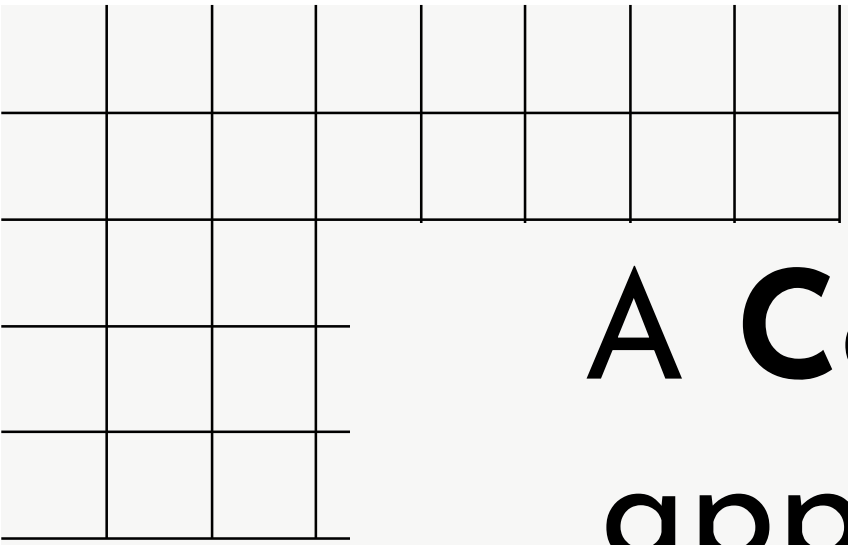
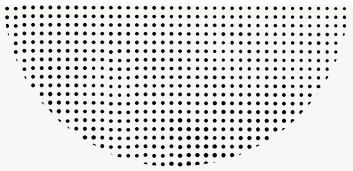
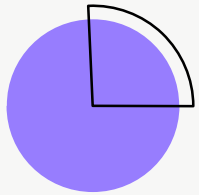




A **Containerized** approach to **API deception** using **Kubernetes**



SCOPO DEL PROGETTO

DECEPTION

Creazione e implementazione di un sistema di deception

DATA COLLECTION

Collezionare, categorizzare e analizzare i dati ricevuti, creare metriche per alimentare sistemi di difesa efficaci

PLUG & PLAY

Uso di Kubernetes per fare il deploy facilmente tramite un unico file ed estendibile al proprio webserver

DECEPTION

- Implementazione di elementi ingannevoli
- Generazione di un alto numero di falsi positivi
- Perdita di tempo e saturazione della memoria degli attaccanti
- Efficace contro attaccanti inesperti
- Nasconde il vero servizio esposto
- Non mette in sicurezza i servizi, servono anche altre misure

SCENARIO

API Server di un servizio di E-Commerce, ma altamente configurabili

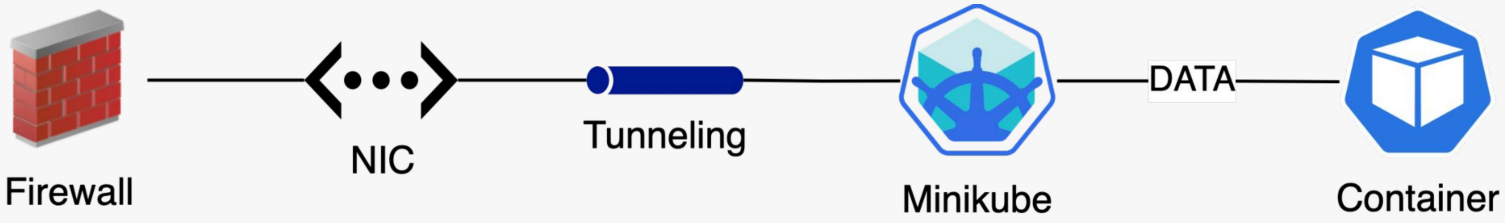
/API/V2/USERS	La finta lista di utenti con username email e password in hash
/API/V2/PRODUCTS	La finta lista di prodotti disponibili, con le loro quantità
/API/V2/ORDERS	La finta lista di ordini, con la possibilità di crearli

Risorse esposte (accessibili via API e autenticazione):

KUBERNETES

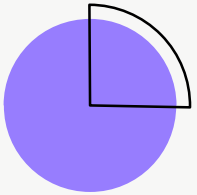
Grazie a Kubernetes il deploy può essere automatizzato, esteso e facilmente configurato a runtime. La divisione delle risorse presenti è nel seguente modo

POD	SERVICES	JOB	CONFIGMAP
Server	Networking	Delivery Dati	Configurazione

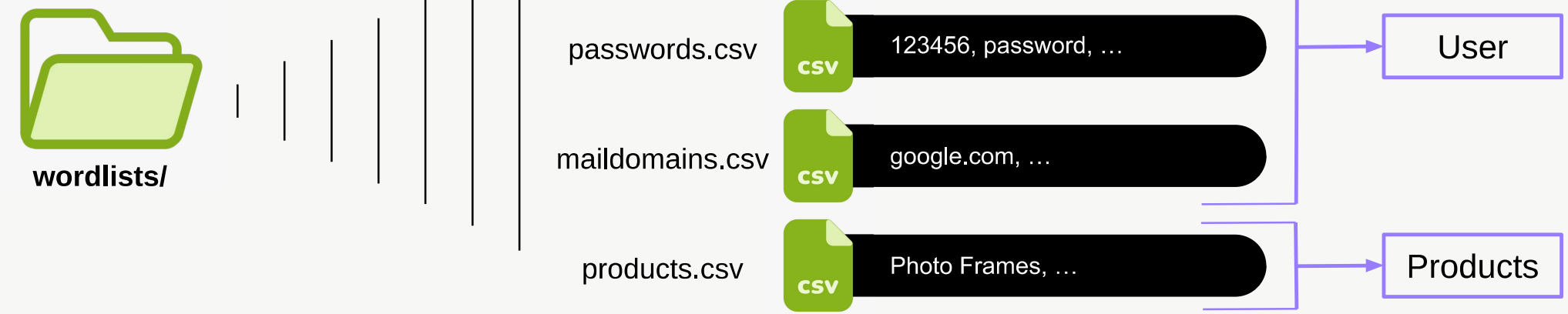


DATA GENERATION

- Dati falsi creati a partire da wordlist pubbliche e comunemente usate dagli attaccanti (es: rockyou.txt)
- API verosimili che espongono finti dati sensibili, per far cadere l’attaccante in Rabbit Hole
- Combinazione casuale di dati generata a runtime, per aumentare l’entropia della risposta
- Casualità nella lunghezza della risposta: Content Length di diversa lunghezza, pagina sempre diversa
- Link generati casualmente



STRUTTURA WORDLIST



Wordlist configurabile a runtime tramite Dockerfile e ConfigMap

OPENAPI SERVER

JAVA APPLICATION

- Applicazione scritta in Java che implementa le funzionalità
- Definizione API tramite annotazioni

```java
@GET
@Produces(MediaType.APPLICATION_JSON)
@RolesAllowed({"admin","dev"})
@Path("info")
public Set<UserInfo> getUsersInfo(){
  ...
}
```

QUARKUS ENGINE

- Application Server multi-threaded gestito da Vert.x core
- Generazione dinamica API tramite estensione SmallRye OpenAPI

OpenAPI v3 specification

```yaml
openapi: 3.0.3
info:
  title: openapi-oauth-client API
  version: 1.0.0-SNAPSHOT
paths:
  /api/v2/orders:
    get:
      tags:
      - Order Creation
      responses:
        "200":
          description: OK
          content:
            application/json:
              schema:
                type: array
                items:
                  type: string
        "401":
          description: Not Authorized
...
```

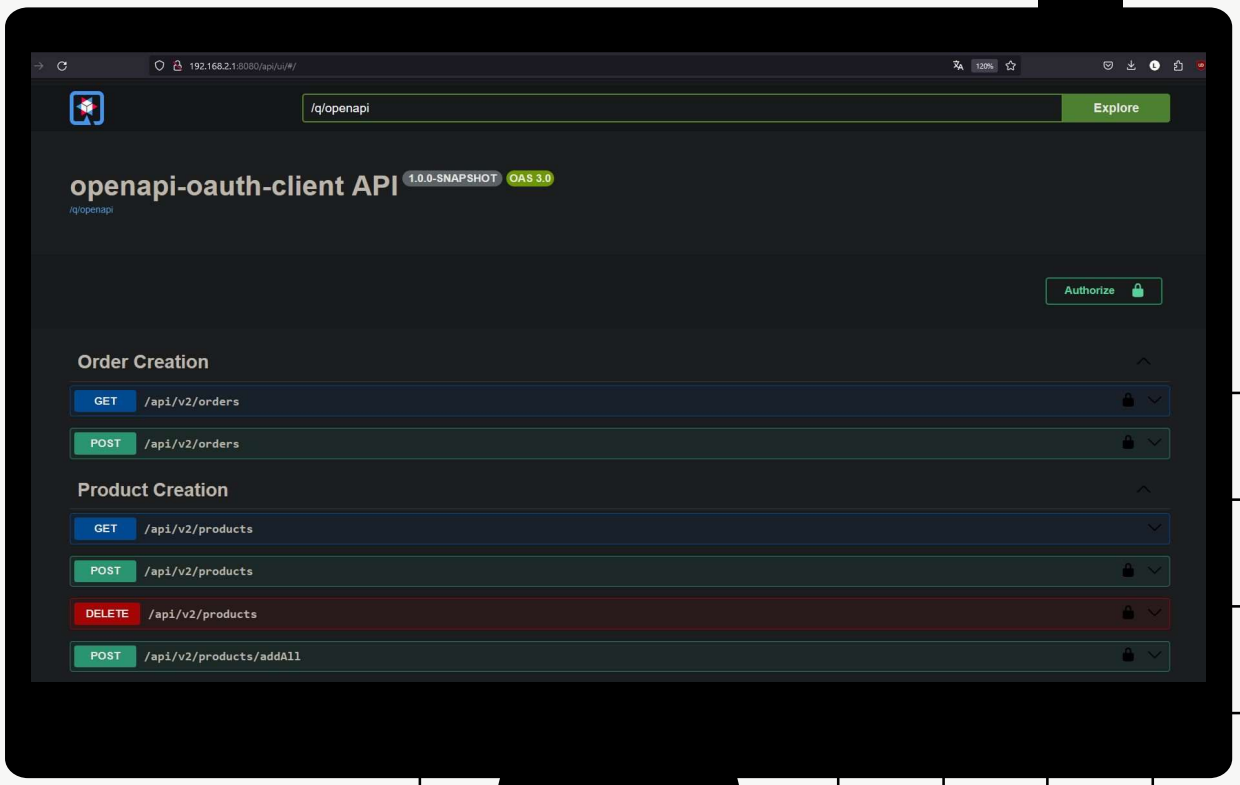
SWAGGER UI

Specifica OpenAPI

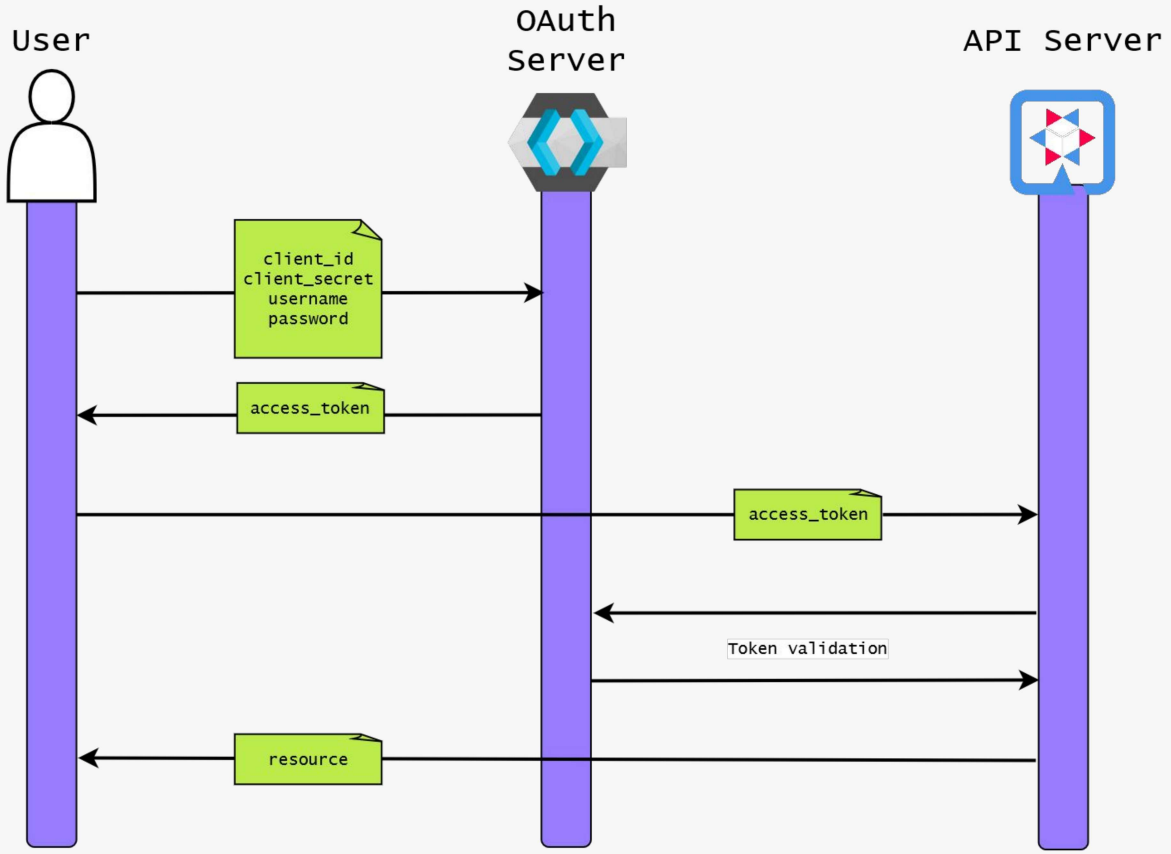
Interfaccia web dinamica

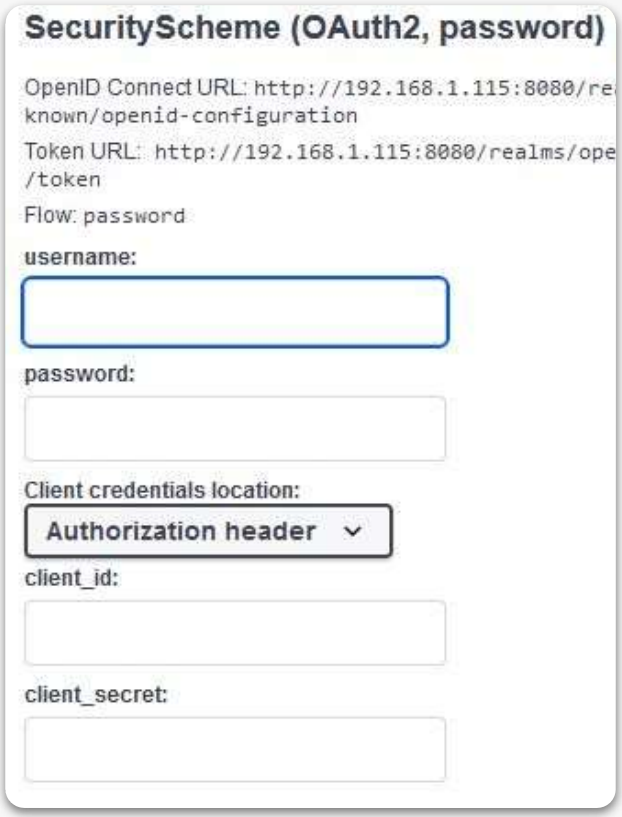
Autenticazione

VIsualizzare e testare API



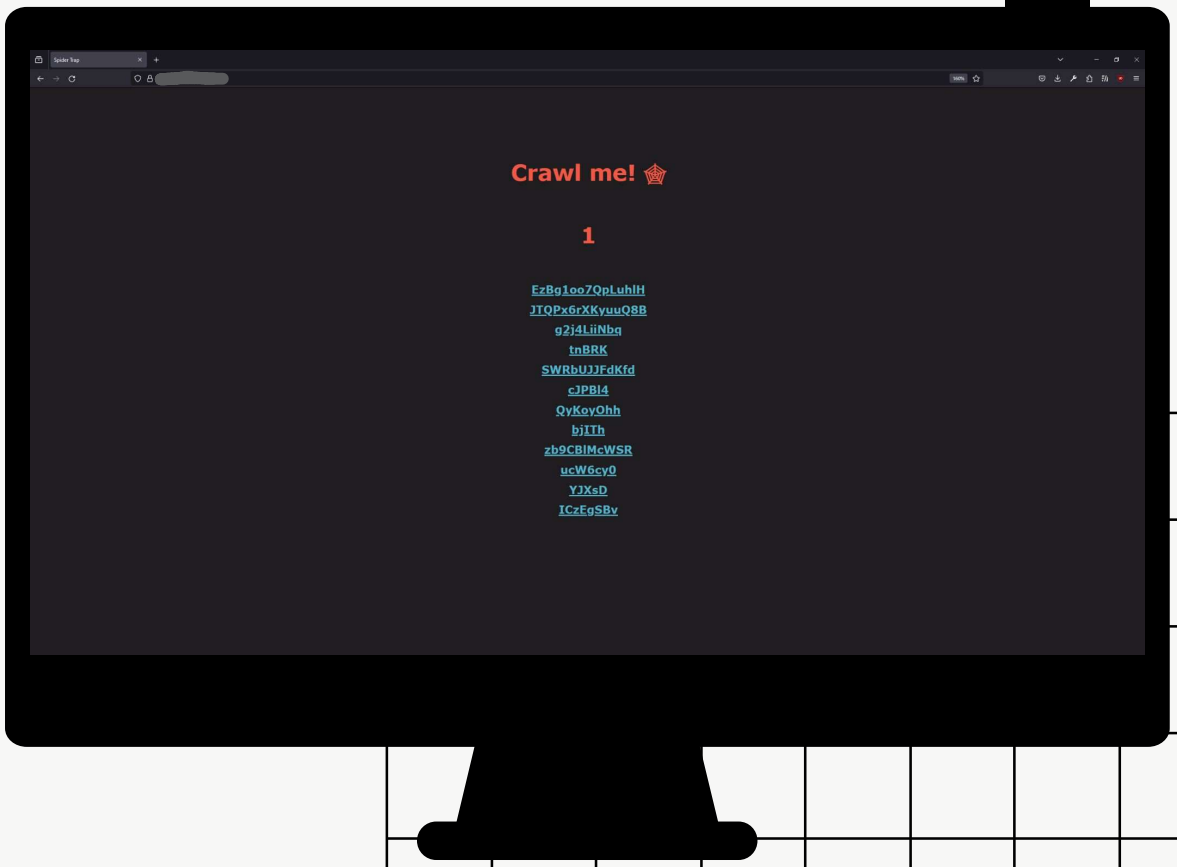
OPENID CONNECT E OAUTH





DECEPTION SERVER

- Il server di deception è raggiungibile tramite qualunque path nel webserver.
- Genera N link di lunghezza casuale
- Non restituisce mai errore



RUNTIME CONFIGURATION

- Configurazione tramite ConfigMap di tutto l'ambiente, compresi i parametri per aggaciarsi al server OAuth.
- Un' altra ConfigMap che configura servizio che si espone e che si vuole proteggere, tramite un deploy NGINX.

```
apiVersion: v1
data:
  QUARKUS_API_SVC: "oauth-quarkus"
  API_SERVER_PORT: "<PORT>"
  API_SERVER_FULL: "https://<SERVER>/api/v2"
  API_SERVER_URL: "https://<SERVER>"
  API_SERVER_PATH: "/api/v2/<API>"
  WORDLIST_PATH: "<PATH-TO-WORDLIST>"
  CHAR_SPACE:
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"
  AUTH_SERVER_URL: "https://<SERVER>/keycloak/realms/openapi-
oauth/protocol/openid-connect/token"
  CLIENT_ID: "<CLIENT-ID>"
  CLIENT_SECRET: "<CLIENT-SECRET>"
  USERNAME: "<USERNAME>"
  PASSWORD: "<PASSWORD>"
  QUARKUS_OIDC_AUTH_SERVER_URL: "https://<SERVER>/keycloak/realms
/openapi-oauth"
  QUARKUS_LOG_LEVEL: "DEBUG"
kind: ConfigMap
metadata:
  creationTimestamp: null
  name: api-config
```

SUPERFICIE D'ATTACCO

- L'autenticazione OAuth viene bucata con attacchi a dizionario, l'attaccante può leggere tutte le API autenticate.

- La compagnia che mantiene il WebServer fa il push di dati sensibili su GitHub e l'attaccate riesce a risalire al Bearer Token usando filtri e cercando nella history dei commit.

- L'attaccante dispone di tecnologia in grado di crackare il token o sfrutta una vulnerabilità per bypassarlo

ATTACCO AGLI UTENTI


```
"email": "charles_white@yahoo.it",
"name": "Charles",
"password":
"JDYkVWs4U1ZHTHNCdVNtRDc1UiRWclVLVnJGSVdPeDlYS2wvSkVpbWhkamVxU1pPQS5IdFJ0OWF1azNvbzkySkttQTN5SEtmRjhsSHZINE5mcTJ0YWE3bEN0Y0h5d0JHUzhQckxzNUg1",
"registrationDate": "2017-02-01T08:14:40",
"surname": "White",
"username": "c.white"
```

```
c.white:$6$Uk8SVGLsBuSmD75R$VrUKVrFIWOx9XKl/JEimhdjeqSZOA.HtRt9auk3oo92JKmA3yHKfF8lHvH4Nfq2taa7lCtcHywBGS8PrLs5H5.
```

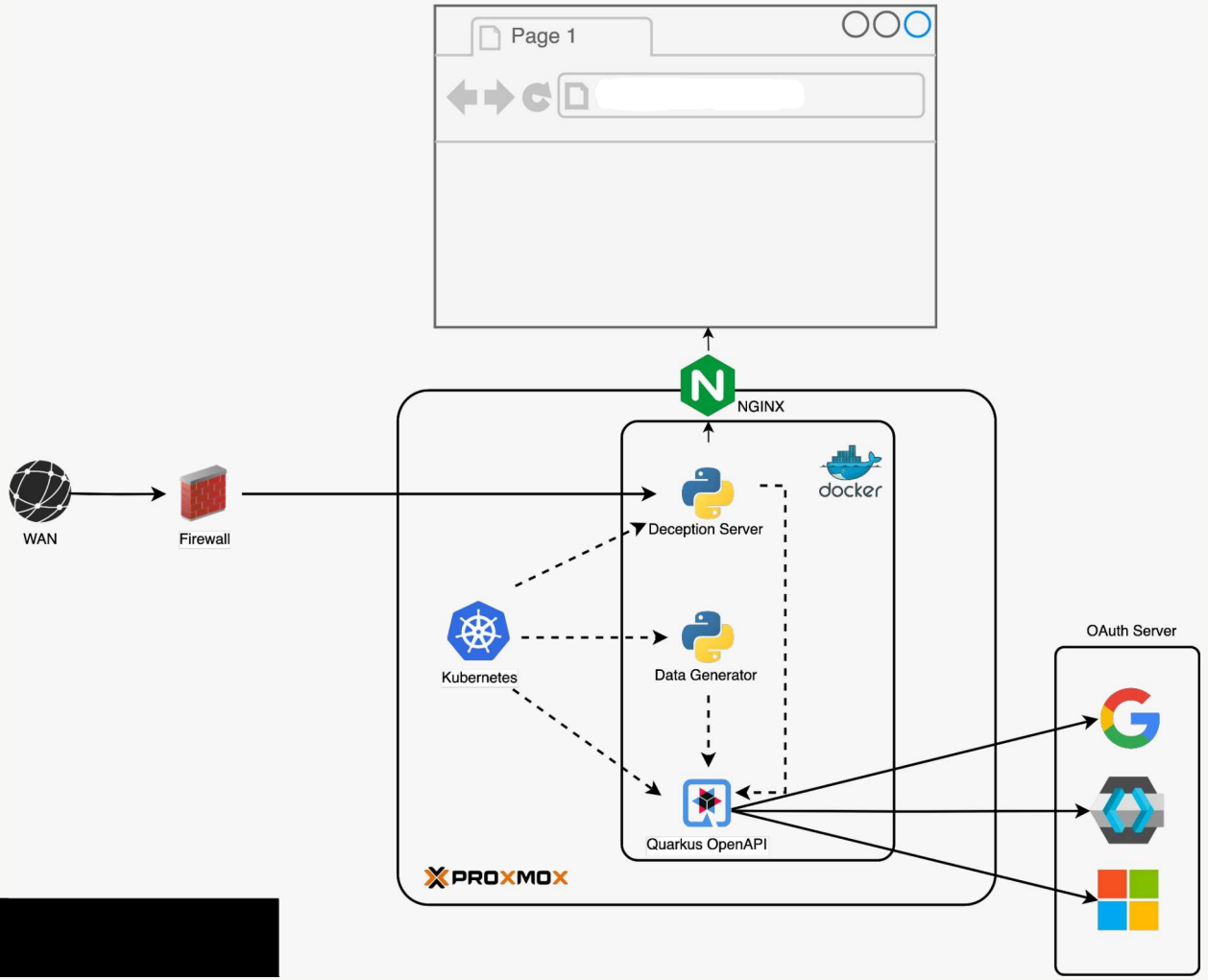

SHA512CRYPT

Phishing

Password Cracking

Password Spraying

ARCHITETTURA



PROXY

```
server {
        listen 443 ssl default_server;
        listen [::]:443 ssl default_server;

        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-Proto $scheme;

        ssl_certificate         /etc/ssl/servercert.pem;
        ssl_certificate_key    /etc/ssl/servercert.key;

        server_name servername.com;
        root /var/www/html;

        location /api/ {
                proxy_pass http://quarkus-oauth/api/;
        }
        location /q/openapi/ {
                proxy_pass http://quarkus-oauth/q/openapi/;
        }
        location /realms/ {
                proxy_pass http://keycloak-server/realms/;
        }
        location /admin/ {
                proxy_pass http://keycloak-server/admin/;
        }
        location /super-secret-and-protected-application/ {
                proxy_pass http://real-server/;
        }
        location / {
                proxy_pass http://deception-server/;
        }
}
```

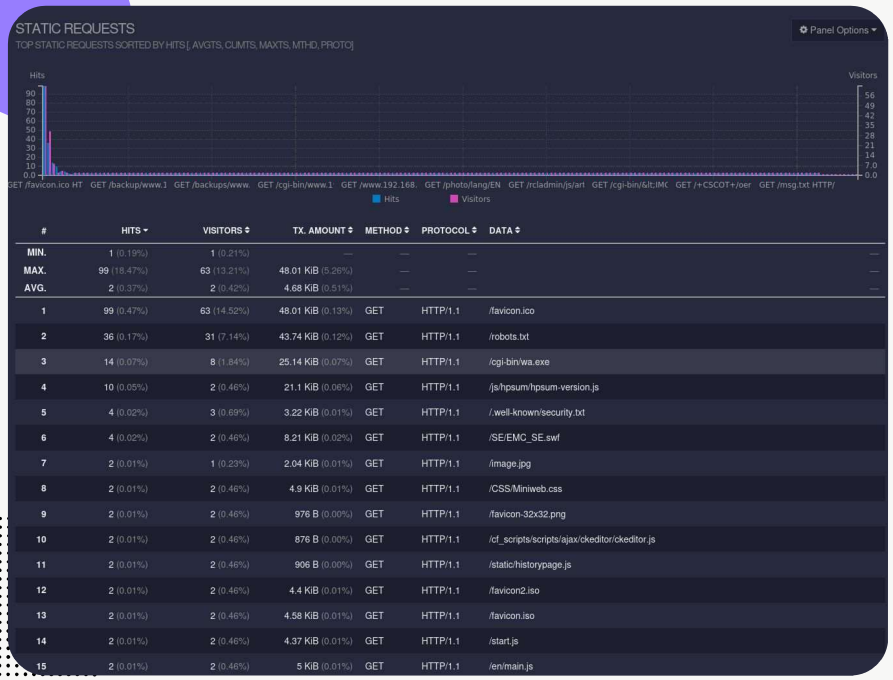
ENUM

GOBUSTER
DIRBUSTER
FEROXBUSTER

```
200      GET       18l      115w     2264c https://deception-server/97pjrSOwgLFL
200      GET       16l      103w     2066c https://deception-server/C9NjIxL5k2FDr2
200      GET       17l      108w     2115c https://deception-server/6QEKdaoGJC1
200      GET       21l      138w     2745c https://deception-server/4BIs6
200      GET       18l      115w     2250c https://deception-server/zGGV7iaIEFOFQhR
200      GET       19l      122w     2409c https://deception-server/jG963jT0jE
200      GET       20l      129w     2534c https://deception-server/catalogsearch
200      GET       15l       94w     1795c https://deception-server/aa78jsQ1ybqxL8D
200      GET       16l      101w     1936c https://deception-server/yjfmwuMEAzlHd
200      GET       17l      108w     2113c https://deception-server/jmLP5pZr
200      GET       18l      115w     2242c https://deception-server/jUGFmAK7eNEEQBq
200      GET       17l      110w     2263c https://deception-server/cayd0R
200      GET       18l      115w     2218c https://deception-server/mLmrV63MMoQZ
200      GET       19l      122w     2347c https://deception-server/graphics
200      GET       18l      115w     2208c https://deception-server/HGoyf4o
200      GET       15l       94w     1759c https://deception-server/AOmdIDlOIJCGW
200      GET       18l      115w     2220c https://deception-server/i
200      GET       16l      101w     1922c https://deception-server/MMWIP
200      GET       20l      129w     2544c https://deception-server/kOxiZ
200      GET       16l      103w     2056c https://deception-server/swf
200      GET       17l      110w     2179c https://deception-server/cUCT6KL
200      GET       20l      131w     2664c https://deception-server/admincp
200      GET       16l      101w     1982c https://deception-server/R3PrR7
200      GET       18l      115w     2230c https://deception-server/gjzaz
200      GET       19l      122w     2364c https://deception-server/cV14j
```

METRICHE

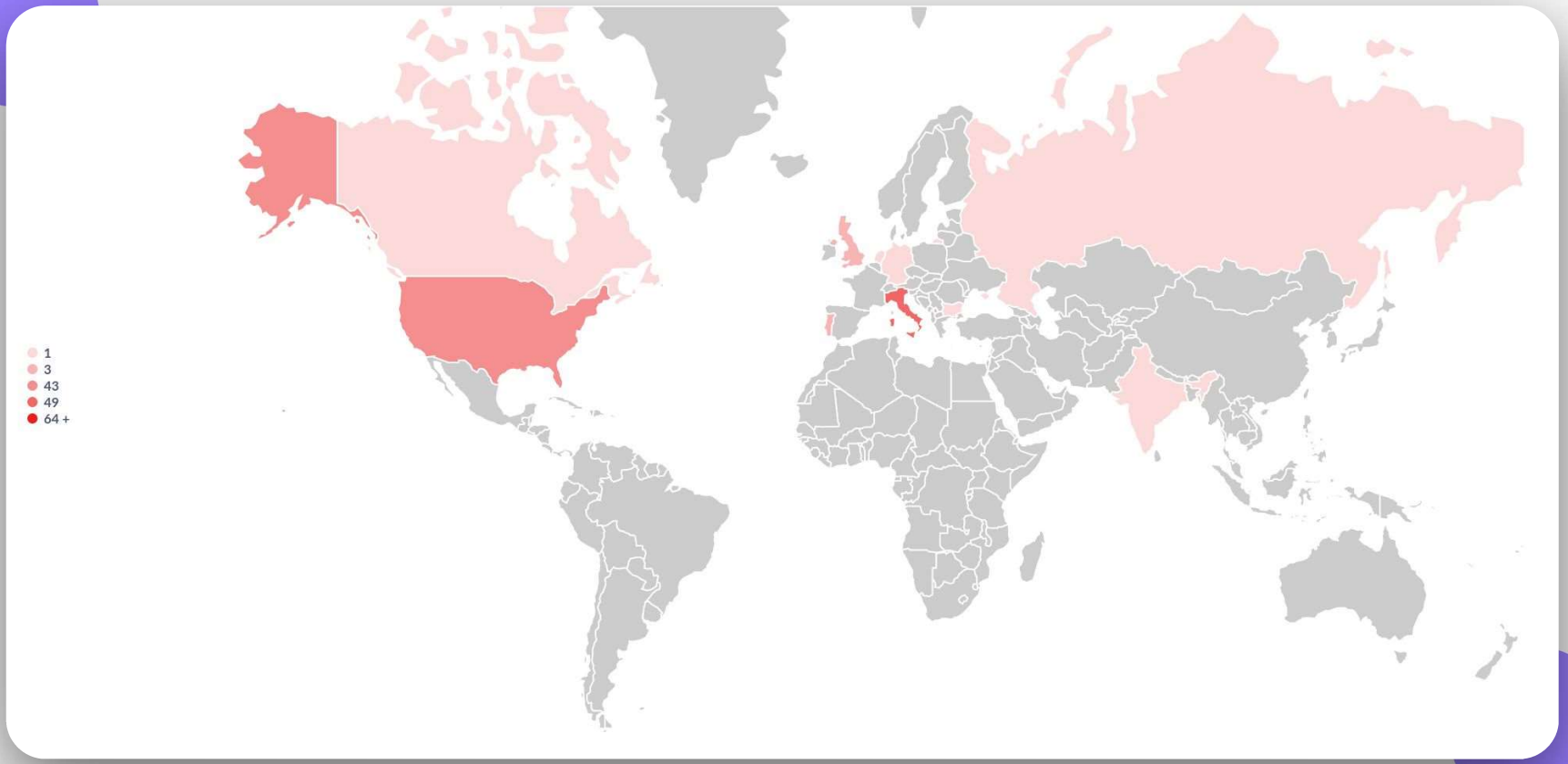
RICHIESTE WEB



#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.19%)	1 (0.21%)	—	—	—	—
MAX.	99 (18.47%)	63 (13.21%)	48.01 KiB (5.26%)	—	—	—
AVG.	2 (0.37%)	2 (0.42%)	4.68 KiB (0.51%)	—	—	—
1	99 (0.47%)	63 (14.52%)	48.01 KiB (0.13%)	GET	HTTP/1.1	/favicon.ico
2	36 (0.17%)	31 (7.14%)	43.74 KiB (0.12%)	GET	HTTP/1.1	/robots.txt
3	14 (0.07%)	8 (1.84%)	25.14 KiB (0.07%)	GET	HTTP/1.1	/cgi-bin/wa.exe
4	10 (0.05%)	2 (0.46%)	21.1 KiB (0.06%)	GET	HTTP/1.1	/js/hpsum/hpsum-version.js
5	4 (0.02%)	3 (0.69%)	3.22 KiB (0.01%)	GET	HTTP/1.1	/.well-known/security.txt
6	4 (0.02%)	2 (0.46%)	8.21 KiB (0.02%)	GET	HTTP/1.1	/SE/EMC_SE.swf
7	2 (0.01%)	1 (0.23%)	2.04 KiB (0.01%)	GET	HTTP/1.1	/image.jpg
8	2 (0.01%)	2 (0.46%)	4.9 KiB (0.01%)	GET	HTTP/1.1	/CSS/Miniweb.css
9	2 (0.01%)	2 (0.46%)	976 B (0.00%)	GET	HTTP/1.1	/favicon-32x32.png
10	2 (0.01%)	2 (0.46%)	876 B (0.00%)	GET	HTTP/1.1	/cf_scripts/scripts/ajax/ckeditor/ckeditor.js
11	2 (0.01%)	2 (0.46%)	906 B (0.00%)	GET	HTTP/1.1	/static/historypage.js
12	2 (0.01%)	2 (0.46%)	4.4 KiB (0.01%)	GET	HTTP/1.1	/favicon2.iso
13	2 (0.01%)	2 (0.46%)	4.58 KiB (0.01%)	GET	HTTP/1.1	/favicon.iso
14	2 (0.01%)	2 (0.46%)	4.37 KiB (0.01%)	GET	HTTP/1.1	/start.js
15	2 (0.01%)	2 (0.46%)	5 KiB (0.01%)	GET	HTTP/1.1	/en/main.js

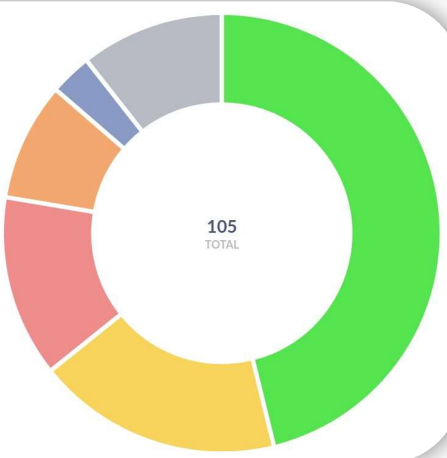
#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	6 (0.03%)	3 (0.69%)	4.36 KiB (0.01%)	—
MAX.	10,187 (48.23%)	82 (18.89%)	17.4 MiB (49.27%)	—
AVG.	2,640 (12.50%)	54 (12.44%)	4.42 MiB (12.50%)	—
1	10,187 (48.23%)	82 (18.89%)	17.4 MiB (49.27%)	09/Dec/2023
2	207 (0.98%)	63 (14.52%)	196.04 KiB (0.54%)	08/Dec/2023
3	104 (0.49%)	47 (10.83%)	53.92 KiB (0.15%)	07/Dec/2023
4	10,087 (47.75%)	63 (14.52%)	17.34 MiB (49.09%)	06/Dec/2023
5	132 (0.62%)	57 (13.13%)	75.09 KiB (0.21%)	05/Dec/2023
6	273 (1.29%)	63 (14.52%)	196.89 KiB (0.54%)	04/Dec/2023
7	127 (0.60%)	56 (12.90%)	67.8 KiB (0.19%)	03/Dec/2023
8	6 (0.03%)	3 (0.69%)	4.36 KiB (0.01%)	02/Dec/2023
TOT.	21,123	434	35.33 MiB	8

RICHIESTE WEB



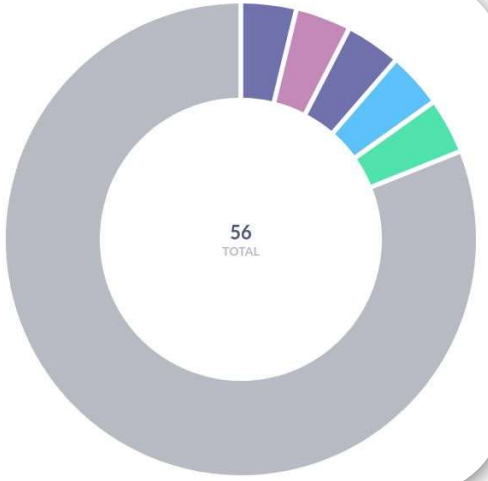
Top ISP

- Vodafone Italia S.p.A.
- CENSYS-ARIN-01
- DIGITALOCEAN-ASN
- CENSYS-ARIN-02
- Sistemas Informaticos, S.A.
- Other



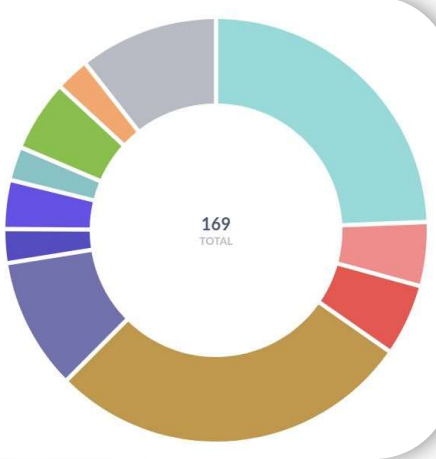
Top IPs

- 162.142.125.221
- 167.248.133.33
- 167.248.133.51
- 167.94.138.124
- 167.94.146.59
- Other



Top Attacks

- LePresidente/http-generic-401-bf
- crowdsecurity/CVE-2022-41082
- crowdsecurity/apache_log4j2_cve-2021-44228
- crowdsecurity/http-bad-user-agent
- crowdsecurity/http-crawl-non_statics
- crowdsecurity/http-cve-2021-41773
- crowdsecurity/http-dos-invalid-http-versions
- crowdsecurity/http-open-proxy
- crowdsecurity/http-path-traversal-probing
- crowdsecurity/http-sensitive-files
- Other



CONCLUSIONI

Il nostro sistema si è rivelato un ottimo modo per porre un primo layer di sicurezza a un ipotetico servizio di API esposto pubblicamente su Internet.

Nonostante la deception non sia una soluzione completa per la difesa delle API resta comunque uno strumento valido e da usare come deterrente per attaccanti inesperti (script kiddies)

L'approccio containerizzato risulta vincente perché in maniera scalabile e parametrizzabile possiamo fornire un servizio di deception configurabile a runtime.

https://github.com/FlippaFloppa/Kubernetes-API-Deception

GRAZIE PER L'ATTENZIONE

Bambini Leonardo
Di Fazio Patrick
Venerandi Lorenzo