



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).*
- *Ánalysis 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), customized on stock android. the scope includes the pre-installed apps with Xiaomi certification signed.					
MUII OS for Xiaomi Phone	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 carácter 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.

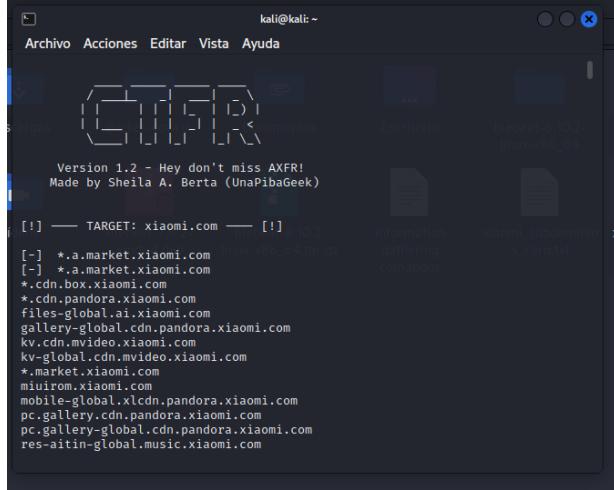
The image shows two terminal windows side-by-side. The left window shows the command: \$ shufldns -d xiaomi.com -w \$HOME/recopilacion/lists/ -r \$HOME/recopilacion/lists/resolvers.txt -silent > xiaomi_subdominios_shuffledns.txt. The right window shows the command: \$ cat xiaomi_subdominios_shuffledns.txt, which lists various subdomains such as relay.xiaomi.com, mail.xiaomi.com, autodiscover.xiaomi.com, www.mail.xiaomi.com, etc.

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:

The image shows two terminal windows side-by-side. The left window shows the command: \$ cero -d xiaomi.com > xiaomi_subdominios_cero.txt. The right window shows the command: \$ cat xiaomi_subdominios_cero.txt, which outputs 'xiaomi.com'. Below it, another command is shown: \$ cat xiaomi_katanaoutput_subdominios.txt, which also outputs 'https://xiaomi.com'.

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.



The screenshot shows a terminal window titled 'kali@kali:~' running the GTFIDF tool. The title bar says 'Archivo Acciones Editar Vista Ayuda'. Below the title bar is a logo for GTFIDF. The main text area displays the following information:

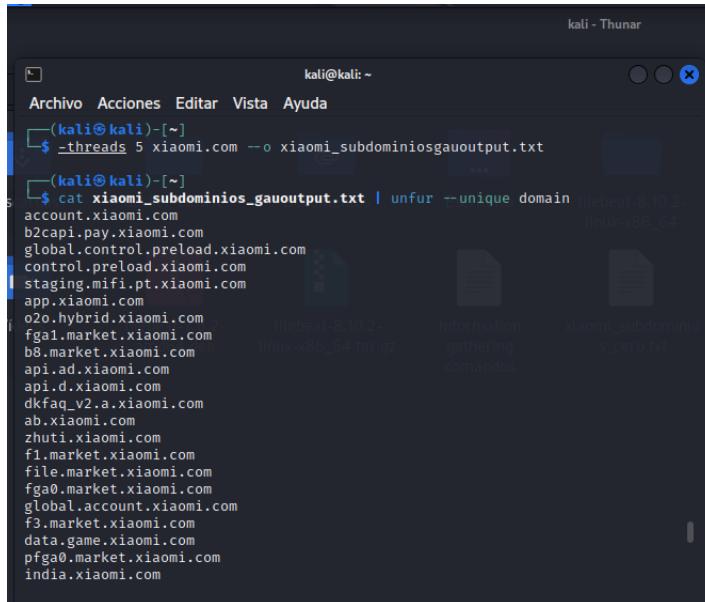
Version 1.2 - Hey don't miss AXFR!
Made by Sheila A. Berta (UnaPibaGeek)

[!] —— TARGET: xiaomi.com —— [!]

```
[-] *.a.market.xiaomi.com
[-] *.a.market.xiaomi.com
*.cdn.box.xiaomi.com
*.cdn.pandora.xiaomi.com
files-global.ai.xiaomi.com
gallery-global.cdn.pandora.xiaomi.com
kv.cdn.mvideo.xiaomi.com
kv-global.cdn.mvideo.xiaomi.com
*.market.xiaomi.com
miuirom.xiaomi.com
mobile-global.xlcnd.pandora.xiaomi.com
pc.gallery.cdn.pandora.xiaomi.com
pc.gallery-global.cdn.pandora.xiaomi.com
res-aitin-global.music.xiaomi.com
```

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.



The screenshot shows a terminal window titled 'kali - Thunar' with the command history visible. The terminal window has a title bar 'kali@kali:~' and a menu bar 'Archivo Acciones Editar Vista Ayuda'. The command line shows:

```
(kali㉿kali)-[~]
$ _threads 5 xiaomi.com --o xiaomi_subdominiosgauoutput.txt
(kali㉿kali)-[~]
$ cat xiaomi_subdominios_gauoutput.txt | unfurl --unique domain
```

The output of the command is displayed below the command line, listing numerous subdomains of xiaomi.com, such as account.xiaomi.com, b2api.pay.xiaomi.com, global.control.preload.xiaomi.com, control.preload.xiaomi.com, staging.mifi.pt.xiaomi.com, app.xiaomi.com, o2o.hybrid.xiaomi.com, fga1.market.xiaomi.com, b8.market.xiaomi.com, api.ad.xiaomi.com, api.d.xiaomi.com, dkfaq_v2.a.xiaomi.com, ab.xiaomi.com, zhuti.xiaomi.com, f1.market.xiaomi.com, file.market.xiaomi.com, fga0.market.xiaomi.com, global.account.xiaomi.com, f3.market.xiaomi.com, data.game.xiaomi.com, pfga0.market.xiaomi.com, and india.xiaomi.com.

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.

```
[kali㉿kali:~] cd cloud_enum
[kali㉿kali:~/cloud_enum]
$ pip install -r ./requirements.txt
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r ./requirements.txt (line 1)) (2.3.0)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r ./requirements.txt (line 2)) (2.28.1)
Collecting requests_futures
  Downloading requests_futures-1.0.1-py3-none-any.whl (7.6 kB)
Installing collected packages: requests_futures
Successfully installed requests_futures-1.0.1

[kali㉿kali:~/cloud_enum]
$ python cloud_enum.py -k xiaomi
#####
#           cloud_enum
#           github.com/initstring
#####

Keywords: xiaomi
Mutations: /home/kali/cloud_enum/enum_tools/fuzz.txt
Brute-list: /home/kali/cloud_enum/enum_tools/fuzz.txt

[+] Mutations list imported: 242 items
[+] Mutated results: 1453 items

*****
amazon_checks
*****

[+] Checking for S3 buckets
Protected S3 Bucket: http://xiamei.s3.amazonaws.com/
OPEN S3 BUCKET: http://xiamei-assets.s3.amazonaws.com/
FILES:
->http://xiamei-assets.s3.amazonaws.com/xiaomi-assets
->http://xiamei-assets.s3.amazonaws.com/cms-dev/
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/K5C-Unboxing.mp4
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/K5C_KSP_Fullscreen.mp4
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/K5S_KSP_Fullscreen.mp4
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/K5S_KSP_Fullscreen_3D.mp4
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/Unboxing_preview.mp4
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/lifestyle_ksp_fullscreen_30.mp4
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/lifestyle_k-sp_tesaser.jpg
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/offers/
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/offers/128G_desktop.jpg
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/offers/64G_desktop.jpg
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/offers/64G_mobile.jpg
->http://xiamei-assets.s3.amazonaws.com/cms-dev/contents/offers/64G_mobile.jpg
```

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

```

Archivo Acciones Editar Vista Ayuda
.kali@kali:~ [~]
$ 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

```

Archivo Acciones Editar Vista Ayuda
.kali@kali:~ [~]
$ 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 dominios: 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 | unfurl --unique domains > xiaomi_subdominios_Ojetivos.txt hemos creado el fichero .txt con nuestros objetivos que sabemos que funcionan y que está en nuestro scope.

```

Archivo Acciones Editar Vista Ayuda
[kali㉿kali:~] cat xiaomi_subdominios_Scope_Vivos.txt | httpx -silent -mc 200,401,403 -o xiaomi_subdominios_Ojetivos.txt
[kali㉿kali:~]
[+] cat xiaomi_subdominios_Ojetivos.txt
ad.pandora.xiaomi.com
3rd.mishop.pandora.xiaomi.com
a.stat.xiaomi.com
activity.xiaomi.com
admin.hybrid.xiaomi.com
alivision.aliasst.xiaomi.com
api.al.xiaomi.com
api.alive.xiaomi.com
a.video.xiaomi.com
api.alicall.alisst.xiaomi.com
api.alicall.pandora.xiaomi.com
api.d.xiaomi.com
api.market.xiaomi.com
app.market.xiaomi.com
assist-review.ai.xiaomi.com
ares.ai.xiaomi.com
apptore.pandora.xiaomi.com
bd.market.xiaomi.com
bd10.market.xiaomi.com
bd-market.xiaomi.com
b1a.market.xiaomi.com
bg8.market.xiaomi.com
b7.market.xiaomi.com
b9.market.xiaomi.com
b9s.market.xiaomi.com
b4.market.xiaomi.com
bgs.cdn.c3.xiaomi.com
bbs.cdn.c3.xiaomi.com
b3.market.xiaomi.com
b2.market.xiaomi.com
bb.market.xiaomi.com
bg.market.xiaomi.com
blog-en-niul-pr1-alisp.alb.xiaomi.com
bgl.market.xiaomi.com
bgp.cdn.c3.xiaomi.com
billapi.xiaomi.com
bgp.orig.cdn.xiaomi.com
bigdata-pm.pandora.xiaomi.com
bigdata-pm.pandora.xiaomi.com
b2c-pr1-c3-c4.alb.xiaomi.com
bss.pandora.xiaomi.com
boss.admin.pandora.xiaomi.com
bossadmin.pandora.xiaomi.com
c1.pandora.xiaomi.com
c3.pandora.xiaomi.com
car.account.xiaomi.com
car.ai.xiaomi.com
car.hybrid.xiaomi.com

```

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_Ojetivos.txt > nmap_output.txt

```

Archivo Acciones Editar Vista Ayuda
[kali㉿kali:~] nmap -sn -IL xiaomi_subdominios_Ojetivos.txt > nmap_output.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-05 23:47 CEST
[kali㉿kali:~]
[+] nmap_output.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-05 23:47 CEST
Nmap scan report for ad.pandora.xiaomi.com (43.224.247.26)
Host is up (0.33s latency).
Nmap scan report for 3rd.mishop.pandora.xiaomi.com (124.251.101.26)
Host is up (0.33s latency).
Nmap scan report for activity.hybrid.xiaomi.com (20.47.97.231)
Host is up (0.076s latency).
Nmap Scan Report for activity.hybrid.xiaomi.com (20.47.97.231)
Host is up (0.076s latency).
Nmap scan report for admin.hybrid.xiaomi.com (183.84.7.86)
Host is up (0.076s latency).
Nmap scan report for alivision.aliasst.xiaomi.com (not scanned); 124.251.100.130
Nmap scan report for alivision.aliasst.xiaomi.com (47.245.110.122)
Host is up (0.077s latency).
Nmap scan report for alivision.aliasst.xiaomi.com (22.115.41.242)
Host is up (0.039s latency).
Nmap scan report for alivision.aliasst.xiaomi.com (not scanned); 212.145.41.219
rDNS record for 212.145.41.242.dns-2x-61-145-212.ipcam.commitel.net
Nmap scan report for ab.app.xiaomi.com (20.47.97.231)
Host is up (0.076s latency).
Nmap scan report for a.video.xiaomi.com (124.251.101.3)
Host is up (0.34s latency).
Other addresses for a.video.xiaomi.com (not scanned); 183.84.5.56
Nmap scan report for api.alicall.alisst.xiaomi.com (20.47.97.231)
Host is up (0.077s latency).
Nmap scan report for api.alicall.pandora.xiaomi.com (20.47.97.231)
Host is up (0.077s latency).
Nmap scan report for api-translator.pandora.xiaomi.com (43.224.247.26)
Host is up (0.076s latency).
Nmap scan report for api.d.xiaomi.com (183.84.7.86)
Host is up (0.33s latency).
Nmap scan report for app.market.xiaomi.com (not scanned); 124.251.100.130
Nmap scan report for app.market.xiaomi.com (161.117.171.225)
Host is up (0.077s latency).
Nmap scan report for app.video.xiaomi.com (124.251.101.3)
Host is up (0.035s latency).
Other addresses for api.video.xiaomi.com (not scanned); 183.84.5.56
Nmap scan report for assist-review.ai.xiaomi.com (20.47.97.231)
Host is up (0.077s latency).
Nmap Scan Report for ares.ai.xiaomi.com (20.47.97.231)
Host is up (0.076s latency).
Nmap scan report for apptore.pandora.xiaomi.com (43.224.247.26)
Host is up (0.25s latency).
Nmap Scan Report for bd.market.xiaomi.com (161.171.35.194)
Host is up (0.026s latency).
Nmap Scan Report for bld.market.xiaomi.com (212.145.209.72)
Host is up (0.005s latency).

```

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

```
[kali㉿kali: ~] nmap -oX mapoutput.htmptmethods.txt stat.xiaomi.com[http://map.org] at 2023-10-06 00:00 CEST
Nmap scan report for 3rd.mishap.panorama.xiaomi.com (124.251.101.26)
Host is up (0.35s latency).

PORT      STATE SERVICE
80/tcp    open  http
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
443/tcp   open  https
|_ http-methods:
|   Supported Methods: GET HEAD
Nmap scan report for a.stat.xiaomi.com (20.47.97.231)
Host is up (0.835s latency).

PORT      STATE SERVICE
80/tcp    open  http
|_ http-methods:
|   Supported Methods: GET HEAD POST
443/tcp   open  https
|_ http-methods:
|   Supported Methods: GET HEAD POST
Nmap scan report for activity.hybrid.xiaomi.com (20.47.97.231)
Host is up (0.653s latency).

PORT      STATE SERVICE
80/tcp    open  http
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
443/tcp   open  https
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
Nmap scan report for elision.aiassistant.xiaomi.com (47.265.110.122)
Host is up (0.17s latency).

PORT      STATE SERVICE
80/tcp    filtered http
443/tcp   open  https
|_ http-methods:
|   Supported Methods: GET HEAD POST PUT DELETE TRACE OPTIONS PATCH
|_ Potentially risky methods: PUT DELETE TRACE PATCH
Nmap scan report for ap.ad.xiaomi.com (212.145.41.242)
Host is up (0.045s latency).
Other addresses for ap.ad.xiaomi.com (not scanned): 212.145.41.210
DNS record for 212.145.41.242: din=242+41+145+212.ipcon.commuil.net

PORT      STATE SERVICE
80/tcp    open  http
```

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 primero 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.

```
(kali㉿kali)-[~]
$ cat xiaomi_subdominios_Objetivos.txt | httpx --status-code --title --cdn

[!] http://api.ad.xiaomi.com [200] []
[!] https://ad01.market.xiaomi.com [200] []
[!] https://bg01.market.xiaomi.com [200] []
[!] https://bg02.market.xiaomi.com [200] []
[!] https://bg03.market.xiaomi.com [200] []
[!] https://api-aicall.aiinst.xiaomi.com [200] []
[!] https://ai-market.xiaomi.com [200] []
[!] https://app-store.xiaomi.com [200] []
[!] https://car-ai.xiaomi.com [200] [Welcome to tenginel]
[!] https://ccr-app.xiaomi.com [200] []
[!] https://ccr-store.xiaomi.com [200] [Welcome to tenginel]
[!] https://ad.pandora.xiaomi.com [200] [Welcome to tenginel]
[!] https://api.developer.xiaomi.com [200] []
[!] https://api-test.xiaomi.com [200] []
[!] https://bill/api.xiaomi.com [200] []
[!] https://a0.app.xiaomi.com [200] []
[!] https://a0.cccs.yintong.xiaomi.com [200] []
[!] https://a0.sso.xiaomi.com [200] [403 forbidden]
[!] https://bgp.dcn.c1.xiaomi.com [200] [403 Forbidden]
[!] https://blog-engine.xiaomi.com [200] []
[!] https://ccr-store.aiinst.xiaomi.com [200] []
[!] https://ccr-test.pandora.xiaomi.com [200] [Welcome to tenginel]
[!] https://api.video.xiaomi.com [200] []
[!] https://ccr-test.pandora.xiaomi.com [200] [Welcome to nginx]
[!] https://ccr-store.xiaomi.com [200] []
[!] https://cc1.pandora.xiaomi.com [200] [Welcome to tenginel]
[!] https://ccg.market.xiaomi.com [200] []
[!] https://ccg-test.xiaomi.com [200] [403 forbidden]
[!] https://a.stat.xiaomi.com [200] [403 Forbiden]
[!] https://boss.video.xiaomi.com [200] [403 Forbidden]
[!] https://ccr-test.pandora.xiaomi.com [200] [Welcome to tenginel]
[!] https://ccs.nfcpay.xiaomi.com [200] [403 forbidden]
[!] https://ccs.pt.xiaomi.com [200] [出错了]
[!] https://ccs-test.xiaomi.com [200] [出错了]
[!] https://ccg-test.xiaomi.com [200] [Welcome to tenginel]
[!] https://cc6.pandora.xiaomi.com [200] []
[!] https://cc6.market.xiaomi.com [200] []
[!] https://ccs-test.pandora.xiaomi.com [200] []
[!] https://ccs.home.xiaomi.com [200] [Bei Authorization Required]
```

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

```
Archivo Acciones Editar Vista Ayuda
:: Progress [1/1] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:01] :: Errors: 0 ::
[kali㉿kali]:~[-]
$ fffuf -w comparto1.txt -t 20 -mc 200 -u https://xiaomi.com/FUZZ

v2.0.0-dev

:: Method      : GET
:: URL         : https://xiaomi.com/FUZZ
:: Wordlist    : FUZZ: /home/kali/comparto1.txt
:: Follow redirects: false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 20
:: Matcher     : Response status: 200

:: Progress: [0/0] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::

[kali㉿kali]:~[-]
$ fffuf -w comparto2.txt -t 20 -mc 200 -u https://xiaomi.com/FUZZ

v2.0.0-dev

:: Method      : GET
:: URL         : https://xiaomi.com/FUZZ
:: Wordlist    : FUZZ: /home/kali/comparto2.txt
:: Follow redirects: false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 20
:: Matcher     : Response status: 200

:: Progress: [1/1] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:01] :: Errors: 0 ::

[kali㉿kali]:~[-]
```

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.

```
kali㉿kali ~
Archivo Acciones Editar Vista Ayuda
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://hot-newsfeed-intl-miui-pri-alisgp.alb.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://hy.game.xiaomi.com
[*] Generic Detection results:
[*] The site https://hy.game.xiaomi.com seems to be behind a WAF or some sort of security solution
[-] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[-] Number of requests: 7
[*] Checking https://hysdk.game.xiaomi.com
[*] Generic Detection results:
[*] The site https://hysdk.game.xiaomi.com seems to be behind a WAF or some sort of security solution
[-] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[-] Number of requests: 7
[*] Checking https://ics-oms.ai.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://image.box.xiaomi.com
[*] Generic Detection results:
[-] The site https://image.box.xiaomi.com is behind Cloudfront (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://ics-staging.ai.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://hybrid.xiaomi.com
[*] Generic Detection results:
[*] The site https://hybrid.xiaomi.com seems to be behind a WAF or some sort of security solution
[-] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[-] Number of requests: 7
[*] Checking https://images.cdn.pt.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://gallery.market.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://im-k-api-io-pri-alisgp.alb.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://image.ccs.pt.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://image.cdn.mvideo.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://in.zhuti.designer.intl.xiaomi.com
```

```
kali㉿kali ~
Archivo Acciones Editar Vista Ayuda
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://comc17.pandora.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://comc17.pandora.xiaomi.com
[*] Generic Detection results:
[-] The site https://comc17.pandora.xiaomi.com seems to be behind a WAF or some sort of security solution
[-] Reason: Blocking is being done at connection/packet level.
[-] Number of requests: 2
[*] Checking https://creditcard.nfcpay.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://ccs.pt.xiaomi.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
[*] Checking https://comc17.pandora.xiaomi.com
[*] Generic Detection results:
[-] The site https://comc17.pandora.xiaomi.com seems to be behind a WAF or some sort of security solution
[-] Reason: Blocking is being done at connection/packet level.
[-] Number of requests: 2
[*] Checking https://creditcard.nfcpay.xiaomi.com
[*] Generic Detection results:
[-] The site https://creditcard.nfcpay.xiaomi.com seems to be behind a WAF or some sort of security solution
[-] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[-] Number of requests: 5
[*] Checking https://data.creator.test.xiaomi.com
[*] Generic Detection results:
[-] The site https://data.creator.test.xiaomi.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[-] Number of requests: 2
[*] Checking https://data.game.xiaomi.com
[*] Generic Detection results:
[-] The site https://data.game.xiaomi.com seems to be behind a WAF or some sort of security solution
[-] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[-] Number of requests: 5
[*] Checking https://de.pandora.xiaomi.com
[*] Generic Detection results:
[-] The site https://de.pandora.xiaomi.com seems to be behind a WAF or some sort of security solution
[-] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[-] Number of requests: 5
[*] Checking https://developer.hybrid.xiaomi.com
[*] Generic Detection results:
[-] The site https://developer.hybrid.xiaomi.com seems to be behind a WAF or some sort of security solution
[-] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[-] Number of requests: 5
[*] Checking https://docs.api.xiaomi.com
```

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 débil y que podría ser atacable.

```
[kali㉿kali: ~] main/xiaomi.com [2024-07-22T01:47:08Z] [rdap-whois:domain] [http] [info] https://rdap.verisign.com/com/v1/domain/xiaomi.com [XIAOMI.COM] [rdap-whois:certificate] [http] [info] https://rdap.verisign.com/com/v1/domain/xiaomi.com [1331] [rdap-whois:email] [http] [info] https://rdap.verisign.com/com/v1/domain/xiaomi.com [abuse@xiaomi.com] [rdap-whois:registrationDate] [http] [info] https://rdap.verisign.com/com/v1/domain/xiaomi.com [2003-07-22T01:47:08Z] [rdap-whois:status] [http] [info] https://rdap.verisign.com/com/v1/domain/xiaomi.com [active] [rdap-whois:nameServers] [http] [info] https://rdap.verisign.com/com/v1/domain/xiaomi.com [NS5.DNSV5.COM,NS4.DNSV5.COM] [rdap-whois:secureDNS] [http] [info] https://rdap.verisign.com/com/v1/domain/xiaomi.com [false] [missing-sri] [http] [info] https://www.mi.com/es/ [https://www.mi.com/sgp/sp_files/store/0.37.6/js/vendor.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/react.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/antd.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/4734.chunk.js,https://cdn.polyfill.io/v3/polyfill.min.js?features=es2015%2Ces2016%2Ces2017%2Ces2018%2Ces2019%2CIntersectionObserverEntry%2CIIntersectionObserver,https://browser.send-cdn.com/7.64.0/bundle.tracing.min.js,,https://i01.apppmfile.com/webfile/globalweb/stat/js/xmat-118n.min.js?v=20220127,https://www.mi.com/sgp/sp_files/store/0.37.6/js/es/runtime.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/3909.chunk.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/editable.chunk.js,,https://i01.apppmfile.com/webfile/globalweb/118n/policy/cookie-clear_min.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/6120.chunk.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/react.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/3253.chunk.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/2999.chunk.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/8633.chunk.js,https://www.mi.com/sgp/sp_files/store/0.37.6/js/2465.chunk.js] [waf-detect:ngingeneric] [http] [info] https://xiaomi.com/ [ssl-issuer] [ssl] [info] xiaomi.com:443 [DigiCert, Inc.] [ssl-subject] [ssl] [info] xiaomi.com:443 [xiaomi.com,xiaomi.com] [deprecated-ssl] [ssl] [info] xiaomi.com:443 [xiaomi] [weak-cipher-suites:tls-1-1] [ssl] [info] xiaomi.com:443 [[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]] [[tls-version] [ssl] [info] xiaomi.com:443 [tls11] [tls-version] [ssl] [info] xiaomi.com:443 [tls12]]
```

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

```
[kali㉿kali]:~$ wpSCAN --url https://xiamon.com
[kali㉿kali]:~$ wpSCAN --url https://xiamon.com --ignore-main-redirect
[kali㉿kali]:~$
```

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.

Enterprise ApplianceDashboardScansAssetsResilienceSecurityConfigurationAdministrationHelp...
Report: Sat, Sep 30, 2023 4:04 PM UTCDetailsFilter:Created: Sat, Sep 30, 2023 4:04 PM UTCModified: Sat, Sep 30, 2023 4:10 PM UTCUser: admin

Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
(2 of 14)	(1 of 1)	(0 of 1)	(0 of 1)	(1 of 1)	(1 of 1)	(1 of 1)	(0 of 1)	(0 of 1)	(0 of 1)	(0 of 1)

Vulnerability

TOP Timestamps Information Disclosure

ICMP Timestamp Reply Information Disclosure

(Applied filter: audit_vulnerabilities level=info|error+100 min_qod>70 host=1 port-reverse|severity=)

#	Severity	QoD	Host IP	Name	Location	Created
1	Info	89 %	58.83.160.156	xiaomi.com	general/tcp	Sat, Sep 30, 2023 4:09 PM UTC
2	Info	89 %	58.83.160.156	xiaomi.com	general/icmp	Sat, Sep 30, 2023 4:09 PM UTC

[<] [1 - 2 of 2] [>]

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 inurl:admin encontramos información de que tipo de administración y configuración tiene el xiaomi galaxi book para poder realizar un ataque.

	For the year ended December 31,		For the three months ended March 31,	
	2017	2016	2017	2016
	RMB '000	%	RMB '000	%
Revenue	66,112,250	100.0	60,041,141	100.0
Cost of sales	(64,111,219)	98.0	(58,069,000)	98.0
Gross profit	2,000,030	4.0	1,972,141	3.2
Selling and marketing expenses	(1,096,242)	(2.9)	(1,022,313)	(4.4)
Research and development expenses	(1,296,242)	(3.8)	(1,231,548)	(4.8)
General and administrative expenses	(1,511,115)	(3.9)	(1,042,280)	(4.5)
Interest income	2,813,153	4.2	2,727,283	4.0
Investments received at fair value through profit or loss	2,813,153	4.2	2,727,283	4.0
Share of earnings of associates and joint ventures accounted for using the equity method	(25,251)	(0.1)	(18,040)	(0.2)
Other income	352,456	0.8	340,493	0.8
Other expenses	448,071	0.4	24,156	0.1
Operating profit	1,772,679	3.9	1,795,064	5.5
Finance (expense) income, net	(85,867)	(0.1)	(66,346)	(0.1)
Fair value change of investment in associates and joint ventures accounted for using the equity method	(8,799,141)(1.1)	(2,521,099)	(0.7)	
Preference shares	(8,404,479)(1.5)	(6,041,647)(0.6)	(0.2)	
(Loss)/profit before income tax	(7,472,511)(1.2)	(1,775,069)	(1.7)	
Income tax expenses	(154,515)	(0.2)	(68,500)	(0.0)
Income tax benefit for the period	(7,627,026)(1.4)	(1,843,569)	(1.8)	
Non-IFRS Measure: Adjusted net profit/(loss) (unaudited)⁽¹⁾	(303,817)	(0.5)	1,095,657	2.8

(1) We define non-IFRS adjusted net profit/(loss) as net profit or loss for the period, as adjusted by adding back the fair value change of convertible notes and the fair value change of investment in associates and joint ventures accounted for using the equity method, the fair value of options and other financial instruments measured at fair value through profit or loss, the fair value of investment in associates and joint ventures accounted for using the equity method, and the fair value of investment in associates and joint ventures accounted for using the fair value through profit or loss method.

TalosAdmin API & Conf

TalosAdmin is mainly used to perform some Topic DDL-related operations: create/modify/delete/inquire/authority control, among others

TalosAdmin API

createTopic (`CreateTopicRequest request`)

Parameter: CreateTopicRequest, the user needs to construct a CreateTopicRequest. Generally speaking, the number of partitions of the Topic needs to be specified. For specific code examples, see examples of topic creation in Demo

Return value: CreateTopicResponse describes the created Topic information, including TopicInfo, through which you can obtain TopicAdminResource to do subsequent operations, including message reading and writing

Exception:

- As for the TException and thrift exception, we look at the stack information, and almost all interfaces may throw this exception. It will not be repeated below;
- As for GalaxyTalosException, the specific error type needs to be adjudged by ErrorCode: `a.getErrorCode() == ErrorCode.TOPIC_EXIST`. The probably cause is: TopicExistException, OperationFailedException, InvalidTopicNameException, among which one should pay attention to `TopicName cannot have a symbol !`, this is an occupant in Talos

describeTopic (`DescribeTopicRequest request`)

Parameter: DescribeTopicRequest is mainly for setting TopicName

Return value: Topic, including TopicInfo and TopicAttribute

Exception: GalaxyTalosException, specifically look at through ErrorCode, probable cause includes: TopicNotExistException, OperationFailedException

Initial Test

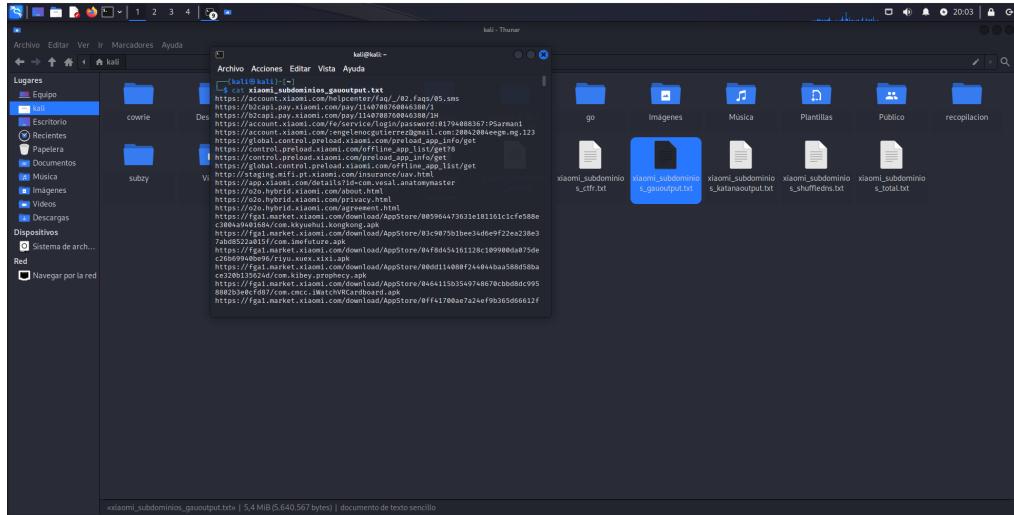
4.3 Metadatos: Usando la herramienta de FOCA hemos podido descargar y acceder a una serie de documentos y nos encontramos 41 usuarios donde cabe destacar varios que se refieren a un administrador o a una cuenta de administrador.

Attribute	Value
Name	如果
Name	win
Name	孙小莉
Name	微软用户
Name	Ryan G. H. Yang
Name	Administrator
Name	何国华
Name	Abby's MBP
Name	lipingcheng
Name	Victoria
Name	stevelin
Name	YiHuHui
Name	Administrator.USER-20150518YP
Name	lumi
Name	MI-Lcy
Name	boyang zong
Name	稻草人7号-李滔
Name	李静文(7208049)

Time	Source	Severity	Message
16:36:39	MetadataSearch	medium	BingWeb search finished successfully!! Total found result count: 0
16:37:19	MetadataSearch	error	An error has occurred on DuckDuckGoWeb: Referencia a objeto no establecida como instancia de un...
16:38:49	MetadataSearch	error	An error has occurred on GoogleWeb: Error en el servidor remoto: (429) Too Many Requests..

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 inurl: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.