INFORME 4

Diego Martín Olea

En esta práctica el/la alumno/a aplicará las técnicas y utilizará las diferentes herramientas vistas durante el módulo.

Preparación:

El/La alumno/a deberá elegir una organización que esté dentro del programa de hackerone.

- ***Crear una cuenta en https://hackerone.com***
- ***Elegir una organización con varios dominios en scope.***
- ***Elegir una organización que permita realizar un reconocimiento vertical amplio (que tenga dominios en scope del estilo: *.dominio.com).***
- ***Comprobar las normas del programa detalladamente asegurando que está permitido atacar dichos dominios***

El objetivo es obtener la máxima información posible de la organización elegida. Esto incluye, pero no limita:

- ***Información de cada dominio.***
- ***Subdominios relacionados (dentro del scope).***
- ***Análisis de vulnerabilidades.***
- ***Información obtenida con técnicas OSINT (correos electrónicos, empleados relevantes, etc.).***

Índice

1. Elección del objetivo **3**

2. Herramientas y desarrollo **3**

2.1. Validacion de servidores 3

2.2. Fuerza bruta 3

2.3. TLS PROBING 4

2.4. SCRAPING 4

2.5. Certificate Transparency Logs 5

2.6. Búsquedas pasivas 5

2.6.1. Archivos web y cache 5

2.6.2. Servidores en la nube 6

2.6.3. Repositorios de código 6

2.7. Validación de dominios 8

2.8. Escaneo de puertos 8

2.9. Análisis web 10

3. Análisis de vulnerabilidades **13**

3.1. Nuclei 13

3.2. Wpscan 13

3.3. Spoofcheck 13

3.4. Greenbone 14

4. Información obtenida con técnicas OSINT **15**

4.1. Maltego 15

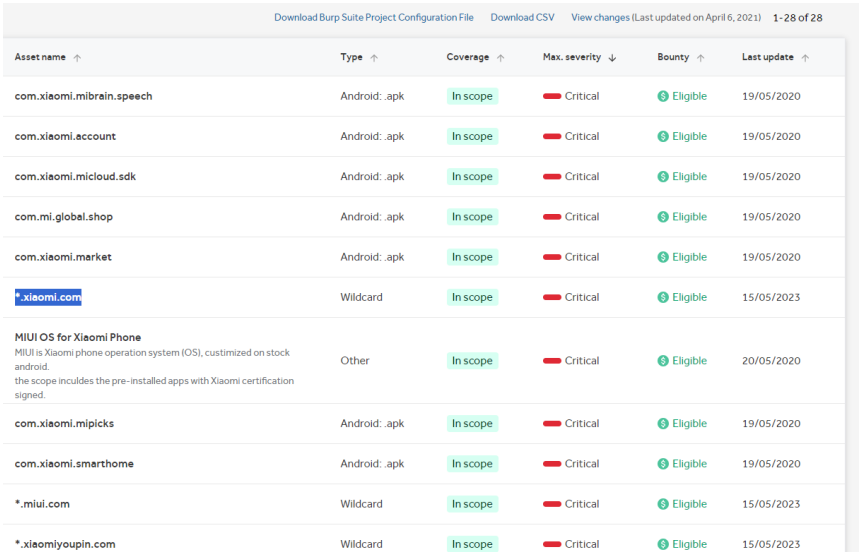
4.2. Controles de búsqueda 15

4.3. Metadatos 16

5. Vulnerabilidades encontradas e información sensible **17**

1. Elección del objetivo

Para la elección de nuestro objetivo nos hemos creado una cuenta en la página web www.hackerone.com y hemos elegido como objetivo la empresa de Xiaomi. Buscando dentro del scope para encontrar y poder elegir un objetivo válido hemos encontrado el dominio *.xiaomi.com
Con este dominio cumplimos los requisitos para poder realizar un reconocimiento vertical amplio y además comprobamos las normas y políticas de la propia empresa de Xiaomi que nos permite hacer este reconocimiento.



Download Burp Suite Project Configuration File | Download CSV | View changes (Last updated on April 6, 2021) | 1-28 of 28

Asset name	Type	Coverage	Max. severity	Bounty	Last update
com.xiaomi.mibrain.speech	Android: .apk	In scope	Critical	Eligible	19/05/2020
com.xiaomi.account	Android: .apk	In scope	Critical	Eligible	19/05/2020
com.xiaomi.micloud.sdk	Android: .apk	In scope	Critical	Eligible	19/05/2020
com.mi.global.shop	Android: .apk	In scope	Critical	Eligible	19/05/2020
com.xiaomi.market	Android: .apk	In scope	Critical	Eligible	19/05/2020
*.xiaomi.com	Wildcard	In scope	Critical	Eligible	15/05/2023
MIUI OS for Xiaomi Phone MIUI is Xiaomi phone operation system (OS), custimized on stock android. the scope inculdes the pre-installed apps with Xiaomi certification signed.	Other	In scope	Critical	Eligible	20/05/2020
com.xiaomi.mipicks	Android: .apk	In scope	Critical	Eligible	19/05/2020
com.xiaomi.smarthome	Android: .apk	In scope	Critical	Eligible	19/05/2020
*.miui.com	Wildcard	In scope	Critical	Eligible	15/05/2023
*.xiaomiyoupin.com	Wildcard	In scope	Critical	Eligible	15/05/2023

2. Herramientas y Desarrollo

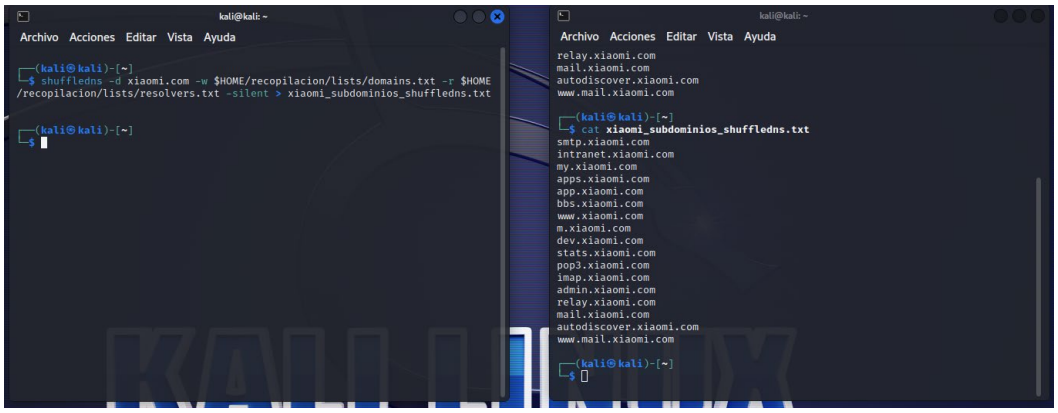
Para realizar nuestro reconocimiento debemos hacer uso de diversas herramientas que nos permitan una recopilación lo mas amplia y completa posible por lo que usaremos distintas herramientas que nos irán proporcionando diferentes resultados y en algunos casos algún resultado distinto que posteriormente limpiaremos para quedarnos con dominios y subdominios de caracter único que nos permita analizar y obtener la mayor información posible. Todos los resultados se volcarán en un fichero .txt que iremos agrupando y una vez que tengamos todos los ficheros .txt de las distintas herramientas los uniremos para tener la lista definitiva de los dominios y subdominios del objetivo. Para ello nombraremos en primer lugar los resultados de cada herramienta como xiaomi_subdominios_HerramientaUsada.txt

2.1 Validación de servidores: Comenzamos el reconocimiento usando el comando dnsvalidator -tL https://raw.githubusercontent.com/blechschmidt/massdns/master/lists/resolvers.txt -threads 100 -o $HOME/recopilacion/lists/resolvers.txt

Este comando nos permite actualizar la lista de los servidores para así poder realizar posteriormente nuestra búsqueda.

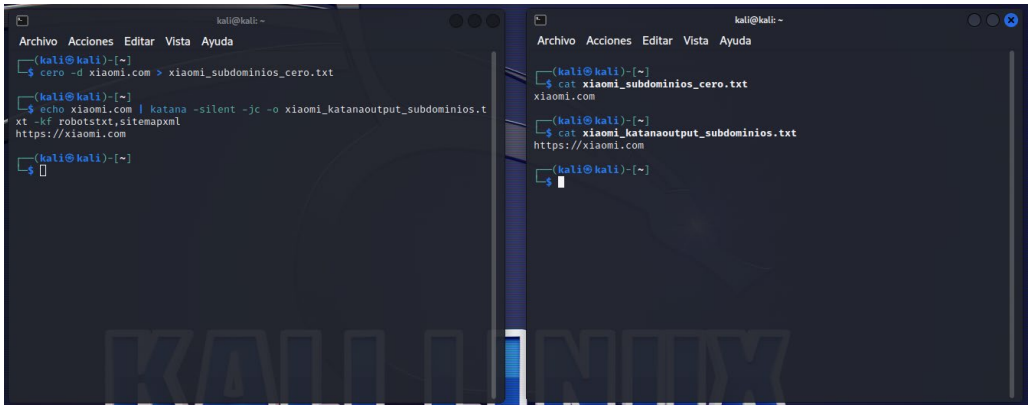
2.2 Fuerza Bruta: Usamos el comando shuffledns -d xiaomi.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/resolvers.txt -silent > xiaomi_subdominios_shuffledns.txt para así obtener los subdominios relacionados con nuestro objetivo que en este caso es xiaomi.com. Con ello conseguimos obtener en un fichero llamado xiaomi_subdominios_shuffledns.txt.

Usando el comando cat en la consola de nuestro Kali y vemos los subdominios obtenidos a partir de los anteriores comandos.

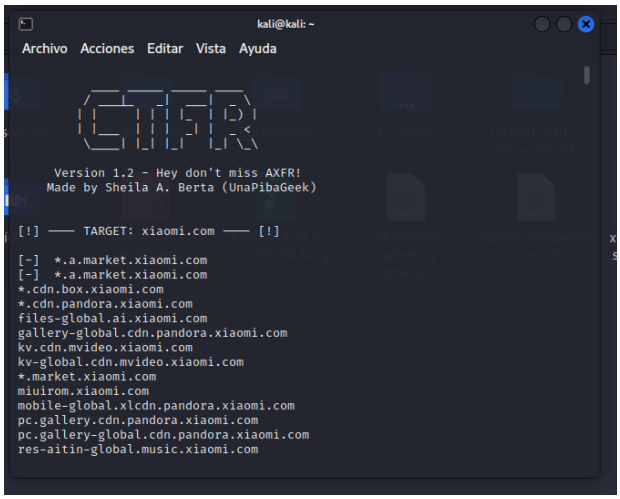


2.3.TLS PROBING: Usando el comando cero -d xiaomi.com > xiaomi_subdominios_cero.txt para analizar los certificados TLS en búsqueda de otros subdominios y almacenarlos en un archivo txt pero solo obtenemos el mismo dominio que es xiaomi.com

2.4 SCRAPING: Usamos la herramienta de katana con el comando echo xiaomi.com | katana -silent -jc -o xiaomi_katanaoutput_subdominios.txt -kf robotstxt,sitemapxml
y obtenemos estos resultados:

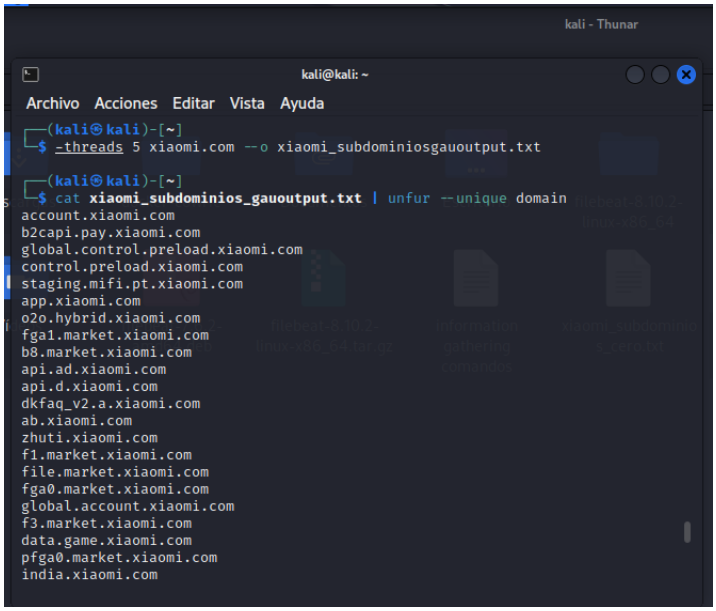


2.5 Certificate Transparency Logs: Usando el comando de ctfr -d xiaomi.com encontramos una lista de subdominios que guardaremos en un archivo para completar nuestra lista.

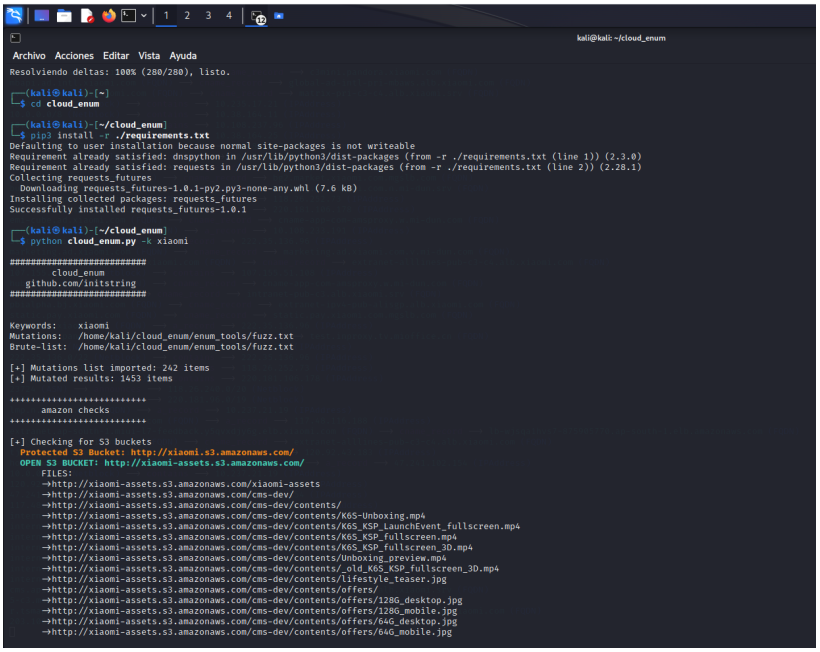


2.6 Búsquedas pasivas:

2.6.1 Archivos web y caché: Usamos el comando de gau --threads 5 xiaomi.com --o xiaomi_subdominios_gauoutput.txt y nos encontramos mas subdominios,posteriormente usamos un cat a xiaomi_subdominios_gauoutput.txt para conseguir los dominios únicos y seguir obteniendo mas subdominios.



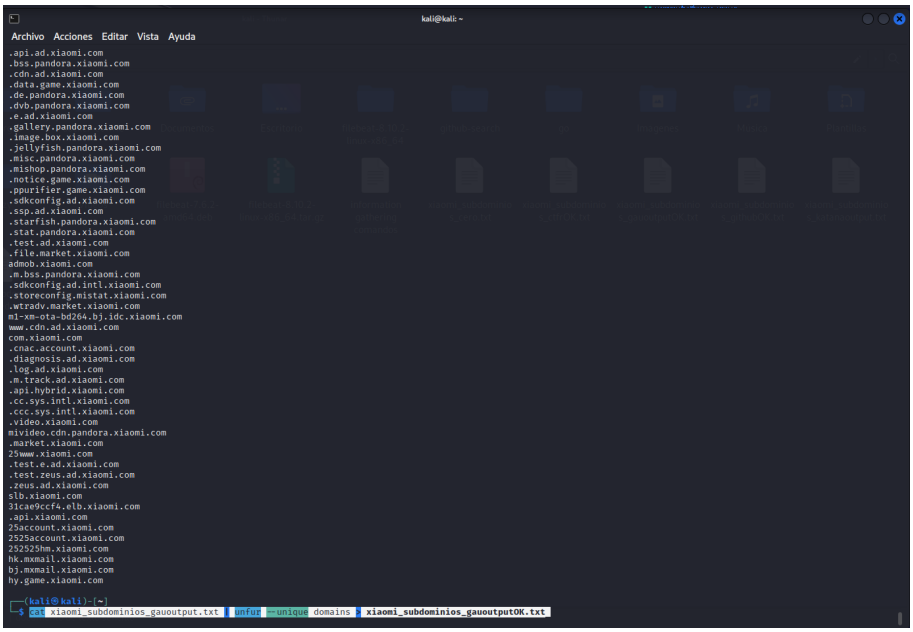
2.6.2 Servidores en la nube: Usamos la herramienta para buscar buckets en servidores en la nube y nos encontramos una serie de carpetas abiertas que habría que ir comprobando para ver si hay algún fallo.



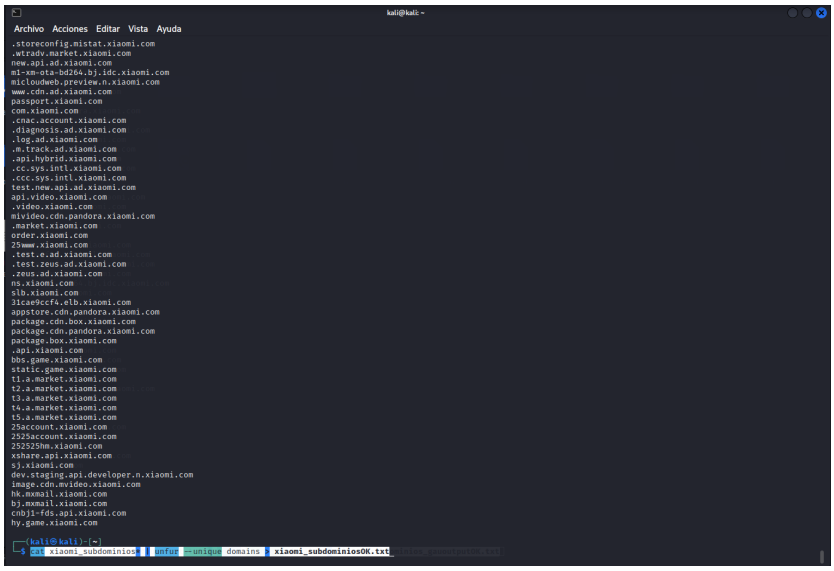
2.6.3 Repositorios de código: Usamos tambien la herramienta para buscar subdominios en github y encontramos numerosos subdominios que hay que limpiar para nuestra lista final.

Una vez que hemos usado todas las herramientas para nuestro reconocimiento debemos proceder a limpiar los ficheros .txt para no salirnos del scope y tener los subdominios que nos interesan eliminando subdominios repetidos ya sea porque las herramientas nos han sacado el mismo y están duplicados,porque aunque contengan el objetivo del scope no son subdominios por lo que se situarían fuera de nuestro objetivo etc. Para ello debemos usar una serie de comandos aplicandolos

a los ficheros que hemos ido guardando de las herramientas usando comandos como este cat xiaomi_subdominios_gauoutput.txt | unfur --unique domains > xiaomi_subdominios_gauoutputOK.txt



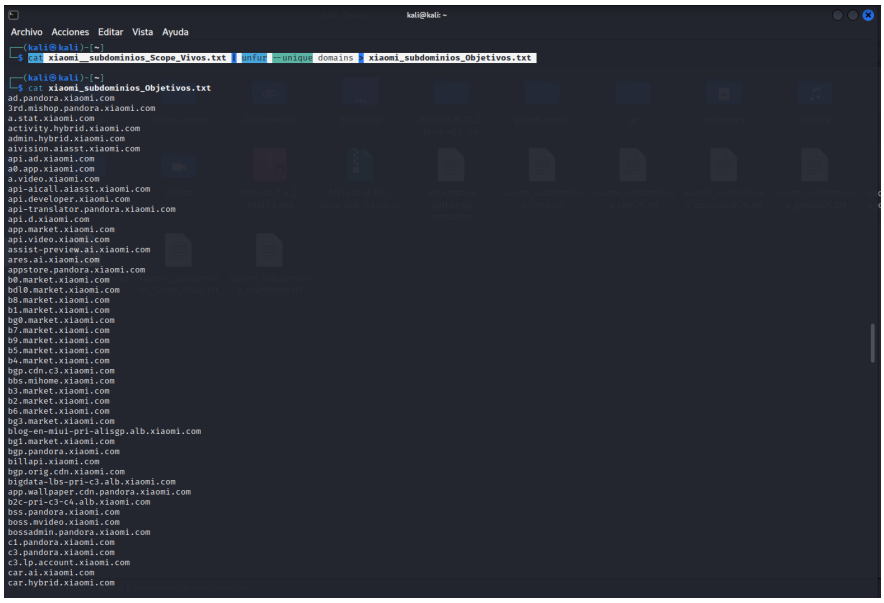
Este comando lo aplicamos a todos los ficheros para así limpiarlos. Una vez que tenemos todos esos ficheros limpios debemos agrupar todos los subdominios en un mismo fichero y a su vez volverlo a limpiar para que los casos concurrentes de las distintas herramientas no nos dupliquen el mismo subdominio. Usamos el comando cat xiaomi_subdominios* | unfur --unique domains > xiaomi_subdominiosOK.txt



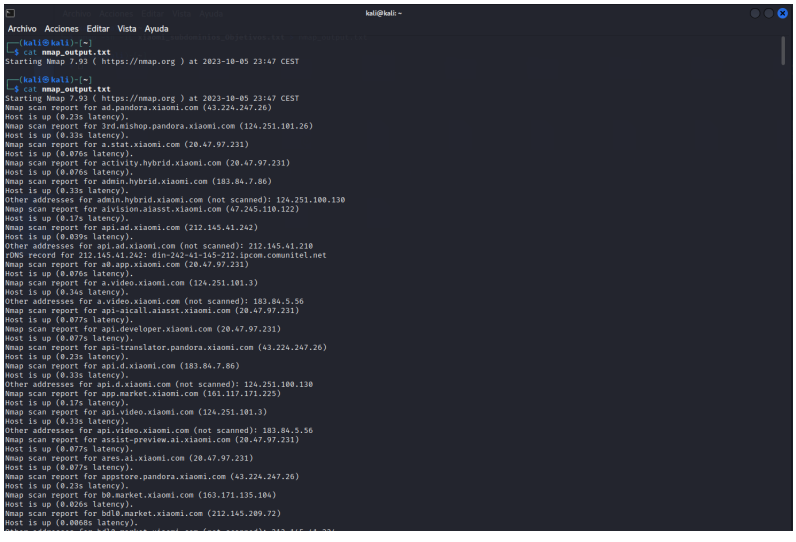
Y ya tendríamos nuestro fichero .txt con todos los subdominios de nuestro scope.

2.7 Validación de dominos: El siguiente paso sería obtener información y validar los dominios de nuestro fichero y ver cuales funcionan para poder buscar fallos para nuestro posterior análisis de vulnerabilidades. Para ello usamos el comando cat xiaomi_subdominios_Scope.txt | httpx -silent -mc 200,401,403 -o xiaomi__subdominios_Scope_Vivos.txt

A partir de esa búsqueda sacamos los subdominios que funcionan y con el comando cat xiaomi__subdominios_Scope_Vivos.txt | unfur --unique domains > xiaomi_subdominios_Objetivos.txt hemos creado el fichero .txt con nuestros objetivos que sabemos que funcionan y que está en nuestro scope.

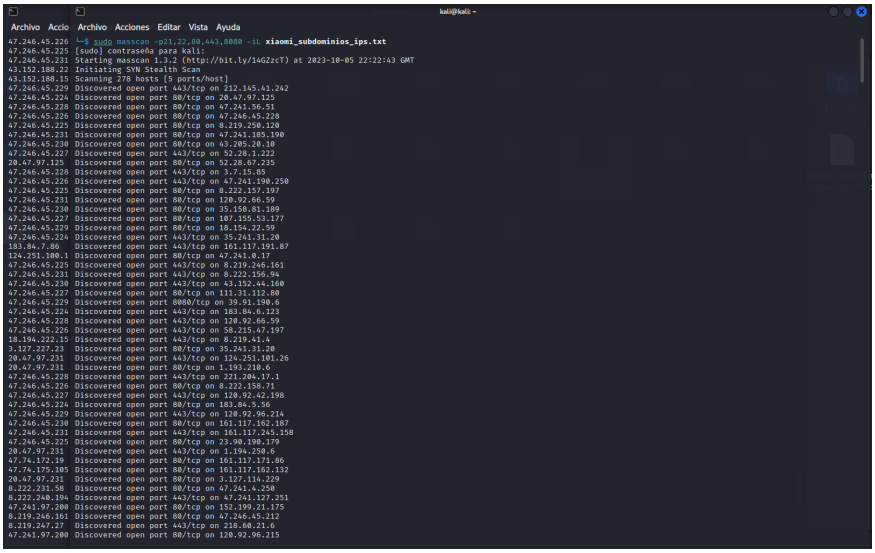


2.8 Escaneo de puertos: Escaneamos con nmap para ver si la IP de los subdominios funciona o hay un firewall que nos bloque. Nos sirve para saber si el host está encendido o no. Usamos el comando nmap -sn -iL xiaomi_subdominios_Objetivos.txt > nmap_output.txt

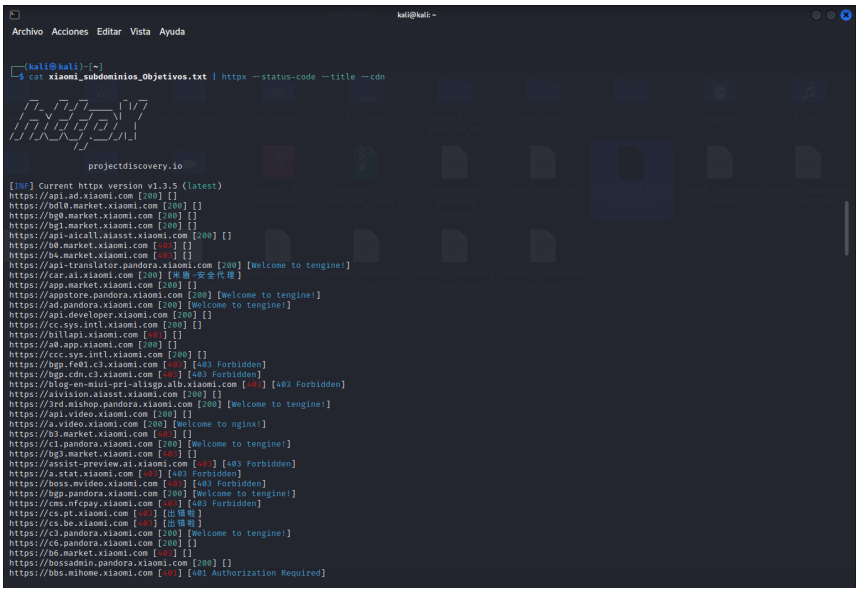


Hacemos diversos escaneos con la herramienta nmap y conseguimos una serie de outputs.

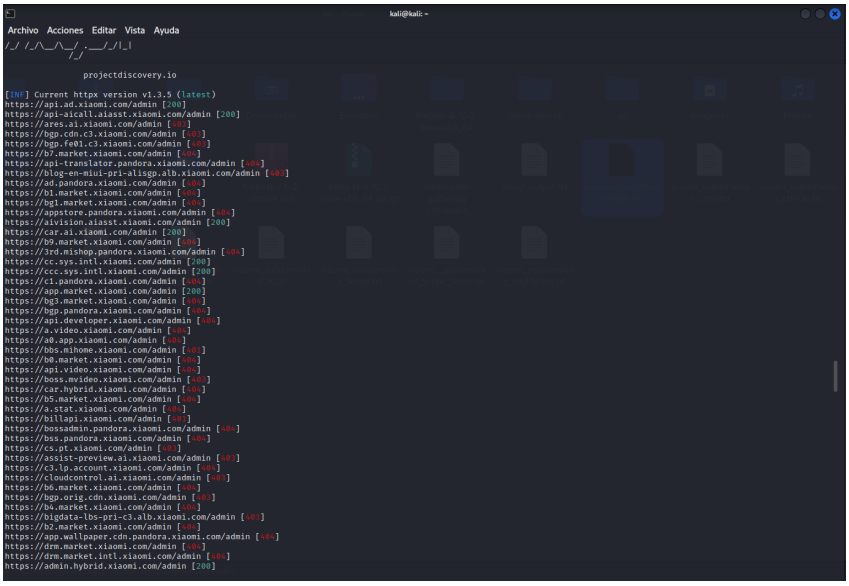
Usamos con el mismo objetivo la herramienta masscan con el comando for subdominio in $(cat xiaomi_subdominios_Objetivos.txt); do dig +short $subdominio | grep -E '([0-9]{1,3}\.){3}[0-9]{1,3}'; done > xiaomi_subdominios_ips.txt para sacar primerlo la IP y luego ver si hay algún puerto abierto que no sea el 80 o el 443 con el comando sudo masscan -p21,22,80,443,8080 -iL xiaomi_subdominios_ips.txt



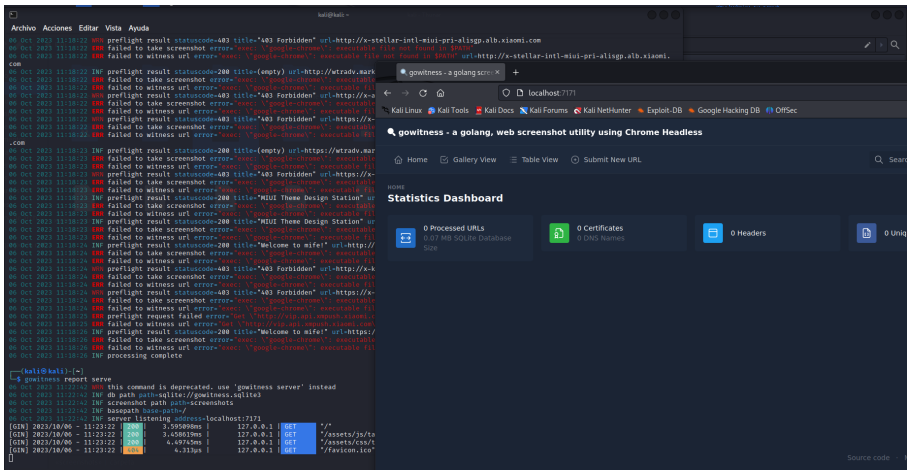
2.9 Análisis web: Al hacer una serie de peticiones con la herramienta httpx nos encontramos una serie de respuestas que podríamos analizar.



Usando el comando cat xiaomi_subdominios_Objetivos.txt | httpx --status-code --title --cdn Hay algunas páginas que responden

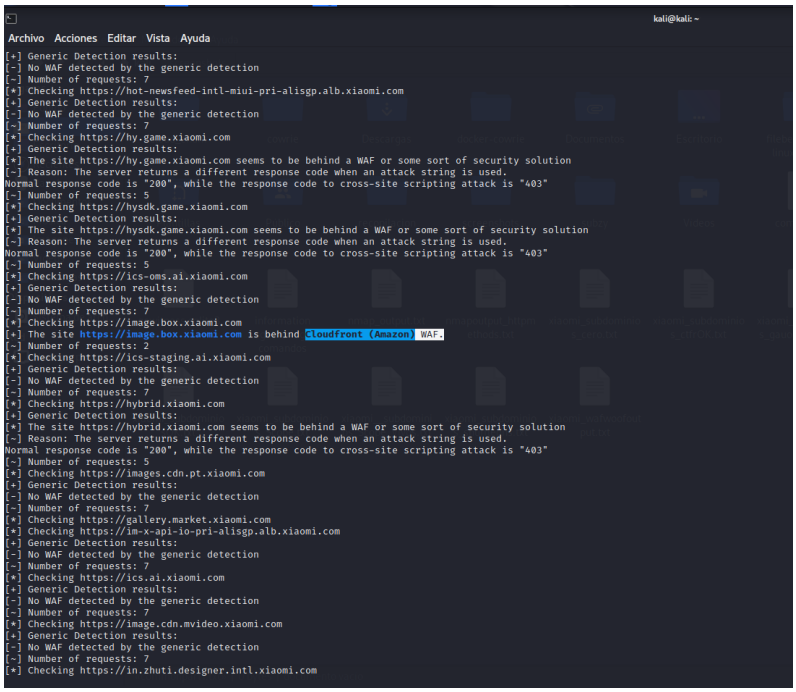


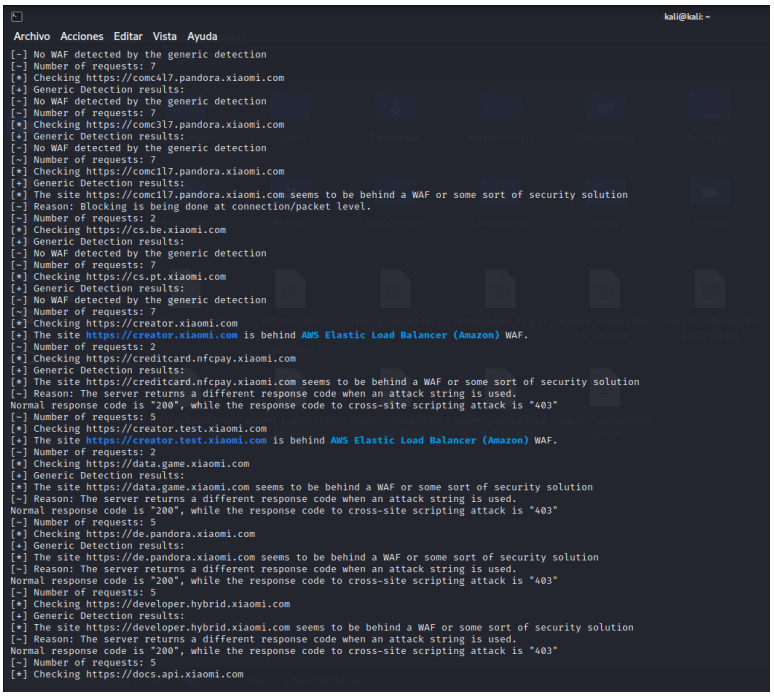
Usando la herramienta de gowitness no encontramos ningún tipo de información relevante.



Al usar la herramienta de FUZZ no encontramos ningún fichero ni nada en el subdominio a analizar

Usando la herramienta de wafw00f encontramos que los subdominios que hemos analizado están bajo dos WAF de los que hemos podido sacar la información que son AWS Elastic Load Balancer (Amazon) WAF y Cloudfront (Amazon) WAF.

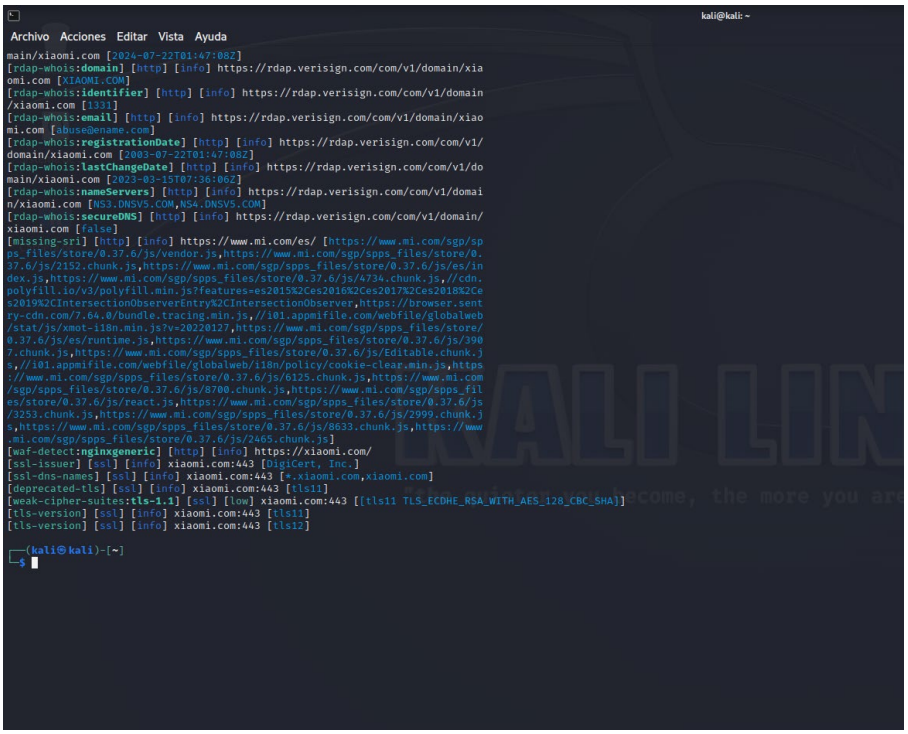




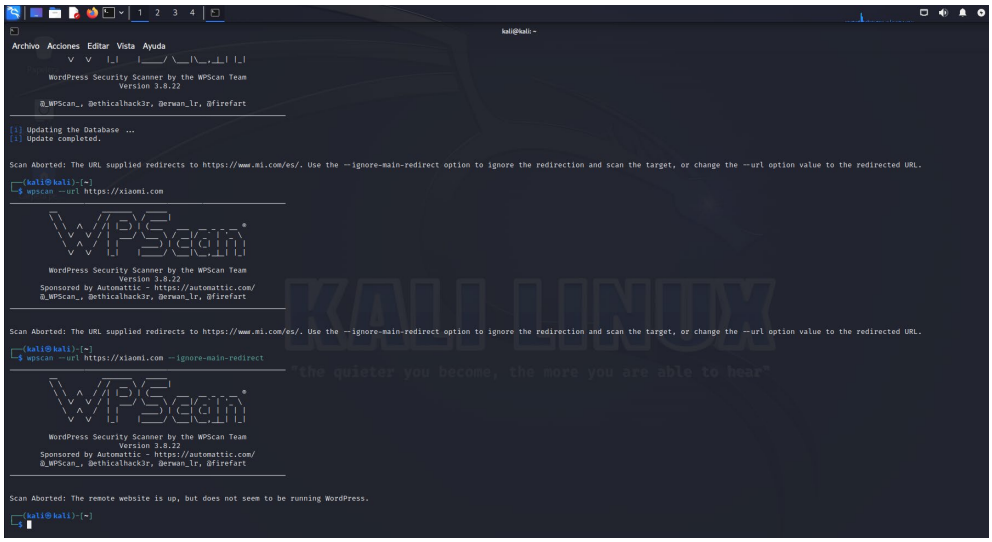
Se ha hecho un reconocimiento con la herramienta de whatweb y en el archivo adjunto se ven los datos e información sacados de la herramienta y el output obtenido.

3. Análisis de vulnerabilidades

3.1 Nuclei: Usando el reconocimiento con la herramienta nuclei nos encontramos un fallo en el que encontramos un algoritmo de cifrado debil y que podría ser atacable.

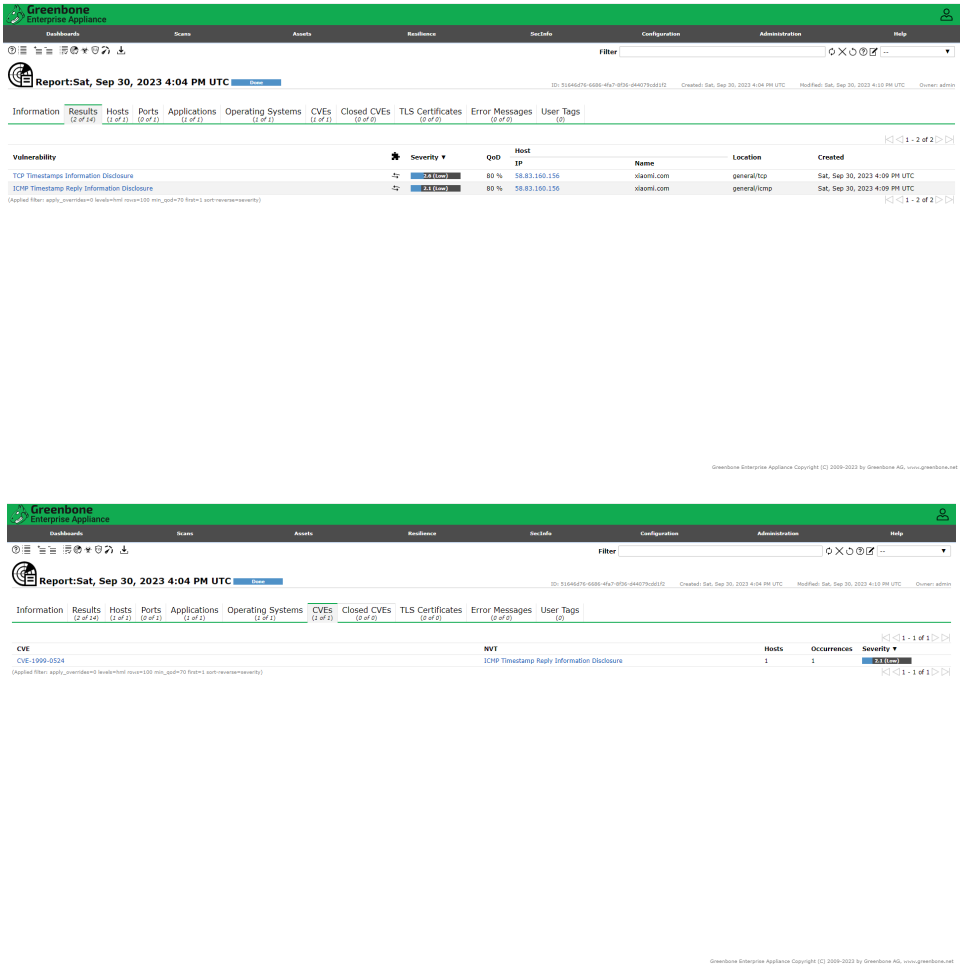


3.2 Wpscan: Con la herramienta de wpscan nos indica que la página web no usa wordpress



3.3 Spoofcheck: Usando la herramienta de spoofcheck nos dice que xiaomi.com no devuelve ningún fallo ni vulnerabilidad.

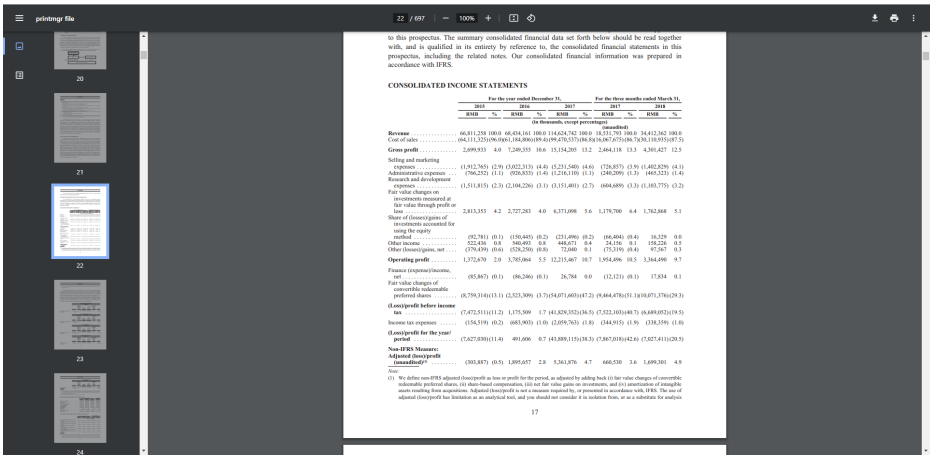
3.4 Greenbone: Usando la herramienta de greenbone y haciendo un escaneo al dominio xiaomi.com y da una serie de fallos de relevancia baja. Y otro subdominio mismos fallos.

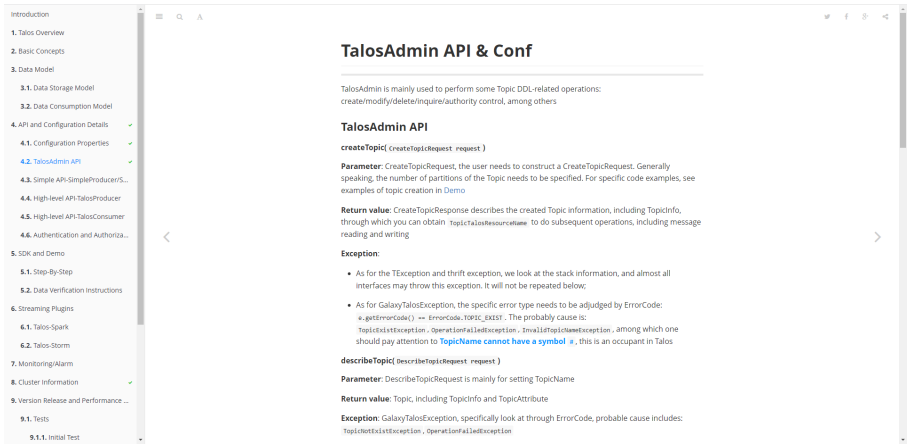


4. **Información obtenida con técnicas OSINT**

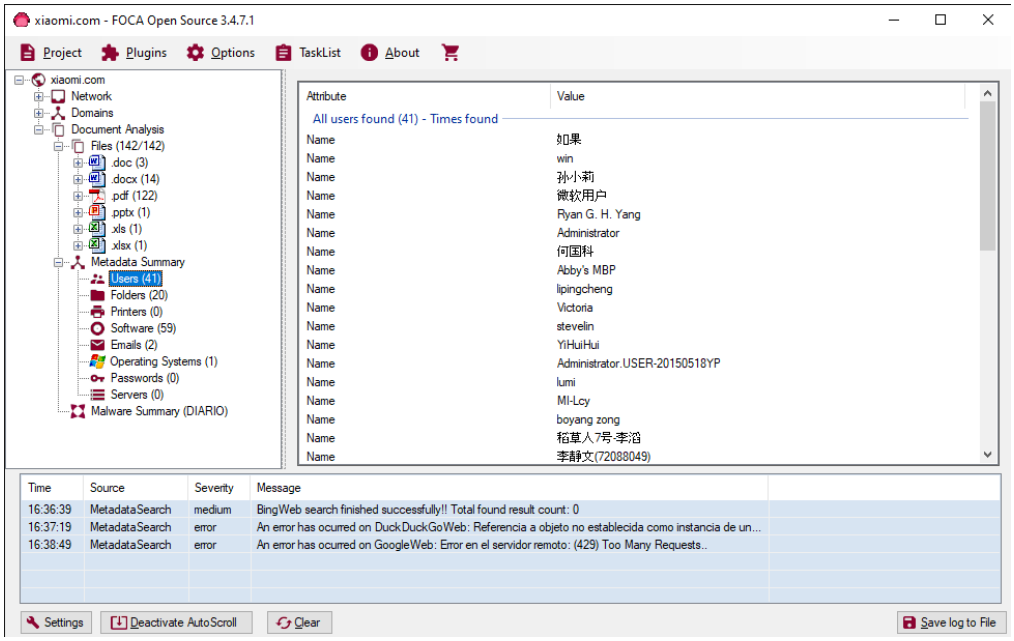
4.1 Maltego:Maltego es un software especializado en tareas OSINT con el hemos podido encontrar en nuestro dominio xiaomi.com una serie de correos que hemos comprobado si hubo alguna brecha de contraseñas y hemos encontrado que la hay.

4.2. Motores de búsqueda: Buscando en google site:xiaomi.com ext:pdf podemos encontrar un pdf de xiaomi con unas cuentas de la empresa y documentos. O en google site:xiaomi.com inrul:admin encontramos información de que tipo de administración y configuración tiene el xiaomi galaxi book para poder realizar un ataque.



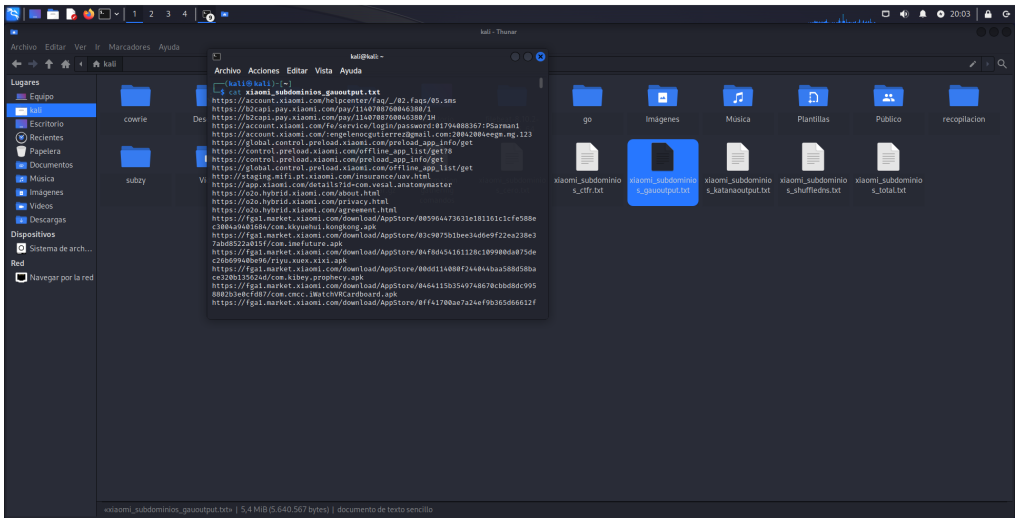


4.3 Metadatos: Usando la herramienta de FOCA hemos podido descargar y acceder a una serie de documentos y nos encontramos 41 usuarios donde cabe destacar varios que se refieren a un administrador o a una cuenta de administrador.



5. Vulnerabilidades encontradas e información sensible

Después de haber acabado el reconocimiento y recabar toda la información hemos podido obtener con la herramienta del 2.5.1 con el comando de gau obtuvimos unos datos de usuario y contraseña junto a un email que deberíamos investigar más en profundidad.



En los servidores de la nube descubrimos una serie de carpetas que habría que revisar.

Con la herramienta de masscan nos hemos encontrado una lista de puertos abiertos que convendría comprobar:
Encontramos el puerto 8080 abierto en algunos subdominios como:
Discovered open port 8080/tcp on 43.132.66.178
Discovered open port 8080/tcp on 221.195.228.1
Discovered open port 8080/tcp on 39.91.190.6
Discovered open port 8080/tcp on 43.132.66.177
Discovered open port 8080/tcp on 115.231.33.1
Discovered open port 8080/tcp on 43.132.64.93
Discovered open port 8080/tcp on 116.253.30.232
Discovered open port 8080/tcp on 163.171.135.102
Discovered open port 8080/tcp on 116.162.19.1
Discovered open port 8080/tcp on 60.221.16.6
Discovered open port 8080/tcp on 117.185.129.99
Discovered open port 8080/tcp on 111.31.112.80
Discovered open port 8080/tcp on 101.33.11.29
Discovered open port 8080/tcp on 1.193.210.6
Discovered open port 8080/tcp on 120.226.43.251
Discovered open port 8080/tcp on 120.226.43.250
Discovered open port 8080/tcp on 111.6.167.86
Discovered open port 8080/tcp on 111.31.112.79
Discovered open port 8080/tcp on 42.81.54.129
Discovered open port 8080/tcp on 122.227.201.1
Discovered open port 8080/tcp on 163.171.160.195
Discovered open port 8080/tcp on 117.141.140.111
Discovered open port 8080/tcp on 101.33.11.110
Discovered open port 8080/tcp on 117.185.129.105
Discovered open port 8080/tcp on 118.112.233.1

Discovered open port 8080/tcp on 23.90.190.178
Discovered open port 8080/tcp on 111.227.116.1
Discovered open port 8080/tcp on 111.6.167.87
Discovered open port 8080/tcp on 221.204.17.1
Discovered open port 8080/tcp on 163.171.135.104
Discovered open port 8080/tcp on 175.6.49.1
Discovered open port 8080/tcp on 43.132.64.96
Discovered open port 8080/tcp on 183.204.72.250
Discovered open port 8080/tcp on 219.144.69.6
Discovered open port 8080/tcp on 23.90.190.179
Discovered open port 8080/tcp on 1.194.250.6
Discovered open port 8080/tcp on 1.194.250.6

Sería destacable ya que este puerto sirve de pruebas y de administración de aplicaciones por lo que sería interesante a la hora de hacer pen testing.

Encontramos el puerto 22 abierto en el subdominio
Discovered open port 22/tcp on 116.253.30.232

Este puerto destacaría al estar abierto ya que es el puerto utilizado por el protocolo SSH (Secure Shell), que se utiliza para la conexión segura a un servidor remoto. Es utilizado por los administradores de sistemas para la gestión de servidores, entre otras aplicaciones con funciones similares.

Con la herramienta de httpx podríamos comprobar ya que hay una serie de páginas que responden. Con la herramienta de wafw00f hemos podido sacar la información de que algun subdominio esta bajo un WAF que son AWS Elastic Load Balancer (Amazon) WAF y Cloudfront (Amazon) WAF.

Con nuclei nos encontramos un cifrado débil y que podría ser explotable.

Con Greenbone nos encontramos una serie de fallos en el reporte al hacer el scan pero nada relevante para la explotación ya que están fuera del scope esas vulnerabilidades.

Con Maltego y ibeenpwned hemos encontrado una serie de correos y brechas de contraseñas donde podríamos encontrar información para poder acceder mediante esos correos.

Buscando en google site:xiaomi.com ext:pdf encontramos una serie de documentos y PDF´s con información de la empresa,contabilidad, cuentas de la propia empresa, y en google site:xiaomi.com inrul:admin encontramos información de que tipo de administración y configuración tiene el xiaomi galaxi book para poder realizar un ataque.

Usando la herramienta de FOCA hemos podido descargar y acceder a una serie de documentos y nos encontramos 41 usuarios donde cabe destacar varios que se refieren a un administrador o a una cuenta de administrador que deberíamos revisar para encontrar información o poder acceder mediante esos usuarios.