ING. REDES INTELIGENTES Y CIBERSEGURIDAD

Universidad Tecnológica de Cancún.

Alumno:

Moo Canul Jesús Enrique

Grupo: IRIYC91

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: ilovepdf.com

Fecha de análisis: 7-0-25

1.1 Subdominios encontrados:

Subdominio	IP	TTL	Ubicación geográfica
api.ilovepdf.com	158.69.69.117	16276	Canadá
1 aspmx.l.google.com	142.251.111.27	15169	Estados Unidos
aspmx2.googlemail.com	172.253.116.26	15169	Estados

1.2 Name Servers (NS):

chip.ns.cloudflare.com

1.3 Registros MX (servidores de correo):

alt2.aspmx.l.google.com

aspmx.l.google.com

aspmx2.googlemail.com

aspmx3.googlemail.com

alt1.aspmx.l.google.com

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

"ms=e98e081db72906061380769ed234aec4dd655d13"

"d1qs8m7x3hcnvysbstx4x7wsryzn649x"

"verificación-de-dominio-openai=dv-eZzkBRH6aayxEP2DVpULUvay"

"stripe-verification=e1b56f230e098d9005533f879bbe16ad14716eb1c2b75afe9d8193b21d733072"

Verificación del dominio Atlassian = moXUMbUmAXnpdjY2BReBz7ZH/DdIRCJ6Ofc76HAVsluNR5a7bHohPQbMaUZKZtvy

"v=spf1 incluye:spf.mandrillapp.com incluye:_spf.google.com incluye:fdspfus.freshemail.io incluye:sendgrid.net ~todos"

"Verificación del sitio de Google=pAhe8fGDtBicW8QIUQxjRPL2ibJAjKgg7W8CNoGxzPA"

"dsxwvtx7z3yc9hl0mpsctdx01gsdfjvq"

2. WHOIS y Datos de Registro

2.1 Registrar: whois.godaddy.com

2.2 Fecha de creación: 2009-12-16

2.3 Fecha de expiración: 2029-12-16

2.4 Estado del WHOIS (público/privado): PUBLICO

2.5 Contacto Técnico +1.4806242599

2.6 Contacto Administrativo: abuse@godaddy.com

3. Metadatos de Documentos (FOCA)

3.1 Lista de documentos recuperados (nombre y URL):

Nombre de documento	URL	Met adat

		os clave (Autor, Software, Fechas)
new_takaful_buss_transfer_scheme_agmt_dtd_080818_32e960eb67.pdf	https://www.takaful-ikhlas.com.my/api/uploads/new_takaful_buss_transfer_scheme_agmt_dtd_080818_32e960eb67.pdf	
Tuvalu-TC-Amdt.-Act-2016-native.pdf	https://assets.tobaccocontrollaws.org/uploads/legislation/Tuvalu/Tuvalu-TC-Amdt.-Act-2016-native.pdf	

3.2 Hallazgos relevantes de metadatos:

- Rutas internas encontradas: https://assets.tobaccocontrollaws.org/uploads/legislation/Tuvalu/Tuvalu-TC-Amdt.-Act-2016-native.pdf

- Autores de documentos: Se encontraron diversos documentos en los cuales se mencionaban datos como nombre de la empresa y de personas

- Software y versiones: NA

4. Servicios Expuestos (Shodan)

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

173.194.76.27

158.69.69.117

4.2 Detalle de servicios expuestos:

IP	Puerto	Servicio/Versión	CVE asociadas	Ubicación geográfica
173.194.76.27	25	SSL CertificateVersion: 3 (0x2	NA	Belgium
158.69.69.117	80/443	SSL CertificateVersion: 3 (0x2)	NA	canada

108.162.192.226	53/2053/2082/8880	CloudFlare	NA	United States
51.210.209.137	2083/3306	cPanel Login/ MariaDB/ Miscellaneous	NA	France

4.3 Observaciones adicionales:

- Puertos críticos expuestos: 80/443/25

- Versiones vulnerables detectadas:NA

5. Hallazgos con Google Dorks

5.1 Consultas utilizadas y resultados encontrados:

Consulta Dork	URL/Resultado encontrado
site:ilovepdf.com intitle:"Index of"	https://desktopupdate.ilovepdf.com/
site:ilovepdf.com intext:"password"	https://www.ilovepdf.com/blog/how-to-unlock-pdf

6. Recomendaciones de Hardening Inicial

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

Revisión y eliminación de archivos expuestos públicamente:

Identificar archivos accesibles mediante Google Dorks (site:ilovepdf.com intitle:"Index of") y restringir su acceso mediante autenticación o eliminación si no son necesarios.

Protección de datos sensibles:

Asegurar que ningún archivo indexado contenga información confidencial como contraseñas o nombres de usuario.

Implementar controles de metadatos para eliminar información sensible antes de publicar documentos (como autores, rutas internas o software usado).

Seguridad en los puertos abiertos:

Restringir el acceso a puertos críticos como 25, 80 y 443 mediante firewalls y políticas de control de acceso.

Fortalecimiento del WHOIS:

Aunque la información del WHOIS es pública, se recomienda revisar qué datos están expuestos y considerar utilizar servicios de privacidad si es apropiado.

Uso de servicios como Shodan para monitoreo constante:

Implementar una estrategia de vigilancia de superficie de exposición a internet (por ejemplo, alertas automáticas en Shodan) para detectar cambios y nuevas vulnerabilidades.

7. Conclusión

Durante el análisis de reconocimiento pasivo del dominio ilovepdf.com, se identificaron múltiples vectores de información pública que podrían ser utilizados en ataques dirigidos. Entre los hallazgos más relevantes se encuentran:

Archivos accesibles públicamente indexados en motores de búsqueda.

Presencia de registros MX y TXT con validaciones de servicios externos.

Puertos abiertos que podrían ser utilizados como punto de entrada.

Este ejercicio permitió comprender cómo la información expuesta públicamente puede ser aprovechada por atacantes sin necesidad de realizar acciones activas. Como lección principal, se destaca la importancia de realizar auditorías OSINT regulares como parte de una estrategia de ciberseguridad preventiva.