GABRIELE ROMANATO

Creare uno script Bash interattivo per generare certificati SSL con Let's Encrypt

L'uso di certificati SSL è fondamentale per garantire la sicurezza delle connessioni web. Let's Encrypt offre certificati SSL gratuiti, e il processo di ottenimento può essere automatizzato con Certbot. Questo articolo spiega come creare uno script Bash interattivo per generare certificati SSL utilizzando Let's Encrypt.

Il nostro obiettivo è creare uno script che:

1. Chieda all'utente di inserire il nome di dominio.
2. Generi un certificato SSL per il dominio inserito.
3. Offra opzioni per il rinnovo automatico e la configurazione del server web (ad esempio, Apache o Nginx).

```
#!/bin/bash

# Funzione per verificare se il comando precedente è riuscito
check_success() {
    if [ $? -ne 0 ]; then
        echo "Si è verificato un errore. Controlla i log per
maggiori dettagli."
        exit 1
    fi
}

echo "Benvenuto nello script per la generazione di
certificati SSL con Let's Encrypt!"

# Chiedi il nome di dominio
read -p "Inserisci il nome di dominio (esempio: esempio.com):
" DOMAIN

# Chiedi se l'utente vuole configurare Apache o Nginx
```

```

echo "Vuoi configurare un server web?"
select webserver in "Apache" "Nginx" "Nessuno"; do
    case $webserver in
        Apache ) WEBSERVER="apache"; break;;
        Nginx ) WEBSERVER="nginx"; break;;
        Nessuno ) WEBSERVER="nessuno"; break;;
    esac
done

# Verifica se Certbot è installato
echo "Verifica dell'installazione di Certbot..."
which certbot > /dev/null
check_success

# Generazione del certificato SSL
echo "Generazione del certificato SSL per il dominio
$DOMAIN..."
if [ "$WEBSERVER" = "apache" ]; then
    sudo certbot --apache -d $DOMAIN
    check_success
elif [ "$WEBSERVER" = "nginx" ]; then
    sudo certbot --nginx -d $DOMAIN
    check_success
else
    sudo certbot certonly --standalone -d $DOMAIN
    check_success
fi

# Chiedi se l'utente vuole configurare il rinnovo automatico
echo "Vuoi configurare il rinnovo automatico dei
certificati?"
select yn in "Sì" "No"; do
    case $yn in
        Sì )
            echo "Configurazione del rinnovo automatico..."
            (crontab -l 2>/dev/null; echo "0 3 * * *
/usr/bin/certbot renew --quiet") | crontab -
            check_success
            echo "Rinnovo automatico configurato con
successo."
            break;;
        No )
            echo "Rinnovo automatico non configurato."

```

```
                break;;
    esac
done

echo "Il certificato SSL per $DOMAIN è stato generato con
successo!"
```

Spiegazione dello script:

1. **Funzione `check_success()`:** Verifica che il comando precedente sia stato eseguito correttamente. Se c'è un errore, lo script si interrompe.
2. **Interattività:** Utilizza `read` per richiedere l'input dell'utente e `select` per presentare opzioni multiple (come la scelta del server web o la configurazione del rinnovo).
3. **Verifica dell'installazione di Certbot:** Usa `which` per controllare che Certbot sia installato. In caso contrario, lo script segnala un errore e si interrompe.
4. **Generazione del certificato SSL:** Esegue Certbot con l'opzione appropriata in base al server web scelto. Se non viene scelto un server web, utilizza l'opzione `standalone` per generare il certificato.
5. **Configurazione del rinnovo automatico:** Aggiunge una voce al crontab per eseguire il rinnovo dei certificati ogni giorno alle 3:00 AM. L'opzione `--quiet` evita la produzione di output a meno che non si verifichino errori.

Conclusione

Lo script qui presentato è un punto di partenza per automatizzare la creazione di certificati SSL con Let's Encrypt. Può essere ulteriormente migliorato per gestire altre funzionalità, come la configurazione avanzata di Apache/Nginx, il supporto per domini multipli o sottodomini, e l'invio di notifiche email in caso di errore.

L'uso di strumenti come Certbot semplifica il processo di gestione dei certificati SSL, garantendo connessioni sicure e riducendo il rischio di errori nella configurazione manuale.