Informe de Reconocimiento y Descubrimiento sobre ClassDojo:

➢ **Descripción de la Aplicación:** ClassDojo es una plataforma educativa que facilita la comunicación entre profesores, estudiantes y padres, promoviendo un entorno de aprendizaje positivo. La aplicación permite a los profesores gestionar el comportamiento en el aula, compartir informes de progreso y enviar mensajes a los padres. Los estudiantes pueden recibir puntos por comportamientos positivos, mientras que los padres pueden seguir el progreso y la participación de sus hijos en tiempo real. ClassDojo también ofrece la posibilidad de crear portafolios digitales donde los estudiantes pueden compartir su trabajo. La plataforma es ampliamente utilizada en escuelas de todo el mundo por su enfoque en la colaboración y el refuerzo positivo.

➢ **Sección para Personal Técnico:**

- ***Metodología y Herramientas usadas para obtener los resultados de Reconocimiento***
  - ***Dominios Identificados:*** Listado presente en el anexo 'domain.txt' en la carpeta 'Anexos' , fuentes:

    > En la pagina https://bugcrowd.com/engagements/classdojo ClassDojo dejo un listado de sus dominios incluyendo aplicaciones móviles (iOS y Android), varias interfaces web y APIs, alojadas principalmente en AWS(Amazon Web Services), por lo que la infraestructura y servicios para la aplicación o los datos están en la nube de Amazon, utilizando tecnologías como ReactJS, que se utiliza para construir y gestionar la interfaz de usuario de la aplicación web, Amazon S3, que se utiliza para almacenar y recuperar archivos en la nube de manera escalable y duradera, y otros servicios.

    > Además para explorar otros dominios y subdominios, y conocer más servicios que tiene ClassDojo:

    - Hice las siguientes búsquedas avanzadas en google (google dorks):
      - ➔ site:classdojo.com
      - ➔ site:classdojo.com -www.classdojo.com
      - ➔ site:classdojo.com -www.classdojo.com -engineering.classdojo.com
      - ➔ site:classdojo.com -www.classdojo.com -engineering.classdojo.com -blog.classdojo.com -tutor.classdojo.com -shop.classdojo.com -external.classdojo.com -www2.classdojo.com
      - ➔ site:classdojo.com -www.classdojo.com -engineering.classdojo.com -blog.classdojo.com -tutor.classdojo.com -shop.classdojo.com -external.classdojo.com -www2.classdojo.com -help.classdojo.com -static.classdojo.com -ideas.classdojo.com

      Obtuve más resultados detallados en el mismo anexo, como más dominios y subdominios, además de descubrir que Classdojo utiliza storybook para su biblioteca de componentes.

      Esto ayuda a tener una visión más completa de la infraestructura de ClassDojo y de los distintos servicios o funcionalidades que están disponibles.
    - Hice uso de la herramienta Sublist3r, herramienta que enumera subdominio de un dominio objetivo, ejecute en la vm, luego de realizar las instalaciones necesarias:
      - ➔ python3 /home/core/Sublist3r/sublist3r.py -d classdojo.com

      Encontró un total de 130 subdominios únicos para classdojo.com.

    > Conclusiones obtenidas a base de estos resultados:

    - Diversidad de Servicios: ClassDojo ofrece una amplia gama de servicios a través de sus diferentes subdominios, desde soporte y ayuda (help.classdojo.com) hasta servicios de tutoría (tutor.classdojo.com) y venta de productos (shop.classdojo.com), incluyendo ademas servicios para distribuir recursos educativos (static.classdojo.com para servir archivos estáticos), un asistente de inteligencia artificial(ai.classdojo.com) y una plataforma para recibir y votar ideas y sugerencias(ideas.classdojo.com).
    - Poseen ell subdominio security.classdojo.com que ofrece información sobre sus prácticas de seguridad y protocolos.
    - Tiene engineering.classdojo.com que es un blog técnico que proporciona información sobre las prácticas de desarrollo y tecnología usadas, donde documentan hallazgos e innovaciones.
    - Por otro lado usan servicios de Storybook, components.classdojo.com muestra que ClassDojo usa Storybook para gestionar su sistema de diseño, facilitando el desarrollo y la documentación de sus componentes de interfaz de usuario.

- Tienen alternativas y redundancia, como www2.classdojo.com está configurado como una alternativa al subdominio principal para manejar la carga o proporcionar redundancia.
- Con los subdominios dev.*.classdojo.com(desarrollo) y staging.*.classdojo.com (puesta en escena) podemos entender que mantiene entornos separados para desarrollo, pruebas y producción, lo cual es una buena práctica para la gestión de software.
- Subdominios como playcanvas.classdojo.com y realtime.classdojo.com sugieren la integración con herramientas y servicios externos, como PlayCanvas para desarrollo de juegos o aplicaciones interactivas, y sistemas de mensajería en tiempo real.
- Los subdominios como sentry.classdojo.com y icinga.classdojo.com sugieren el uso de herramientas de monitoreo y gestión de errores (Sentry) y monitoreo de infraestructura (Icinga), lo cual es crucial para la estabilidad y seguridad del servicio.
- Los subdominios como cdn.classdojo.com y api.classdojo.com sugieren que utiliza una infraestructura distribuida para el contenido y las APIs, lo que es indicativo de prácticas de escalabilidad y rendimiento.

- ***Dispositivos y Servicios Descubiertos:*** Listado presente en el anexo 'fqdn.txt' en la carpeta 'Anexos', fuentes:

  > Inicie haciendo una búsqueda en shodan (hostname:classdojo.com) para encontrar dispositivos directamente asociados, me dio un total de 16 resultados.

  Donde:

  - ➔ Servicios dados por las siguientes organizaciones: Amazon Data Services NoVa (9), Amazon Technologies Inc. (6), Amazon.com, Inc. (1) .
  - ➔ EL tipo de dispositivo parecen ser todos servidores web dado el código de respuesta HTTP 404 Not Found y la presencia de certificados SSL/TLS (Secure Sockets Layer/Transport Layer Security, protocolos de seguridad que se utilizan para cifrar la comunicación entre cliente y servidor cuyo objetivo principal es proteger los datos que se transmiten a través de la red para evitar que sean interceptados o manipulados por terceros).
  - ➔ Todas las IPs usan certificados SSL/TLS emitidos por Amazon con un rango de versiones soportadas de TLS, hay algunas áreas que podrían mejorarse, como desactivar versiones antiguas de TLS (v1 y v1.1).
  - ➔ El uso de HSTS (HTTP Strict Transport Security)se menciona en algunas respuestas (es un mecanismo de seguridad web que ayuda a proteger a los usuarios de ciertos tipos de ataques, le indica al navegador que solo se debe conectar a través de HTTPS y nunca permitir conexiones a través de HTTP), lo que es positivo desde un punto de vista de seguridad, ya que obliga a los navegadores a usar siempre conexiones HTTPS.
  - ➔ Se están utilizando dos tipos de servidores web: awselb/2.0 (AWS Elastic Load Balancer, es un servicio de Amazon Web Services que distribuye el tráfico de red o de aplicación entre varios servidores para garantizar que el sitio web o la aplicación puedan manejar altas cargas de tráfico de manera eficiente) y nginx (es un servidor web y proxy inverso con alto rendimiento y bajo consumo de recursos).
  - ➔ Todas las IPs comparten un certificado SSL emitido por Amazon RSA 2048 M02 o M03, y el destinatario del certificado es *.classdojo.com, esto muestra que se está utilizando un wildcard certificate (certificado comodín, '*'), lo que permite asegurar múltiples subdominios bajo classdojo.com.

  > Además hice una búsqueda en Censys que es otra poderosa herramienta de búsqueda para descubrir dispositivos en internet, obtuve 31 resultados en total, con 18 dispositivos nuevos no encontrados en la anterior, aplique el filtro que es para buscar dispositivos y servicios directamente asociados al dominio, limitándo a los certificados emitidos para dominios específicos :

  services.tls.certificates.leaf_data.subject.common_name: "*.classdojo.com"

  En los resultados obtenidos:

  - ➔ La mayoría de las IPs tienen puertos 80 (HTTP) y 443 (HTTPS) abiertos, lo que indica que estos servidores están configurados para alojar sitios web o servicios web.
  - ➔ La mayoría de las IPs están asociadas con instancias EC2 (Elastic Compute Cloud, permite a los usuarios alquilar máquinas virtuales (VMs) en la nube para ejecutar aplicaciones, sitios web, bases de datos y más) de AWS.
  - ➔ Estos resultados son consistentes con la información obtenida en la búsqueda inicial.

  > Por otro lado, como extra, utilice Nmap como herramienta para escanear la red e identificar dispositivos y servicios.

→ Realice un escaneo general e intensivo ejecutando en la vm con una VPN, Surfshark, activada como método de precaución ante un posible bloqueo:

nmap -p- -T4 -iL domains.txt -oN nmapRes.txt

Donde:

- ➔ -iL domains.txt: indica que la lista de dominios a escanear se encuentra en el archivo domains.txt (uno que prepare solo con los dominios), Nmap leerá cada línea de este archivo como una dirección de destino. (disponible en la carpeta "Datos extra")
- ➔ -oN nmapRes.txt: especifica que la salida del escaneo se guardará en un archivo llamado nmapRes.txt, lo que te permite revisar los resultados y conservar registro de lo escaneado. (disponible en la carpeta "Datos extra")
- ➔ -p- : especifica el rango de puertos a escanear es todos los puertos posibles (del 1 al 65535).
- ➔ -T4: ajusta el nivel de velocidad del escaneo. Los niveles de -T van de 0 a 5, donde -T4 es bastante rápido y adecuado para redes rápidas y sin restricciones. Los niveles más altos aumentan la velocidad del escaneo a costa de mayor probabilidad de ser detectado y mayor carga en la red.

> Conclusiones obtenidas en base al resultado del escaneo:

- Inicialmente hubo varias fallas al intentar resolver los subdominios, lo que significa que muchos de esos ya no están activos o no pueden ser resueltos. En los dominios que sí se resolvieron, los puertos 80 (HTTP) y 443 (HTTPS) están abiertos en la mayoría de los hosts, común en aplicaciones web como lo es esta, esto representa que solo tienen abiertos los puertos necesarios.
- El escaneo finalizó sin que hayan bloqueado la ip, considerando que se escaneo todos los puertos de forma T4, que es rápido aunque no agresivo, este aún puede ser detectado por sistemas de seguridad más avanzados y robustos, lo que no ocurrió en este caso una señal de que no está configurado de forma tan rigurosa para detectarlos.
- Por otro lado el dominio: segurity.classdojo.com tiene una gran cantidad de puertos abiertos, un total de 63.560, donde la mayoría tienen servicios unknown, osea que Nmap no pudo identificar el servicio que está escuchando en ese puerto.
- Como en-> rDNS record for 3.162.185.88: server-3-162-185-88.eze50.r.cloudfront.net, hay muchos más que muestran el uso de CloudFront CDN (Red de Distribución de Contenidos), al estar detrás de un CDN las IPs reales de los servidores de origen están ocultas, lo que dificulta los escaneos directos y los ataques a los servidores internos.
- Así también como en este caso: rDNS record for 54.159.194.171: ec2-54-159-194-171.compute-1.amazonaws.com la presencia de compute-1.amazonaws.com en el rDNS confirma que la IP pertenece a un servidor de Amazon Elastic Compute Cloud (EC2), EC2 es un servicio de Amazon Web Services (AWS) que proporciona instancias de servidores virtuales en la nube.

- ***Correo Electrónico:*** Listado presente en el anexo 'email.txt' en la carpeta 'Anexos', fuentes:

> Inicie haciendo las siguientes búsqueda avanzada en google:

- ➔ intext:@classdojo.com : diseñado para buscar páginas que contengan el texto @classdojo.com lo que podría permitirme encontrar direcciones de correo electrónico con ese dominio pero no obtuve resultados.
- ➔ filetype:txt intext:@classdojo.com : con esta búsqueda accedi a la pagina https://shop.classdojo.com/robots.txt, (disponible en el archivo robot.txt en la carpeta "Datos extra") este se usa para definir reglas para los bots de motores de búsqueda sobre cómo deben interactuar con el sitio web, es muy común en las plataformas web para definir qué partes del sitio están permitidas o restringidas para ser rastreadas; en este archivo específico, se listan varias rutas y parámetros que los bots no deben rastrear o indexar. Asi tambien encontre varias paginas mas que parecen ser de configuración para bloques de anuncios o lista de bloqueo DNS pero nada de mails.
- ➔ site:classdojo.com intext:@classdojo.com : con esta búsqueda puede acceder al mail de contacto de classdojo en el sitio https://www.classdojo.com/es-es/contact/?redirect=true y al mail para hacer consultas sobre las políticas de privacidad obtenido en esta pagina https://www.classdojo.com/es-es/privacy?redirect=true, luego en varios sitios más se repiten los mismos dos mails (como https://www.facebook.com/classdojo).
- ➔ intext:"@classdojo.com" -intitle:"@classdojo.com", no obtuve resultados nuevos.

> Para obtener más información pase a realizar búsquedas en TheHarvester, que es una herramienta que se utiliza para recolectar correos electrónicos, subdominios, direcciones IP y nombres de empleados de diferentes fuentes públicas, la utilice en una vm de kali-linux ejecutando el comando:

➔ theHarvester -d example.com -b all, con este obtuve un total de 6 mails, 5 nuevos.

Donde: -d classdojo.com especifica el dominio en el que deseas buscar, -b all busca en todos los motores de búsqueda disponibles en The Harvester.

→ Como los correos electrónicos '0_10_@classdojo.com y '@classdojo.com parecen poco convencionales y podrían no ser válidos los verifique en https://www.verifyemailaddress.org/ donde se indican que parece ser que no existen, estos correos podrían ser errores en la recolección de datos o el resultado de un mal formato en las búsquedas de theHarvester.

> Continúe mi búsqueda con Recon-ng: ejecute los siguientes comandos en la máquina virtual de kali-linux, los resultados de las búsquedas se pueden observar en el archivo 'mail-recon-ng.txt' en la carpeta 'Datos extra' :

➔ Inicialmente probé con el módulo recon/companies-contacts/pen y no obtuve resultados.
➔ Continúe probando con el módulo recon/domains-contacts/whois_pocs con el cual tampoco obtuve resultados
➔ Continúe probando el módulo recon/companies-multi/whois_miner que tampoco obtuvo resultados.
➔ Continúe probando el módulo recon/companies-domains/pen que no obtuvo resultados.
➔ Continúe probando el módulo recon/domains-contacts/pgp_search que no obtuvo resultados.
➔ Continúe probando el módulo recon/domains-contacts/wikileaker, dio dos páginas como resultado las cuales analice con VirusTotal antes de abrirlas, no tenian nada sobre mails: https://search.wikileaks.org/?query=&exact_phrase=classdojo&include_external_sources=True&order_by=newest_document_date&page=1
➔ Continúe probando el módulo recon/profiles-contacts/dev_diver no encontró mails.

> Conclusiones obtenidas en base a los resultados:

- Dado los resultados obtenidos con las búsquedas avanzadas puedo suponer que ClassDojo no tiene correos electrónicos filtrados en documentos accesibles públicamente más allá de las páginas de contacto y políticas de privacidad que están bien organizados y disponibles en secciones específicas de sus sitios, sin aparentes filtraciones adicionales en documentos de texto públicos.
- Dados los resultados obtenidos con theHarvester pareciera que ClassDojo puede tener configuraciones de privacidad que limitan la exposición de los correos electrónicos.
- Con Recon-ng no pude agregar información útil, parece consistente con la prolijidad con la que manejan sus contactos hasta el momento.
- Los correos electrónicos encontrados incluyen direcciones generales y específicas para contacto con ClassDojo.

- ***Usuarios:*** Listado de nombres de usuario incluidos en el anexo 'username.txt' en la carpeta 'Anexos'.

> Inicie sacando los posibles nombres de usuarios de los mails válidos que encuentre.

> Comencé haciendo búsquedas avanzadas en google:

➔ site:classdojo.com intext:username ->el resultado de la búsqueda son múltiples páginas con archivos PDF que contienen datos con respecto a cómo realizar registros para poder acceder a las clases o PDF que explican el uso del entorno; en estos documentos se menciona la palabra "username", pero no se encontraron nombres de usuario específicos ni información adicional que permita identificar usuarios individuales.
➔ site:classdojo.com filetype:txt intext:username ->esta no arrojó resultados.

> Continue haciendo búsquedas en theHarvester en una máquina virtual de linux ejecute:

➔ theHarvester -d classdojo.com -b all
- No obtuve ningún nombre de usuario como resultado, almacene en este caso el resultado ligeramente diferente de la búsqueda en el archivo 'theHarvester.txt' en la carpeta Datos extra.

> Continue haciendo búsquedas en shodan con la idea de que los nombres de usuario pueden aparecer en los banners de ciertos servicios, como FTP, Telnet, o SMTP, probe buscando esto, y diversas combinaciones:

- ➔ hostname:"classdojo.com" port:21,990,25,465,587,23 "username"
- ➔ hostname:"classdojo.com" port:21,990,25,465,587,23
- ➔ hostname:"classdojo.com" port:21
- ➔ hostname:"classdojo.com" port:990 …. y así con cada puerto
- ➔ Sin resultados obtenidos, lo que es consistente con los resultados obtenidos en la búsqueda anterior.

Donde: - port:21,990 son puertos para FTP (21 para FTP estándar y 990 sobre TLS)

- port:25,465,587 son puertos para SMTP (25 para SMTP estándar, 465 sobre SSL, y 587 sobre TLS),
- port:23: es el puerto para Telnet,
- además hostname:"classdojo.com" limita la búsqueda a servidores relacionados con el dominio classdojo.com
- y "username" busca en los banners o respuestas de los servidores que puedan contener la palabra "username", también probé con la palabra "login" y "password".

> Mi siguiente paso fue utilizar recon-ng usando módulos para consultar contacts, los resultados de las búsquedas se pueden observar en el archivo 'username-recon-ng.txt' en la carpeta 'Datos extra', ya hice búsquedas con varios modules de contacts para buscar mails y no obtuve nombres de usuarios pero me quedo este por probar:

- ➔ Utilice el módulo recon/profiles-contacts/github_users (para este tuve que configurar una clave desde github.com), obtuvo contacto como resultado con el nombre 'ClassDojo'.

> Busque repositorios públicos relacionados con ClassDojo que puedan tener nombres de usuarios en sus commits o archivos:

- ➔ Con una búsqueda avanzada en google: site:github.com "classdojo" "username"

  - Encontre archivos en git sobre políticas de privacidad, seguridad, términos, manejo de cookies y condiciones en cada una de sus versiones.

  - Encontre una lista que reconoce a usuarios que colaboraron en chequia en la pagina https://github.com/gayanvoice/top-github-users/blob/main/markdown/public_contributions/czechia.md donde se hace mension a una persona que tiene el tag @classdojo en la seccion de 'empresa', al entrar en su perfil de git aparece como empleado asociado a classdojo, en sus seguidores aparece otro usuario que tambien figuran como empleado de classdojo, incluyó como posibles nombres de usuarios sus nombres, sus apodos, y el nombre de su pagina web de donde saque el instagram y el linkeding.

  - Encontré reportes de errores y correcciones de bugs, estructuras HTML que incluyen 'classdojo'

  - Aparece otro usuario de git que tiene registrado que trabaja en classdojo, como antes, en sus seguidos/seguidores hay otro usuario, en el cual se siguen con otro más.

  - También hay varios archivos para administrar configuraciones sobre distintos dominios en los que aparece classdojo.com.

> Además realice una búsqueda en la aplicación linkedin buscando directamente información sobre la empresa.

- ➔ Busque en la sección de Personas, encontré 801 usuarios asociados, como resultado un total de 113 nombre, todos diferentes a los encontrados por git (me crucé con un par de los mismos usuarios pero su perfil y nombre no eran accesibles), los demás aparecen como Miembro de Linkedin o eran personas que no estaban directamente asociadas con ClassDojo.

> Finalmente busque en la página de class dojo:

- ➔ En la parte de Engineering encontré 3 aportes que hicieron 3 personas, de los cuales 2 se tenían adjunto sus usuario de git del cual pude sacar mas datos nombres, y en el área de centro de privacidad encontre a 4 personas más.

> Conclusiones obtenidas en base a los resultados:

- Es posible que los nombres de usuario no estén disponibles públicamente o que ClassDojo haya implementado medidas de seguridad sólidas para proteger esta información.

- Es posible que la información de nombres de usuario esté protegida por medidas que previenen la exposición en los banners (información que un servicio revela en la respuesta inicial cuando alguien se conecta a él) de los servidores, como ocultando los servicios que suelen tener información de los nombres de usuarios para que no estén expuestos en internet o estén protegidos detrás de un firewall u otro sistema de protección.
- La ausencia de nombres de usuario específicos en las búsquedas indican que ClassDojo ha implementado medidas de seguridad para proteger esta información.

- ***Trabajadores más importantes de la organización:***: El listado de los 5 trabajadores más importantes para la organización (en base a su jerarquía dentro de la organización) incluidos en el anexo 'people.txt' en la carpeta 'Anexos'.

  > Comencé buscando un organigrama o un indicio que me permita identificar a los trabajadores más importantes dentro de ClassDojo, realizando las siguientes búsquedas.

  - ➔ En la página oficial de ClassDojo investigue en el área Empresa 'Sobre nosotros', 'Prensa', 'Ingenieria', donde hay información de el propósito y la motivación de ClassDojo, testimonios sobre padres, madres y usuarios de la aplicación, además algunos comentarios sobre nuevos empleados.
  - ➔ En las redes sociales Instagram, Twitter(así figura en su web), Facebook, en todos lados se encuentran testimonios sobre docentes, directores y alumnos que comentan cómo es usar classdojo y diversas formas similares de promoción.
  - ➔ En Linkedin en la sección de publicaciones y personas no obtuve indicios claros que destacarán la jerarquía dentro de la organización.

  > Pase a buscar empleados basándose en la jerarquía común de las empresas de desarrollo de software para identificar a los trabajadores más importantes de ClassDojo, muchas organizaciones de tecnología suelen tener una estructura basada en roles ejecutivos clave, que comienzan con la letra "C" , comence a buscar empleados con títulos como: CEO (La persona que dirige la empresa), CTO (responsable de la estrategia tecnológica de la empresa), COO (encargado de las operaciones diarias de la empresa), CFO (responsable de las finanzas de la empresa), CPO (encargado de la estrategia del producto), CMO (supervisa el departamento de marketing) , CIO(Director de sistemas de información) y otros.

  - ➔ En la página de la empresa, en el área de "Centro de Privacidad" (https://www.classdojo.com/es-es/privacycenter/), que ya visitamos antes, aparece la mención de la actual CPO.
  - ➔ En linkedin en el área de personas, en el recorrido previo: encontré al CEO, al CFO.
  - ➔ Con búsquedas avanzadas en google:

    -> con "ClassDojo" "CTO" encontré al CTO

    Sin embargo con las siguientes no hubo resultado, buscando en varios roles:

    ->"ClassDojo" "COO"->site:linkedin.com "COO" "ClassDojo"->site:classdojo.com "COO" ->"ClassDojo" "CIO" ->site:linkedin.com "CiO" "ClassDojo"

    ->site:crunchbase.com "CMO" "ClassDojo" -> site:theorg.com "CMO" "ClassDojo" (crunchbase.com y theorg.com son bases de datos donde muchas empresas tecnológicas registran a sus ejecutivos clave)->site:linkedin.com "CMO" "ClassDojo"

    Con combinaciones como las anteriores con los siguientes->"CHRO" "ClassDojo" ->"CCO" "ClassDojo" ->"CSO" "ClassDojo"
  - ➔ Como no obtuve resultados con estos roles específicos busque al co-fundador que dice ser el presidente de classDojo en linkedin y en artículos, el otro co-fundador es el CEO.

  > Conclusiones obtenidas en base a los resultados:

  - Aunque no encontrara un organigrama detallado ClassDojo parece seguir un esquema tradicional de empresa de tecnología, con un CEO, TCO, CTO Y CPO aunque no pude encontrar otro, logue identificar al cofundador (Liam Don) que en colaboración con el CEO (Sam Chaudhary) fundaron la empresa © ClassDojo, Inc.
  - Los roles no eran fáciles de rastrear y estaban distribuidos entre los demás empleados.

- ***Contactos para reportes:*** Contactos para realizar reportes a la organización, los datos de contacto y el medio se encuentran incluidos en el anexo 'reports.txt'.

  > Comencé consultando información con con whois del dominio TLD classdojo.com, para identificar quién gestiona el dominio:

  - ➔ whois classdojo.com → me dio como resultado información acerca del dominio (nombre, ubicación, el id del registro, fecha de creación, actualización y vencimiento), además de

un listado de los servidores de nombres (donde volvemos a ver que hace uso de AWS (Amazon Web Services) para su infraestructura de DNS).

Además en la sección 'Registrar ..' podemos destacar información sobre la empresa que registró el dominio, incluyendo así los datos de contacto asociados a la gestión del dominio.

> Continue consultando en whois por la dirección ip de classdojo, para identificar quién gestiona los bloques ip.

- ➔ primero hice una consulta con dig al dominio luego hice whois con una de las ip resultantes, ejecute dig classdojo.com luego whois 18.65.48.58

  Como resultado obtuve información sobre la organización que gestiona los bloques de ip, que es Amazon Technologies Inc., además aparecen contactos adicionales para Amazon con roles técnicos y organizacionales.
- ➔ Recurrí al archivo 'nmapRes.txt' (en Datos extras) donde verifica lo obtenido y además indica que classdojo tiene bloques ip gestionados por Cloudflare Inc, por lo que consulte agregue el contacto.

> Finalmente para concluir con la búsqueda decidí buscar información de la organización en bgp para consultar sobre el AS (Sistema Autónomo) y rdap, en los resultado confirman la información ya obtenida, agregando información sobre los servidores de mails, DNS, TXT records y bloques ip.

- ➔ https://bgp.he.net/dns/classdojo.com#_dns
- ➔ https://client.rdap.org/?type=domain&object=Classdojo.com

> Conclusiones obtenidas en base a los resultados:

- ClassDojo está registrado bajo el dominio classdojo.com el es gestionado por MESH DIGITAL LIMITED, empresa que es responsable del registro y administración del dominio incluyendo aspectos como la renovación y la actualización de los registros DNS.
- La infraestructura (conjunto de recursos y componentes necesarios para el funcionamiento y soporte de sistemas, aplicaciones y servicios) de DNS está alojada en Amazon Web Services y en Cloudflare Inc., osea que algunos de los registros DNS están gestionados a través de la infraestructura en la nube de Amazon y otros bloques IP también están gestionados por Cloudflare Inc., lo que puede indicar que ClassDojo utiliza servicios de Cloudflare para mejorar el rendimiento y la seguridad de su infraestructura web.

- ***Software:*** Los productos de software utilizados por la organización se encuentran incluidos en el Anexo 'software.txt'.

  > Comencé haciendo un nmap para identificar sistemas operativos en la lista de dominios asociados a la organización antes usada (ubicada en la carpeta 'Datos Extra' con el nombre 'domains.txt') ya que puede descubrir el sistema operativo en base a las respuestas a distintos paquetes (TCP, UDP, ICMP, etc). Durante el proceso algunos dominios no pudieron ser resueltos, lo que puede deberse a que ya estén inactivos o sus registros caducados (la lista contiene todos los dominios encontrados que se asocian con classdojo).

  - ➔ Para llevar a cabo el escaneo ejecute en la consola de la máquina virtual con la VPN (surfshark) activada (softNmap.txt se incluye en Datos extra):

    sudo nmap -iL ./…/domains.txt -O -oN ./…/softNmap.txt

  Así obtuve información acerca de los sistemas operativos que nmap pudo identificar, de los dominios en la lista, con un alto porcentaje de probabilidades de que todos usen Oracle VirtualBox y QEMU.

  > Conclusiones obtenidas en base a los resultados:

  - Por un lado, la detección de Oracle VirtualBox indica que ClassDojo está usando máquinas virtuales para sus servidores.
  - Por otro lado, QEMU (Quick Emulator) es una herramienta de virtualización y emulación de hardware usado para ejecutar SO invitados en una máquina virtual, es flexible y capaz de emular una amplia gama de arquitecturas de hardware.
  - El uso de máquinas virtuales puede proporcionar una capa adicional de seguridad y flexibilidad, pero también requiere una gestión y monitoreo adecuados para mantener sus virtudes ya que las máquinas virtuales pueden estar sujetas a vulnerabilidades específicas relacionadas con la virtualización.

- ***Leaks:*** Listado de fuentes donde se encontró información leakeada de la organización se encuentra en el archivo leaks.txt.

  > Inicie el proceso haciendo las siguientes búsquedas avanzadas en google.

  - ➔ site:classdojo.com filetype:pdf OR filetype:doc OR filetype:xls OR filetype:csv → (csv, Comma-Separated Values, es un formato de archivo de texto usado para almacenar datos en una tabla, .xls es un archivo de Microsoft Excel), con la intención de encontrar como resultado datos sensibles en formatos comunes, obtuve múltiples archivos PDF públicos que se suben a classdojo para organizar clases o informar sobre actividades.
  - ➔ site:classdojo.com OR filetype:doc OR filetype:xls OR filetype:csv→ como resultado obtuve un archivo DOC publico en el que informaba sobre el uso de classdojo en las aulas y solicitar los mails de los padres.
  - ➔ site:classdojo.com inurl:backup OR inurl:old OR inurl:confidential→ con la intención de buscar versiones antiguas de sistemas o documentos marcados como confidenciales pero no obtuve ningún resultado.
  - ➔ site:github.com "classdojo" password OR api_key OR token → para encontrar posibles credenciales expuestas en github, como resultado obtuve varios repositorios que he visitado con anterioridad, en los demás tenía esas palabras como nombres de variables o se hablaba de el tema, por la cantidad se puede deducir que github es un recurso muy utilizado.
  - ➔ site:pastebin.com "classdojo.com" OR "classdojo" → con la intencion de ver si se subio algo de la organización en pastebin que es un sitio donde se comparten datos filtrados, dio como resultado una filtración de lo que parece credenciales, pero cuando entras sale que la información ha sido eliminada, debe haber estado disponible en 2018.
  - ➔ site:reddit.com intext:"classdojo" leak OR dump OR database→ para buscar en foros donde se discuten filtraciones de datos, encontré foros con personas hablando de su experiencia con la aplicación y datos triviales pero no leaks.
  - ➔ site:forum.com intext:"classdojo" leak OR dump OR database→ para buscar en foros donde se discuten filtraciones de datos, con este no obtuve ningún resultado.

  > Busque directamente en pastebin.com, es una plataforma para compartir textos y documentos y se usa a menudo para publicar datos filtrados o información confidencial, busque para classdojo y classdojo.com.

  - ➔ Encontró un archivo donde hay un mail de Classdojo, después otros archivos que tienen un dominio de classdojo y parte de un HTML.
  - ➔ Encontró un archivo con datos relacionados con la verificación de un correo de alguien dentro de la organización de Classdojo.

  > Busque en DeHashed que es una herramienta de búsqueda y análisis de datos de brechas de seguridad y filtraciones de datos, en esta busque con el dominio de classdojo y classdojo.com

  - ➔ Encontró 72 y 128 resultados, respectivamente, que coinciden con los dominios, aunque no pude acceder a los datos ya que figuraban como no disponibles, deben haber sido eliminados ya que dehashed tiene la opción de "solicitar eliminación de entrada" para proteger los datos.

  > Busque en Have I Been Pwned y Breach Directory que buscan información en bases de datos filtradas por emails con los emails que encontré con anterioridad.

  - ➔ hello@classdojo.com y parents@classdojo.com en Have I Been Pwned indican que quizás podría estar filtrada la contraseña, de las demás no se ha encontrado nada.
  - ➔ en Breach Directory dio como resultado que no se encontró filtración.

  > Conclusiones obtenidas en base a los resultados:

  - En las búsquedas en Google Dorks no revelaron información sensible o crítica ni confidencial en los formatos de archivo comunes.
  - Además no se encontraron credenciales expuestas directamente en repositorios de GitHub, aunque hubo menciones a variables relacionadas con credenciales además de reportes de bugs ya solucionados, lo que puede indicar la necesidad de mayor precaución en el uso de estos recursos.
  - Por otro lado se encontraron archivos antiguos en Pastebin que ya se encuentran eliminados lo que significa que en algún momento pudo haber filtraciones.
  - Los resultados en DeHashed y Have I Been Pwned indican que las direcciones de correo electrónico asociadas con ClassDojo no parecen estar comprometidas actualmente,

aunque algunos correos en Have I Been Pwned podrían haber estado asociados con contraseñas filtradas en el pasado.

- Finalmente no se encontraron foros ni archivos PDF o de otro formato con datos sensibles.

- ***Bloques IP y Proveedores de servicios:*** Listado de bloques IP utilizados por la organización el el archivo 'ip_blocks.txt' y lista de proveedores de tecnologías incluidos en el archivo 'providers.txt'.

  > Voy a utilizar el listado de direcciones IP que obtuve de TheHarvester para identificar los bloques IP utilizados por la organización.

  - ➔ Como resultado encontré 312 direcciones asociadas, el resultado las muestra ordenadas en conjuntos de direcciones que pertenecen al mismo bloque, voy a hacer consultas en una VM de Kali para conocer los bloques ip de estas.
  - ➔ En el documento 'block_whois.txt' en 'Datos extra' se encuentran los resultados de las consultas.

  > Además decidí verificar que en la información encontrada estén incluidos los bloques encontrados con anterioridad en https://bgp.he.net/dns/classdojo.com#_dns y así fue.

  > Con toda la información que fui recopilando pude identificar a los proveedores de servicios de Classdojo.

  > Conclusiones obtenidas en base a los resultados:

  - La mayoría de las direcciones están asociadas con Amazon Web Services utilizando diversas regiones.
  - Por otro lado varios bloques corresponden a Cloudflare lo que indica que Classdojo está utilizando sus servicios para protección de sitios web y optimización de rendimiento mediante CDN (Redes de Distribución de Contenidos).
  - Además se observan bloques de Vercel y Fly.io lo que refleja que Classdojo utiliza múltiples plataformas para desplegar diferentes aplicaciones y microservicios.
  - El hecho de que sean tantos bloques y algunos muy grandes sugiere que está preparada para manejar gran cantidad de tráfico y usuarios, que se diseñó para escalar según sea necesario.

- ***Servidores de correo electrónico:*** Listado de servidores de correo electrónico en el anexo ip_addresses_mail.txt.

  > En la busqueda en dgp https://bgp.he.net/dns/classdojo.com#_dns, obtuvimos como resultado 5 servidores de mails con distintas prioridades y dirección ip. Para verificarlo hice una consulta dig a classdojo.com (dig MX classdojo.com) que dio los mismos resultados, y consulte además las direcciones para ver si la información está actualizada, los resultados se encuentran disponibles en la carpeta 'Datos extra' en el documento dig_mails.txt.

  - ➔ Class dojo tiene 5 servidores de emails (SMTP) con distintas prioridades para distribuir la carga de la forma que consideran más conveniente, en la página bgp los nombres de los servidores son correctos, al igual que sus prioridades, pero sus direcciones ip están desactualizadas.

  > Conclusiones obtenidas en base a los resultados:

  - Classdojo usa servicios de Google para gestionar sus correos electrónicos, lo cual asegura la fiabilidad y seguridad ya que google es una empresa con muchos años de desarrollo y buena fama.
  - La organización de los servidores permite realizar una buena distribución de carga mejorando así la eficiencia de entrega de correos, y tienen varias opciones en caso de que alguno falle.
  - Todos los servidores tienen tanto ipv4 como ipv6 lo que indica que están preparados para manejar ipv6.
  - Que las direcciones ip estén desactualizadas en dgp puede significar que Classdojo cambia regularmente las ip en periodos menores a los que dgo actualiza sus datos.

- ***Servidores de Nombres de Dominio:*** Listado de servidores DNS presente en el anexo ip_addresses_dns.txt.

  > En la busqueda en dgp https://bgp.he.net/dns/classdojo.com#_dns obtuvimos como resultado 4 servidores de nombres con sus dirección ip. Para verificarlo hice una consulta dig a classdojo.com (dig NS classdojo.com) que dio los mismos resultados, y consulte

además las direcciones para ver si la información está actualizada, los resultados de las consultas se encuentran disponibles en la carpeta 'Datos extra' en el documento dig_dns.txt.

➔ Los datos obtenidos están actualizados en dpg y son consistentes.

> Intente hacer una transferencia de zona con dig sobre cada DNS (dig AXFR NomServdns classdojo.com) los resultados se encuentran en una sección ('transferencia de Zona') al final del archivo dig_dns.txt.

➔ La transferencia de zona no fue posible lo que es se debe a que está bien configurado ya que solo debes permitírselo a los servidores secundarios autorizados.

> Conclusiones obtenidas en base a los resultados:

- Classdojo tiene servidores DNS distribuidos en diferentes dominios (.org, .net,.com, .co.uk), esto significa que configuraron su infraestructura de nombres de dominio para que haya redundancia y escalabilidad global (capacidad para manejar un aumento en la carga de trabajo o el número de solicitudes), esto permite que los usuarios de varias partes del mundo puedan acceder a los servidores de Classdojo de manera eficiente.
- Todos los servidores pertenecen a AWS, osea que utilizas AWS para gestionar el enrutamiento de sus nombres de dominio.
- Que la transferencia de zona no sea exitosa es una buena práctica de seguridad ya que evita que la exposición de todos los registros DNS sean expuestos a zonas no autorizadas.
- Nuevamente tienen direcciones en ipv4 y en ipv6 esto significa que están preparados para manejar tráfico en ambas versiones del protocolo de internet.

- ***Servidores webs:*** Listado de servidores Webs presente en el anexo ip_addresses_www.txt.

> Hice una consulta dig a classdojo.com (dig A classdojo.com) que dio los 4 servidores webs de classdojo, los resultados de la consultas se encuentran disponibles en la carpeta 'Datos extra' en el documento dig_curl_www.txt.

➔ Realice, además, consultas curl para solicitar las cabecera HTTP(-I), sobre cada servidor web, para poder conocer información adicional (curl -I dirIPServWeb), los resultados de las consultas se encuentran en el documento dig_curl_www.txt.

➔ Los resultados de las consultas curl indican que ClassDojo utiliza CloudFront.

➔ Los servidores responden 403 Forbidden, que significa que detectó que no tengo permisos para acceder directamente a estas ips, que tienen acceso restringido, esto es parte de las configuraciones de CloudFront pues CDN es como una capa de seguridad y caché entre los usuarios y los servidores de origen.

> Conclusiones obtenidas en base a los resultados:

- Classdojo utiliza CloudFront para sus servidores webs, un servicio de red de entrega de contenido (CDN) proporcionado por Amazon Web Services (AWS), proporciona escalabilidad y redundancia para manejar grandes volúmenes de datos.
- Las solicitudes no autorizadas no llegan a los servidores web reales, lo que ayuda a proteger los servidores de origen contra accesos no deseados y posibles ataques.
- Sus configuraciones son prolijas y seguras, la configuración de CloudFront y el uso de un CDN demuestran una gestión adecuada para garantizar un rendimiento óptimo y una buena capa de protección.

- ***Otros servidores:*** Listado otros servidores presente en el anexo ip_addresse_srv.txt, el cual está vacío.

> Hice una consulta dig a classdojo.com (dig SRV classdojo.com), sobre el registro SRV (Service) que puedan estar asociados con otros servicios, en este caso no fue así y no obtuve resultado.

> Continué haciendo una consulta por censys (también la había realizado por shodan pero parece no estar funcionando), obtuve como resultado solo servidores HTTP encontrados con anterioridad, información que se encuentran en el anexo fqdn.txt.

→No se identificaron otros tipos de servidores (más allá de HTTP) en los registros SRV ni en la búsqueda en Censys. Esto sugiere que ClassDojo no está utilizando registros SRV para servicios adicionales en su configuración DNS y que parece no tener servidores de otros tipos a los ya encontrados.

- ***Analisis de puertos y servicios en direcciones IP:*** Listado de de puertos abiertos para las direcciones de los servidores de mails, DNS y los webs encontrados, por cada puertos abiertos se detalla protocolo, servicio y la versión del servicio que está corriendo en el mismo, esta información se encuentra en el anexo de nombre ip_addresses_A_B_C_D.txt.

  > Realice un Nmap, donde recorre el archivo 'direcc_analizadas.txt' con una lista de als direcciones a analizar, disponible en la carpeta 'Datos extras', toma una a una las direcciones ,escanea sus puertos (de 1-65535) y realiza en análisis del servicio(-sV), luego guarda los resultados en el documento 'nmap_results.txt' (también disponible en la carpeta 'Datos extras') para analizar los resultados. Este proceso lo realice con la VPN activada.

  ➔ Ejecute: nmap -sV -p- -iL ../direcc_analizadas.txt -oN ../nmap_results.txt
  ➔ Donde: -sV= detecta versiones de servicios, -p-= escanea todos los puertos (1-65535), -iL direcc_analizadas.txt= lee las direcciones IP desde el archivo direcc_analizadas.txt, -oN nmap_results.txt= guarda los resultados en el archivo nmap_results.txt.

  > Conclusiones obtenidas en base a los resultados:

  - Todos los servidores tienen el puerto 35 abierto y están ejecutando puerto DNS usando ISC BIND que es uno de los servidores DNS más populares.
  - Los puertos 80 (HTTP) y 443 (HTTPS) estan abiertos en la mayoría de los servidores, en los que están asociados a CloudFront (usado para la entrega de contenido y gestión de tráfico) están claramente identificados con la versión Amazon CloudFront httpd (indicando que forman parte de la infraestructura de distribución de contenido (CDN)), en otros servidores HTTP y HTTPS no tiene una versión clara.
  - En la mayoría está abierto el puerto 5060 asociado con SIP, el protocolo de inicio de sesión, usado para establecer, mantener y finalizar llamadas de voz y videos sobre IP, esto indica que soporta servicios VoIP o una infraestructura de comunicación.
  - Los servicios en los puertos 5060, 8080 y algunos servidores de HTTP y HTTPS no tienen una versión clara, lo cual es una señal de que podrían haber sido configurados de manera deliberada para no exponer información innecesaria como una medida de seguridad, o puede ser una señal de servicios mal configurados o sin mantenimiento.

■ ***Conclusiones finales - con un resumen de todos los hallazgos :***

- Se puede decir que ClassDojo tiene una base sólida para mantener y gestionar sus dominios debido a la infraestructura y los servicios que utiliza ya que la combinación de diferentes tecnologías y servicios, como AWS, ReactJS, Amazon S3, y otras, permite a ClassDojo ofrecer una infraestructura robusta y flexible que puede adaptarse a las necesidades cambiantes de la aplicación y de los usuarios, está bien preparado para manejar el rendimiento, la escalabilidad, la durabilidad y la seguridad de sus aplicaciones.
- Hace uso de Storybook para desarrollar, documentar y probar los componentes de la interfaz de usuario (UI) de manera aislada, lo que facilita la creación y el mantenimiento de la UI, este en sí mismo no tiene implicaciones directas de seguridad más allá de cómo se configura y se utiliza en un entorno específico (https://components.classdojo.com//?path=/docs/dojo-design-system--docs evidencia su uso, https://storybook.js.org/ es el sitio de la organización).
- El uso de Amazon EC2 (Elastic Compute Cloud) de Amazon Web Services (AWS) tiene varias implicaciones positivas y beneficios, Amazon EC2 proporciona varias capas de seguridad, incluyendo grupos de seguridad, redes privadas virtuales (VPC), y opciones de cifrado. Se puede personalizar la configuración de seguridad para proteger instancias, en general, Amazon EC2 es una solución poderosa y flexible para la computación en la nube, ideal para una amplia variedad de aplicaciones y casos de uso.
- La infraestructura de ClassDojo está bien organizada y asegurada con certificados SSL (Secure Sockets Layer, Capa de Conexión Segura) y HSTS (Strict Transport Security-Seguridad, obliga a los navegadores a utilizar solo conexiones HTTPS), ya que todas las IPs encontradas en shodan y censys, de los dispositivos que están conectados a internet soportan alguna versión de TLS(Transport Layer Security, Seguridad de la Capa de Transporte) que es un protocolo de seguridad (protocolo criptográfico) que se utiliza para cifrar y proteger las comunicaciones a través de redes, su objetivo principal es garantizar la confidencialidad, la integridad y la autenticidad de los datos transmitidos entre dos partes, por ejemplo, aunque se recomienda desactivar las versiones más antiguas y obsoletas (TLS 1.0 y 1.1) para fortalecer la seguridad.
- Utilizar un CDN como CloudFront ayuda a mejorar el rendimiento y la seguridad, al distribuir el contenido a través de una red global de servidores y proteger contra ataques como DDoS (de denegación de servicio distribuida), Amazon CloudFront es un servicio de Content Delivery

Network (CDN), proporcionado por Amazon Web Services (AWS), es una infraestructura de servidores distribuidos que trabajan juntos para entregar contenido web (como archivos multimedia, aplicaciones web, archivos estáticos, entre otros) de manera rápida, segura y eficiente a los usuarios finales.

- Classdojo parece no está configurada de forma precisa para detectar escaneo de todos los puertos, acción que previene que alguien realice un escaneo intensivo y pueda conocer alguna vulnerabilidad, la configuración de un sistema para manejar escaneos de puertos y prevenir que se realizan escaneos exhaustivos es crucial para mantener la seguridad y prevenir amenazas.
- El que el dominio security.classdojo.com/ tenga tantos puertos abiertos, del 1 al 65.535 con 1975 que podrían estar cerrados, es una señal de que puede estar configurado de manera insegura o mal gestionada, lo que potencialmente lo deja vulnerable a ataques. Es poco común que tantos puertos estén abiertos a propósito. Lo ideal es que solo los puertos necesarios para las operaciones de la aplicación o del servicio estén abiertos, mientras que los demás deberían estar cerrados o filtrados.
- Classdojo cuenta con un archivo robot.txt que es una buena práctica en la gestión de sitios web, esto puedes evitar que ciertos bots y rastreadores accedan a áreas del sitio que contienen información sensible o privada, aunque no garantiza la seguridad completa puede reducir el riesgo de exposición no intencional, tener un archivo robot.txt bien configurado es recomendado para la administración de sitios web, ya que ayuda a controlar el rastreo y la indexación del contenido permitiendo configurar los sitios que se desean que aparezcan o no en las búsquedas según convenga.
- Con respecto a sus documentos públicos y páginas de contacto, los correos electrónicos disponibles están bien organizados en las secciones de contacto y políticas de privacidad en el sitio web de ClassDojo, parece ser que tiene buenas políticas de privacidad que limitan la exposición de correos electrónicos no intencional en documentos públicos y accesibles.
- Parece ser que en Classdojo implementaron prácticas seguras de configuración de DNS y correo electrónico que impiden la exposición de información sensible como nombres de usuarios en subdominios o registros públicos.
- ClassDojo ha demostrado tener buenas medidas para la protección de datos sensible como nombres de usuarios, así también tiene medidas para proteger los datos sensibles que se comparten en los banner de los servicios que pueden tener información sensible, como SMTP, FTP y telnet, lo que es muy importante ya un banner que es un mensaje que un servidor envía al cliente cuando se establece una conexión, estos pueden ser parte del protocolo de comunicación del servicio y suelen ser visibles cuando se realiza una conexión con el puerto del servicio. Además en el filtro de shodan no aparecen estos servicios por lo que puede que usen firewalls u otras medidas de protección para bloquear el acceso a estos servicios desde fuentes públicas.
- Classdojo cumple con una jerarquía organizacional convencional de una empresa de tecnología, la identidad de los jefes no es tan fácil de encontrar, la jerarquía interna parece no estar claramente visible en los registros públicos
- Las empresas que alojan los bloques de ip de Classdojo son Amazon Technologies Inc. y Cloudflare Inc., quien se encarga de gestionar el dominio es MESH DIGITAL LIMITED que es una empresa especializada en la gestión de dominios y servicios relacionados.
- Se detectó que Classdojo tiene como sistema operativo Oracle VirtualBox y QEMU lo que ofrece muchas ventajas en términos de seguridad, flexibilidad y disminución de costos, permite el aislamiento de entornos y así realizar una gestión eficiente de los recursos. Sin embargo, los dispositivos de virtualización también pueden ser un objetivos de ataques, ya que las vulnerabilidades en el hipervisor (en este caso, virtualbox y QEMU) pueden ser potencialmente explotadas para escapar de la máquina virtual y comprometer al sistema anfitrión.
- Además, las máquinas virtuales al estar conectadas tanto a una red física como a redes virtuales, requieren de la implementación rigurosa de políticas de seguridad adecuadas y un monitoreo continuo para garantizar la seguridad del entorno virtualizado. Por otro lado, la gestión de múltiples máquinas virtuales puede introducir una capa adicional de complejidad a la infraestructura, lo que requiere una adecuada planificación y administración para evitar riesgos.
- Aunque no se encuentren datos sensibles leaackeados, es importante asegurarse de que todas las credenciales, tokens y contraseñas sean fuertes y están gestionadas de forma adecuada. Esto incluye que se realicen cambios de contraseñas cada cierto periodo de tiempo y que se utilice un segundo factor de autenticación cuando sea posible. Es muy importante continuar monitoreando posibles filtraciones y realizar auditorías regulares de seguridad para detectar nuevas amenazas o posibles vulnerabilidades.

- Se realizó un análisis exhaustivo de los bloques IP asociados Classdojo mediante diversas herramientas, como TheHarvester y consultas a bases de datos Whois, en los resultados muestra que la infraestructura de la organización está distribuida en múltiples bloques de direcciones IP que pertenecen principalmente a proveedores de servicios en la nube como Amazon Web Services (AWS) y Cloudflare, los cuales abarcan un rango amplio de direcciones, lo que indica una infraestructura robusta y globalizada. Por esto es importante revisar las políticas de privacidad de los proveedores para garantizar la protección adecuada de los datos.
- Como servidor de correos Classdojo utiliza servicios de Google, lo que es una buena decisión ya que google tiene una mayor capacidad de almacenamiento y gestión de mails que otros servicios, además es seguro y confiable, por otro lado cuenta con múltiples herramientas y configuraciones disponibles para manejar el tráfico mails corporativos. La existencia de múltiples servidores de correo con diferentes prioridades permite distribuir la carga y asegurar que el servicio siga funcionando ante posibles fallas.
- La infraestructura de nombres de dominio de classdojo se encuentra bien distribuida, permitiendo redundancia y escalabilidad. Además, está bien configurada para evitar transferencia de zona a quien no lo tiene permitido, y además está preparada para manejar tanto ipv4 como ipv6.
- Classdojo utiliza CloudFront para manejar el tráfico de sus servidores webs, este ofrece escalabilidad y redundancia, lo que ayuda a manejar grandes volúmenes de tráfico. Además ofrece CDN (red de distribución de contenido) que agrega una capa de seguridad a los servidores webs, cuando queremos acceder a uno de estos en realidad se lo solicitamos al CDN, este analiza la solicitud y si cumple con las normas y reglas de seguridad la pasa a los servidores reales protegiendolos de que accedemos directamente a ellos.
- Finalmente, el análisis detallado de los puertos y servicios en las direcciones IP asociadas a los servidores de ClassDojo ha revelado una infraestructura bien distribuida que utiliza una variedad de servicios y tecnologías clave, como Amazon CloudFront y BIND DNS, lo que refuerza la escalabilidad y confiabilidad de la plataforma. Sin embargo, el hecho de que algunos servicios como HTTP/HTTPS y SIP (puerto 5060) no ofrezcan información clara sobre sus versiones puede ser una medida de seguridad, pero también podría sugerir falta de mantenimiento o configuraciones inseguras. Por otro lado puerto 5060, que está asociado al protocolo SIP para VoIP, es un área de interés particular desde el punto de vista de la seguridad, ya que este protocolo es conocido por ser susceptible a ciertos tipos de ataques, como spoofing o DoS, debido a la naturaleza de sus protocolos, (la forma en que se transmite la información y su dependencia de la infraestructura de red) si no está configurado correctamente.

➢ **<u>Sección para Entrega Gerencial:</u>**

- Resumen Ejecutivo:
  - ➢ ClassDojo presenta una infraestructura sólida (la base tecnológica sobre la que se construyen y operan los servicios), confiable y bien organizada con los servicios de proveedores confiables como Amazon Web Services (AWS), que es es un servicio de computación en la nube que ofrece una amplia gama de herramientas y servicios para gestionar y almacenar aplicaciones, y Cloudflare, que por su lado es principalmente un servicio de seguridad y rendimiento web con el propósito es proteger los sitios web contra ataques (como los ataques DDoS) y mejorar la velocidad de carga con una red de distribución de contenido, además ofrece firewalls y otras herramientas para mejorar la seguridad y estabilidad de los sitios web. AWS y Cloudflare permiten mantener los servicios de manera segura, escalable y con un alto rendimiento. A lo largo del análisis, no se han encontrado filtraciones activas de datos sensibles ni vulnerabilidades críticas que pudieran comprometer la seguridad de los usuarios.
  - ➢ Uno de los descubrimientos más llamativos es el uso de tecnologías modernas para el desarrollo y la administración de sus plataformas, como Storybook para el diseño de interfaces y CloudFront para la distribución de contenido. Estas herramientas aseguran que ClassDojo no solo sea eficiente, sino que también esté protegido frente a ataques comunes.
  - ➢ En cuanto a la protección de datos, la compañía ha implementado correctamente protocolos de seguridad, como el cifrado de comunicaciones a través de TLS, todos sus sitios están certificados con HTTPS. No obstante, se ha detectado que algunos servidores tienen una cantidad inusualmente alta de puertos abiertos(puertas digitales que están abiertas y permiten conexiones, esto puede ser un problema porque más puertas abiertas significan más oportunidades para que un atacante entre), lo cual podría significar una configuración inadecuada o una gestión insuficiente en algunos casos.

- Se puede concluir que ClassDojo está claramente comprometido con la seguridad y eligió conscientemente sus proveedores y configuraciones, hasta hace uso de programas de descubrimiento de vulnerabilidades, como Bugcrowd, donde expertos de diferentes áreas colaboran para detectar posibles fallos de seguridad. Esto demuestra una actitud proactiva, toma la iniciativa para anticiparse a los problemas o necesidades, hacia la seguridad y el mantenimiento de la confianza de los usuarios, algo clave al momento de enfrentar la inseguridad digital moderna.

- Evaluación de Riesgos:
  - Se recomienda revisar la configuración de puertos para minimizar el riesgo de exposición y asegurar que solo los servicios esenciales estén accesibles. Sin duda es prudente realizar auditorías de seguridad regulares para mantener la infraestructura protegida frente a posibles nuevas amenazas, tal como parece estarlo, estar alerta a las vulnerabilidades es esencial para poder evitar incidentes o hacer un plan para reaccionar a tiempo y de manera adecuada minimizando pérdidas.
  - Por otro lado, a pesar de la solidez de la infraestructura, algunos puntos de mejora incluyen la necesidad de revisar configuraciones de seguridad en ciertos servidores y eliminar el soporte para versiones obsoletas de protocolos como TLS 1.0 y 1.1. Asegurar que las credenciales y contraseñas se gestionen adecuadamente, con políticas de rotación de contraseñas y autenticación de dos factores, también contribuirá a minimizar riesgos futuros.
  - ClassDojo ha demostrado que toma la seguridad de sus usuarios en serio, pero debe continuar implementando buenas prácticas y actualizando su infraestructura según las amenazas emergentes en el panorama digital.