



# HackLab On A Budget

Michael Koerfer and Christopher Cotter

28.12.2017

# Overview

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

The background is a deep blue gradient. On the left, there's a faint grid of small squares. On the right, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

# Hardware



- 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/>



The background is a deep blue gradient. On the left, there's a faint grid of small squares. On the right, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

# Software

- 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/>



The background is a deep blue gradient. On the left, there's a faint grid of small squares. On the right, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

# Virtualization

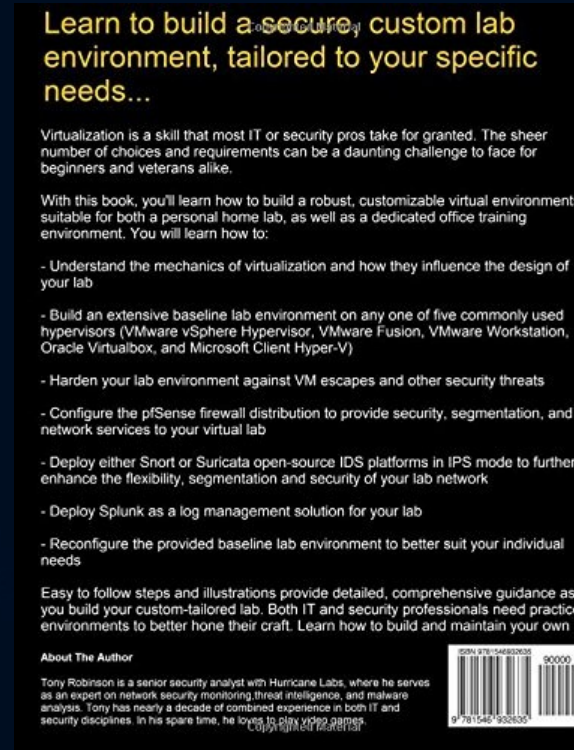
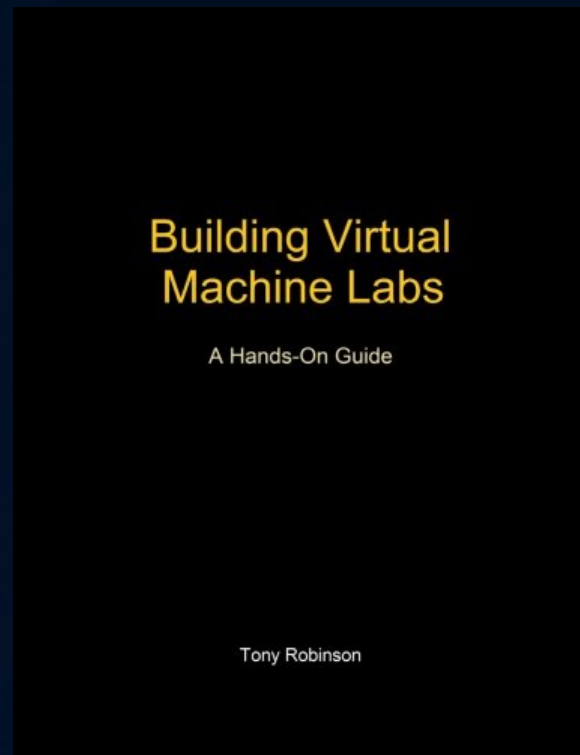
- VMWare HackLab

- <https://media.hacking-lab.com/installation/vmware/>
- <https://null-byte.wonderhowto.com/how-to/hack-like-pro-create-virtual-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-install-virtualbox-guest-additions-packages-kali-linux/>

- Building Virtual Machine (Hack)Labs
  - <https://www.amazon.com/Building-Virtual-Machine-Labs-Hands/dp/1546932631>

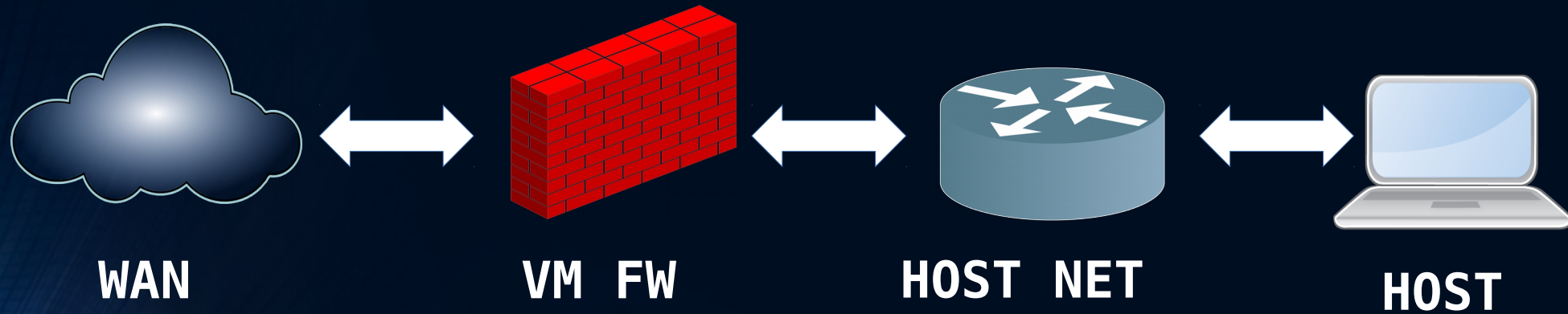




# Pentester Tips

- 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**

The background is a deep blue gradient. On the left, there are faint, curved lines. In the center, a grid of small, light blue squares is visible, creating a sense of depth. On the right, more pronounced curved lines sweep across the frame, suggesting a tunnel or a dynamic flow.

Live Demo

- 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 Popular Applications

- Adobe
- Apple
- Microsoft
- Oracle

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

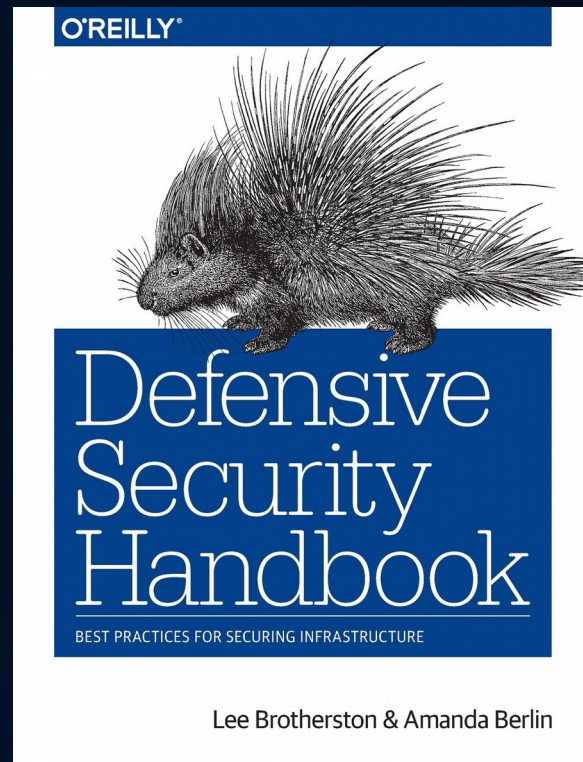
- Pentester lab resources

- <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-and-how-to-play-ctf>

- How to build infrastructure (nids/router/fw)
  - [https://doc.pfsense.org/index.php/PfSense\\_on\\_VMware\\_vSphere/\\_ESXi15899/](https://doc.pfsense.org/index.php/PfSense_on_VMware_vSphere/_ESXi15899/)
  - [https://s3.amazonaws.com/snort-org-site/production/document\\_files/files/000/000/069/original/Snort-IPS-Tutorial.pdf](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>



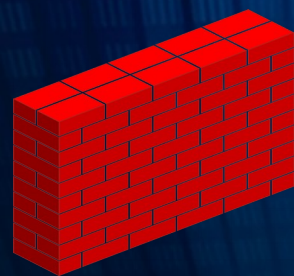


The background is a deep blue gradient. On the left, there are faint, curved lines. In the center, a grid of small, light blue squares is visible, creating a sense of depth. On the right, more pronounced curved lines sweep across the frame, giving it a dynamic, tunnel-like appearance.

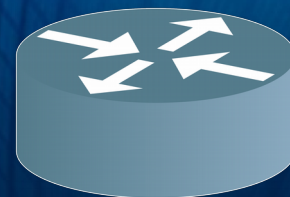
Live Demo



**WAN**



**VM FW**



**FW NET**



**KALI**



**VULNIX**



The background is a deep blue gradient. On the left side, there is a faint, light blue grid pattern. On the right side, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

With a Budget



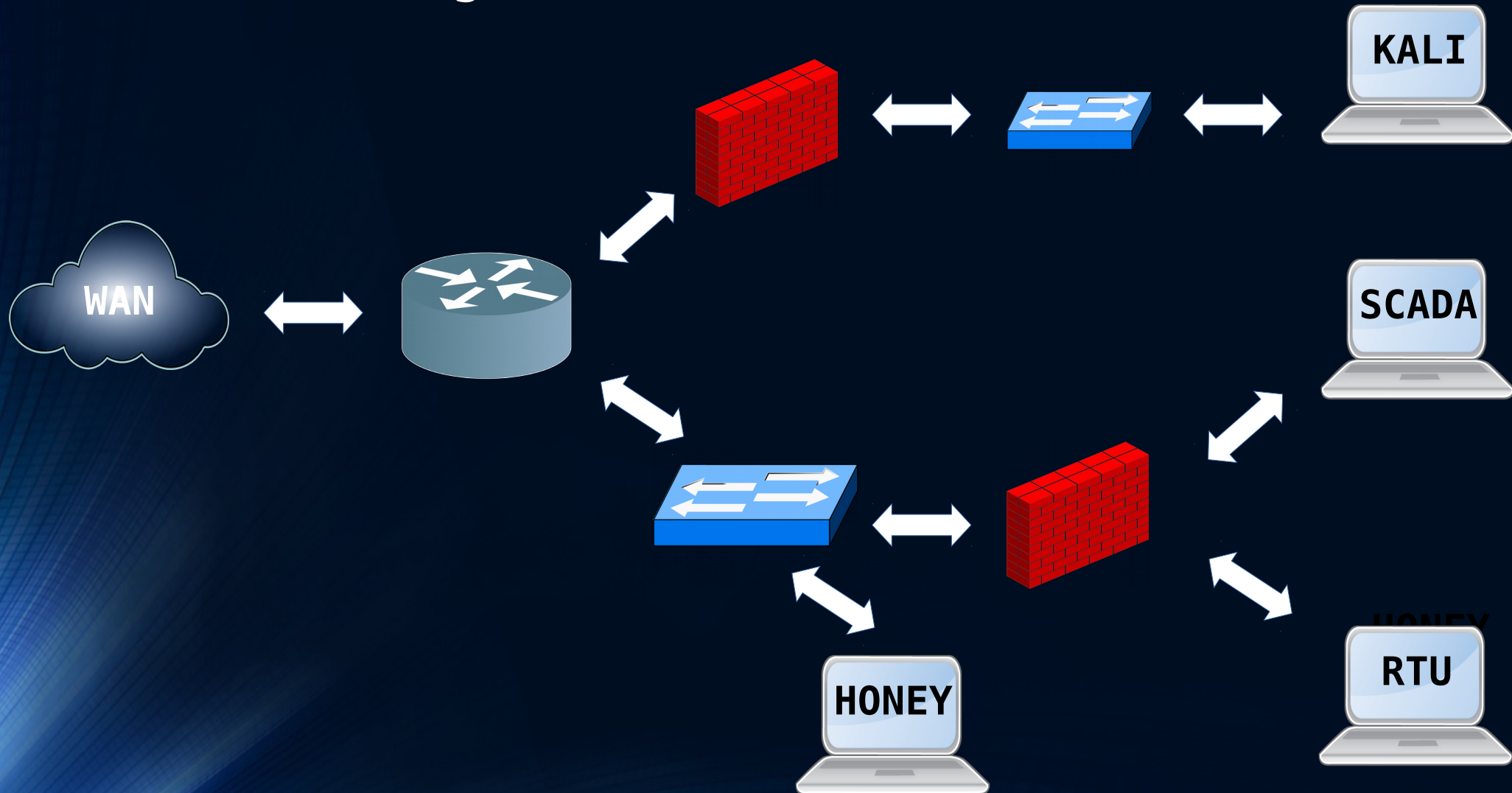
## • Hardware Based

- 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-on-your-raspberry-pi>

```
GREETINGS FROM RASPBERRY PI - RUNNING MVS/3580 V1.2 !!!!!
```

```
      .ee.   .ee.  
    ' \ ' ' / '  
      .e .eee.e.  
    : .e.'e'.e. :  
  e (   ) (   ) e  
( : 'e'.e.'e' : )  
  e .e (   ) e .e  
    ( : 'e' : ) RASPBERRY PI - MVS STYLE!  
    'e .eee. e'  
      'e'
```

```
READY
```

The background is a deep blue gradient. On the left, there's a faint grid of small squares. On the right, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

# Sparse Money

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.



The background is a deep blue gradient. On the left, there's a faint grid of small squares. On the right, there are several concentric, curved lines that create a sense of depth and movement, resembling a tunnel or a stylized eye.

# Credits

- @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: [michael\\_koerfer@posteo.de](mailto:michael_koerfer@posteo.de)

Twitter: [@D\\_70WN](https://twitter.com/D_70WN)

Co-Author: Christopher Cotter

E-mail: [ccotter8@gmail.com](mailto:ccotter8@gmail.com)

