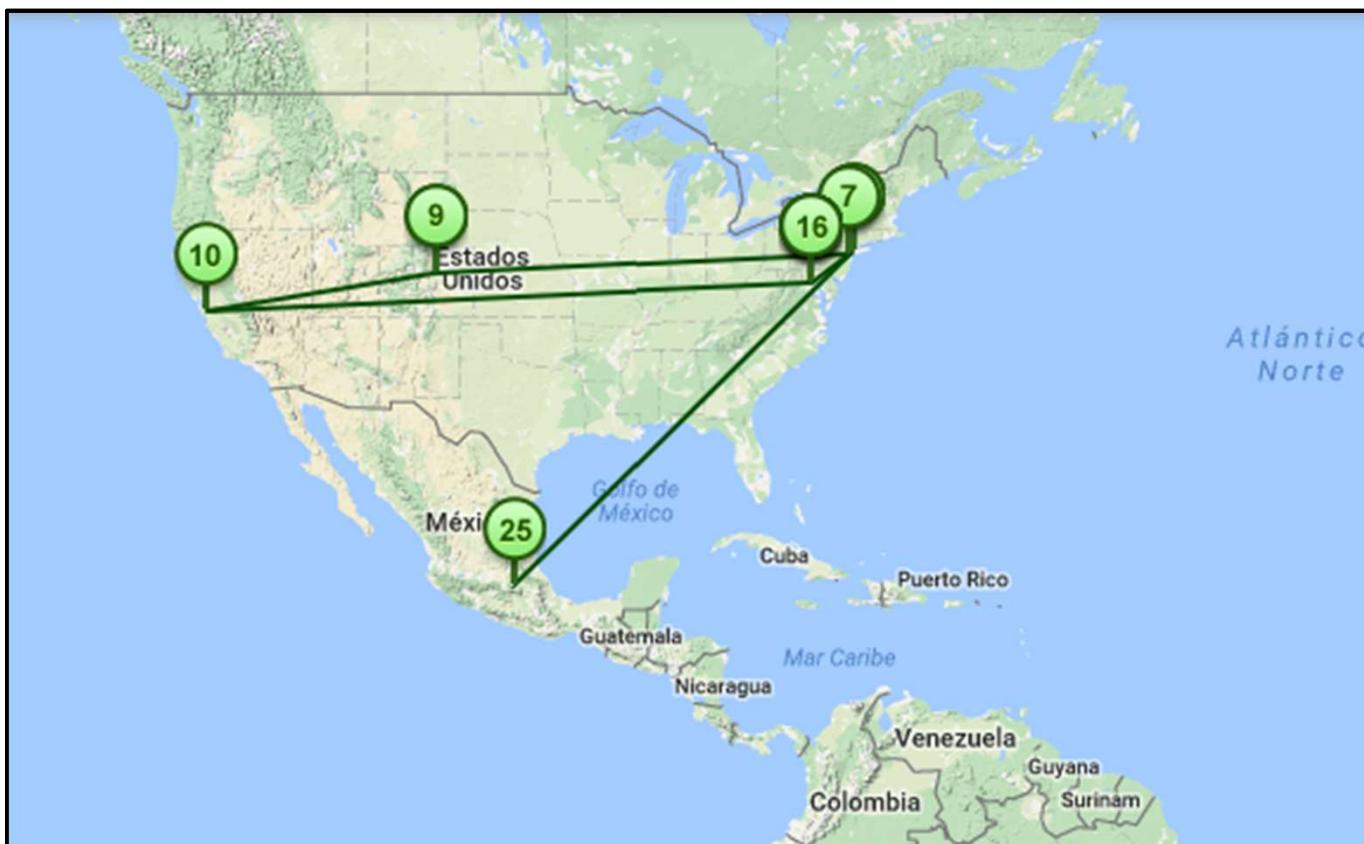
Simply enter the URL or the IP address in the form to perform a traceroute to your website from the US, Europe and Asia simultaneously. Identify and isolate network connectivity issues now!

unam.mx

(monitis.com, 2017)

Práctica #3: Desarrollo

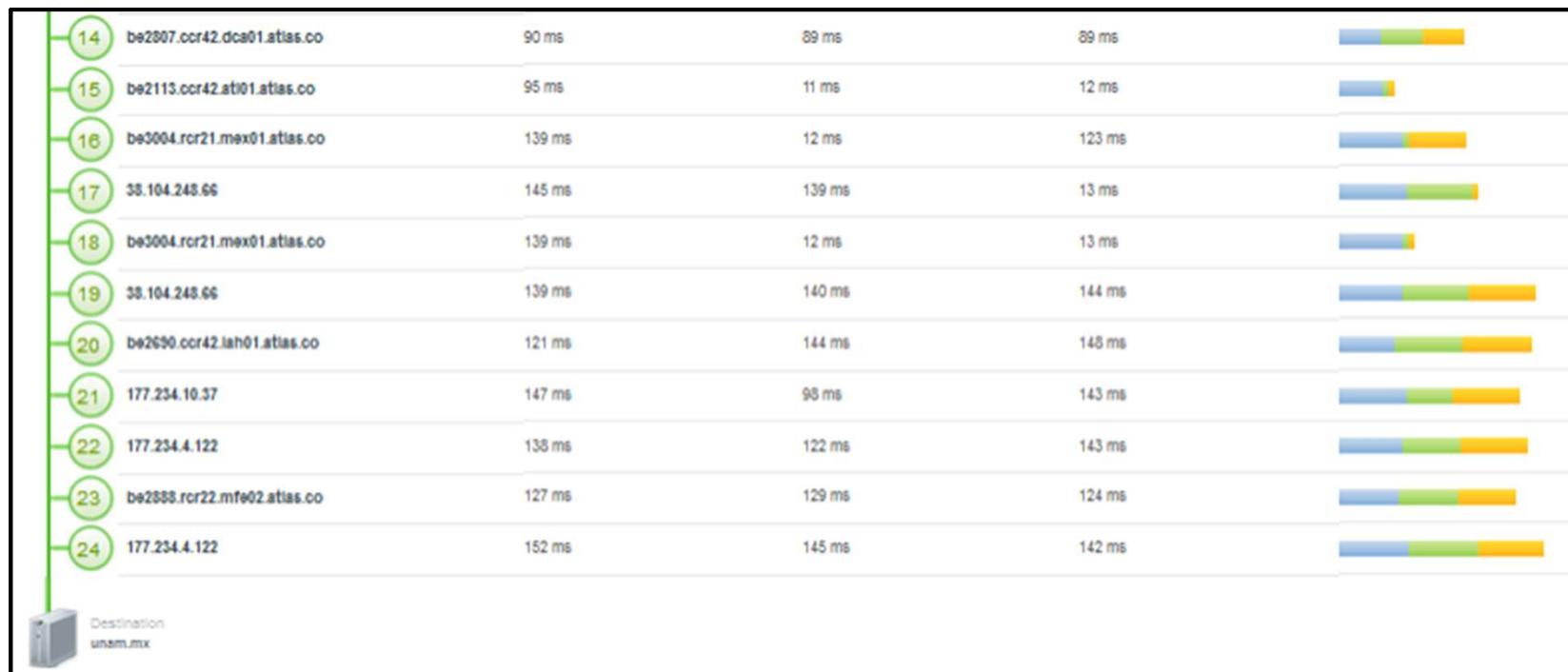
Se muestran los resultados en el mapa



(monitis.com, 2017)

Práctica #3: Desarrollo

Se muestran los resultados de la traza por salto



(monitis.com , 2017)

Práctica #3: Conclusiones

- Número de dispositivos entre fuente y destino.
- Tiempos de llegada en cada intermediario y en el destino.
- Ubicación geográfica de cada dispositivo involucrado en la traza.
- Nombres de dispositivos clave y posibles proveedores de red.

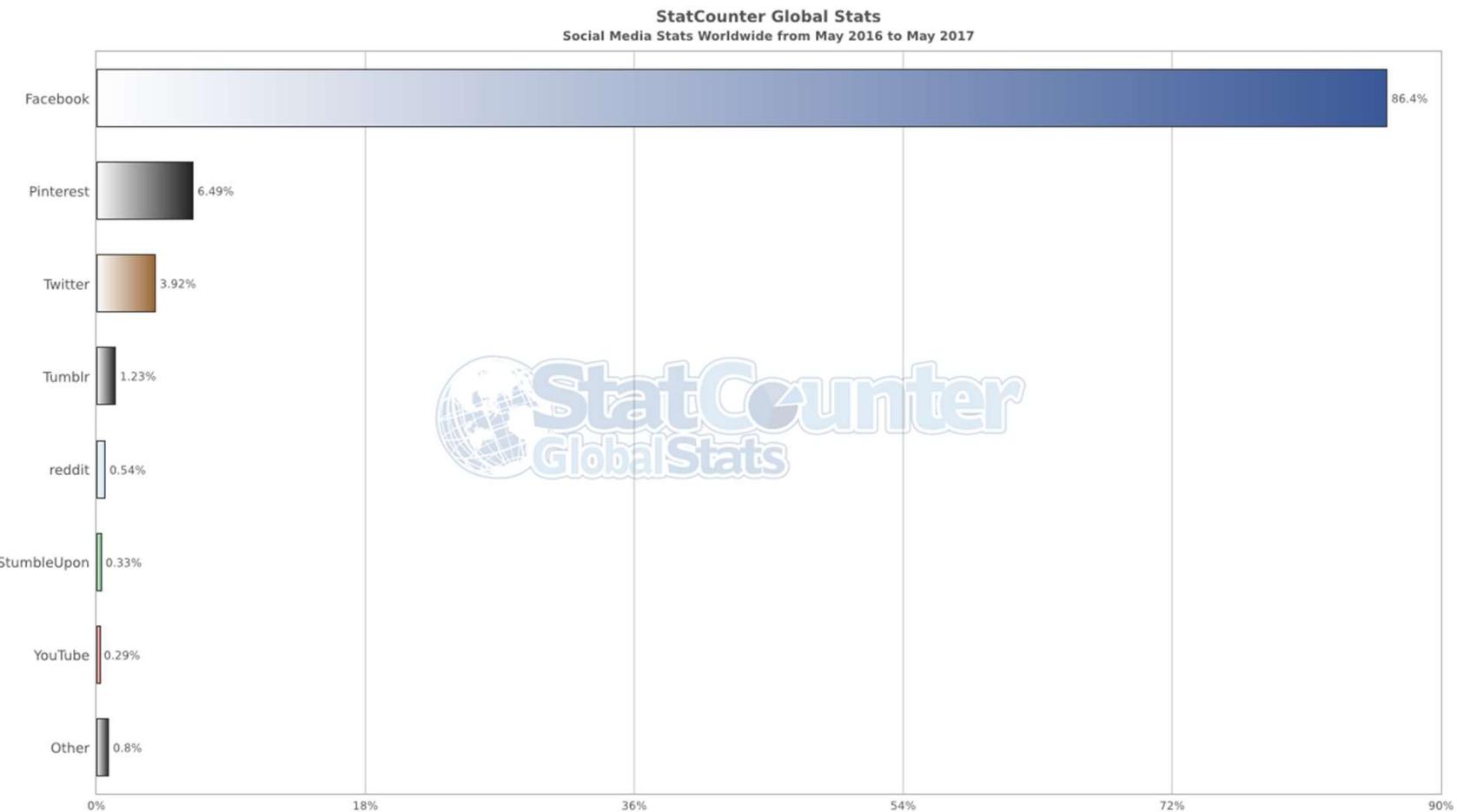
OSINT (OPEN SOURCE INTELLIGENCE)

Redes sociales y buscadores de personas

El uso de las redes sociales ha propiciado la divulgación de información personal en Internet.

Resulta sencillo encontrar perfiles de personas con sólo saber su nombre o bien a través de una foto en el perfil de alguien más.

Redes sociales y buscadores de personas



(statcounter.com, 2017)

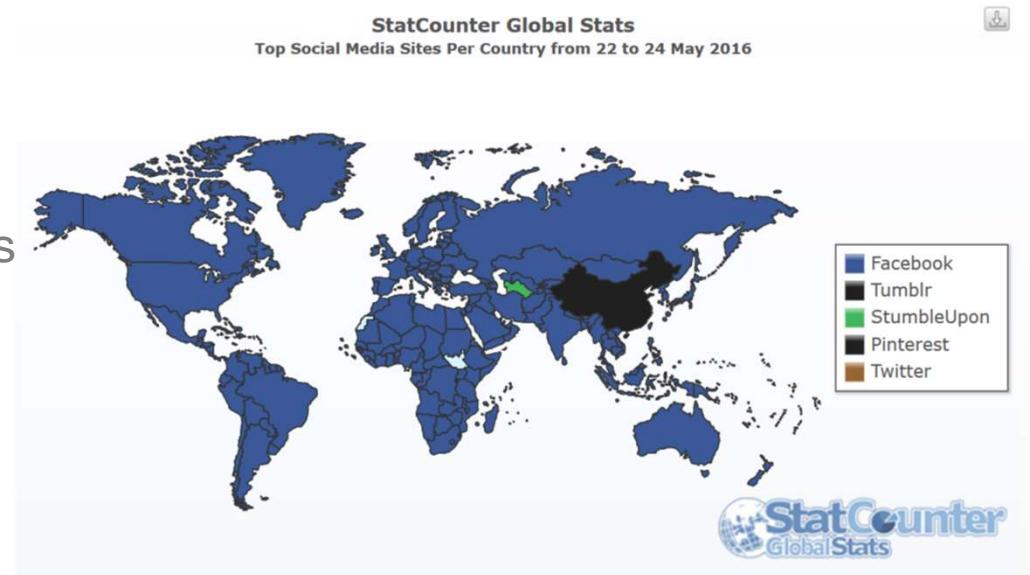
Facebook

Mayor cantidad de usuarios registrados.

Se pueden obtener los siguientes datos de usuario:

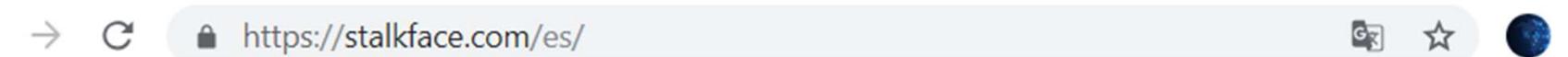
http://gs.statcounter.com/#all-social_media-ww-daily-20160522-20160524-map

- Nombre completo
- Fechas y lugar de nacimiento
- Fotos de familiares y amistades
- Ubicaciones
- Correo electrónico
- Datos de escuela
- Datos de trabajo



(statcounter.com, 2016)

Facebook



StalkFace

Español

Like

Share

Para espiar a alguien, ingrese el **enlace del perfil de Facebook** debajo:

https://m.facebook.com/zuck

Espiar

Atención: esta herramienta no viola la privacidad de la configuración de Facebook. 'Sólo Yo' permanece 'Sólo Yo'. Sólo muestra contenido oculto a lo cual ya tienes acceso

Twitter

- Sitio de microblogging que permite compartir información mediante mensajes cortos.
- Dirección de correo electrónico
- Edad
- Datos financieros
- Contactos de familia
- Contactos de trabajo
- Intereses
- Perfil socioeconómico
- Ubicación



Twitter

Mentions: @username

Exact Phrase: "frase"

OR: term (OR term)*

Links to website: url: url

Exclude: -term

Lenguaje: lang: es

Filtros:

Img/Video: term filter:media

Img: term filter:images

Verificación: filter:verified

Listas: username\listname

#retweets: min_retweets: number

Coordenadas:

geocode:latitude,longitude,
radio.

geocode:19.321856592772193,
-99.18476635210197,.4km

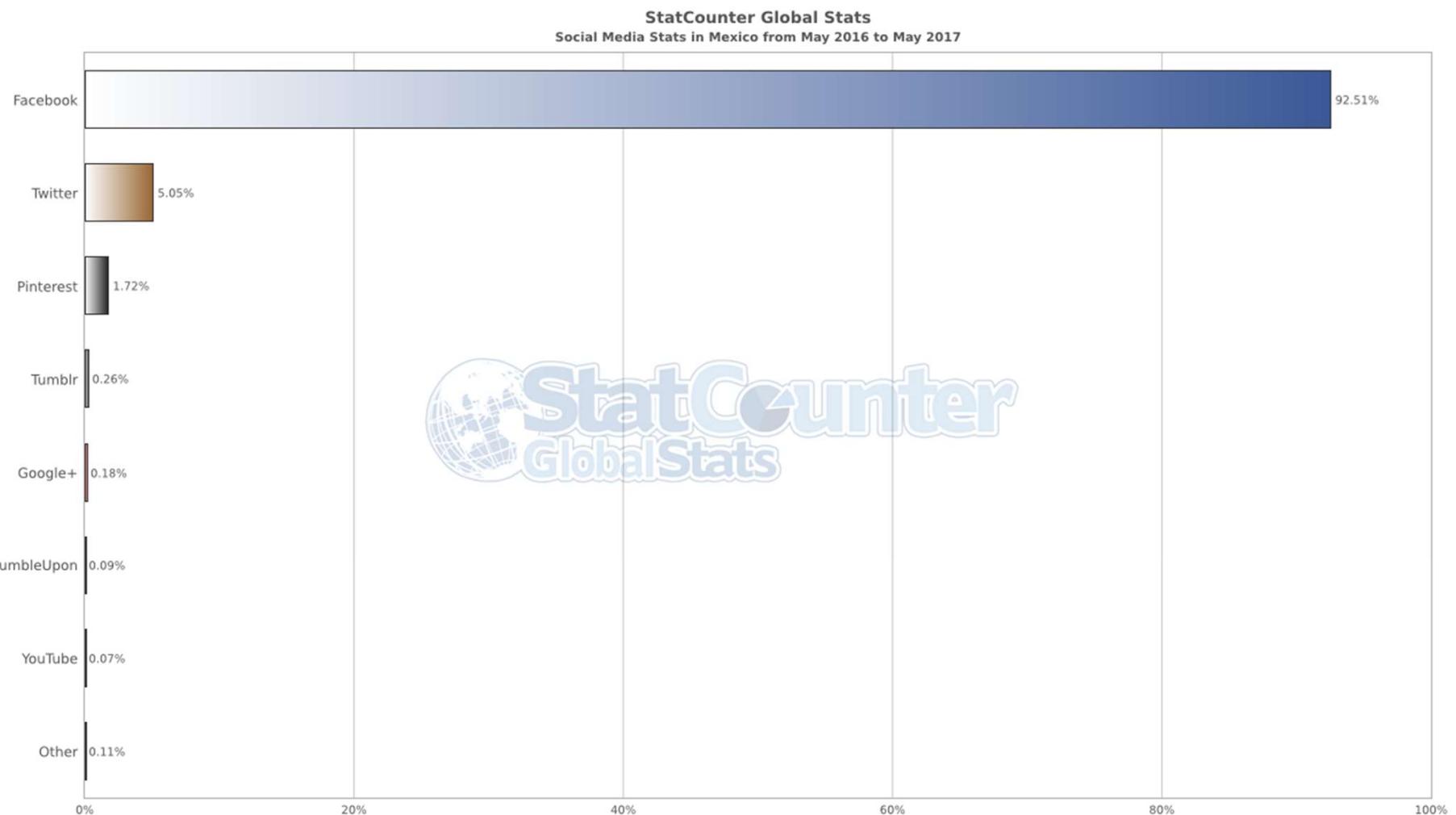


Redes sociales y buscadores de personas

pipl

namechechr

Red social más utilizada en México (Junio 2017)



(statcounter.com, 2016)

Google Hacking

- Técnica muy efectiva para buscar sitios vulnerables e información sensible de las organización a evaluar
- Operadores avanzados
- Motor de búsqueda de Google
- Internet y navegador web

- Características
- Acepta como máximo 10 cadenas
- No es sensible a mayúsculas o minúsculas
- Existen operadores booleanos (|)

Google Hacking (continuación)

Existen operadores avanzados para realizar consultas específicas, los cuales tienen la siguiente sintaxis:

- operador_avanzado:término_búsqueda

- El término se maneja de la misma forma que una búsqueda sencilla, una palabra o frase.
- Si es una frase, no debe existir ningún espacio entre los dos puntos.
- Puede utilizar operadores booleanos (OR, +). No se deben poner en lugar de los dos puntos.
- Todos los operadores que empiezan con ALL no se pueden mezclar con otros operadores.

Operadores avanzados de Google Hacking

intitle

allintitle

inurl

allinurl

site

link

inanchor

daterange

cache

info

related

phonebook

rphonebook

bphonebook

autor

group

msgid

insubject

stocks

define

intitle

- Encuentra cadenas de texto en el título de una página.
- Se puede mezclar con otros operadores.

- allintitle

- Encuentra todo el término de búsqueda en el título de la página.
- No se puede mezclar con otros operadores o términos de búsqueda.
- Ejemplo: allintitle:"crack passwords"

inurl

- Encuentra una cadena en la URL de una página.
- Se puede mezclar con otros operadores.
- Ejemplo: inurl:admin backup

allinurl

- Encuentra el término de búsqueda completo en la URL de una página.
- No se puede mezclar con otros operadores.
- Ejemplo: allinurl:"admin backup"

filetype

- Encuentra tipos de archivos específicos basados en la extensión del archivo.
- Requiere un término de búsqueda adicional.
- Se puede mezclar con otros operadores.
- Ejemplo: filetype:pdf seguridad

site

- Hace una búsqueda restringida a un sitio o dominio en particular.
- Se puede usar con otros operadores avanzados.
- Ejemplo: site:unam.mx

link

- Busca enlaces a un sitio o página en particular.
- No se puede mezclar con otros operadores o términos de búsqueda.
- Ejemplo: **link:www.defcon.org**

inanchor

- Encuentra una cadena en el texto del enlace.
- Se puede usar con otros operadores avanzados.
- Ejemplo: **inanchor:click**

date range

- Busca páginas publicadas en un cierto rango de fechas.
- Los parámetros para este operador siempre deben ser expresados como un rango, separados por un guión.
- Recibe un término de búsqueda.
- El formato para la fecha utilizado es Julian.
- Ejemplo: **daterange: 2452164-2452164 “osama”**

numrange

- Encuentra un número en un rango particular.
- Requiere dos parámetros, un número menor y otro mayor, separados por un guión.
- Se puede usar con otros operadores avanzados.
- Ejemplo: **numrange:550000000-5599999999 filetype:sql**

cache

- Muestra la versión en cache de una página.
- No se puede mezclar con otros operadores o términos de búsqueda.
- Ejemplo: cache:google.com

related

- Muestra sitios que Google ha determinado con relación a un sitio.
- No puede ser utilizado con otros operadores avanzados o términos de búsqueda
- Ejemplo: related:www.unam.mx

PRÁCTICA #4: GOOGLE HACKING Y METADATOS

Práctica #4: Google Hacking

Google hacking es una técnica que utiliza operadores avanzados para realizar consultas específicas, con el objetivo de encontrar información sensible acerca de una organización o un sitio en particular.

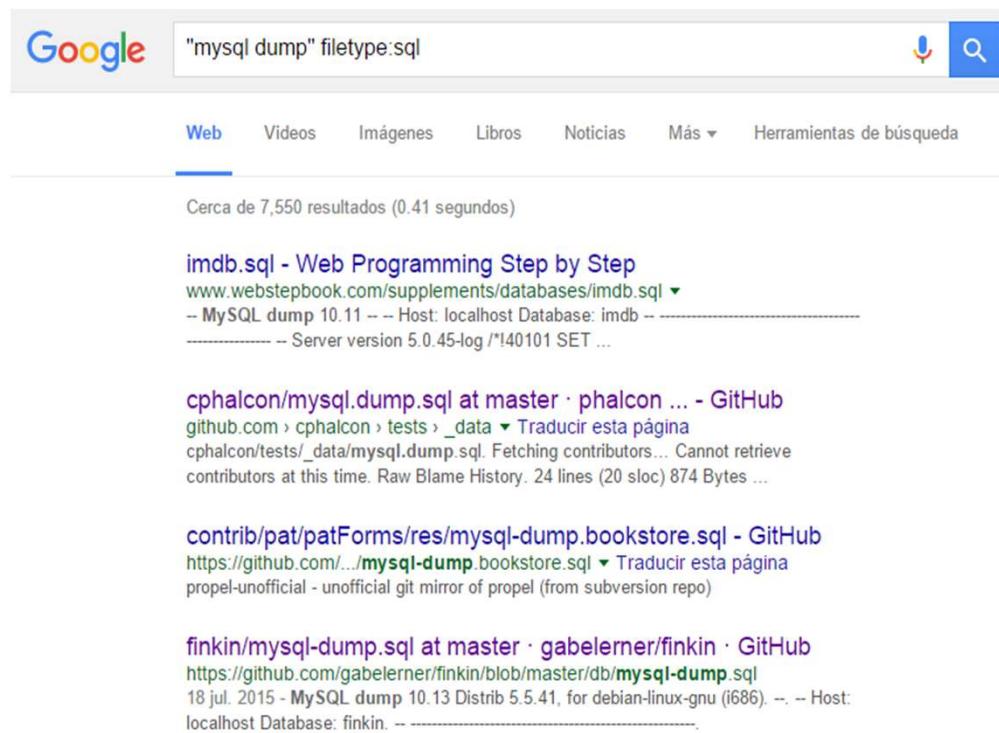


(Google Inc., 2016)

Práctica #4: Desarrollo

Buscar sitios web que alojen respaldos de bases de datos del manejador MySQL, buscando específicamente los archivos .sql

“mysql dump” filetype:sql



A screenshot of a Google search results page. The search query is "mysql dump" filetype:sql. The results are filtered to show only web pages. There are approximately 7,550 results. The first result is a link to a MySQL dump file from a website called "Web Programming Step by Step". The second result is a GitHub repository for a MySQL dump file. The third result is another GitHub repository for a MySQL dump file. The fourth result is a GitHub repository for a MySQL dump file.

Google "mysql dump" filetype:sql

Web Videos Imágenes Libros Noticias Más ▾ Herramientas de búsqueda

Cerca de 7,550 resultados (0.41 segundos)

[imdb.sql - Web Programming Step by Step](#)
www.webstepbook.com/supplements/databases/imdb.sql ▾
-- MySQL dump 10.11 -- Host: localhost Database: imdb --

-- Server version 5.0.45-log /*!40101 SET ...

[cphalcon/mysql.dump.sql at master · phalcon ... - GitHub](#)
github.com/cphalcon/tests/_data ▾ Traducir esta página
cphalcon/tests/_data/mysql.dump.sql. Fetching contributors... Cannot retrieve
contributors at this time. Raw Blame History. 24 lines (20 sloc) 874 Bytes ...

[contrib/pat/patForms/res/mysql-dump.bookstore.sql - GitHub](#)
https://github.com/.../mysql-dump.bookstore.sql ▾ Traducir esta página
propel-unofficial - unofficial git mirror of propel (from subversion repo)

[finkin/mysql-dump.sql at master · gabelerner/finkin · GitHub](#)
https://github.com/gabelerner/finkin/blob/master/db/mysql-dump.sql
18 jul. 2015 - MySQL dump 10.13 Distrib 5.5.41, for debian-linux-gnu (i686). --. -- Host:
localhost Database: finkin. --

(Google Inc., 2016)

Práctica #4: Desarrollo

Buscar cámaras sin protección con ayuda de la siguiente búsqueda:
inurl:view.shtml

The screenshot shows a Google search results page. The search query "inurl:view.shtml" is entered in the search bar. Below the search bar, there are tabs for "Web", "Videos", "Imágenes", "Noticias", "Maps", "Más ▾", and "Herramientas de búsqueda". The "Web" tab is selected. A message indicates "Cerca de 78,900 resultados (0.16 segundos)". A suggestion to "Buscar solo resultados en español" is shown. The first result is a link to "Var_AXIS 2130R PTZ Network Camera - Site Web officiel" from "webcam.salisbury.edu/view/view.shtml". The link has a green downward arrow and the text "Traducir esta página". A note below the link states: "No se dispone de una descripción de este resultado debido a robots.txt. Más información." At the bottom of the search results, it says "(Google Inc., 2016)".

(Google Inc., 2016)

Práctica: Desarrollo

Low hanging fruits

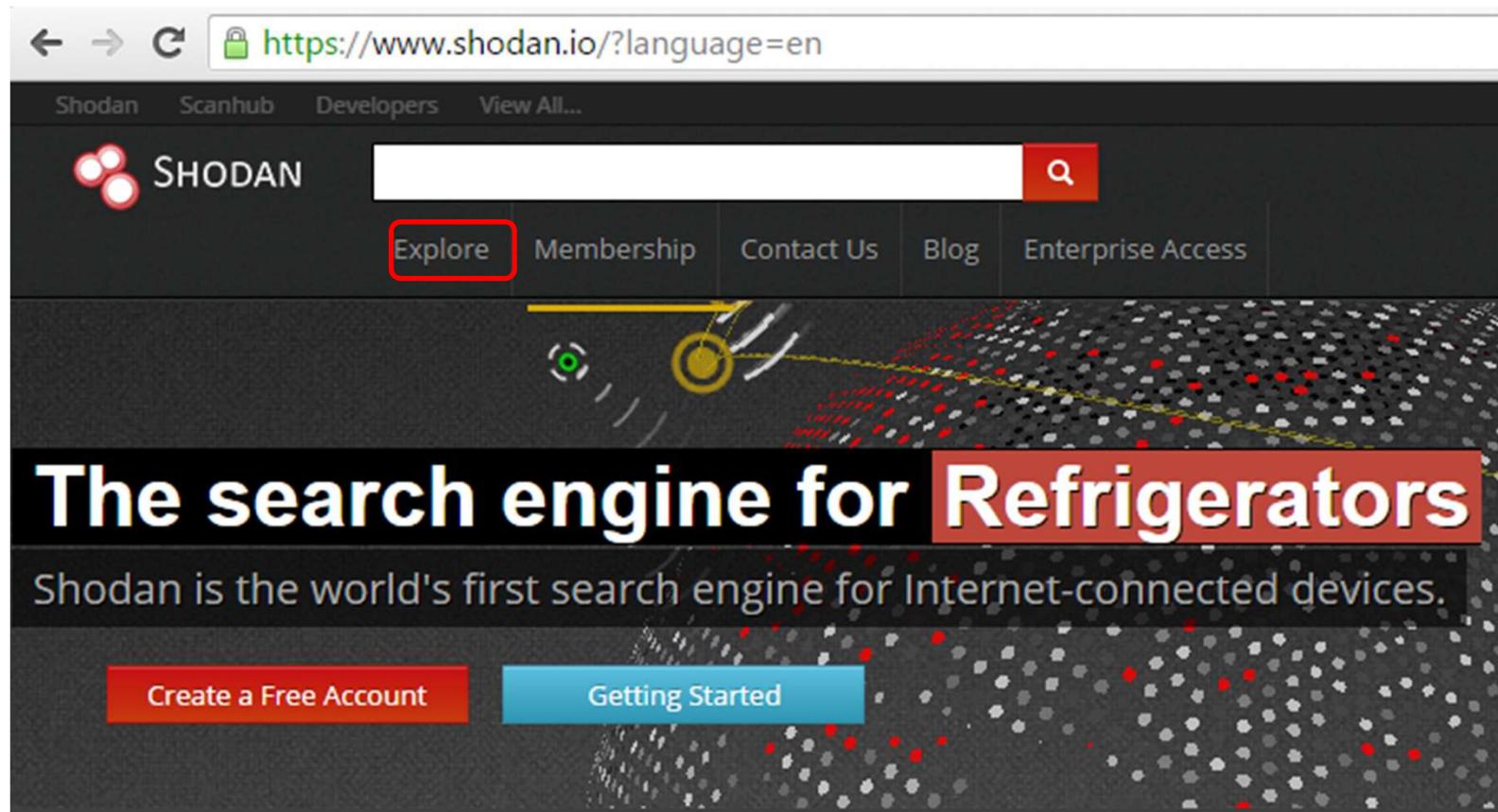


PASTEBIN

PRÁCTICA #4: BUSCADORES

Práctica #4: Desarrollo

Ir a Explore para comenzar a buscar dispositivos de internet.



Práctica #4: Desarrollo

Se puede observar el top de búsquedas más recorridas en Shodan, dar clic en algunas de estas búsquedas y tratar de encontrar algún dispositivo con un servicio de relevancia.

[Ir a images.shodan.io](http://images.shodan.io)

Explore

Discover the Internet using search queries shared by other users.

Popular Searches		Recently Shared		Spotlight
6,491	Webcam best ip cam search I have found yet.	2010-03-15	3	RT-N66U 1
2,088	Cams admin admin	2012-02-06	1	Arqiva On The Net Arqiva On The Net
1,499	Netcam Netcam	2012-01-13	1	Belarus sasas
863	dreambox dreambox	2010-08-13	4	Scada Ports Scada Ports
508	default password Finds results with "default password" in the banner; the named defaults might work!	2010-01-14	1	Scada Ports Scada ports

[More popular searches...](#) [More recent searches...](#)

 Industrial Control Systems [Learn more](#)

Popular Tags

webcam	76
scada	68
camera	57
cam	57
router	54
test	53
http	51
ftp	49
1	42

SHODAN

country:**CENSYS**

código (mx)

product:

"Microsoft IIS httpd"

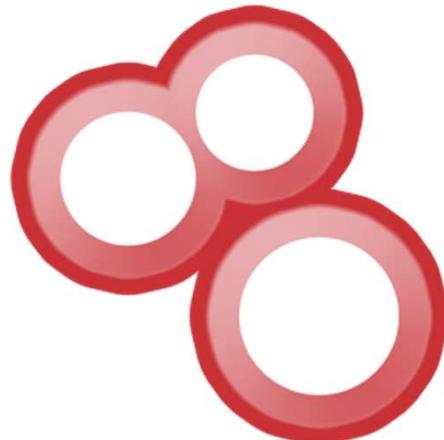
version: "6.0"

www-authenticate: "basic"

port: port_number

ip: segmento[/mascara]

category: categoría (malware)



censys

country:

location.country_code: MX

ip: iprange[/mask] (132.248.0.0/24)

Estructura:

port.service.attribute.attribute: val

Ejemplo:

21.ftp.banner.banner: 230

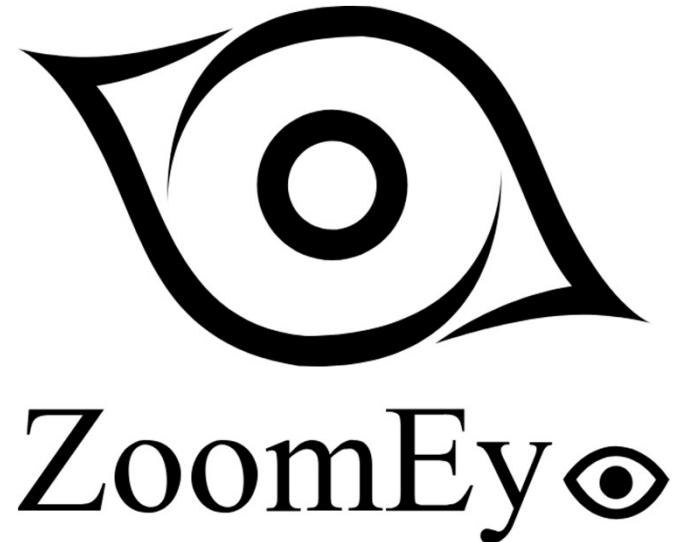
INSECAM

ZOOMEYE

insecam.org/en/bycity/Mexico%20City/

→ X ⓘ https://www.insecam.org/en/

Insecam



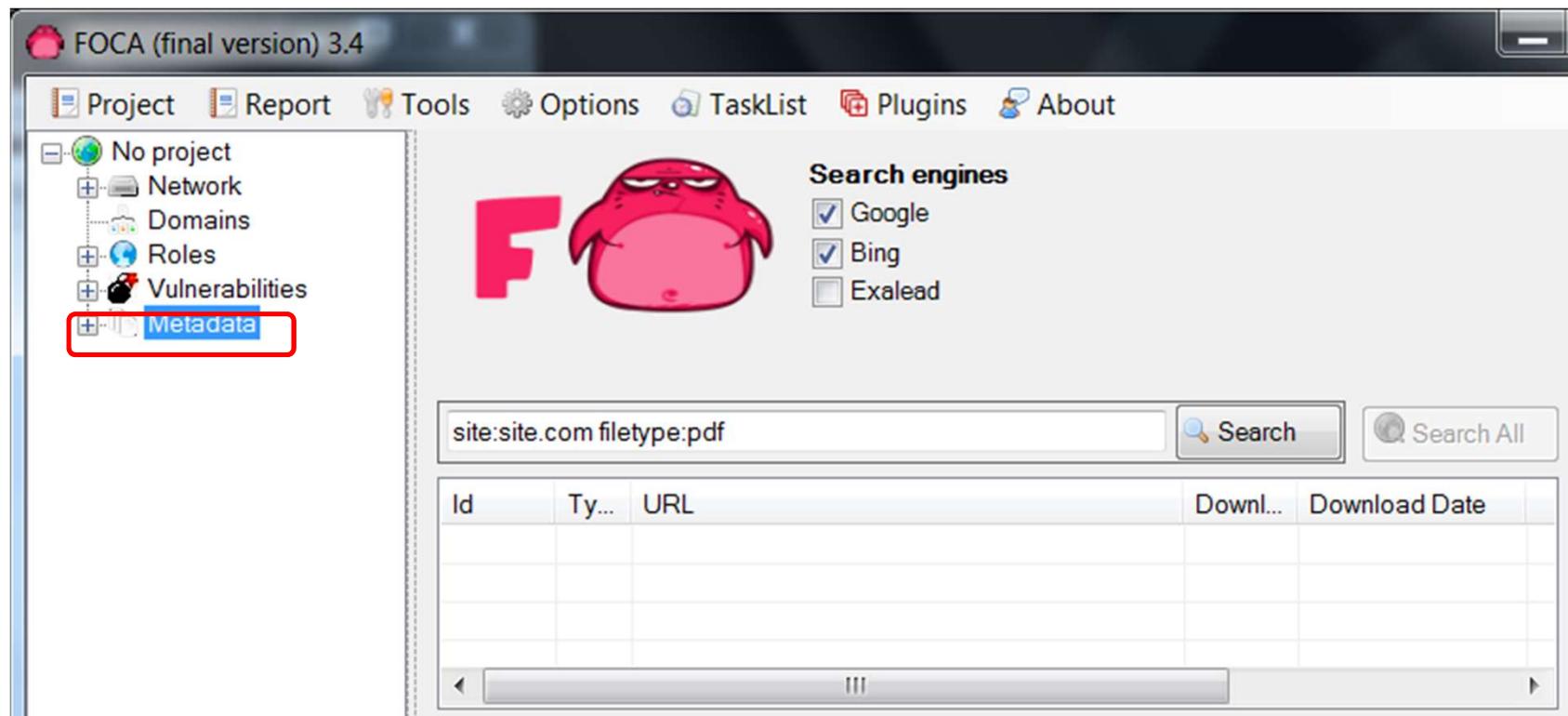
PRÁCTICA #5: METADATOS

Práctica #4: Desarrollo

- Metadatos: datos que contiene información relativa a un documento o archivo (fotos, videos, audio, texto, principalmente).
- Proporcionan características de un archivo, así como multitud de información relacionada con su procedencia.
- Son útiles para catalogar información y optimizar las búsquedas.

Práctica #4: Desarrollo

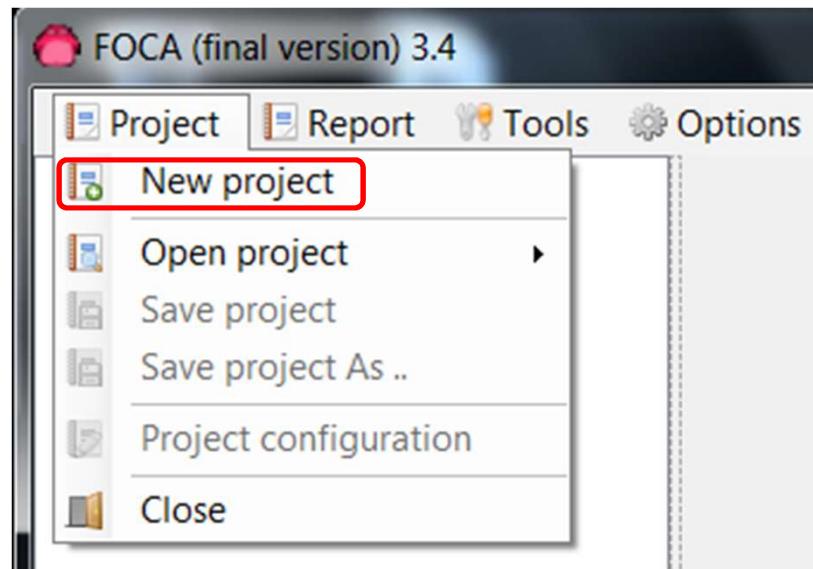
Ejecutar FOCA y dar clic en la opción de metadatos.



Práctica #4: Desarrollo

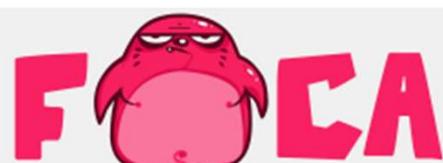
Se puede escanear un sitio completo rápidamente y de una manera muy sencilla con FOCA.

Primeramente localizar y ejecutar FOCA, ir a Project y dar clic en New project.



Práctica #4: Desarrollo

Aparecerá una especie de formulario que hay que llenar acorde a la siguiente imagen, dar clic en el botón create.

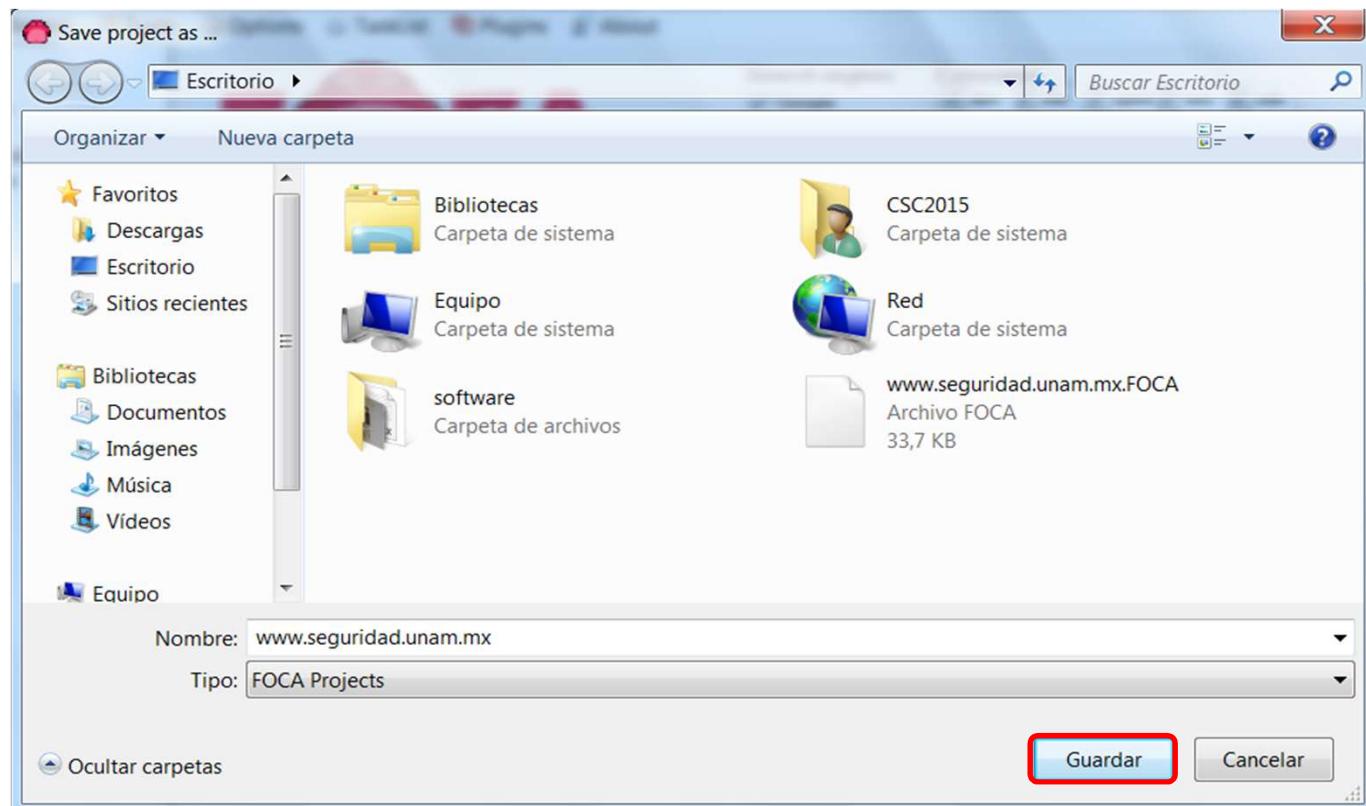


The image shows a screenshot of a software application window titled "FOCA". The interface is a form for creating a new project. Several fields have red boxes around them, indicating they are required or highlighted:

- Project name: "seguridad"
- Domain website: "www.seguridad.unam.mx"
- Folder where save documents: "C:\Users\CSC2015\Desktop" (with a small folder icon next to it)
- Project date: "01/01/0001 0:00:00"
- Autosave project each: "0 minutes" (with a dropdown arrow icon)
- Create button: A button labeled "Create" with a small icon, which is also highlighted with a red box.
- Cancel button: A standard "Cancel" button.

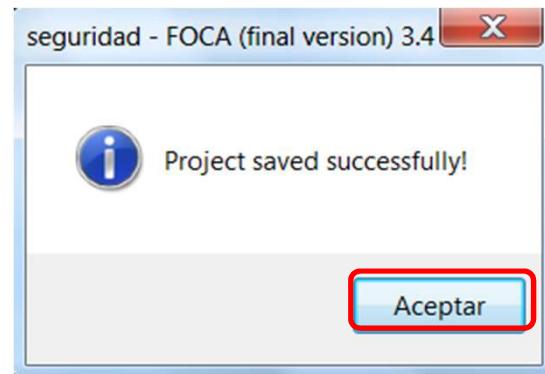
Práctica #4: Desarrollo

Se desplegará una ventana que pide una confirmación para guardar el proyecto en la ruta elegida, dar clic en guardar.

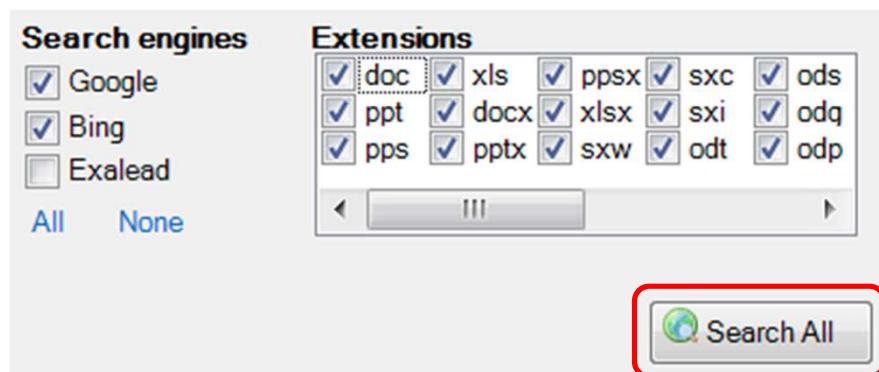


Práctica #4: Desarrollo

Aparecerá una ventana mencionando que el “Proyecto ha sido salvado satisfactoriamente” dar clic en aceptar.

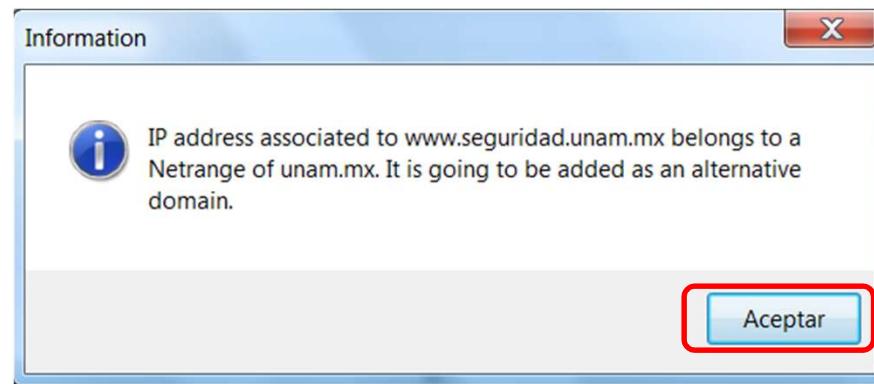


Posteriormente existen unas opciones para personalizar la búsqueda, si no se desean modificar estas configuraciones dar clic en “Search all”



Práctica #4: Desarrollo

Seguramente aparecerá una ventana mencionado que un dominio alternativo va ser adicionado, dar clic en aceptar.



Práctica #4: Desarrollo

Observar los archivos encontrados por FOCA, para extraer sus metadatos es necesario descargar el archivo y posteriormente dar clic en la opcion en “Extract Metadata”.

The screenshot shows the FOCA search interface. At the top, there's a logo of a pink cartoon character and a search bar with the placeholder "Search engines". Below the search bar, three checkboxes are checked: Google, Bing, and Exalead. There are also "All" and "None" buttons. The main area is titled "Custom search" and contains a table with columns: Id, Ty..., URL, and Downl... (Download). The table lists several files:

Id	Ty...	URL	Downl...
W10	doc	http://www.seguridad.unam.mx/eventos/reto/r...	X
W11	doc	http://www.seguridad.unam.mx/eventos/reto/r...	X
W12	doc	http://www.seguridad.unam.mx/eventos/reto/r...	X
W13	doc	http://www.seguridad.unam.mx/eventos/reto/r...	X
W14	doc	http://www.seguridad.unam.mx/eventos/reto/r...	X
W15	doc	http://www.seguridad.unam.mx/eventos/reto/r...	X
W16	pdf	http://www.seguridad.unam.mx/eventos/reto/r...	X
W17	pdf	http://www.seguridad.unam.mx/eventos/reto/r...	X
W18	pdf	http://www.seguridad.unam.mx/eventos/reto/r...	X

For each file, there are several options in a context menu:

- Download (highlighted with a red box)
- Download All
- Delete
- Delete All
- Extract Metadata
- Extract All Metadata
- Analyze Metadata

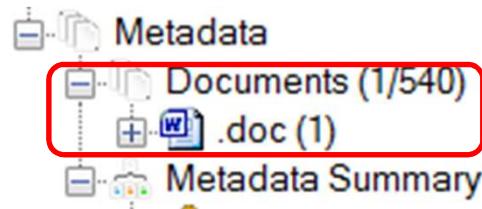
This screenshot shows the same FOCA search interface as the previous one, but with a different context menu for the first file (W10). The menu items are:

- Download
- Download All
- Delete
- Delete All
- Extract Metadata (highlighted with a red box)
- Extract All Metadata
- Analyze Metadata

The rest of the interface and the table of results are identical to the first screenshot.

Práctica #4: Desarrollo

Enseguida se abrirá una pestaña donde aparece la extensión del archivo al cual se le extrajeron los metadatos.



Al desplegar la pestaña de la extensión, aparecerá el nombre del archivo que se descargó, dar clic sobre el y observar los metadatos.

The screenshot shows a navigation pane on the left with icons for 'seguridad', 'Network', 'Domains', 'Roles', 'Vulnerabilities', and 'Metadata'. Under 'Metadata', 'Documents (1/540)' is expanded, showing a file named 'r3_tecnico7.doc'. A red box highlights this file. To the right is a table titled 'Attribute' and 'Value' showing metadata for the file. The table includes:

Attribute	Value
Modified date	25/03/2006 18:15:00
Other Metadata	
Application	Microsoft Office
Encoding	Latin I
Statistics	Pages: 1 Words: 11005 Characters: 62730 Lines: 522 Paragraphs: 25
Revisions	25
Template	Normal.dot
Operating system	Windows XP
Edition time	2982616.02:41:00
Title	El reto forense no da los elementos necesarios, por lo cual se pr...

A red box highlights the entire table area.

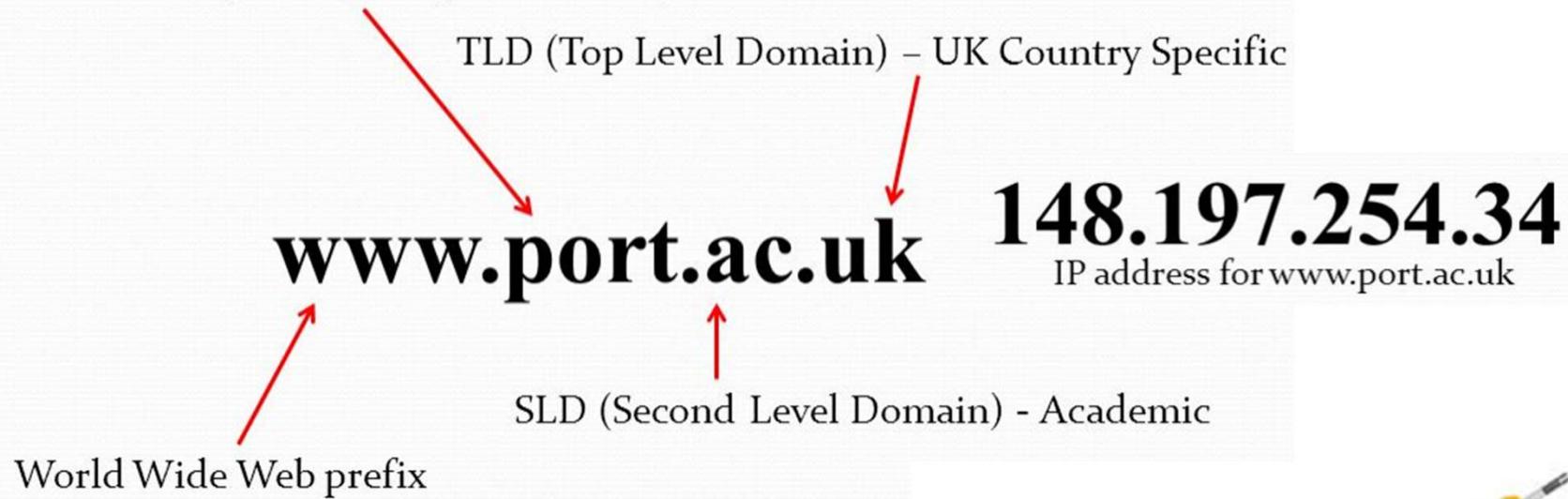
Práctica #4: Desarrollo

- Aprovechar el verdadero potencial del motor de búsquedas de Google.
- Operadores avanzados para filtrar las búsquedas.
- Obtención de información sensible (metadatos), de un sitio completo.
- Herramientas que facilitan la etapa de reconocimiento en un *pentest*
- No siempre los resultados obtenidos son verdaderos pues existen *honeypots* de captura de Google hacking.

PRÁCTICA #5: DOMINIOS

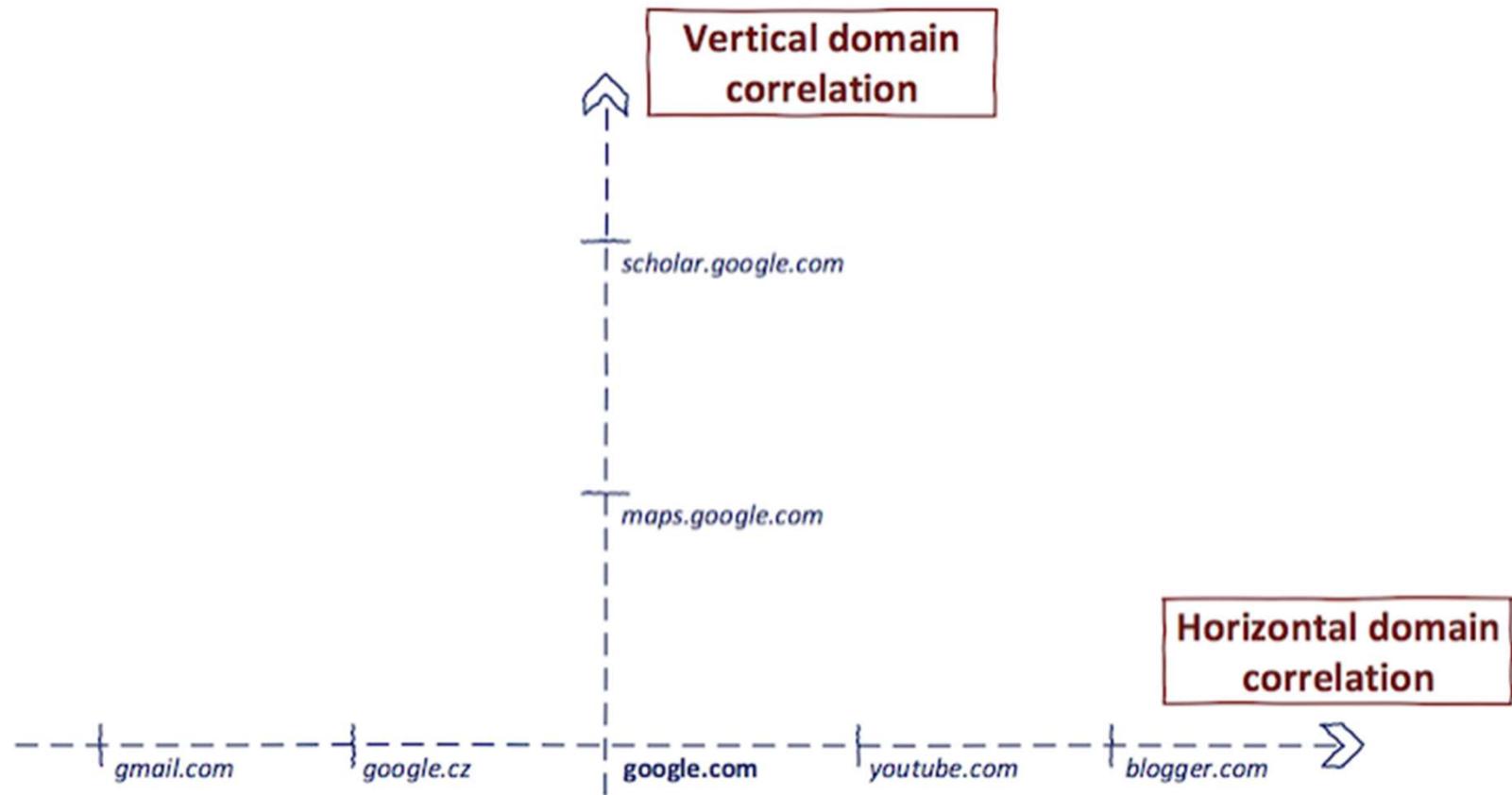
RELACIONES

Domain Name Syntax (string) - University of Portsmouth



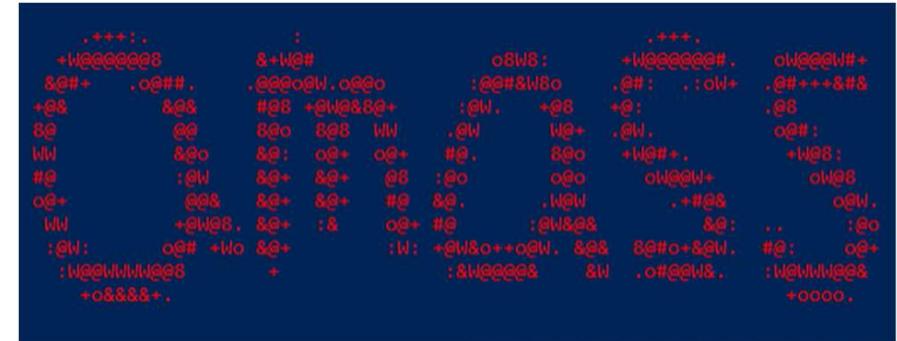
- Vertical
- Horizontal





- **Vertical:** Encontrar dominios con la misma base
- **Horizontal:** Encontrar otros dominios relacionados al objetivo

VERTICAL



```
python sublist3r.py -d domain -e  
[Google,Yahoo,Ask,Bing,Baidu,Netcraft,DNS  
dumpster,Virustotal,ThreatCrowd,SSL  
Certificates,PassiveDNS]
```

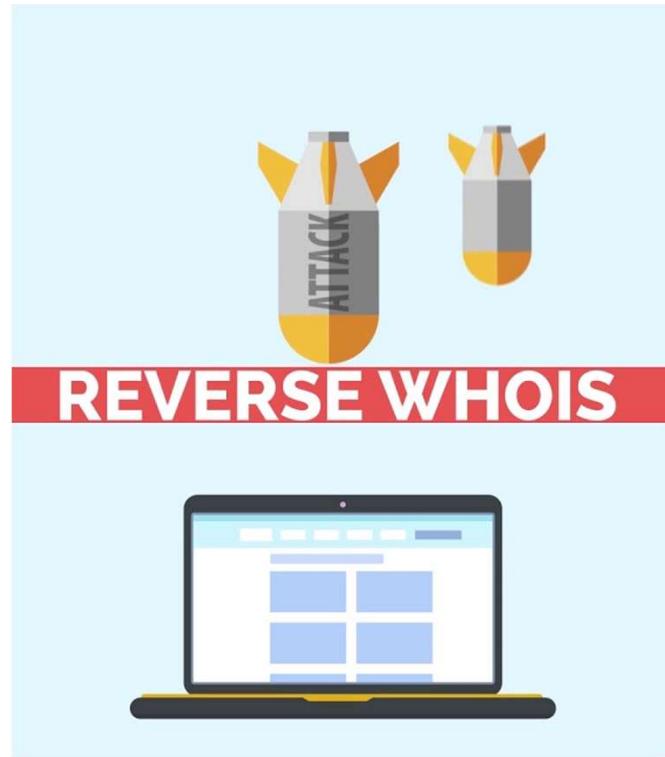


HORIZONTAL

Búsqueda inversa: nombre del registrante

whois -> reverse_whois_lookup

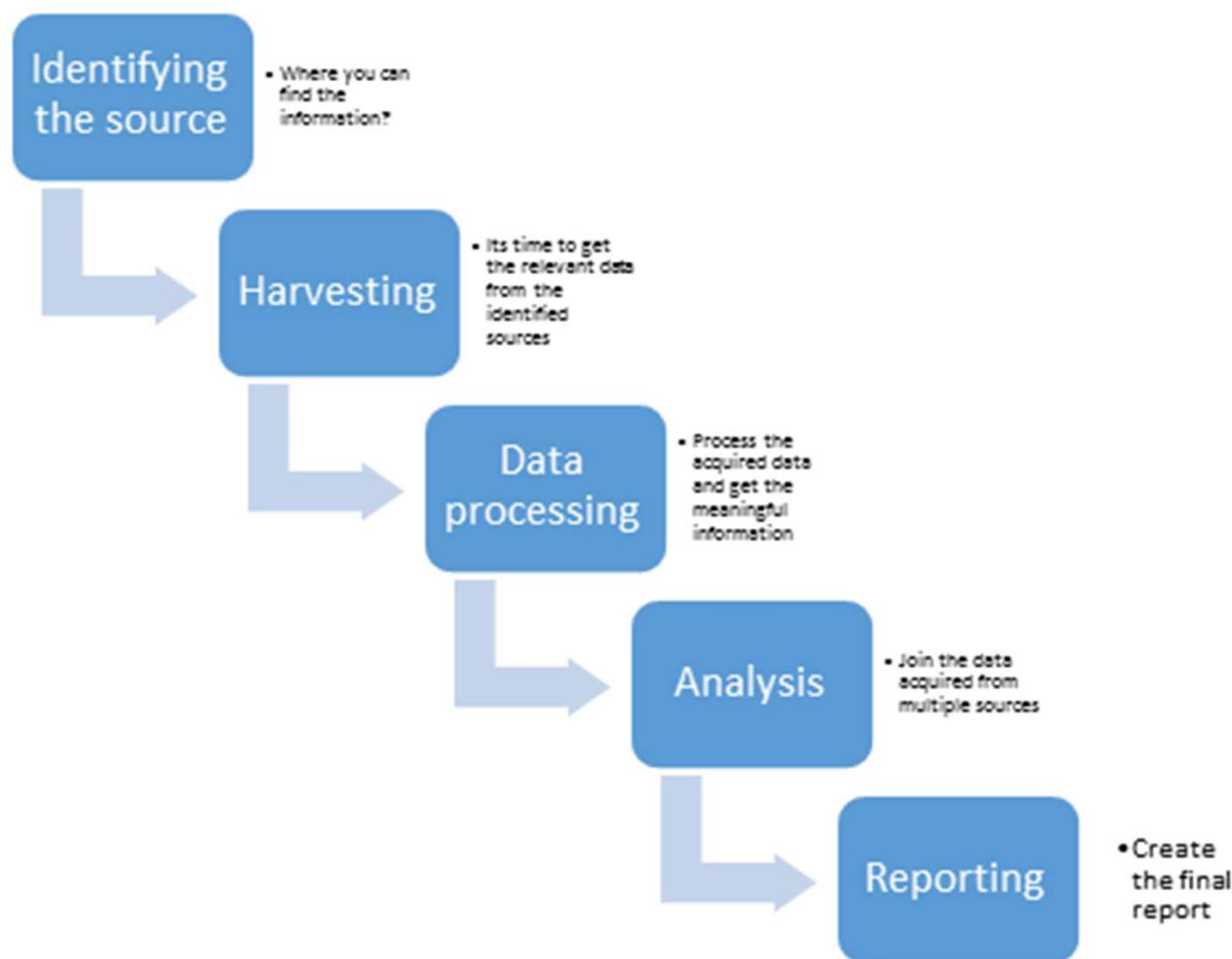
<https://whois.mx/> -> viewdns.info/reversewhois/



robtex

**Built
With**[®]

NETCRAFT



Práctica. Reflexión.

- ¿Qué quiero aprender?
- ¿Sombrero blanco o negro?
- ¿Por qué seguridad de la información, que tan lejos quiero llegar?
- ¿Equipo azul o rojo?

TAREA: READ TEAM

