Building Your Own Kickass Home Lab

Jeff McJunkin
Jeff McJunkin, Senior Technical Analyst, Counter Hack
SANS Instructor
Architect of NetWars Experience 4.0

Career:
Desktop admin -> sys/net admin -> web/net pen test -> whatever I do now
Obligatory Table of Contents for today’s talk

Why build a lab?
Hardware
Hypervisor
Software
Stuff on the Internets
Example labs
Why build a lab?
Why build a home lab?

- For ongoing skills development
- To answer interesting questions:
  - Can payloads make it through our filtering?
  - Can an attacker pivot from X server to Y server / to our internal network?
  - How easy/awesome is Google Rapid Response?
  - How difficult is Microsoft LAPS (Local Administrator Password Solution)?
  - Can you detect timestomping?
Hardware
Don’t I need a whole lot of hardware?

- You don’t need a whole rack
- You (probably) don’t even need dedicated hardware!
Whaddya buyin’?

How much RAM do you need, really? 16 gigs? 32?

What if you need more VM’s for a particular exercise?

What if you want to do nested virtualization (VMware Workstation with one or more ESXi VM’s, which have their own VM’s)?

What if you don’t want to pause some VM’s to save RAM when working on others?
Okay, Whaddya Mean By “Kickass”?

Off-lease server hardware is ludicrously cheap.

But what about the SOAF?

^ “Significant Other Acceptance Factor”, obviously.

If we could somehow get it into a quiet desktop case, that would be great!

(Power usage is around 60 watts idle, or ~$5/month)
Let’s Talk About Specifics

tl;dr -- Check the next slide

- Off-lease server hardware in a tower case
- Motherboard / CPU combo from Natex for $500
- Case for $100
- Power supply for $80
- As much SSD as you want / can afford

^

(I end up on this side)
CPU / Motherboard combo: http://www.natex.us/Intel-S2600CP2J-Dual-E5-2670-128Gb-Kit-p/s2600cp-cpu-128gb-12800.htm

Case: https://www.amazon.com/gp/product/B00KFAG6DA/ref=oh_aui_detailpage_o01_s00?ie=UTF8&th=1


CPU fan (purchase two!): https://www.amazon.com/gp/product/B005O65JXI/ref=oh_aui_detailpage_o06_s00?ie=UTF8&psc=1

Storage:

SSD: https://www.amazon.com/Samsung-2-5-Inch-Internal-MZ-75E1T0B-AM/dp/B00OBRFFAS/ref=sr_1_1?ps=pc&ie=UTF8&gid=1476484732&sr=1-1

Slow spinning disk (don’t host VM’s here!): https://amzn.com/B008JLL4M or https://amzn.com/B01LYVD7ME if you don’t mind refurbished HDD’s (buy two!)
Intel S2600CP2J Motherboard Dual E5-2670 SR0KX 128Gb. PC3-12800R

List Price: $830.00  
Sale Price: $498.00  
Savings: $332.00  

Qty: 1  
ADD TO CART  
ADD TO WISH LIST

Stock Status: In Stock  
Availability: Usually Ships in 1 to 2 Business Days  
Product Code: S2600CP-CPU-128GB-12800
Assembled, it looks like this, except the motherboard power supply cable *does* fit :)

Building your own PC is like LEGO's, for IT folk.
Hypervisor
Which Hypervisor Should I Choose?

You can have a home lab without having a Type One* Hypervisor

For most folk, VMware Workstation will run just fine, as long as:

- You’re okay with *only* running a couple dozen VM’s at a time
- You can fit everything you need in the one workstation (i.e., no clustering, no separate Cisco switching and such)

Why not VirtualBox? You can, but pre-built appliances are more often for VMware.

* e.g., VMware vSphere ESXi, Citrix Xen, or Microsoft Hyper-V
But isn’t VMware Workstation less efficient than ESXi?

Yes.

However, it doesn’t really matter.

~85-90% efficiency will suffice for a lab, as opposed to ~95-98% efficiency with ESXi.
Software
Microsoft Software

You don’t need to spend a lot of money licensing Microsoft products!

- modern.ie (90 days between reverts)
- Windows Server trials (180 days between reverts)

Want full editions for minimal cost?

- MSDN:AA, Dreamspark, Microsoft Imagine, through your affiliated colleges
Pre-Built Linux Appliances

- Big shout-out to TurnKey Linux here!
  - Vulnerable by default, lots of extra plugins, old versions still available*
  - ... for lots of different pieces of software!
- Metasploitable v2 from Rapid7 is great as well

* [http://turnkey.interhost.co.il/opennode/](http://turnkey.interhost.co.il/opennode/) (it’s tough to find older TurnKey Linux builds)
TurnKey Linux
Windows software

- Ninite.com is **such** a relief here…
- Icecast 2.0.1 is a great and reliable service-side exploit ([http://downloads.xiph.org/releases/icecast/icecast2_win32_2.0.1_setup.exe](http://downloads.xiph.org/releases/icecast/icecast2_win32_2.0.1_setup.exe))
This installer includes
change apps

1. Download
Your installer will begin downloading shortly. If it didn’t start you can retry the download.

2. Run
Just run the Ninite.exe and relax. Ninite’s automation will install the apps in the background and without any toolbars or junk.

3. Share
Your friends will thank you when they save time with Ninite.
### Application Status

<table>
<thead>
<tr>
<th>Application</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>Downloading</td>
</tr>
<tr>
<td>Python</td>
<td>Waiting to download</td>
</tr>
<tr>
<td>WinDirStat</td>
<td>Waiting to download</td>
</tr>
<tr>
<td>7-Zip</td>
<td>Waiting to download</td>
</tr>
<tr>
<td>PUTTY</td>
<td>Waiting to download</td>
</tr>
<tr>
<td>Notepad++</td>
<td>Waiting to download</td>
</tr>
<tr>
<td>WinSCP</td>
<td>Waiting to download</td>
</tr>
<tr>
<td>VLC</td>
<td>Waiting to download</td>
</tr>
<tr>
<td>Foxit Reader</td>
<td>Waiting to download</td>
</tr>
<tr>
<td>LibreOffice</td>
<td>Waiting to download</td>
</tr>
<tr>
<td>Paint.NET</td>
<td>Waiting to download</td>
</tr>
</tbody>
</table>
Stuff on the Internets
Care for your own domain?


(including basic DNS records)
Yes! **jrmlabs.tk** is available!

<table>
<thead>
<tr>
<th>Domain</th>
<th>Status</th>
<th>Price</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>jrmlabs</td>
<td>FREE</td>
<td>USD 0.00</td>
<td>Select</td>
</tr>
<tr>
<td>.tk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>jrmlabs</td>
<td>FREE</td>
<td>USD 0.00</td>
<td>Select</td>
</tr>
<tr>
<td>.ml</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>jrmlabs</td>
<td>FREE</td>
<td>USD 0.00</td>
<td>Select</td>
</tr>
<tr>
<td>.ga</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Get one of these domains. They are free!
Low $ VPS FTW

Why?

- Outbound C2 is most convenient with an Internet-accessible host
- We need an authoritative DNS server for dnscat2: (https://github.com/iagox86/dnscat2)

Here, you’ll need your own easily-accessible public IP.

https://www.digitalocean.com/ for $5/month is probably reasonable :)

Point your NS records (from Freenom or otherwise) at your new public IPv4 addr.
Why not build your own DNS server, too?!
Why not build your own DNS server, too?!
Why not build your own DNS server, too?!
Administering BIND9 DNS is an exercise in pain, consider avoiding it if at all possible

Instead, use Freenom’s own DNS manager (“buy” a second free domain) or consider Amazon Route 53 ($0.50/domain/month + $0.40 per million queries)

You can return private IP addresses from these public DNS servers
  ○ Yes, it “leaks” your internal addressing, but who cares? It’s a lab!
Putting together complex networks?

**DO**: New vmnet interfaces with Virtual Network Editor
- This makes everything accessible directly from the host, no painful pivoting required.
  - Of course, you can still pivot if you want
- Note: Your host will “steal” .1 and .2 in every new subnet.

**DON’T**: LAN Segments through VM Settings
- Why? So your host can access every single network directly
- Exception: If you’re doing malware analysis or otherwise *want* isolation

**pfSense is a beautiful, beautiful piece of software**
- Free layer 3 router and layer 4 firewall, lots of plugins, freely available
A call for simplicity

- You know that interesting question you’re trying to answer?
- Make the lab as simple as possible!
  - Fewer parts to fail
- Many questions can be answered by 2-3 VM’s in the same subnet
Basic VM isolation with pfSense, using three interfaces:

1. “Internet” (NAT with port forward set up for DMZ VMs)
2. DMZ (10.10.10.254/24 / vmnet1 / Host-Only network)
3. Internal (10.10.20.254/24 / vmnet2 / Host-Only network)

Why .254? Because VMware Workstation itself takes .1 and .2
Example Lab - Basic Enterprise Network, part 2

1. Kali VM (one interface, NAT network)
2. TurnKey Linux WordPress (two interfaces, DMZ and internal networks)
3. Metasploitable 2 (two interfaces, DMZ and internal networks)
4. Server 2008 R2 trial (one interface, internal network)
5. modern.ie Windows 7 client (one interface, internal network)
Example Lab - Basic Enterprise Network, part 3

1. Log in to Kali (make SSH super-convenient, consider key-based login with PuTTY and set up a shortcut)
2. Exploit Metasploitable 2 or WordPress
3. Pivot to internal network, exploit Icecast 2.0.1 on Windows client
4. Dump hashes on client
5. Pivot and exploit server
6. Dump domain hashes
7. ...profit?
Raphael Mudge, the creator of Cobalt Strike and Armitage, put together his own freely-available set of lab VM’s:

http://blog.cobaltstrike.com/2015/06/04/cobalt-strike-penetration-testing-labs-download/

It also includes a great walk-through video! Lots of content to go through.

Want even more? He has his Advanced Threat Tactics material online as well:

https://www.vulnhub.com/ is a great resource here, complete with walkthroughs!

The SEED Project (http://www.cis.syr.edu/~wedu/seed/all_labs.html) has both downloadable VM’s with a specific challenge, and the complete corresponding walkthroughs.
Vulnerability and Attack Labs

People learn from mistakes. In security education, we study mistakes that lead to software vulnerabilities. Studying mistakes from the past not only help students understand why systems are vulnerable, why a "seemly-benign" mistake can turn into a disaster, and why many security mechanisms are needed. More importantly, it also helps students learn the common patterns of vulnerabilities, so they can avoid making similar mistakes in the future. Moreover, using vulnerabilities as case studies, students can learn the principles of secure design, secure programming, and security testing.

(1) Software in general

1. Shellshock Vulnerability Lab (new): exploit Bash's Shellshock vulnerability
2. Set-UID Program Vulnerability Lab: exploit the vulnerabilities of the privileged Set-UID programs. (Survey Results)
   - For Ubuntu9.11 VM
   - For Ubuntu11.04 and Ubuntu12.04 VMs
3. Buffer Overflow Vulnerability Lab: exploit the buffer overflow vulnerability using the shell-code approach. (Survey Results)
   - For Ubuntu9.11 VM
   - For Ubuntu11.04 VM
   - For Ubuntu12.04 VM
4. Return-to-libc Attack Lab: exploit the buffer-overflow vulnerabilities using the return-to-libc attack. (Survey Results)
5. Format String Vulnerability Lab: exploit the format string vulnerability. (Survey Results)
6. Race Condition Vulnerability Lab: exploit the race condition vulnerability. (Survey Results)
What else can I do?

I hear Counter Hack makes Holiday Hack Challenges for free every year…

We keep them online afterwards, too! Forever!

- Have you ever Shellshocked a system?
- Have you ever read data from a remote box using Heartbleed?

Well, now you can! Search for “2014 Holiday Hack Challenge” and try it yourself!
A Christmas Hacking Carol

2014 Holiday Hacking Challenge
By Ed Skoudis, Josh Wright, and Tom Hessman (featuring the voice stylings of Mr. James Lyne)

Stave 1: Marley's Ghost

Marley was dead: to begin with. There is no doubt whatever about that. The paperwork for decommissioning Marley, Scrooge's old server, was signed by the ops team, the clerk, the shredding company, and the chief mourner. Scrooge signed it: he had accidentally bricked that machine himself now seven years ago to the very day. Old Marley was as dead as a doornail.

For I don't know how many years, Scrooge relied on Marley as his main hacking machine. He developed all kinds of exploits on his trusty server and had built quite a successful business using that box. Indeed, his firm was known as Scrooge-and-Marley, and he had never bothered to remove Marley's name from the company website after the unfortunate bricking incident. There it stood, years afterwards, on the webpage title bar -- Scrooge-and-Marley -- hacker and machine, names side by side. Sometimes people new to the business
Too long; didn’t listen --

- **Hardware?** Read slide notes, base build is ~$800 for 128 GB of RAM, 16 cores
- **Hypervisor?** VMware Workstation is the most commonly-used, and lets you use the host for other things as well!
- **Windows OS?** modern.ie gives client OS for 90 days, 180 day trials of Server also free
- **Linux OS?** TurnKey Linux and Metasploitable 2
Thanks for joining!
Any questions?
@jeffmcjunkin
jeff@counterhack.com
Bonus Content
Separate email for phishing?

Sure, you can probably use a Gmail account for this.*

Yandex Mail is also free**: [https://yandex.com/support/mail/](https://yandex.com/support/mail/)

* But srsly, I’m not a lawyer

** And probably isn’t as good at spam filtering
Care for a gently-used domain name?

- For phishing campaigns, sometimes we want a domain that’s been around the block.
- This gives us a better chance of not being flagged when sending emails, as well as a better chance of being in URL / domain name whitelists.
- Consider [https://www.expireddomains.net/](https://www.expireddomains.net/), find a domain to create a phishing campaign around and purchase it cheaply.
What about defense?

- Take a look at ProcFilter for running Yara rules on your endpoints: https://github.com/godaddy/procfilter
- ...and for generating those Yara rules, consider https://github.com/Neo23x0/yarGen
- I strongly recommend full packet captures at the border with 10+ terabytes of local disk
  - Consider Security Onion, which will do this automatically with a network tap