

Security Awareness Infrastructure

Infrastruttura per la sicurezza aziendale

INDICE

- Introduzione
- Analisi
- Progettazione
- Implementazione
- Test
- Conclusioni

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

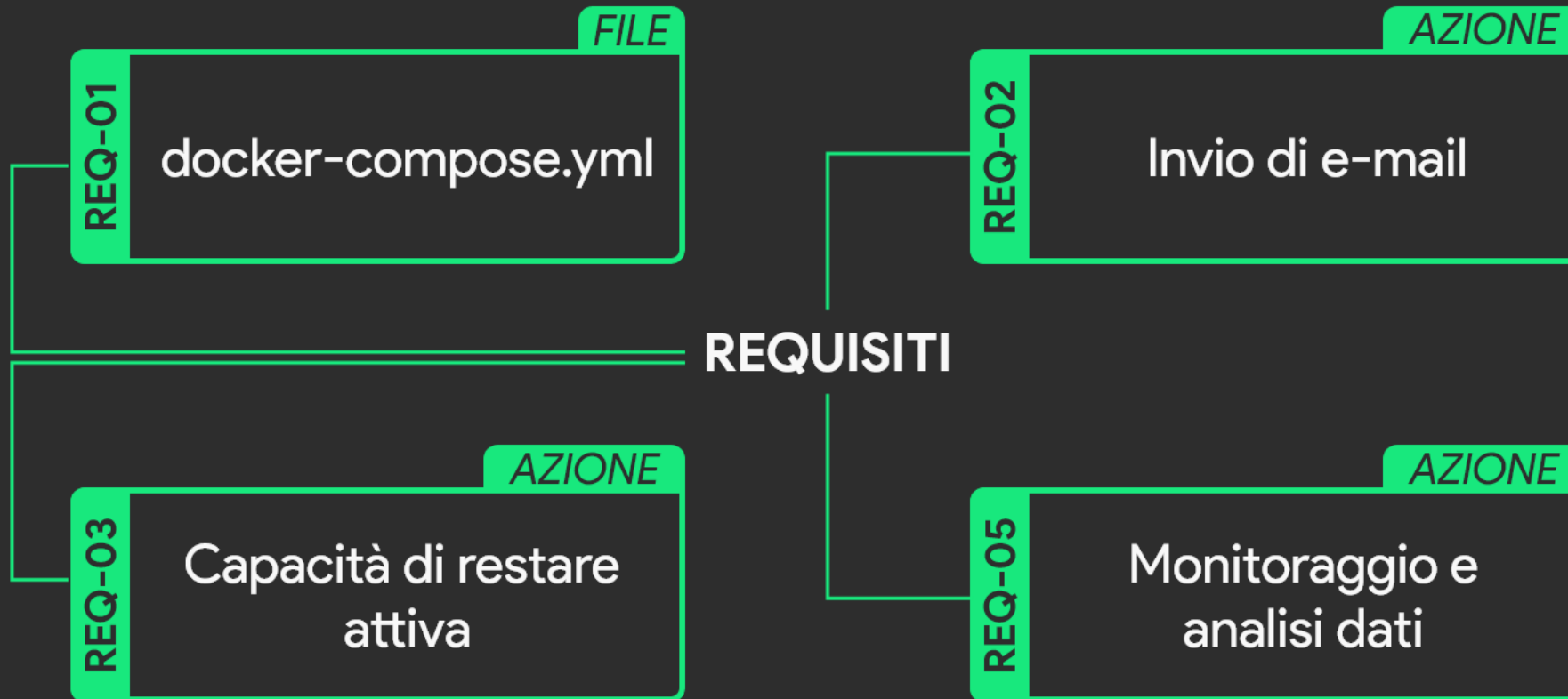
INTRODUZIONE

| | LUN | MAR | MER | GIO | VEN | SAB | DOM |
|-----|-----|-----|-----|-----|-----|-----|-----|
| MAR | | | | | 29 | 30 | 31 |
| APR | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| APR | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| APR | 15 | 16 | 17 | | | | |

ANALISI

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

ANALISI



PROGETTAZIONE



MAIL SERVER

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



GOPHISH

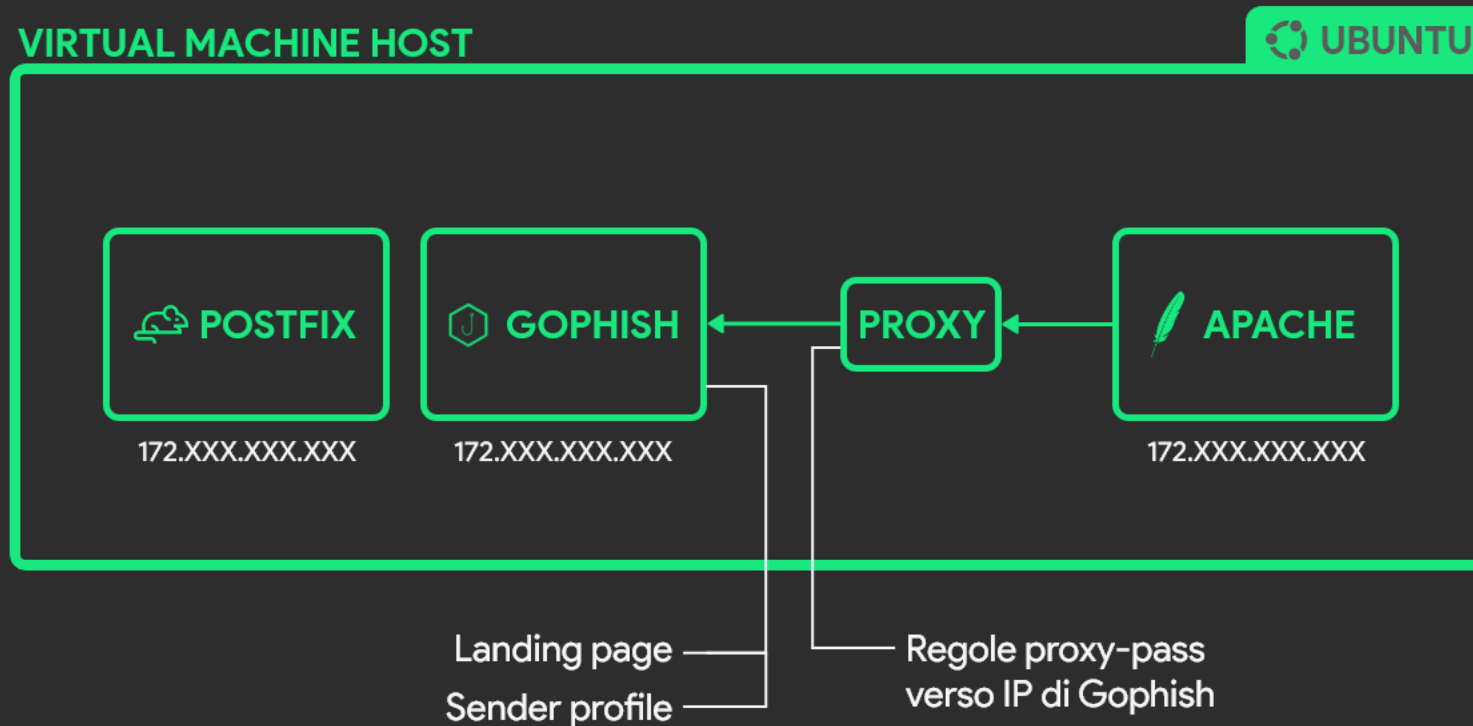
GOPHISH – Abilitato in un container Docker, è considerato il cuore del progetto.



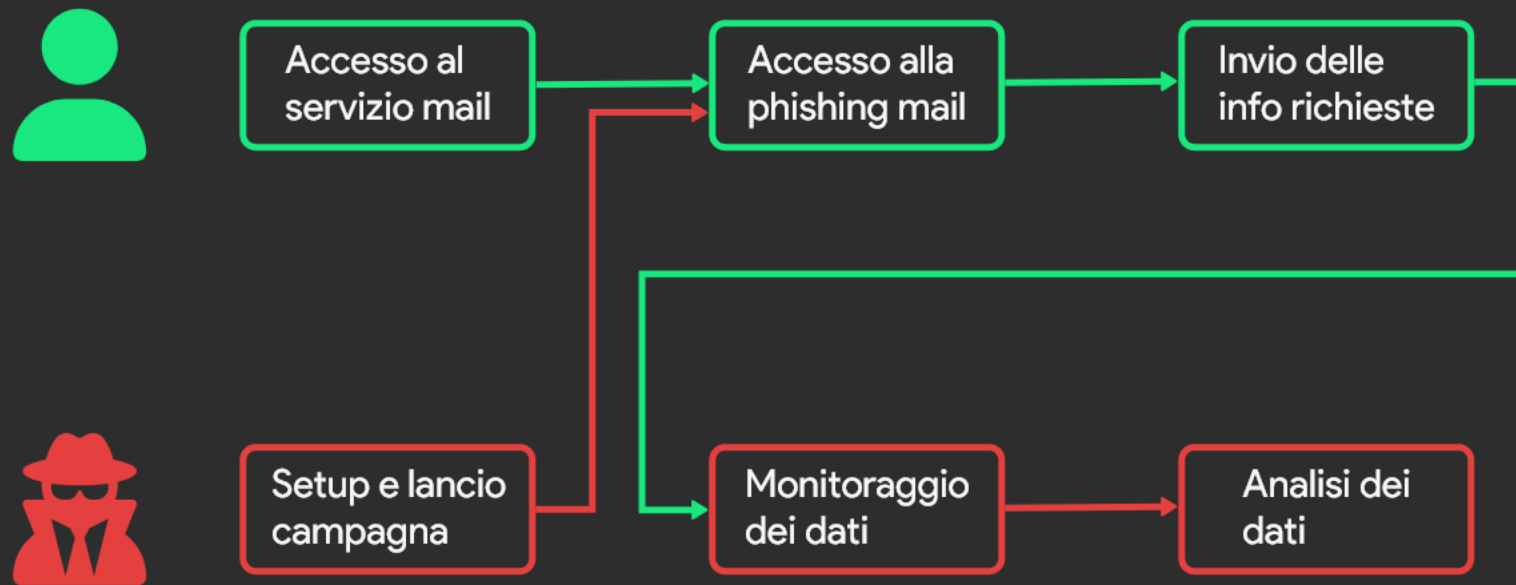
WEB SERVER

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

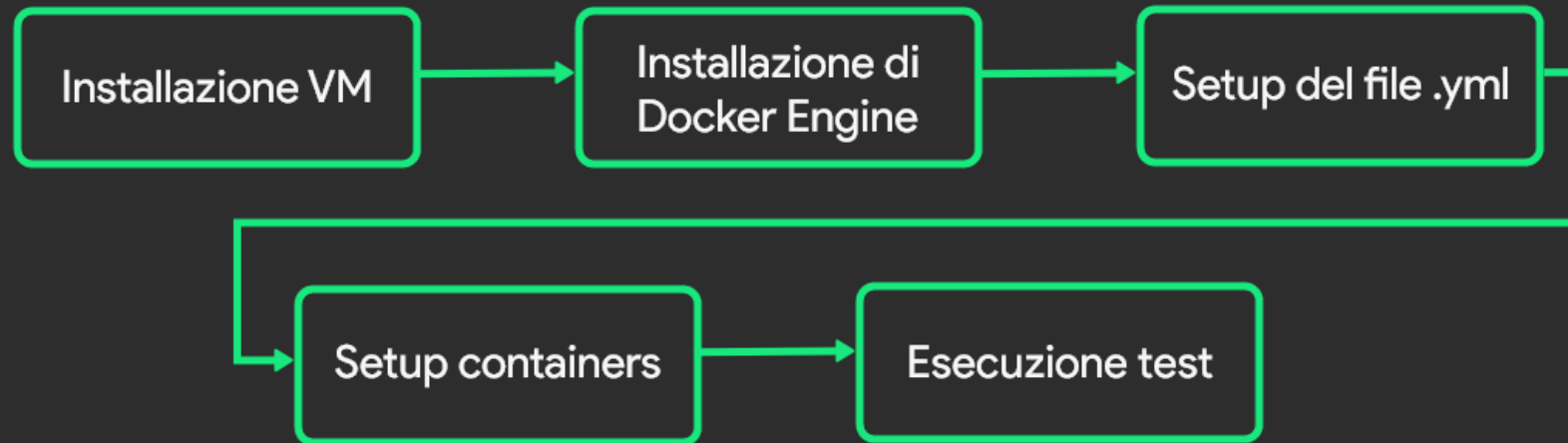
PROGETTAZIONE



PROGETTAZIONE



IMPLEMENTAZIONE

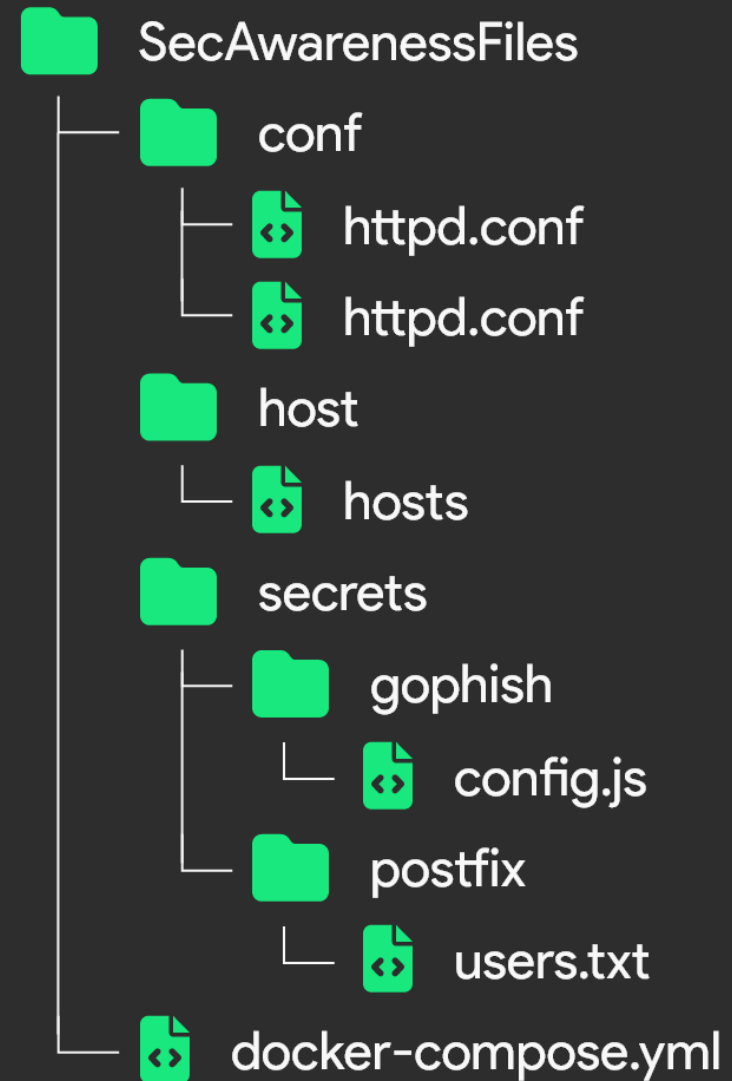


IMPLEMENTAZIONE

Altri file

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

- Chiavi pubbliche/private



IMPLEMENTAZIONE

Sample: docker-compose.yml

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

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

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

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

```
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**