Formato de Auditoría OSINT: Reconocimiento Pasivo de Dominio

Introducción

Objetivo: Realizar un reconocimiento pasivo completo de un dominio utilizando dnsdumpster.com, centrolops.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: cecyteqroo.edu.mx

Fecha de análisis: 15/06/25

1.1 Subdominios encontrados:

Subdominio	IP	TTL	Ubicación geográfica
consulta-tu-nomina.cecyteqroo.edu.mx	207.7.87.18	53	US
cpanel.cecyteqroo.edu.mx	38.124.220.159	52	MX
erp.cecyteqroo.edu.mx	207.7.87.18	53	US
ns2.cecyteqroo.edu.mx	207.7.87.180	53	US
server.cecyteqroo.edu.mx	38.124.220.159	52	MX

1.2 Name Servers (NS):

- ns1.mxwebserver.com

- ns2.mxwebserver.com

1.3 Registros MX (servidores de correo):

- 5 alt2.aspmx.l.google.com

- 1 aspmx.l.google.com

- 10 alt3.aspmx.l.google.com

- 10 alt4.aspmx.l.google.com

- 5 alt1.aspmx.l.google.com

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

- "v=spf1 ip4:38.124.220.159 include:relay.mailchannels.net ip4:38.124.220.159 ip4:67.222.137.54 include:spf.mxwebserver.com +a +mx +ip4:209.236.114.106 +ip4:209.236.114.107 ~all"

2. WHOIS y Datos de Registro

2.1 Registrar: AKKY ONLINE SOLUTIONS, S.A. DE C.V.

2.2 Fecha de creación: 2002-08-22

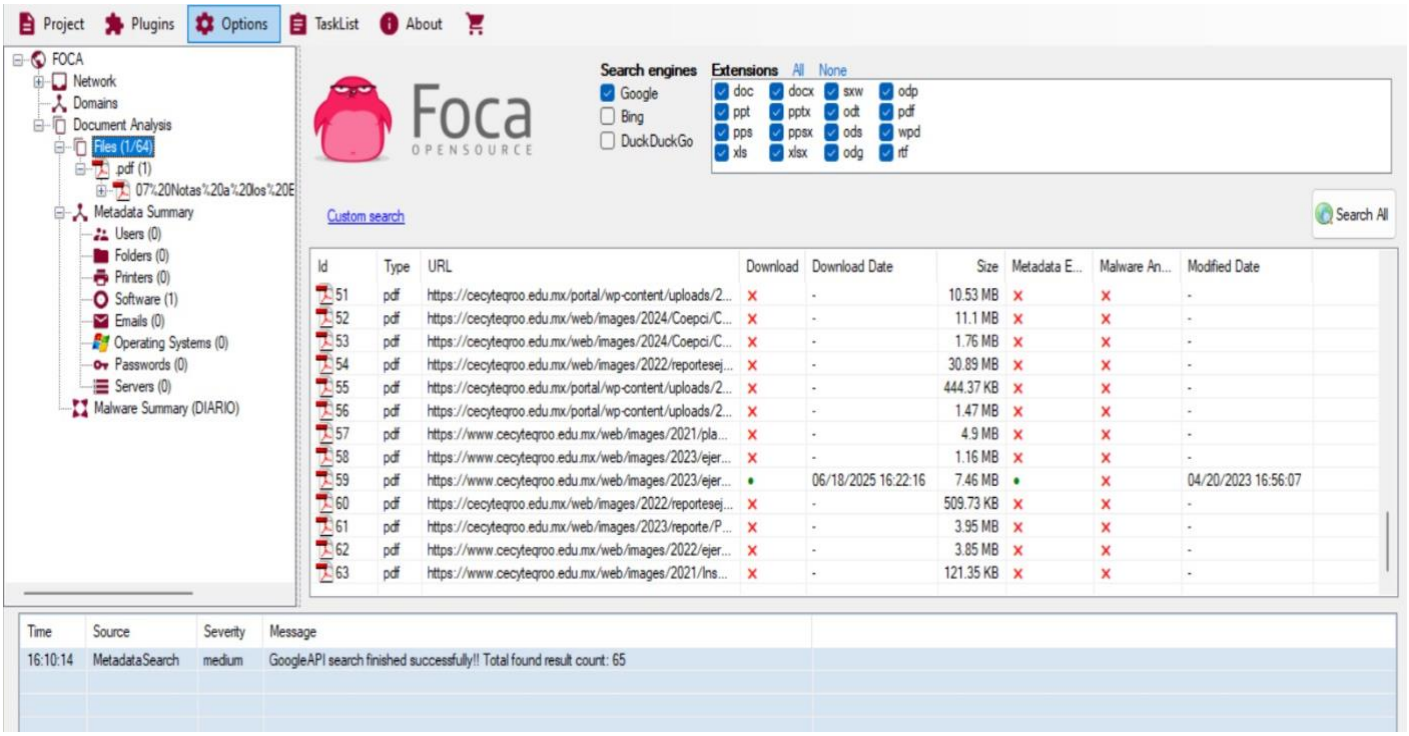
2.3 Fecha de expiración: 2025-08-21

2.4 Estado del WHOIS (público/privado): público

2.5 Contacto Técnico: TuSite Administracion de Dominios

2.6 Contacto Administrativo: JOEL HERNAN DZUL BALAM

3. Metadatos de Documentos (FOCA)



3.1 Lista de documentos recuperados (nombre y URL):

Nombre de documento	URL	Metadatos clave (Autor, Software, Fechas)
07 Notas a los Estados Financieros.pdf	https://www.cecyteqroo.edu.mx/web/images/2023/ejerciciofiscal/1ertrismestre/07%20Notas%20a%20los%20Estados%20Financieros.pdf	Nitro Pro 13 (13.49.2.993

3.2 Hallazgos relevantes de metadatos:

- Rutas internas encontradas:

- Autores de documentos:

- Software y versiones:

4. Servicios Expuestos (Shodan)

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

-207.7.87.18

-38.124.220.159

-207.7.87.18

-207.7.87.180

-38.124.220.159

4.2 Detalle de servicios expuestos:

IP	Puerto	Servicio/Versión	CVE asociadas	Ubicación geográfica
207.7.87.18	21, 22, 80, 443, 8888	Pure-FTPd, OpenSSH, ApacheHttpd, nginx	NA	US
38.124.220.159	21, 26, 53, 80, 110, 143, 443, 465, 587, 993, 995, 2082, 2083, 2086, 2087	Pure-FTPd, nginx	NA	MX
207.7.87.18	21, 22, 80, 443, 8888	Pure-FTPd, OpenSSH, ApacheHttpd, nginx	NA	US
207.7.87.180	21, 22, 80, 443, 8888	Pure-FTPd, OpenSSH, ApacheHttpd, nginx	NA	US
38.124.220.159	21, 26, 53, 80, 110, 143, 443, 465, 587, 993, 995, 2082, 2083, 2086, 2087	cPanel, Pure-FTPd, nginx	NA	MX

4.3 Observaciones adicionales:

- Puertos críticos expuestos: Puerto 22 abierto para SSH, Puerto 21 para FTP

- Versiones vulnerables detectadas:

5. Hallazgos con Google Dorks

5.1 Consultas utilizadas y resultados encontrados:

Consulta Dork	URL/Resultado encontrado

5.2 Descripción de riesgos de cada hallazgo:

- Hallazgo 1:

- Hallazgo 2:

- Hallazgo 3:

6. Recomendaciones de Hardening Inicial

Basado en los hallazgos anteriores, sugerir medidas para mejorar la seguridad:

1. Cerrar puertos criticos, SSH y FTP

2.

3.

4.

5.

7. Conclusión

Resumen de los hallazgos más relevantes y lecciones aprendidas:

En este dominio no habian demasiadas cosas que visualizer, como vulnerabilidades, en cuanto a los archivos y los google dorks tampoco habia algo interesante, lo unico fue una pagina para consultar la nomina, supongo de empleados, esto lo encontre al momento de hacer la busqueda de dominios con DNSDumpster.