Build your own Open Source Penetration Testing Lab

FSec - FOI Security Symposium
22.9.2011 and 23.9.2011 – Varaždin

Phillip Bailey

www.bailey.st

phillip@bailey.st

Penetration testing
and
Security Assessment

Why do we need a pen test lab?

Legal issues

Why do we need a pen test lab?

Legal issues

Hack black boxes in a real life scenario

Why do we need a pen test lab?

Legal issues

Hack black boxes in a real life scenario

Security (Intentional or not, Arp poison, DoS, etc-etc, attacks on the Corporate, University, Hackerspace, network.)

Why do we need it Virtual and Open Source?

$$ Hardware cost savings $$

Why do we need it Virtual and Open Source?

$$ Hardware cost savings $$

Easy to maintain, replicate and redeploy.

Why do we need it Virtual and Open Source?

$$ Hardware cost savings $$

Easy to maintain, replicate and redeploy.

Modify, customize and share.

Who When Where

Security consultants

Ethical hacking University courses

Security tools developers

Corporate Information Security departments

Hackerspaces

Capture the flag competitions

Home

A bit of structure

Hardware

Virtualization platform

Methodologies and docs

Vulnerable machines and weak applications

PenTest tools and Linux distros

Network Security Monitoring tools

Hardware

Hardware

Minimal Configuration

Server/Workstation
- 2GB RAM
- 320 GB Disk Drive

Network Switch

Laptops

Large Deployment

Server (some cores)
- 8 GB RAM
- 2 TB Disk Drive

Network Switch (managed)

Router (VPN Capable)

WiFi AP

Dedicate NSM/IDS Server

Laptops

Virtualization platforms

Methodologies and docs

OSSTMM - Open Source Security Testing Methodology Manual www.isecom.org

ISSAF penetration testing framework www.oissg.org

OWASP Testing Guide www.owasp.org

Keep your own Wiki!!!

It's all about boxes

White-box testing

VS

Black-box testing

Vulnerable machines and weak applications (WebApps)

OWASP Hackademic Challenges

Realistic scenarios with known vulnerabilities in a safe, controllable environment.

UltimateLAMP

WordPress, MediaWiki, TikiWiki, Gallery, Moodle, PHPWebSite, Joomla, eGroupWare, Drupal, Php Bulletin Board, Sugar CRM WebCalendar, Dot project, PhpAdsNew, OsCommerce, ZenCart, PhphMyAdmin, Webmin,Mutillidae 1.5 OWASP top 10

Vulnerable machines and weak applications (Sys&Serv)

Kioptrix Level 1
Remote OpenSSL exploit

De-ICE PenTest LiveCDs
Weak credential and misconfigured services

Metasploitable
Tomcat 5.5 (with weak credentials), distcc, and an older mysql.

PenTest tools and Linux distros

Tools

Nmap

Metasploit

Social Engineering Toolkit

Arachni

W3af

Sqlninja

Ncrack

WATOBO

Sqlmap

Linux Distributions

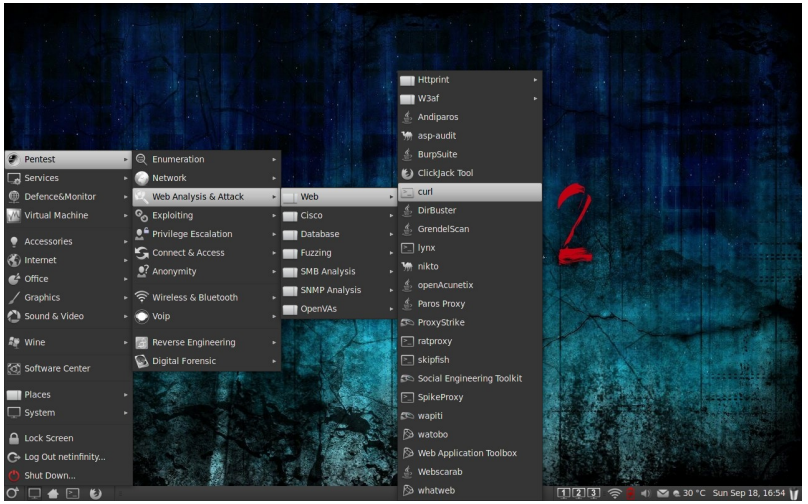
NodeZero

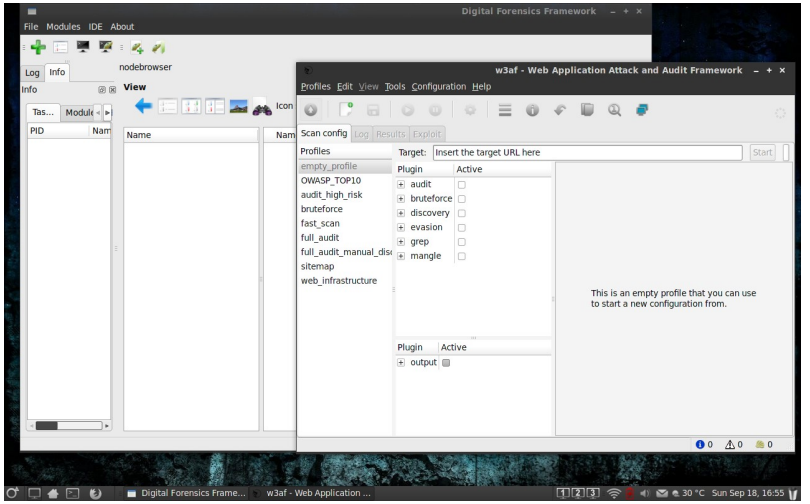
Make your own

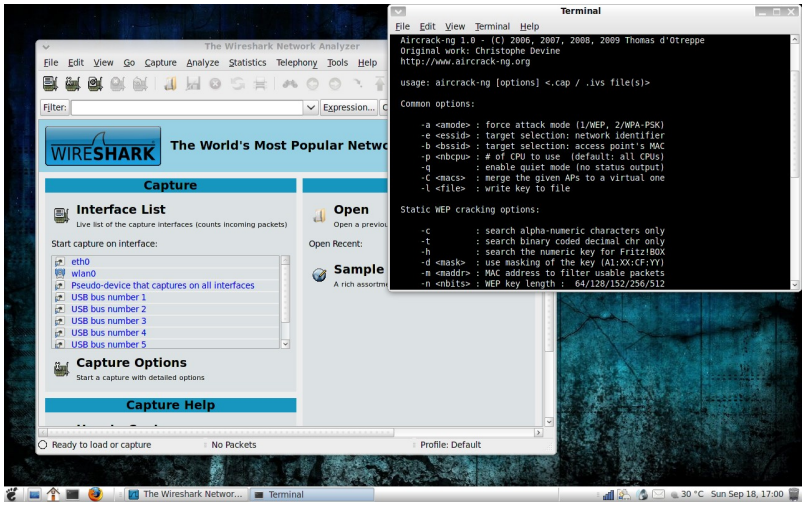
Google for “pentes linux distro”

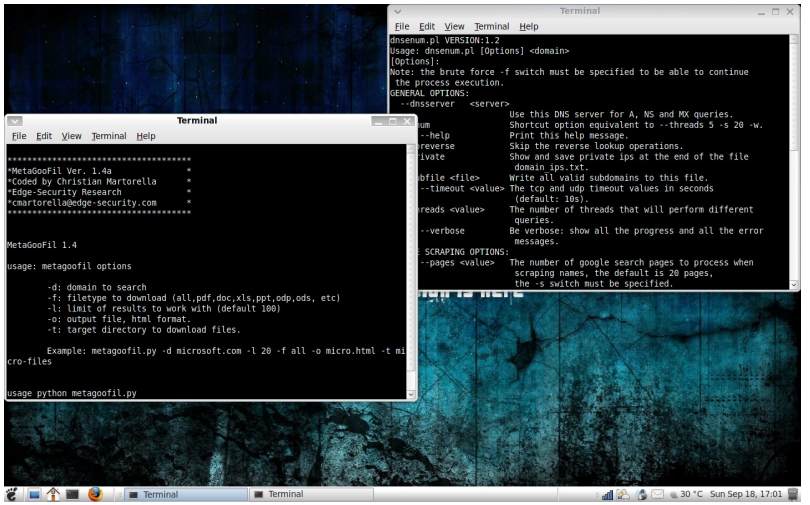
NodeZero - netinfinity.org

NodeZero - netinfinity.org









Network Security Monitoring

Insta-Snorby

Snort Engine

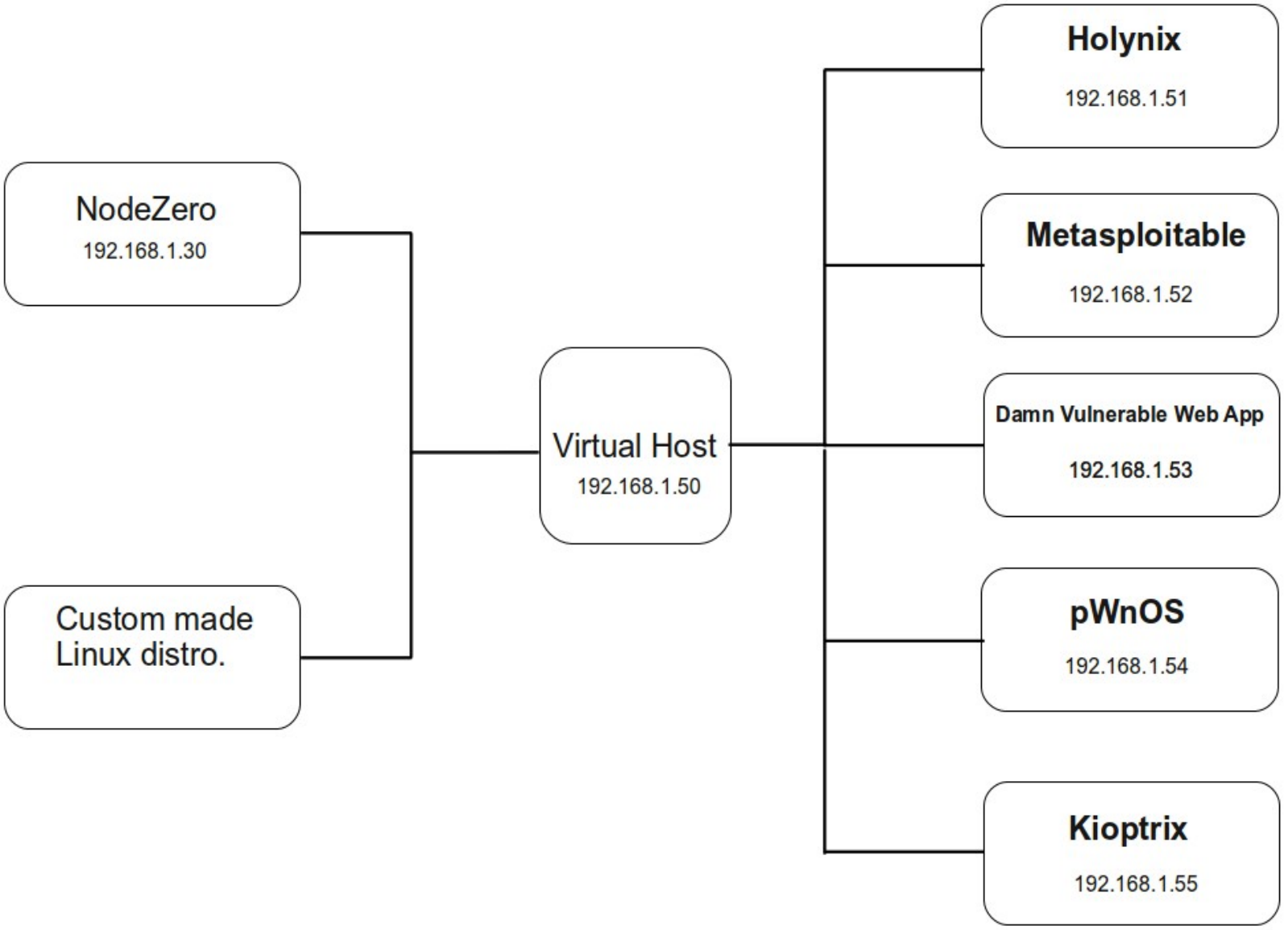
Smooth-Sec

Suricata Engine

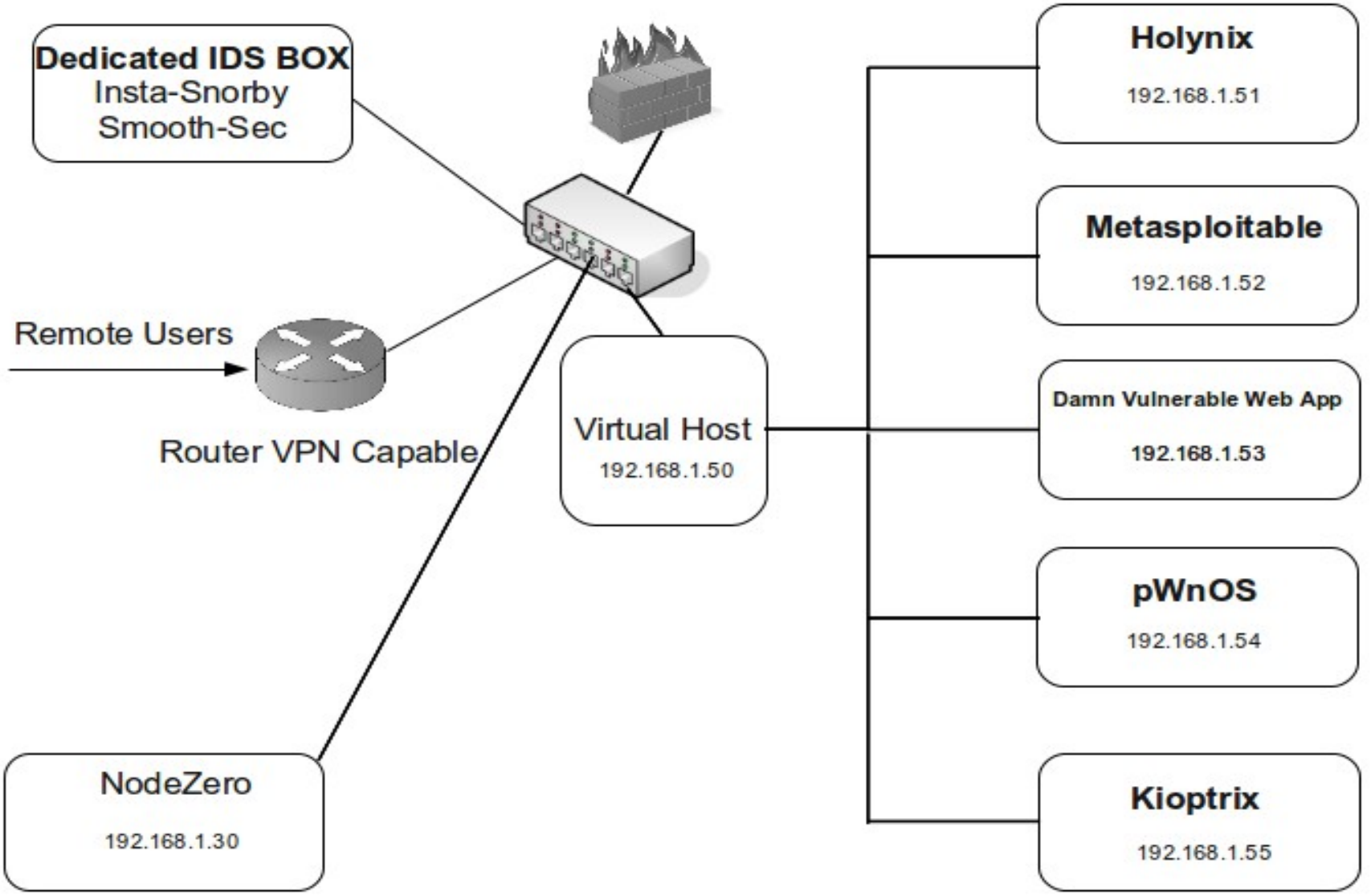
https://github.com/Snorby/insta-snorby

https://sourceforge.net/projects/smoothsec

Small environment lab.



Big deployment lab



Notes

Pentest lab vulnerable servers-applications list
http://tiny.cc/vmlist

Linux Penetration Testing distributions list
http://tiny.cc/pentestdistro

Hvala!

Phillip Bailey

www.bailey.st

phillip@bailey.st