

Forum:[Hack Forums](#)

Thread: [Kali Linux \(Tutorial 1 \) \(TheHarvester\)](#)

Zero_Luffy - October 6, 2014, 6:24 pm

Hi, I'm IT Security and Programming student, in my counter a mate of mine is working about Project to Kali Linux, so I decided to be Posting his tutorial so that People can have some idea about tool on Kali lot of time I saw People posting thread about How to use Kali tool.

Collect Domain, E-mail address & Document Metadata information from the Target
The Kali Linux tools grouped in this category can be used to collect domain, e-mail address, and document metadata information from the target. These tools use a search engine to do their actions. The advantage of these tools is that they use search engine sites. So, you don't access the target website yourself, instead the search engine site will do that for you. As a result, the target website will not know about your action.

Let us explore several of these tools.

theharvester

The theharvester tool is an e-mail accounts, username, and hostname/subdomains gathering tool. It collects information from various public sources. As of Version 2.2, the public sources that are supported are as follows:

- Google
- Google profiles
- Bing
- PGP
- LinkedIn
- Yandex
- People123
- Jigsaw
- Shodan

To access theharvester in Kali Linux, you can use the console and type the following command:

```
# theharvester
```

This will display the usage information and example on your screen as shown below.

[img]http://2.bp.blogspot.com/-RiFCI5famSY/U-tfkZFxA1I/AAAAAAAAAKM/gzJXpJ0u8ts/s1600/1.jpg[/img]

If we want to find the e-mail addresses and hostnames for a target domain using Google and limit the result to 100, the following is the appropriate command:

```
# theharvester -d google.com -l 100 -b google
```

The following e-mail addresses and hostnames are found:

[img]http://4.bp.blogspot.com/-6trl0GreNBI/U-tgt_fPK7I/AAAAAAAAAKU/HDdHONEjI9U/s1600/2.jpg[/img]

From the preceding result, we notice that we are able to get several e-mail addresses and hostnames from the Google search engine.

If we want to gather more information, let's say we want to collect the username from the target, we can use linkedin.com to do this. The following is the command for that:

```
# theharvester -d google.com -l 100 -b linkedin
```

The following is the result:

[img]http://1.bp.blogspot.com/-2IF_7FXGRNk/U-thpKSOUWI/AAAAAAAAAkc/WtR3uRohZm0/s1600/3.jpg[/img]

The preceding list of usernames collected from LinkedIn will be useful in a penetration testing step later if we want to do an attack, such as a social engineering attack

Tutorial created by : Mr Tandel :)

ZeZil - October 6, 2014, 6:34 pm

Nice tutorial. You will have your work cut out for you even covering half of the tools on Kali though. Well done anyway and I hope to see more tutorials!

DrDinosaur - October 6, 2014, 7:13 pm

This isn't much of a tutorial. You're only showing the output of two simple commands on one tool.

severos - October 7, 2014, 2:49 am

(Oct 6, 2014 07:13 PM)DrDinosaur Wrote: [\[CITE\]](#) This isn't much of a tutorial. You're only showing the output of two simple commands on one tool.

exactly my thoughts, I was hoping for a more detailed tutorial that explains the principle of how the tool work and what possible modifications for the tool for better results.

herrdeutschland - October 7, 2014, 1:34 pm

very good thanks for this nice informative tutorial ,i hope you will make it even better

kane2026 - November 15, 2014, 5:58 am

theHarvester hardly needs to have a lengthy tutorial. That said, often results used on targets seem arbitrary. You can add -f filename.txt to store output in a file

techme1 - November 18, 2014, 12:27 am

nice tutorial but i am facing one problem i.e domain abc.com now in this domain 100 emails are created but harvester shows only 10 emails only whereas this domain abc.com emails are also can access from gmail.com because domain abc.com server emails are on google clouds

_Silky - November 18, 2014, 1:26 am

(Nov 15, 2014 06:58 AM)kane2026 Wrote: [\[CITE\]](#) theHarvester hardly needs to have a lengthy tutorial. That said, often results used on targets seem arbitrary. You can add -f filename.txt to store output in a file

Really? It can be a lengthy tutorial if OP knew what happens behind the scenes.

And you're not going to find shit with Google (unless of course you search "google.com"), Google has a nice algorithm that blocks that shit, mostly. PGP and Bing is where you'll find the good shit.

techme1 - November 20, 2014, 9:45 pm

(Nov 18, 2014 01:27 AM)techme1 Wrote: [\[CITE\]](#) nice tutorial but i am facing one problem i.e domain abc.com now in this domain 100 emails are created but harvester shows only 10 emails only whereas this domain abc.com emails are also can access from gmail.com because domain abc.com server emails are on google clouds
reply my above post i really need help

imnottellingyou - August 28, 2016, 4:40 am

dose this still work in kali linux? when i try i get no lluck

ryxzen - September 5, 2016, 10:32 am

May i ask if this is still working or is there any update on this TUT? Thanks mate.

Cimex - September 5, 2016, 7:55 pm

(Sep 5, 2016 10:32 AM)ryxzen Wrote: [\[CITE\]](#) May i ask if this is still working or is there any update on this TUT? Thanks mate.

Yes, this is still a working tool.