

**TRABAJO DE INVESTIGACIÓN - HACKING ÉTICO Y LAS VULNERABILIDADES
DE LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE
TACNA, 2024**

Anexo 1. Parte práctica

i. Escenario donde se realizaron las pruebas de hacking ético

Para las pruebas de hacking ético, se utilizó la metodología de pruebas de penetración de OWASP TOP 10, dado que nos permite comprender y mitigar los riesgos de seguridad más críticos de los sistemas de información de la Municipalidad Provincial de Tacna.

ii. Ámbito del test

Se basa en las pruebas realizadas, las cuales fueron:

- ✓ Pruebas a puertos abiertos
- ✓ Pruebas hacia servidores web
- ✓ Prueba de Fallos Criptográficos
- ✓ Pruebas de Vulnerabilidad

iii. Desarrollo

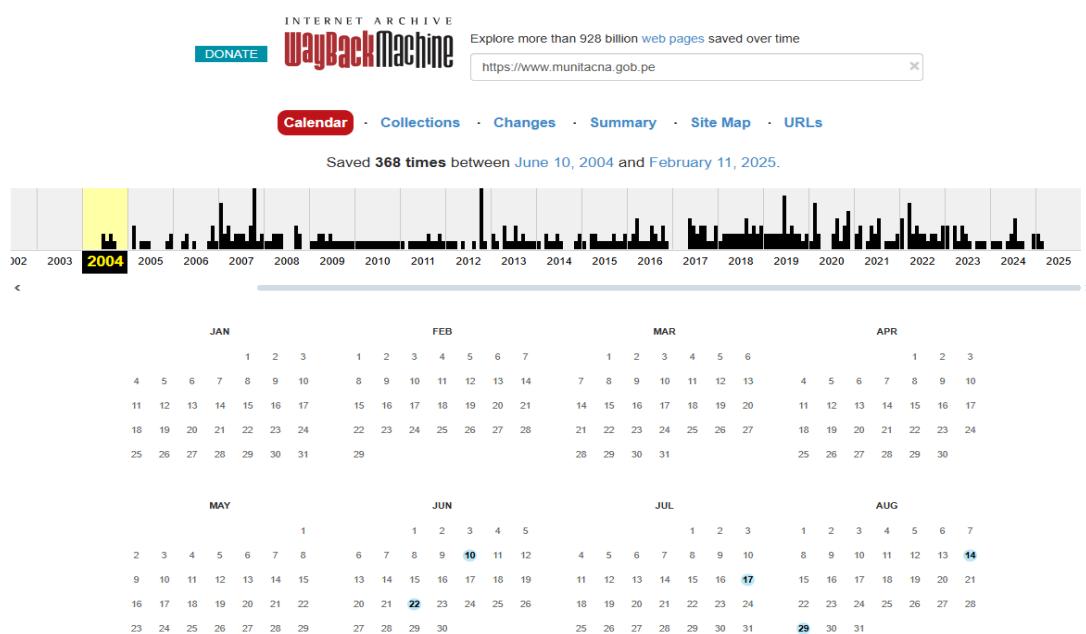
a) Wayback Machine

Wayback Machine es una plataforma que permite acceder a copias archivadas de sitios web, facilitando la exploración de sus versiones anteriores. Es especialmente útil para recuperar información que ha sido eliminada, estudiar la evolución estructural y visual de un sitio, o realizar análisis históricos del contenido digital. Aunque no es una herramienta reciente en el ámbito de análisis web, sigue siendo sumamente valiosa para investigaciones forenses, auditorías digitales y estudios de OSINT Open Source Intelligence (Inteligencia de Fuentes Abiertas).

Descripción: como se muestra en la imagen, la plataforma Wayback Machine cuenta con un repositorio de la página web (<https://www.munitacna.gob.pe>) de la Municipalidad Provincial de Tacna desde el 10 de junio del 2004.

Figura 1

Página Web - Wayback Machine - Consulta 2004

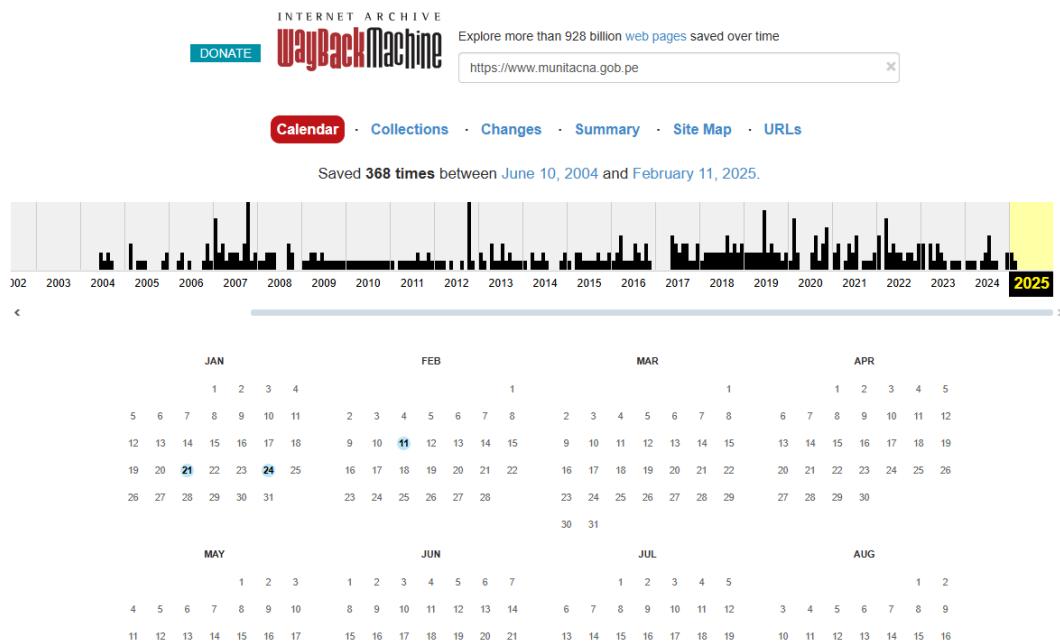


Nota. Elaboración propia

Descripción: la última modificación de la página web (<https://www.munitacna.gob.pe>), registrada en la plataforma es del 11 de febrero del 2025.

Figura 2

Página Web - Wayback Machine - Consulta 2025

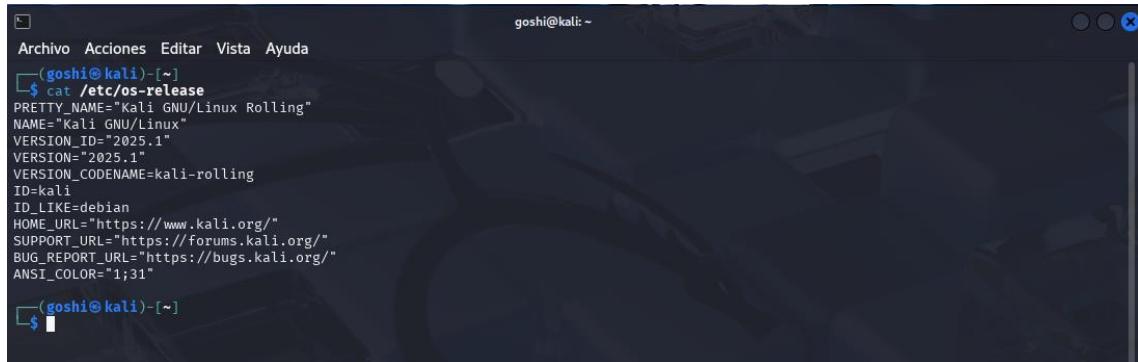


Nota. Elaboración propia

b) KALI LINUX

Kali Linux es una distribución de código abierto basada en Linux, diseñada específicamente para llevar a cabo pruebas de penetración, análisis forense digital y tareas relacionadas con la ciberseguridad. Su amplio conjunto de herramientas preinstaladas lo convierte en una plataforma robusta para profesionales en evaluación de seguridad informática.

Descripción: Para este caso se utilizó la distribución de Kali Linux, de versión 2025.1. Como se muestra en la imagen.

Figura 3**Sistema Operativo - Kali Linux**


```
(goshi㉿kali)-[~]
$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2025.1"
VERSION="2025.1"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
(goshi㉿kali)-[~]
$
```

Nota. Elaboración propia

c) WHOIS

WHOIS es un protocolo de consulta utilizado para acceder a bases de datos que almacenan información registral sobre nombres de dominio y direcciones IP. A través de este servicio, es posible recuperar detalles del registrante, como el nombre del titular, información de contacto, fechas de creación y expiración del dominio, así como datos del registrador.

Sistema Principal - Municipalidad Provincial de Tacna

Dirección Web: www.munitacna.gob.pe

Descripción: para obtener la información de la página web (<https://www.munitacna.gob.pe>), abrimos un terminal en Kali Linux, e ingresamos el comando **whois munitacna.gob.pe** el cual nos mostrara la información detallada.

Figura 4

Comando whois para ver información del dominio.



```

goshi@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
(goshi@kali)-[~] $ whois munitacna.gob.pe
Domain Name: munitacna.gob.pe
Sponsoring Registrar: NIC.PE
Domain Status: ok
Registrant Name: municipalidad provincial de tacna
Admin Name: Luis S.J. Trabucco Vizcarra
Admin Email: lsjtrabucco@hotmail.com
Name Server: ns1.rcp.net.pe
Name Server: ns2.rcp.net.pe
>>> Last update of WHOIS database: 2025-04-20T16:57:33.344Z <<<
La informacion de esta pagina se provee exclusivamente para fines relacionados con la delegacion de nombres de dominios, su publicidad y la operacion del DNS administrado por el NIC .Pe.
Queda absolutamente prohibido el uso de los datos proporcionados para cualquier otra finalidad distinta a la indicada, incluyendo el envio de correo electronico comercial no solicitado, de acuerdo a lo dispuesto en la Ley N 28493 - Ley Peruana Antispam.
La base de datos generada a partir del sistema de delegacion de nombres de dominio peruanos esta protegida por las leyes nacionales de Propiedad Intelectual y los tratados internacionales que sobre la materia ha suscrito el Peru. En ese sentido, su autorizacion es exclusivamente para visualizar y conocer el contenido de la misma, por lo que queda expresamente prohibida su reproduccion, comunicacion, distribucion, transformacion y cualquier otro uso distinto al autorizado.

(goshi@kali)-[~] $ 

```

Nota. Elaboración propia

d) ESCANEOS DE RED CON NMAP

Nmap, abreviatura de Network Mapper, es una herramienta de código abierto basada en línea de comandos en entornos Linux, utilizada principalmente para realizar escaneos de direcciones IP y puertos dentro de una red, así como para identificar aplicaciones activas.

Esta utilidad es ampliamente empleada por administradores de red para identificar dispositivos conectados, descubrir servicios y puertos abiertos, y detectar posibles vulnerabilidades en los sistemas analizados.

Sistema Principal - Municipalidad Provincial de Tacna

Dirección Web: sistram.munitacna.gob.pe/

Figura 5

Página Web de la Municipalidad Provincial de Tacna.



Nota. Elaboración propia

Descripción: ejecutamos el comando **nmap -sC -sV -oN scan.txt munitacna.gob.pe** en la consola. Donde:

- ✓ **-sC** Incluye en el análisis actual el conjunto por defecto de scripts (algunos pueden ser intrusivos).
- ✓ **-sV** identifica servicios y versiones
- ✓ **-oN** Registra en un fichero una salida muy similar a la mostrada por pantalla en modo interactivo.
- ✓ **scan.txt** archivo donde se guardará el registro.

Como se muestra en la imagen se tienen abiertos los puertos:

- ✓ 80/tcp
- ✓ 443/tcp

Figura 6

Escaneo de Red con el comando nmap – Pagina Web Municipalidad Provincial de Tacna

```
(goshi㉿kali)-[~]
$ nmap -sC -sV -oN scan.txt munitacna.gob.pe
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-20 12:01 -05
Nmap scan report for munitacna.gob.pe (168.121.50.246)
Host is up (0.049s latency).
rDNS record for 168.121.50.246: mail.munitacna.gob.pe
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd
|_http-title: Did not follow redirect to https://www.munitacna.gob.pe/
|_http-server-header: Apache
113/tcp   closed ident
443/tcp   open  ssl/https Apache httpd (PHP 7.3.28)
|_http-title: Municipalidad Provincial de Tacna
| ssl-cert: Subject: commonName=.munitacna.gob.pe
| Subject Alternative Name: DNS:*.munitacna.gob.pe, DNS:munitacna.gob.pe
| Not valid before: 2024-05-27T00:00:00
| Not valid after:  2025-05-28T23:59:59
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache
|_http-cors: GET POST PUT DELETE OPTIONS

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.46 seconds
```

Nota. Elaboración propia

Sistema de Mesa de Partes Virtual - Municipalidad Provincial de Tacna

Dirección Web: sistram.munitacna.gob.pe/

Figura 7

Página Web de Mesa de Partes Virtual - Municipalidad Provincial de Tacna.

Mesa de Partes Virtual - Municipalidad Provincial de Tacna

La Municipalidad Provincial de Tacna pone a su disposición la MESA DE PARTES VIRTUAL, para la recepción de documentos y solicitudes durante el Estado de Emergencia.

En cumplimiento de la Ley N° 29535 capítulos I, II y III que establece el derecho a la accesibilidad de la información, así como también el fomento de la comunicación, plataformas de atención al usuario, para personas con discapacidad.

HORARIO DE REGISTRO Y RECEPCIÓN:

LA ATENCIÓN DE NUESTRA MESA DE PARTES VIRTUAL SON LAS 24 HORAS DEL DÍA, LOS 7 DÍAS DE LA SEMANA

Nota. Elaboración propia

Descripción: ejecutamos el comando **nmap -sC -sV -oN scan.txt sistram.munitacna.gob.pe** en la consola. Donde:

- ✓ **-sC** Incluye en el análisis actual el conjunto por defecto de scripts (algunos pueden ser intrusivos).
- ✓ **-sV** identifica servicios y versiones
- ✓ **-oN** Registra en un fichero una salida muy similar a la mostrada por pantalla en modo interactivo.
- ✓ **scan.txt** archivo donde se guardará el registro.

Como se muestra en la imagen se tienen abiertos los puertos:

- ✓ 80/tcp
- ✓ 443/tcp

Figura 8

Escaneo de Red con el comando nmap - Página Web de Mesa de Partes Virtual - Municipalidad Provincial de Tacna

```
(goshi㉿kali)-[~]
$ nmap -sC -sV -oN scan.txt sistram.munitacna.gob.pe
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 21:41 -05
Nmap scan report for sistram.munitacna.gob.pe (168.121.50.253)
Host is up (0.034s latency).
rDNS record for 168.121.50.253: mail.munitacna.gob.pe
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.20.1
|_http-title: Did not follow redirect to https://sistram.munitacna.gob.pe/
|_http-server-header: nginx/1.20.1
113/tcp   closed ident
443/tcp   open  ssl/http nginx 1.20.1
|_tls-nextprotoneg:
|   h2
|_http/1.1
|_http-server-header: nginx/1.20.1
| tls-alpn:
|   h2
|_http/1.1
| ssl-cert: Subject: commonName=*.munitacna.gob.pe
| Subject Alternative Name: DNS:*.munitacna.gob.pe, DNS:munitacna.gob.pe
| Not valid before: 2025-05-29T00:00:00
|_Not valid after:  2026-06-29T23:59:59
|_ssl-date: TLS randomness does not represent time
|_http-cors: GET POST PUT DELETE OPTIONS
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.57 seconds
(goshi㉿kali)-[~]
```

Nota. Elaboración propia

Sistema de Correo - Municipalidad Provincial de Tacna

Dirección Web: mail.munitacna.gob.pe

Figura 9

Página Web de Sistema de Correo - Municipalidad Provincial de Tacna



Nota. Elaboración propia

Descripción: ejecutamos el comando **nmap -sC -sV -oN scan.txt mail.munitacna.gob.pe** en la consola. Donde:

- ✓ **-sC** Incluye en el análisis actual el conjunto por defecto de scripts (algunos pueden ser intrusivos).
- ✓ **-sV** identifica servicios y versiones
- ✓ **-oN** Registra en un fichero una salida muy similar a la mostrada por pantalla en modo interactivo.
- ✓ **scan.txt** archivo donde se guardará el registro.

Como se muestra en la imagen se tienen abiertos los puertos:

- ✓ 80/tcp
- ✓ 443/tcp
- ✓ 25/tcp
- ✓ 80/tcp
- ✓ 443/tcp
- ✓ 465/tcp
- ✓ 993/tcp

Figura 10

Escaneo de Red con el comando nmap - Página Web de Sistema de Correo - Municipalidad Provincial de Tacna

```
(goshi㉿kali)-[~]
$ nmap -sC -sV -oN scan.txt mail.munitacna.gob.pe
Starting Nmap 7.91 ( https://nmap.org ) at 2025-06-07 21:43 -05
Nmap scan report for mail.munitacna.gob.pe (168.121.50.250)
Host is up (0.032s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp          Postfix smtpd
|_smtp-commands: SMTP: EHLO 220 mail.munitacna.gob.pe ESMTP Postfix\x0D
80/tcp    open  http         nginx 1.20.1
|_http-server-header: nginx/1.20.1
|_http-title: Site doesn't have a title (text/html).
113/tcp   closed ident
443/tcp   open  ssl/http     nginx
|_ssl-date: TLS randomness does not represent time
|_tls-alpn:
| h2
| http/1.1
|_ssl-cert: Subject: commonName@mail.munitacna.gob.pe
| Subject Alternative Name: DNS:mail.munitacna.gob.pe, DNS:www.mail.munitacna.gob.pe
| Not valid before: 2024-09-30T00:00:00
| Not valid after:  2025-10-31T23:59:59
|_http-title: Zimbra Web Client Sign In
| tls-nextprotoneg:
| h2
| http/1.1
465/tcp   open  ssl/smtp     Postfix smtpd
|_ssl-cert: Subject: commonName@mail.munitacna.gob.pe
| Subject Alternative Name: DNS:mail.munitacna.gob.pe, DNS:www.mail.munitacna.gob.pe
| Not valid before: 2024-09-30T00:00:00
| Not valid after:  2025-10-31T23:59:59
|_smtp-commands: mail.munitacna.gob.pe, PIPELINING, SIZE 50331648, VRFY, ETRN, AUTH LOGIN PLAIN, AUTH=LOGIN PLAIN, ENHANCEDST
ATUSCODES, BBITMIME, DSN, CHUNKING
|_ssl-date: TLS randomness does not represent time
993/tcp   open  ssl/imap-proxy Zimbra imaps
|_imap-capabilities: CATENATE completed OK CHILDREN NAMESPACES CONSTORE AUTH=PLAINA0001 QUOTA IMAP4rev1 ACL UNSELECT WITHIN U
IDPLUS BINARY IDLE QRESYNC SORT LITERAL+ RIGHTS=ektx SEARCHRES LIST-STATUS SASL-IR ENABLE LIST-EXTENDED XLIST ESEARCH MULT
IAPPEND I18NLEVEL=1 THREAD=ORDEREDSUBJECT ESORT
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName@mail.munitacna.gob.pe
| Subject Alternative Name: DNS:mail.munitacna.gob.pe, DNS:www.mail.munitacna.gob.pe
| Not valid before: 2024-09-30T00:00:00
| Not valid after:  2025-10-31T23:59:59
Service Info: Hosts: -mail.munitacna.gob.pe, mail.munitacna.gob.pe

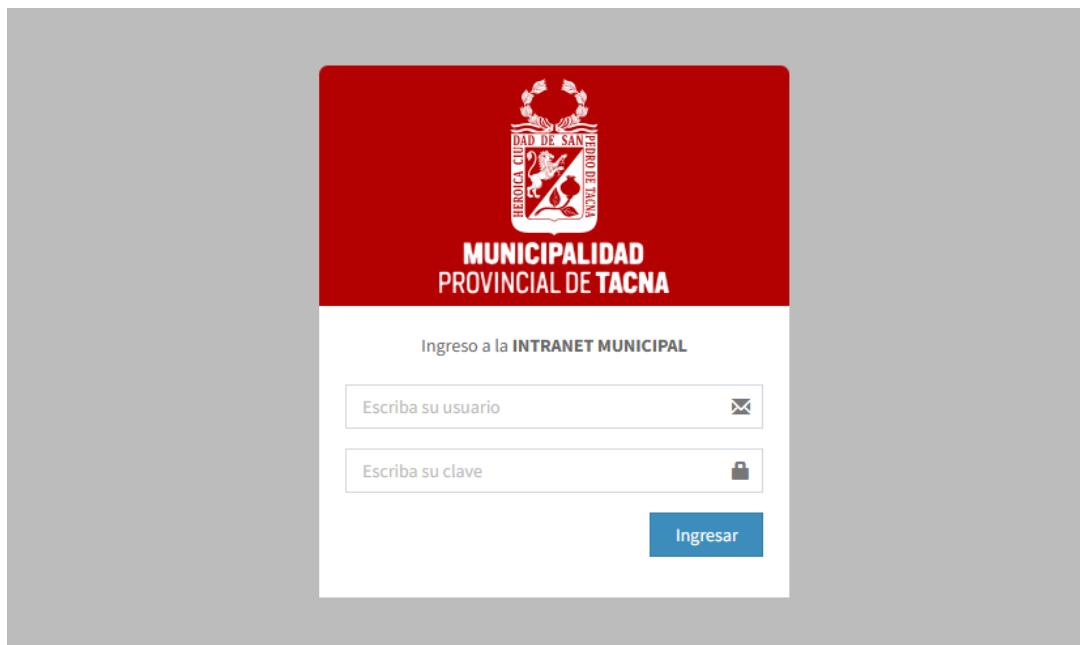
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.34 seconds
```

Nota. Elaboración propia

Sistema de Sistema Intranet - Municipalidad Provincial de Tacna
 Dirección Web: app.munitacna.gob.pe

Figura 11

Página Web de Sistema Intranet - Municipalidad Provincial de Tacna



Nota. Elaboración propia

Descripción: ejecutamos el comando **nmap -sC -sV -oN scan.txt app.munitacna.gob.pe** en la consola. Donde:

- ✓ **-sC** Incluye en el análisis actual el conjunto por defecto de scripts (algunos pueden ser intrusivos).
- ✓ **-sV** identifica servicios y versiones
- ✓ **-oN** Registra en un fichero una salida muy similar a la mostrada por pantalla en modo interactivo.
- ✓ **scan.txt** archivo donde se guardará el registro.

Como se muestra en la imagen se tienen abiertos los puertos:

- ✓ 80/tcp
- ✓ 443/tcp

Figura 12

Escaneo de Red con el comando nmap - Página Web de Intranet - Municipalidad Provincial de Tacna

```
(goshi㉿kali)-[~]
$ nmap -sC -sV -oN scan.txt app.munitacna.gob.pe
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-07 21:46 -05
Nmap scan report for app.munitacna.gob.pe (168.121.50.253)
Host is up (0.033s latency).
rDNS record for 168.121.50.253: mail.munitacna.gob.pe
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx 1.20.1
|_http-server-header: nginx/1.20.1
|_http-title: Site doesn't have a title (text/html).
113/tcp   closed ident
443/tcp   open  ssl/http nginx 1.20.1
|_tls-alpn:
|  h2
|_http/1.1
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=*.munitacna.gob.pe
| Subject Alternative Name: DNS:*.munitacna.gob.pe, DNS:munitacna.gob.pe
| Not valid before: 2025-05-29T00:00:00
| Not valid after:  2026-06-29T23:59:59
|_http-server-header: nginx/1.20.1
|_tls-nextprotoneg:
|  h2
|_http/1.1
|_http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.94 seconds
```

Nota. Elaboración propia

e) ENUMERACIÓN

La enumeración es una fase del reconocimiento activo en la que se recopila información detallada del sistema objetivo, con el fin de identificar su configuración, servicios activos, recursos compartidos y otros componentes del entorno que puedan ser aprovechados en una evaluación de seguridad.

Representa una etapa esencial dentro de una prueba de penetración, ya que implica establecer una conexión activa con el sistema objetivo para obtener la mayor cantidad de información posible. Estos datos, como usuarios, servicios, recursos compartidos o configuraciones del sistema, pueden ser fundamentales para identificar vectores de ataque y facilitar la explotación posterior del entorno.

DNSenum

Es una herramienta robusta diseñada para realizar una enumeración DNS avanzada. Permite desde la recopilación de registros DNS convencionales hasta la ejecución de fuerza bruta sobre subdominios y la realización de consultas recursivas. Gracias a su

amplia funcionalidad, se convierte en un recurso esencial durante auditorías de seguridad y pruebas de penetración.

Sistema Principal - Municipalidad Provincial de Tacna

Dirección Web: sistram.munitacna.gob.pe/

Descripción: ejecutamos el comando **dnsenum --enum munitacna.gob.pe** en la consola. Donde:

- ✓ **--enum** Le dice a la herramienta que realice una enumeración DNS estándar

Figura 13

Enumeración de DNS con el comando dnsenum

```

Archivo  Acciones  Editar  Vista  Ayuda

[(goshi㉿kali)-~]
$ dnsenum --enum munitacna.gob.pe
dnsenum VERSION:1.3.1
      munitacna.gob.pe

Host's addresses:
_____
munitacna.gob.pe.          4945     IN    A      168.121.50.246

Name Servers:
_____
NS2.RCP.NET.pe.           193     IN    A      209.45.127.3
NS.RCP.NET.pe.            1625     IN    A      161.132.17.10

Mail (MX) Servers:
_____
errdomain.                 0     IN    A      127.0.0.1

Trying Zone Transfers and getting Bind Versions:
_____
Trying Zone Transfer for munitacna.gob.pe on NS2.RCP.NET.pe ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for munitacna.gob.pe on NS.RCP.NET.pe ...
AXFR record query failed: NOTAUTH

```

```

Scraping munitacna.gob.pe subdomains from Google:
_____
— Google search page: 1 —
registro
mail
w
app
app

— Google search page: 2 —

— Google search page: 3 —

Google Results:
_____
registro.munitacna.gob.pe.      7200    IN   A       168.121.50.246
mail.munitacna.gob.pe.          7200    IN   A       168.121.50.250
app.munitacna.gob.pe.          7200    IN   A       168.121.50.253
w.munitacna.gob.pe.            7200    IN   A       168.121.50.253

Brute Forcing with /usr/share/dnsenum/dns.txt:
_____
apps.munitacna.gob.pe.        7200    IN   A       168.121.50.243
intranet.munitacna.gob.pe.     7200    IN   A       168.121.50.244
smtp.munitacna.gob.pe.        7200    IN   CNAME  mailersend.net.
mailersend.net.                300     IN   A       104.26.6.57
mailersend.net.                300     IN   A       172.67.74.79
mailersend.net.                300     IN   A       104.26.7.57

[+] goshi@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda

Launching Whois Queries:
_____
whois ip result:  168.121.50.0      →      168.121.50.0/28

munitacna.gob.pe_____
168.121.50.0/28

Performing reverse lookup on 16 ip addresses:
_____
0 results out of 16 IP addresses.

munitacna.gob.pe ip blocks:
_____
done.

[(goshi@kali)-[~]] $ [ ]

```

Nota. Elaboración propia

f) FALLOS CRIPTOGRAFICOS CON SSLSCAN

SSLSCAN

sslscan es una herramienta utilizada para analizar servicios que utilizan SSL/TLS (Secure Sockets Layer – protocolo que permite a los sistemas verificar la identidad y, posteriormente, establecer una conexión de red cifrada con otro sistema), como HTTPS, con el propósito de identificar los algoritmos de cifrado y protocolos que son compatibles con el servidor. Esta utilidad permite evaluar la configuración de seguridad y detectar posibles debilidades en la implementación del cifrado.

Descripción: ejecutamos el comando **sslscan** en la consola. Para verificar si tenemos instalada la herramienta y su versión.

Figura 14

Verificación del servicio SSL/TLS, con el comando **sslscan**

```

goshi@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
(goshi@kali)-[~]
$ sslscan
[...]
2.1.5
OpenSSL 3.4.0 22 Oct 2024

Command:
  sslscan [options] [host:port | host]

Options:
  --targets=<file>      A file containing a list of hosts to check.
  --sni-name=<name>      Hostname for SNI
  --ipv4, -4              Only use IPv4
  --ipv6, -6              Only use IPv6

  --show-certificate     Show full certificate information
  --show-certificates   Show chain full certificates information
  --show-client-cas     Show trusted CAs for TLS client auth
  --no-check-certificate Don't warn about weak certificate algorithm or keys
  --ocsp                 Request OCSP response from server
  --pk=<file>           A file containing the private key or a PKCS#12 file
                        containing a private key/certificate pair
  --pkpass=<password>   The password for the private key or PKCS#12 file
  --certs=<file>         A file containing PEM/ASN1 formatted client certificates

```

Nota. Elaboración propia

Sistema Principal - Municipalidad Provincial de Tacna

Dirección Web: www.munitacna.gob.pe

Descripción: ejecutamos el comando **sudo sslscan munitacna.gob.pe** en la consola.

Donde:

- ✓ **sudo** permite ejecutar comandos o programas con los permisos con los privilegios administrativos del usuario root.

- ✓ **ssllscan** analiza los servicios SSL/TLS para identificar vulnerabilidades de seguridad

como se muestra en la imagen se tiene habilitado varios protocolos de SSL, el protocolo que permite SSLv3 y utiliza cifrados DES y RC4. Esta en rojo lo que indica una configuración insegura.

Figura 15

Ejecución del ssllscan a la página web – Municipalidad Provincial de Tacna

```
goshi@kali: ~
Archivo Acciones Editar Vista Ayuda
(goshi@kali)-[~]
$ sudo ssllscan munitacna.gob.pe
[sudo] contraseña para goshi:
Version: 2.1.5
OpenSSL 3.4.0 22 Oct 2024

Connected to 168.121.50.246

Testing SSL server munitacna.gob.pe on port 443 using SNI name munitacna.gob.pe

SSL/TLS Protocols:
SSLv2 disabled
SSLv3 enabled
TLSv1.0 enabled
TLSv1.1 enabled
TLSv1.2 enabled
TLSv1.3 disabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Secure session renegotiation supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

goshi@kali: ~
Archivo Acciones Editar Vista Ayuda
Supported Server Cipher(s):
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 2048 bits
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
Accepted TLSv1.2 128 bits DHE-RSA-AES128-SHA256 DHE 2048 bits
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-CAMELLIA256-SHA DHE 2048 bits
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.2 128 bits DHE-RSA-AES128-SHA DHE 2048 bits
Accepted TLSv1.2 128 bits DHE-RSA-SEED-SHA DHE 2048 bits
Accepted TLSv1.2 128 bits DHE-RSA-CAMELLIA128-SHA DHE 2048 bits
Accepted TLSv1.2 256 bits AES256-GCM-SHA384
Accepted TLSv1.2 128 bits AES128-GCM-SHA256
Accepted TLSv1.2 256 bits AES256-SHA256
Accepted TLSv1.2 128 bits AES128-SHA256
Accepted TLSv1.2 256 bits AES256-SHA
Accepted TLSv1.2 128 bits CAMELLIA256-SHA
Accepted TLSv1.2 128 bits AES128-SHA
Accepted TLSv1.2 128 bits SEED-SHA
Accepted TLSv1.2 128 bits CAMELLIA128-SHA
Accepted TLSv1.2 128 bits TLS_RSA_WITH_RC4_128_MD5
Accepted TLSv1.2 128 bits TLS_RSA_WITH_RC4_128_SHA
Accepted TLSv1.2 128 bits TLS_RSA_WITH_IDEA_CBC_SHA
Accepted TLSv1.2 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.2 112 bits TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.2 128 bits TLS_ECDHE_RSA_WITH_RC4_128_SHA
```

```

goshi@kali: ~
Archivo Acciones Editar Vista Ayuda
Accepted TLSv1.2 112 bits TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
Preferred TLSv1.1 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.1 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
Accepted TLSv1.1 256 bits DHE-RSA-CAMELLIA256-SHA DHE 2048 bits
Accepted TLSv1.1 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.1 128 bits DHE-RSA-AES128-SHA DHE 2048 bits
Accepted TLSv1.1 128 bits DHE-RSA-SEED-SHA DHE 2048 bits
Accepted TLSv1.1 128 bits DHE-RSA-CAMELLIA128-SHA DHE 2048 bits
Accepted TLSv1.1 256 bits AES256-SHA
Accepted TLSv1.1 256 bits CAMELLIA256-SHA
Accepted TLSv1.1 128 bits AES128-SHA
Accepted TLSv1.1 128 bits SEED-SHA
Accepted TLSv1.1 128 bits CAMELLIA128-SHA
Accepted TLSv1.1 128 bits TLS_RSA_WITH_RC4_128_MD5
Accepted TLSv1.1 128 bits TLS_RSA_WITH_RC4_128_SHA
Accepted TLSv1.1 128 bits TLS_RSA_WITH_IDEA_CBC_SHA
Accepted TLSv1.1 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.1 112 bits TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.1 128 bits TLS_ECDHE_RSA_WITH_RC4_128_SHA
Accepted TLSv1.1 112 bits TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
Preferred TLSv1.0 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.0 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
Accepted TLSv1.0 256 bits DHE-RSA-CAMELLIA256-SHA DHE 2048 bits
Accepted TLSv1.0 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
Accepted TLSv1.0 128 bits DHE-RSA-AES128-SHA DHE 2048 bits
Accepted TLSv1.0 128 bits DHE-RSA-SEED-SHA DHE 2048 bits
Accepted TLSv1.0 128 bits DHE-RSA-CAMELLIA128-SHA DHE 2048 bits
Accepted TLSv1.0 256 bits AES256-SHA
Accepted TLSv1.0 256 bits CAMELLIA256-SHA
Accepted TLSv1.0 128 bits AES128-SHA
Accepted TLSv1.0 128 bits SEED-SHA
Accepted TLSv1.0 128 bits CAMELLIA128-SHA
Accepted TLSv1.0 128 bits TLS_RSA_WITH_RC4_128_MD5
Accepted TLSv1.0 128 bits TLS_RSA_WITH_RC4_128_SHA
Accepted TLSv1.0 128 bits TLS_RSA_WITH_IDEA_CBC_SHA
Accepted TLSv1.0 112 bits TLS_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.0 112 bits TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Accepted TLSv1.0 128 bits TLS_ECDHE_RSA_WITH_RC4_128_SHA
Accepted TLSv1.0 112 bits TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

Server Key Exchange Group(s):
TLSv1.2 128 bits secp256k1
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 260 bits secp521r1 (NIST P-521)

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: *.munitacna.gob.pe
AltNames: DNS:*.munitacna.gob.pe, DNS:munitacna.gob.pe
Issuer: Sectigo RSA Domain Validation Secure Server CA

Not valid before: May 27 00:00:00 2024 GMT
Not valid after: May 28 23:59:59 2025 GMT
(goshi@kali)-[~]
$
```

Nota. Elaboración propia

Sistema de Mesa de Partes Virtual - Municipalidad Provincial de Tacna

Dirección Web: sistram.munitacna.gob.pe/

Descripción: ejecutamos el comando **sudo ssldump sistram.munitacna.gob.pe** en la consola. Donde:

- ✓ **sudo** permite ejecutar comandos o programas con los permisos con los privilegios administrativos del usuario root.

- ✓ **ssllscan** analiza los servicios SSL/TLS para identificar vulnerabilidades de seguridad

Como se muestra en la imagen se tiene habilitado varios protocolos de SSL, así como los protocolos TLS se encuentran habilitados.

Figura 16

Ejecución del ssllscan a la Página Web Mesa de Partes Virtual – Municipalidad Provincial de Tacna

```
(goshi㉿kali)-[~]
$ sudo ssllscan sistram.munitacna.gob.pe
[sudo] contraseña para goshi:
Version: 2.1.5
OpenSSL 3.4.0 22 Oct 2024

Connected to 168.121.50.253

Testing SSL server sistram.munitacna.gob.pe on port 443 using SNI name sistram.munitacna.gob.pe

SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 disabled
TLSv1.1 disabled
TLSv1.2 enabled
TLSv1.3 enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):

Preferred TLSV1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
Accepted TLSV1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253
Accepted TLSV1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
Accepted TLSV1.3 128 bits TLS_AES_128_CCM_SHA256 Curve 25519 DHE 253
Preferred TLSV1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSV1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSV1.2 256 bits ECDHE-ARIA256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSV1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSV1.2 128 bits ECDHE-ARIA128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSV1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve 25519 DHE 253
Accepted TLSV1.2 256 bits ECDHE-RSA-CAMELLIA256-SHA384 Curve 25519 DHE 253
Accepted TLSV1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253
Accepted TLSV1.2 128 bits ECDHE-RSA-CAMELLIA128-SHA256 Curve 25519 DHE 253
Accepted TLSV1.2 256 bits ECDHE-RSA-AES256-SHA Curve 25519 DHE 253
Accepted TLSV1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSV1.2 256 bits AES256-GCM-SHA384
Accepted TLSV1.2 256 bits AES256-CCM
Accepted TLSV1.2 256 bits ARIA256-GCM-SHA384
Accepted TLSV1.2 128 bits AES128-GCM-SHA256
Accepted TLSV1.2 128 bits AES128-CCM
Accepted TLSV1.2 128 bits ARIA128-GCM-SHA256
Accepted TLSV1.2 64 bits AES256-CCM8
Accepted TLSV1.2 256 bits AES128-CCM8
Accepted TLSV1.2 256 bits AES256-SHA256
Accepted TLSV1.2 256 bits CAMELLIA256-SHA256
Accepted TLSV1.2 128 bits AES128-SHA256
Accepted TLSV1.2 128 bits CAMELLIA128-SHA256
Accepted TLSV1.2 256 bits AES256-SHA
Accepted TLSV1.2 256 bits CAMELLIA256-SHA
Accepted TLSV1.2 128 bits AES128-SHA
Accepted TLSV1.2 128 bits CAMELLIA128-SHA
```

```

goshi@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  128 bits  CAMELLIA128-SHA

Server Key Exchange Group(s):
TLSv1.3  128 bits  secp256r1 (NIST P-256)
TLSv1.3  192 bits  secp384r1 (NIST P-384)
TLSv1.3  256 bits  secp512r1 (NIST P-521)
TLSv1.3  128 bits  x25519
TLSv1.3  224 bits  x448
TLSv1.3  112 bits  fdhe2048
TLSv1.3  128 bits  fdhe3072
TLSv1.3  150 bits  fdhe4096
TLSv1.3  175 bits  fdhe6144
TLSv1.3  192 bits  fdhe8192
TLSv1.2  128 bits  secp256r1 (NIST P-256)
TLSv1.2  192 bits  secp384r1 (NIST P-384)
TLSv1.2  256 bits  secp512r1 (NIST P-521)
TLSv1.2  128 bits  x25519
TLSv1.2  224 bits  x448

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: *.munitacna.gob.pe
AltNames: DNS:*.munitacna.gob.pe, DNS:munitacna.gob.pe
Issuer: Sectigo RSA Domain Validation Secure Server CA

Not valid before: May 29 00:00:00 2025 GMT
Not valid after: Jun 29 23:59:59 2026 GMT
(goshi@kali)-[~]
$
```

Nota. Elaboración propia

Sistema de Sistema de Correo - Municipalidad Provincial de Tacna

Dirección Web: mail.munitacna.gob.pe

Descripción: ejecutamos el comando **sudo ssllscan mail.munitacna.gob.pe** en la consola. Donde:

- ✓ **sudo** permite ejecutar comandos o programas con los permisos con los privilegios administrativos del usuario root.
- ✓ **ssllscan** analiza los servicios SSL/TLS para identificar vulnerabilidades de seguridad

Como se muestra en la imagen se tiene habilitado varios protocolos de SSL, así como los protocolos TLSv1.3 se encuentra deshabilitado indicando una advertencia.

Figura 17

Ejecución del ssllsacn a la Página Web de Correo – Municipalidad Provincial de Tacna

```
(goshi㉿kali)-[~]
$ sudo ssllsacn mail.munitacna.gob.pe
Version: 2.1.5
OpenSSL 3.4.0 22 Oct 2024

Connected to 168.121.50.250

Testing SSL server mail.munitacna.gob.pe on port 443 using SNI name mail.munitacna.gob.pe

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    disabled
TLSv1.1    disabled
TLSv1.2    enabled
TLSv1.3    disabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256
Accepted   TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
```



```
(goshi㉿kali)-[~]
Archivo  Acciones  Editar  Vista  Ayuda
Accepted   TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
Accepted   TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
Accepted   TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
Accepted   TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
Accepted   TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted   TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted   TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted   TLSv1.2 128 bits DHE-RSA-AES128-SHA256 DHE 2048 bits
Accepted   TLSv1.2 128 bits DHE-RSA-AES128-SHA256 DHE 2048 bits
Accepted   TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 2048 bits
Accepted   TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 2048 bits
Accepted   TLSv1.2 128 bits AES128-GCM-SHA256 DHE 2048 bits
Accepted   TLSv1.2 256 bits AES256-GCM-SHA384 DHE 2048 bits
Accepted   TLSv1.2 64 bits DHE-RSA-AES128-CCM8 DHE 2048 bits
Accepted   TLSv1.2 128 bits DHE-RSA-AES128-CCM8 DHE 2048 bits
Accepted   TLSv1.2 64 bits AES128-CCM8
Accepted   TLSv1.2 128 bits AES128-CCM
Accepted   TLSv1.2 128 bits AES128-SHA256
Accepted   TLSv1.2 128 bits AES128-SHA
Accepted   TLSv1.2 64 bits DHE-RSA-AES256-CCM8 DHE 2048 bits
Accepted   TLSv1.2 256 bits DHE-RSA-AES256-CCM8 DHE 2048 bits
Accepted   TLSv1.2 64 bits AES256-CCM8
Accepted   TLSv1.2 256 bits AES256-CCM
Accepted   TLSv1.2 256 bits AES256-SHA256
Accepted   TLSv1.2 256 bits AES256-SHA
Accepted   TLSv1.2 128 bits secp256r1 (NIST P-256)

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: mail.munitacna.gob.pe
Altname: DNS:mail.munitacna.gob.pe, DNS:www.mail.munitacna.gob.pe
Issuer: Sectigo RSA Domain Validation Secure Server CA

Not valid before: Sep 30 00:00:00 2024 GMT
Not valid after: Oct 31 23:59:59 2025 GMT

(goshi㉿kali)-[~]
```

Nota. Elaboración propia

Sistema Sistema Intranet - Municipalidad Provincial de Tacna

Dirección Web: app.munitacna.gob.pe

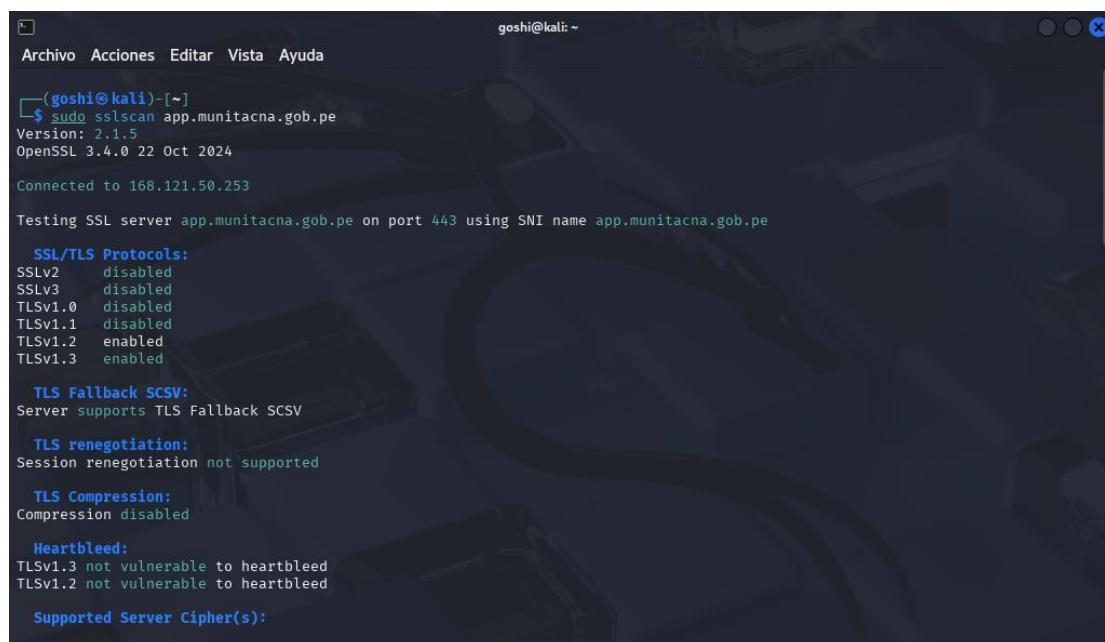
Descripción: ejecutamos el comando **sudo ssllscan app.munitacna.gob.pe** en la consola. Donde:

- ✓ **sudo** permite ejecutar comandos o programas con los permisos con los privilegios administrativos del usuario root.
- ✓ **ssllscan** analiza los servicios SSL/TLS para identificar vulnerabilidades de seguridad

Como se muestra en la imagen se tiene habilitado varios protocolos de SSL, así como los protocolos TLS se encuentran habilitados.

Figura 18

Ejecución del ssllscan a la Página Web de Intranet – Municipalidad Provincial de Tacna



```

goshi@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
(goshi@kali)-[~]
$ sudo ssllscan app.munitacna.gob.pe
Version: 2.1.5
OpenSSL 3.4.0 22 Oct 2024
Connected to 168.121.50.253

Testing SSL server app.munitacna.gob.pe on port 443 using SNI name app.munitacna.gob.pe

SSL/TLS Protocols:
SSLv2    disabled
SSLv3    disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):

```

```
goshi@kali: ~
Archivo Acciones Editar Vista Ayuda

Supported Server Cipher(s):
Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
Accepted TLSv1.3 128 bits TLS_AES_128_CCM_SHA256 Curve 25519 DHE 253
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-ARIA256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-ARIA128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-CAMELLIA256-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-CAMELLIA128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.2 256 bits AES256-GCM-SHA384
Accepted TLSv1.2 256 bits AES256-CCM
Accepted TLSv1.2 256 bits ARIA256-GCM-SHA384
Accepted TLSv1.2 128 bits AES128-GCM-SHA256
Accepted TLSv1.2 128 bits AES128-CCM
Accepted TLSv1.2 128 bits ARIA128-GCM-SHA256
Accepted TLSv1.2 64 bits AES256-CCM8
Accepted TLSv1.2 64 bits AES128-CCM8
Accepted TLSv1.2 256 bits AES256-SHA256
Accepted TLSv1.2 256 bits CAMELLIA256-SHA256
Accepted TLSv1.2 128 bits AES128-SHA256
Accepted TLSv1.2 128 bits CAMELLIA128-SHA256
Accepted TLSv1.2 256 bits AES256-SHA
Accepted TLSv1.2 256 bits CAMELLIA256-SHA
Accepted TLSv1.2 128 bits AES128-SHA
```

```
goshi@kali: ~
Archivo Acciones Editar Vista Ayuda

Accepted TLSv1.2 128 bits AES128-SHA
Accepted TLSv1.2 128 bits CAMELLIA128-SHA

Server Key Exchange Group(s):
TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 260 bits secp521r1 (NIST P-521)
TLSv1.3 128 bits x25519
TLSv1.3 224 bits x448
TLSv1.3 112 bits ff3dhe2048
TLSv1.3 128 bits ff3dhe3072
TLSv1.3 150 bits ff3dhe4096
TLSv1.3 175 bits ff3dhe6144
TLSv1.3 192 bits ff3dhe8192
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 260 bits secp521r1 (NIST P-521)
TLSv1.2 128 bits x25519
TLSv1.2 224 bits x448

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: *.munitacna.gob.pe
AltNames: DNS:*.munitacna.gob.pe, DNS:munitacna.gob.pe
Issuer: Sectigo RSA Domain Validation Secure Server CA

Not valid before: May 29 00:00:00 2025 GMT
Not valid after: Jun 29 23:59:59 2026 GMT
└─(goshi@kali)-[~]
```

Nota. Elaboración propia

g) SSL LABS

SSLabs es una herramienta sin fines comerciales que tiene por objeto facilitar informes sobre el estado de salud de los Certificados SSL.

Sistema Principal - Municipalidad Provincial de Tacna

Dirección Web: www.munitacna.gob.pe

Así mismo, ingresamos mediante el navegador a la página (<https://www.ssllabs.com>), y en **hostname** ingresamos el url de la página web de la Municipalidad Provincial de Tacna. (www.munitacna.gob.pe) y damos clic en la opción **submit**.

Figura 19

Sistema Web de SSL Labs

The screenshot shows the Qualys SSL Labs interface. At the top, there's a navigation bar with links for Home, Projects, Qualys Free Trial, and Contact. Below that, a breadcrumb trail indicates the user is at Home > Projects > SSL Server Test. The main title is "SSL Server Test". A note below it states: "This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will." A form field labeled "Hostname:" contains "www.munitacna.gob.pe", with a "Submit" button next to it. There's also a checkbox for "Do not show the results on the boards".

Recently Seen		Recent Best		Recent Worst	
partnerit.freshdesk.com	Err	staging.bellringersites.com	A+	www.adolek.com.tw	F
ual-crm.libertymutual.com.cn		sureviewtest.ipglobal.com	A	groomteamusa.com	T
washtechtga.com		umpquabank.creditlens.moody's...	A	nhuserapp.zxnyun.com	F
jatelindo.co.id		ilandsub.rakacha.info	A	alharamain.gov.sa	T
redmine.nac.jp		bptransrater.in	A	appokgo.com	T
cdoevents.jkapi.in		citrixdr.multiplan.com	A	papersiqn.com	T
globalsign.com		alainpicard.ca	B	jkg_mrkim.co.kr	T
sciencecouncil.noaa.gov		chatloop.io	B	polo.idemia.com	F
www.shop.myastro.online		titancraft.com	B	jltcuavpn.fmltcu.disa.mil	T
web.mercavalencia.com		jarvis-gylling-3.technetblog....	B	rsp.txcourts.gov	T

SSL Report v2.3.1

Copyright © 2009-2025 Qualys, Inc. All Rights Reserved. [Privacy Policy](#). [Terms and Conditions](#)

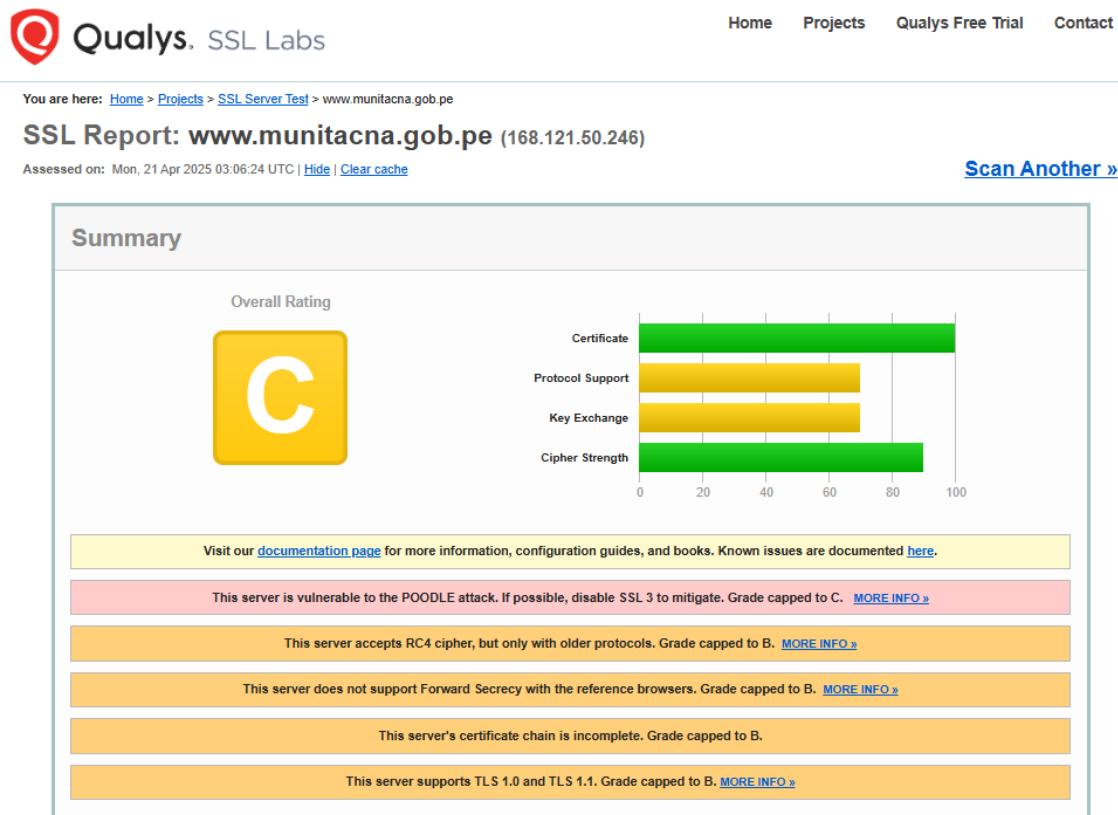
[Try Qualys for free!](#) Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including [certificate security](#) solutions.

Nota. Elaboración propia

Esperamos que la herramienta realice las pruebas de comprobacion de los certificados SSL, como se visualiza en la imagen el servidor de la Municipalidad Provincial de Tacna es vulnerable a **ATAQUES POODLE** (exploit cibernético grave de vulnerabilidad, que permite a un atacante descifrar datos en conexiones SSL), por lo que se recomienda desactivar el SSL3.

Figura 20

Resultados de la prueba de comprobación de seguridad SSL – Sistema Principal – Municipalidad Provincial de Tacna



Certificate #1: RSA 2048 bits (SHA256withRSA)

[Server Key and Certificate #1](#)

Subject	*.munitacna.gob.pe Fingerprint SHA256: 38ff0de78cc2573ae510b64157e08244e8d372dbedab72d90820c88eeaea1fc Pin SHA256: 6hIZpfS07Syt0dcL5FgagzCijvx0sZMTGBSqhYBZPM8=
Common names	*.munitacna.gob.pe
Alternative names	*.munitacna.gob.pe munitacna.gob.pe
Serial Number	740c6e304909c0e4b93bb3e10c2206d6
Valid from	Mon, 27 May 2024 00:00:00 UTC
Valid until	Wed, 28 May 2025 23:59:59 UTC (expires in 1 month and 8 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo RSA Domain Validation Secure Server CA AIA: http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP: http://ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

[Additional Certificates \(if supplied\)](#)

Certificates provided	1 (1602 bytes)
Chain issues	Incomplete

[Certification Paths](#) [+]

[Click here to expand](#)

Configuration

[Protocols](#)

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3 INSECURE	Yes
SSL 2	No

[Cipher Suites](#)

# TLS 1.2 (server has no preference)	[+]
# TLS 1.1 (server has no preference)	[+]
# TLS 1.0 (server has no preference)	[+]
# SSL 3 (server has no preference)	[+]

Protocol Details	
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0xa, TLS 1.0: 0xa
POODLE (SSLv3)	Vulnerable INSECURE (more info) SSL 3: 0xa
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0x000a
GOLDENDOODLE	No (more info) TLS 1.2 : 0x000a
OpenSSL 0-Length	No (more info) TLS 1.2 : 0x000a
Sleeping POODLE	No (more info) TLS 1.2 : 0x000a
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	Yes IN SECURE (more info)
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	With some browsers (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported Named Groups	secp256k1, secp256r1, secp384r1, secp521r1 (Server has no preference)
SSL 2 handshake compatibility	Yes

Nota. Elaboración propia

Sistema de Mesa de Partes Virtual - Municipalidad Provincial de Tacna

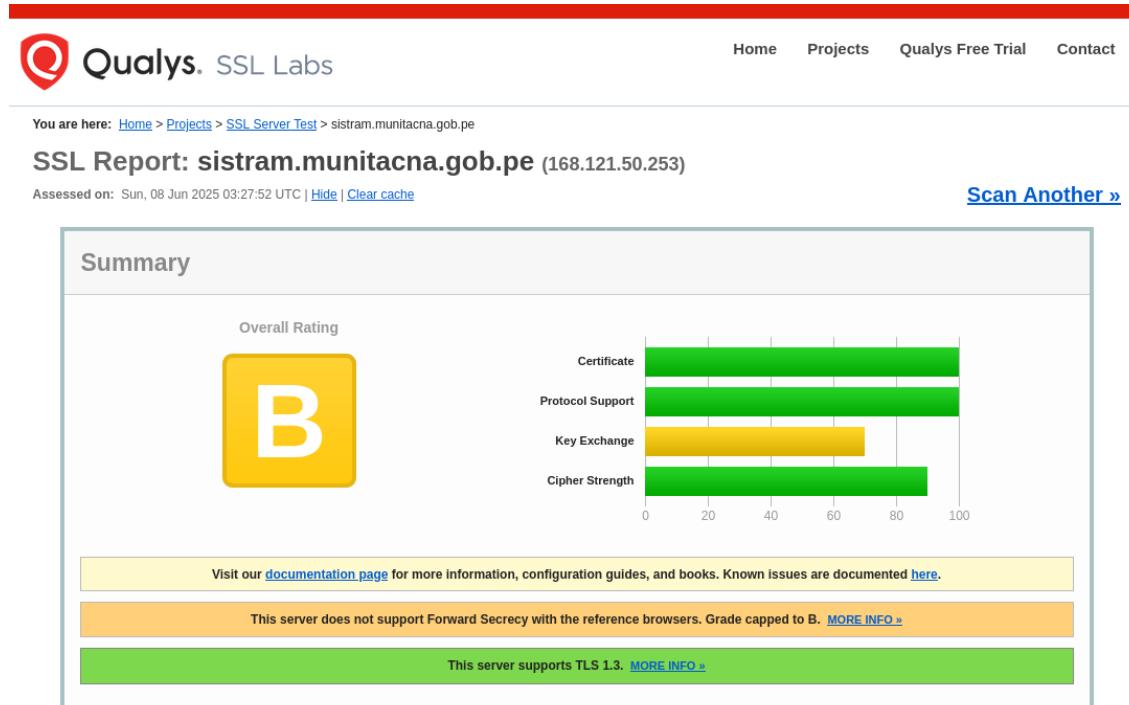
Dirección Web: sistram.munitacna.gob.pe

Así mismo, ingresamos mediante el navegador a la página (<https://www.ssllabs.com>), y en **hostname** ingresamos el url de la página web de la Municipalidad Provincial de Tacna. (sistram.munitacna.gob.pe) y damos clic en la opción **submit**.

Esperamos que la herramienta realice las pruebas de comprobacion de los certificados SSL, como se visualiza en la imagen el sistema de Mesa de Partes de la Municipalidad Provincial de Tacna no soporta Forward Secrecy.

Figura 21

Resultados de la prueba de comprobación de seguridad SSL de la Pagina Web de Mesa de Partes – Municipalidad Provincial de Tacna



Nota. Elaboración propia

Sistema de Correo - Municipalidad Provincial de Tacna

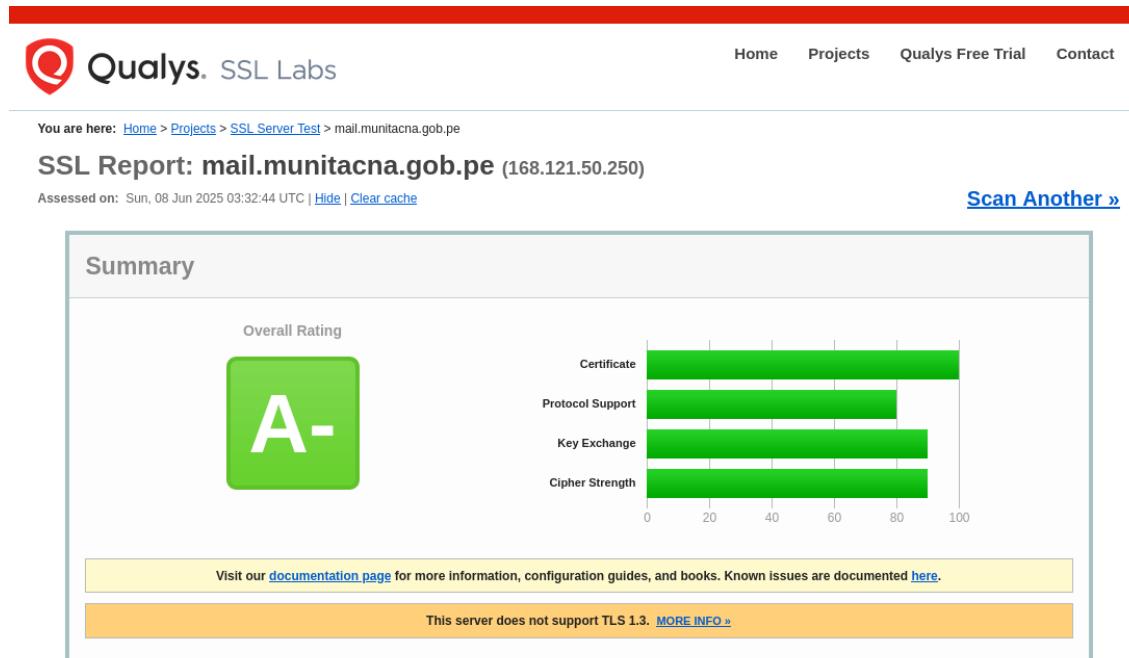
Dirección Web: mail.munitacna.gob.pe

Así mismo, ingresamos mediante el navegador a la página (<https://www.ssllabs.com>), y en **hostname** ingresamos el url de la página web de la Municipalidad Provincial de Tacna. (mail.munitacna.gob.pe) y damos clic en la opción **submit**.

Esperamos que la herramienta realice las pruebas de comprobacion de los certificados SSL, como se visualiza en la imagen el sistema de Correo de la Municipalidad Provincial de Tacna no soporta TLS 1.3 esto indica una vulnerabilidad importante dado que este protocolo actual mas seguro.

Figura 22

Resultados de la prueba de comprobación de seguridad SSL de la Página Web del Sistema de Correo – Municipalidad Provincial de Tacna



Nota. Elaboración propia

Sistema Intranet - Municipalidad Provincial de Tacna

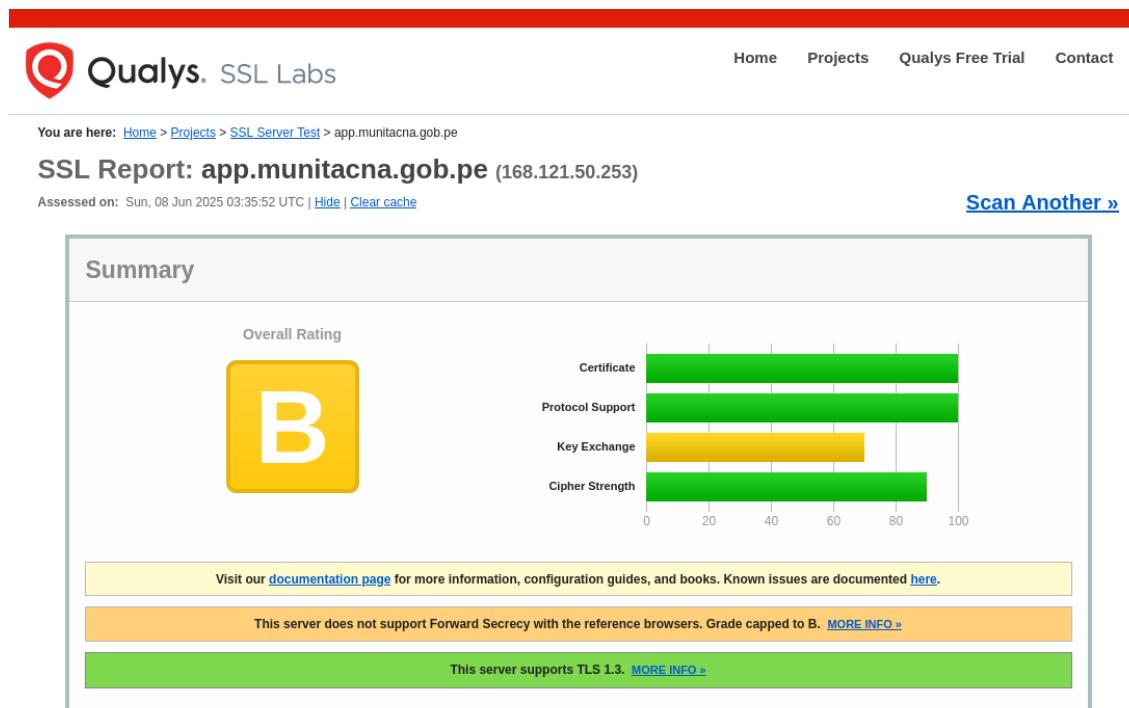
Dirección Web: app.munitacna.gob.pe

Así mismo, ingresamos mediante el navegador a la página (<https://www.ssllabs.com>), y en **hostname** ingresamos el url de la página web de la Municipalidad Provincial de Tacna. (app.munitacna.gob.pe) y damos clic en la opción **submit**.

Esperamos que la herramienta realice las pruebas de comprobacion de los certificados SSL, como se visualiza en la imagen el sistema de Intranet de la Municipalidad Provincial de Tacna no soporta Forward Secrecy.

Figura 23

Resultados de la prueba de comprobación de seguridad SSL de la Página Web del Sistema de Intranet – Municipalidad Provincial de Tacna



Nota. Elaboración propia

h) VULNERABILIDAD WEB CON OWASP ZAP

ZAP

Zed Attack Proxy (ZAP) es una herramienta gratuita y de código abierto para realizar pruebas de penetración, desarrollada y respaldada por el proyecto OWASP (Open Web Application Security Project). Su propósito principal es evaluar la seguridad de aplicaciones web.

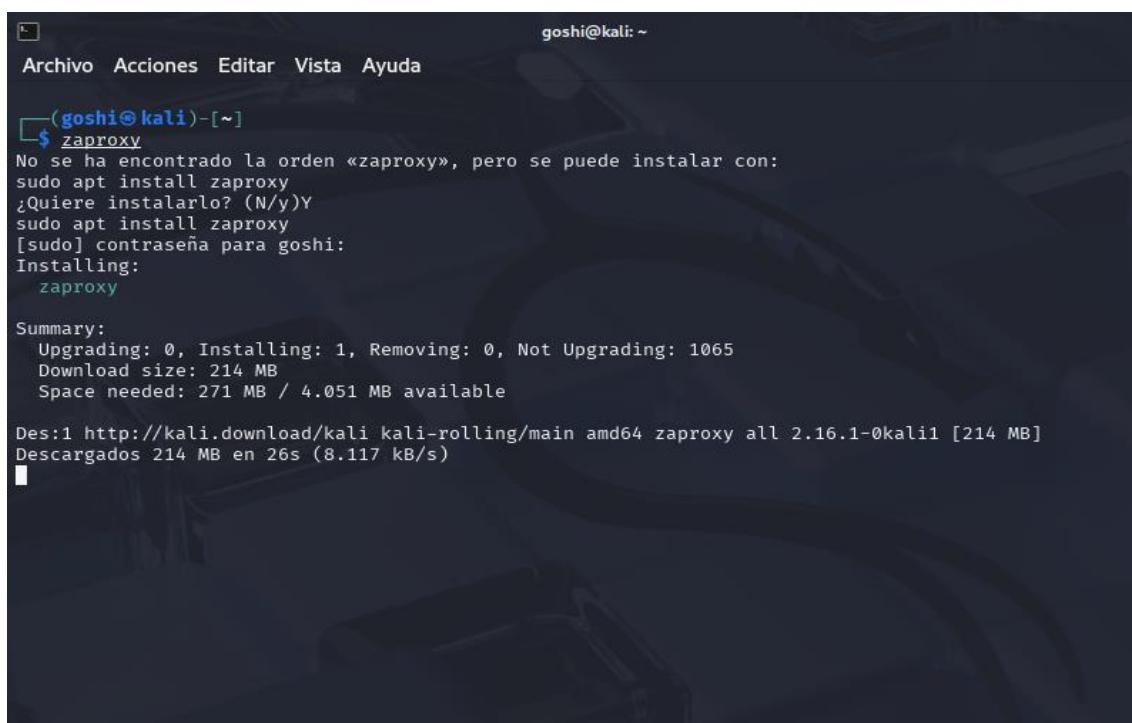
OWASP ZAP

OWASP ZAP (Zed Attack Proxy) es una herramienta open source enfocada en la seguridad de aplicaciones web. Creada por la comunidad del Open Web Application Security Project (OWASP), ofrece a desarrolladores y expertos en seguridad una solución eficaz para identificar y corregir vulnerabilidades en sus aplicaciones web.

Instalamos el zaproxy, para ello en la consola ingresamos el siguiente comando **zaproxy**

Figura 24

Herramienta zaproxy



```

goshi@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda

(goshi@kali)-[~]
$ zaproxy
No se ha encontrado la orden «zaproxy», pero se puede instalar con:
sudo apt install zaproxy
¿Quiere instalarlo? (N/y)Y
sudo apt install zaproxy
[sudo] contraseña para goshi:
Installing:
    zaproxy

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1065
  Download size: 214 MB
  Space needed: 271 MB / 4.051 MB available

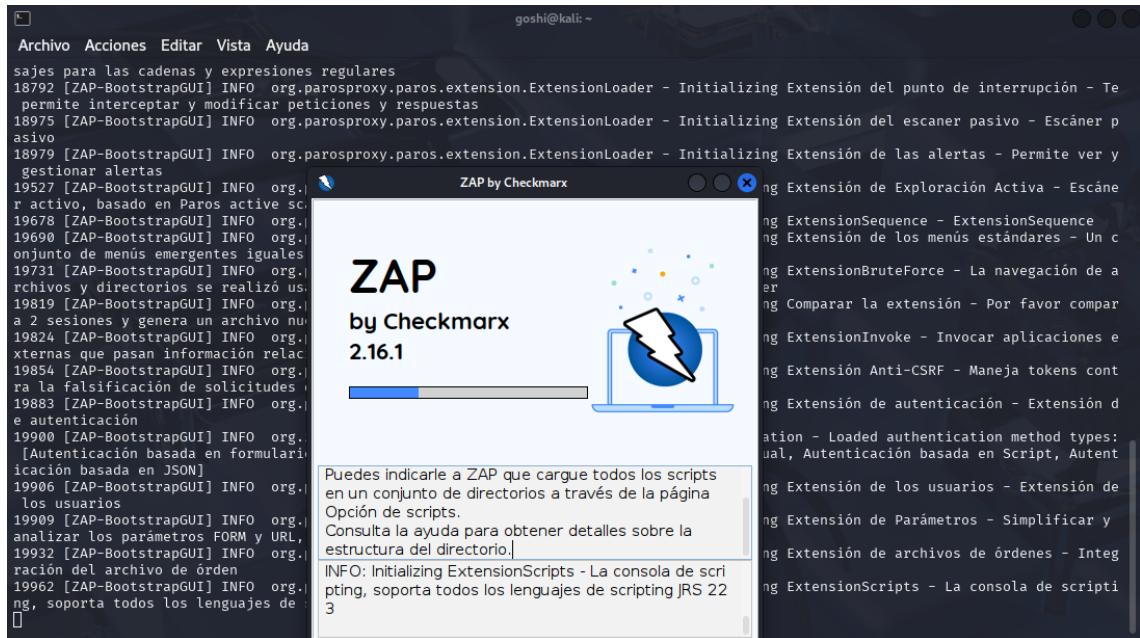
Des:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.16.1-0kali1 [214 MB]
Descargados 214 MB en 26s (8.117 kB/s)
  
```

Nota. Elaboración propia

Una vez instalado ingresamos en la consola el comando **zaproxy**, y esperamos que inicie la herramienta

Figura 25

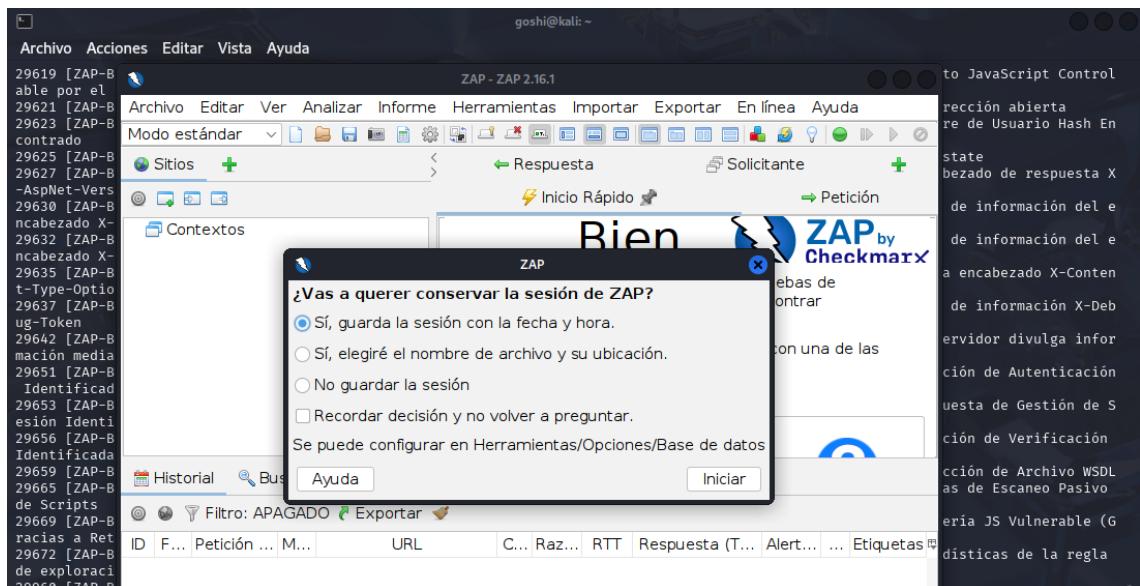
Cargado el entorno grafico de ZAP



Nota. Elaboración propia

Figura 26

Herramienta ZAP

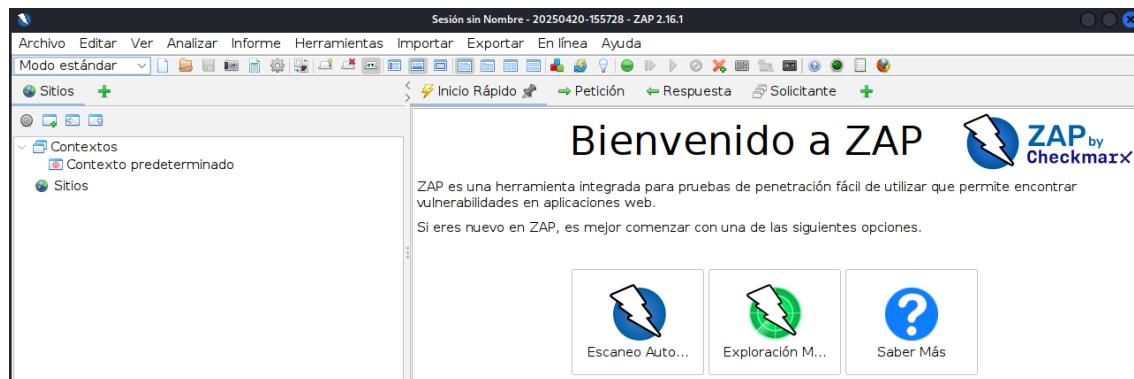


Nota. Elaboración propia

Seleccionamos la opción de **Escaneo Automatizado**.

Figura 27

Herramienta ZAP



Nota. Elaboración propia

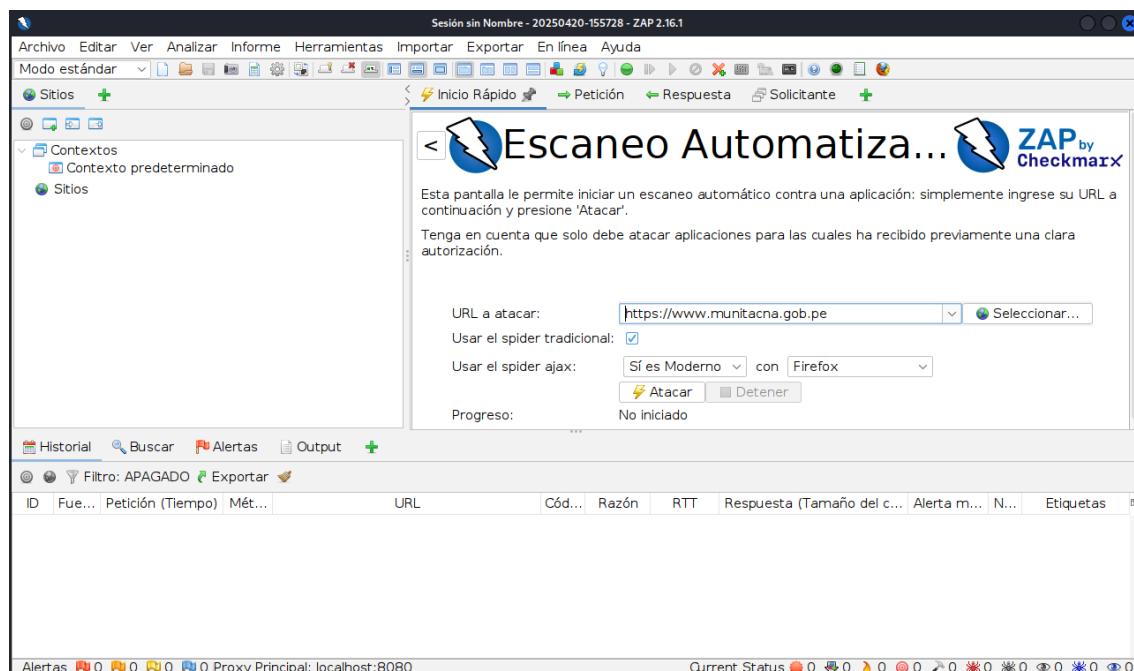
Sistema Principal - Municipalidad Provincial de Tacna

Dirección Web: www.munitacna.gob.pe

Para realizar la prueba de vulnerabilidad, en la opción de URL a atacar, ingresamos la url de la Municipalidad Provincial de Tacna (<https://www.munitacna.gob.pe>). Como se muestra en la imagen. Y damos clic en la opción **atacar**.

Figura 28

Prueba de escaneo automatizado

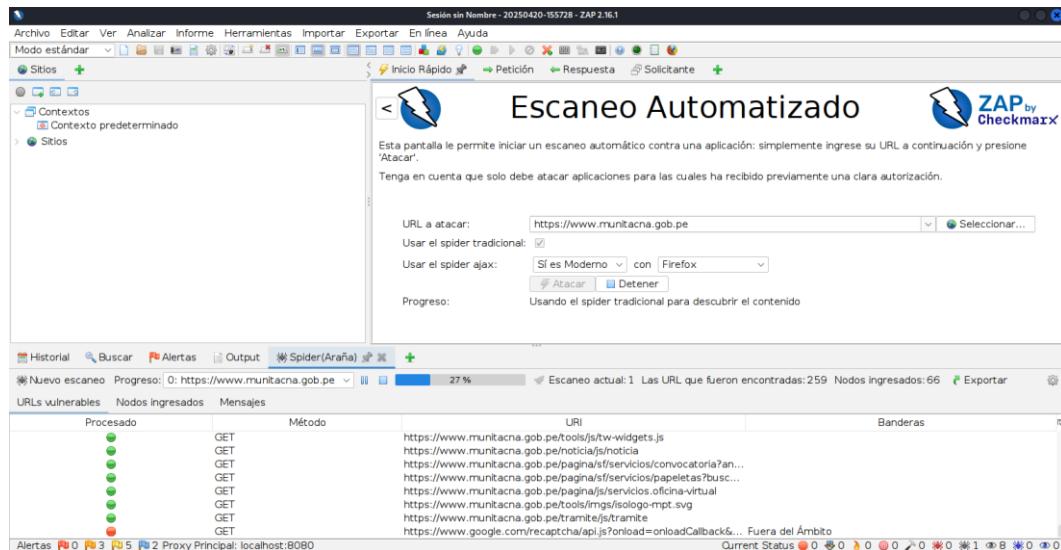


Nota. Elaboración propia

La herramienta ZAP iniciará el rastreo de la aplicación web utilizando su herramienta de spider (araña) y realizará un análisis pasivo de cada página detectada. Posteriormente, empleará su escáner activo para lanzar ataques sobre todas las páginas, funciones y parámetros identificados.

Figura 29

Ejecución del escaneo automatizado con ZAP

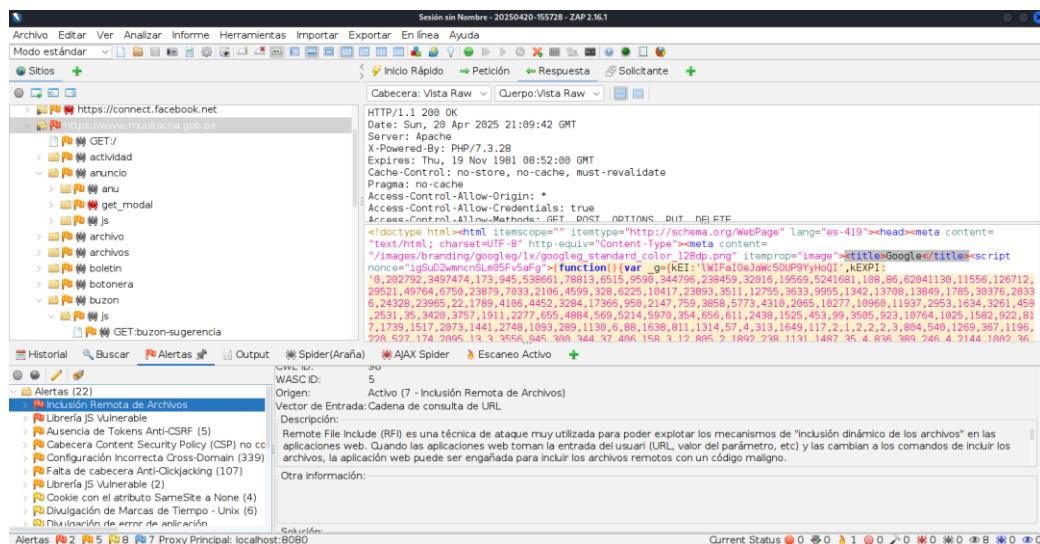


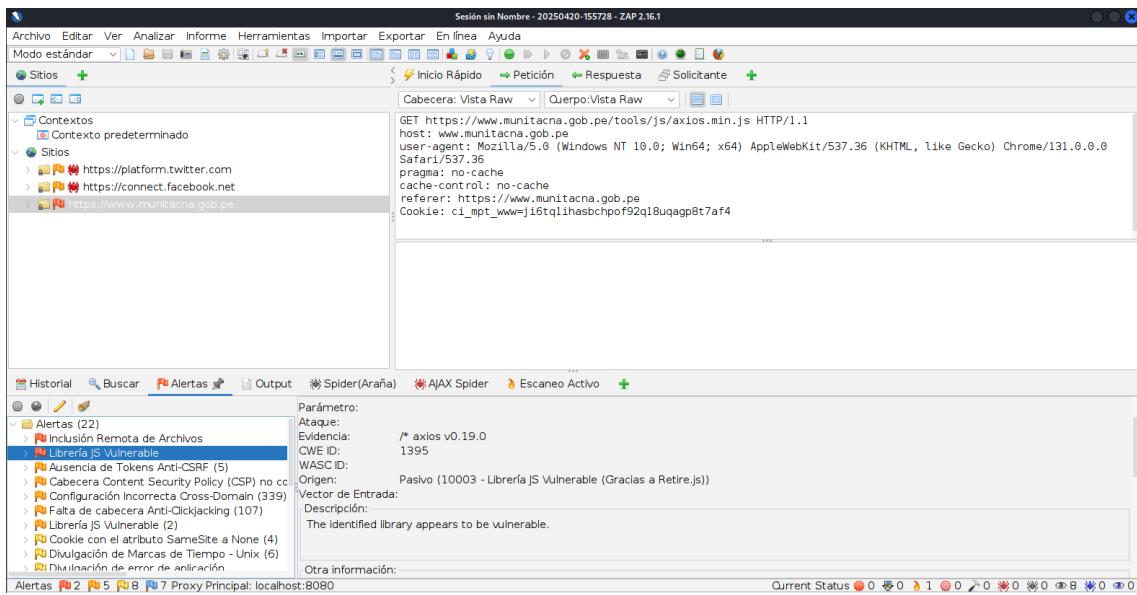
Nota. Elaboración propia

En la pestaña **Alertas**, nos muestra 2 alertas de vulnerabilidad (Alta) que son **Inclusión Remota de Archivos y Librería JS Vulnerable**.

Figura 30

Resultado de pruebas, alerta de vulnerabilidad de Pagina Web – Municipalidad Provincial de Tacna.



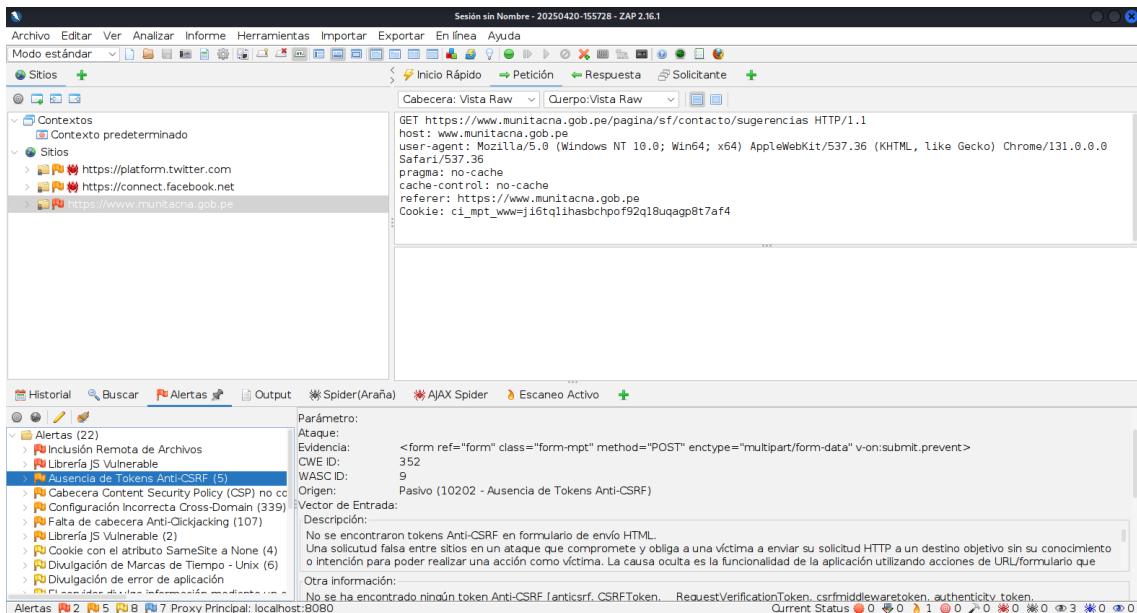


Nota. Elaboración propia

Así como alertas de vulnerabilidad (Medio).

Figura 31

Resultado de prueba, alertas de vulnerabilidad nivel medio



Nota. Elaboración propia

Sistema de Mesa de Partes Virtual - Municipalidad Provincial de Tacna

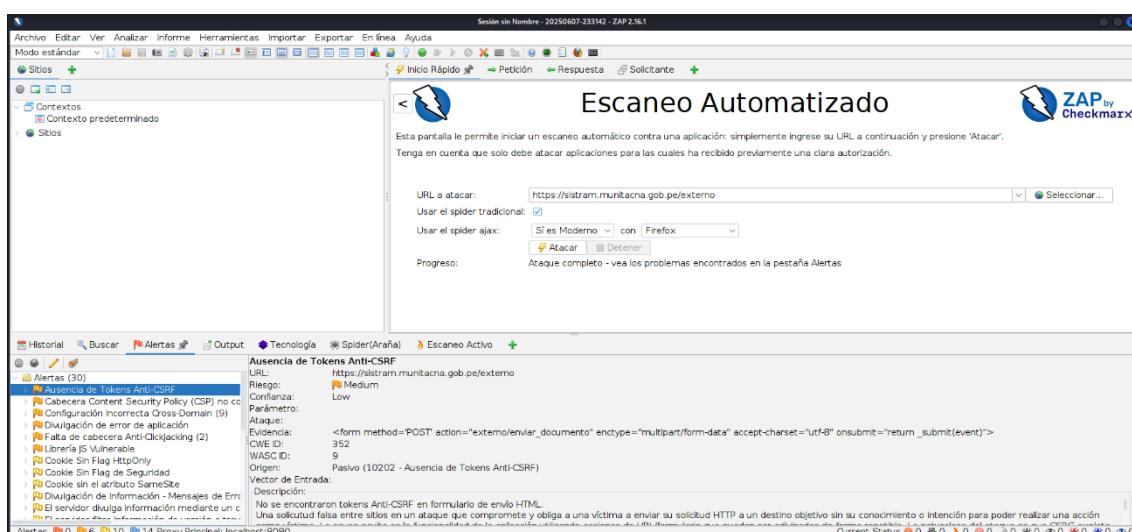
Dirección Web: sistram.munitacna.gob.pe

Iniciamos la herramienta zaproxy, para ello en la consola ingresamos el siguiente comando **zaproxy**

Para realizar la prueba de vulnerabilidad, en la opción de URL a atacar, ingresamos la url del Sistema de Mesa de Partes Virtual de la Municipalidad Provincial de Tacna (sistram.munitacna.gob.pe). Como se muestra en la imagen. Y damos clic en la opción **atacar**.

Figura 32

Resultado de prueba, alertas de vulnerabilidad nivel medio



Nota. Elaboración propia

En la pestaña Alertas, nos muestra alertas de vulnerabilidad (Media) que son como, por ejemplo:

- ✓ Ausencia de Token's Anti-CSRF.
- ✓ Cabecera Content Secutry Police (CSP).
- ✓ Configuración Incorrecta de CrossDomain
- ✓ Divulgación de Error de Aplicación.
- ✓ Falta de Cabecera Anti-Clickjacking.
- ✓ Librería Js Vulnerable.

Sistema de Correo - Municipalidad Provincial de Tacna

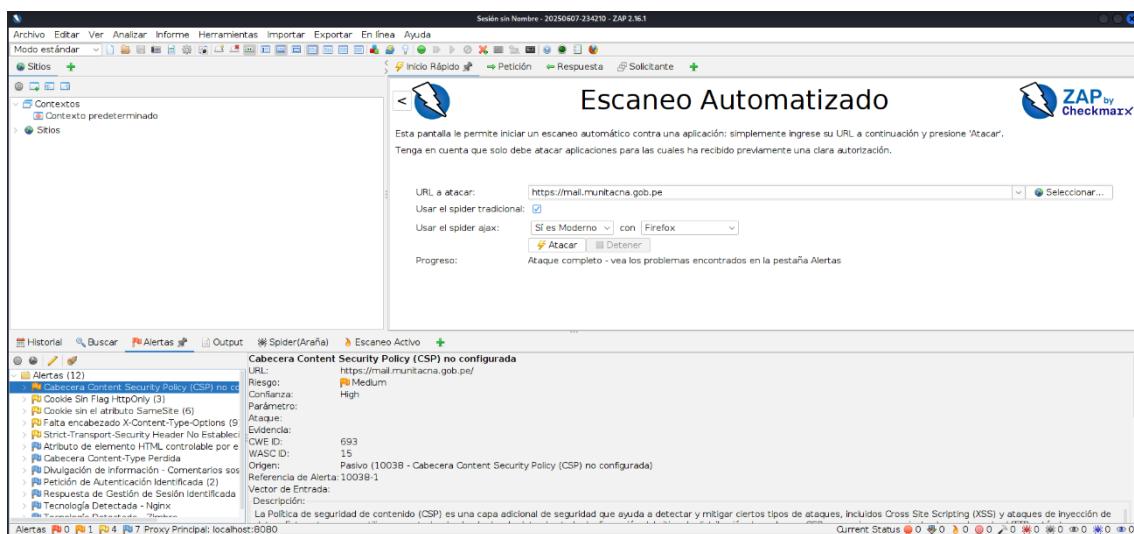
Dirección Web: mail.munitacna.gob.pe

Iniciamos la herramienta zaproxy, para ello en la consola ingresamos el siguiente comando **zaproxy**

Para realizar la prueba de vulnerabilidad, en la opción de URL a atacar, ingresamos la url del Sistema de Correo - Municipalidad Provincial de Tacna (mail.munitacna.gob.pe). Como se muestra en la imagen. Y damos clic en la opción **atacar**.

Figura 33

Resultado de prueba, alertas de vulnerabilidad nivel medio



Nota. Elaboración propia

En la pestaña Alertas, nos muestra alertas de vulnerabilidad (Media) que son como, por ejemplo:

- ✓ Cabecera Content Secutly Police (CSP).
- ✓ Cookie Sin Flag HttpOnly.
- ✓ Cookie sin el Articulo SameSite.
- ✓ Falta encabezado X-Content-Type-Options.
- ✓ Strict-Transport-Security Header No Establecido.

Sistema de Intranet - Municipalidad Provincial de Tacna

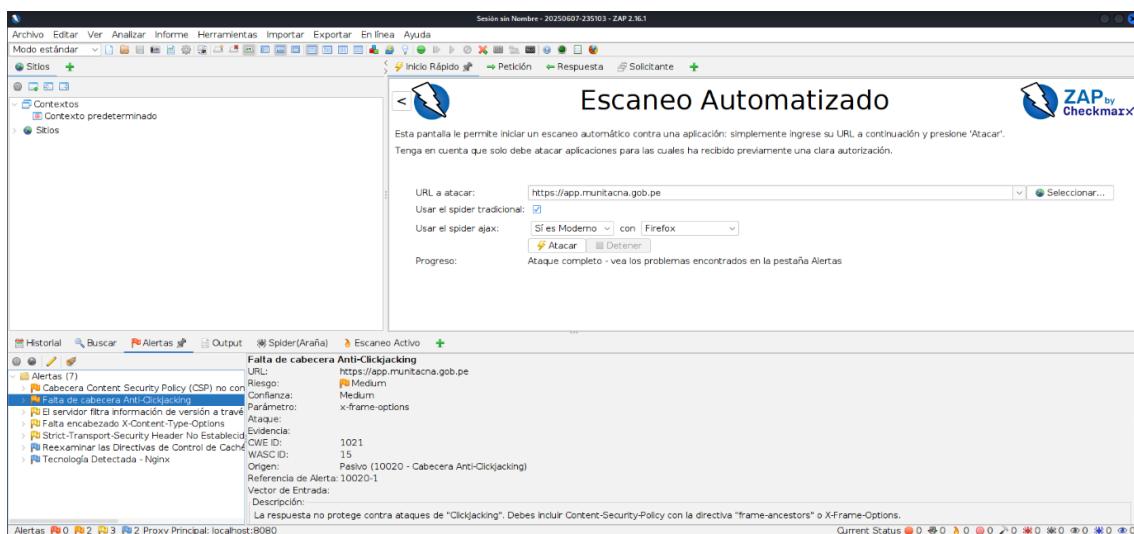
Dirección Web: app.munitacna.gob.pe

Iniciamos la herramienta zaproxy, para ello en la consola ingresamos el siguiente comando **zaproxy**

Para realizar la prueba de vulnerabilidad, en la opción de URL a atacar, ingresamos la url del Sistema de Intranet - Municipalidad Provincial de Tacna (app.munitacna.gob.pe). Como se muestra en la imagen. Y damos clic en la opción **atacar**.

Figura 34

Resultado de prueba, alertas de vulnerabilidad nivel medio



Nota. Elaboración propia

En la pestaña Alertas, nos muestra alertas de vulnerabilidad (Media) que son como, por ejemplo:

- ✓ Cabecera Content Security Policy (CSP).
- ✓ Falta de Cabecera Anti-Clickjacking.
- ✓ El Servidor Filtra Información de Version.
- ✓ Falta encabezado X-Content-Type-Options.
- ✓ Strict-Transport-Security Header No Establecido.

Resultado de Pruebas de Hacking Ético:

Las pruebas de hacking ético realizadas a los sistemas de información de la Municipalidad Provincial de Tacna permitieron identificar diversas vulnerabilidades que podrían comprometer la seguridad e integridad de la información gestionada por la entidad. Estos hallazgos evidencian la necesidad de implementar medidas correctivas y reforzar los mecanismos de protección para garantizar la confidencialidad, disponibilidad y autenticidad de los datos, así como prevenir posibles accesos no autorizados.

Anexo 2. Informe de Hacking Ético Realizado a Los Sistemas de Información de La Municipalidad Provincial De Tacna

Entidad: Municipalidad Provincial de Tacna
Fecha del Informe: Junio de 2025
Realizado por: Bach. Ivonne Soledad González Nina
Bach. Giordy Alex Mamani Aguilar
Período de pruebas: Mayo a Junio de 2025

1. Resumen Ejecutivo

Se realizó las pruebas de hacking ético con la finalidad de realizar un análisis de vulnerabilidades de los sistemas de los Sistemas de Información de la Municipalidad de Tacna, con el propósito de evaluar su nivel de exposición frente a potenciales ataques que pudieran comprometer la disponibilidad, integridad y confidencialidad de la información corporativa. Todas las acciones realizadas durante la verificación de vulnerabilidades se desarrollaron de manera controlada, empleando herramientas confiables y especializadas para este tipo de pruebas.

2. Objetivo

Esta evaluación de Hacking Ético tuvo como objetivo detectar vulnerabilidades críticas en los sistemas de información de la Municipalidad Provincial de Tacna, mediante la realización de simulaciones de ataques reales que permitieran analizar la seguridad de sus activos tecnológicos, sin comprometer la integridad de los sistemas ni la información.

3. Alcance

3.1. Aplicaciones web:

Dominio Principal

- Municipalidad Provincial de Tacna
Dirección Web (<https://www.munitacna.gob.pe>)

Sub Dominios

- Mesa de Partes Virtual - Municipalidad Provincial de Tacna
Dirección Web (<https://sistram.munitacna.gob.pe>)
- Sistema de Correo - Municipalidad Provincial de Tacna
Dirección Web (<https://mail.munitacna.gob.pe>)
- Intranet - Municipalidad Provincial de Tacna
Dirección Web (<https://app.munitacna.gob.pe>)

4. Cronograma de Actividades

Durante los meses de mayo y junio de 2025, se llevó a cabo un proceso de evaluación de seguridad mediante pruebas de hacking ético en los sistemas de información de la Municipalidad Provincial de Tacna. Las actividades se iniciaron los primeros días de mayo.

Posteriormente, se procedió con el análisis de vulnerabilidades y el mapeo de servicios, utilizando herramientas automatizadas y revisión manual. así también se ejecutó pruebas de penetración externas, dirigidas a los servicios accesibles desde internet, incluyendo aplicaciones web y puertos abiertos.

Destacando los hallazgos, las vulnerabilidades detectadas y las recomendaciones para mitigarlas. Finalmente, en junio, La elaboración del informe técnico, marcando la conclusión de las actividades planificadas.

5. Metodología

- **Reconocimiento:** Identificación de sistemas de información.
- **Análisis de vulnerabilidades:** Uso de herramientas automáticas y revisión manual.
- **Explotación controlada:** Pruebas prácticas para validar vulnerabilidades.
- **Post-explotación:** Análisis del impacto y persistencia.
- **Reporte:** Documentación de hallazgos y recomendaciones.

6. Resumen de Vulnerabilidades

DOMINIO PRINCIPAL – PAGINA WEB MUNICIPALIDAD PROVINCIAL DE TACNA			
Dirección Web (https://www.munitacna.gob.pe)			
RIESGO	DESCRIPCIÓN	IMPACTO	PRIORIDAD
Recolección de Información	Protocolo Whois - Información vulnerable debido a la publicación de información pública que puede ser utilizada con fines maliciosos. puede ser utilizada para phishing, spam o para fines de espionaje	Medio	Media
Escaneo de Puertos	Herramienta Nmap - Se identificó puertos abiertos (80 y 443), como posibles vulnerabilidades en los sistemas analizados.	Alta	Alta
Escaneo de Vulnerabilidades	Herramienta DNSenum – Se muestra información de datos del servidor DNS de un dominio, como los registros NS, MX y las transferencias de zona, que son posibles vulnerabilidades. Por ejemplo, si las transferencias de zona no están debidamente protegidas, un atacante podría acceder a información sensible del sistema.	Medio	Media
Falta de Certificados SSL/TLS	Herramienta SSLScan – el sitio web presenta protocolos de conexión con una configuración no segura (SSLv3 y utiliza cifrados DES y RC4). Ya que se expone la información a riesgos de seguridad, como ataques de MITM (Man-in-the-Middle), intercepción de datos y falta de confianza de los usuarios	Alta	Alta
Falta de Certificados SSL/TLS	Herramienta SSL Labs – como se muestra en el reporte de información, el sistema web es altamente vulnerable a ataques POODLE. Por lo que se	Alta	Alta

	recomienda desactivar el protocolo de conexión SSL3.		
Pruebas de Penetración	Herramienta OWASP ZAP – el escaneo automatizado del sistema web indica que, se tiene varias alertas de vulnerabilidad (Alta), como: - Inclusión Remota de Archivos: Remote File Include (RFI). - Librería jS Vulnerable	Alta	Alta

SUB DOMINIO – MESA DE PARTES VIRTUAL – MUNICIPALIDAD PROVINCIAL DE TACNA			
Dirección Web (https://sistram.munitacna.gob.pe)			
RIESGO	DESCRIPCIÓN	IMPACTO	PRIORIDAD
Escaneo de Puertos	Herramienta Nmap - Se identificó puertos abiertos (80, 443), como posibles vulnerabilidades en los sistemas analizados y el puerto cerrado (113)	Alta	Alta
Falta de Certificados SSL/TLS	Herramienta SSLScan – el sitio web presenta protocolos de conexión: SSLv2 y SSLv3, así como TLSv1.0, TLSv1.1, TLSv1.2 y TLSv1.3, los cuales no son presentan vulnerabilidad.	Baja	Baja
Falta de Certificados SSL/TLS	Herramienta SSL Labs – como se muestra en el reporte de información, el sistema web no cuenta con (Forward Secrecy), es una característica de seguridad criptográfica que garantiza que el compromiso de una clave de cifrado a largo plazo no compromete la seguridad de las sesiones anteriores.	Alta	Alta
Pruebas de Penetración	Herramienta OWASP ZAP – el escaneo automatizado del sistema web indica que, se tiene varias alertas de vulnerabilidad (Media), como:	Medio	Media

	<ul style="list-style-type: none"> - Ausencia de Token's Anti-CSRF. - Cabecera Content Secuty Police (CSP). - Configuración Incorrecta de CrossDomain - Divulgación de Error de Aplicación. - Falta de Cabecera Anti-Clickjacking. - Librería Js Vulnerable. 		
--	--	--	--

SUB DOMINIO – SISTEMA DE CORREO – MUNICIPALIDAD PROVINCIAL DE TACNA			
Dirección Web (https://mail.munitacna.gob.pe)			
RIESGO	DESCRIPCIÓN	IMPACTO	PRIORIDAD
Escaneo de Puertos	Herramienta Nmap - Se identificó puertos abiertos (25, 80, 443, 465 y 993), como posibles vulnerabilidades en los sistemas analizados y el puerto cerrado (113).	Alta	Alta
Falta de Certificados SSL/TLS	Herramienta SSLScan – el sitio web presenta protocolos de conexión: SSLv2 y SSLv3, así como TLSv1.0, TLSv1.1, TLSv1.2 los cuales no son presentan vulnerabilidad. el protocolo TLSv1.3 se encuentra deshabilitado y que es vulnerable siendo este el protocolo actual más seguro, y representando una vulnerabilidad para el sistema	Baja	Baja
Falta de Certificados SSL/TLS	Herramienta SSL Labs – como se muestra en el reporte de información, el sistema web no soporta el protocolo TLS v1.3 mismo que utiliza cifrado más robusto, eliminando algoritmos con vulnerabilidades conocidas. Representando así una vulnerabilidad importante.	Alta	Alta

Pruebas de Penetración	Herramienta OWASP ZAP – el escaneo automatizado del sistema web indica que, se tiene varias alertas de vulnerabilidad (Media), como: - Cabecera Content Security Policy (CSP). - Cookie Sin Flag HttpOnly. - Cookie sin el Artículo SameSite. - Falta encabezado X-Content-Type-Options. - Strict-Transport-Security Header No Establecido.	Medio	Media
------------------------	--	-------	-------

SUB DOMINIO – INTRANET – MUNICIPALIDAD PROVINCIAL DE TACNA			
Dirección Web (https://sistram.munitacna.gob.pe)			
RIESGO	DESCRIPCIÓN	IMPACTO	PRIORIDAD
Escaneo de Puertos	Herramienta Nmap - Se identificó puertos abiertos (80 y 443), como posibles vulnerabilidades en los sistemas analizados y el puerto cerrado (113).	Alta	Alta
Falta de Certificados SSL/TLS	Herramienta SSLScan – el sitio web presenta protocolos de conexión: SSLv2 y SSLv3, así como TLSv1.0, TLSv1.1, TLSv1.2 y TLSv1.3, los cuales no presentan vulnerabilidad.	Baja	Baja
Falta de Certificados SSL/TLS	Herramienta SSL Labs – como se muestra en el informe de información, el sistema web no cuenta con (Forward Secrecy), es una característica de seguridad criptográfica que garantiza que el compromiso de una clave de cifrado a largo plazo no compromete la seguridad de las sesiones anteriores.	Alta	Alta
Pruebas de Penetración	Herramienta OWASP ZAP – el escaneo automatizado del sistema web indica	Medio	Media

	<p>que, se tiene varias alertas de vulnerabilidad (Media), como:</p> <ul style="list-style-type: none"> - Cabecera Content Security Policy (CSP). - Falta de Cabecera Anti-Clickjacking. - El Servidor Filtra Información de Version. - Falta encabezado X-Content-Type-Options. - Strict-Transport-Security Header No Establecido. 		
--	--	--	--

7. Vulnerabilidades Críticas Importantes

7.1. Vulnerabilidad de Índice de Exposición: Se detectó que los Sistemas de Información Web (Dominio y Sub Dominios) de la Municipalidad Provincial de Tacna, presentan puertos abiertos, lo que significan una brecha de vulnerabilidad importante ya que el sistema está expuesto a explotaciones y ataques como:

- Una **conexión RDP** sin protección puede ser aprovechada por atacantes para robar credenciales y obtener acceso no autorizado a un servidor, o bien para desplegar software malicioso como ransomware.
- Un **ataque de denegación de servicio (DoS)** consiste en saturar un servicio específico mediante múltiples solicitudes desde distintas máquinas. Por ejemplo, se pueden sobrecargar los puertos de un servidor web, consumiendo su ancho de banda y recursos, lo que impide el acceso de usuarios legítimos.
- Los puertos utilizados por servicios web suelen ser objetivos comunes para ataques como la **inyección SQL** o la **falsificación de solicitudes entre sitios (CSRF)**, los cuales buscan explotar debilidades dentro de las aplicaciones web.
- En los **ataques de intermediario (Man-in-the-middle)**, los atacantes pueden interceptar datos transmitidos a través de puertos no cifrados

para obtener información sensible. Un caso común es el desvío del tráfico de correo electrónico con el fin de espiar su contenido.

7.2. Vulnerabilidad en la Falta de Certificados SSL/TLS: Se detectó los Sistemas de Información Web (Dominio y Sub Dominios) de la Municipalidad Provincial de Tacna, el sistema web principal es vulnerable al ataque POODLE (Padding Oracle On Downgraded Legacy Encryption) es una falla de seguridad que aprovecha una debilidad en el protocolo SSL 3.0, permitiendo a los atacantes acceder a datos cifrados. Esta vulnerabilidad puede ser utilizada para descifrar y obtener información sensible de comunicaciones en línea.

Así como, el sistema de Mesa de Partes Virtual y el sistema de Intranet, **no cuenta con (Forward Secrecy)**, es una característica de seguridad criptográfica que garantiza que el compromiso de una clave de cifrado a largo plazo no compromete la seguridad de las sesiones anteriores.

El sistema de Correo, **no soporta el protocolo TLS v1.3** mismo que utiliza cifrado más robusto, eliminando algoritmos con vulnerabilidades conocidas. Representando así una vulnerabilidad importante.

8. Recomendaciones

8.1. Cifrado y comunicaciones seguras

- Uso de HTTPS utilizando certificados TLS actualizados.
- Deshabilita protocolos inseguros como SSL 3.0 y TLS 1.0 (por ejemplo, para mitigar ataques como POODLE).
- Asegura el almacenamiento y transmisión segura de datos sensibles (contraseñas, tokens).

8.2. Control de acceso robusto

- Uso de autenticación fuerte (preferiblemente con MFA - autenticación multifactor).
- Aplicar principios de mínimos privilegios para usuarios y servicios.
- Gestionar sesiones de manera segura (con expiración, tokens únicos, etc.).

8.3. Realizar pruebas de penetración (pentesting)

- Contratar o realizar auditorías regulares de seguridad ética para identificar vulnerabilidades.
- Incluir pruebas de inyección SQL, XSS, CSRF, RCE, etc.
- Corregir las vulnerabilidades identificadas antes de que sean explotadas.

8.4. Uso de herramientas de análisis y monitoreo

- Implementar sistemas de detección de intrusos (IDS) y análisis de logs.
- Usa herramientas como OWASP ZAP, para análisis proactivo.
- Supervisa el tráfico inusual o comportamientos anómalos.

8.5. Capacitación y concienciación

- Capacitar a desarrolladores y administradores en buenas prácticas de seguridad.
- Fomentar una cultura de seguridad dentro del equipo técnico y administrativo.
- Simula ataques controlados para medir la respuesta ante incidentes.

9. Conclusiones

La evaluación de seguridad ha revelado vulnerabilidades significativas en los sistemas de información que, de no ser corregidas, podrían ser explotadas por actores maliciosos con distintos niveles de capacidad técnica. Estas debilidades comprometen la confidencialidad, integridad y disponibilidad de los sistemas de información de la Municipalidad Provincial de Tacna.

Se recomienda atender de forma prioritaria las vulnerabilidades críticas y de alto riesgo, así como establecer mecanismos de control y monitoreo continuo que garanticen una defensa efectiva frente a amenazas actuales y emergentes.

Para asegurar la eficacia de las remediaciones implementadas y medir el avance en la mejora de la postura de seguridad, se sugiere realizar una nueva auditoría técnica dentro de un periodo de 6 a 12 meses.