



SHADOWCIRCLE 2.0 (blue lagoon) SPECIFICATIONS

specifications

WintermeW

wintermew(at)digi-nation(dot)com

Keywords: shadowcircle, live-cd, pentest, 2.0, specifications

Contents

1	Introduction	2
2	Release Goals	2
3	Main Changes	3
4	Main Packages Versioning	3
5	Roadmap	3
5.1	Milestone 1: 15/01/2010	3
5.2	Milestone 2: 15/02/2010	4
5.3	Milestone 3: 15/03/2010	4
5.4	Milestone 4: 30/04/2010	4
6	Final Words	4

1 Introduction

This document aims to shortly present the second iteration of the shadowcircle pentesting distribution, in order to give people a project visibility over the next few months, and give them the opportunity to actively interact with its development.

2 Release Goals

Probably the most important thing to retain about this upcoming release is that shadowcircle will stop using backtrack as its base system and then grow by itself.

Shadowcircle 2 will also finally see the removal of every single piece of non FOS software, which is a very good thing. To achieve this goal we had to create a Maltego replacement named 'zer0farm' (<http://www.zer0farm.org>, website not created yet), which is being developed at this time.

Our other focus for this version will be the online documentation and more important, the local contextual help / documentation. Finally, we will also improve performance and reduce the memory footprint, while still looking for and integrating the cutting-edge security tools.

3 Main Changes

- Forking from ubuntu Lucid Lynx, benefits of LTS.
- XFCE desktop 4.6
- Removing of Maltego, replacement by zer0farm (1)
- Removing of Dirbuster, replacement by Dirbuster-ng (1)
- Adding of a local knowledge-base tool written in C/GTK+ (1)
- Update and integration of all the tools previously available in Release 1.0
- Integration of an usb image creator w/ GUI
- Integration of ipmorph, if a refactored QT-less version is ever released.
- Integration of the most important firecat extentions.

(1) These tools are currently being developed as side projects, and we need contributors for them. If you are interested in being part of these projects, write a mail to [sc\(at\)digi-nation\(dot\)com](mailto:sc(at)digi-nation(dot)com).

4 Main Packages Versioning

- Kernel 2.6.31
- Xorg 7.5
- xfce 4.6
- firefox 3.6
- python 2.6.3
- php 5.2.10
- Metasploit 3.4 (1)
- nmap 5.10
- wireshark 1.3.x
- inguma 0.0.7 (remains as is)
- Fasttrack 4.0
- OpenVAS Server 3.0
- OpenVAS Client 3.0

(1) Considering the current development speed of metasploit framework, this revision is subject to changes

5 Roadmap

This section defines the most important steps of the project.

Also please take into account that the deadlines are purely indicative and are mostly subject to changes, specially concerning the beta releases.

5.1 Milestone 1: 15/01/2010

- preparing of the lucid lynx base system, kernel customization (wlan reinject, network stacks customization..).
- Integration of apt packages already in the shadowcircle 1.0 packages base.
- graphical work and integration.

5.2 Milestone 2: 15/02/2010

- pentest tools updates and integration.
- First Beta Release.

5.3 Milestone 3: 15/03/2010

- fixing of critical bugs from beta 1 feedbacks.
- dirbuster-ng integration.
- knowledge-base tool integration.
- Second Beta Release.

5.4 Milestone 4: 30/04/2010

- extensive testing, fixing of remaining critical bugs.
- zer0farm integration.
- removing of JRE.
- Final Release.

6 Final Words

Developing this second version of shadowcircle will be yet another great adventure that we want to share with all the people who have IT security interests. There's a lot to do but we truly think that the result can be worth the pain.

The shadowcircle core team.