

# Metagoofil

在笔测试期间进行文档和元数据侦察的最佳工具之一是metapril，由边缘安全组的Christian Martorella @laramies编写。源代码可以在这里找到：<https://github.com/laramies/metagoofil>，

但默认情况下，它带有Kali。该工具已经有几年没有更新了，可以使用一些薄层色谱。

——Christian Martorella @laramies

## 一，帮助文档

usage: metagoofil.py [-h] -d 域 [-e 延时] [-f] [-i URL\_TIMEOUT] [-l SEARCH\_MAX] [-n  
DOWNLOAD\_FILE\_LIMIT] [-o SAVE\_DIRECTORY] [-r NUMBER\_OF\_THREADS] -t  
FILE\_TYPES [-u [USER\_AGENT]] [-w]

Metagoofil - Search and download specific filetypes

optional arguments:

-h, --help	显示此帮助消息并退出
-d DOMAIN	要搜索的域。
-e DELAY	搜索之间的延迟(秒)。如果太小，谷歌可能会屏蔽你的知识产权；如果太大，你的搜索可能需要一段时间。默认:30.0
-f	将html链接保存到html_links_&lt;TIMESTAMP &gt;.txt文件。
-i URL_TIMEOUT	不可访问/过期页面超时前等待的秒数。默认值:15
-l SEARCH_MAX	要搜索的最大结果。默认值:100
-n DOWNLOAD_FILE_LIMIT	每个文件类型可下载的最大文件数。默认值:100
-o SAVE_DIRECTORY	保存下载文件的目录。DEFAULT是cwd, " "
-r NUMBER_OF_THREADS	搜索线程数。默认值:8
-t FILE_TYPES	要下载的文件类型(pdf、doc、xls、ppt、odp、ods、docx、xlsx、pptx)。要搜索所有17,576个三字母文件扩展名，请键入“all”
-u [USER_AGENT]	针对-d域的文件检索的用户代理 no -u = "Mozilla/5.0(兼容; Google bot/2.1; +http://www.Google.com/bot.html)

-u =随机用户-代理  
-u“我的自定义用户代理2.0”=您的自定义用户代理  
下载文件，而不仅仅是查看搜索结果

usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f] [-i URL\_TIMEOUT] [-l SEARCH\_MAX] [-n  
DOWNLOAD\_FILE\_LIMIT] [-o SAVE\_DIRECTORY] [-r  
NUMBER\_OF\_THREADS] [-t  
FILE\_TYPES [-u [USER\_AGENT]] [-w]

Metagoofil - Search and download specific filetypes

optional arguments:  
-h, --help show this help message and exit  
-d DOMAIN Domain to search.  
-e DELAY Delay (in seconds) between searches. If it's too small  
Google may block your IP, too big and your search may take a while. DEFAULT:  
30.0  
-f Save the html links to html\_links\_<TIMESTAMP>.txt file.  
-i URL\_TIMEOUT Number of seconds to wait before timeout for  
unreachable/stale pages. DEFAULT: 15  
-l SEARCH\_MAX Maximum results to search. DEFAULT: 100  
-n DOWNLOAD\_FILE\_LIMIT Maximum number of files to download per filetype.  
DEFAULT: 100  
-o SAVE\_DIRECTORY Directory to save downloaded files. DEFAULT is cwd, "."  
-r NUMBER\_OF\_THREADS Number of search threads. DEFAULT: 8  
-t FILE\_TYPES file\_types to download  
(pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx). To search all 17,576 three-letter  
file extensions, type "ALL"  
-u [USER\_AGENT] User-Agent for file retrieval against -d domain.  
no -u = "Mozilla/5.0 (compatible; Googlebot/2.1;  
+http://www.google.com/bot.html)"  
-u = Randomize User-Agent  
-u "My custom user agent 2.0" = Your customized User-  
Agent  
-w Download the files, instead of just viewing search  
results.

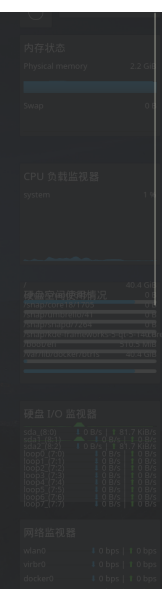
无法正常运行，当前系统环境:

Linux parrot 5.4.0-4parrot1-amd64 #1 SMP Parrot 5.4.19-4parrot1 (2020-02-27) x86\_64 GNU/Linux

```
[root@parrot: /home/kun]
# metagoofil -d woshicainiao.cn -t pdf
[*] Adding -w for you
[*] Downloaded files will be saved here: /home/kun
[*] Searching for 100 .pdf files and waiting 30.0 seconds between searches
Traceback (most recent call last):
  File "/usr/lib/python3.8/urllib/request.py", line 1319, in do_open
    h.request(req.get_method(), req.selector, req.data, headers,
  File "/usr/lib/python3.8/http/client.py", line 1230, in request
    self._send_request(method, url, body, headers, encode_chunked)
  File "/usr/lib/python3.8/http/client.py", line 1276, in _send_request
    self.send_headers(body, encode_chunked=encode_chunked)
  File "/usr/lib/python3.8/http/client.py", line 1225, in send_headers
    self.send_output(message_body, encode_chunked=encode_chunked)
  File "/usr/lib/python3.8/http/client.py", line 1004, in send_output
    self.send(msg)
  File "/usr/lib/python3.8/http/client.py", line 944, in send
    self.connect()
  File "/usr/lib/python3.8/http/client.py", line 1392, in connect
    super().connect()
  File "/usr/lib/python3.8/http/client.py", line 915, in connect
    self.sock = self._create_connection()
  File "/usr/lib/python3.8/socket.py", line 808, in create_connection
    raise err
  File "/usr/lib/python3.8/socket.py", line 796, in create_connection
    sock.connect(sa)
ConnectionRefusedError: [Errno 111] Connection refused

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/share/metagoofil/metagoofil.py", line 323, in <module>
    go()
  File "/usr/share/metagoofil/metagoofil.py", line 147, in go
    for url in googlesearch.search(
  File "/usr/lib/python3.8/dist-packages/googlesearch/__init__.py", line 257, in search
    get_page(url_home % vars(), user_agent)
  File "/usr/lib/python3.8/dist-packages/googlesearch/__init__.py", line 154, in get_page
    response = urlopen(request)
  File "/usr/lib/python3.8/urllib/request.py", line 222, in urlopen
    return opener.open(url, data, timeout)
  File "/usr/lib/python3.8/urllib/request.py", line 525, in open
    response = self._open(req, data)
  File "/usr/lib/python3.8/urllib/request.py", line 542, in _open
    result = self._call_chain(self.handle_open, protocol, protocol +
```



如果你恰好对Metagoofil有相关方面的使用（正常使用），或者说是解决方法，请联系:backsunli@yeah.net