

Desarrollo de la Prueba - Seguridad de Servicios Críticos en Entornos Linux

INTEGRANTES : ALEX HENRIQUEZ - MACARENA QUIJADA - SIMON VELASQUEZ

Requerimiento 1: Seguridad de Acceso Remoto SSH (3 Puntos)

Objetivo

Implementar una configuración segura para el servicio SSH que contemple: cambiar el puerto por defecto, restringir el acceso a usuarios específicos y deshabilitar autenticación por contraseña (usar autenticación por llave).

1.1. Configuración de SSH y Firewall

Se configura el archivo `sshd_config` para cambiar el puerto por defecto a 2222, deshabilitar la autenticación por contraseña (`PasswordAuthentication no`), y restringir el acceso al usuario `alexxyugen` (`AllowUsers alexxyugen`). Además, se verifica que el firewall permite el tráfico en el nuevo puerto.

Comandos Ejecutados:

```
sudo grep -E 'Port|PasswordAuthentication|AllowUsers' /etc/ssh/sshd_config  
sudo firewall-cmd --list-all
```

Evidencia (Captura de Pantalla):

```
[alexxyugen@localhost ~]$ sudo grep -E 'Port|PermitRootLogin|PubkeyAuthentication|PasswordAuthentication|AllowUsers' /etc/ssh/sshd_config  
[sudo] password for alexxyugen:  
Port 2222  
PermitRootLogin no  
PubkeyAuthentication yes  
PasswordAuthentication no  
# PasswordAuthentication. Depending on your PAM configuration,  
# the setting of "PermitRootLogin without-password".  
# PAM authentication, then enable this but set PasswordAuthentication  
#GatewayPorts no  
AllowUsers alexxyugen  
[alexxyugen@localhost ~]$
```

```
[alexuyugen@localhost ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client dns ssh
  ports: 2222/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

1.2. Verificación de Acceso por Llave

Se demuestra que el acceso remoto al servidor SSH es exitoso utilizando únicamente la autenticación por llave, sin solicitar contraseña.

Comando Ejecutado (desde la máquina cliente):

```
ssh -p 2222 alexuyugen@192.168.196.137
```

Evidencia (Captura de Pantalla):

```
PS C:\Users\Alex Henriquez> ssh -p 2222 alexuyugen@192.168.196.137
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Jul 29 20:11:39 2025 from 192.168.196.1
[alexuyugen@localhost ~]$ |
```

Requerimiento 2: Gestión Segura de DNS (BIND) (3 Puntos)

Objetivo

Configurar un servidor DNS que resuelva correctamente un dominio interno, restrinja consultas externas e incluya validación de seguridad básica (como DNSSEC si aplica o listas de control de acceso).

2.1. Configuración del Dominio Interno y Restricción de Consultas

Se muestra el archivo de zona para el dominio interno zero.lan y se evidencia que las directivas allow-query y allow-recursion en named.conf restringen las consultas a la red local y localhost.

Comandos Ejecutados:

```
cat /var/named/db.zero.lan
sudo grep -E 'allow-query|allow-recursion' /etc/named.conf
```

Evidencia (Captura de Pantalla):

```
[alexuyugen@localhost ~]$ sudo cat /var/named/db.zero.lan
[sudo] password for alexuyugen:
$TTL      604800
@         IN      SOA      ns1.zero.lan. admin.zero.lan. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       ns1.zero.lan.
@         IN      A        192.168.196.137
ns1       IN      A        192.168.196.137
www       IN      A        192.168.196.137
; This is a zone-signing key, keyid 65346, for zero.lan.
; Created: 20250725015435 (Thu Jul 24 21:54:35 2025)
; Publish: 20250725015435 (Thu Jul 24 21:54:35 2025)
; Activate: 20250725015435 (Thu Jul 24 21:54:35 2025)
zero.lan. IN DNSKEY 256 3 8 AwEAAAGnETRWlaOpulKJOhG8gDKyFRfcBczAM7cwfdzoVKXoMZPa09LF x0yzy3rLRR5iZauqCSA4FNgn9ywfCSCr8dKygM3H72qrx8LE5H8eKCR PGD3FMyPWnIS9
hatmdz6Ru/r6Jg+yEHrYjl+vdcJ7r-fye+vqxyus6z U7dazHJD
; This is a key-signing key, keyid 6661, for zero.lan.
; Created: 20250725015425 (Thu Jul 24 21:54:25 2025)
; Publish: 20250725015425 (Thu Jul 24 21:54:25 2025)
; Activate: 20250725015425 (Thu Jul 24 21:54:25 2025)
zero.lan. IN DNSKEY 257 3 8 AwEAAAZe2Mmum4JAuAK0HE7wp+Iqie63Fj7dEbStrfIPj1eMLvfrq/U4f DKjRPxU7VJeB6/ryBqU1pWb2FYDFG03y3ot8fXfG1HAV7QJv7CTcQyzd H0gmbzUgjD4+Tc
O+M1NnjdyIgxurEtBWVxHDajHUTCnvB40Lk9H5rojd 9XwPJHCQfGHl6o8mAxuPFxBHrgySh26GITT0DmOXUe6JyLolJfAs67X Y30Bz79Jy4J9CgMKgzujKA5jltyF7pItCurqZNzD3DWZdCFhLK0Aqpey
oFViVm8vM36lFsqHflcddNXNevP+WExvRcEH6CeCIU5sivk1ZS2JxILJ Glon2APcQrU=
[alexuyugen@localhost ~]$
```

```
[alexuyugen@localhost ~]$ sudo grep -E 'allow-query|allow-recursion' /etc/named.conf
    allow-query      { localhost; 192.168.196.0/24; };
    allow-recursion { 192.168.196.0/24; localhost; localnets; }; //
[alexuyugen@localhost ~]$
```

2.2. Validación de Seguridad y Funcionamiento (DNSSEC)

Se verifica la sintaxis de la configuración de BIND y se demuestra la implementación y validación de DNSSEC para el dominio zero.lan, confirmando que la zona está firmada y validada criptográficamente.

Comandos Ejecutados:

```
sudo named-checkconf
sudo dig @localhost zero.lan DNSKEY +dnssec
```

Evidencia (Captura de Pantalla):

```
[alexuyugen@localhost ~]$ sudo named-checkconf
[alexuyugen@localhost ~]$ sudo dig @localhost zero.lan DNSKEY +dnssec

<<>> DiG 9.16.23-RH <<>> @localhost zero.lan DNSKEY +dnssec
(2 servers found)
; global options: +cmd
Got answer:
-->HEADER<<- opcode: QUERY, status: NOERROR, id: 58482
; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
EDNS: version: 0, flags: do; udp: 1232
COOKIE: a88122b078a4f15f01000006889734d6f34c1bde42e1975 (good)
;; QUESTION SECTION:
zero.lan.                IN      DNSKEY

;; ANSWER SECTION:
zero.lan. 604800 IN DNSKEY 256 3 8 AwEAAAGnETRWlaOpulkJOhG8gDKyFRfcbczAM7cwfDzoVhXoMzPa09LF x0yzy3rLRR5iZauqC5A4FNgGN9yWFCSCr8dKygm3H72
qrXBLE5H8eKCR PGD3FMyPWRnIS9hatmdz6Ru/r6Jg+yEHrRYjl+vdcJ7rfye+vxxyus6z U7dazHJD
zero.lan. 604800 IN DNSKEY 257 3 8 AwEAAZe2Mmum4JAuAK0hE7wp+Iqie63Fj7dEbStrfIPj1eMLvfrq/U4f DKjRPxU7VJeB6/ryBqU1pWb2FYDFG03y3ot8FXfG1HA
v7QJv7CtCQyzd H0gmbzUgjd4+Tc0+M1NnjdyIgxurEtBwVxHDajHUTcnvB40Lk9H5rojd 9XwPJHCQfGHL6o8mAxuPFxBHrgySh26GITt0DmOXUe6JyLoLjFAs67X Y30Bz79Jy4J9CgMKgzujKA5j1tyF
7pItCurqZNzD3DmZdCFhLK0Aqpey oFViVm8vM36lFsqHfLcddNXNevP+WExvRcEH6CeCIU5sIvk1ZS2JxILJ GLon2APcQrU=
zero.lan. 604800 IN RRSIG DNSKEY 8 2 604800 20250824010856 20250725010856 6661 zero.lan. gmGjF96f7DVTz/1/bVMsTZu3j6yAvN/vq6e+AnM2GS2hG
kxb4t92RBvF vA6X0Tsw1070EInc7e2MPM7oTPVbvIAS0VqRSdg6peR3SLCpZi09dBYH 2PjtXGH8g96rt+ykDyw+GxG/k5j5R6Za/fujZ6TMTYeywBREAGSM0ZRO 5qlVanBfeUo4/p5SGnLPygRnbCPPgL
mW2SRurbLRo9o/Ccw/+IGHTarC r56gnNrLtmIG4u2nLjWlG0Hi8GrnCCotIdZmSYMFERDGCNv2Gks9HVS4 0skSEIDuHkS4U494rzD2k0tmva0AOx89M2bzC9V9xcM3QvsemERRPnn16 YjUTbw==
zero.lan. 604800 IN RRSIG DNSKEY 8 2 604800 20250824010856 20250725010856 65346 zero.lan. YIRFI/VKjtzaJPr8mmQjhaJj4PdZy18s07azWn3mJnAL
8HfoH2oA3of2 80242zGF1Id+CBGaRi0kAuH6pbt9ia8/g8XMqev1p7IxJwiNuAJ65KL hFpadhca0P6aURvjAB9AKLxBQzridm17goh7XQBMoYbmQUhwrjhaQuDM Kko=

;; Query time: 3 msec
;; SERVER: ::1#53(::1)
;; WHEN: Tue Jul 29 21:20:13 -04 2025
;; MSG SIZE rcvd: 953

[alexuyugen@localhost ~]$
```

Requerimiento 3: Fortalecimiento de un Servidor Web Apache (4 Puntos)

Objetivo

Instalar y configurar Apache para servir un sitio web ficticio, aplicando buenas prácticas de seguridad: deshabilitar listados de directorios, ocultar información de la versión del servidor, configurar acceso HTTPS con un certificado autofirmado y crear reglas de restricción de acceso por IP a una sección del sitio.

3.1. Instalación de Apache y Hardening Básico

Se verifica la instalación y el estado de Apache, y se evidencia la configuración para ocultar la versión del servidor (ServerTokens Prod, ServerSignature Off) y deshabilitar los listados de directorios (Options -Indexes).

Comandos Ejecutados:

```
sudo systemctl status httpd
sudo grep -E 'ServerTokens|ServerSignature|Options -Indexes'
/etc/httpd/conf/httpd.conf
curl -I http://192.168.196.137
```

Evidencia (Captura de Pantalla):

```
[alexuyugen@localhost ~]$ systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: active (running) since Tue 2025-07-29 21:32:32 -04; 30s ago
     Docs: man:httpd.service(8)
  Main PID: 2666 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
     Tasks: 177 (Limit: 10723)
    Memory: 27.3M
       CPU: 90ms
    CGroup: /system.slice/httpd.service
            └─2666 /usr/sbin/httpd -DFOREGROUND
              └─2667 /usr/sbin/httpd -DFOREGROUND
                └─2668 /usr/sbin/httpd -DFOREGROUND
                  └─2669 /usr/sbin/httpd -DFOREGROUND
                    └─2670 /usr/sbin/httpd -DFOREGROUND

jul 29 21:32:32 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
jul 29 21:32:32 localhost.localdomain httpd[2666]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.1
jul 29 21:32:32 localhost.localdomain httpd[2666]: Server configured, listening on: port 80
jul 29 21:32:32 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
[alexuyugen@localhost ~]$ sudo grep -E 'ServerTokens|ServerSignature|Options -Indexes' /etc/httpd/conf/httpd.conf
ServerTokens Prod
ServerSignature Off
Options -Indexes
[alexuyugen@localhost ~]$
```

```
[alexuyugen@localhost ~]$ curl -I http://192.168.196.137
HTTP/1.1 403 Forbidden
Date: Wed, 30 Jul 2025 01:33:55 GMT
Server: Apache
Last-Modified: Sat, 17 May 2025 02:45:05 GMT
ETag: "1dc4-6354be2d9ae40"
Accept-Ranges: bytes
Content-Length: 7620
Content-Type: text/html; charset=UTF-8

[alexuyugen@localhost ~]$
```

3.2. Configuración HTTPS con Certificado Autofirmado

Se muestra la configuración del VirtualHost para el puerto 443 (HTTPS), utilizando un certificado autofirmado y su clave privada.

Se demuestra la existencia y los permisos correctos del directorio `/etc/ssl/private`, así como la existencia y los permisos adecuados de la clave privada y el certificado autofirmado. Posteriormente, se muestra la configuración del VirtualHost para el puerto 443 (HTTPS) en Apache.

```
[root@localhost /]# ls -ld /etc/ssl/private/
drwx-----. 2 root root 26 jul 29 21:53 /etc/ssl/private/
[root@localhost /]# ls -l /etc/ssl/private/mi_sitio.key
ls -l /tmp/mi_sitio.csr
-rw-r-----. 1 root apache 1704 jul 29 21:53 /etc/ssl/private/mi_sitio.key
-rw-r--r--. 1 root root 1005 jul 29 21:55 /tmp/mi_sitio.csr
[root@localhost /]# ls -l /etc/ssl/certs/mi_sitio.crt
-rw-r--r--. 1 root root 1269 jul 29 21:56 /etc/ssl/certs/mi_sitio.crt
[root@localhost /]# ls -l /etc/ssl/private/mi_sitio.key
-rw-r-----. 1 root apache 1704 jul 29 21:53 /etc/ssl/private/mi_sitio.key
[root@localhost /]#
```

Contenido del archivo de configuración del VirtualHost SSL

Evidencia (Captura de Pantalla):

```
GNU nano 5.6.1 /etc/httpd/conf.d/mi_sitio_ssl.conf
<VirtualHost *:443>
  ServerName 192.168.196.137|
  DocumentRoot /var/www/mi_sitio/public_html

  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/mi_sitio.crt
  SSLCertificateKeyFile /etc/ssl/private/mi_sitio.key

  <Directory "/var/www/mi_sitio/public_html">
    Options -Indexes +FollowSymLinks
    AllowOverride All
    Require all granted
  </Directory>

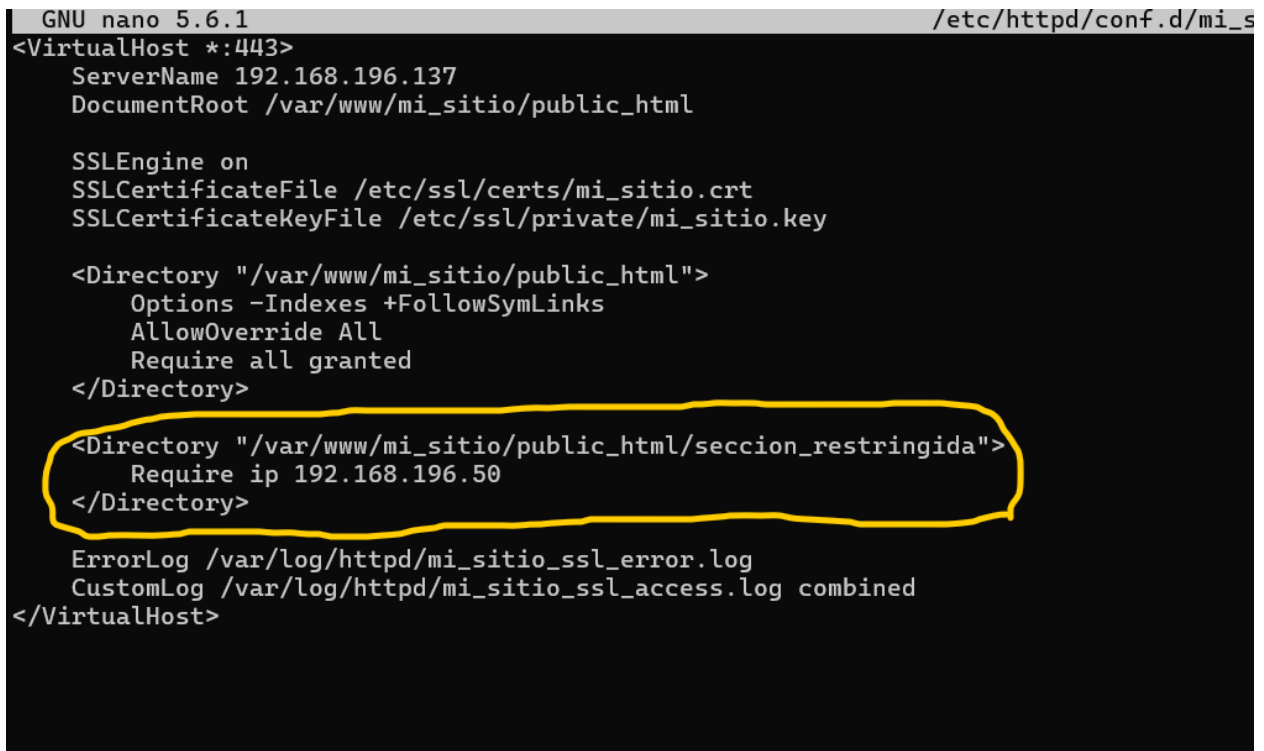
  ErrorLog /var/log/httpd/mi_sitio_ssl_error.log
  CustomLog /var/log/httpd/mi_sitio_ssl_access.log combined
</VirtualHost>
```

3.3. Creación de Reglas de Restricción de Acceso por IP

Se evidencia la configuración de un bloque <Directory> dentro del VirtualHost HTTPS que restringe el acceso a una sección específica del sitio (/seccion_restringida) a una dirección IP determinada.

Bloque <Directory> añadido en mi_sitio_ssl.conf (dentro del VirtualHost 443):

Evidencia (Captura de Pantalla):



```
GNU nano 5.6.1 /etc/httpd/conf.d/mi_s
<VirtualHost *:443>
  ServerName 192.168.196.137
  DocumentRoot /var/www/mi_sitio/public_html

  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/mi_sitio.crt
  SSLCertificateKeyFile /etc/ssl/private/mi_sitio.key

  <Directory "/var/www/mi_sitio/public_html">
    Options -Indexes +FollowSymLinks
    AllowOverride All
    Require all granted
  </Directory>

  <Directory "/var/www/mi_sitio/public_html/seccion_restringida">
    Require ip 192.168.196.50
  </Directory>

  ErrorLog /var/log/httpd/mi_sitio_ssl_error.log
  CustomLog /var/log/httpd/mi_sitio_ssl_access.log combined
</VirtualHost>
```

3.4. Verificación de Todas las Configuraciones de Apache

Se realizan pruebas para demostrar el correcto funcionamiento de HTTPS y la restricción de acceso por IP.

Comandos Ejecutados:

```
sudo systemctl restart httpd
curl -vk https://192.168.196.137/
curl -k https://192.168.196.137/seccion_restringida/
```

Evidencia (Captura de Pantalla):

```
[root@localhost /]# curl -vk https://192.168.196.137/
* Trying 192.168.196.137:443...
* Connected to 192.168.196.137 (192.168.196.137) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
* TLSv1.0 (OUT), TLS header, Certificate Status (22):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS header, Finished (20):
* TLSv1.2 (IN), TLS header, Unknown (23):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.2 (IN), TLS header, Unknown (23):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS header, Unknown (23):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.2 (IN), TLS header, Unknown (23):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.2 (OUT), TLS header, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS header, Unknown (23):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: C=CL; ST=Araucania; L=Villarrica; O=DesafioLATAM; CN=192.168.196.137
*  start date: Jul 30 01:56:58 2025 GMT
*  expire date: Jul 30 01:56:58 2026 GMT
*  issuer: C=CL; ST=Araucania; L=Villarrica; O=DesafioLATAM; CN=192.168.196.137
*  SSL certificate verify result: self-signed certificate (18), continuing anyway.
* TLSv1.2 (OUT), TLS header, Unknown (23):
> GET / HTTP/1.1
> Host: 192.168.196.137
> User-Agent: curl/7.76.1
> Accept: */*
```

```
>
* TLSv1.2 (IN), TLS header, Unknown (23):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.2 (IN), TLS header, Unknown (23):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* old SSL session ID is stale, removing
* TLSv1.2 (IN), TLS header, Unknown (23):
* Mark bundle as not supporting multiuse
< HTTP/1.1 403 Forbidden
< Date: Wed, 30 Jul 2025 02:38:56 GMT
< Server: Apache
< Last-Modified: Sat, 17 May 2025 02:45:05 GMT
< ETag: "1dc4-6354be2d9ae40"
< Accept-Ranges: bytes
< Content-Length: 7620
< Content-Type: text/html; charset=UTF-8
<
<!doctype html>
```



```
[alexuyugen@localhost ~]$ curl -k https://192.168.196.137/seccion_restringida/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
</body></html>
[alexuyugen@localhost ~]$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.196.157 netmask 255.255.255.0 broadcast 192.168.196.255
    inet6 fe80::20c:29ff:fe61:f996 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:61:f9:96 txqueuelen 1000 (Ethernet)
    RX packets 40058 bytes 57590589 (54.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13322 bytes 754967 (737.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 23 bytes 2283 (2.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23 bytes 2283 (2.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[alexuyugen@localhost ~]$ █
```

(captura desde el cliente al servidor apache)