

Hardening y configuración avanzada de Nginx

Volodimir Yarmash Yarmash

Contexto.....	1
Personalización.....	1
1. Instalación y Cambio de Puerto.....	2
2. Server Blocks (Sitios Web Virtuales).....	3
3. Hardening de Configuración.....	4
4. Control de Acceso y Restricciones.....	5
5. Reglas de Seguridad Avanzada.....	7
Final del ejercicio.....	8

Contexto

Trabajáis como Administradores de Sistemas en una empresa de ciberseguridad. Se os ha asignado un servidor Debian 13 en Proxmox que debe ser securizado antes de salir a producción.

Personalización

Para que el ejercicio sea válido, deberás sustituir los siguientes valores en toda la configuración:

- [DNI3]: Las últimas 3 cifras de tu DNI (ej: si es 12345678, usarás 678).
- [DNI1]: La última cifra de tu DNI (ej: si es 12345678, usarás 8).
- [USER]: Tu nombre de usuario en Pasen (ej: jgonrod365).
- [PC]: Tu número de PC en clase con dos dígitos.
- [IP_PROFE]: La dirección IP 10.4.1.101
- [TU_IP]: La dirección IP que te corresponda.

Trabajarás en una máquina virtual propia:

- Se clonará (clonación completa) a partir de la plantilla con ID 410, y su nombre

será Nginx-[USER]

- El hostname de tu Debian será nginx-[USER]. Para ello, puedes usar el comando `hostnamectl`. Asegúrate que se ha cambiado en los ficheros `/etc/hostname` y `/etc/hosts`.
- Tu dirección IP debe ser estática y será 10.4.1.108 con máscara de red 255.255.0.0, con puerta de enlace 10.4.254.255

```
GNU nano 8.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

auto ens18
iface ens18 inet static
    address 10.4.1.108
    netmask 255.255.0.0
    gateway 10.4.254.255
    dns-nameservers 8.8.8.8

# This is a autoconfigured IPv6 interface
iface ens18 inet6 auto

root@nginx-vyaryar541:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:f2:30:de brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    altname enxbc2411f230de
    inet 10.4.1.108/16 brd 10.4.255.255 scope global ens18
        valid_lft forever preferred_lft forever
```

1. Instalación y Cambio de Puerto

Instala el servidor Nginx, pero no lo dejes con la configuración de fábrica.

1. Puerto de escucha: Por seguridad (u ocultación), el servidor no debe usar el puerto 80. Configúralo para que escuche en el puerto 2[DNI3].

o Ejemplo: Si tu [DNI3] es 678, tu puerto será el 2678.

2. Página de inicio: Modifica el archivo `/var/www/html/index.html` para que muestre: "Servidor SEGURO de [USER] funcionando en el puerto 2[DNI3]".

```
GNU nano 8.4 /etc/nginx/sites-available/default *
#
# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.
##
# Default server configuration
#
server {
    listen 2541 default_server;
    listen [::]:2541 default_server;

    # SSL configuration
    #
    # listen 443 ssl default_server;
    # listen [::]:443 ssl default_server;
    #
    # Note: You should disable gzip for SSL traffic.
    # See: https://bugs.debian.org/773332
    #
    # Read up on ssl_ciphers to ensure a secure configuration.
    # See: https://bugs.debian.org/765782

    # ...
}

^G Ayuda ^O Guardar ^F Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea
```

2. Server Blocks (Sitios Web Virtuales)

Un Server Block es una configuración que permite que un solo servidor Nginx aloje varios sitios web diferentes (similar a los Virtual Hosts de Apache).

1. Nuevo Sitio: Crea un Server Block para el dominio ficticio vyaryar541.seguridad.test.
2. Raíz propia: Los archivos de este sitio deben estar en /var/www/vyaryar541/public_html.
3. Contenido: Crea un index.html dentro de esa carpeta que identifique este nuevo sitio.
4. Activación: El sitio debe estar correctamente enlazado en sites-enabled.

Creamos la ruta entera con el comando:

```
sudo mkdir -p /var/www/vyaryar541/public_html
```

Agregamos permisos de

```
GNU nano 8.4 /var/www/vyaryar541/public_html/index.html
<html>
  <head>
    <title>vyaryar541</title>
  </head>
  <body>
    <h1>Exito! </h1>
  </body>
</html>
```

Ahora nos dirigimos a sites_available y creamos un documento de texto vyaryar541.seguridad.test e introducimos el código siguiente:

```
GNU nano 8.4 /etc/nginx/sites-available/vyaryar541.seguridad.test *
server {
    listen 2541;
    listen [::]:2541;

    root /var/www/vyaryar541/public_html;
    index index.html index.htm;

    server_name vyaryar541.seguridad.test;

    location / {
        try_files $uri $uri/ =404;
    }
}
```

Ahora debemos permitir el puerto 2541, por eso debemos instalar uncomplicated firewall e introducir este comando:

```
root@nginx-vyaryar541:~# ufw allow ssh
Rules updated
Rules updated (v6)
root@nginx-vyaryar541:~# ufw allow 2541/tcp
Rules updated
Rules updated (v6)
root@nginx-vyaryar541:~#
```

3. Hardening de Configuración

Aplica las siguientes medidas de seguridad para securizar el servidor frente a ataques:

1. Ocultación de Versión: Configura Nginx para que no muestre su número de versión en las cabeceras HTTP ni en las páginas de error (server_tokens).
2. Listado de Directorios: Asegúrate de que si una carpeta no tiene un index.html, el servidor no muestre la lista de archivos (autoindex).
3. Prevención de DoS: Limita el tamaño de subida de archivos a [DNI1] MB (client_max_body_size) para evitar que saturen tu disco duro con archivos gigantes.
4. Cabecera Anti-Clickjacking: Añade la cabecera de seguridad X-FrameOptions con el valor SAMEORIGIN.

Entramos en Nginx.conf y agregamos la configuración del enunciado

```
GNU nano 8.4 /etc/nginx/nginx.conf *
    worker_connections 768;
    # multi_accept on;
}

http {

    ##
    # Basic Settings
    ##

    sendfile on;
    tcp_nopush on;
    types_hash_max_size 2048;
    server_tokens off; # Recommended practice is to turn this off
    autoindex off;
    client_max_body_size 1M;
    add_header X-Frame-Options "SAMEORIGIN"

    # server_names_hash_bucket_size 64;
    # server_name_in_redirect off;
```

4. Control de Acceso y Restricciones

Vamos a restringir quién puede entrar a ciertas partes de tu web.

1. Protección por IP: Crea una ubicación (location) llamada /config. Solo el profesor (10.4.1.101) y tú mismo podréis entrar. El resto del mundo recibirá un error 403 Forbidden.

2. Autenticación por Contraseña: La carpeta /admin debe pedir usuario y contraseña.

o Usuario: admin

o Contraseña: [USER]

o Nota: Deberás instalar las utilidades de Apache (apache2-utils) para generar el archivo de claves.

Debemos instalar los utils con el comando `sudo apt install apache2-utils`

Creamos también el usuario nuevo con la contraseña de mi ipasen y dos carpetas con dos mensajes para saber si se ha logrado la entrada.

Abrimos la configuración en `nano /etc/nginx/sites-available/default` aplicamos los siguientes cambios:

```
GNU nano 8.4 /etc/nginx/sites-available/default
root /var/www/html;

# Add index.php to the list if you are using PHP
index index.html index.htm index.nginx-debian.html;

server_name _;

location /config {
    allow 10.4.1.101;
    allow 10.4.1.108;
    allow 127.0.0.1;
    deny all;
}

location /admin {
    auth_basic "Area solo administradores";
    auth_basic_user_file /etc/nginx/.htpasswd;
}
```

He cambiado la ruta para la conf de sites-avaiables: `sudo nano /etc/nginx/sites-available/puerto2541` ya que he tenido problemas por temas del puerto por defecto. Este es el contenido:

```
GNU nano 8.4 /etc/nginx/sites-available/puerto2541 *

listen 2541;
server_name _;

# Forzamos la raíz aquí
root /var/www/html;
index index.html;

# Logs específicos para ver errores de este puerto
access_log /var/log/nginx/puerto2541_access.log;
error_log /var/log/nginx/puerto2541_error.log;

location / {
    try_files $uri $uri/ =404;
}

location /config/ {
    allow 10.4.1.101;
    allow 10.4.1.108;
    allow 127.0.0.1;

    deny all;
}

location /admin/ {
    auth_basic "Area Restringida";
    auth_basic_user_file /etc/nginx/.htpasswd;
}
```

La comprobacion:

```
root@nginx-vyaryar541:~# curl -u admin:vyaryar541 http://10.4.1.108:2541/admin/
<h1>Zona ADMIN - Con contraseña</h1>
root@nginx-vyaryar541:~# curl -I http://10.4.1.108:2541/admin/
HTTP/1.1 401 Unauthorized
Server: nginx
Date: Sun, 25 Jan 2026 19:07:53 GMT
Content-Type: text/html
Content-Length: 172
Connection: keep-alive
WWW-Authenticate: Basic realm="Area Restringida"
```

5. Reglas de Seguridad Avanzada

Configura filtros inteligentes para detectar comportamientos sospechosos.

1. Bloqueo por User-Agent: Si alguien intenta acceder a tu web usando la herramienta curl desde la terminal, el servidor debe denegar el acceso (403). Solo se debe permitir el acceso desde navegadores normales.
2. Página 404 Personalizada: Si alguien busca un archivo que no existe, Nginx debe mostrar un archivo propio llamado error404.html con un diseño personalizado, en lugar de la página blanca y negra de Nginx.

Generamos un archivo de error diseñado con html en la ruta: `/var/www/html/error404.html`
Después hacemos unos cambios en el archivo de configuración nuevo:

```
GNU nano 8.4 /etc/nginx/sites-available/puerto2541 *

access_log /var/log/nginx/puerto2541_access.log;
error_log /var/log/nginx/puerto2541_error.log;

if ($http_user_agent ~* "curl") {
    return 403;
}

error_page 404 /error404.html;

location = /error404.html {
    root /var/www/html;
    internal;
}

location / {
    try_files $uri $uri/ =404;
}

location /config/ {
```

Restart a nginx y comprobamos con un curl:

```
nginx: configuration file /etc/nginx/nginx.conf test is successful
root@nginx-vyaryar541:~# curl -v http://10.4.1.108:2541/config/
* Trying 10.4.1.108:2541...
* Connected to 10.4.1.108 (10.4.1.108) port 2541
* using HTTP/1.x
> GET /config/ HTTP/1.1
> Host: 10.4.1.108:2541
> User-Agent: curl/8.14.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 403 Forbidden
< Server: nginx
< Date: Mon, 26 Jan 2026 00:00:17 GMT
< Content-Type: text/html
< Content-Length: 146
< Connection: keep-alive
<
<html>
<head><title>403 Forbidden</title></head>
<body>
```

Y si lo vemos a través de un navegador (w3m) pues nos da la respuesta:

```
Zona CONFIG - Solo IPs permitidas
```

Final del ejercicio

Una vez hayas completado el ejercicio, apaga la máquina virtual y realiza una instantánea.

Las modificaciones posteriores a esta instantánea se perderán, ya que el profesor la restaurará antes de comenzar la corrección.

Entrega

Realiza un documento en formato PDF con los cambios efectuados y súbelo a Moodle.

Este documento se utilizará como consulta en caso de duda durante la corrección, la cual se realizará a base de consultar el servidor web a partir de otra máquina virtual.