

Weaponry 2.0

Penetration Testing, Software as an Appliance
by Petko D Petkov (pdp)
pdp@corsaire.com



uri:about:www.pdp.io

- Principle Consultant, Corsaire
- GNUCITIZEN, Hakiri, HoH
- HRP, Book Author, Speaker
- Hacking Web 2.0, Client-side Security
- QuickTime, SecondLife, CITRIX, Acrobat, Gmail, Flash, etc...



What is this all about?

- This talk is **NOT** about:
 - selling products or services
 - showing how things should be done



What is this all about?

- This talk **IS** all about:
 - starting a dialog
 - enabling communication
 - facilitating communities

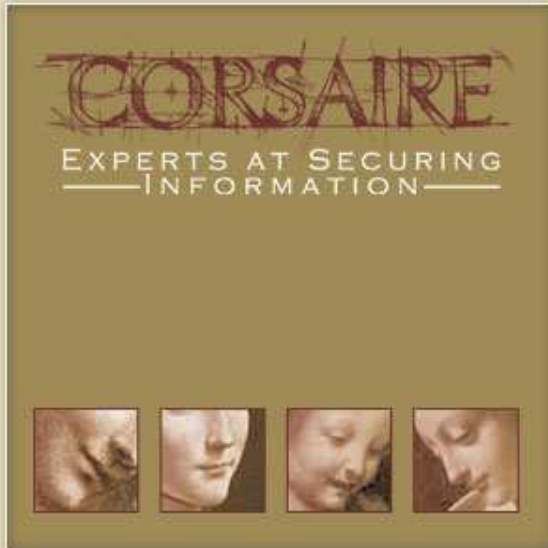


SIDE STORY

??????

CORSAIRE





Penetration Testing

Penetration Testing Today, Common Annoyances,
Possible Solutions



Penetration Testing Today

- Types of Penetration Tests

- WhiteBox
- BlackBox
- GrayBox
- Regular
- Once-off
- Onsite
- Off-site
- Etc...

Penetration Testing Today

- Penetration Testing Practices
 - Network Infrastructure
 - Wireless Infrastructure
 - Telephony
 - Other Radio
 - VoIP
 - Web Application
 - Etc...

Penetration Testing Today

■ The Toolkit

- Hardware: WiFi, Bluetooth, RFID, etc...
- Networking: Tcpdump, Wireshark, Yersinia, etc...
- Scanners: Nmap, Amap, Nikto, iWar, etc...
- Vulnerability Assessment: Nessus, OpenVas, Nmap, etc...
- Exploits: *[disperse repositories]*
- Frameworks: Metasploit, Netifera, Inguma, FastTrack, etc...
- Environments: BackTrack, Operator, PHLACK, Auditor, etc...
- Others: *[personal collections of tools]*

Common Annoyances

- In Penetration Testing

- It becomes increasingly more complicated
- It takes more and more effort regardless how much we automate
- It cannot be generalised because of the introduced complexities
- Etc...



Common Annoyances

■ In Tools

- Most of them were written to solve simple problems
- No interoperation or data sharing
- Most of them break for no apparent reason
- Most of them require significant understanding of how they work
- Most of them are not easy to configure
- Most of them try to lock you into their own world
- Etc...

Common Annoyances

- In Penetration Testing Workflows
 - We constantly loose valuable data
 - Even simple operations such as portscanning are not simple at all
 - Etc...



Possible Solutions

- Don't bother at all
 - We can just ignore our frustrations



Possible Solutions

- Turn everything into a Framework
 - Come up with the rules, setup the scene and ask everybody to play nice



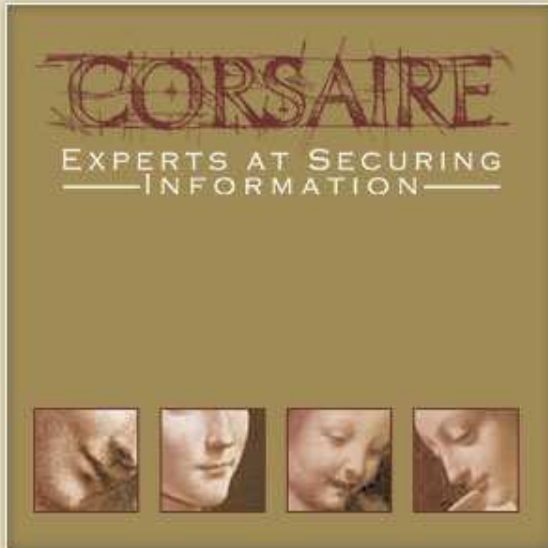
Possible Solutions

- Change the Lens
 - Come up with something new and see what the community says

SIDE STORY JERIKO

CORSAIRE





Software as Appliance

What is Software as Appliance, Experiments with QEMU, Experiments with EC2



What is Software as Appliance

- Basic Definition

- It is a software application combined with just enough operating system
- It is a software system which runs in optimal mode
- It can be virtualized
- It can be a livecd



What is Software as Appliance

- What does it Mean?
 - It means simplified deployment
 - It means improved isolation
 - It means self-contained



What is Software as Appliance

- What does it do to Penetration Testing?
 - If you have used Backtrack before you already know how it feels



Experiments with QEMU

- What is QEMU
 - It is a processor emulator
 - It is a hosted virtual machine monitor
 - It can run virtually on any PC
 - It can run even when the user has limited rights
 - PC on USB concept is real

Experiments with QEMU

- Penetration Testing Environment Orchestration
 - QEMU raw image
 - Ubuntu JeOS
 - Jeriko
 - Specialized Security Toolkit
 - Python
 - XMLRPC
 - SSH

Experiments with QEMU

■ Results

- It is simple to use and execute
- It is convenient
- It works at micro level
- It works at macro level



Experiments with EC2

- What is EC2?
 - It is Amazon's commercial web service
 - It allows scalable deployment
 - It bundles numerous nice technologies



Experiments with EC2

Penetration Testing Environment Orchestration

- Any EC2 Image
- Jeriko
- Specialized Security Toolkit
- Python
- XMLRPC
- SSH

Experiments with EC2

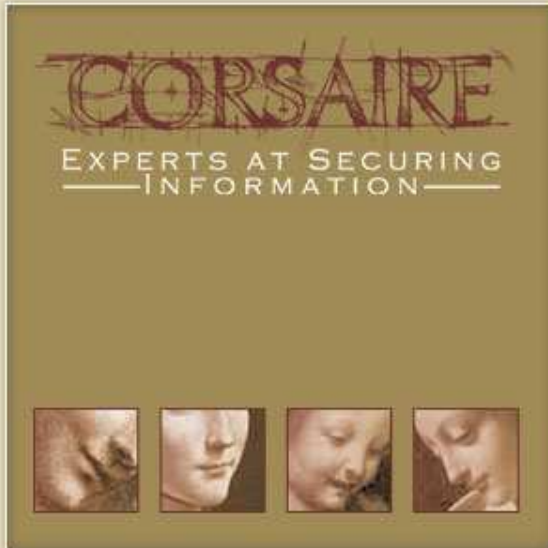
■ Results

- It is simple to use and execute
- It is convenient
- It works on demand
- It works at micro level
- It works at macro level
- It is GEO aware

SIDE STORY TALES OF A SCAN

CORSAIRE



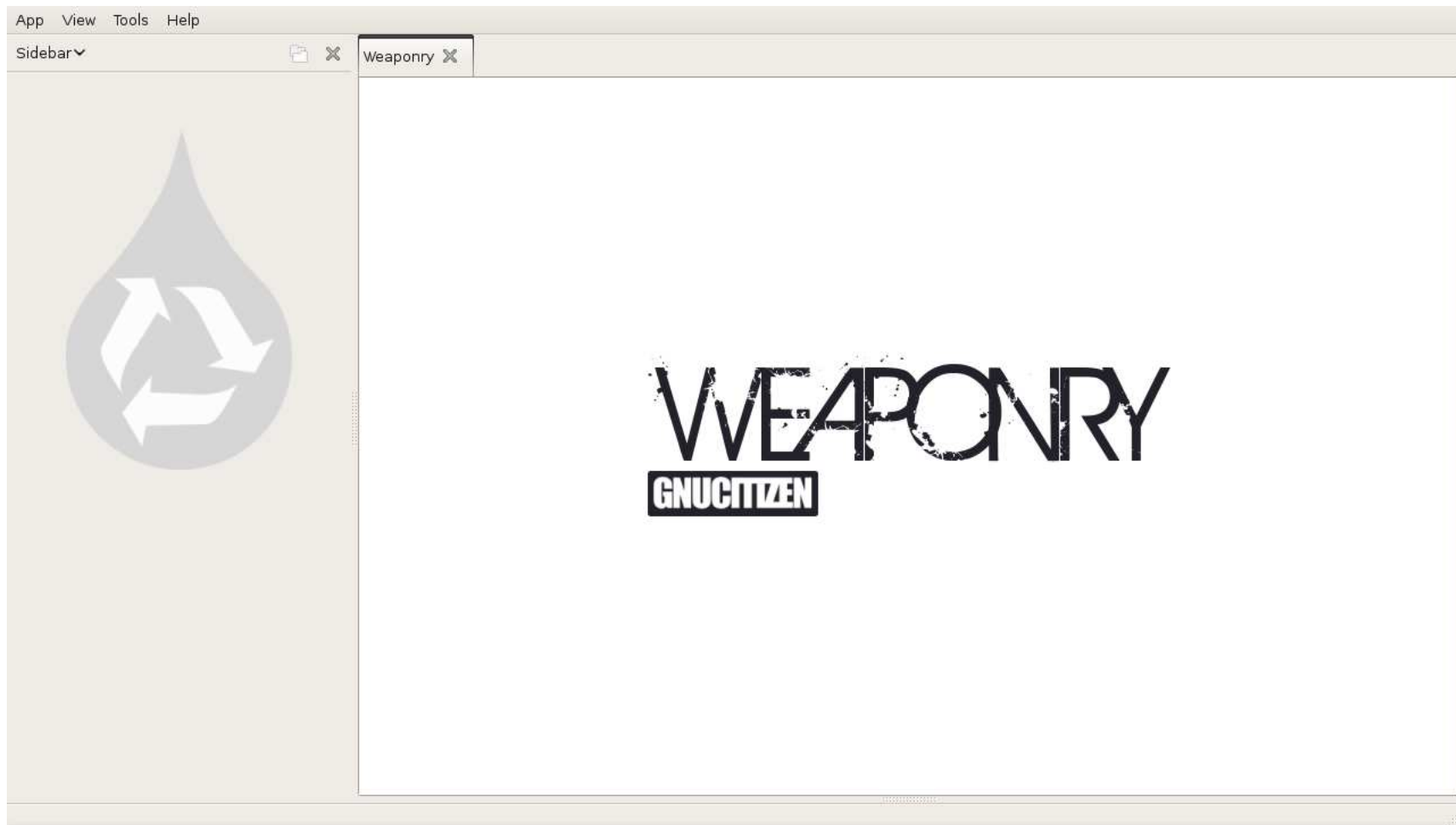


Weaponry

What is Weaponry, System Design, What is Next



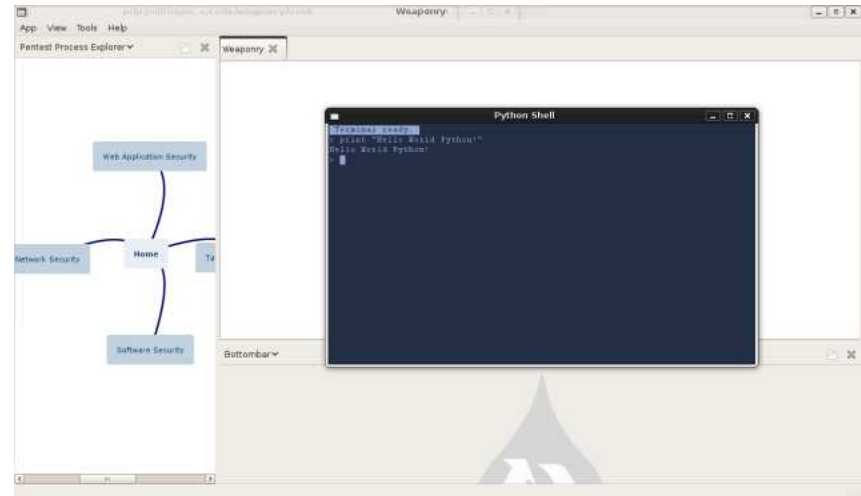
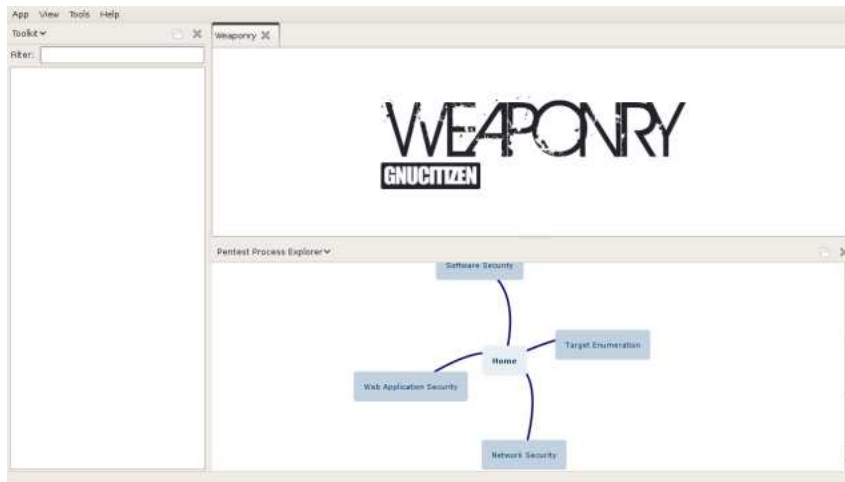
What is Weaponry



CORSAIRE



What is Weaponry



CORSAIRE

What is Weaponry

The screenshot displays the Weaponry application interface with several windows open:

- Weaponry**: The main application window with a sidebar menu containing:
 - Configuration Manager: Manager for the Preferences Subsystem
 - Default Passwords: Default Passwords Index
 - Error Console: System Error Console
 - Extension Manager: Manager for Weaponry Addons
 - Pentest Map: Pentester Mindmap
 - Python Shell: Interface to the standard Python shell
- Default Passwords Explorer**: A table listing default passwords for various vendors.

Vendor	Username	Password
3Com	admin	syn
3Com	read	syn
3Com	write	syn
3Com	monitor	mo
- Add-ons**: A window showing available add-ons: Extensions, Themes, Languages, and Plugins.
- Pentest Map**: A mind map diagram with a central node 'Home' and branches for 'Software Security', 'Network Security', and 'Gathering'.
- Python Shell**: A terminal window displaying a list of Python modules and their attributes, including 'netlink', 'socket', 'ssl', and 'sys'.



System Design

■ Use

- To be used as an environment not a toolkit
- To be used to ease complexity
- To be used as a zoomable lens
- To aggregate and analyze data
- To facilitate the process rather than obstruct it
- To guide
- To be free



System Design

- Zoomable Lens
 - It is almost like having different layers of view
 - We can zoom in and zoom out of complexity



System Design

- The Architecture
 - It is open source
 - It is based on XULRunner
 - It makes use of Python
 - It is extremely light and well designed
 - Writing extensions for the system is a breeze



What is Next

- In Terms of Weaponry
 - It is an experiment
 - It is an ongoing project

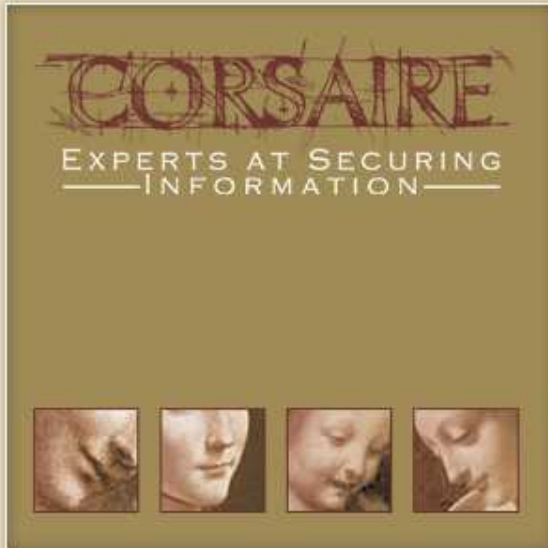
What is Next

- In Terms of Penetration Testing
 - We are building some demo systems
 - We are still experimenting



What is Next

- In Terms of the Idea
 - Urging the community to join the conversation



Conclusion

and thank you for attending

