BUILDING A HACKLAB (AND A LITTLE ABOUT THE CTF SETUP)

Adrian Crenshaw

About Adrian

- I run Irongeek.com
- I have an interest in InfoSec education
- I don't know everything - I'm just a geek with time on my hands

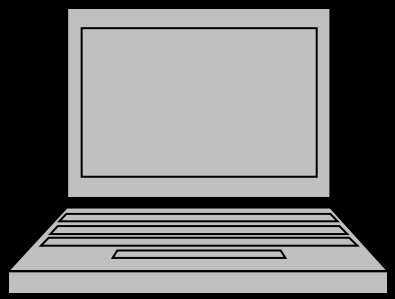
What is this talk about

Building a “HackLab”

1. Inexpensive ways to acquire hardware and software.
2. Learning about tools, vulnerabilities and exploits without getting to know Bubba.
3. Software and items built for learning.

Useful things to have

- A NAT box
- WiFi Routers (DD-WRT)
- Lots of network cable
- Switches
- Any networkable junk you can find
- KVMs
- Oh, and computers



Inexpensive Hardware

Institution

- Out of date PCs and Servers

Private

- Dumpster diving
- School disposals
- Government disposals
- Friends giving you old hardware in exchange for help
- Run a blog and just ask for it

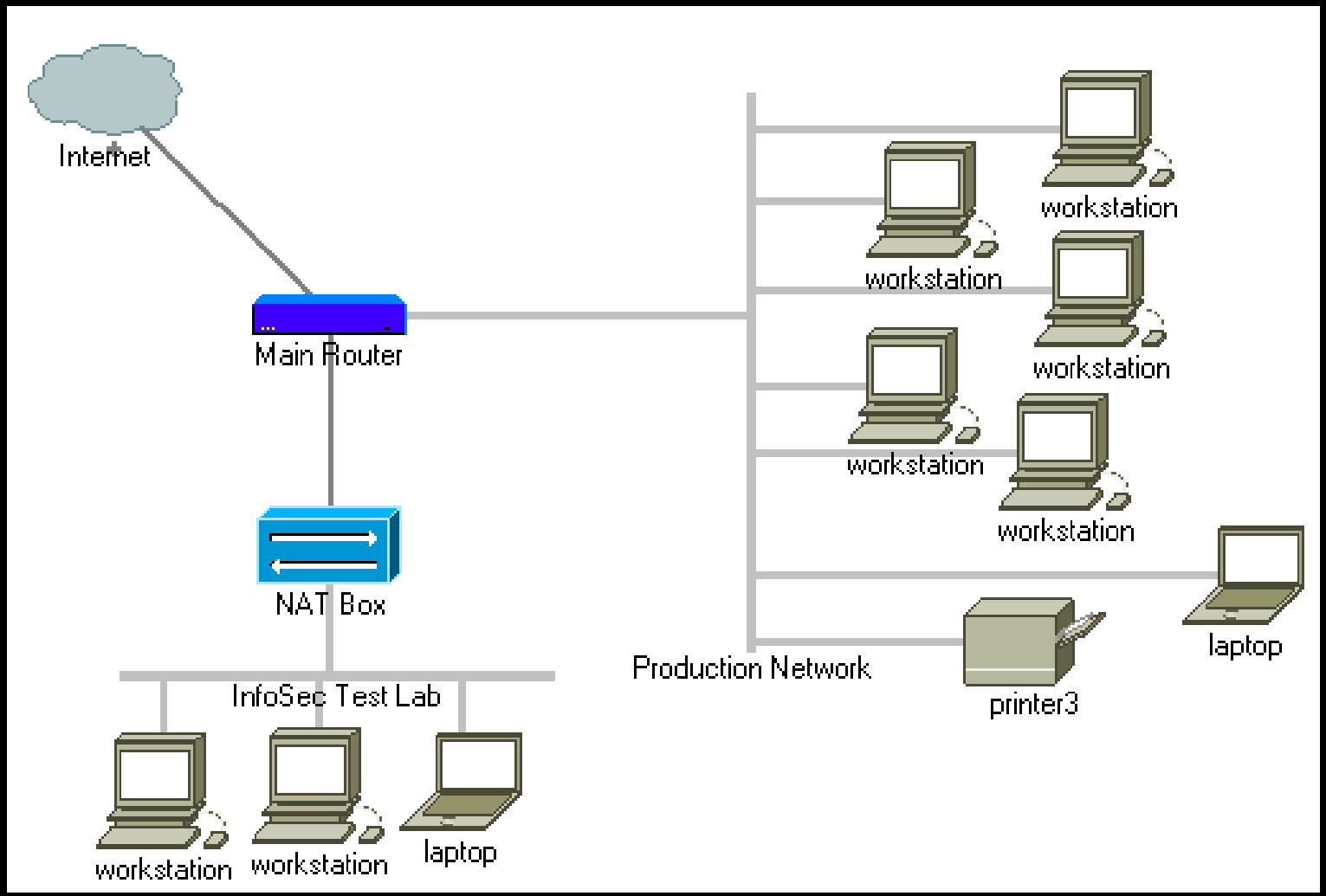
More source for cheap hardware and network nick knacks

- http://www.govdeals.com
- http://www.dealextreme.com
- http://www.techbargains.com

Cheap software

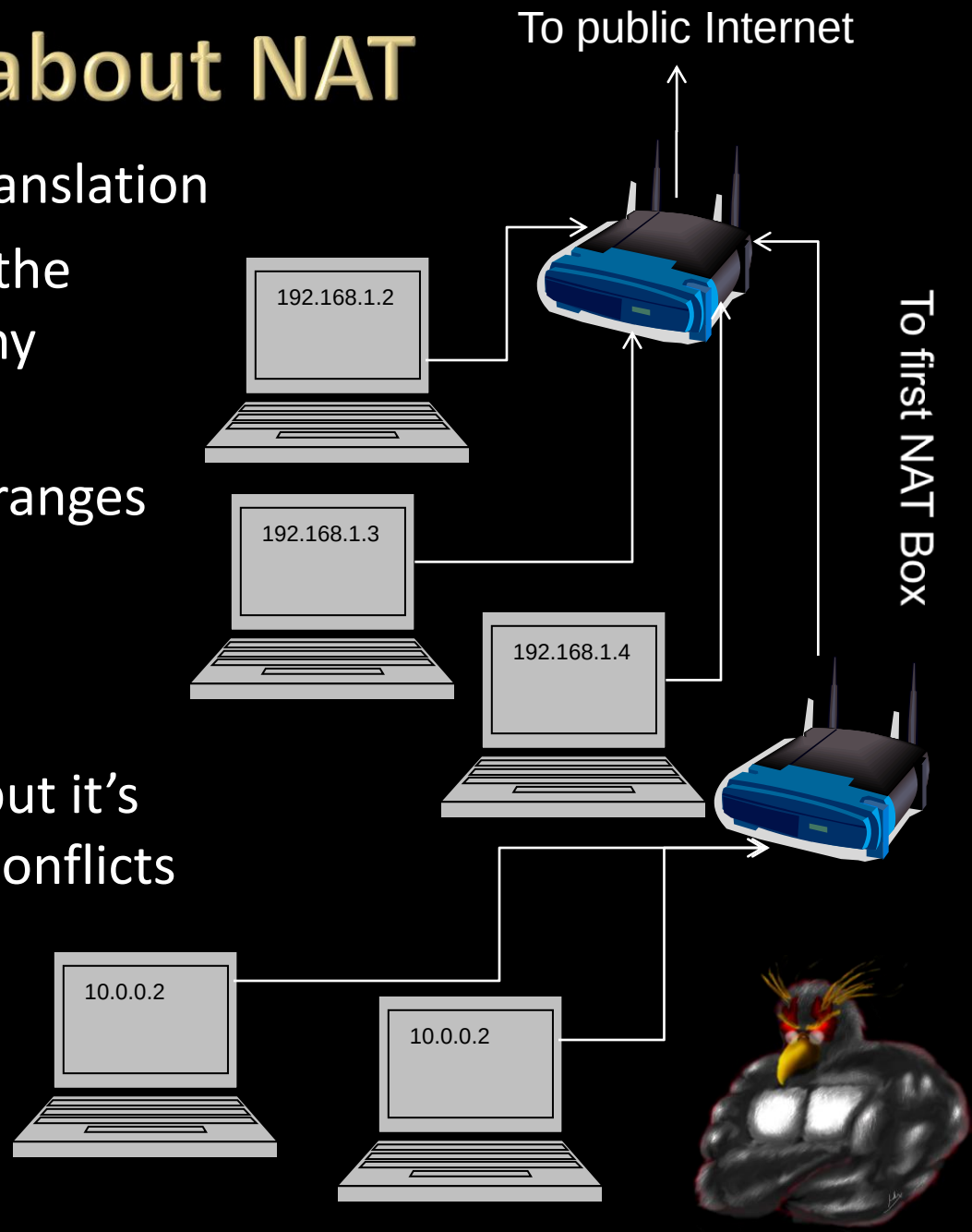
- Go open source
  Linux, FreeBDS, Apache, etc.
- Microsoft
  https://www.dreamspark.com/default.aspx
- Run a blog and just ask for it

Lab Layout


Internet
Main Router
NAT Box
InfoSec Test Lab
workstation
workstation
laptop
Production Network
workstation
workstation
workstation
workstation
workstation
printer3
laptop

A bit about NAT

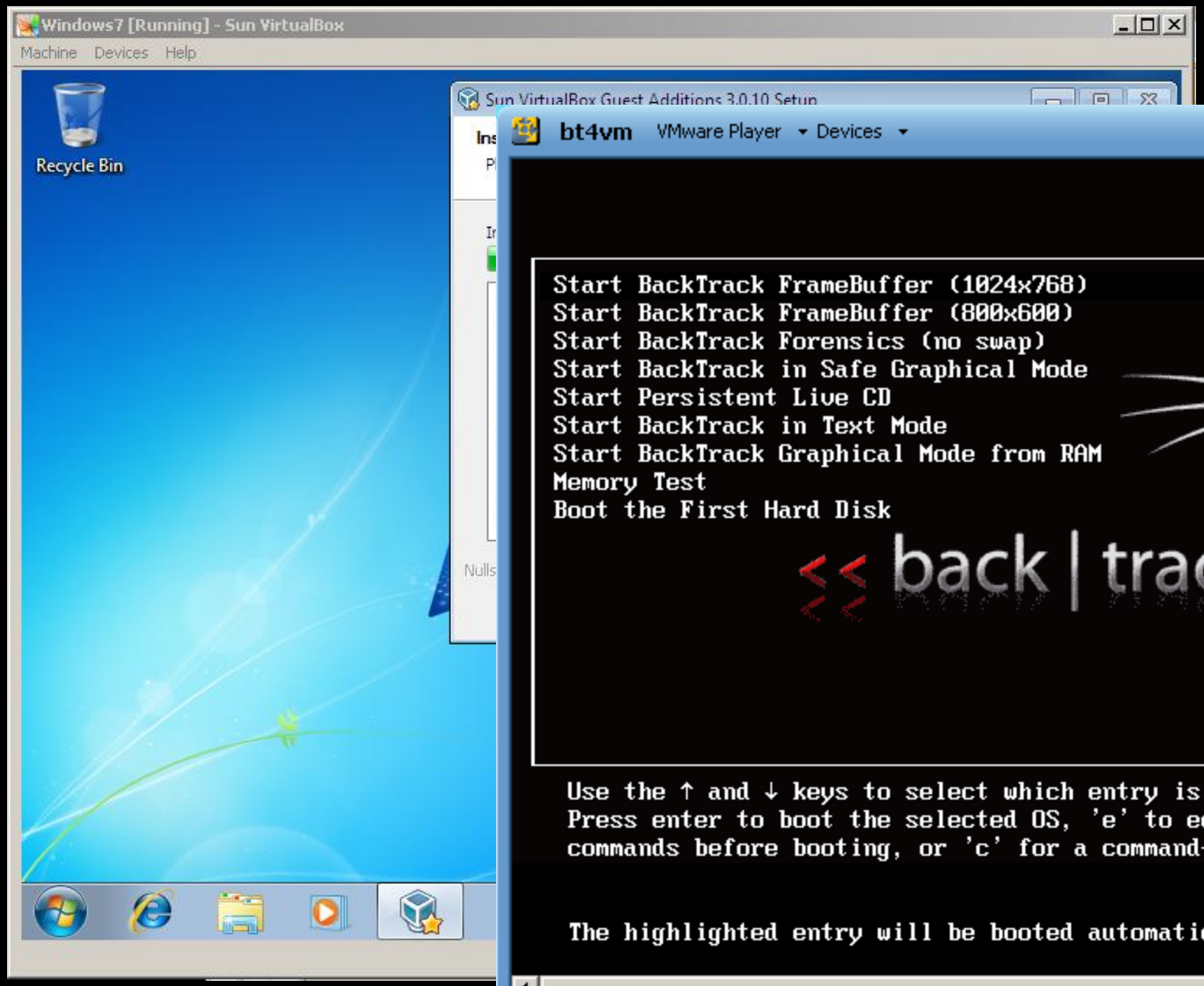
- NAT = Network Address Translation
- 1 public IP can be used as the outside connection to many internal IPs
- Reserved non-routable IP ranges
  192.168.*.*
  172.16.*.*-172.31.*.*
  10.*.*.*
- You can stack NAT boxes, but it's best not to have IP range conflicts



Network Layout: The importance of separation

- Air gap is best, but NAT will do
- Forward ports on the router for VPN/RDP/VNC
- You don't want to accidentally attack boxes outside of your lab
- Inside the lab you may have deliberately insecure boxes you don't want others to get to

Virtual Machines



http://Irongeek.com

Reasons why VMs are so great

- One computer can act like many
- You can hose a system, and easily recover from backup
- Somewhat safer from a sandbox standpoint
- Easy to hand out a custom environment to a class

Options, Options, Options

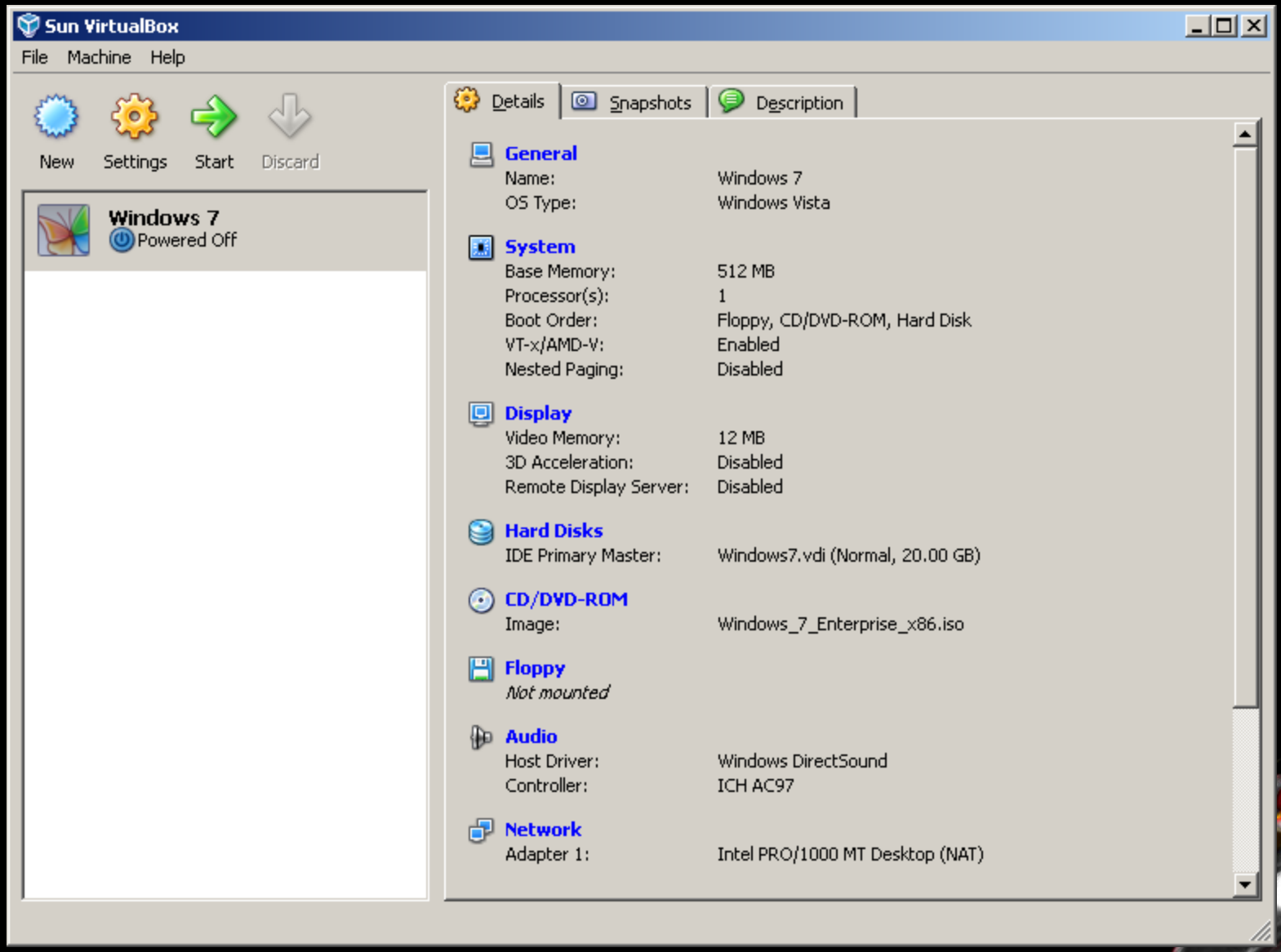
- Comparisons
  http://en.wikipedia.org/wiki/Comparison_of_platform_virtual_machines
- VMPlayer
  http://www.vmware.com/products/player/
  Plus
  http://vmxbuilder.com/
- VirtualBox
  http://www.virtualbox.org/

VM Concepts

- Host OS vs. Guest OS
- Snapshots
- Networking modes

  Bridged: The VM acts as if it's part of your real network.
  NAT: Your VM is behind a virtual NAT router, protecting it from the outside LAN, but still allowing other VMs ran on the same machine to contact it.
  Host-Only: You would want to choose this option if you don't want the VM to be able to bridge to the Internet using NAT. It would be a good idea to use this option if you are testing out any worm or viral code.
- VM Tools
- Sparse drive space
- USB Support

Virtual Box Demo



Sources for VMs if you don't want to roll your own

- VM Appliances
  http://www.vmware.com/appliances/
  http://ovfappliances.com/
- Formats
  - OVF:Open Virtualization Format
  - VMX/VMDK: VMWare
  - XML/VDI: VirtualBox
- C:\Users\adrian\.VirtualBox

Memory Needs

- Linux 128MB: Could be more or less depending on the desktop interface you use and what services you decide to run.
- Windows 9x, 64MB: It should feel quite spry.
- Windows 2000/2003/XP, 128MB: yes, you would want more if you can get it, but you can get away with 128MB if necessary.
- Windows Vista, 256MB: Don't send me hateful emails, it can be done. You have to set it to at least 512MB to install Vista, but thereafter you can shrink it down to only 256MB. It's ugly, but it works.
- Windows 7: Just go with 512.

Things to hack

- Deliberately vulnerably web apps
- Old software
- Specially build scenarios

Deliberately vulnerably web apps

- Hacme Series from Foundstone (Hacme Travel, Hacme Bank, Hacme Shipping, Hacme Books)
  http://www.foundstone.com/us/resources-free-tools.asp
- WebGoat
  http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
- Mutillidae
  http://www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10

Old software

- Check the vendors site for old versions
- Old, not slipstreamed OS CDs
- Old Apps Repository
  http://oldapps.com/

Specially built scenarios

- De-ICE & pWnOS Live CDs
  http://heorot.net/livecds/

- Damn Vulnerable Linux
  http://www.damnvulnerablelinux.org/

Things to hack with

- So many tools, so little time to install them all:
  - Nmap
    http://nmap.org/
  - Metasploit
    http://www.metasploit.com/
  - Wireshark
    http://www.wireshark.org/
  - Kismet
    http://www.kismetwireless.net/
  - Nessus
    http://www.nessus.org/nessus/
  - Cain
    http://www.oxid.it/cain.html
  - Netcat\Ncat
    http://netcat.sourceforge.net/
  - Ettercap
    http://ettercap.sourceforge.net/
  - Nikto
    http://cirt.net/nikto2
  - Paros Proxy
    http://www.parosproxy.org
  - Burp Suite
    http://www.portswigger.net/suite/
  - XSS Me
    https://addons.mozilla.org/en-US/firefox/addon/7598
  - SQL Inject Me
    https://addons.mozilla.org/en-US/firefox/addon/6727?src=reco
  - Tamper Data
    https://addons.mozilla.org/en-US/firefox/addon/966
- Great list of security tools
  http://sectools.org/

Easy way with Live CDs and VMs

- BackTrack
  http://www.remote-exploit.org/backtrack_download.html

- Samurai WTF
  http://samurai.inguardians.com/

- DEFT Linux
  http://www.deftlinux.net/

Staying up to date on trends and exploits

- Milw0rm
  http://www.milw0rm.com/
- SANS Internet Storm Center
  http://isc.sans.org/
- PacketStorm
  http://www.packetstormsecurity.org/
- BugTraq
  http://www.securityfocus.com/archive/1
- RootSecure
  http://www.rootsecure.net/

Podcasts: Learn about new tools as they come out

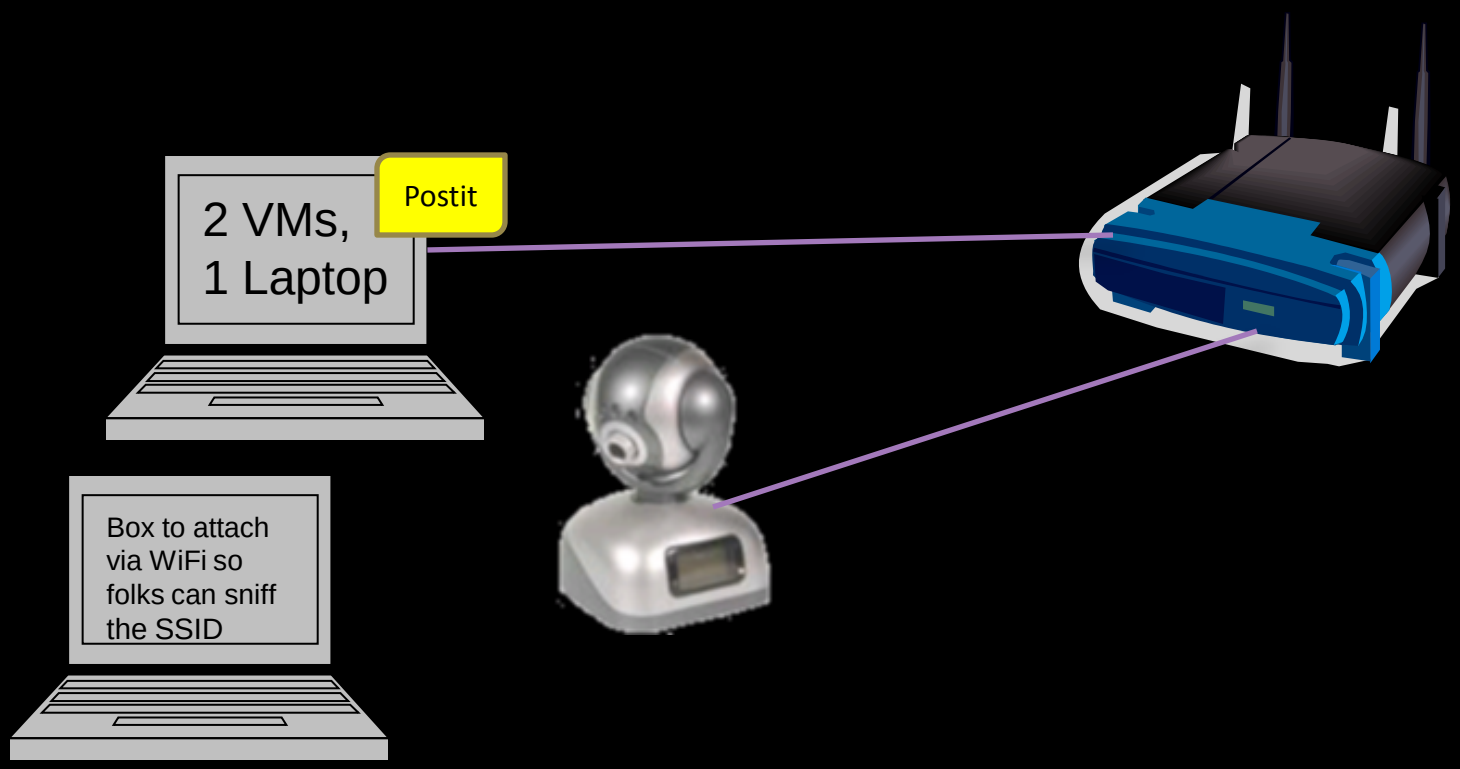
- Pauldotcom
  http://www.pauldotcom.com/
- Exotic Liability
  http://www.exoticliability.com/
- Security Justice
  http://securityjustice.com/
- Securabit
  http://www.securabit.com/

Links

- Original Article: http://www.irongeek.com/i.php?page=security/building-an-infosec-lab-on-the-cheap
- Insecure web apps http://www.irongeek.com/i.php?page=security/deliberately-insecure-web-applications-for-learning-web-app-security
- Hackerspaces http://hackerspaces.org

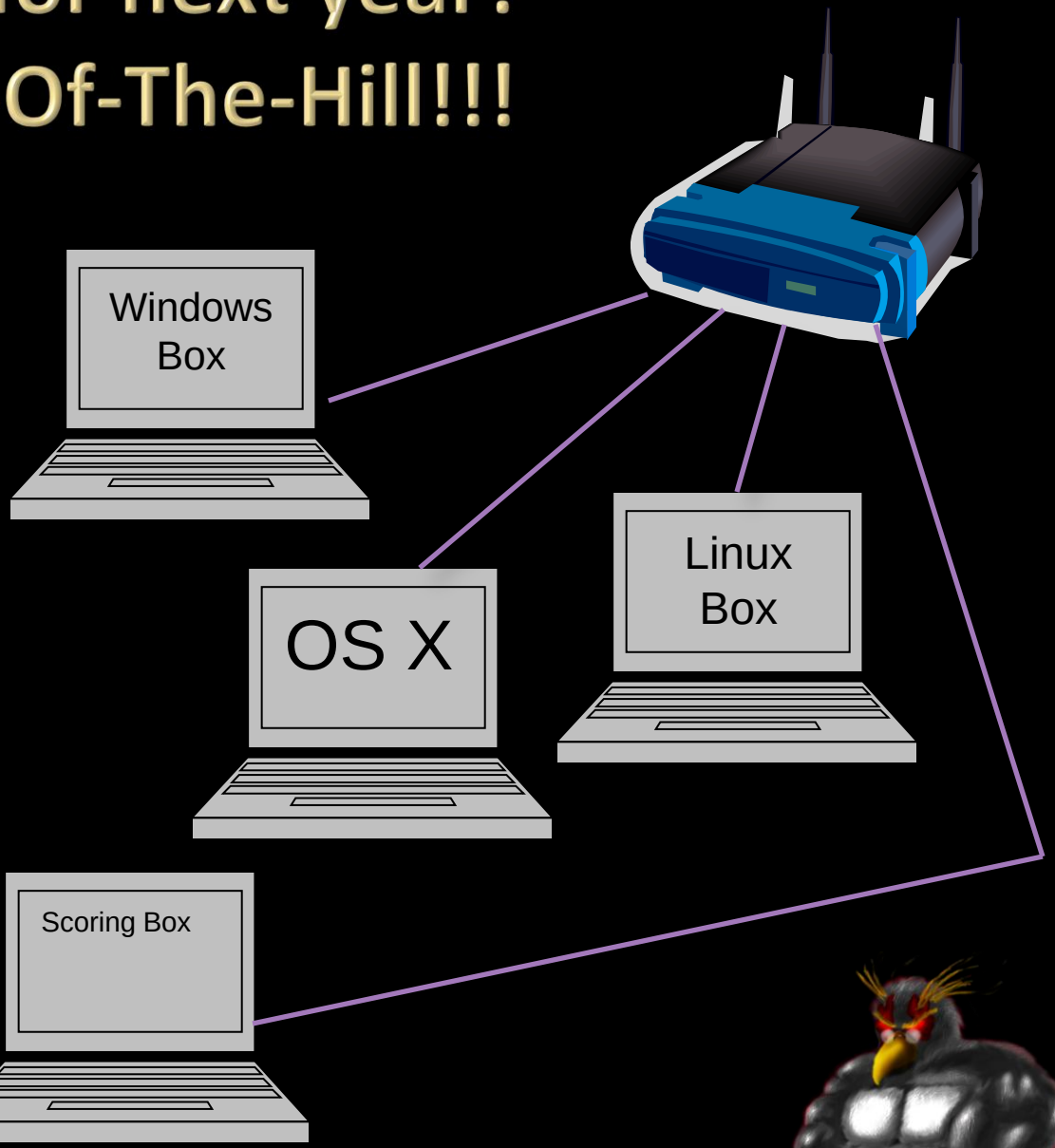
The CTF Setup: A Hacklab in Action

- Lets watch the video
  http://www.irongeek.com/i.php?page=videos/louisville-infosec-ctf-2009



Plan for next year?
King-Of-The-Hill!!!

- Keep a box and hold it
- Set your flag by defacing the website with your team's name
- Must keep services running to get points
- Can patch to keep others out
- Can attack network layer



Events

- Free ISSA classes
- ISSA Meeting
  http://issa-kentuckiana.org/
- Louisville Infosec
  http://www.louisvilleinfosec.com/
- Phreaknic/Notacon/Outerz0ne
  http://phreaknic.info
  http://notacon.org/
  http://www.outerz0ne.org/

Thanks

- Folks at Binrev and Pauldotcom
- Louisville ISSA
- Free ISSA Classes

Helping with the free classes

- Got old hardware you would like to donate?
- Is there a subject you would like to teach?
- Let others know about upcoming classes, and the videos of previous classes.

QUESTIONS?

42