Formato de Auditoría OSINT: Reconocimiento Pasivo de Dominio

Introducción

Objetivo: Realizar un reconocimiento pasivo completo de un dominio utilizando dnsdumpster.com, centrales.net, FOCA, Shodan, Google Dorks y otras herramientas de OSINT. Llena cada sección con la información obtenida durante la actividad.

1. Mapeo DNS y Subdominios

Dominio objetivo: clinicavitalia.com

Fecha de análisis: 04/08/2025

1.1 Subdominios encontrados:

Subdominio	IP	TTL	Ubicación geográfica
portal.clinicavitalia.com	104.26.12.45		Cloudflare - Estados Unidos
intranet.clinicavitalia.com	201.151.33.210		México, Ciudad de México
mail.clinicavitalia.com	162.241.120.34		Estados Unidos
citas.clinicavitalia.com	104.26.12.45		Cloudflare - Estados Unidos
lab.clinicavitalia.com	201.151.33.211		México, Ciudad de México

http/https tech & titles: Todas las direcciones de Cloudflare muestran el mensaje 'Direct IP access not allowed'. Los servidores internos utilizan Apache 2.4.54, MariaDB y Microsoft-IIS/10.0 según la tecnología detectada.

1.2 Name Servers (NS):

lisa.ns.cloudflare.com

tom.ns.cloudflare.com

1.3 Registros MX (servidores de correo):

0 mail.clinicavitalia.com

1.4 Registros TXT (SPF, DMARC, etc.):

"v=spf1 +mx +a +ip4:162.241.120.34 +include:secureserver.net ~all"

2. WHOIS y Datos de Registro

2.1 Registrar: NameCheap, Inc.

2.2 Fecha de creación: 05/15/2012

2.3 Fecha de expiración: 05/15/2027

2.4 Estado del WHOIS (público/privado): Privado

2.5 Contacto Técnico: --- REDACTED FOR PRIVACY

2.6 Contacto Administrativo: --- REDACTED FOR PRIVACY

3. Metadatos de Documentos (FOCA)

3.1 Lista de documentos recuperados (nombre y URL):

Nombre de documento	URL	Metadatos clave (Autor, Software, Fechas)
informe_cardiologia.pdf	https://clinicavitalia.com/docs/informe_cardiologia.pdf	Autor: Dra. M. López | Software: Microsoft Word 2019 | Fecha: 2023-08-10
manual_pacientes.docx	https://clinicavitalia.com/manuales/manual_pacientes.docx	Autor: Ing. J. Torres | Software: Word 2016 | Fecha: 2024-01-15
resultados_lab.xlsx	https://lab.clinicavitalia.com/files/resultados_lab.xlsx	Autor: Bioq. P. Hernánde

z | Software: Excel 2019 | Fecha: 2025-02-22

3.2 Hallazgos relevantes de metadatos:

Rutas internas encontradas:
https://intranet.clinicavitalia.com/private/
https://lab.clinicavitalia.com/data/

Autores de documentos:
Dra. M. López
Ing. J. Torres
Bioq. P. Hernández

Software y versiones:
Microsoft Word 2019
Word 2016
Excel 2019
Adobe Photoshop CC 2022

4. Servicios Expuestos (Shodan)

4.1 Lista de IPs a verificar (extraídas en Sección 1):

104.26.12.45
201.151.33.210
162.241.120.34
201.151.33.211

4.2 Detalle de servicios expuestos:

IP	Puerto	Servicio/Versión	CVE asociadas	Ubicación geográfica
201.151.33.210	443/tcp	Microsoft-IIS/10.0	CVE-2020-0609, CVE-2020-0610	México, CDMX
201.151.33.210	3306/tcp	MariaDB 10.3.29	CVE-2021-27928	México, CDMX
162.241.120.34	22/tcp	OpenSSH 8.4p1	CVE-2023-	Estados Unidos,

			51767	Dallas
201.151.33.211	8080/tcp	Apache Tomcat 9.0.54	CVE-2021-41079	México, CDMX

4.3 Observaciones adicionales:

Puertos críticos expuestos: 3306 (MariaDB), 8080 (Apache Tomcat) y 22 (SSH).
Versiones vulnerables detectadas: MariaDB 10.3.29 y Apache Tomcat 9.0.54 requieren actualización.

5. Hallazgos con Google Dorks

5.1 Consultas utilizadas y resultados encontrados:

Consulta Dork	URL/Resultado encontrado
site:clinicavitalia.com	Página principal y varios subdominios indexados.
inurl:intranet	Se detectaron portales internos con login expuesto.
filetype:pdf clinicavitalia	Documentos PDF públicos con información interna.
intitle:Clinicavitalia	Resultados con títulos de páginas de servicios médicos.

5.2 Descripción de riesgos de cada hallazgo:

Hallazgo 1: Subdominios y páginas indexadas en buscadores.
Riesgo: Bajo.

Hallazgo 2: Portal de intranet visible públicamente.
Riesgo: Alto.

Hallazgo 3: Documentos PDF con datos internos.
Riesgo: Medio-Alto.

Hallazgo 4: Información de servicios médicos accesible.
Riesgo: Medio.

6. Recomendaciones de Hardening Inicial

- Actualizar versiones vulnerables detectadas.
- Restringir acceso público a la intranet.
- Revisar documentos expuestos y eliminar datos sensibles.
- Implementar autenticación multifactor en SSH.
- Configurar correctamente DMARC y DKIM.

7. Conclusión

La auditoría OSINT al dominio clinicavitalia.com permitió identificar subdominios con servicios expuestos, versiones de software vulnerables y documentos internos disponibles públicamente. Se recomienda aplicar medidas inmediatas de hardening y monitoreo continuo para mitigar riesgos.