

Building a Portable Security Environment with

bin pack

Garrett Gee | ToorCon 12



Who am I?

- Penetration Tester
- Researcher / Developer
 - Portable Linux Auditing CD (PLAC)
 - BinPack
- Entrepreneur
 - Infosec Events
 - West Coast Hackers

- <http://GarrettGee.com>



Intro – Portable Environments

- Full OS Environment
 - Linux: Knoppix, Backtrack, Pentoo, etc
 - Windows: WinPE, BartPE
- Full Application Suites
 - Linux: None
 - Windows: LiberKey
- Application Collections
 - Linux: PAFL
 - Windows: PortableApps, winPenPack, DemocraKey, Lupo PenSuite



Use Cases

- Team / Group Settings
 - Penetration Testing Teams
 - Training Classes
- Rapid Deployment Scenarios
 - Repair Toolkit
- Finding / Testing New Tools



Filling the Windows Gap

- Version 1 – Application Collection
 - 30 MB in 2007
 - 900 MB in 2009
- Version 2 – Full Application Suite



Features

- Modular
 - Easy Install / Upgrade / Remove
- Portable
 - Dynamic GUI Menu
 - Dynamic Shell Path
- Rapid Deployment
 - Pre-Defined Package Lists
- Packages



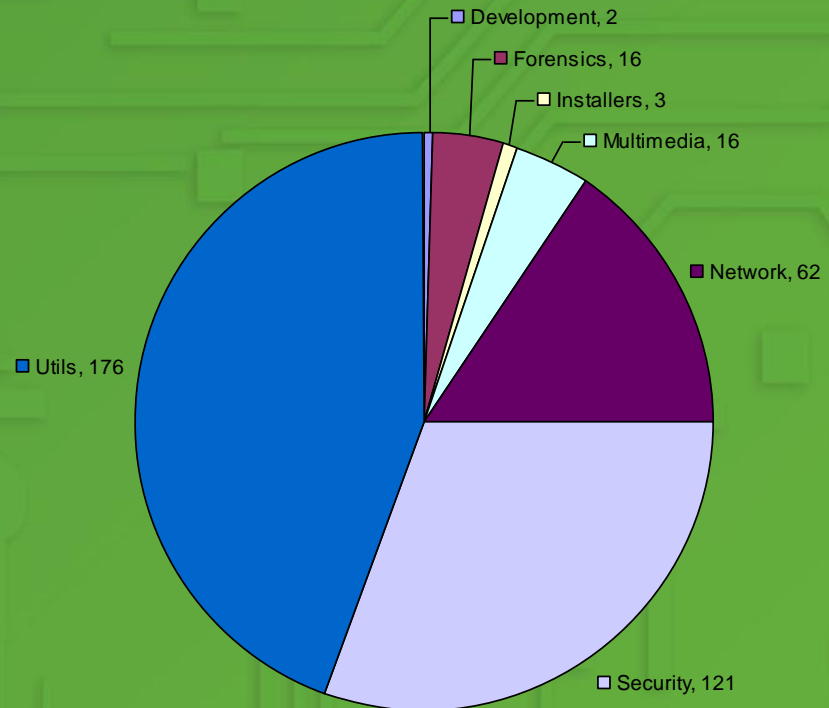
Packages and Lists

- 7 Categories / 396 Packages

- Development
- Forensics
- Installers
- Multimedia
- Network
- Security
- Utils

- 9 Package Lists

- SecTools100
- Best of Series



DEMO

The screenshot shows the BinPack application window. The title bar reads "BinPack" and the menu bar contains "File" and "Help". Below the menu bar is a toolbar with buttons for "Upgrades and Not Installed", "D", "F", "I", "M", "N", "S", "U", and a search box. The main area is divided into three sections:

- Package Lists Available:** A list of package files with checkboxes, including core-suite.txt, foundstone-vuln-scanners.txt, multimedia-bestof.txt, network-bestof.txt, nirsoft-all.txt, putty-suite.txt, sectools100.txt, sectools125.txt, security-bestof.txt, sysinternals-all.txt, sysinternals-core.txt, sysinternals-pstools.txt, and utils-bestof.txt.
- Package List:** A table with columns for Package, Category, and Sub Category. The "w3af gui" package is selected and highlighted.
- Package Details:** A text area showing information for the selected package, including Name, Homepage, Description, Version, Build, Release Date, Zipped Size, Extracted Size, Category, and Sub-Category.

Buttons at the bottom left include "Save Installed as List", "Save Selected as List", "Install Package(s)", and "Remove Package(s)".

Package	Category	Sub Category
<input checked="" type="checkbox"/> w3af gui	Security	Web Hacking
<input checked="" type="checkbox"/> wapiti	Security	Web Hacking
<input checked="" type="checkbox"/> webscarab	Security	Web Hacking
<input checked="" type="checkbox"/> websecurify	Security	Web Hacking
<input checked="" type="checkbox"/> wfuzz	Security	Web Hacking
<input type="checkbox"/> wikto	Security	Web Hacking
<input type="checkbox"/> WinDump	Security	Network Sniffer
<input type="checkbox"/> WinFingerprint	Security	Windows Enumeration
<input checked="" type="checkbox"/> winfo	Security	Windows Enumeration
<input type="checkbox"/> WinInterrogate	Security	Windows Enumeration
<input type="checkbox"/> wipersec	Security	Web Hacking

Name: w3af gui
Homepage:
Description: w3af

Version: 1.0.rc3
Build: 1
Release Date: 2010-07-12 18:29:55
Zipped Size: 91008248
Extracted Size: 243290813

Category: Security
Sub-Category: Web Hacking



What's Next?

- More Package Support
 - Development Tools and Forensics
- Full OS Environment
- Mac OSX



Other Talking Points

- System Design
- Custom Repositories



Supporting Information

- Project Homepage
 - <http://westcoasthackers.net/projects/binpack/>
- Mailing List
 - <http://groups.google.com/group/westcoasthackers-binpack>
- Direct Contact
 - <http://westcoasthackers.net/contact/>
- Blog
 - <http://westcoasthackers.net/blog/>

