

Creando una Trayectoria Profesional en Seguridad Digital:

Análisis de Amenazas (sesión teórica)

Agosto, 2021

Tabla de contenidos

Capacitación en Ciberseguridad OEA

Análisis de Amenazas

Conceptos básicos

Pruebas de penetración/Análisis de Vulnerabilidades

Reconocimiento de información en Internet

Geolocalización de direcciones IP

Capacitación en Ciberseguridad OEA

Análisis de Amenazas

Se presentará una introducción conceptual y práctica sobre técnicas ofensivas orientadas a explicar el panorama de amenazas digitales a los cuales está expuesta un organización y/o individuo. **El módulo contiene una práctica y un examen en línea.**

Análisis de Amenazas (1/2)

En esta sesión se abordarán los siguientes temas:

- ▶ Conceptos básicos: vulnerabilidad , amenaza y riesgo
- ▶ Pruebas de penetración y análisis de vulnerabilidades
- ▶ ¿Qué es el CVSS (Common Vulnerability Score System) y CVE (Common Vulnerabilities and Exposures)?
- ▶ Etapas de una prueba de penetración
- ▶ La definición del alcance
- ▶ Breve introducción al reconocimiento de información en Internet (OSINT)
- ▶ Levantamiento de información en la red
- ▶ Registros Whois, DNS y geo-localización
- ▶ Identificación de puertos abiertos, reconocimiento de servicios y *banners*

Análisis de Amenazas (2/2)

- ▶ Reconocimiento de sistemas, plataformas y aplicaciones
- ▶ Explotación
- ▶ Ataques a contraseñas
- ▶ Seguridad en aplicaciones web
- ▶ Breve introducción al top 10 de OWASP
- ▶ Ataques client-side
- ▶ Breve introducción a la seguridad en dispositivos móviles
- ▶ Breve introducción a la seguridad en dispositivos inalámbricos (802.11)

Conceptos básicos (1/3)

- ▶ **Vulnerabilidad:** debilidad en el software, hardware o procedimiento que puede permitir un acceso o maniobra no autorizada. Se caracteriza por la ausencia o debilidad de un control, permitiendo la explotación
- ▶ **Amenaza:** cualquier daño potencial a la información o los sistemas
- ▶ **Riesgo:** probabilidad de que un elemento de amenaza tome ventaja de una vulnerabilidad y genere un impacto al negocio
- ▶ **Control:** contra-medida implementada para mitigar (o reducir) el riesgo potencial

Conceptos básicos (2/3)

Vulnerabilidad , amenaza, riesgo y control

Existe una amenaza: un nuevo ataque de ejecución remota para el APT de Linux (CVE-2019-3462). A menos que la empresa **no utilice la versión afectada**, la aplicación no está expuesta y no hay vulnerabilidad.

Si la vulnerabilidad reside en el entorno, se puede aplicar un *control* (por ejemplo un parche o actualización) para reducir el riesgo.

Conceptos básicos (3/3)

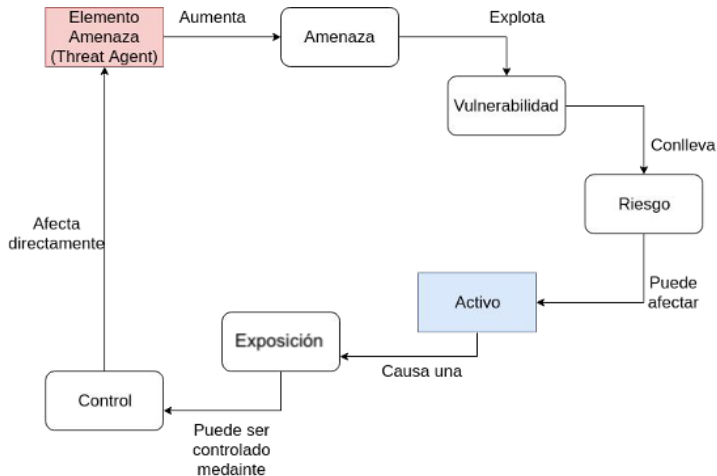


Figura 1: Cadena de detección y tratamiento de amenazas.

Pruebas de penetración/Análisis de Vulnerabilidades (1/8)

- ▶ **Pruebas de penetración:** pruebas ofensivas contra los mecanismos de defensa existentes en un entorno, usualmente ejecutadas de forma manual. Son pruebas aprobadas y coordinadas con los dueños/custodios de los sistemas
- ▶ **Análisis de vulnerabilidades:** pruebas automatizadas donde se analizan los servicios y sistemas informáticos

CVE (Common Vulnerabilities and Exposures)

- ▶ CVE es una **lista de información sobre vulnerabilidades conocidas**, en la que cada referencia tiene un número de identificación único. De esta forma ofrece una nomenclatura común para el conocimiento público de este tipo de problemas, facilitando la compartición de datos sobre dichas vulnerabilidades
- ▶ Fue definido y es mantenido por *The MITRE Corporation* con fondos de la *National Cyber Security Division* del gobierno de los Estados Unidos
- ▶ La información y nomenclatura de esta lista es utilizada en la *National Vulnerability Database* (<https://nvd.nist.gov/>), el repositorio de información sobre vulnerabilidades.

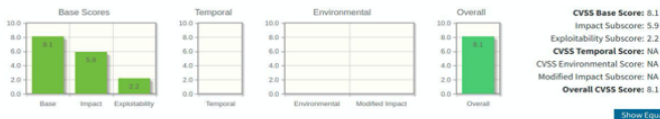
CVSS (Common Vulnerability Score System)

- ▶ Es un estándar de la industria abierto para **evaluar la severidad de las vulnerabilidades de seguridad de un sistema informático**
- ▶ CVSS asigna puntajes de severidad a las vulnerabilidades, permitiendo priorizar las respuestas y los recursos de acuerdo con la amenaza
- ▶ Si bien muchos utilizan solo el puntaje CVSS base para determinar la gravedad de una vulnerabilidad, también existen puntajes temporales y ambientales para tener en cuenta la disponibilidad de las mitigaciones y la forma en que los sistemas vulnerables serán evaluados dentro de una organización

Pruebas de penetración/Análisis de Vulnerabilidades (4/8)

Common Vulnerability Scoring System Calculator Version 3 CVE-2017-0144

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the [CVSS standards guide](#) to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS v3 Vector
AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | **High (AC:H)**

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*

None (UI:N) | Required (UI:R)

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | **High (C:H)**

Integrity Impact (I)*

None (I:N) | Low (I:L) | **High (I:H)**

Availability Impact (A)*

None (A:N) | Low (A:L) | **High (A:H)**

Figura 2: CVSS calculando las métricas de una vulnerabilidad.

MITRE ATT&CK framework

El MITRE ATT&CK framework es una matriz de tácticas y técnicas utilizadas por cazadores de amenazas, equipos de red team y ciber-defensores para clasificar amenazas y evaluar el riesgo de una organización.

La matriz completa se puede observar en este [enlace](#) .

Pruebas de penetración/Análisis de Vulnerabilidades (6/8)

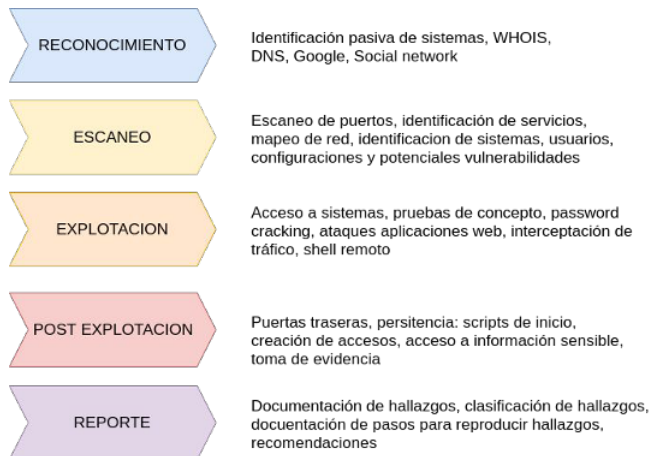


Figura 3: Etapas de una prueba de penetración.

Pruebas de penetración/Análisis de Vulnerabilidades (7/8)

A continuación se lista la definición del alcance de una prueba de penetración:

1. **Definir objetivos:** direcciones IP, URLs, apps o dispositivos
2. **Definir topología:** pruebas a la red interna/ externa/
aplicaciones / inalámbricos / ingeniería social, etc.
3. **Definir un estándar/lista de verificación:** OSSTMM /
NIST 800-15/ PTES/ ISSAF, etc.
4. **Definir el tipo de metodología:**
Blackbox/GreyBox/Whitebox
5. **Definir reglas:** ej. No DoS
6. **Definir tiempos de ejecución y entrega**
7. **Definir tiempos de contacto,** por ej. 24/7
8. **Definir contenido del reporte:** ¿Técnico o ejecutivo?

Pruebas de penetración/Análisis de Vulnerabilidades (8/8)

9. Definir si se ejecutaran pruebas subsecuentes (post-pruebas)

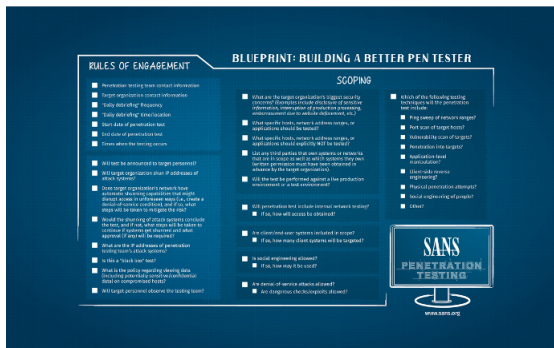


Figura 4: El SANS Intitute provee una guía denominada **Blueprint** con recomendaciones para pruebas de penetración en diferentes servicios.

Reconocimiento de información en Internet (1/22)

Reconocimiento de información en Internet

Existen múltiples fuentes de datos públicas en Internet, donde se puede identificar información sobre un objetivo:

- ▶ Registros WHOIS
- ▶ Registros DNS
- ▶ Entradas en redes sociales, blogs y boards
- ▶ Documentos expuestos en Internet
- ▶ Historial de páginas <https://web.archive.org>
- ▶ Registros en entidades estatales

Reconocimiento de información en Internet (2/22)

Open-source intelligence (OSINT)

- ▶ Open-source intelligence (OSINT) consiste en la recopilación de **información de fuentes disponibles públicamente** para ser utilizadas en un contexto de inteligencia
- ▶ En la comunidad de inteligencia, el término abierto (open) se refiere a fuentes de datos abiertas y públicas (a diferencia de fuentes encubiertas o clandestinas ¿Deep web?)
- ▶ **No está relacionado con software de código abierto**

Existen herramientas y páginas que permiten automatizar la búsqueda de dominios, organizaciones o personas en Internet.
Muchas de ellas requieren registro o pago.

Reconocimiento de información en Internet (3/22)

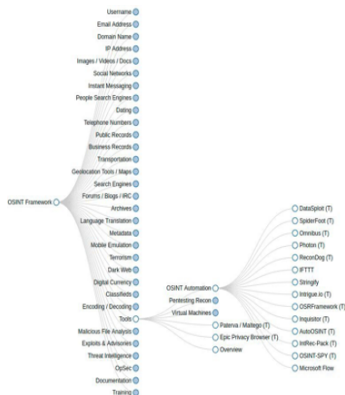


Figura 5: Taxonomía de las búsquedas OSINT

<https://osintframework.com/>

Reconocimiento de información en Internet (4/22)

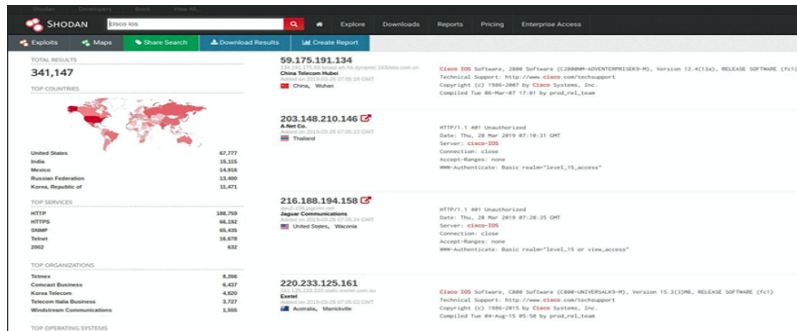


Figura 6: Shodan una maquinaria de búsqueda para dispositivos de IoT.

Reconocimiento de información en Internet (5/22)

Seguridad en en el Internet de las Cosas (IoT)

Es el área de seguridad de la información relacionada a salvaguardar los **dispositivos conectados al Internet de las Cosas (IoT)**.

Reconocimiento de información en Internet (6/22)





INTERNET OF THINGS	INTERNET OF THINGS (Cont)	INTERNET OF THINGS (Cont)	FIRST GENERATION GOOGLETV
BLU-RAY PLAYERS  <ul style="list-style-type: none">Sony BDP-S5100<ul style="list-style-type: none">Sony BDP-S5100 <ul style="list-style-type: none">LG BP350LG BP530 <ul style="list-style-type: none">Panasonic Blu-Ray<ul style="list-style-type: none">DMP-BDT230DMP-BD871	 <ul style="list-style-type: none">Netgear NTV200-100NAS<ul style="list-style-type: none">Netgear NTV200-100NAS <ul style="list-style-type: none">Boxee Box<ul style="list-style-type: none">Boxee <ul style="list-style-type: none">Google Chromecast<ul style="list-style-type: none">Google ChromecastChromecast forum <ul style="list-style-type: none">Roku Streaming Players<ul style="list-style-type: none">Roku <ul style="list-style-type: none">Samsung Allshare Cast<ul style="list-style-type: none">Samsung Allshare Cast <ul style="list-style-type: none">Steam Link<ul style="list-style-type: none">Steam Link	VOIP  <ul style="list-style-type: none">Ooma Telo<ul style="list-style-type: none">Ooma Telo Medical  <ul style="list-style-type: none">SJM Merlin at Home<ul style="list-style-type: none">SJM Merlin at Home Networking  <ul style="list-style-type: none">Belkin N300<ul style="list-style-type: none">Belkin N300 <ul style="list-style-type: none">Google (TP-Link)<ul style="list-style-type: none">Google OnHub (TP-Link)Google OnHub Forum <ul style="list-style-type: none">Google (ASUS)<ul style="list-style-type: none">Asus OnHubGoogle OnHub Forum	Logitech Revue  <ul style="list-style-type: none">Revue software rootLogitech Revue UART rootRevue forumInfo on Logitech Revue Sony NSZ-GT1  <ul style="list-style-type: none">Sony NSZ-GT1 (Bluray Player)<ul style="list-style-type: none">NSZ-GT1 Forum Sony NSX-##GT1  <ul style="list-style-type: none">Sony NSX-40GT1 (Internet TV)<ul style="list-style-type: none">NSX-40GT1 Forum Sony Generic  <ul style="list-style-type: none">Sony Bootloader HW RootSony Unsigned Kamels (SW Root)Sony SATA HW RootI've rooted... now what?!

Figura 7: exploitee.rs es un sitio para reportar y analizar dispositivos de IoT con diferentes vulnerabilidades.

Reconocimiento de información en Internet (7/22)

Background

Site title	OAS - Organization of American States: Democracy for peace, security, and development	Date first seen	January 1996
Site rank	82981	Primary language	English
Description	Not Present		
Keywords	Not Present		
Netcraft Risk Rating (FAQ)	0/10		

Network

Site	http://www.oas.org	Netblock Owner	RCN
Domain	oas.org	Nameserver	oasurk3.oas.org
IP address	207.237.157.11 (usuckus)	DNS admin	system@oasum1.oas.org
IPv6 address	Not Present	Reverse DNS	oas.org
Domain registrar	pir.org	Nameserver organisation	whois.pir.org
Organisation	US	Hosting company	RCN Corporation
Top Level Domain	Organization websites (.org)	DNS Security Extensions	unknown
Hosting country	US		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	netcraft
RCN 450 College Road East Princeton NJ US 08540	207.237.157.11	Linux	Microsoft-IIS/5.5	1-Feb-2019	
RCN 450 College Road East Princeton NJ US 08540	207.237.157.11	unknown	Microsoft-IIS/5.5	9-Jan-2017	
RCN 450 College Road East Princeton NJ US 08540	207.237.157.11	Linux	Microsoft-IIS/6.0	29-Jun-2016	
RCN 450 College Road East Princeton NJ US 08540	207.237.157.11	unknown	Microsoft-IIS/6.0	5-Dec-2014	
RCN 450 College Road East Princeton NJ US 08540	207.237.157.11	Windows Server 2003	Microsoft-IIS/6.0	12-Jun-2014	
Organization of American States 1808 F Street Washington DC US 20006	189.75.107.11	Windows Server 2003	Microsoft-IIS/6.0	10-Feb-2004	
Organization of American States 1808 F Street Washington DC US 20006	189.75.107.11	NT4/Windows 98	Microsoft-IIS/4.0	8-Feb-2001	

Figura 8: **Netcraft** : herramienta de recopilación de datos enfocada al ciber-crimen.

Reconocimiento de información en Internet (8/22)

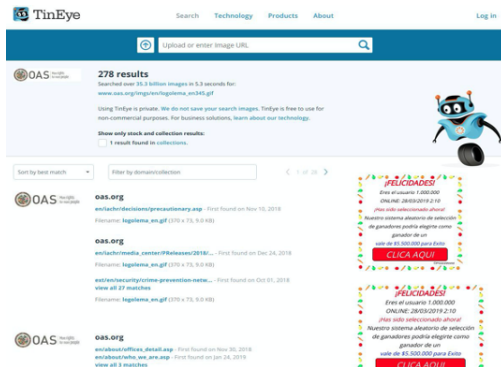


Figura 9: TinEye : herramienta para la búsqueda reversa de imágenes.

Reconocimiento de información en Internet (9/22)

En la siguientes lista se describen algunas herramientas para el análisis de tipo OSINT:

- ▶ [AbuseIPDB](#): analiza la reputación de direcciones IP
- ▶ [BrightCloud URL/IP Lookup](#): presenta información histórica de la reputación de un sitio web
- ▶ [CheckPhish](#): analiza si una URL ha sido reportada como sitio de *phishing*
- ▶ [Email Blocklist Checker](#): analiza el un correo, nombre de dominio o dirección IP en relación a listas negras de correo
- ▶ [NAMECHK](#): comprueba si un nombre de usuario está disponible en más de 150 servicios en línea
- ▶ [desenmascara.me](#): analiza si un sitio contiene productos fraudulentos

Reconocimiento de información en Internet (10/22)

- ▶ [Google Safe Browsing](#): analiza el estatus de navegación segura de un sitio web
- ▶ [IPQualityScore](#): presenta un puntaje de riesgo a un dominio o una dirección IP
- ▶ [Scamadviser](#): analiza si un sitio contiene información de ventas fraudulentas
- ▶ [Twitonomy](#): busca, filtra y obtiene datos estadísticos de perfiles en la red social Twitter
- ▶ [Tweet Map](#): muestra en un mapa geográfico las tendencias de Twitter en tiempo real
- ▶ [Trends Map](#): muestra en un mapa geográfico las tendencias de Twitter en tiempo real en términos de *hashtags*
- ▶ [FB People Directory](#): directorio de nombres de personas en Facebook

Reconocimiento de información en Internet (11/22)

- ▶ **FlightAware**: radar de vuelos en tiempo real
- ▶ **AnnualReports**: reportes financieros anuales de compañías al rededor del mundo
- ▶ **Pipl**: buscador de personas que las relaciona con distintas redes sociales y vínculos en Internet
- ▶ **METAPICZ**: Permite extraer los metadatos a fotografías y con esto conocer distinta información como: el modelo de la cámara empleada, software de edición, fechas y modelos de dispositivos que fueron utilizados
- ▶ **FOCA/Evil FOCA**: conjunto de programas que que permiten extraer y analizar los metadatos a distintos tipos de documentos, pudiendo así, tener datos como: autoría, fechas de modificación, tipo de software que lo genera y la distinta información relacionada con los archivos recuperados

Reconocimiento de información en Internet (12/22)

Metadatos en archivos gráficos

- ▶ Múltiples formatos gráficos soportan la opción de agregar metadatos a las imágenes, incluyendo las coordenadas en la toma de la fotografía, el tipo de dispositivo de captura, las configuraciones de la cámara, etc.
- ▶ Exchangeable image file format (Exif) es una especificación para formatos de archivos de imagen usado por las cámaras digitales
- ▶ La especificación Exif usa los formatos de archivos existentes como JPEG, TIFF Rev. 6.0, y RIFF y el formato de archivo de audio WAVE, a los que se agregan etiquetas específicas de los metadatos

Reconocimiento de información en Internet (13/22)

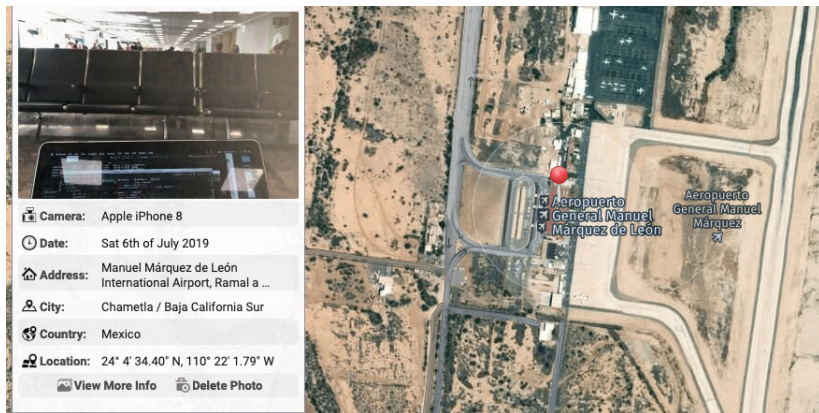


Figura 10: Ejemplo de una imagen con metadatos relacionados a una ubicación geográfica, mediante la herramienta [pic2map](#).

Reconocimiento de información en Internet (14/22)

Bases de datos WHOIS

- ▶ WHOIS es un protocolo TCP basado en petición/respuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet
- ▶ Las consultas WHOIS se han realizado tradicionalmente usando una interfaz de línea de comandos, pero actualmente existen multitud de páginas web que permiten realizar estas consultas

Reconocimiento de información en Internet (15/22)

The screenshot shows the 'who.is' website interface. At the top, there is a search bar with the text 'Search for domains or IP addresses.' and a magnifying glass icon. To the right of the search bar are links for 'Premium Domains', 'Transfer', 'Features', 'Login', and 'Sign Up'. Below the search bar, the text '207.237.157.11 address profile' is displayed. Underneath this, there are two tabs: 'Whois' (which is selected) and 'Diagnostics'. The main content area is titled 'IP Whois' and contains two sections of text. The first section provides technical details about the IP range, and the second section provides contact information for the organization.

who.is Search for domains or IP addresses. Premium Domains Transfer Features Login Sign Up

207.237.157.11 address profile

Whois Diagnostics

IP Whois

NetRange: 207.237.0.0 - 207.237.255.255
CIDR: 207.237.0.0/16
NetName: RCN-BLK-13
NetHandle: NET-207-237-0-0-1
Parent: NET207 (NET-207-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: RCN (RTSL-6)
RegDate: 1996-10-28
Updated: 2013-10-02
Ref: https://rdap.arin.net/registry/ip/207.237.0.0

Orgname: RCN
Orgid: RTSL-6
Address: 650 college road East
City: Princeton
StateProv: NJ
PostalCode: 08540
Country: US
RegDate: 2013-07-09
Updated: 2017-01-28
Comment: For all abuse issues, please contact abuse@rcn.com
Ref: https://rdap.arin.net/registry/entity/RTSL-6

Figura 11: Análisis de direcciones IP públicas mediante la herramienta [who.is](#).

Reconocimiento de información en Internet (16/22)

Componentes de un DNS

- ▶ **Clientes:** se ejecuta en la computadora del usuario y genera peticiones de resolución de nombres a un servidor DNS (Por ejemplo: *¿Qué dirección IP corresponde a nombre.dominio?*)
- ▶ **Los Servidores DNS:** contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada
- ▶ **Las Zonas de autoridad:** es una parte del espacio de nombre de dominios sobre la que es responsable un servidor DNS, que puede tener autoridad sobre varias zonas. (por ejemplo: *subdominio.wikipedia.org, subdominio.com, etc.*)

Reconocimiento de información en Internet (17/22)

A continuación se listan los tipos de registros DNS:

- ▶ **A Dirección (address)**: este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4
- ▶ **AAAA Dirección (address)**: este registro se usa en IPv6 para traducir nombres de hosts a direcciones IPv6
- ▶ **CNAME Nombre canónico (canonical Name)**: se usa para crear nombres de servidores de alojamiento adicionales, o alias como *ftp.ejemplo.com.* y *www.ejemplo.com.*
- ▶ **MX Intercambio de correo (mail exchange)**: asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. Tiene un balanceo de carga y prioridad para el uso de uno o más servicios de correo

Reconocimiento de información en Internet (18/22)

- ▶ **PTR Indicador (pointer)**: también conocido como *registro inverso*, funciona a la inversa del registro A, traduciendo IPs en nombres de dominio. Se usa en el archivo de configuración de la zona DNS inversa
- ▶ **SOA Autoridad de la zona (source of authority)**: proporciona información sobre el servidor DNS primario de la zona
- ▶ **NS Servidor de nombres (name server)**: define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio
- ▶ **TXT Registro de texto (text record)**: permite asignar texto arbitrario a un hostname

Reconocimiento de información en Internet (19/22)

oas.org
DNS information

Whois DNS Records Diagnostics

DNS Records for oas.org

Hostname	Type	TTL	Priority	Content
oas.org	SOA	3599		oasunix1.oas.org sysadmin@oasunix1.oas.org 2019062803 9600 1200 36000 1800
oas.org	NS	3599		auth1.dns.rcn.net
oas.org	NS	3599		auth2.dns.rcn.net
oas.org	NS	3599		auth3.dns.rcn.net
oas.org	NS	3599		auth4.dns.rcn.net
oas.org	NS	3599		oasunix1.oas.org
oas.org	NS	3599		oasunix2.oas.org
oas.org	A	1689		207.237.157.11
oas.org	MX	890	10	storkft2.oas.org
oas.org	MX	890	10	storkft1.oas.org
www.oas.org	A	3058		207.237.157.11

Figura 12: Análisis de registros DNS: <https://who.is/dns/oas.org>

Reconocimiento de información en Internet (20/22)

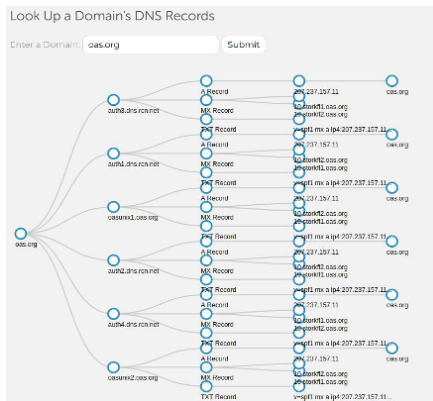


Figura 13: Jerarquía de registros DNS:

<https://tools.liquidweb.com/dns?domain=oas.org>

Transferencia de zona DNS

- ▶ Es un tipo de transacción DNS, utilizada para replicar bases de datos de registros DNS a través de un conjunto de servidores
- ▶ Se producirá una transferencia de zona en los siguientes escenarios:
 - ▶ *Al iniciar el servicio DNS en el servidor DNS secundario*
 - ▶ *Cuando caduca el tiempo de actualización*
 - ▶ *Cuando se guardan los cambios en el archivo de zona principal y hay una notificación lista*

Reconocimiento de información en Internet (22/22)

¡Un atacante puede explotar un servidor DNS no asegurado, para obtener la base de datos de los registros DNS!

(Observar el siguiente código).

```
$ dig axfr @nsztl1.digi.ninja zonetransfer.me
```

Lo anterior es denominado **DNS Zone Transfer Attack**

Geolocalización de direcciones IP (1/2)

- ▶ Existen métodos para deducir la geo-localización de un dispositivo conectado a Internet
- ▶ La identificación de un dispositivo se puede usar para determinar el país, la ciudad o región, el código postal y la ubicación geográfica de un objeto. Las fuentes de estas consultas son las *Regional Internet Registry (RIR)*, que son las organizaciones que administran la asignación de números en Internet globalmente (e.j.: *ARIN*, *LACNIC*).
- ▶ Otros métodos incluyen los metadatos de imagen o información de tarjetas de crédito

Geolocalización de direcciones IP (2/2)

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2019-3-1)

IP Address	Country	Region	City
207.237.157.11	United States 	New Jersey	Princeton
ISP	Organization	Latitude	Longitude
RCN	Not Available	40.3675	-74.6695

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
207.237.157.11	United States 	New Jersey	Princeton
ISP	Organization	Latitude	Longitude
Sidera Networks LLC	RCN Corporation (rcn.com)	40.3756	-74.6597

Geolocation data from [DB-IP](#) (Product: Full, 2019-3-2)

IP Address	Country	Region	City
207.237.157.11	United States 	Virginia	Ashburn
ISP	Organization	Latitude	Longitude
RCN	RCN Corporation	39.0161	-77.4594

Figura 14: Geo-localización de direcciones IP <https://www.iplocation.net>