



SHERLOCK: MINIGUIA DE OSINT CORPORATIVO PARA RED TEAM Y CIBERINTELIGENCIA



Técnicas reales para detectar
exposición digital, suplantación,
shadow IT y errores humanos

Aplicado en contextos de pruebas
de intrusión, Red Team y defensiva
ofensiva

Daniel Espinosa Delgado

Ethical Hacker / OSINT /

Red Team

LinkedIn: D4nYeD

Abril 2025



Guía Completa OSINT Empresarial con Sherlock





Autor: Daniel Espinosa Delgado | @D4nYeD

 Abril 2025 | Licencia: Educativa y profesional – se permite compartir con atribución

¿Qué es Sherlock?

Sherlock es una herramienta OSINT que permite detectar la **presencia pública de alias o usuarios** en más de **300 servicios online** (GitHub, Instagram, TikTok, Reddit, Twitter, Pastebin, etc.).

 En entornos corporativos, su valor es enorme para:

-  Huella digital de empleados
-  Preparación de campañas de Red Team o phishing ético
-  Defensa ante suplantación de marca o personal
-  Reconocimiento ofensivo previo a pruebas técnicas


Aviso Legal

Todo lo descrito en esta guía debe ejecutarse **solo con consentimiento y en entornos controlados**. Sherlock **no accede a información privada**, pero su mal uso puede tener consecuencias legales. **Esto es OSINT. No hacking ilegal.**

EJEMPLOS DE USO DE SHERLOCK


Reutilización de alias en redes personales

`sherlock lucasrodriguez lrodriguez`

 Detecta si empleados usan su alias profesional en redes personales: riesgo de exposición accidental.

Preparación de campañas de spear phishing realista

`sherlock ricardoit sandracontabilidad`

 Extrae hobbies, imágenes, detalles de su entorno... y simula correos más creíbles.



Detección de Shadow IT (Dropbox, Mega, GitHub...)

holehe jramirez@empresa.com

sherlock jramirez jramirez2023

- Identifica servicios no aprobados por IT, pero usados por empleados.

Análisis de ex-empleados (riesgo residual)

sherlock cgarcia

- Detecta si aún usan el alias de la empresa en GitHub, Pastebin, etc. Pueden filtrar info antigua.

Identificar cuentas vulnerables a password spraying

sherlock -f usuarios.txt --print-found

- Mapea plataformas donde hay cuentas con nombres predecibles. Cruza con contraseñas débiles.

Cultura interna visible en redes

sherlock lfernandez

- Detección de QR visibles, pantallas, eventos internos, insignias... en redes como Instagram, TikTok o Twitter.

Suplantación de identidad de marca

sherlock empresa_support empresahelp empresa_rrhh

- Cuentas que podrían estar suplantando la empresa para estafas, ingeniería social o phishing.

Monitorear nombres de productos internos

sherlock secureXpro helixcloud aurorax

- Evita que alguien use nombres de proyectos aún no públicos como alias en plataformas sociales.

Buscar scripts internos o configuraciones filtradas

sherlock deployKube configBackup ssh_config

- Detecta si nombres de archivos o scripts internos están publicados por error.
-



Validar si leaks expuestos coinciden con cuentas reales

```
cat leak.txt | grep "@empresa.com" | cut -d@ -f1 > leaked_users.txt  
sherlock -f leaked_users.txt
```

- Cruza leaks antiguos con Sherlock para evaluar qué cuentas siguen activas.

Confirmar presencia digital antes de ataques simulados

```
sherlock jgomez_admin
```

- Sherlock te dice si el alias existe en GitHub, StackOverflow, etc. Ideal para fase de footprinting.

Verificar publicaciones técnicas con info sensible

```
sherlock mariadevops infosecmarko
```

- Encuentra si desarrolladores hablan de configuraciones, errores o proyectos reales.

Estudio de exposición masiva en redes por evento

```
sherlock -f asistentes_evento.txt
```

- Evalúa si asistentes a una conferencia de la empresa están sobreexpuestos en plataformas públicas.

Auditoría interna de seguridad de RRHH / Soporte

```
sherlock soporte_empresa rrhh_empresa
```

- Confirma si existen cuentas falsas o clones que intentan parecer oficiales.

Integración en un pipeline OSINT corporativo

```
holehe user@empresa.com
```

```
sherlock user
```

- 🔧 Puedes automatizar esto en un script que recoja correos → extraiga usuarios → cruce con Sherlock → y te devuelva presencia en plataformas sensibles.
-



Bonus Técnicos Avanzados

- `sherlock -f users.txt --print-found --tor` 🗝️ Uso de red Tor para anonimato
- `sherlock --timeout 3 --rate-limit 10` 🚦 Limita velocidad para evitar bloqueos o captchas
- `sherlock alias --proxy "socks5://127.0.0.1:9050"` 🌐 Proxifica búsquedas



Herramientas que combinan bien con Sherlock

Herramienta	Uso Complementario
Holehe	Verifica si un correo existe en servicios
HaveIBeenPwned	Busca leaks por dominio o usuario
theHarvester	Saca correos, subdominios, alias
Recon-ng	Framework modular para automatizar OSINT
GitHub Dorks	Encuentra código sensible filtrado
Shodan	Encuentra IPs o dispositivos públicos



Propuesta de estructura para pipeline OSINT empresarial

1. Extraer correos corporativos (@empresa.com)
2. Convertirlos en alias potenciales
3. Buscar con Sherlock
4. Validar con Holehe
5. Cruzar con HaveIBeenPwned y GitHub Dorks
6. Documentar hallazgos y exponer recomendaciones



Conclusión

Si tus empleados usan su alias profesional en redes, foros o GitHub...
Entonces tu empresa está expuesta, aunque no lo sepas.

Sherlock es una herramienta de **prevención** tanto como de exploración.
Úsala para **pensar como atacante** antes de que lo haga uno real.



Contacto: danyjerez@proton.me



LinkedIn: Daniel Espinosa Delgado



Licencia: Educativa y profesional – Se permite compartir con atribución
