

Forum:[Hack Forums](#)

Thread: [Hacking Tools | Darknet - The Darkside](#)

iamVIP - June 16, 2010, 4:01 am

Samurai Web Testing Framework v0.8 Released – Pen Testing Security LiveCD

The Samurai Web Testing Framework is a live linux environment that has been pre-configured to function as a web pen-testing environment. The CD contains the best of the open source and free tools that focus on testing and attacking websites.

It's been quite a while since the latest fairly major update of SamuraiWTF (around a year ago).

This is quite a major release with the integration of metasploit, target applications and tons of tool updates. It is now DVD sized as it has out grown the CD release.

Starting with reconnaissance, we have included tools such as the Fierce domain scanner and Maltego. For mapping, we have included tools such WebScarab and ratproxy. We then chose tools for discovery. These would include w3af and burp. For exploitation, the final stage, we included BeEF, AJAXShell and much more. This CD also includes a pre-configured wiki, set up to be the central information store during your pen-test.

The Samurai project team is happy to announce the release of a development version of the Samurai Web Testing Framework. This release is currently a fully functional linux environment that has a number of the tools pre-installed.

You can download SamuraiWTF v0.8 here:

Quote:<http://depositfiles.com/files/2iscwf71n>

Knock v1.3b – Subdomain Enumeration/Brute-Forcing Tool

Knock is a python script designed to enumerate sub-domains on a target domain through a wordlist.

Usage

```
$ python knock.py [ url ] [ wordlist ]
```

You can view a demo of the tool enumerating Facebook sub-domains on Youtube here:

Facebook and Knock v.1.2

Knock works on Linux, Windows and MAC OSX with a python version 2.6.x (or minor).

Requirements

- Python version 2.6.x or minor.

- A wordlist

You can download Knock v1.3b here:

Quote:<http://depositfiles.com/files/xf5hm3g9x>

WhatWeb – Next Gen Web Scanner – Identify CMS (Content Management System)

Identify content management systems (CMS), blogging platforms, stats/analytics packages, javascript libraries, servers and more. When you visit a website in your browser the transaction includes many unseen hints about how the webserver is set up and what software is delivering the webpage. Some of these hints are obvious, eg. “Powered by XYZ” and others are more subtle. WhatWeb recognises these hints and reports what it finds.

WhatWeb has over 80 plugins and needs community support to develop more. Plugins can identify systems with obvious signs removed by looking for subtle clues. For example, a WordPress site might remove the tag but the WordPress plugin also looks for “wp-content” which is less easy to disguise. Plugins are flexible and can return any datatype, for example plugins can return version numbers, email addresses, account ID’s and more.

There are both passive and aggressive plugins, passive plugins use information on the page, in cookies and in the URL to identify the system. A passive request is as light weight as a simple GET / HTTP/1.1 request. Aggressive plugins guess URLs and request more files. Plugins are easy to write, you don’t need to know ruby to make them.

Aggressive plugins can identify versions of Joomla, phpBB, etc by making extra requests to the webserver.

Log Output

There are currently 3 types of log output. They are:

- Brief logging
- Full logging
- XML logging

Plugins

There are over 90 plugins as of version 0.4.3. Plugins are easy to make. Matches are made with regular expressions, Google Hack Database queries, and custom ruby code. For now the probability means maybe (25%), probably (75%) and certain (100%).

You can download WhatWeb 0.4.3 here:

Quote:<http://depositfiles.com/files/ie0yv1ugd>

Bruter v1.0 Final Released – Parallel Network Login Brute Forcing Tool

Bruter is a parallel network login brute-forcer on Win32. This tool is intended to demonstrate the importance of choosing strong passwords. The goal of Bruter is to support a variety of services that allow remote authentication.

It currently supports following services:

- FTP
- HTTP (Basic)
- HTTP (Form)
- IMAP

MSSQL
MySQL
POP3
SMB-NT
SMTP
SNMP
SSH2
Telnet
VNC

Recent Changes

Re-licensed to new-BSD license
Added proxy support (CONNECT, SOCKS4, SOCKS5)
Allowed more delimiter in combo file
Added password length filtered in combo and dictionary mode
Fixed miscellaneous bugs
Updated openssl library to 0.9.8n

You can download Bruter v1.0 Final here:

Quote: <http://depositfiles.com/files/mu5zew5cs>

FOCA – Network Infrastructure Mapping Tool

FOCA 2 has a new algorithm which tries to discover as much info related to network infrastructure as possible. In this alpha version FOCA will add to the figured out network-map, all servers than can be found using a recursive algorithm searching in Google, BING, Reverse IP in BING, Well-known servers and DNS records, using an internal PTR-Scaning, etc

To configure this algorithm you can use the new DNS Search panel and the info extracted will be showed up in three panels:

Domains
IP addresses
PC/Servers

ChangeLog 2.0.1:

Fix error searching EXIF information
Fix error in DNS Transfer Zone requests

ChangeLog 2.0:

DNS enumeration added using subdomains Web Search, zone transfer, dictionary and bing IP search.

Added panels Domains & IP
Documents grouped by document type
Used ListView groups
Better Network Map representation
Bing only search supported filetype documents
Fix error analysing metadata

Download FOCA 3.5.9 here:

Quote:<http://depositfiles.com/files/y8v8c0vgp>

-mothered- - June 16, 2010, 4:46 am

Well I truly have to thank you for this. The main tool that I'm after, Is the Bruter tool. This has definitely captured my Interest, hence shall download straight after this post.

Much appreciated mate.

g4ia - August 18, 2010, 9:25 am

Hey I dled those things those are faked shit1 it installed something called chameleon
it sucks it's malware!

sunilbabu1252 - August 18, 2010, 12:10 pm

it is better to maintain more photos in your tutorial.