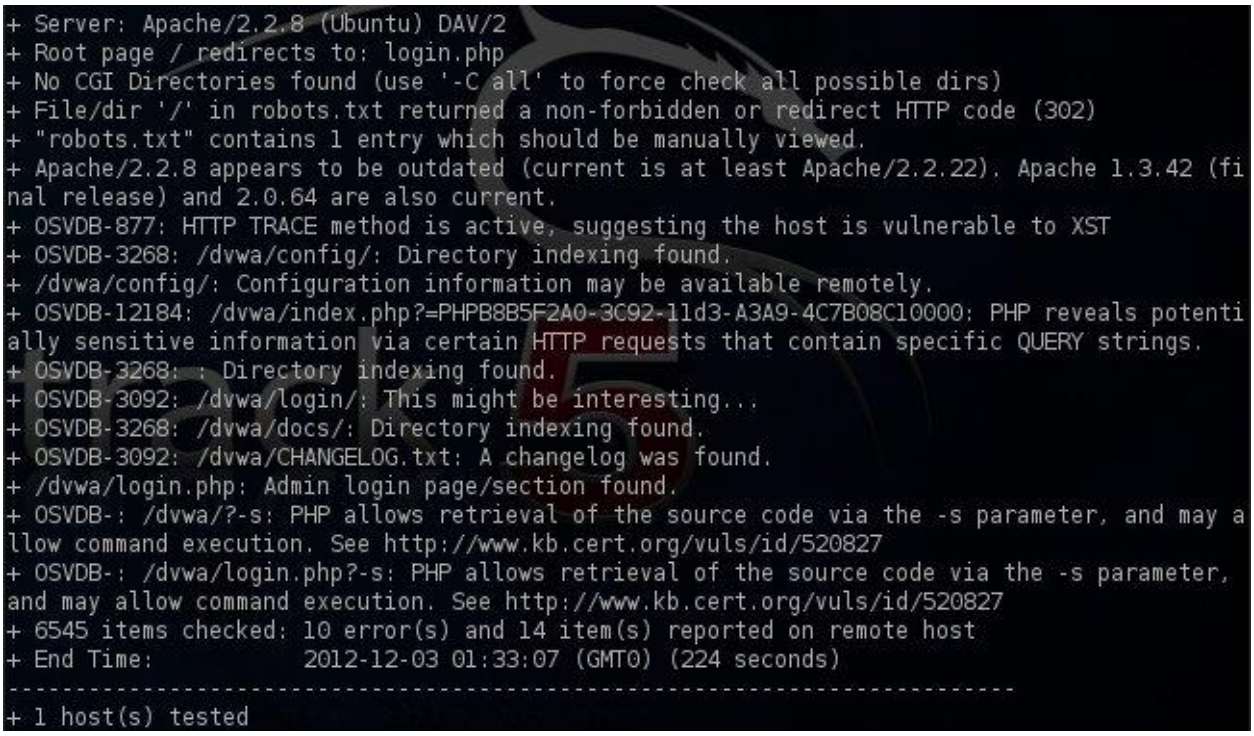
Module 2: Footprinting Lab Introduction

Footprinting: this is a technique for gathering information on computer systems and the entities they belong to.

Google Hacking

- **filetype: type** -searches for only files of a specific type. Example: filetype: doc would
- return Microsoft Word documents
- **intitle: string** -searches for pages that contain the string in the title. Example: intitle: login
- would return results with the word login in the title
- **inurl: string** -displays pages with the string in the URL. Example: inurl:passwd would
- show all pages with the word passwd in the URL.
- **site: domain** -displays pages for a specific website or domain. Can be combined with other
- search terms. Example: site:microsoft.com passwds would show all pages with the text
- passwds in the website.

Nikto


+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (fi
nal release) and 2.0.64 are also current.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /dvwa/config/: Directory indexing found.
+ /dvwa/config/: Configuration information may be available remotely.
+ OSVDB-12184: /dvwa/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potenti
ally sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-3092: /dvwa/login/: This might be interesting...
+ OSVDB-3268: /dvwa/docs/: Directory indexing found.
+ OSVDB-3092: /dvwa/CHANGELOG.txt: A changelog was found.
+ /dvwa/login.php: Admin login page/section found.
+ OSVDB-: /dvwa/?-s: PHP allows retrieval of the source code via the -s parameter, and may a
llow command execution. See http://www.kb.cert.org/vuls/id/520827
+ OSVDB-: /dvwa/login.php?-s: PHP allows retrieval of the source code via the -s parameter,
and may allow command execution. See http://www.kb.cert.org/vuls/id/520827
+ 6545 items checked: 10 error(s) and 14 item(s) reported on remote host
+ End Time: 2012-12-03 01:33:07 (GMT0) (224 seconds)
+ 1 host(s) tested

theHarvester