Informe de reconocimiento

Reddit

Alejandro Parrado Di Domenico

16 de septiembre del 2022

Introducción

En el presente informe se presentará el procedimiento de recopilación de información llevado a cabo sobre la plataforma Reddit, y los resultados obtenidos a partir de la publicación encontrada en HackerOne que se puede ver mediante el siguiente enlace. Desde la obtención de subdominios a partir de los dominios indicados dentro del scope, hasta el análisis de vulnerabilidades presentes en ellos.

Scope

El scope que está indicado en la página de HackerOne es el siguiente:

- reddit.com
- snooguts.net
- redd.it
- redditblog.com
- redditmedia.com
- redditstatic.com
- reddituploads.com
- redditinc.com
- reddithelp.com

Procedimiento

Información sobre el dominio

Para hallar información sobre el dominio se lanzó primeramente una petición *whois*.

- `whois reddit.com`

Obteniendo el siguiente output.

- Domain Name: REDDIT.COM
- Registry Domain ID: 153584275_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.**markmonitor**.com
- Registrar URL: http://www.**markmonitor**.com
- Updated Date: 2022-03-28T09:30:06Z
- Creation Date: 2005-04-29T17:59:19Z
- Registry Expiry Date: 2024-04-29T17:59:19Z
- Registrar: **MarkMonitor Inc.**
- Registrar IANA ID: 292
- Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
- Registrar Abuse Contact Phone: +1.2086851750
- Name Server: NS-1029.AWSDNS-00.ORG
- Name Server: NS-1887.AWSDNS-43.CO.UK
- Name Server: NS-378.AWSDNS-47.COM
- Name Server: NS-557.AWSDNS-05.NET
- Registrant Organization: **Reddit Inc.**
- Registrant State/Province: **CA (California)**
- Registrant Country: US

A partir de esto es posible identificar que la empresa mediante la cual se hizo el registro del dominio fue MarkMonitor Inc. que es una plataforma dedicada a manejar, administrar y proteger la presencia de otras empresas en internet. También sabemos que la sede principal de Reddit se encuentra en de California, Estados Unidos.

Footprinting

Reconocimiento de dominios en scope

- **reddit.com** - Es el dominio principal
- **snooguts.net** - Dominio perteneciente a Reddit, también registrado con MarkMonitor, pero el sitio no se encuentra funcional.
- **redd.it** - Redirije a reddit.com, probablemente ha sido registrado con la intención de evitar domain spoofing.
- **redditblog.com** - Redirije a redditinc.com/blog .
- **redditmedia.com** - Redirije a reddit.com .
- **redditstatic.com** - No se encuentra en línea.
- **reddituploads.com** - No se encuentra en línea.
- **redditinc.com** - Landpage de Reddit.
- **reddithelp.com** - Centro de ayuda de Reddit.

Aún haciendo búsquedas con WayBackMachine no fue posible encontrar un momento en que los dominios fuera de línea hubieran estado funcionales.

Búsqueda de subdominios

Para hacer la búsqueda de subdominios se utilizaron varias herramientas:

PureDNS

- `puredns bruteforce ../SecLists/Discovery/DNS/subdomains-top1million-110000.txt reddit.com -r resolvers.txt -w ../../Desktop/Projects/Reddit/domains_and_subdomains/reddit.txt`

Obteniendo el output ubicado en **domains_and_subdomains/reddit.txt**

Amass

- `amass enum -src -d example.com`

Obteniendo los subdominios ubicados en **domains_and_subdomains/amass_output.txt**

CTFR

- `python3 ctfr.py -d 'example.com'`

Obteniendo los subdominios ubicados en **domains_and_subdomains/ctfr_output.txt**

Al analizar los resultados de las herramientas **PureDNS** y **Amass** se descubrió que la mayoría de los subdominios eran usuarios o comunidades dentro de la plataforma, ejemplo:

El subdominio **agus.reddit.com** redirige a la dirección https://www.reddit.com/r/agus/ que es el perfil de un usuario. Esto significa un problema al buscar subdominios de interés.

IP'S

IP de reddit.com

Para hallar la dirección IP a la que apunta el dominio reddit.com se utilizó la herramienta **nslookup**:

- `nslookup reddit.com`

Obteniendo las siguientes IP's:

- 151.101.65.140
- 151.101.1.140
- 151.101.129.140
- 151.101.193.140

Rangos reservados de IP's

Para buscar los rangos de IP reservados por Reddit, se utilizó la plataforma de Hurricane Electric: https://bgp.he.net/dns/reddit.com .

Se obtuvieron los siguientes rangos de IP's:

- 151.101.0.0/16
- 151.101.128.0/22
- 151.101.0.0/22
- 151.101.192.0/22

- 151.101.64.0/22

Fingerprinting

Para iniciar con el fingerprinting se hizo un escaneo de puertos al dominio reddit.com:

- `sudo nmap -Pn -sS -sV –top-ports 100 -F reddit.com`

Obteniendo los siguientes puertos abiertos:

Puerto	Servicio	Versión
80/tcp	http-proxy	Varnish
443/tcp	ssl/https	Varnish

Esto supone que no hay ninguna vulnerabilidad en cuanto a puertos abiertos se refiere, ya que el puerto 80 es el que nos permite establecer una conexión HTTP con la aplicación web y el 443 establece la conexión HTTPS con TLS por debajo, permitiéndonos tener una comunicación cifrada .

Escaneo con Spiderfoot

Se ha lanzado la herramienta gráfica de Spiderfoot con todos sus módulos con el siguiente comando.

- `./sf.py -l 127.0.0.1:5001`

Gracias a esto se ha recopilado la siguiente información de valor:

Prestador de servicio de Cloud Storage

Reddit utiliza **Amazon AWS** como prestador de servicios de Cloud Storage, y sus direcciones son las siguientes:

- https://reddit-app.s3.amazonaws.com
- https://reddit.blob.core.windows.net

La primera dirección se encuentra **abierta**, y es posible acceder a 18 archivos, entre los cuales la mayoría son favicons de la misma página.

País

Por la información del dominio reddit.com sabemos que la compañía se encuentra principalmente en **Estados Unidos**.

Direcciones de correo

En los registros DNS de SPF de reddit no se ha encontrado **ningún** problema, tras hacer la búsqueda con la herramienta DMARC Analyzer.

A continuación se listan direcciónes de correo e información sobre estos.

- alexis@reddit.com
    - Es la dirección de correo del CO-Fundador de reddit (Alexis Ohanian)

      I'm a reddit co-founder. Ask me anything.

      Got a few messages requesting this, so I figured I'd give it a go.

      Oh, and if you're not satisfied with answers here, feel free to ask publicly on the twitter - @kn0thing or privately - alexis@reddit.com
    - Podemos encontrarlo en una publicación que él mismo hizo en la plataforma
    - Mediante una búsqueda en Have I Been Pwned se ha encontrado que el correo ha sido filtrado en 17 leaks. Entre los cuales se destacan los siguientes por ser los más recientes:
        - Twitter (Enero de 2022)
        - Gravatar (Octubre de 2020)
- reddit@reddit.com
    - Correo electrónico oficial de Reddit
    - Ha sido encontrado en leaks, entre los que se destacan:
        - Covve (Febrero de 2020)
        - Gravatar (Octubre de 2020)
- press@reddit.com
    - Correo de prensa de Reddit
    - El último leak en el que se encontró fue en verification.io (2019)

Usando la herramienta Hunter.io se han encontrado las siguientes direcciones de correo:

- garrett.hoffman@reddit.com - Garrett Hoffman, ML Engineer. Su perfil de Linkedin
- michael.guido@reddit.com - Michael Guido, Jefe de relaciones con inversionistas. Su perfil de Linkedin
- jen@reddit.com - Jen L. Wong, COO de Reddit. Su perfil de Linkedin

- peter.yang@reddit.com - Peter Yang, Líder de Producto. Su perfil de Linkedin
- lei.gong@reddit.com - Lei Gong, Ex Gerente de Producto, Su perfil de Linkedin
- ama@reddit.com - Ama Tatum
- adriana@reddit.com - Adriana Smith
- neil@reddit.com - Neil Marti
- kristine@reddit.com - Kristine Smith
- roxy.young@reddit.com - Roxy Young, Directora de Marketing, Su perfil de Linkedin

Estas direcciones siguen el patrón **{first}@reddit.com** y **{first}.{last}@reddit.com**

Análisis de Vulnerabilidades

Greenbone Security Manager

Se realizó un escaneo en búsqueda de vulnerabilidades con la herramienta Greenbone Security Manager a los siguientes dominios (dentro del scope):

- reddit.com
- redditblog.com
- redditinc.com
- reddithelp.com

Se han encontrado 5 vulnerabilidades de tipo **Log**, por lo que presentan un nivel de 0 en cuanto a gravedad. Se listan a continuación:

- **CPE Inventory** - Tras haber cambios en los sistemas, no se han actualizado los CPE de la organización, por lo que permanecen los antiguos. Es necesario revisar dentro del Diccionario CPE del Nist para hacer los cambios necesarios.
- **Hostname Determination Reporting** - El script informa sobre cómo se determinó el nombre de host del objetivo.
- **OS Detection Consolidation and Reporting.**
- **Traceroute** - Traceroute es un paquete npm que se utiliza para enumerar referencias en un repositorio remoto de git. Las versiones afectadas de este paquete son vulnerables a la inyección de comandos debido al uso inseguro de exec .
- **ICMP Timestamp Detection** - En teoría, esta información podría usarse para explotar generadores débiles de números aleatorios basados en el tiempo en otros servicios.

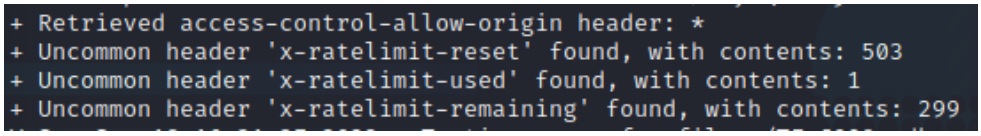
Nikto

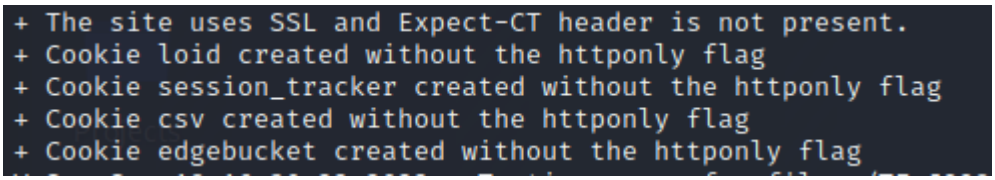
Se lanzó un escaneo con la herramienta Nikto, en búsqueda de:

- Fallos de configuración de servidores y software
- Archivos inseguros
- Sistemas o programas desactualizados

- `nikto -h https://www.reddit.com -Display V -Tuning 12`

Sin embargo solo se encontraron alertas por configuraciones extrañas de Headers, tales como:





Análisis TLS / SSL

Se ha utilizado la herramienta SSL Server Test para verificar los certificados SSL del dominio reddit.com, obteniendo que todos tienen una puntuación de A +, lo que significa que todo está correctamente configurado.

Server	Test time	Grade
151.101.193.140 Ready	Sun, 18 Sep 2022 16:07:40 UTC **Duration:** 90.365 sec	A+
151.101.129.140 Ready	Sun, 18 Sep 2022 16:09:10 UTC **Duration:** 90.967 sec	A+
151.101.65.140 Ready	Sun, 18 Sep 2022 16:10:41 UTC **Duration:** 90.846 sec	A+
151.101.1.140 Ready	Sun, 18 Sep 2022 16:12:12 UTC **Duration:** 90.470 sec	A+
2a04:4e42:200:0:0:0:0:396 Ready	Sun, 18 Sep 2022 16:13:43 UTC **Duration:** 89.934 sec	A+
2a04:4e42:0:0:0:0:0:396 Ready	Sun, 18 Sep 2022 16:15:13 UTC **Duration:** 90.690 sec	A+
2a04:4e42:600:0:0:0:0:396 Ready	Sun, 18 Sep 2022 16:16:43 UTC **Duration:** 97.647 sec	A+
2a04:4e42:400:0:0:0:0:396 Ready	Sun, 18 Sep 2022 16:18:21 UTC **Duration:** 89.573 sec	A+