Sri Lanka Institute of Information Technology

Specialized in Cyber Security

Year 2, Semester 2

IE2062 – Web Security

Bug Bounty – Report 06

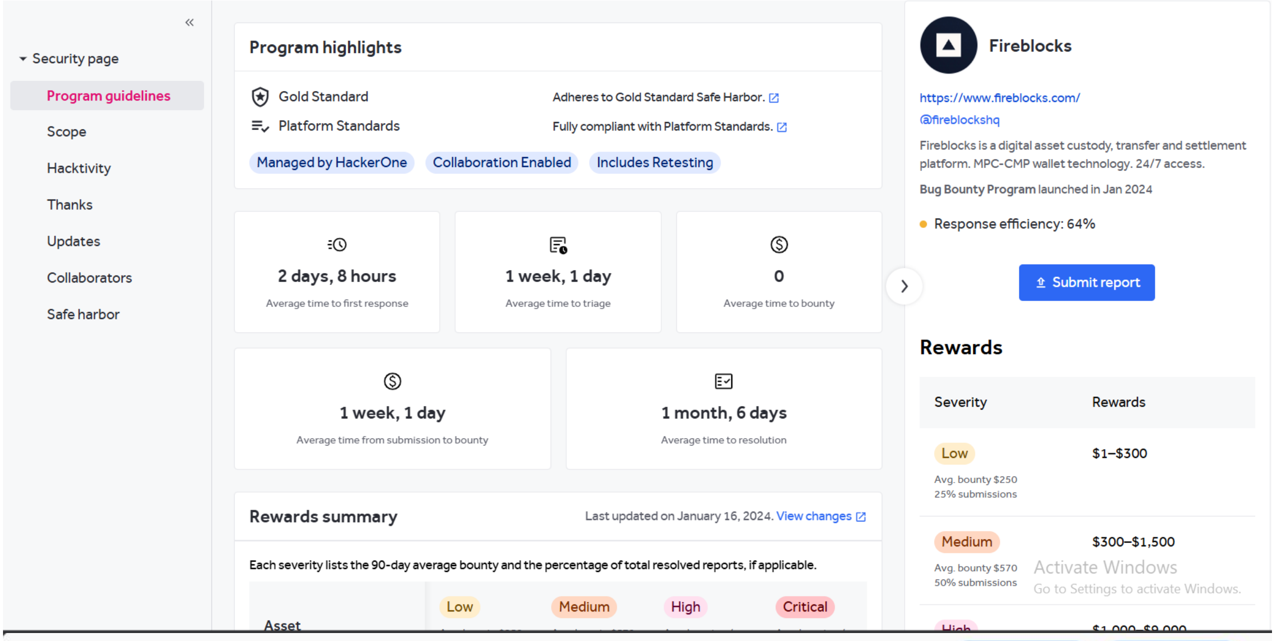
Student ID No.	**Name**
IT23136106	D.M.M. Pasindu Supushmika

Table of Contents

1. Website Overview

Fireblocks – Digital asset infrastructure built for scale and trusted for security

HackerOne Link: Fireblocks | Bug Bounty Program Policy | HackerOne



Program highlights

Gold Standard — Adheres to Gold Standard Safe Harbor.

Platform Standards — Fully compliant with Platform Standards.

Managed by HackerOne | Collaboration Enabled | Includes Retesting

2 days, 8 hours Average time to first response	1 week, 1 day Average time to triage	0 Average time to bounty
1 week, 1 day Average time from submission to bounty	1 month, 6 days Average time to resolution	

Rewards summary — Last updated on January 16, 2024. View changes

Each severity lists the 90-day average bounty and the percentage of total resolved reports, if applicable.

Asset	Low	Medium	High	Critical

Fireblocks

https://www.fireblocks.com/

@fireblockshq

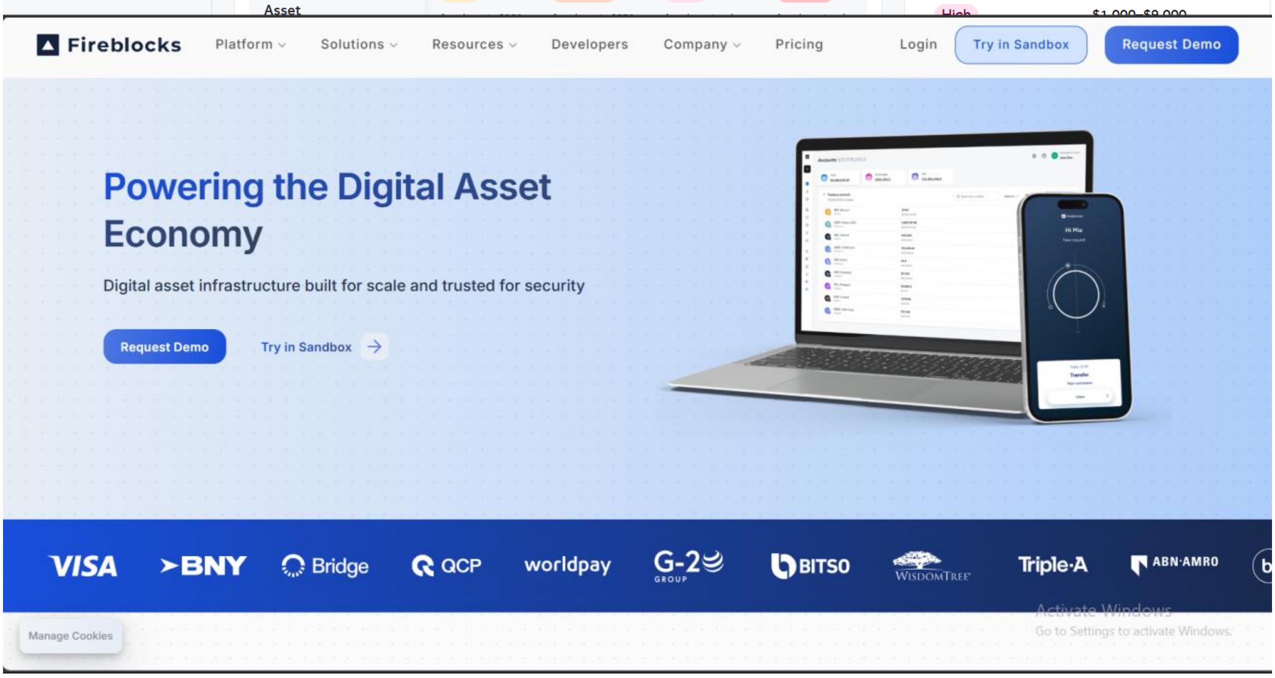
Fireblocks is a digital asset custody, transfer and settlement platform. MPC-CMP wallet technology. 24/7 access.

Bug Bounty Program launched in Jan 2024

● Response efficiency: 64%

Rewards

Severity	Rewards
Low Avg. bounty $250 25% submissions	$1–$300
Medium Avg. bounty $570 50% submissions	$300–$1,500
High	$1,000–$9,000



Powering the Digital Asset Economy

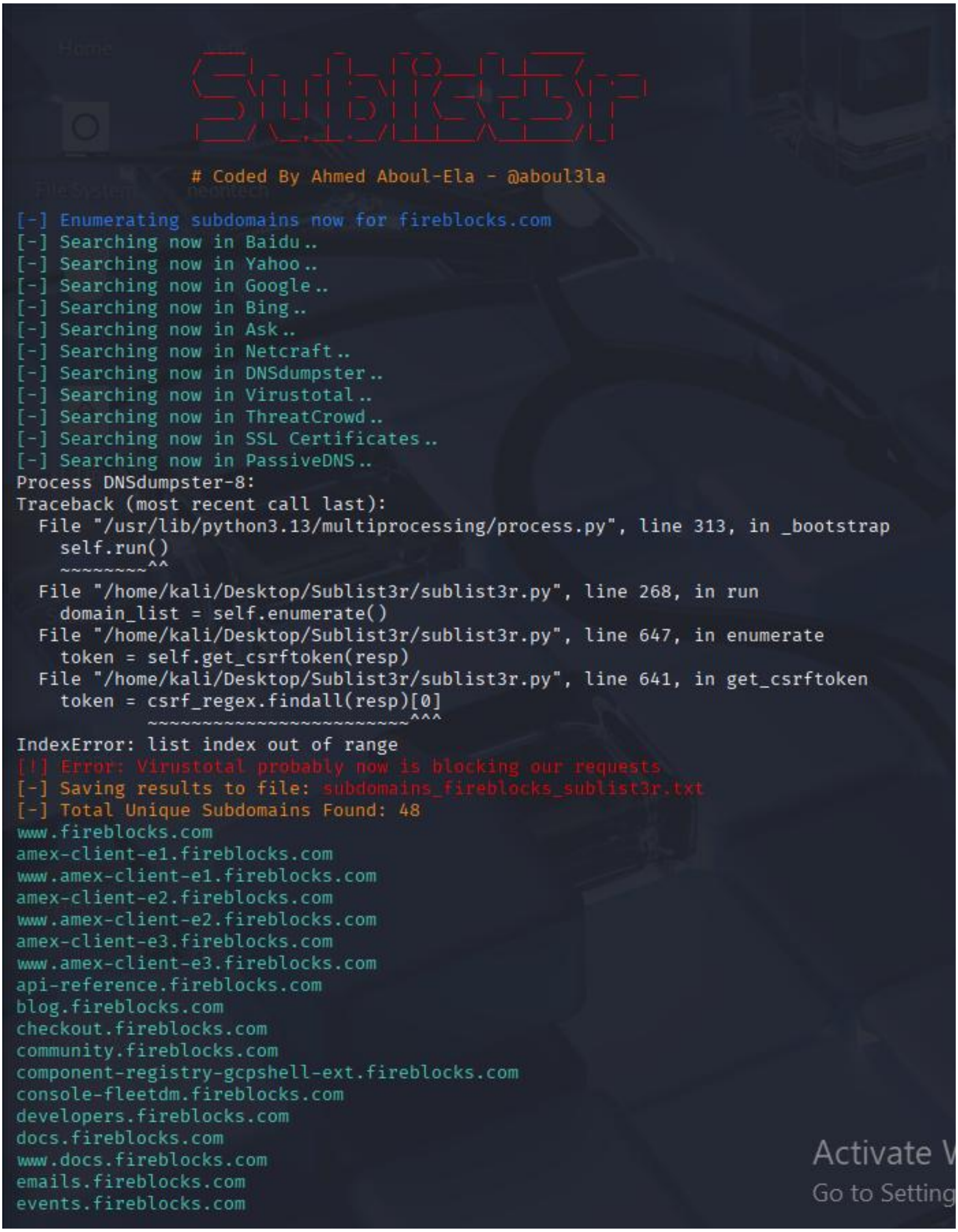
Digital asset infrastructure built for scale and trusted for security

Step 01: Gather Information.

a. Sub-domain Discovery

i. Sublist3r: subdomains_fireblocks_sublist3r.txt

Tool : Sublist3r
Code : python3 sublist3r.py -d fireblocks.com -o subdomains_fireblocks_sublist3r.txt
Explanation:
python3 sublist3r.py - Run the script using python
-*d fireblocks*- Target domain
-*o subdomains_fireblocks_sublist3r.txt* – Output file where the result is saved

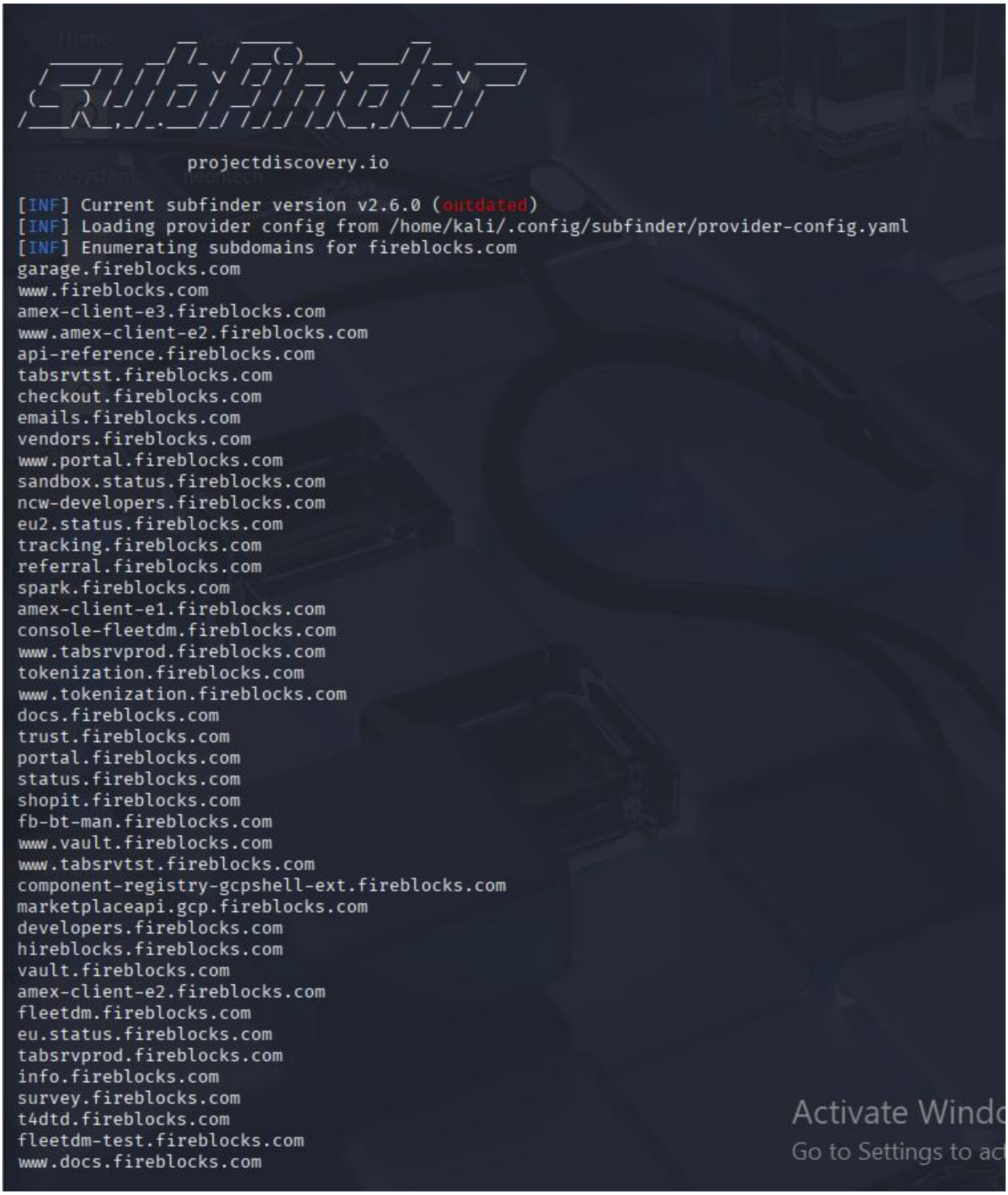


```
                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for fireblocks.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
    ~~~~~~~~^^
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 647, in enumerate
    token = self.get_csrftoken(resp)
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 641, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
            ~~~~~~~~~~~~~~~~~~~~~~~~^^^
IndexError: list index out of range
[!] Error: Virustotal probably now is blocking our requests
[-] Saving results to file: subdomains_fireblocks_sublist3r.txt
[-] Total Unique Subdomains Found: 48
www.fireblocks.com
amex-client-e1.fireblocks.com
www.amex-client-e1.fireblocks.com
amex-client-e2.fireblocks.com
www.amex-client-e2.fireblocks.com
amex-client-e3.fireblocks.com
www.amex-client-e3.fireblocks.com
api-reference.fireblocks.com
blog.fireblocks.com
checkout.fireblocks.com
community.fireblocks.com
component-registry-gcpshell-ext.fireblocks.com
console-fleetdm.fireblocks.com
developers.fireblocks.com
docs.fireblocks.com
www.docs.fireblocks.com
emails.fireblocks.com
events.fireblocks.com
```

```
www.fireblocks.com
amex-client-e1.fireblocks.com
www.amex-client-e1.fireblocks.com
amex-client-e2.fireblocks.com
www.amex-client-e2.fireblocks.com
amex-client-e3.fireblocks.com
www.amex-client-e3.fireblocks.com
api-reference.fireblocks.com
blog.fireblocks.com
checkout.fireblocks.com
community.fireblocks.com
component-registry-gcpshell-ext.fireblocks.com
console-fleetdm.fireblocks.com
developers.fireblocks.com
docs.fireblocks.com
www.docs.fireblocks.com
emails.fireblocks.com
events.fireblocks.com
fb-bt-man.fireblocks.com
fleetdm.fireblocks.com
fleetdm-test.fireblocks.com
garage.fireblocks.com
marketplaceapi.gcp.fireblocks.com
hireblocks.fireblocks.com
info.fireblocks.com
ncw-developers.fireblocks.com
portal.fireblocks.com
www.portal.fireblocks.com
referral.fireblocks.com
shopit.fireblocks.com
spark.fireblocks.com
status.fireblocks.com
eu.status.fireblocks.com
eu2.status.fireblocks.com
sandbox.status.fireblocks.com
survey.fireblocks.com
t4dtd.fireblocks.com
tabsrvprod.fireblocks.com
www.tabsrvprod.fireblocks.com
tabsrvtst.fireblocks.com
www.tabsrvtst.fireblocks.com
tokenization.fireblocks.com
www.tokenization.fireblocks.com
tracking.fireblocks.com
trust.fireblocks.com
vault.fireblocks.com
www.vault.fireblocks.com
vendors.fireblocks.com
```

ii. Subfindre: subfinder_result_fireblock.txt

Tool **:** Subfinder
Code **:** subfinder -d fireblocks.com -o subfinder_result.txt
Explanation:
bfinder - run subfinder too
l -d fireblocks.com - Mention the target website
-o subfinder_result.txt – Mention the output file



```
               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for fireblocks.com
garage.fireblocks.com
www.fireblocks.com
amex-client-e3.fireblocks.com
www.amex-client-e2.fireblocks.com
api-reference.fireblocks.com
tabsrvtst.fireblocks.com
checkout.fireblocks.com
emails.fireblocks.com
vendors.fireblocks.com
www.portal.fireblocks.com
sandbox.status.fireblocks.com
ncw-developers.fireblocks.com
eu2.status.fireblocks.com
tracking.fireblocks.com
referral.fireblocks.com
spark.fireblocks.com
amex-client-e1.fireblocks.com
console-fleetdm.fireblocks.com
www.tabsrvprod.fireblocks.com
tokenization.fireblocks.com
www.tokenization.fireblocks.com
docs.fireblocks.com
trust.fireblocks.com
portal.fireblocks.com
status.fireblocks.com
shopit.fireblocks.com
fb-bt-man.fireblocks.com
www.vault.fireblocks.com
www.tabsrvtst.fireblocks.com
component-registry-gcpshell-ext.fireblocks.com
marketplaceapi.gcp.fireblocks.com
developers.fireblocks.com
hireblocks.fireblocks.com
vault.fireblocks.com
amex-client-e2.fireblocks.com
fleetdm.fireblocks.com
eu.status.fireblocks.com
tabsrvprod.fireblocks.com
info.fireblocks.com
survey.fireblocks.com
t4dtd.fireblocks.com
fleetdm-test.fireblocks.com
www.docs.fireblocks.com
```

garage.fireblocks.com
www.fireblocks.com
amex-client-e3.fireblocks.com
www.amex-client-e2.fireblocks.com
api-reference.fireblocks.com

tabsrvtst.fireblocks.com
checkout.fireblocks.com
emails.fireblocks.com
vendors.fireblocks.com
www.portal.fireblocks.com
sandbox.status.fireblocks.com
ncw-developers.fireblocks.com
eu2.status.fireblocks.com
tracking.fireblocks.com
referral.fireblocks.com
spark.fireblocks.com
amex-client-e1.fireblocks.com
console-fleetdm.fireblocks.com
www.tabsrvprod.fireblocks.com
tokenization.fireblocks.com
www.tokenization.fireblocks.com
docs.fireblocks.com
trust.fireblocks.com
portal.fireblocks.com
status.fireblocks.com
shopit.fireblocks.com
fb-bt-man.fireblocks.com
www.vault.fireblocks.com
www.tabsrvtst.fireblocks.com
component-registry-gcpshell-ext.fireblocks.com
marketplaceapi.gcp.fireblocks.com
developers.fireblocks.com
hireblocks.fireblocks.com
vault.fireblocks.com
amex-client-e2.fireblocks.com
fleetdm.fireblocks.com
eu.status.fireblocks.com
tabsrvprod.fireblocks.com
info.fireblocks.com
survey.fireblocks.com
t4dtd.fireblocks.com
fleetdm-test.fireblocks.com
www.docs.fireblocks.com
www.amex-client-e1.fireblocks.com
www.amex-client-e3.fireblocks.com
blog.fireblocks.com
community.fireblocks.com
events.fireblocks.com

b. Live Subdomain Discovery

Tool : httpx: livesub_results.txt

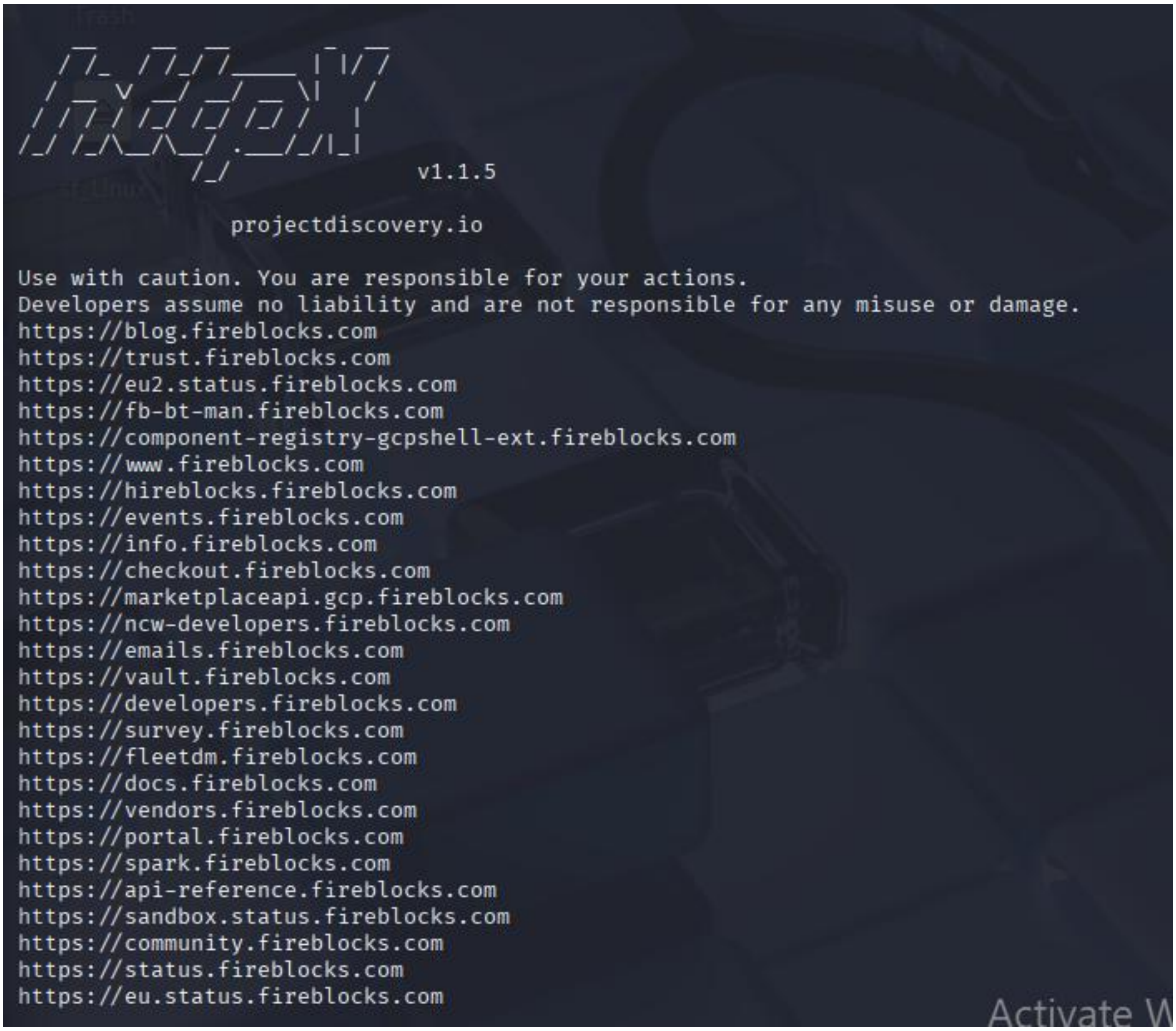
Code : httpx-toolkit -l subfinder_result_fireblock.txt -o livesub_results.txt

Explanation:

httpx-toolkit - run the httpx tool

-*l subfinder_result_fireblock.txt* – mention the file containing input

-*o livesub_results.txt* – mention the file which should write the output



```
    __    __  __       _  __
   / /_  / /_/ /_____ | |/ /
  / __ \/ __/ __/ __ \|   /
 / / / / /_/ /_/ /_/ /   |
/_/ /_/\__/\__/ .___/_/|_|
             /_/              v1.1.5

                projectdiscovery.io

Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible for any misuse or damage.
https://blog.fireblocks.com
https://trust.fireblocks.com
https://eu2.status.fireblocks.com
https://fb-bt-man.fireblocks.com
https://component-registry-gcpshell-ext.fireblocks.com
https://www.fireblocks.com
https://hireblocks.fireblocks.com
https://events.fireblocks.com
https://info.fireblocks.com
https://checkout.fireblocks.com
https://marketplaceapi.gcp.fireblocks.com
https://ncw-developers.fireblocks.com
https://emails.fireblocks.com
https://vault.fireblocks.com
https://developers.fireblocks.com
https://survey.fireblocks.com
https://fleetdm.fireblocks.com
https://docs.fireblocks.com
https://vendors.fireblocks.com
https://portal.fireblocks.com
https://spark.fireblocks.com
https://api-reference.fireblocks.com
https://sandbox.status.fireblocks.com
https://community.fireblocks.com
https://status.fireblocks.com
https://eu.status.fireblocks.com
```

https://blog.fireblocks.com
https://trust.fireblocks.com
https://eu2.status.fireblocks.com
https://fb-bt-man.fireblocks.com
https://component-registry-gcpshell-ext.fireblocks.com
https://www.fireblocks.com
https://hireblocks.fireblocks.com
https://events.fireblocks.com
https://info.fireblocks.com
https://checkout.fireblocks.com
https://marketplaceapi.gcp.fireblocks.com
https://ncw-developers.fireblocks.com
https://emails.fireblocks.com
https://vault.fireblocks.com
https://developers.fireblocks.com
https://survey.fireblocks.com
https://fleetdm.fireblocks.com
https://docs.fireblocks.com
https://vendors.fireblocks.com
https://portal.fireblocks.com
https://spark.fireblocks.com
https://api-reference.fireblocks.com
https://sandbox.status.fireblocks.com
https://community.fireblocks.com
https://status.fireblocks.com
https://eu.status.fireblocks.com

c. IP Discovery

Tool: nslookup: nslookup_result.txt

Code: since we whole file with subdomains, to find IP addresses using “nslookup“ we need to make a loop until all the Ips of all the subdomains are found.

```
while read sub; do
 echo "Looking up: $sub" >> nslookup_result.txt
  nslookup "$sub" | awk '/^Name:|^Address:/' >> nslookup_result.txt
  echo "------------------------" >> nslookup_result.txt
done < livesub_results.txt
```

Explanation:

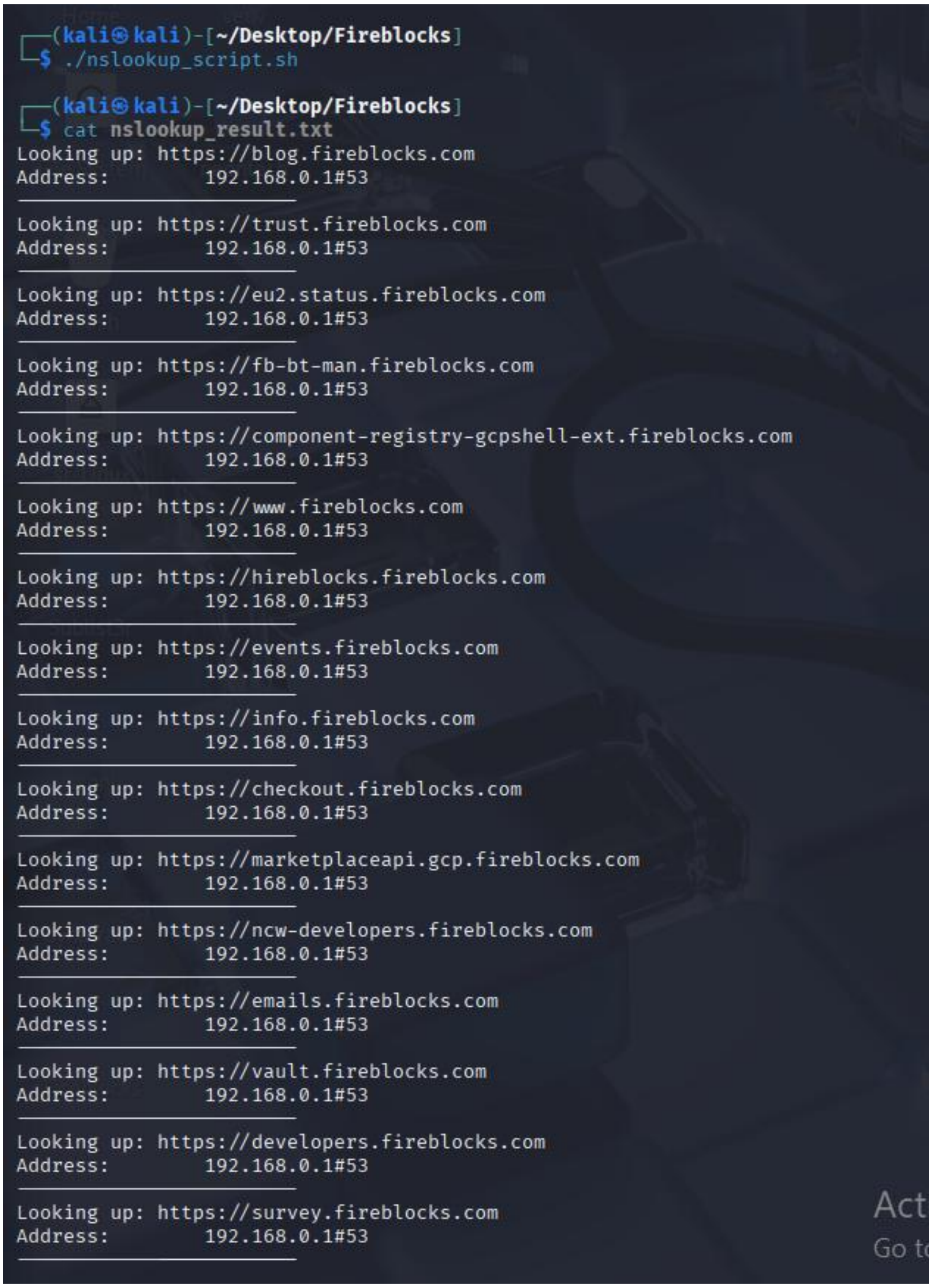
While read sub; do - start of the loop

Echo “Looking up: $sub”>>nslookup_result.txt - print message “Looking up: subdomain” into the file “*nslookup_result*.txt”

nslookup “$sub” | awk ‘/^Name:|^Address:/’ >> nslookup_result.txt - run the nslookup command

echo “___________________” >> nslookup_result.txt - separate one subdomain details from another

done < livesub_results.txt - End the loop and continue until the lines in the livesub_results.txt



```
┌──(kali㉿kali)-[~/Desktop/Fireblocks]
└─$ ./nslookup_script.sh

┌──(kali㉿kali)-[~/Desktop/Fireblocks]
└─$ cat nslookup_result.txt
Looking up: https://blog.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://trust.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://eu2.status.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://fb-bt-man.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://component-registry-gcpshell-ext.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://www.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://hireblocks.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://events.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://info.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://checkout.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://marketplaceapi.gcp.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://ncw-developers.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://emails.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://vault.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://developers.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
Looking up: https://survey.fireblocks.com
Address:        192.168.0.1#53
────────────────────────
```

IP list:

```
Looking up: https://blog.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://trust.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://eu2.status.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://fb-bt-man.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://component-registry-gcpshell-ext.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://www.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://hireblocks.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://events.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://info.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://checkout.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://marketplaceapi.gcp.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://ncw-developers.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://emails.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://vault.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://developers.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://survey.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://fleetdm.fireblocks.com
Address:        192.168.0.1#53
------------------------
Looking up: https://docs.fireblocks.com
Address:        192.168.0.1#53
------------------------
```

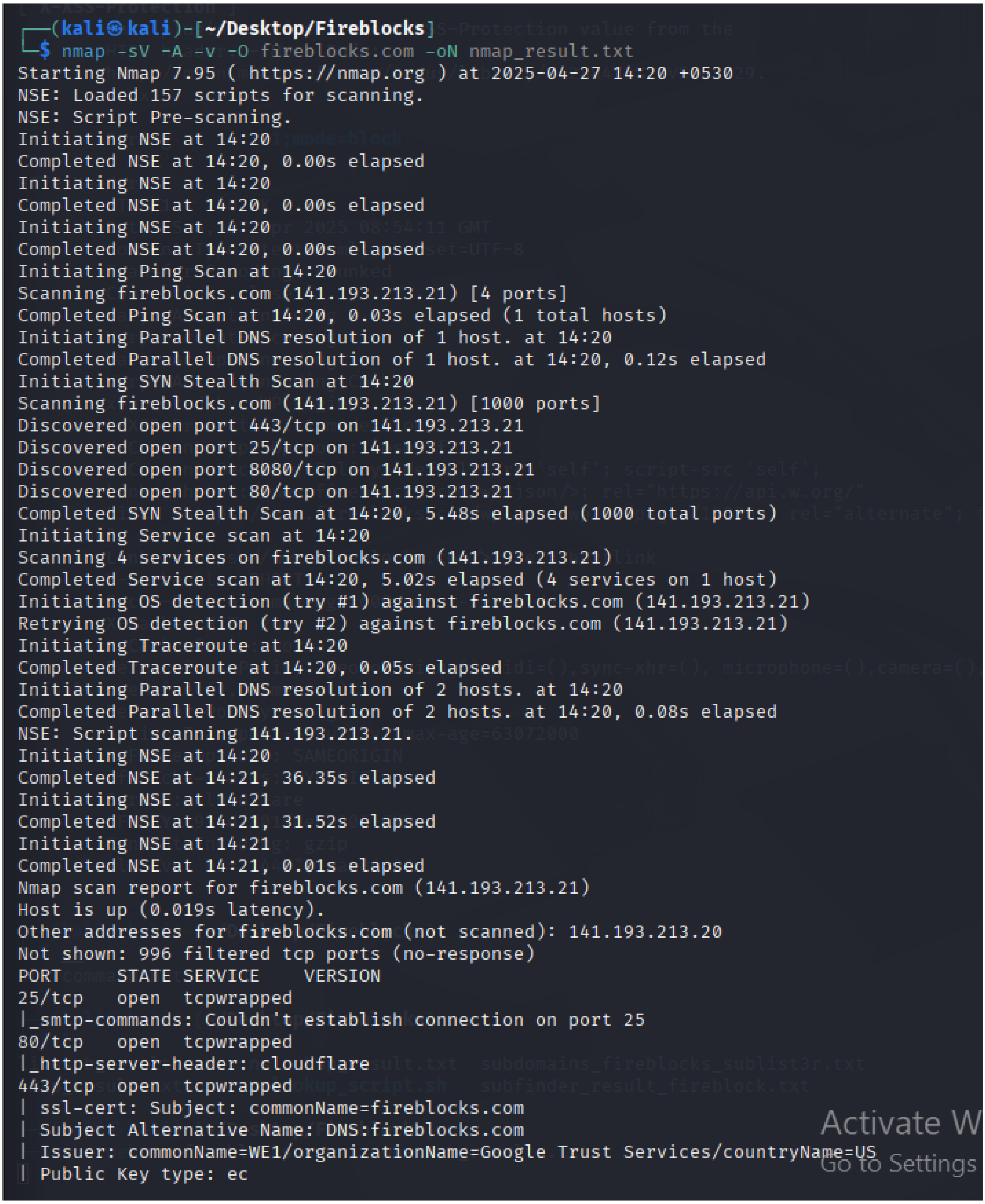
d. Open Ports

Tool: nmap: nmap_result.txt

Code: nmap -sV -A -v -O fireblocks.com -oN nmap_results.txt

Explanation:

nmap - start the tool
-sV - Service and version detection
-A - OS detection, version detection, script scanning
-v - increase verbosity level
-O - Os detection
- *fireblocks.com* - target website
-oN nmap_results.txt - result in an output text file



```
┌──(kali㉿kali)-[~/Desktop/Fireblocks]
└─$ nmap -sV -A -v -O fireblocks.com -oN nmap_result.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 14:20 +0530
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:20
Completed NSE at 14:20, 0.00s elapsed
Initiating NSE at 14:20
Completed NSE at 14:20, 0.00s elapsed
Initiating NSE at 14:20
Completed NSE at 14:20, 0.00s elapsed
Initiating Ping Scan at 14:20
Scanning fireblocks.com (141.193.213.21) [4 ports]
Completed Ping Scan at 14:20, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:20
Completed Parallel DNS resolution of 1 host. at 14:20, 0.12s elapsed
Initiating SYN Stealth Scan at 14:20
Scanning fireblocks.com (141.193.213.21) [1000 ports]
Discovered open port 443/tcp on 141.193.213.21
Discovered open port 25/tcp on 141.193.213.21
Discovered open port 8080/tcp on 141.193.213.21
Discovered open port 80/tcp on 141.193.213.21
Completed SYN Stealth Scan at 14:20, 5.48s elapsed (1000 total ports)
Initiating Service scan at 14:20
Scanning 4 services on fireblocks.com (141.193.213.21)
Completed Service scan at 14:20, 5.02s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against fireblocks.com (141.193.213.21)
Retrying OS detection (try #2) against fireblocks.com (141.193.213.21)
Initiating Traceroute at 14:20
Completed Traceroute at 14:20, 0.05s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 14:20
Completed Parallel DNS resolution of 2 hosts. at 14:20, 0.08s elapsed
NSE: Script scanning 141.193.213.21.
Initiating NSE at 14:20
Completed NSE at 14:21, 36.35s elapsed
Initiating NSE at 14:21
Completed NSE at 14:21, 31.52s elapsed
Initiating NSE at 14:21
Completed NSE at 14:21, 0.01s elapsed
Nmap scan report for fireblocks.com (141.193.213.21)
Host is up (0.019s latency).
Other addresses for fireblocks.com (not scanned): 141.193.213.20
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
25/tcp   open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp   open  tcpwrapped
|_http-server-header: cloudflare
443/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=fireblocks.com
| Subject Alternative Name: DNS:fireblocks.com
| Issuer: commonName=WE1/organizationName=Google Trust Services/countryName=US
| Public Key type: ec
```

e. Used Technologies

Tool: whatweb - whatweb_results.txt

Code: whatweb -v fireblocks.com > whatweb_result.txt

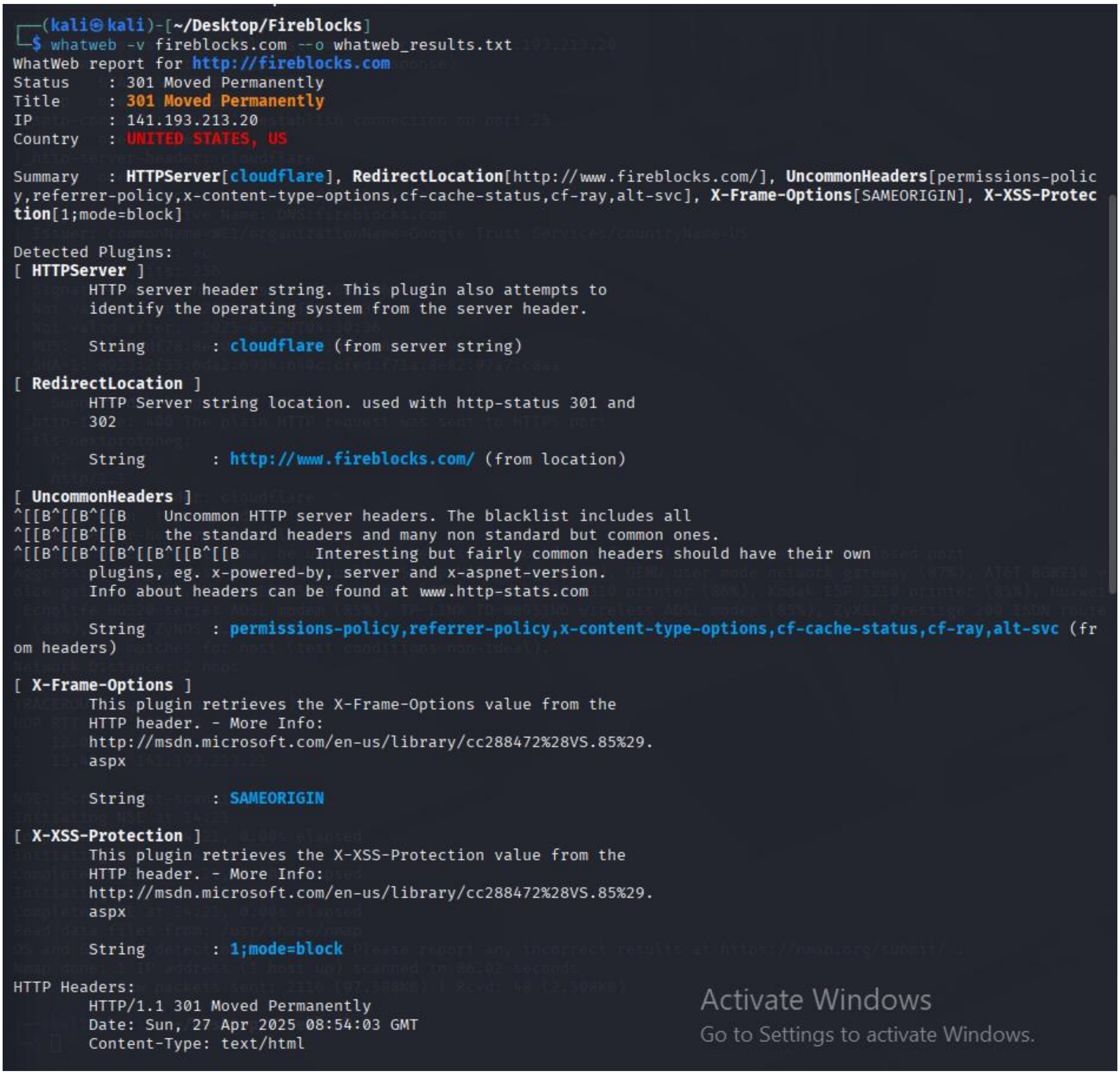
Explanation:

whatweb - start whatweb tool

-v - verbose

fireblocks - target website

> *whatweb_result.txt* - file with the output

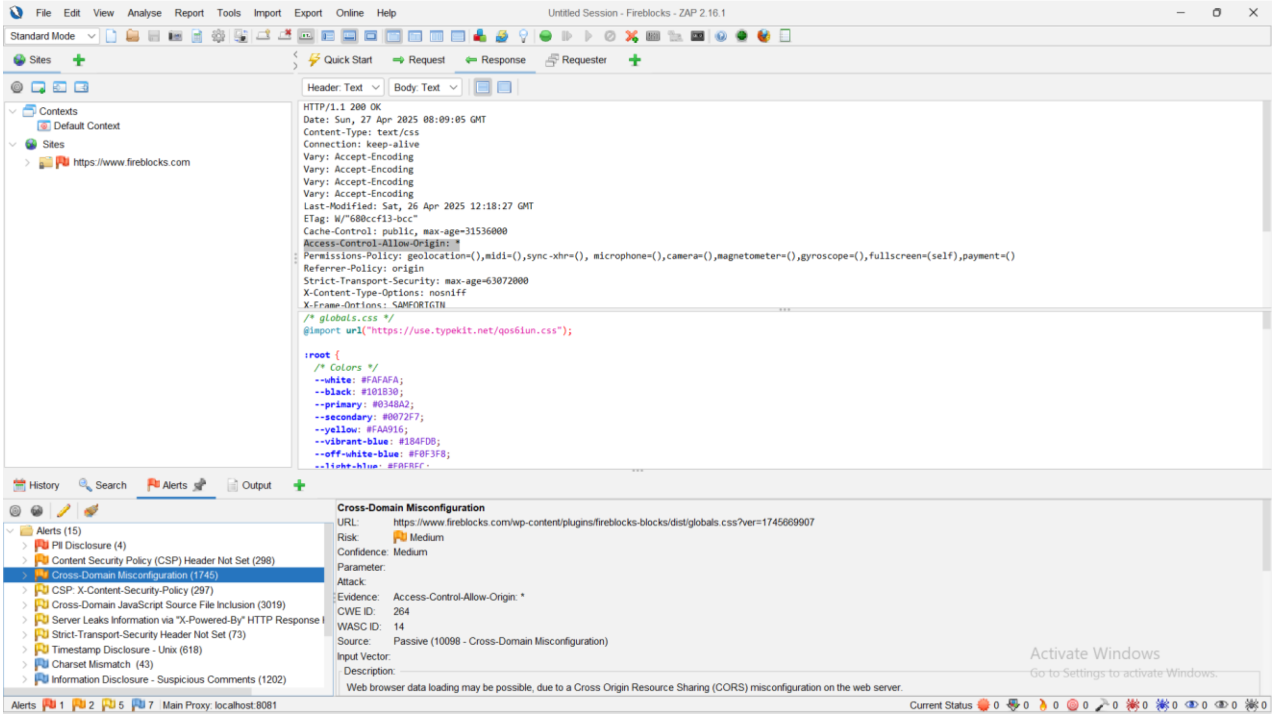


```
┌──(kali㉿kali)-[~/Desktop/Fireblocks]
└─$ whatweb -v fireblocks.com --o whatweb_results.txt
WhatWeb report for http://fireblocks.com
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 141.193.213.20
Country   : UNITED STATES, US

Summary   : HTTPServer[cloudflare], RedirectLocation[http://www.fireblocks.com/], UncommonHeaders[permissions-polic
y,referrer-policy,x-content-type-options,cf-cache-status,cf-ray,alt-svc], X-Frame-Options[SAMEORIGIN], X-XSS-Protec
tion[1;mode=block]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : cloudflare (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : http://www.fireblocks.com/ (from location)

[ UncommonHeaders ]
^[[B^[[B^[[B    Uncommon HTTP server headers. The blacklist includes all
^[[B^[[B^[[B    the standard headers and many non standard but common ones.
^[[B^[[B^[[B^[[B^[[B^[[B        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : permissions-policy,referrer-policy,x-content-type-options,cf-cache-status,cf-ray,alt-svc (fr
om headers)

[ X-Frame-Options ]
        This plugin retrieves the X-Frame-Options value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : SAMEORIGIN

[ X-XSS-Protection ]
        This plugin retrieves the X-XSS-Protection value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : 1;mode=block

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Date: Sun, 27 Apr 2025 08:54:03 GMT
        Content-Type: text/html
```

3. Step 02: Scanning and vulnerability identification

a. Identify Potential Vulnerabilities

Tool : OWASP ZAP
Vulnerability : Cross Domain Misconfiguration



```
HTTP/1.1 200 OK
Date: Sun, 27 Apr 2025 08:09:05 GMT
Content-Type: text/css
Connection: keep-alive
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Accept-Encoding
Last-Modified: Sat, 26 Apr 2025 12:18:27 GMT
ETag: W/"680ccf13-bcc"
Cache-Control: public, max-age=31536000
Access-Control-Allow-Origin: *
Permissions-Policy: geolocation=(),midi=(),sync-xhr=(), microphone=(),camera=(),magnetometer=(),gyroscope=(),fullscreen=(self),payment=()
Referrer-Policy: origin
Strict-Transport-Security: max-age=63072000
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

```
/* globals.css */
@import url("https://use.typekit.net/qos6iun.css");

:root {
  /* Colors */
  --white: #FAFAFA;
  --black: #101B30;
  --primary: #0348A2;
  --secondary: #0072F7;
  --yellow: #FAA916;
  --vibrant-blue: #184FDB;
  --off-white-blue: #F0F3F8;
  --light-blue: #F0FBFC;
```

Alerts (15)
- PII Disclosure (4)
- Content Security Policy (CSP) Header Not Set (298)
- Cross-Domain Misconfiguration (1745)
- CSP: X-Content-Security-Policy (297)
- Cross-Domain JavaScript Source File Inclusion (3019)
- Server Leaks Information via "X-Powered-By" HTTP Response I
- Strict-Transport-Security Header Not Set (73)
- Timestamp Disclosure - Unix (618)
- Charset Mismatch (43)
- Information Disclosure - Suspicious Comments (1202)

Cross-Domain Misconfiguration
URL: https://www.fireblocks.com/wp-content/plugins/fireblocks-blocks/dist/globals.css?ver=1745669907
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:
Description:
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

Alerts 1 2 5 7 Main Proxy: localhost:8081
Current Status 0 0 0 0 0 0 0 0 0 0 0

Cross Domain Misconfiguration:

URL: https://www.fireblocks.com/wp-content/plugins/fireblocks-blocks/dist/globals.css?ver=1745669907
Risk: Medium
Confidential: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:

- Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server..
- Other Info: The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
- Solution: Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
- Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
- Reference: https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

- Alert Tags:
  - OWASP_2021_A01: https://owasp.org/Top10/A01_2021-Broken_Access_Control/
  - OWASP_2017_A05: https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html
  - CWE-264: https://cwe.mitre.org/data/definitions/264.html

b. Cross Domain Misconfiguration

Cross Domain Misconfiguration occurs when a web application improperly trusts and communicates with untrusted domains, or misconfigures policies that control cross-origin interactions (like CORS - Cross-Origin Resource Sharing). This flaw can allow attackers to bypass the same-origin policy, leading to unauthorized access, data leaks, and even account hijacking by exploiting trust between domains.

Cause of Cross Domain Misconfiguration website:

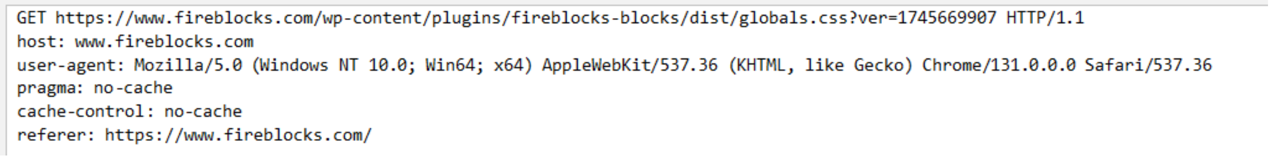
- Setting overly permissive CORS policies (e.g., Access-Control-Allow-Origin: *)
- Allowing credentials (cookies, HTTP authentication) in CORS requests to any origin
- Trusting user-supplied or dynamically constructed origins without proper validation
- Incorrect configuration of postMessage between windows or frames
- Enabling cross-domain access for sensitive APIs without strict validation
- Lack of strict domain whitelisting or misconfigured subdomains

Propositions to Mitigation or Fix:

- Implement Strict CORS Policies: Only allow specific trusted domains instead of using wildcards
- Validate Origins Carefully: Never dynamically reflect user-supplied Origin headers without validation
- Avoid Sending Credentials Unnecessarily: Use Access-Control-Allow-Credentials: true only when absolutely necessary and with trusted origins
- Secure Cross-Origin Communications: Validate messages carefully when using postMessage APIs
- Regular Configuration Reviews: Regularly audit CORS and cross-domain settings during security assessments
- Use Subdomain Isolation: Separate sensitive parts of applications onto different, carefully managed subdomains
- Employ Web Application Firewalls (WAFs): Use WAFs to detect and block misconfigured CORS behavior

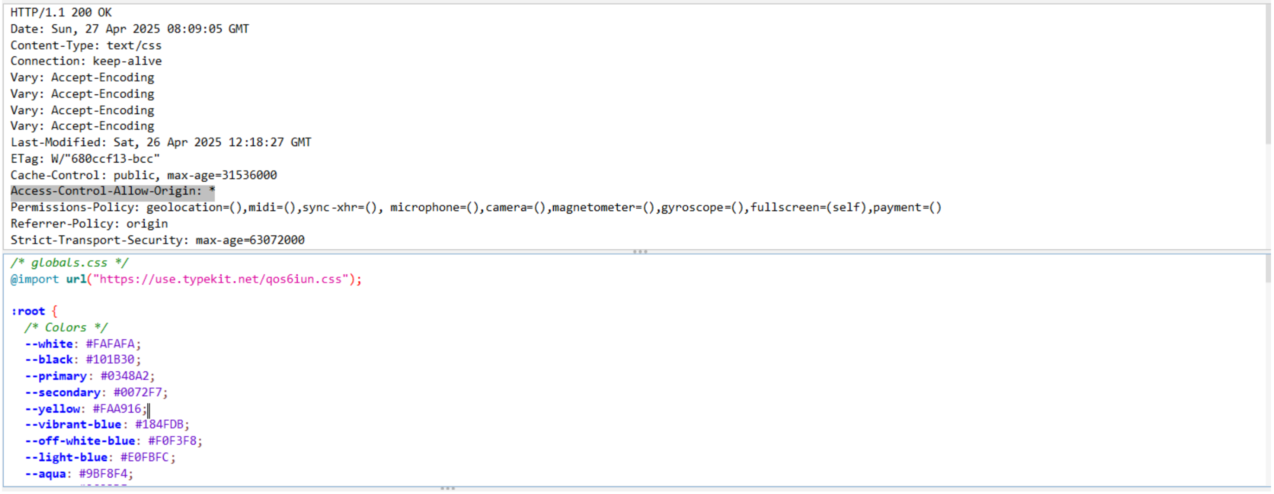
4. Step 03: Exploitation and Validation

Request:



```
GET https://www.fireblocks.com/wp-content/plugins/fireblocks-blocks/dist/globals.css?ver=1745669907 HTTP/1.1
host: www.fireblocks.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://www.fireblocks.com/
```

Response:



```
HTTP/1.1 200 OK
Date: Sun, 27 Apr 2025 08:09:05 GMT
Content-Type: text/css
Connection: keep-alive
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Accept-Encoding
Last-Modified: Sat, 26 Apr 2025 12:18:27 GMT
ETag: W/"680ccf13-bcc"
Cache-Control: public, max-age=31536000
Access-Control-Allow-Origin: *
Permissions-Policy: geolocation=(),midi=(),sync-xhr=(), microphone=(),camera=(),magnetometer=(),gyroscope=(),fullscreen=(self),payment=()
Referrer-Policy: origin
Strict-Transport-Security: max-age=63072000
```

```
/* globals.css */
@import url("https://use.typekit.net/qos6iun.css");

:root {
  /* Colors */
  --white: #FAFAFA;
  --black: #101B30;
  --primary: #0348A2;
  --secondary: #0072F7;
  --yellow: #FAA916;
  --vibrant-blue: #184FDB;
  --off-white-blue: #F0F3F8;
  --light-blue: #E0FBFC;
  --aqua: #9BF8F4;
```

5. Step 04: Mitigation / Fix

Immediate Mitigation Actions:
1. Restrict CORS to Trusted Domains.
2. Configure CORS at the CDN level.

Long Term Prevention:
1. For static files avoid CORS unless necessary
2. For APIs use authentication even with CORS and implement CSRF tokens for state-changing requests.