HackLab For A Shoestring Budget

Michael Koerfer - 10.09.2017

Overview

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

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

- Build a whitebox for this
- What types of hardware to buy

- Checkout out a SHUTTLE Barebone XPC slim Dx30 Celeron

  - Intel Core i5 3.5 Ghz
  - 16 GB RAM
  - 120 GB HDD
  - Amazon $199

- 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/

Software

- Where you can 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 you can 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/

Virtualization

- VMWare HackLab

- https://media.hacking-lab.com/installation/vmware/

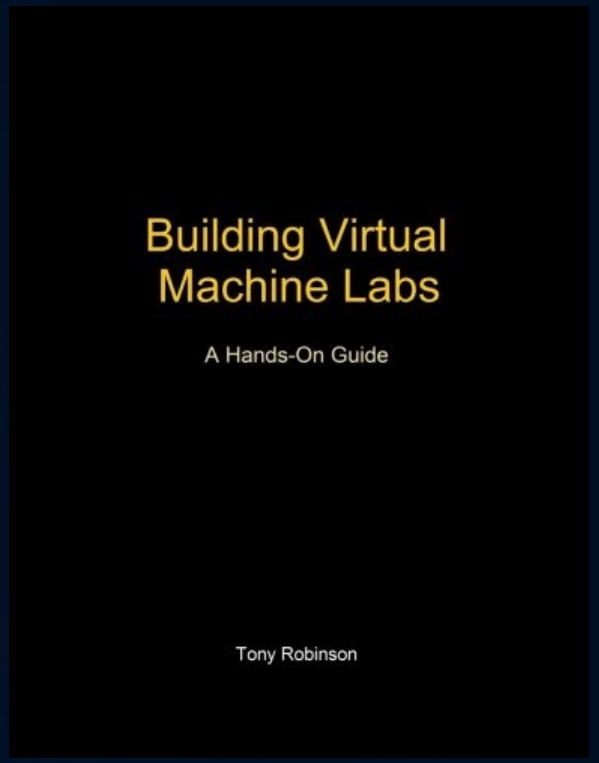
- https://null-byte.wonderhowto.com/how-to/hack-like-pro-create-virtual-hacking-lab-0157333/

- 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

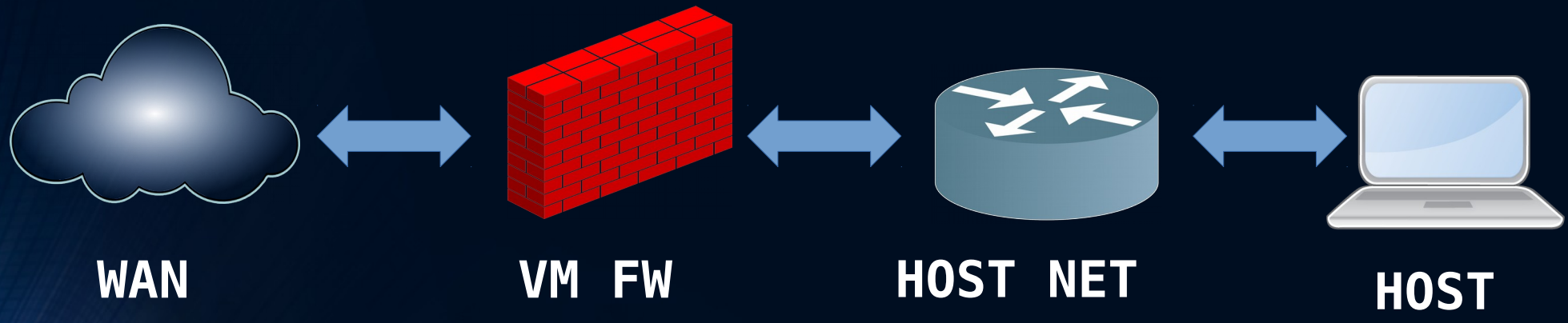
- https://www.amazon.com/Building-Virtual-Machine-Labs-Hands/dp/1546932631



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**

- 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 what 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 ressources

- 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

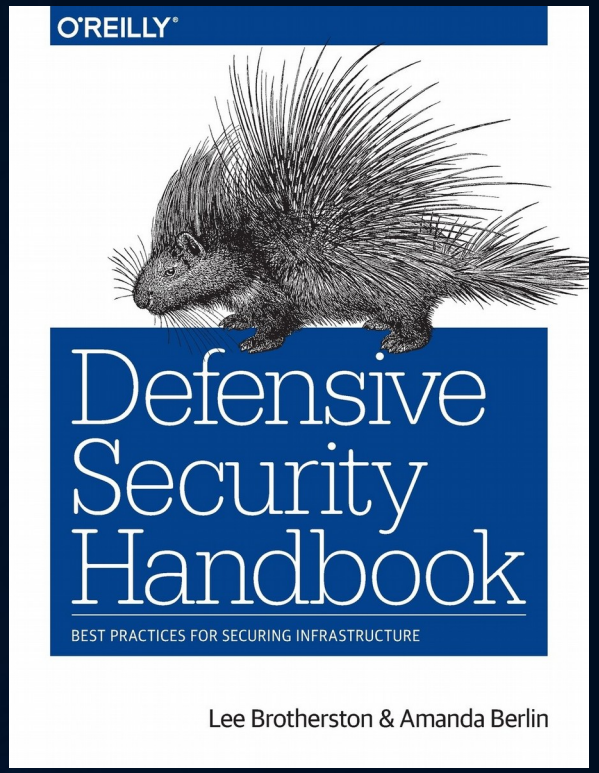
- How to build infrastructure (nids/router/fw)?

- https://doc.pfsense.org/index.php/PfSense_on_VMware_vSphere_/_ESXi_15899/

- https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/069/original/Snort-IPS-Tutorial.pdf

- Building Defensiv Security

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



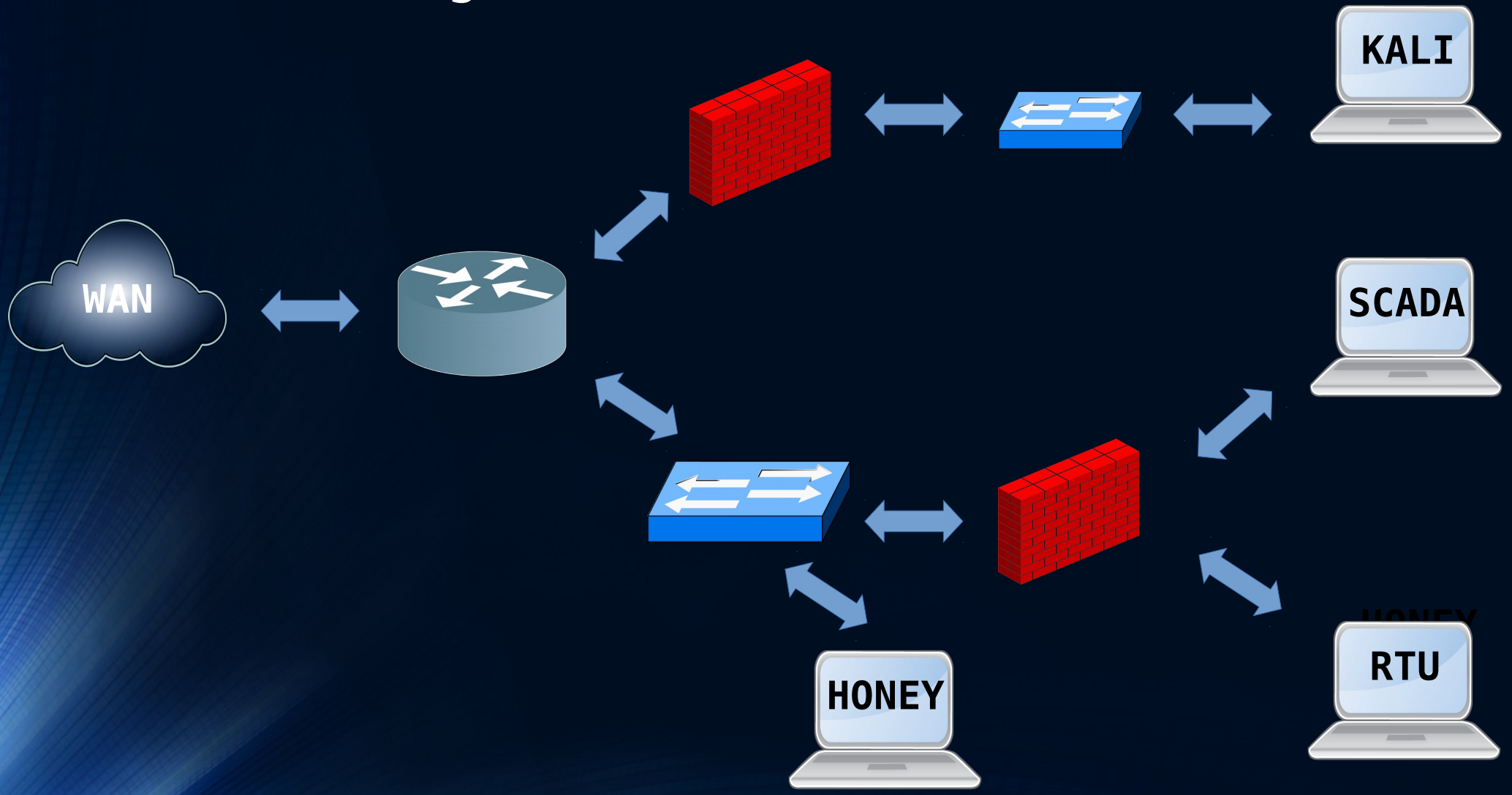
With a Budget

- 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

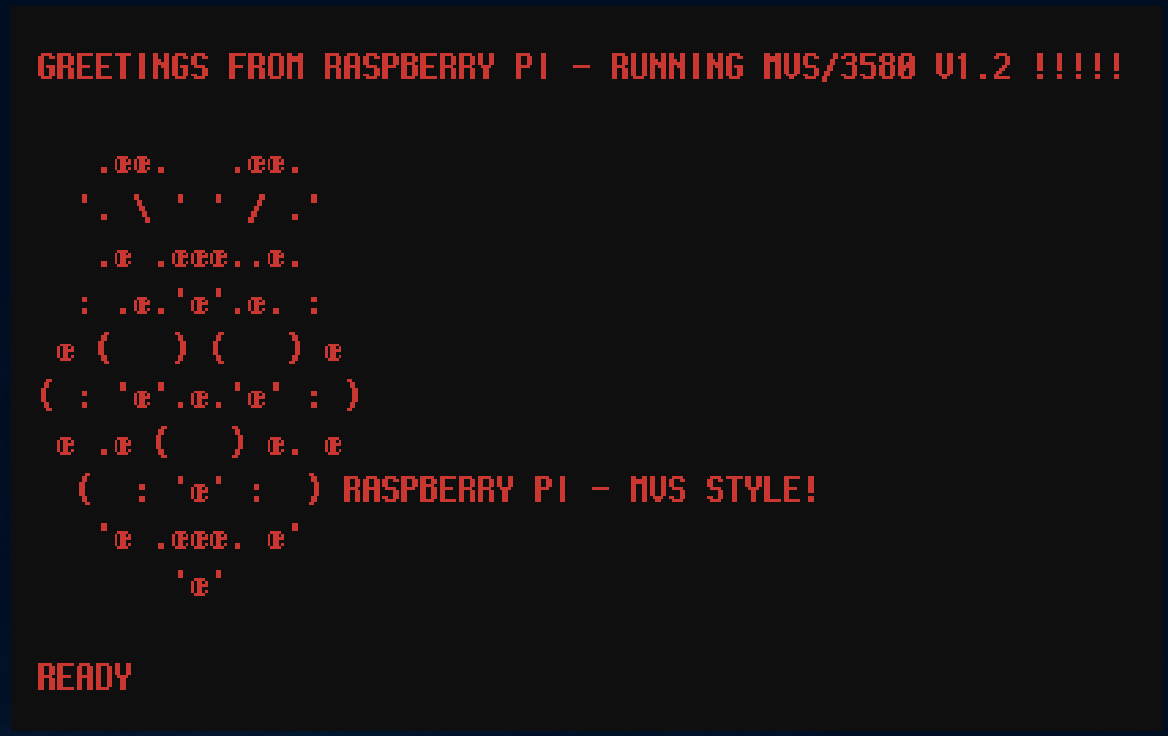
- How to design the hardware network?



- 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



Sparse Money

Especially at the beginning or by the loss of the job due to a termination, illness or accident, etc., where you have absolutely a sparse money, there is also a solution for that! I experienced it myself!

Go to flea markets or recycling companies and bargain like on a 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 giving up, working on you and going to the library, reading blogs, learn as much as you can. Nobody can take this from you anymore!**

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

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

Twitter: @D_70WN