Hardening

Per eseguire un hardening efficace di vtenext su stack **LAMP (Linux, Apache, MySQL, PHP)** Ubuntu 24.04 si consiglia di seguire i seguenti passi suddivisi per i vari componenti dello stack.

Linux

Si consiglia di installare fail2ban in modo da bloccare tentativi di scansioni da parte di tool automatici / scanner di vulnerabilità.
Per farlo:

```
sudo apt install fail2ban
```

Verificate che il servizio sia attivo:

```
systemctl status fail2ban
```

Creare un file personalizzato che registri la definizione di un nuovo filtro in modo da bloccare l'ip sorgente della scansione.
Il filtro rileva gli status HTTP 404 e li riporta al motore di fail2ban per la valutazione

```
sudo nano /etc/fail2ban/filter.d/apache-404.conf
```

contenuto:

```
[Definition]


failregex = ^<HOST> .* "(GET|POST|HEAD|PUT).*" 404
ignoreregex =.*(robots.txt|favicon.ico|jpg|png|gif)
```

Attivare il filtro creato creando in file

```
sudo nano /etc/fail2ban/jail.local
```

con il seguente contenuto:

```
[DEFAULT]


ignoreip = 127.0.0.1/8 ::1
```

```
[apache-404]

enabled = true
port = http,https
filter = apache-404
action = iptables-allports[protocol=all, blocktype=DROP]

logpath = /var/log/apache2/access.log

bantime  = 3600
findtime = 120
maxretry = 100
```

Nella configurazione sopra, viene letto il file "access.log" e se il filtro "apache-404" rileva un numero di tentativi uguale o superiore a "maxretry" nell'arco di "findtime" secondi, l'ip sorgente da cui arrivano le richieste web sarà bannato per "bantime" secondi.
Per bannato si intente l'applicazione della "action" ovvero il drop delle connessioni.

Riavviare il servizio fail2ban

```
systemctl reload fail2ban
```

Richiamando il comando

```
sudo fail2ban-client status
```

saranno mostrate le configurazioni attive per cui fail2ban opera.

E' inoltre disponibile il comando fail2ban-client che permette di visualizzare lo stato dei blocchi IP attivi per un determinato "filtro".
Considerando il filtro "apache-404" per visualizzare lo stato:

```
sudo fail2ban-client status apache-404
```

Rimuovere un ban:

```
fail2ban-client set apache-404 unbanip 1.2.3.4
```

Bannare manualmente:

```
fail2ban-client set apache-404 banip 1.2.3.4
```

Apache

E' utile nascondere le informazioni relative alla versione di apache in modo da evitare attacchi mirati.

Modificare:

```
sudo nano /etc/apache2/conf-enabled/security.conf
```

Impostare:

```
ServerTokens Prod
ServerSignature Off
TraceEnable Off
```

Riavviare:

```
sudo systemctl restart apache2
```

MySQL

Mysql fornisce un comando dedicato a questo scopo che è possibile richiamare.
Questo comando avvia un wizard da terminale dove verifica lo stato attuale e propone delle modifiche che si possono accettare o meno.

```
mysql_secure_installation
```

Esempio di output

```
root@ubuntu24:~# mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: y
```

```
There are three levels of password validation policy:

LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 1

Skipping password set for root as authentication with auth_socket is used by default.
If you would like to use password authentication instead, this can be done with the
"ALTER_USER" command.
See https://dev.mysql.com/doc/refman/8.0/en/alter-user.html#alter-user-password-management for
more information.

By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.


Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.


Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y
 - Dropping test database...
```

```
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done!
```

NB. Si consiglia sempre di creare un utente MySQL dedicato per il singolo database di vtenext.
Nel caso il server condividesse più installazioni di vtenext (come ad esempio l'ambiente di produzione e quello di test) è sempre consigliato creare utenze diverse in modo da evitare propagazioni indesiderate su altri database/ambienti di lavoro.

Revision #15
Created 2026-06-09 09:41:49 UTC by ddalmaso
Updated 2026-06-10 14:06:27 UTC by ddalmaso