La herramienta **Changeme** es un escáner de contraseñas predeterminadas diseñado para ayudar en evaluaciones de seguridad, especialmente en la etapa de **explotación** de vulnerabilidades o penetración de redes. Puede ser útil en una explotación de varias formas:

1. **Identificación de contraseñas por defecto**: **Changeme** escanea dispositivos o servicios para encontrar credenciales que no han sido modificadas desde su configuración predeterminada, lo cual es un fallo de seguridad muy común. Muchos dispositivos y aplicaciones vienen con contraseñas preestablecidas (por ejemplo, "admin/admin" o "root/root"). Si esas credenciales no se han cambiado, un atacante podría explotarlas fácilmente para acceder al sistema.
2. **Automatización de ataques**: En lugar de que un atacante pruebe manualmente varias contraseñas en diferentes servicios, **Changeme** automatiza este proceso, facilitando la explotación masiva de dispositivos vulnerables con configuraciones predeterminadas.
3. **Reconocimiento de servicios vulnerables**: **Changeme** está diseñado para trabajar con varios protocolos y servicios (HTTP, SSH, FTP, etc.). Si en un entorno hay múltiples dispositivos o servicios con credenciales predeterminadas, esto puede abrir puertas para que un atacante obtenga acceso no autorizado y escale privilegios.
4. **Securización post-explotación**: Aunque su principal función es encontrar credenciales predeterminadas, también puede ser útil para verificar si un entorno ha sido correctamente asegurado después de una explotación o auditoría de seguridad, asegurando que no queden credenciales predeterminadas.

Opciones:

-h, --help Mostrar este mensaje de ayuda y salir

--all, -a Escanear todos los protocolos

--category CATEGORÍA, -c CATEGORÍA

Categoría de credenciales predeterminadas para escanear

--contributors Mostrar los contribuyentes del archivo de credenciales

--debug, -d Salida de depuración

--delay RETRASO, -dl RETRASO

Especificar un retraso en milisegundos para evitar códigos de estado 429 valor predeterminado=500

--dump Imprimir todas las credenciales cargadas

--dryrun Imprimir las URL que se escanearán, pero no escanearlas

--fingerprint, -f Tomar huellas digitales de los objetivos, pero no comprobar las credenciales

--fresh Limpiar los escaneos anteriores y comenzar de nuevo

--log REGISTRO, -l REGISTRO Escribir registros en el archivo de registro

--mkcred Crear archivo de credenciales

--name NOMBRE, -n NOMBRE Limitar las pruebas al nombre de la credencial suministrada

--noversion No realizar una comprobación de la versión

--proxy PROXY, -p PROXY

Proxy HTTP(S)

--output SALIDA, -o SALIDA

Nombre del archivo de resultados. La extensión del archivo determina el tipo (csv, html, json).

--oa Archivos de resultados de salida en formatos csv, html y json

--protocols PROTOCOLOS

Lista separada por comas de protocolos para probar: http,ssh,ssh\_key. El valor predeterminado es http.

--portoverride Analizar todos los protocolos en todos los puertos especificados

--redishost REDISHOST

Servidor Redis

--redisport REDISPORT

Servidor Redis

--resume, -r Reanudar el análisis anterior

--shodan\_query SHODAN\_QUERY, -q SHODAN\_QUERY

Consulta de Shodan

--shodan\_key SHODAN\_KEY, -k SHODAN\_KEY

Clave de API de Shodan

--ssl Forzar credenciales a SSL y volver a no SSL si ocurre un error SSL

--threads SUBPROCESOS, -t SUBPROCESOS

Número de subprocesos, predeterminado=10

--timeout TIMEOUT Tiempo de espera en segundos para una solicitud, predeterminado=10

--useragent USERAGENT, -ua USERAGENT

Cadena de agente de usuario a utilizar

--validate Validar archivos de credenciales

--verbose, -v Salida detallada