þÿ

/////////////////////////////////////

Reconnaissance

We want to begin a pen test by reviewing the target s website. We may actually use a tool called HTT rack to make a page-by-page copy of the website. HTT rack is a free program that creates an identical, off-line copy of the target website. The copied website will include all the pages, links, pictures, and code from the original website; however, it will reside on your local computer. Using a website copying tool like HTT rack allows us to explore and thoroughly mine the website off-line without having to spend additional time traipsing around on the company s web server.

To install HTTrack open the console and type:

sudo apt-get install httrack

Once it is installed, begin HTTrack by typing httrack in the console:

Backtrack Tutorials httrack startNext, name your project whatever you want. Select a path where you want to save the off-line copy. I just left it as default (/home/websites). Just hit enter to leave it as such. Then enter the site you want to copy. I am using my own site since I will not get in trouble for copying it. (Please do not copy my site & Thanks!).

Backtrack Tutorials httrack project namePick an action you want. If you want to copy the site, press 1 then enter. HTTrack has a few options for you to pick from including a proxy to help cover your tracks. I am just using the basics for demonstration. I recommend you use a proxy when doing a real pen test.

backtrack tutorials | httrack downloadAfter HTTrack finishes, you will have a complete off-line copy of the target site which you can review for information.
The Harvester

The Harvester is a simple Python script written by Christian Martorella at Edge Security. This tool allows us to quickly catalog both e-mail addresses and subdomains that are directly related to the target system.

The Harvester can be used to search Google, and Bing for e-mails, hosts, and subdomains. It can also search LinkedIn for user names.Often times you will find an email address, which could double as a login or user-name.

To use theHarvester first type in your console:

root@bt:~# cd /pentest/enumeration/theharvester

root@bt:~# ./theHarvester.py -d backtracktutorials.com -l 10 -b google.com

 d is used to specify the target domain.
A lowercase l (that s L not a 1 2) is used to limit the number of results returned to us. In this
case, the tool was instructed to return only 10 results. The b is used to specify what public repository we
want to search. We can choose among Google, Bing, PGP, or LinkedIn.
Backtrack Tutorials: theHarvester Scan

I scanned my own domain and didn t find anything & yet!