

HackLab On A Budget

Michael Koerfer and Christopher Cotter

28.12.2017

Overview |

- Hardware
- Software
- Virtualization
- Pentester Tips
- Live Demo
- With a Budget
- Sparse Money



Use an old machine/old laptop

- As an example, you can use a laptop to run some VMs.



- Intel Core 2 Duo 2.4 Ghz CPU
- 4 GB RAM
- 100 GB HDD
- 14.1" TFT
- ebay \$59 \$149

• How to build a Whitebox?

- https://www.altaro.com/vmware/building-vsphere-6-x-home-lab/
- https://www.altaro.com/vmware/vsphere-home-lab-free/
- http://archive.bnetweb.org/index.php?topic=7370.0
- https://www.seas.upenn.edu/~cis196/VM/





- Where can you find the OS?
- https://www.microsoft.com/en-gb/software-download/
- https://www.techspot.com/downloads/operating-systems/
- https://www.vulnhub.com/entry/hacklab-vulnix,48/

- Where can you find the vulns?
- http://www.oldapps.com/
- http://www.oldversion.com/

Common vuln. targets that people use

- https://sourceforge.net/projects/websecuritydojo/
- https://github.com/rapid7/metasploitable3
- https://github.com/Hackademic/hackademic/



VMWare HackLab

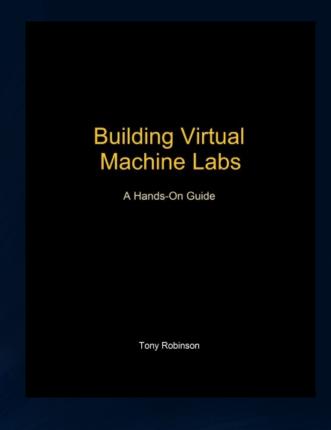
- https://media.hacking-lab.com/installation/vmware/
- https://null-byte.wonderhowto.com/how-to/hack-like-pro-createvirtual-hacking-lab-0157333/

VirtualBox HackLab

- https://hackmethod.com/building-hack-lab-free-part-1/
- https://hackmethod.com/building-hack-lab-free-part-2/
- https://www.blackmoreops.com/2014/06/10/correct-way-installvirtualbox-guest-additions-packages-kali-linux/

Building Virtual Machine (Hack)Labs

- https://www.amazon.com/Building-Virtual-Machine-Labs-Hands/dp/1546932631



Learn to build a secure, custom lab environment, tailored to your specific needs...

Virtualization is a skill that most IT or security pros take for granted. The sheer number of choices and requirements can be a daunting challenge to face for beginners and veterans alike.

With this book, you'll learn how to build a robust, customizable virtual environments suitable for both a personal home lab, as well as a dedicated office training environment. You will learn how to:

- Understand the mechanics of virtualization and how they influence the design of your lab
- Build an extensive baseline lab environment on any one of five commonly used hypervisors (VMware vSphere Hypervisor, VMware Fusion, VMware Workstation, Oracle Virtualbox, and Microsoft Client Hyper-V)
- Harden your lab environment against VM escapes and other security threats
- Configure the pfSense firewall distribution to provide security, segmentation, and network services to your virtual lab
- Deploy either Snort or Suricata open-source IDS platforms in IPS mode to further enhance the flexibility, segmentation and security of your lab network
- Deploy Splunk as a log management solution for your lab
- Reconfigure the provided baseline lab environment to better suit your individual needs

Easy to follow steps and illustrations provide detailed, comprehensive guidance as you build your custom-tailored lab. Both IT and security professionals need practice environments to better hone their craft. Learn how to build and maintain your own

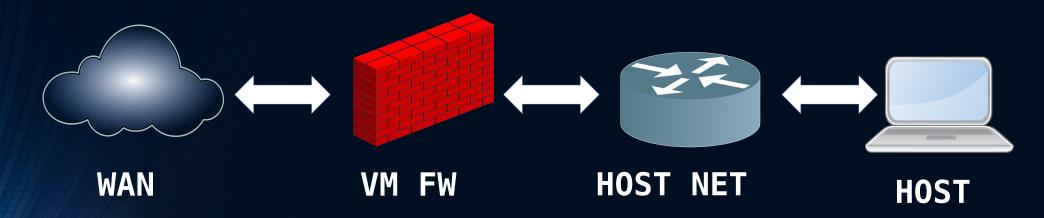
About The Autho

Tony Robinson is a senior security analyst with Hurricane Labs, where he serves as an expert on network security monitoring threat intelligence, and malware analysis. Tony has nearly a decade of combined experience in both IT and security disciplines. In his spare time, he loves to play yelpo gagnes.

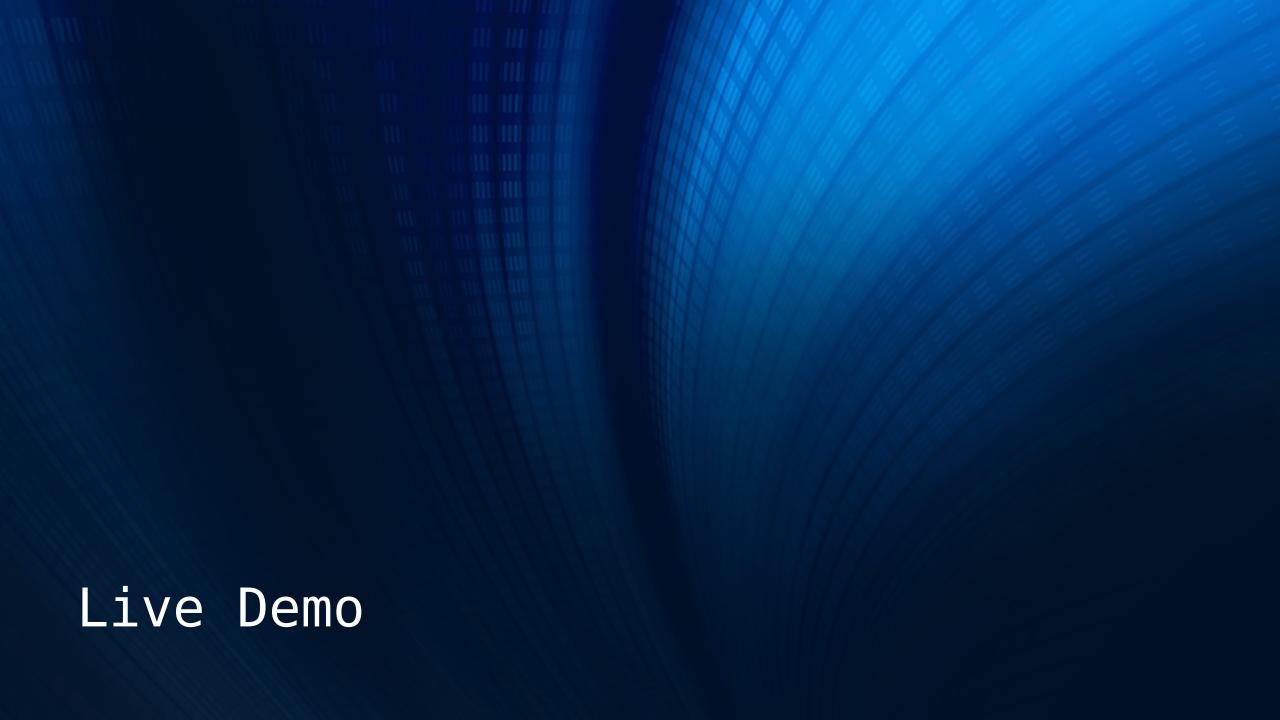




- How to design the network
- KISS (Keep It Simple, Stupid)
- Flat architecture first



- Think about DMZ, Router, Switches (over aged vulns)
- Focus on client-side applications and web applications



How to keep up with the latest vulns
 Download the latest tools and exploits each week

- Exploits
- https://packetstormsecurity.com/files/tags/exploit/
- https://www.exploit-db.com/

- Tools
- https://packetstormsecurity.com/files/tags/tool/
- http://sectools.org/

What types of vulns to put into the network

Use Popualar Applications

- Adobe
- Apple
- Microsoft
- Oracle

Don't try software that isn't often used in corporated envoirment. A lot of the exploits on exploit-db and similar sites are people learning exploit dev

Pentester lab resources

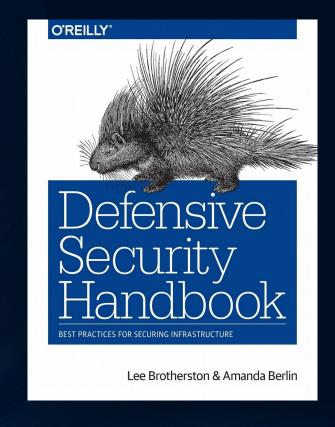
- https://gns3vault.com/labs/
- https://www.cybrary.it/forums/topic/how-to-set-up-pentesterlab/
- https://de.slideshare.net/null0x00/how-to-setup-a-pen-test-lab-andhow-to-play-ctf

How to build infrastructure (nids/router/fw)

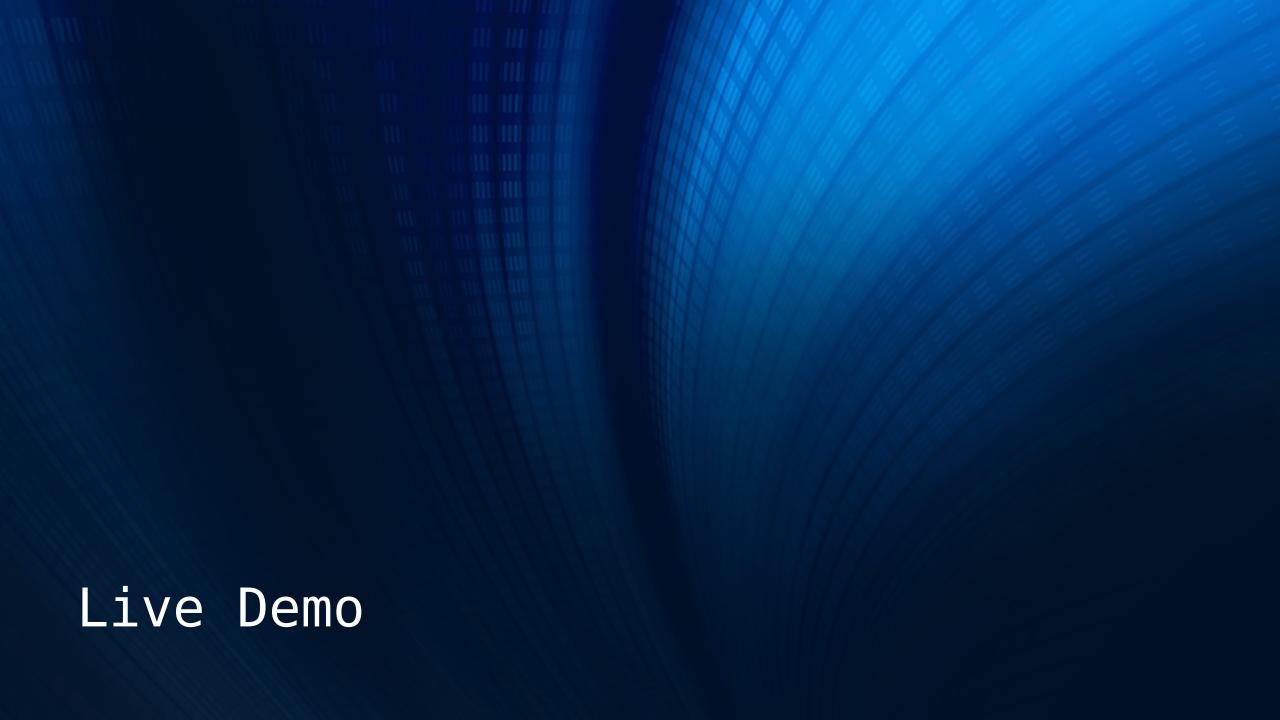
- https://doc.pfsense.org/index.php/PfSense_on_VMware_vSphere_/_ESXi
 15899/
- https://s3.amazonaws.com/snort-org-site/production/document_files/ files/000/000/069/original/Snort-IPS-Tutorial.pdf

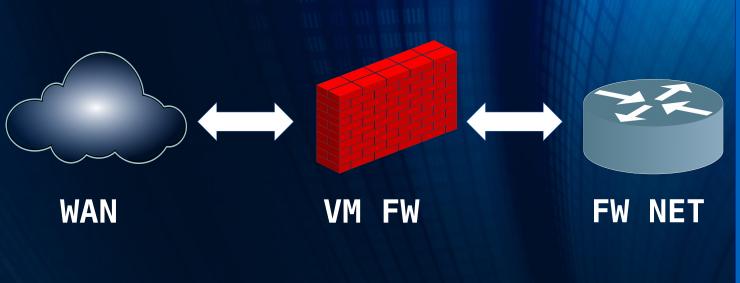
Building Defensive Security

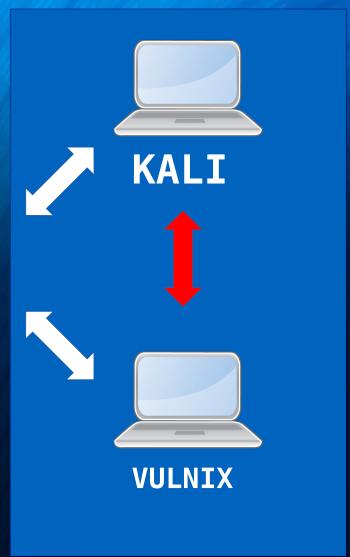
https://www.amazon.de/Defensive-Security-Handbook-Practices-Infrastructure/dp/1491960388



O'REILLY® Defensive Security Handbook Despite the increase in high-profile hacks, record-breaking data leaks, and "Anyone who's been ransomware attacks, many organizations don't have the budget to establish asked to build a or outsource an information security (InfoSec) program, forcing them to security program from learn on the job. For companies obliged to improvise, this pragmatic guide provides a security-101 handbook with steps, tools, processes, and ideas to the ground up will help you drive maximum-security improvement at little or no cost. get immediate value Each chapter in this book provides step-by-step instructions for dealing adding the Defensive with a specific issue, including breaches and disasters, compliance, Security Handbook as a network infrastructure and password management, vulnerability scanning, reference." and penetration testing, among others. Network engineers, system administrators, and security professionals will learn tools and techniques to help improve security in sensible, manageable chunks. Security & Privacy, Google ■ Learn fundamentals of starting or redesigning an InfoSec "The Defensive Security Handbook gives us ■ Create a base set of policies, standards, and procedures a solid curriculum ■ Plan and design incident response, disaster recovery, for 'Security 101' and beyond, starting with ■ Bolster Microsoft and Unix systems, network infrastructure, fundamental concepts and password management and working through ■ Use segmentation practices and designs to compartmentalize a variety of practical Explore automated process and tools for vulnerability steps to build a robust information security Securely develop code to reduce exploitable errors program." Understand basic penetration testing concepts through purple Jack Daniel Lee Brotherston has spent more than a decade working in Information Security across many verticals including finance, telecommunications, hospitality, entertainment, and government. Amanda Berlin is an Information Security Architect, co-hosts the "Brakeins Down Security' podcast, and writes for several blogs. NETWORK SECURITY Twitter: @oreillymedia facebook.com/oreilly CAN \$52.99 ISBN: 978-1-491-96038-7









Hardware Based

```
- 1x Thinkpad - T470 $1600
```

- 2x Firewall - ALIX 2D13 \$430

- 1x Router - UBIQUIT ER-X \$55

- 2x Switch - TP-SG2008 \$140

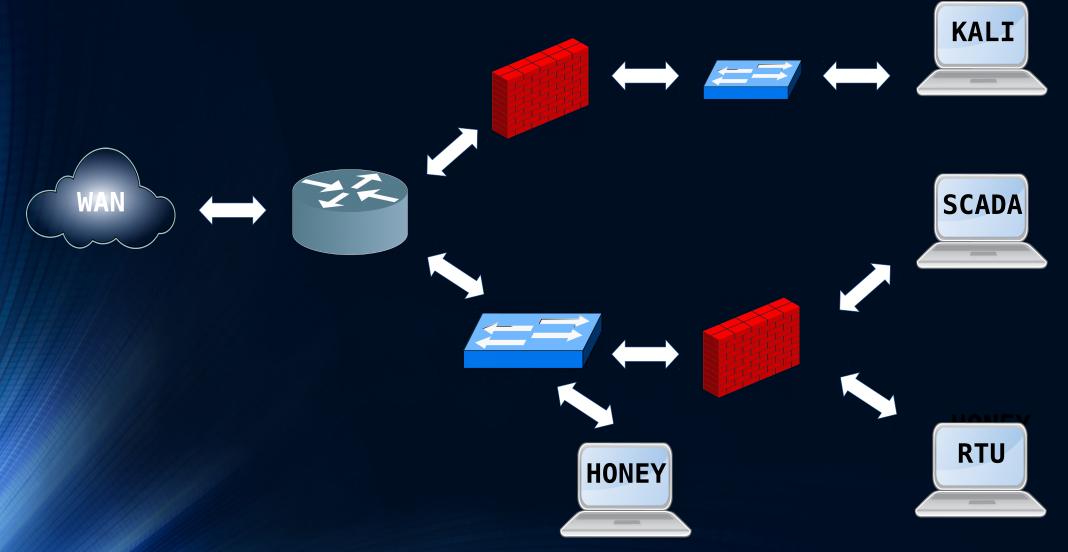
- 1x Thinclient - FUTRO S550 \$20

- 2x SBC - RPi3 \$110

- Some Stuff - USB/CABLE \$80

Everything available at Amazon

How to design the hardware network



You want to play with a big machine?

- Not many have a mainframe at home but there is a good solution.
- https://mainframed767.tumblr.com/post/166521465227/a-mainframe-onyour-raspberry-pi



Especially at the beginning or after the loss of a job due to termination, illness, accident, etc., when you're absolutely short on money, there is also a solution for that! I have experienced it myself!

Go to flea markets or recycling companies and bargain like you would at an oriental bazaar.

You can start small, with a thinclient e.g. Futro S550 for \$20

There is no shame in having to start over. Never give up, work on educating yourself, go to the library, read blogs and learn as much as you can. Nobody can take this from you anymore!

If you are in this situation, I wish you heartfelt strength and success for the new beginning.



- @da_667
- @InfoSystir
- @mainframed767
- @hacks4pancakes
- @thegrugq
- @HackingDave
- @KirilsSolovjovs
- @Nickf4rr
- @snowfensive
 and so many more for the inspiration!

Questions ???????

Thank you

Author: Michael Koerfer

E-mail: d_town@fnordeingang.de

Twitter: @D_70WN

Co-Author: Christopher Cotter

E-mail: ccotter8@gmail.com



