Information is a weapon, a successful penetration testing and a hacking process need a lot of relevant information that is why, information gathering so called foot printing is the first step of hacking. An intelligent penetration tester use some intelligent tools and techniques to get the right information on a right time, for social engineering (human hacking) you need relevant information about a person. So the point of this little discussion is to realize the importance of information gathering.

After getting some knowledge about information gathering you might be interested to know how to perform it. TheHarvester is a tool for gathering e-mail accounts, user names and hostnames/subdomains from different public sources like search engines and PGP key servers. This tools has designed to help the penetration tester on a earlier stage, it is an effective and simple tool that is very easy to use.

Supported Sources for Information Gathering

- Google - emails,subdomains/hostnames
- Google profiles - Employee names
- Bing search - emails, subdomains/hostnames/virtual hosts
- Pgp servers - emails, subdomains/hostnames
- Linkedin - Employee names
- Exalead - emails,subdomain/hostnames

Related Information Gathering Tutorials

Foot-printing or information gathering is not a new term and we have discussed so many articles with different tools and techniques before for both Windows and Linux (Ubuntu, Backtrack), here is the comprehensive list of articles.

FootPrinting-First Step Of Ethical Hacking
Maltego– Information Gathering Tool Tutorial

What Is TheHarvester

http://www.ehacking.net/2011/08/theharvester--backtrack--5--information.html
If you are using backtrack 5 and other versions of backtrack than you not need to download and run harvester because it is available on backtrack, while for other Linux distributions like ubuntu download and install it. However you can use Theharvester for other Operating system because it need python to run. If you are using Blackbuntu than theharvester available on it.

**TheHarvester Tutorial**

Theharvester is a very easy tool to use just follow the tutorial to get the best result. For backtrack open terminal and locate the directory.

```
root@bt:/pentest/enumeration/theharvester#
```

For other distributions locate the directory. For best result I use the command

```
root@bt:/pentest/enumeration/theharvester# ./theHarvester.py -d google.com -l 500 -b google
```

So here is the result with complete details.

```
www.ehacking.net
```

I hope you are enjoying the reading, now use the wonderful tool by yourself and if you have any question ask via comment box.

Note: If you want to learn more about Linux and Windows based Penetration testing, you might want to subscribe our RSS feed or become our Facebook fan! You will get all the latest updates at both the places.

Related articles

- Book Reveals, Prevents, The Art of Human Hacking (prweb.com)
- BackBox – Linux distribution based website Hacked (thehackernews.com)
- UPDATE: The Social–Engineer Toolkit v2.1! (pentestit.com)

Related post

Backbox
- Ncat– Netcat Windows and Linux Tutorial
• Grendel Scan Web Application Security Scanner
• Social Engineering toolkit Tutorial–Backtrack 5

BackTrack
• Fern wifi Cracker– A Wireless Penetration Testing Tool
• DarkMYSQLi– MYSQL Injection Tool Tutorial
• Tabnapping Tutorial– Social Engineering Toolkit Backtrack 5
• Autopwn Metasploit Backtrack 5– Postgresql Solved

Like liked this.

Add New Comment

Login

Showing 0 comments

Subscribe by email RSS

Reactions

Show more reactions

Which operating system do you like most?

Windows
Linux
MAC

Popular Threads

• How to Find An Email of Facebook Friend | Ethical Hacking–Your Way To The World Of IT Security
  9 comments · 3 days ago

• A History of Hacking [INFOGRAPHIC] | Ethical Hacking–Your Way To The World Of IT Security
  2 comments · 3 days ago

• Complemento Backtrack 5 Toolkit | Ethical Hacking–Your Way To The World Of IT Security
  2 comments · 1 week ago

Recent Comments

• Anonymous– 1337 yes u can send him a link and u wil get there ip sent to your email

Fast Track Hacking–Backtrack5 Tutorial | Ethical Hacking–Your Way To The World Of IT Security · 16 hours ago
Ethical Hacking
for this purpose you need to make some changes on the kernel side, basically backtrack is based...
How To Install Backtrack 5 Dual Boot-Tutorial | Ethical Hacking-Your Way To The World Of IT Security · 2 days ago

revisualize
Is there a way to rename the bootloader to not read "Ubuntu, with Linux 2.6.38" and have it...
How To Install Backtrack 5 Dual Boot-Tutorial | Ethical Hacking-Your Way To The World Of IT Security · 2 days ago

Powered by Disqus