

A. A. 2023/24

# SAMBA DECEPTION COMPONENT GENERATOR

PROGETTO CYBERSECURITY M

---

CASSANELLI ANTONIO  
FOCARDI LEONARDO  
GALEONE CHRISTIAN

# PROGETTO

Creazione di uno script Python che consenta di personalizzare l'implementazione del container SAMBA.  
Lo script permette di

Abilitare condivisioni pubbliche e private

Creare un file system gerarchico popolato

Autenticarsi tramite protocollo LDAP

Creare utenti e gruppi locali

Build e Run file creati

Cancellazione file creati

# DECEPTION COMPONENT

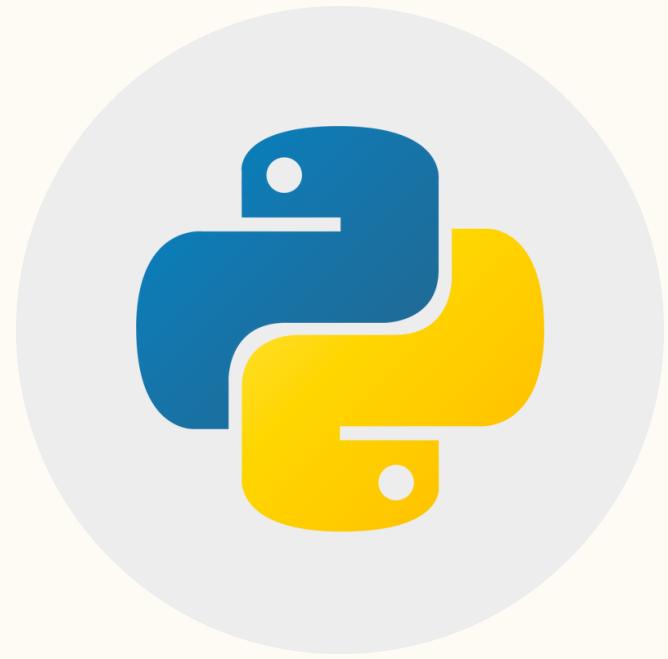
A cosa serve

Rileva minacce in modo precoce

Analizza il comportamento degli attaccanti

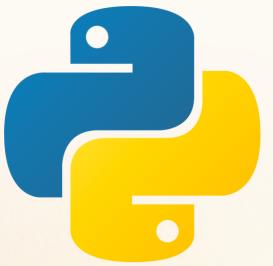
Protegge le risorse critiche

# TECNOLOGIE



---

# PYTHON



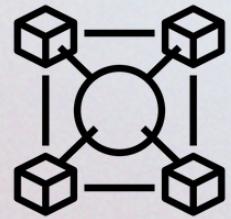
Linguaggio di programmazione ad alto livello orientato a oggetti

---



## Linguaggio interpretato

Il programma viene eseguito direttamente dal codice sorgente



## Interoperabilità con altri linguaggi

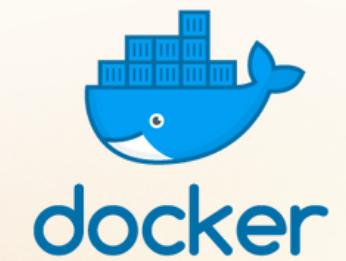
Facilità di scrittura di comandi bash



## Versatilità

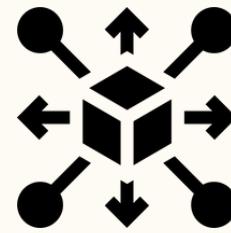
Utilizzato in moltissimi settori IT

# DOCKER



Sistema per l'automazione del deployment di un'applicazione

---



## Distribuzione rapida di software

Consente di testare e distribuire applicazioni facilmente



## Funzionamento standardizzato

L'uso dei container facilita l'esecuzione in qualsiasi ambiente

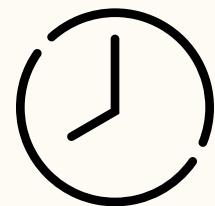


## Spazio e spese ridotti

I container semplificano l'esecuzione di codice sui server, contribuendo a risparmiare soldi

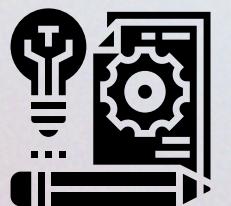
# UBUNTU

Sistema operativo gratuito e open source basato su GNU/Linux.



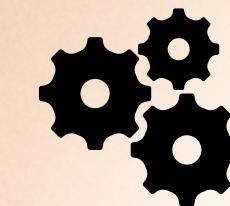
## Supporto a lungo termine

Aggiornamenti periodici



## Modificabile ed adattabile

Personalizzazione del sistema operativo in base alle proprie esigenze



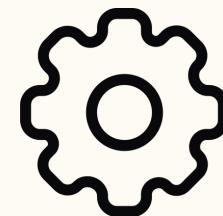
## Configurazione

Il sistema riconosce i componenti integrati durante l'avvio

# SAMBA

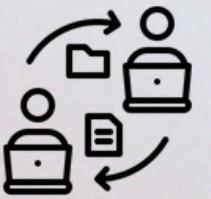
SAMBA

Implementazione open source per l'impegno condiviso di risorse



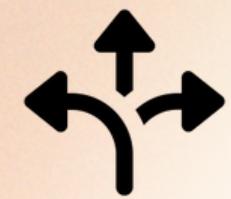
## Configurazione

Modifica della  
configurazione di samba  
tramite un unico file



## Condivisione file

Cartelle condivise via  
rete



## Flessibilità e libertà

Interoperabilità tra  
sistemi operativi

# smb.conf

Configurazione utenti e gruppi

Configurazione log

Configurazione permessi

Configurazione protocolli

## [global]

```
workgroup = WORKGROUP  
log file = /var/log/samba  
/log.%m
```

...

## [homes]

```
comment = Home Directories  
browseable = no
```

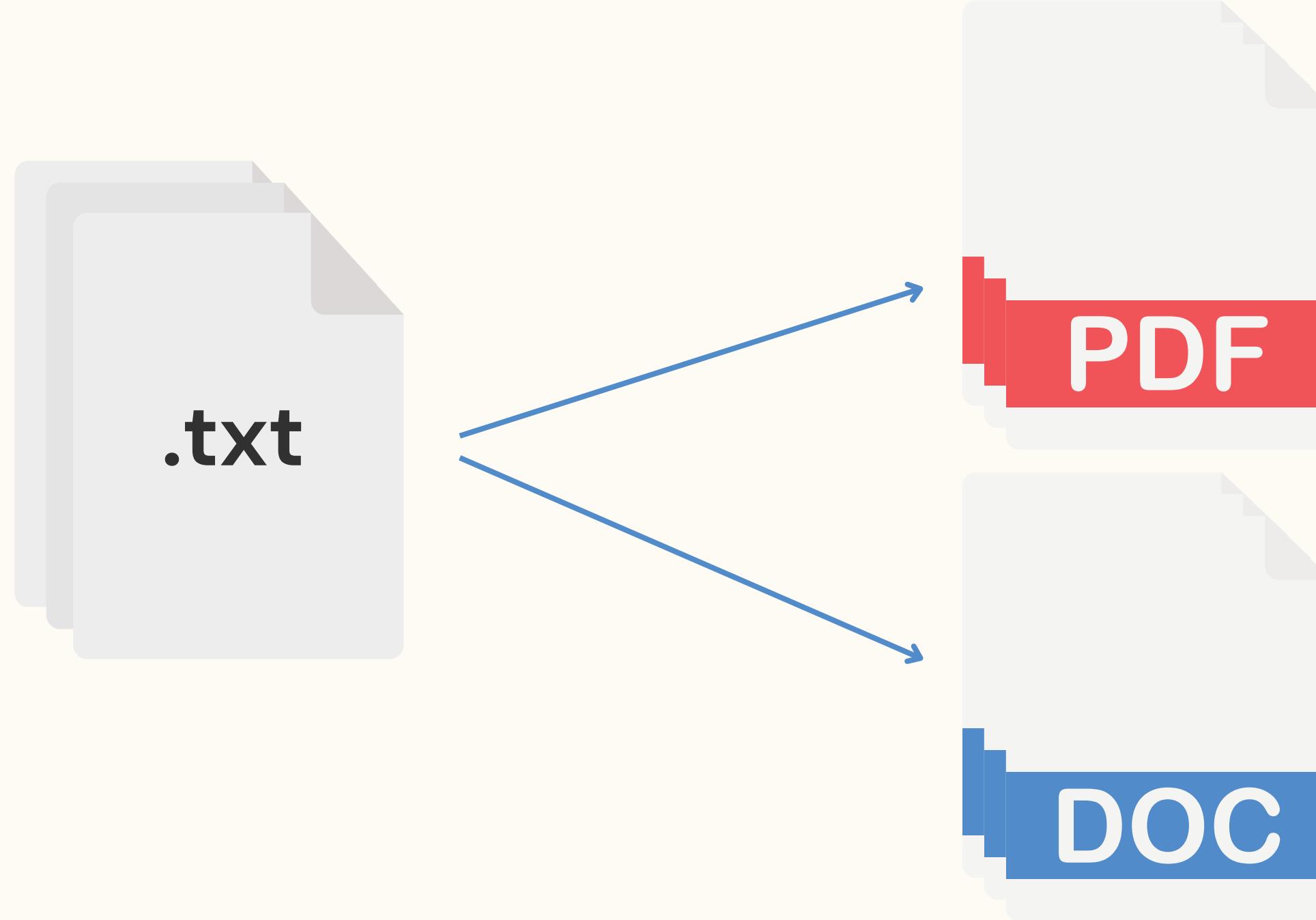
...

## [public]

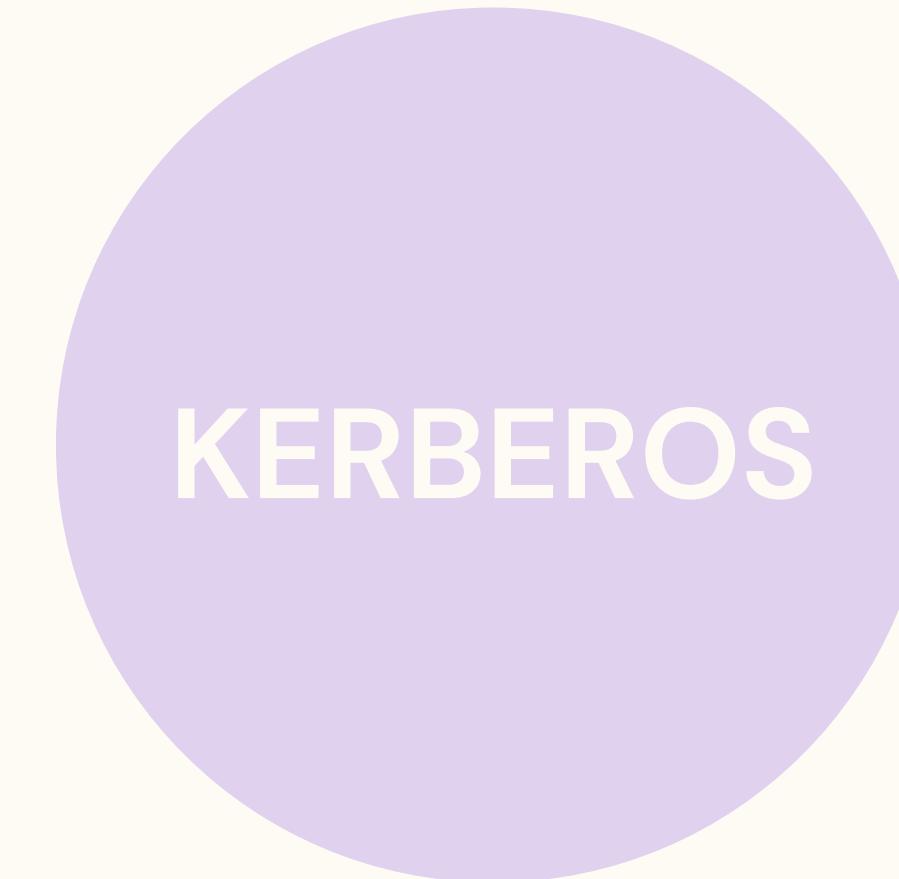
SAMBA

# PANDOC

Convertitore di documenti software

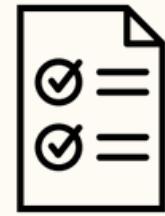


# PROTOCOLLI



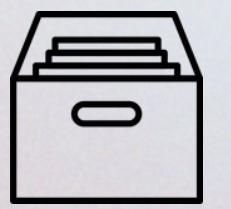
# LDAP

## Lightweight Directory Access Protocol



### Protocollo Standard

Utilizzato per accedere e mantenere servizi di directory



### Archiviazione dati in directory

Leggero ed efficiente



### Autenticazione utenti

Autenticazione centralizzata e protezione dei dati dell'utente

# KERBEROS

---



## Protocollo di autenticazione

Autenticazione centralizzata



## Ticket di autenticazione

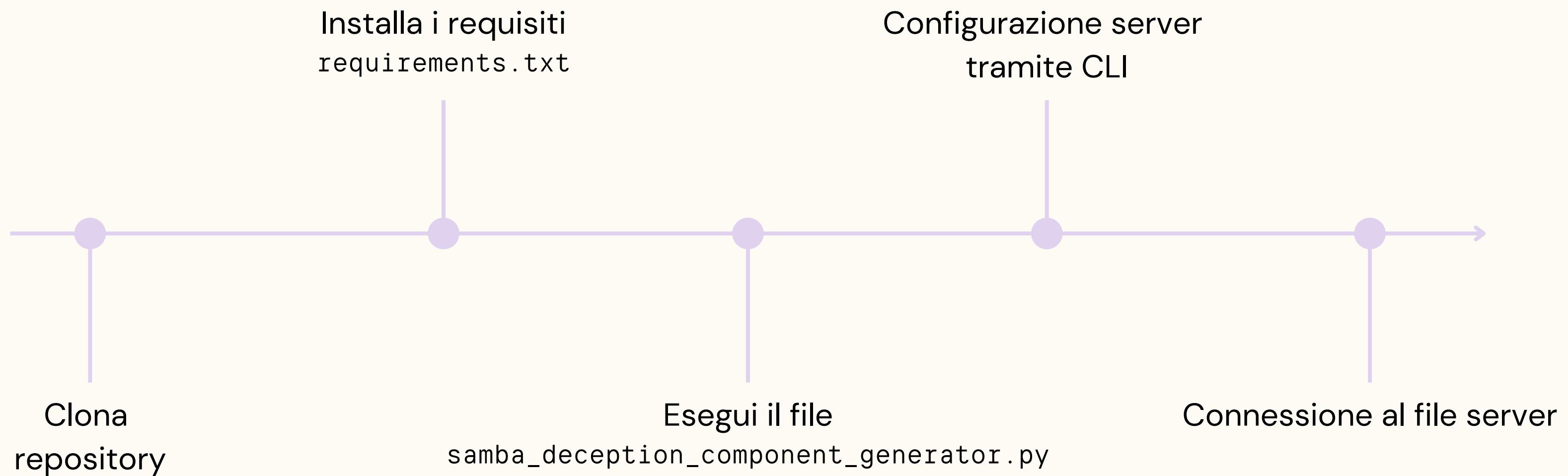
Utilizzato per accedere alle risorse, senza inserire nuovamente le credenziali



## Crittografia simmetrica

Chiavi condivise all'interno del sistema

# UTILIZZO



# **FILE GENERATI**

---

# setup.py

Creazione supporto per  
il server

Creazione utenti e  
gruppi

Creazione file

`create_user(username, password)`

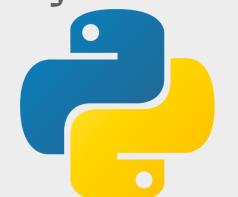
`create_group(group_name, list)`

`makeFS(type)`

`create_files(dim_min, dim_max, num_file)`

`setup_ldap(domain, adminpasswd)`

`kinit_user(username, password)`



# start.sh

Avvia i servizi del docker

```
service smbd restart &  
smbd --foreground --no-process-group
```

oppure

```
echo "search <nomedominio>  
nameserver 127.0.0.1  
" > /etc/resolv.conf  
service samba-ad-dc start  
/bin/bash
```

</>

# dockerfile

Ha il compito di creare  
l'immagine del server  
Samba, partendo  
dall'immagine di Ubuntu  
20.04

```
FROM ubuntu:20.04

RUN apt-get update && \
    apt-get install -y samba ...

COPY setup.py /
RUN python3 /setup.py && rm
/setup.py

...
COPY start.sh /start.sh
RUN chmod +x start.sh
EXPOSE 139 445
CMD /start.sh
```



# VULNERABILITÀ

---

# NTLM

Protocollo di autenticazione di Windows utilizzato da SMB quando non viene implementato LDAP.

1

Pass-The-Hash Attacks

Man-In-The-Middle Attacks

Esposizione delle credenziali

# SMB + LDAP

v4.0.0+

Erronea validazione dei  
permessi per la modifica  
delle password tramite  
LDAP.

# SAMBA-TOOL

v4.0+

Tool di amministrazione AD-DC (Domain Controller)

Invio di password in chiaro quando opera con un server LDAP remoto.

# KERBEROS

4

Pass-The-Ticket Attacks

Golden Ticket Attacks

Furto di credenziali

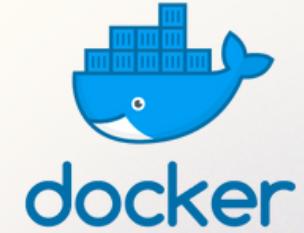
# **SVILUPPI FUTURI**

---



## Utilizzo LLAMA per i file

Generazione dei file in  
modo più casuale



## Supporto Docker con LDAP

Build e run del docker  
automatici dopo  
l'autenticazione con  
LDAP



## Monitoring log interattivo

Per l'analisi approfonidita  
dei log di Samba



## Maggior efficienza

Rendere l'immagine OCI  
più leggera ed efficiente

# **GRAZIE PER L'ATTENZIONE!**

---

Repo Github



CASSANELLI ANTONIO  
FOCARDI LEONARDO  
GALEONE CHRISTIAN