Building a Portable Security Environment with

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

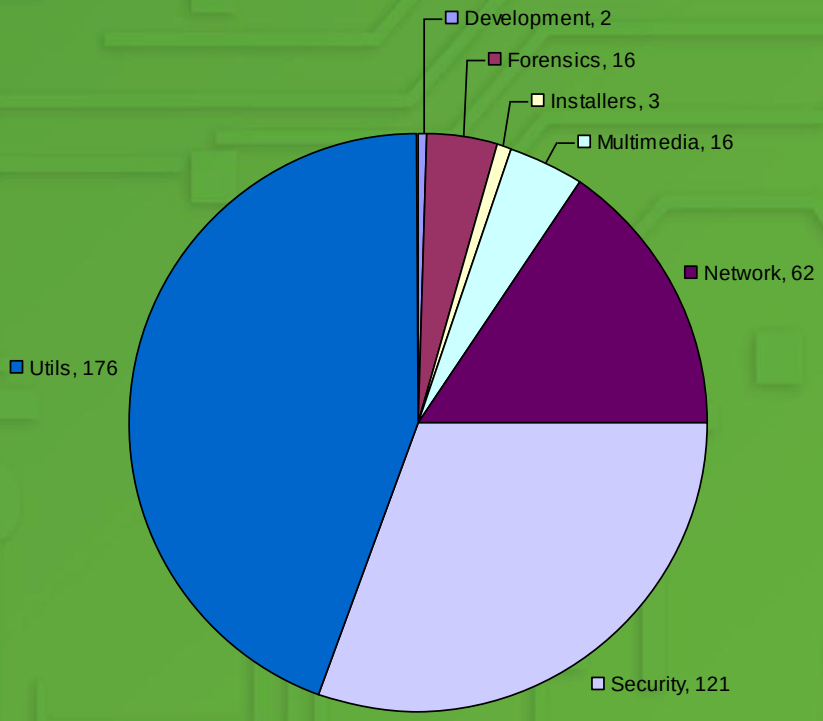
- Version 1 – Application Collection
  - 30 MB in 2007
  - 900 MB in 2009
- Version 2 – Full Application Suite

Features

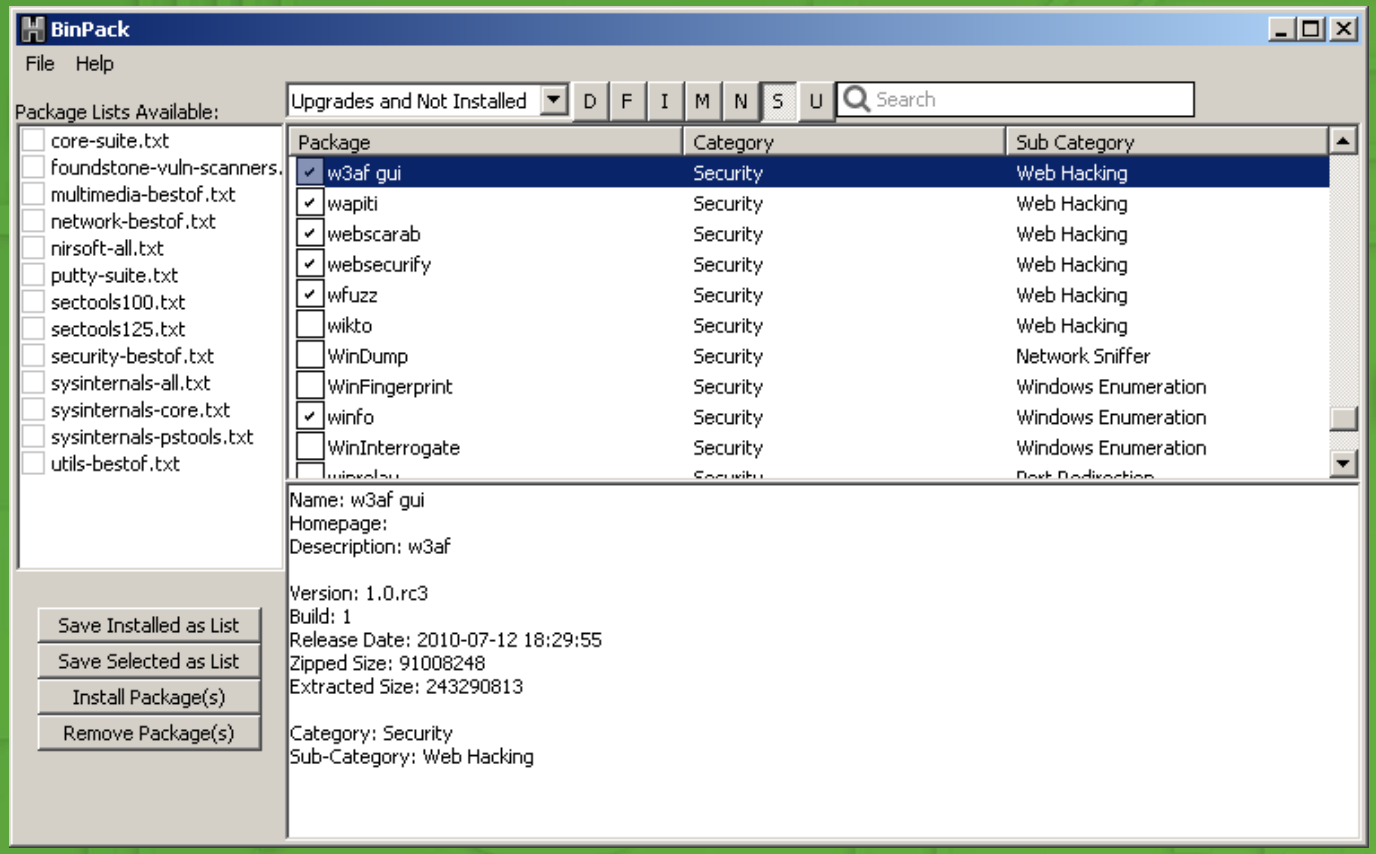
- Modular
  - Easy Install / Upgrade / Remove
- Portable
  - Dynamic GUI Menu
  - Dynamic Shell Path
- Rapid Deployment
  - Pre-Defined Package Lists
- Packages

Packages and Lists

- 7 Categories / 396 Packages
  - Development
  - Forensics
  - Installers
  - Multimedia
  - Network
  - Security
  - Utils
- 9 Package Lists
  - SecTools100
  - Best of Series



DEMO


BinPack
File
Help
Package Lists Available:
core-suite.txt
foundstone-vuln-scanners.
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
utils-bestof.txt
Upgrades and Not Installed
D
F
I
M
N
S
U
Search
Package
Category
Sub Category
w3af gui
Security
Web Hacking
wapiti
Security
Web Hacking
webscarab
Security
Web Hacking
websecurify
Security
Web Hacking
wfuzz
Security
Web Hacking
wikto
Security
Web Hacking
WinDump
Security
Network Sniffer
WinFingerprint
Security
Windows Enumeration
winfo
Security
Windows Enumeration
WinInterrogate
Security
Windows Enumeration
Name: w3af gui
Homepage:
Desecription: 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
Save Installed as List
Save Selected as List
Install Package(s)
Remove Package(s)

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/