Vulnerability scanners has changed the world of penetration testing, by the right tools and techniques you can test any network and web application for vulnerabilities, there are so many tools available for both network and web application penetration testing. As discussed different tools before this time we will discuss about Skipfish.

Skipfish is an automatic web application security tool, that has been designed to find the vulnerabilities on a web application, find vulnerability on your website before than a hacker find and exploit it.

Skipfish is applicable on cross platform includes Linux, BSD, MAC and windows. It is a power full scanner that crawls targeted website and fully scanned all the pages, it available on backtrack 5, you can get it Application-->backtrack-->Vulnerability assessment--> web application assessment--> web vulnerability scanner--> skipfish

**Key Features**

- **High speed**: pure C code, highly optimized HTTP handling, minimal CPU footprint – easily achieving 2000 requests per second with responsive targets.
- **Ease of use**: heuristics to support a variety of quirky web frameworks and mixed-technology sites, with automatic learning capabilities, on-the-fly wordlist creation, and form autocompletion.
- **Cutting-edge security logic**: high quality, low false positive, differential security checks, capable of spotting a range of subtle flaws, including blind injection vectors

**Download**

Skipfish Tutorial

**Ethical Hacking Training**
2011 Ethical Hacking course Includes cert, and hacking software
InfoSecInstitute.com/Ethical_Hacking

If you are using backtrack5 than you can easily use skipfish while if you are using some other distro of Linux and other operating system than follow the steps below:
Goto terminal and install skipfish dependencies:

```
ehacking@ubuntu:~ $ sudo apt-get install libidn11-dev
ehacking@ubuntu:~ $ sudo apt-get list
```

http://www.ehacking.net/2011/06/skipfish-backtrack5-tutorial.html
ehacking@ubuntu:~ $ sudo apt-get install libssl-dev zlib1g-dev

After all the next step is to install skipfish, follow the steps. Download the skipfish link has been shared above.

   ehacking@ubuntu:~ $ sha1sum skipfish-1.84b.tgz

Match the checksum with the one provided on the website, than right click on downloaded file extract it, than on the terminal go to the extracted file.

   ehacking@ubuntu:~ $ cd skipfish-1.84b
   ehacking@ubuntu:~ $ skipfish-1.84b $ make
   ehacking@ubuntu:~ $ skipfish-1.84b $ cp dictionaries/complete.wl skipfish.wl
   ehacking@ubuntu:~ $ skipfish-1.84b $ mkdir results

Done now its time to start a attack on web application using skipfish, use this command

   ./skipfish -o /pentest/web/skipfish/b -W dictionaries/complete.wl
http://www.yourweb.com

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

Related post

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

Backtrack5
- DarkMYSQLi– MYSQL Injection Tool Tutorial
- Tabnapping Tutorial– Social Engineering Toolkit Backtrack 5
- Autopwn Metasploit Backtrack 5– Postgresql Solved
- Complemento Backtrack 5 Toolkit
Skipfish - Backtrack5 Tutorial | Ethical Hacking - Your Way To The World Of IT Security

Add New Comment

Showing 0 comments

Subscribe by email  RSS

Reactions

Show more reactions

Which operating system do you like most?

- Windows
- Linux
- MAC

Vote

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

Powered by Disqus

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

http://www.ehacking.net/2011/06/skipfish-backtrack5-tutorial.html
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