Security Awareness Infrastructure

Infrastruttura per la sicurezza aziendale

INDICE

INTRODUZIONE

Il contesto

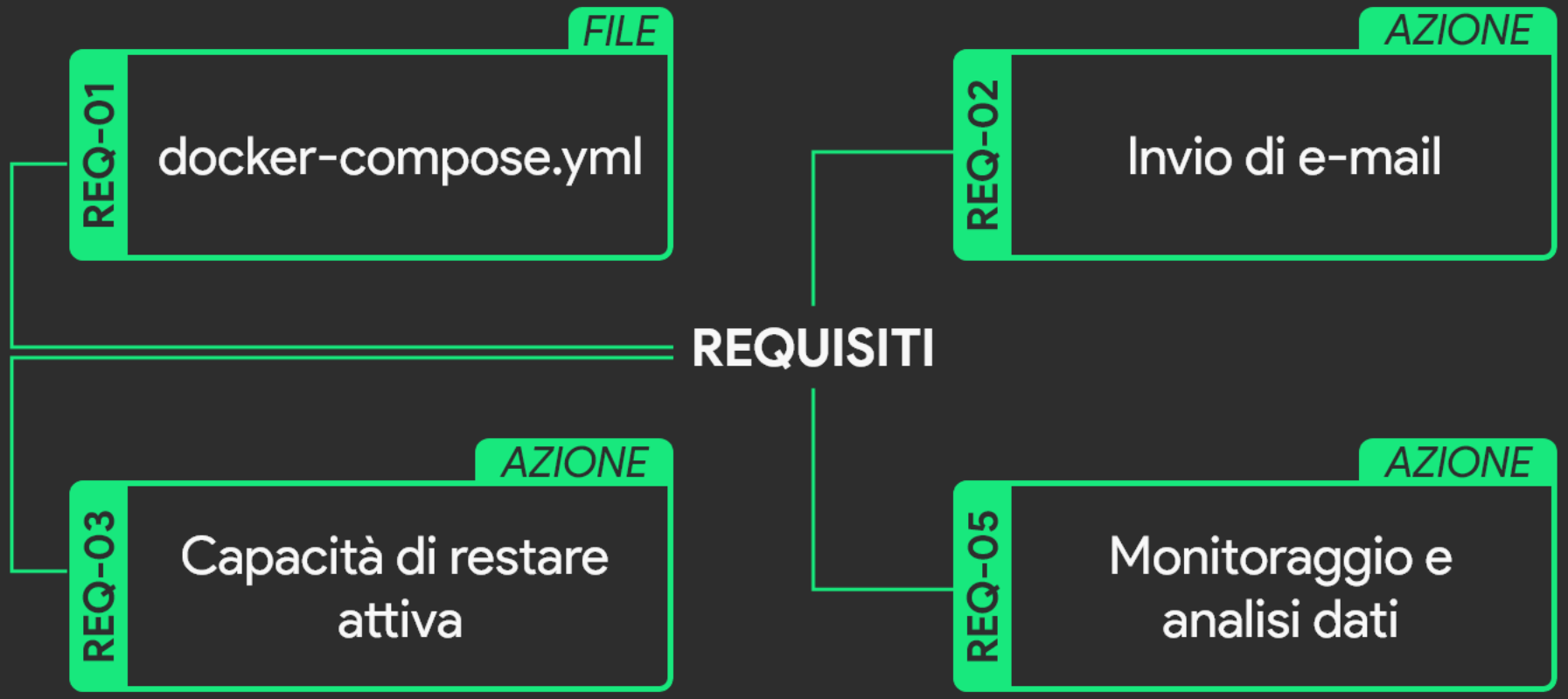
- Alfabetizzazione informatica **alta**
- Consapevolezza dei rischi online **bassa**
- Attacchi informatici, come il **phishing**, minacciano le aziende
- Progetto mirato a testare la **consapevolezza** del personale e implementare soluzioni

INTRODUZIONE

ANALISI

- Creazione di un infrastruttura di phishing
- Utilizzo di tecnologie di containerizzazione
- Utilizzo di Gophish, Apache/nginx e Postfix

ANALISI


REQUISITI
REQ-01
FILE
docker-compose.yml
REQ-02
AZIONE
Invio di e-mail
REQ-03
AZIONE
Capacità di restare attiva
REQ-05
AZIONE
Monitoraggio e analisi dati

PROGETTAZIONE

MAIL SERVER

POSTFIX – Docker per contenere il mail server che funge da sender delle email delle campagne di phishng.

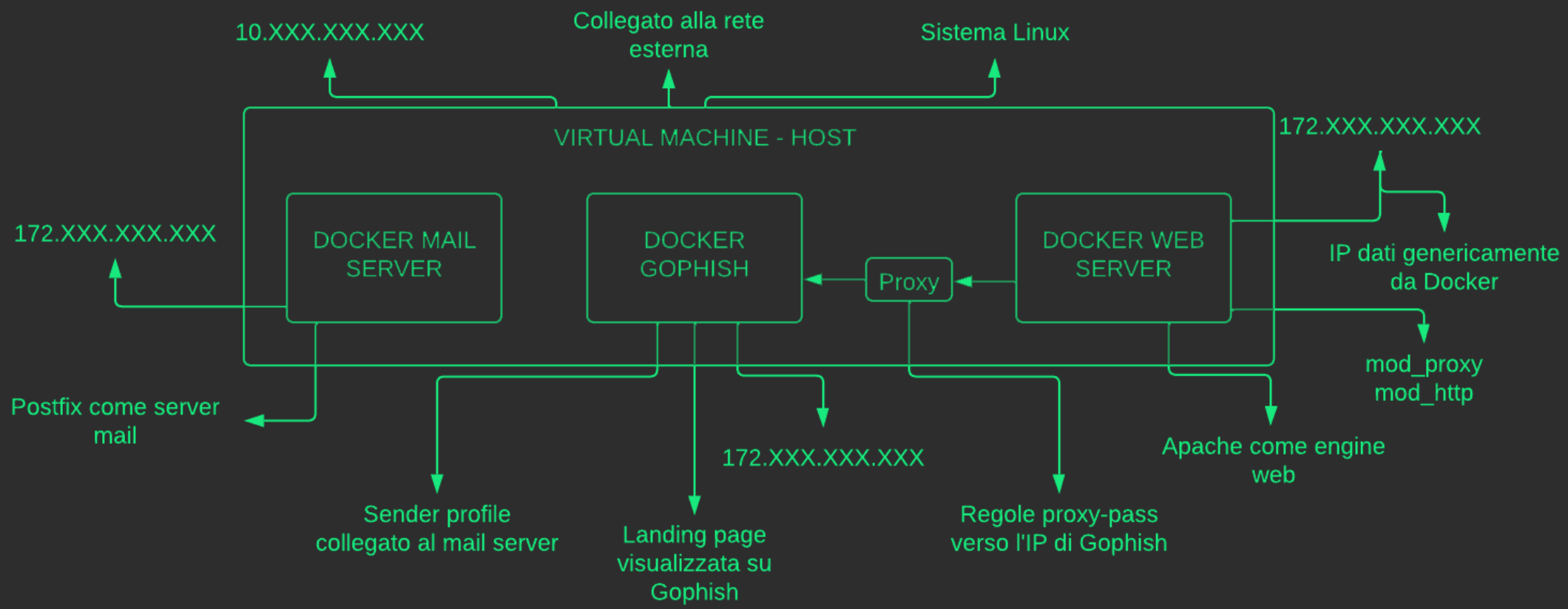
GOPHISH

GOPHISH – Abilitato in un container Docker, è considerato il cuore del progetto.

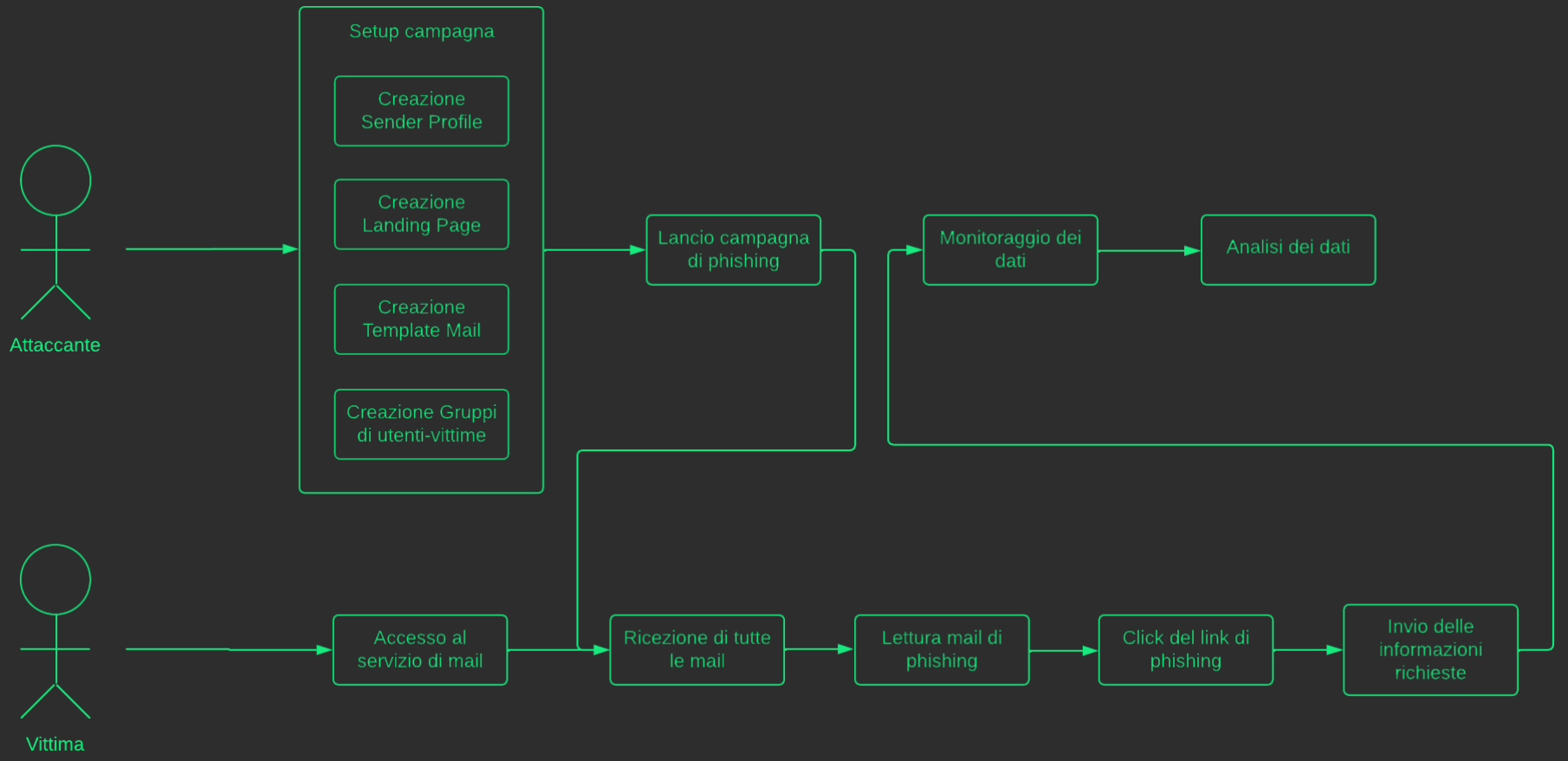
WEB SERVER

APACHE – Web server avviato con Docker che espone il dominio/sito esca.

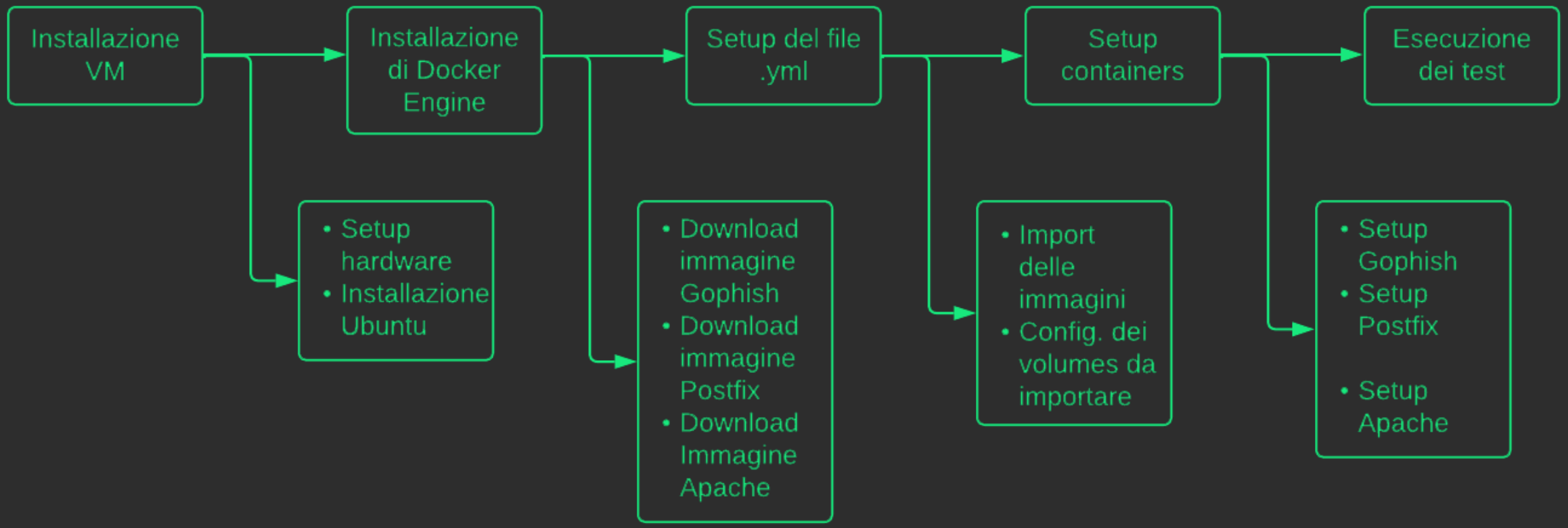
PROGETTAZIONE



PROGETTAZIONE



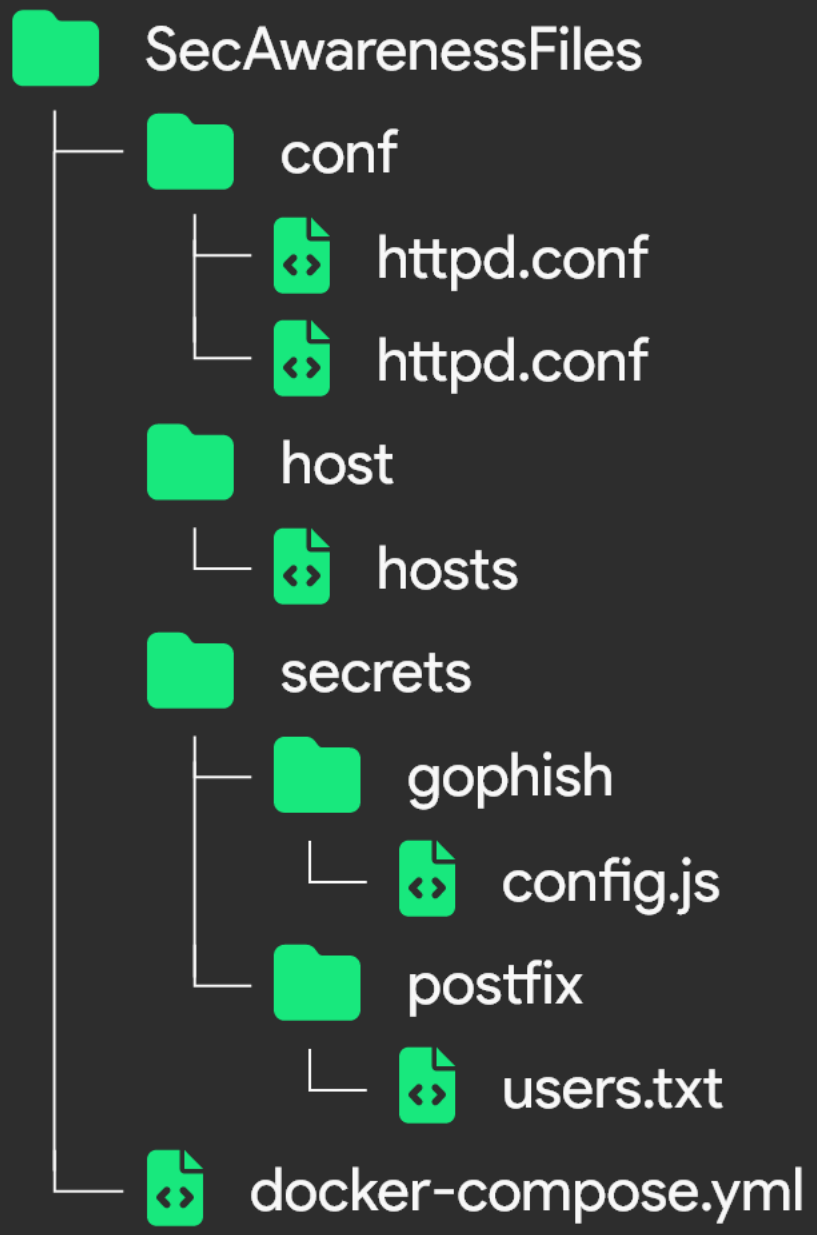
IMPLEMENTAZIONE



IMPLEMENTAZIONE

Altri file

Sono presenti altri file all'interno delle cartelle gophish e postfix



IMPLEMENTAZIONE

Sample: docker-compose.yml

```yaml
services:
  gophish:
    image: cisagov/gophish:0.0.8
    container_name: gophishenv
    init: true
    restart: always
```

```yaml
ports:
  - target: 3333
    published: 3333
    protocol: tcp
    mode: host
```

```yaml
secrets:
  - source: gophish_config_json
    target: config.json
```

```yaml
environment:
  - PRIMARY_DOMAIN=mircosoft.com
  - RELAY_IP=172.18.0.0/24
```

```yaml
volumes:
  - ./conf/httpd.conf:/usr/local/apache2/conf/
```

TEST

Test in parallelo

Test condotti durante l'implementazione dell'infrastruttura per evitare problemi in successione.

Test finali

Test finali condotti dopo avere completato l'implementazione. Necessari per verificare eventuali mancanze o errori da sistemare

TEST

TC-01	Verifica l'accesso remoto alla virtual machine	FALLITO
TC-04	Invio delle e-mail da Postfix verso l'inbox correttamente	PASSATO
TC-05	Creazione in modo corretto di una campagna di phishing	PASSATO
TC-06	Invio di e-mail di phishing da parte della campagna di Gophish	PARZIALE

CONCLUSIONI

- Mancanze
- Sviluppi futuri
- Demo

GRAZIE PER L’ATTENZIONE