به نام خداوند خورشید و ماه که دل را به نامش خرد داد راه

آشنایی با ابزار ***The Harvester*** در کالی لینوکس

سایت مرجع :

Kaliuser

اولین مرجع فارسی زبان اختصاصی کاربران سیستم عامل کالی لینوکس

بهار ۱۳۹۶

معرفی اجمالی ابزار *theharvester*

هدف این برنامه گردآوری اطلاعات مربوط به ایمیل ، زیردامنه[۱] ، هاست ، اسامی کارکنان، پورت های باز و بنر های یک سایت یا هدف[۲] با استفاده از موتور های جستجو یا دیتابیس هایی واقع در سرور ها یا کامپیوتر های خاص، می باشد .

این برنامه به منظور کمک به متخصصین امنیت و تست نفوذ در مراحل اولیه عملیات برای پی بردن به مشخصات کاربردی "هدف" بر روی اینترنت به کار میرود. از طرفی می تواند به هر کسی که قصد دارد بداند که یک مهاجم[۳] توانایی دست یابی به کدام یک از اطلاعات مربوط به سازمان آن ها را دارد.

امکانات پکیج *theharvester*

برای استفاده از این ابزار کافیست مانند تصویر زیر در ترمینال در حالت روت[٤] بنویسید *theharvester* :

```
root@kali:~# theharvester

*******************************************************************
*                                                                 *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___|  \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.2a                                          *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************
```

---

۱. Subdomain
۲. Target
۳. Attacker
٤. **برای رفتن به حالت روت کافیست قبل از دستور مورد نظر عبارت sudo را تایپ کنید و یا همین که وارد ترمینال شدید بنویسید su و اینتر را زده و رمز را وارد کنید**

امکانات موجود در این ابزار به همراه های سویچ های لازم برای استفاده از آن ها را می بینید :

```
Usage: theharvester options

       -d: Domain to search or company name
       -b: Data source (google,bing,bingapi,pgp,linkedin,google-profiles,people123,jigsaw,all)
       -s: Start in result number X (default 0)
       -v: Verify host name via dns resolution and search for virtual hosts
       -f: Save the results into an HTML and XML file
       -n: Perform a DNS reverse query on all ranges discovered
       -c: Perform a DNS brute force for the domain name
       -t: Perform a DNS TLD expansion discovery
       -e: Use this DNS server
       -l: Limit the number of results to work with(bing goes from 50 to 50 results,
       -h: use SHODAN database to query discovered hosts
            google 100 to 100, and pgp doesn't use this option)
```

نحوه استفاده از ابزار *theharvester*

با زدن اسم این ابزار در ترمینال در همین ابتدای کار تمام سوئیچ ها به همراه چند مثال[1] به نمایش در میاد :

```
Examples: theharvester -d microsoft.com -l 500 -b google
            theharvester -d microsoft.com -b pgp
            theharvester -d microsoft -l 200 -b linkedin
```

سوئیچ d برای مشخص کردن دامنه هدف بعد از آن و l برای محدود کردن تعداد نتایج جستجو و سوئیچ b برای آوردن نام مرجع لازم برای استخراج اطلاعات از آن است.

به عنوان مثال اگر بخواهیم اطلاعات مربوط به ایمیل های اساتید و آی پی های بخش های مختلف دانشگاه تبریز رو از طریق یکی از مورد هایی که خوده برنامه در قسمت توضیح سویچ ها برای سویچ b ذکر کرده (مثلا گوگل) بدست بیاریم، در ترمینال مینویسیم :

```
root@kali:~# theharvester -d tabrizu.ac.ir -l 20 -b google -f 1.html
```

سوئیچ اختیاری h رو هم برای ذخیره نتایج در یک فایل با نام دلخواه مثلا؛ 1.html در فولدر Home، به کار بردیم، که اگه این سوئیچ را استفاده نکنید همه نتایج در خود ترمینال نمایش داده خواهد شد.

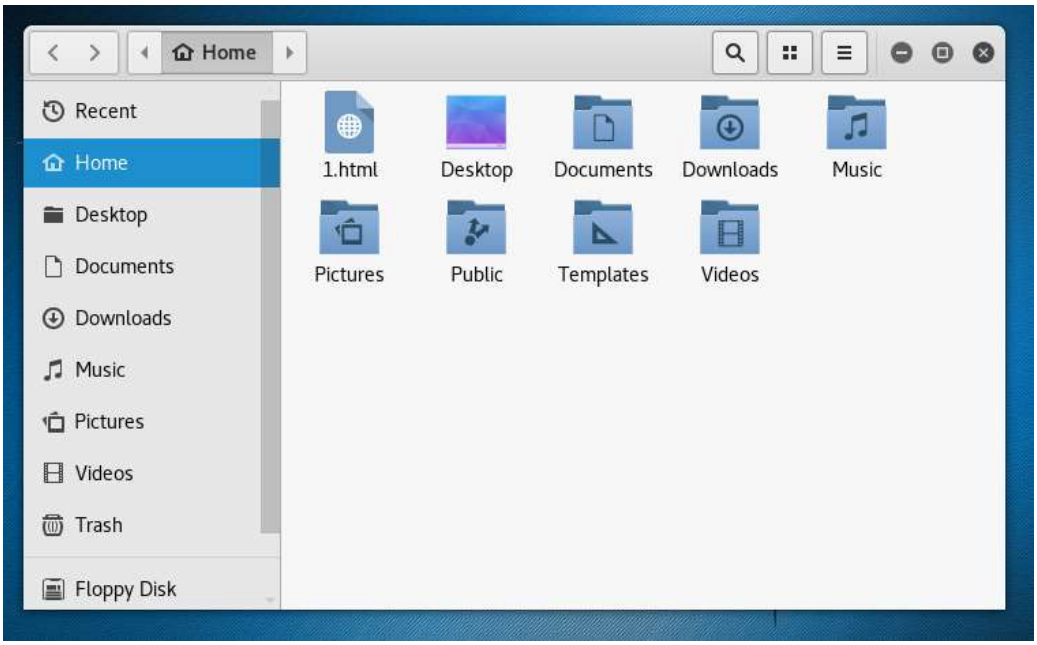
---

۱. Example

که برای مثال؛ نتایج مربوط به ایمیل ها مانند شکل زیر خواهد بود :

```
[+] Emails found:
------------------
Jashnvareh@tabrizu.ac.ir
sabahi@tabrizu.ac.ir
yazdanpanah@tabrizu.ac.ir
n.talebi@tabrizu.ac.ir
hashemzadeh@tabrizu.ac.ir
bmohammadi@tabrizu.ac.ir
h_hosseini@tabrizu.ac.ir
ssadr@tabrizu.ac.ir
m_zarifi@tabrizu.ac.ir
zdaie@tabrizu.ac.ir
jsobhi@tabrizu.ac.ir
malekshahi@tabrizu.ac.ir
adjab@tabrizu.ac.ir
s_mahmoudi@tabrizu.ac.ir
m.mehdinejad92@ms.tabrizu.ac.ir
sayyad.nojavan@tabrizu.ac.ir
kazem.zare@tabrizu.ac.ir
babaei@tabrizu.ac.ir
nadiri@tabrizu.ac.ir
```

و فایل گزارش در فولدر Home قابل دستیابی است :



با آرزوی بهترین ها برای شما، کالی یوزر