Reconocimiento activo y pasivo de recursos

Reconocimiento pasivo.

Es la obtención de información pública sin interactuar directamente con los servidores objetivo (sin enviar paquetes ni autenticarse). Útil para mapear superficie de ataque sin dejar rastro.

Herramientas utilizadas:

- **Google Dorks.** Consultas avanzadas a motores de búsqueda para localizar páginas, archivos y configuraciones expuestas.
- **Shodan / Censys / FOFA.** Motores de búsqueda de Internet que indexan dispositivos y servicios expuestos (banners, puertos, certificados).
- **Amass / Sublist3r**. Descubrimiento de subdominios mediante fuentes públicas, certificados y técnicas OSINT.
- **DNSdumpster:** Mapeo DNS público, registros y hosts visibles desde fuentes públicas.
- **crt.sh:** base pública de certificados TLS/SSL; útil para encontrar subdominios públicos vía registros de certificados.

Google Dorks.

Filtra resultados de Google para encontrar páginas, ficheros o directorios específicos, por ejemplo:

- site:dominio.gob.bo intitle:"login" => Busca páginas dentro del dominio que contienen "login" en el título.
- site:dominio.gob.bo filetype:env OR filetype:sql OR filetype:bak => Busca archivos con extensiones típicas de backups o configuración.
- site:dominio.gob.bo "index of" "backup" => Detecta índices de directorios que contengan la palabra backup.
- site:dominio.gob.bo inurl:admin OR inurl:dashboard => Encuentra URLs con “admin” o “dashboard” en la ruta.

Ejemplo de salida:

- Resultado 1: https://intranet.dominio.gob.bo/admin/login —

"Página de acceso administración"
- Resultado 2: https://www.dominio.gob.bo/.env.bak — "Archivo .env (posible fuga de credenciales)"
- Resultado 3: https://archivos.dominio.gob.bo/index of/backup/ — "Índice público con backups"

Shodan / Censys / FOFA

Permiten consultar por IP, dominio o servicio para ver los banners, puertos y software expuesto, por ejemplo:

Consulta: dispositivo con ip 200.12.34.56, resumen de salida:

- Host: 200.12.34.56
- Puertos abiertos: 22 (OpenSSH 7.6p1), 80 (nginx 1.14.0), 443 (nginx + certificado)
- Banner: "Apache/2.4.29 (Ubuntu)"
- Geolocalización: Bolivia (país de origen según IP)

Sublist3r.

Permite la enumeración de subdominios mediante consultas a múltiples fuentes públicas.

```
python3 sublist3r.py -d dominio.gob.bo -o subdoms.txt
```

Salida en archivo subdoms.txt:

```
cat subdoms.txt:
portal.dominio.gob.bo
mail.dominio.gob.bo
sri.dominio.gob.bo
dev.dominio.gob.bo
```

Amass (modo pasivo)
Agrega resultados de múltiples fuentes (crt.sh, ASN, servicios públicos) para hallar subdominios.

```
amass enum -passive -d dominio.gob.bo -o amass.txt
```

Salida en archivo amass.txt.

```
cat amass.txt, ejemplo
portal.dominio.gob.bo
```

```
api.dominio.gob.bo
backup.dominio.gob.bo
```

Uso de crt.sh

Busca certificados emitidos que incluyan subdominios del dominio objetivo.

URL de ejemplo: https://crt.sh/?q=%25.dominio.gob.bo

Resumen de la salida:

```
Certificado emitido: *.dominio.gob.bo — emitido 2025-03-12 — CN: api.dominio.gob.bo
```

DNSdumpster

Devuelve un mapa DNS público (registros A, MX, NS, subdominios detectados).
Resumen de la salida:

```
Registros A:
portal.dominio.gob.bo -> 200.12.34.10
mail.dominio.gob.bo -> 200.12.34.20

Registros MX:
mx1.dominio.gob.bo -> 200.12.34.30
```

Una vez realizado el reconocimiento pasivo es recomendable:

- Consolidar resultados en ficheros (subdoms.txt, amass.txt, crt_domains.txt).
- Correlacionar IPs con ASN y whois para identificar infraestructura.
- Registrar fechas de captura y fuentes (para trazabilidad).

Reconocimiento activo.

Es la interacción directa con el objetivo (escanear puertos, enumerar directorios, consultas DNS directas). Dejará registros en el objetivo; se debe realizar solo con autorización.

Herramientas utilizadas:

- **Nmap:** escaneo de puertos y fingerprinting de servicios/sistema operativo.
- **dig / host:** consultas DNS directas para obtener registros A, MX, TXT, etc.
- **gobuster / ffuf:** fuerza bruta de directorios/archivos web (enumeración de rutas).
- **curl:** realizar peticiones HTTP(S) y extraer cabeceras, cuerpos y respuestas.

Nmap para puertos comunes.

Escanea los puertos más comunes y detecta versiones de servicios.

```
nmap -sT -sV --top-ports 100 -T2 dominio_o_ip
```

Explicación breve de flags:

- -sT : TCP connect scan (no requiere privilegios root).
- -sV : detección de versión del servicio.
- --top-ports 100 : escanear los 100 puertos más comunes.
- -T2 : velocidad de escaneo conservadora.

Ejemplo resumen de salida:

```
Nmap scan report for dominio_o_ip (200.12.34.10)
Host is up (0.023s latency).
PORT STATE SERVICE  VERSION
22/tcp  open  sshOpenSSH 7.6p1 Ubuntu
80/tcp  open  http  nginx 1.14.0
443/tcp open  https nginx 1.14.0
Service Info: OS: Linux
```

Nmap para escaneo completo y OS detection.

Realiza un escaneo más agresivo y detección de SO (requiere privilegios).

```
sudo nmap -sS -p- -sV -O -T3 dominio_o_ip
```

Explicación breve de flags:

- -sS : SYN scan (stealthy, requiere root).
- -p- : escanea todos los puertos (1-65535).
- -O : detección de sistema operativo.
- -T3 : velocidad moderada.

Ejemplo resumen de salida:

```
PORTSTATE SERVICE VERSION
21/tcp open  ftp  vsftpd 3.0.3
22/tcp open  ssh  OpenSSH 7.6p1
```

```
80/tcp open  http nginx 1.14.0
443/tcpopen  httpsnginx 1.14.0
OS details: Linux 4.x
```

DNS (dig / host).

Realiza consultas directas al servidor DNS para obtener registros.

```
dig dominio.gob.bo  => Consulta A/AAAA/other por defecto; muestra servidores autoritativos y TTL.
```

```
Salida ejemplo (dig):
 ; <<>> DiG 9.16.1 <<>> dominio.gob.bo
 ;; ANSWER SECTION:
 dominio.gob.bo.  3600  IN  A  200.12.34.10
 ;; AUTHORITY SECTION:
 dominio.gob.bo.  172800 IN NS ns1.dominio.gob.bo.
 ;; ADDITIONAL SECTION:
 ns1.dominio.gob.bo. 172800 IN A 200.12.34.2
```

```
host subdominio.dominio.gob.bo   => Respuesta simple: subdominio.dominio.gob.bo has address 200.12.34.20
```

Gobuster.

Realiza la enumeración de directorios y archivos web mediante fuerza bruta con wordlists.

```
gobuster dir -u [https://dominio.gob.bo](https://dominio.gob.bo) -w wordlist.txt
```

Explicación:

- dir : modo directorios
- -u : URL objetivo
- -w : palabra lista para probar rutas

Ejemplo de salida:

```
/admin (Status: 200)
/backup (Status: 403)
/config.php (Status: 200)
/robots.txt (Status: 200)
```

Uso de ffuf.

Es un fuzzer web rápido, útil para encontrar endpoints ocultos o parametrizados.

```
ffuf -u [https://dominio.gob.bo/FUZZ](https://dominio.gob.bo/FUZZ) -w wordlist.txt
```

Salida ejemplo:

```
Found: /secret (Status: 200, Size: 1534)
Found: /old-admin (Status: 200, Size: 4210)
```

Uso de curl.

Tiene el objetivo de solicitar recursos HTTP(S), ver cabeceras y contenido; útil para comprobar respuestas, cookies y cabeceras de seguridad.

```
curl -I [https://dominio.gob.bo](https://dominio.gob.bo)  => Obtiene solo cabeceras (HEAD).
```

Ejemplo de salida (cabeceras):

```
HTTP/1.1 200 OK
Server: nginx/1.14.0
Content-Type: text/html; charset=UTF-8
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

```
curl -L -s -D - [https://dominio.gob.bo/login](https://dominio.gob.bo/login) -o /dev/null => Sigue redirecciones (-L), imprime cabeceras (-D -), suprime el cuerpo (-o /dev/null).
```

Se recomienda:

- Respetar límites de velocidad y ventanas de tiempo para evitar DoS involuntario (-T2/-T3 en nmap).
- Realizar escaneos iniciales con perfiles conservadores y aumentar detalle solo con autorización.
- Usar IPs y ranges detectados para correlacionar servicios y subdominios.

Divulgación de Credenciales

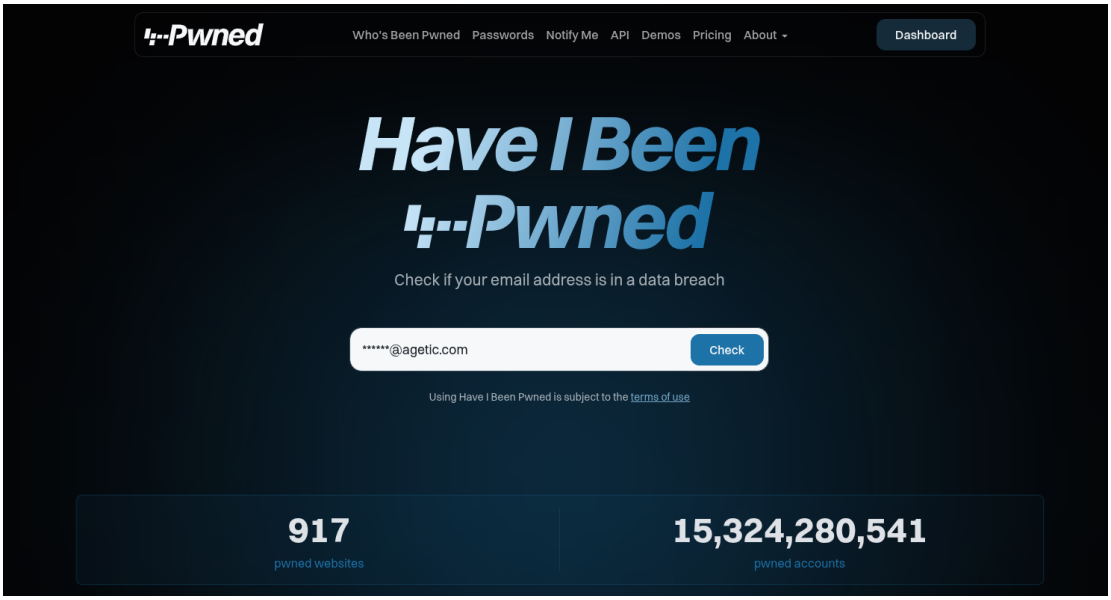
Identificación de credenciales expuestas públicamente.

Herramientas

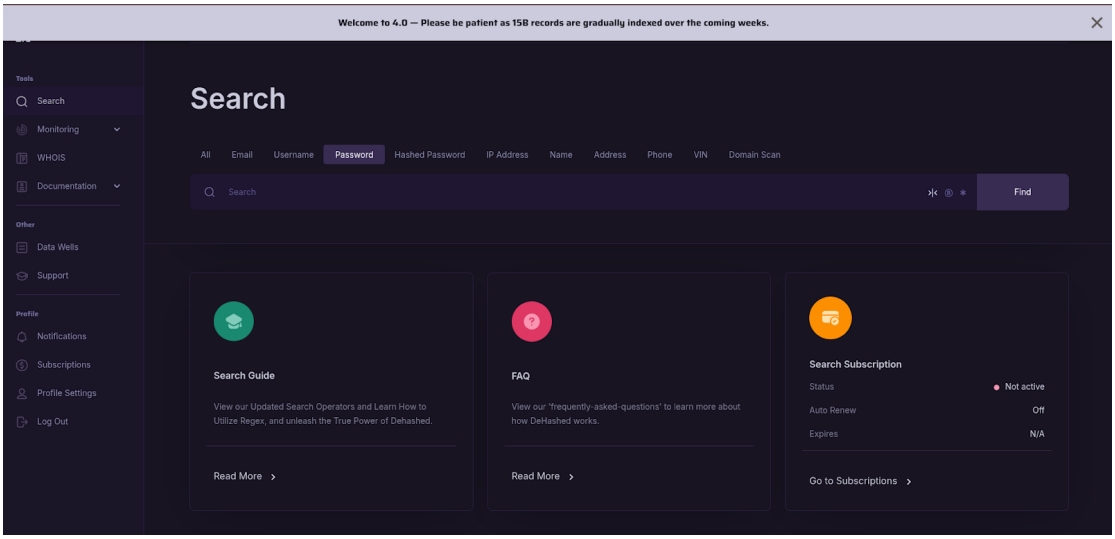
- Have I Been Pwned
- DeHashed
- Leak-Lookup

Enlaces

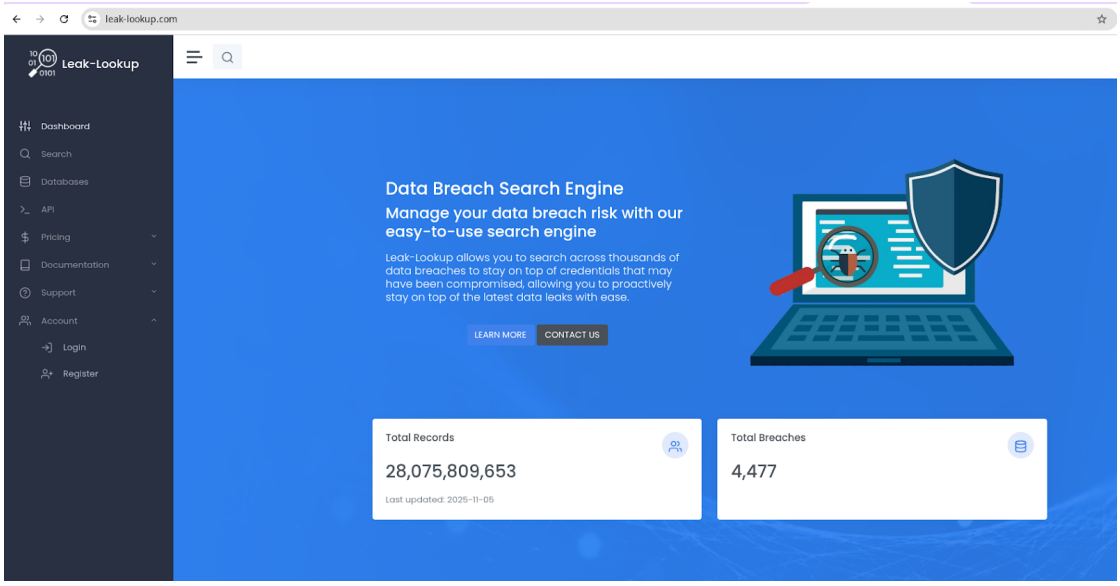
- https://haveibeenpwned.com/



- https://app.dehashed.com/login



- https://leak-lookup.com/



Procedimiento

- Buscar correos filtrados.
- Registrar hallazgos.

Revision #5
Created 5 noviembre 2025 16:54:22 by Ricardo Chavez
Updated 5 noviembre 2025 17:27:53 by Ricardo Chavez