Building Your Own Kickass Home Lab

Jeff McJunkin

(updated 2023-07-20)

https://t.me/learningnets

echo $(whoami)

Jeff McJunkin, Founder of Rogue Valley Information Security

SANS Principal Instructor / Author (SEC580)

Architect of SANS NetWars Experience 4.0 and 5.0

Certifications: GCED, GCFA, GCIA, GXPN, GCIH, GMOB, GPEN, GPYC, GREM, GSEC, GCPT, GSE, CISSP (I may have a problem)

Career:

Desktop/sys/net admin -> web/net pen test -> Counter Hacking -> consulting

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
  - Offense
  - Defense
  - Forensics
- 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 Velociraptor?
  - How difficult is Microsoft LAPS (Local Administrator Password Solution)?
  - Can you detect timestomping?

Life is full of interesting questions. By having a home lab, we can have a *safe* place to find the answers to those questions.

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!

Credit: reddit.com/r/CablePorn

reddit.com/r/homelab

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 and workstation hardware is ludicrously cheap

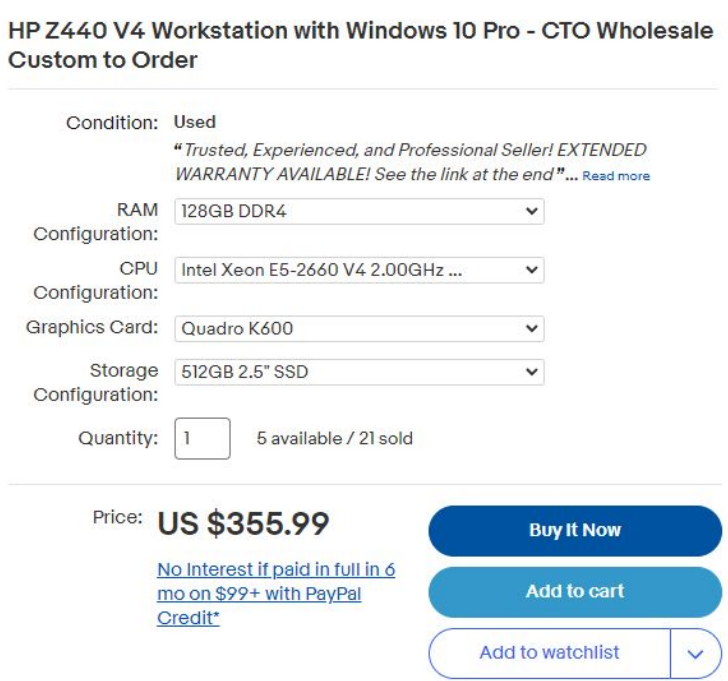
But what about the SOAF?

^ “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

- Pre-built HP workstation for ~$350
- Or build your own, 12-core AMD Zen 3 starts around $870
- As much SSD as you want / can afford

The specifics

Pre-built desktop:
https://www.ebay.com/itm/175147646467
(HP Z440)

Or build it yourself:
https://pcpartpicker.com/list/dshDkX (AMD Zen 3 compatible, starting at ~$700 with 8 cores and 64GB memory)

Storage:
SSD: https://www.amazon.com/dp/B07TLYWMYW (if using the AMD Zen 3 build above)
SSD: https://pcpartpicker.com/products/internal-hard-drive/#R=4,5&f=3&m=12,23,32,34,38&t=0 (otherwise)
Slow spinning disk: https://pcpartpicker.com/products/internal-hard-drive/#A=4000000000000,16000000000000&R=4,5&t=7200

Never run more than one Windows machine from a spinning disk.

In fact, in general avoid running VM's from spinning disks :)

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!

- Windows 11 Dev Environment
- Windows Server trials (180 days between reverts)

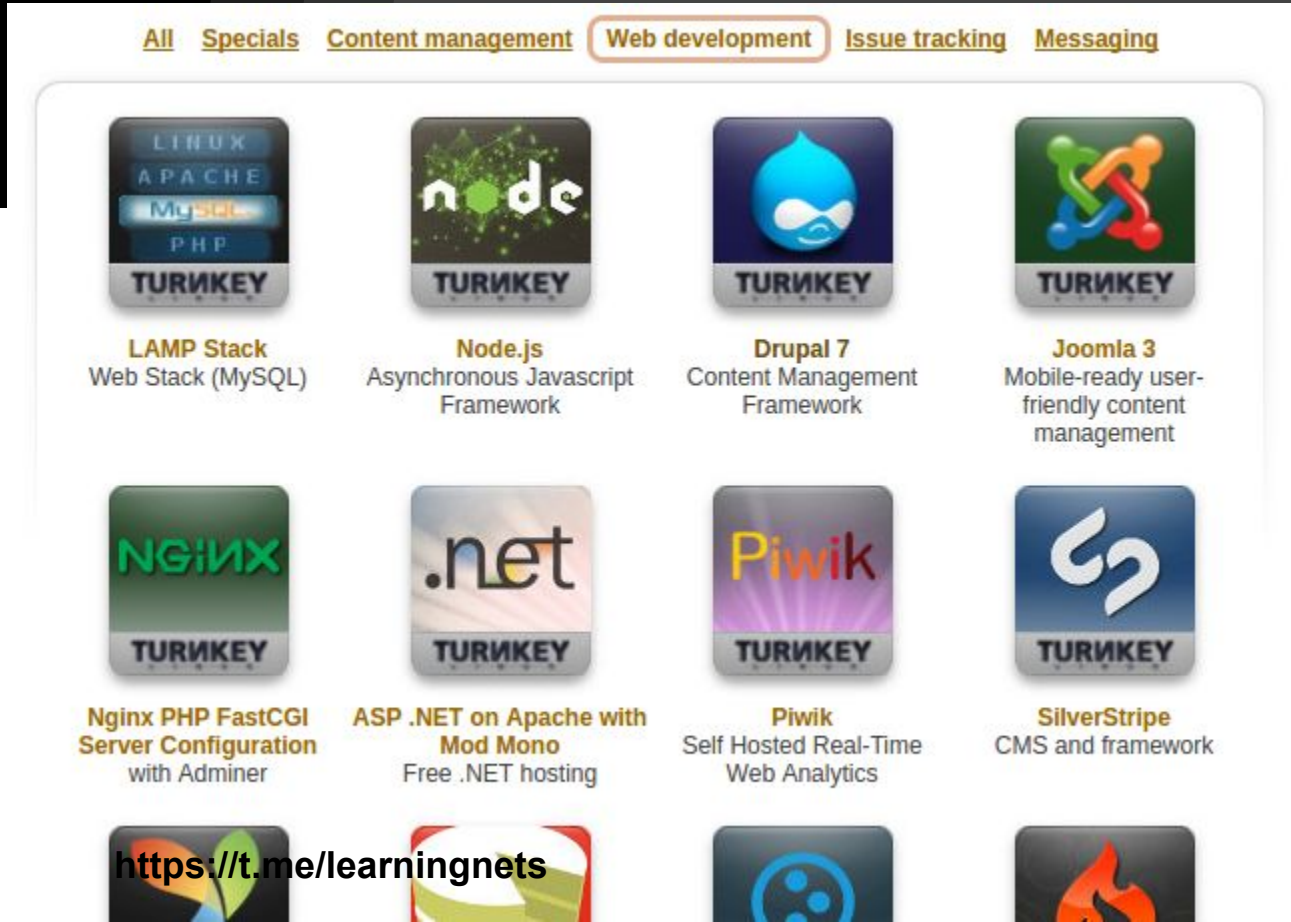
Want full editions for minimal cost?

- ~~MSDN:AA~~ ~~Dreamspark~~ ~~Microsoft Imagine~~ Microsoft Azure Dev Tools for Teaching, 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: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- SecGen builds *unique* vulnerable VM's each time using Puppet and VirtualBox: https://github.com/cliffe/SecGen
- https://www.mirrorservice.org/sites/turnkeylinux.org/images/iso/
  - (it's tough to find older TurnKey Linux builds)

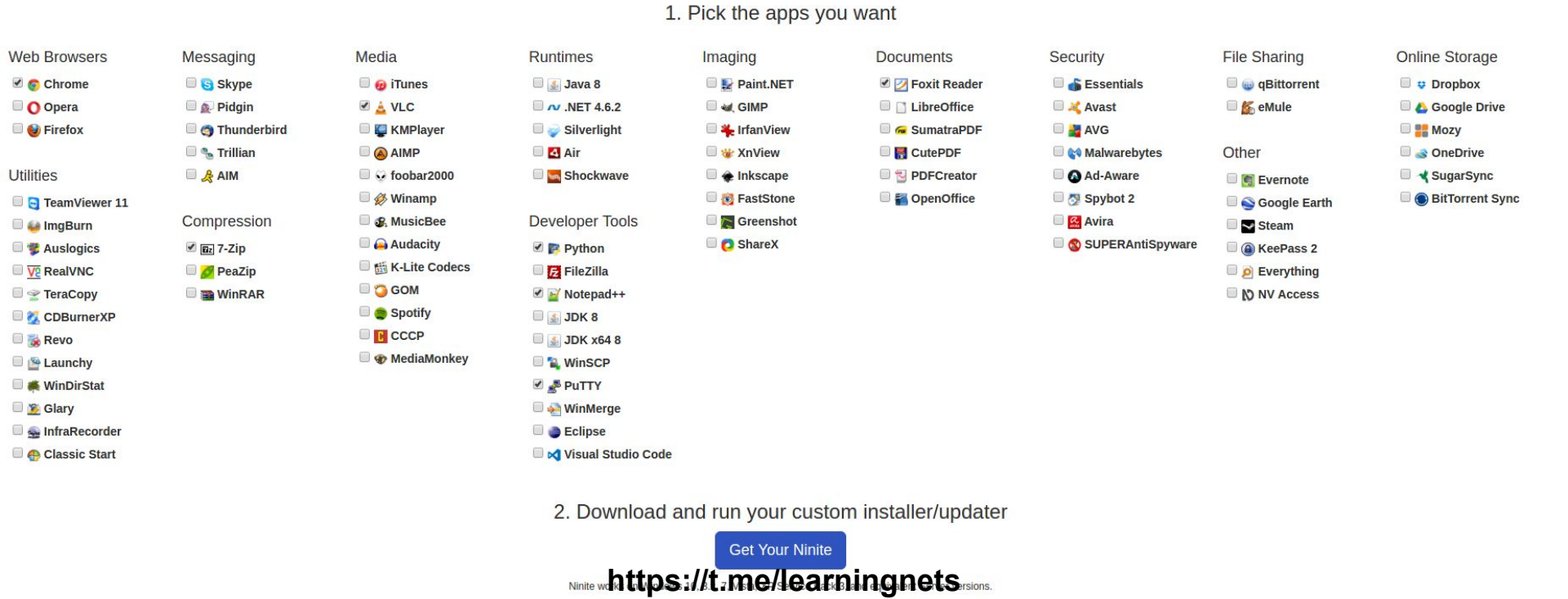
TurnKey Linux

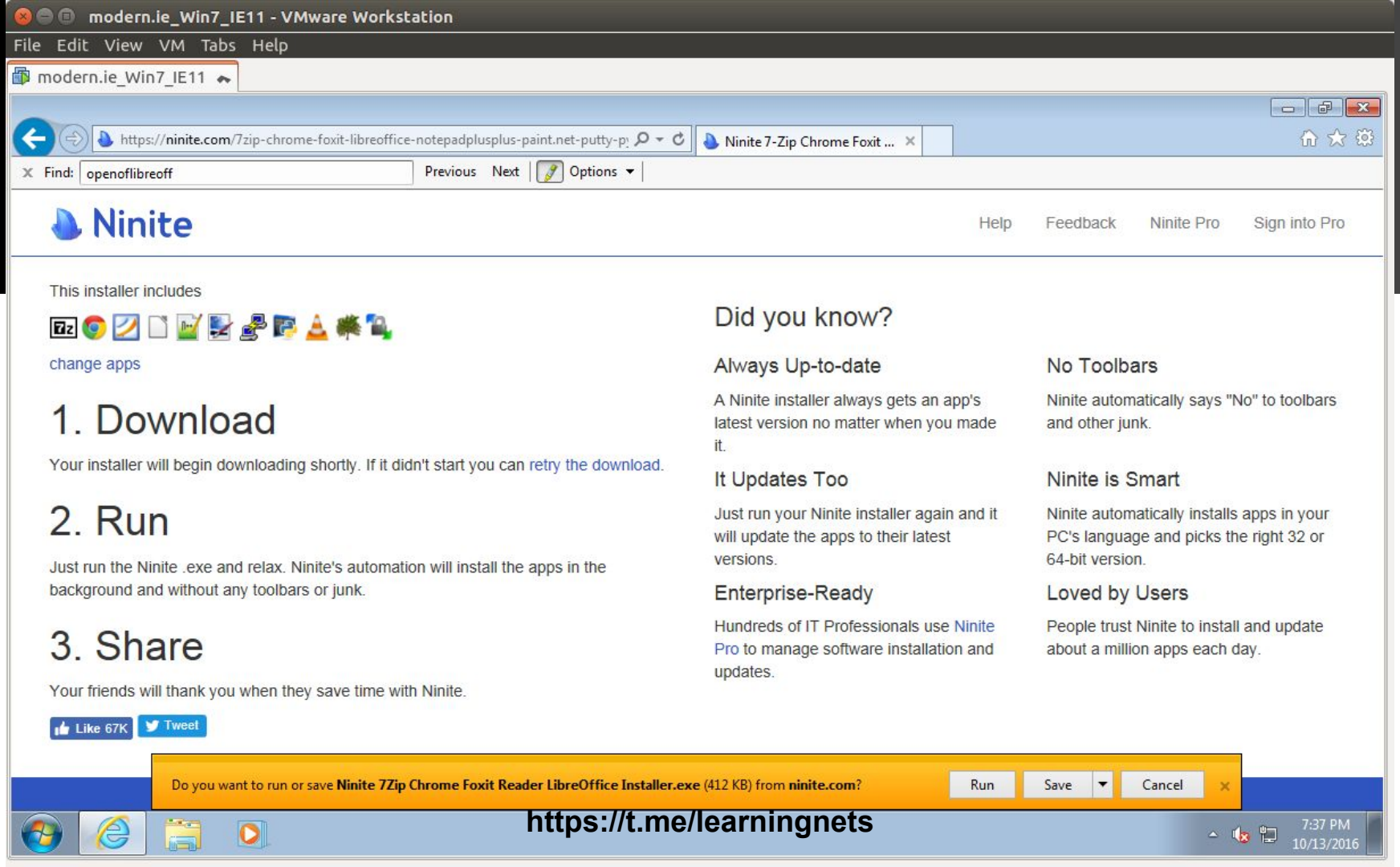


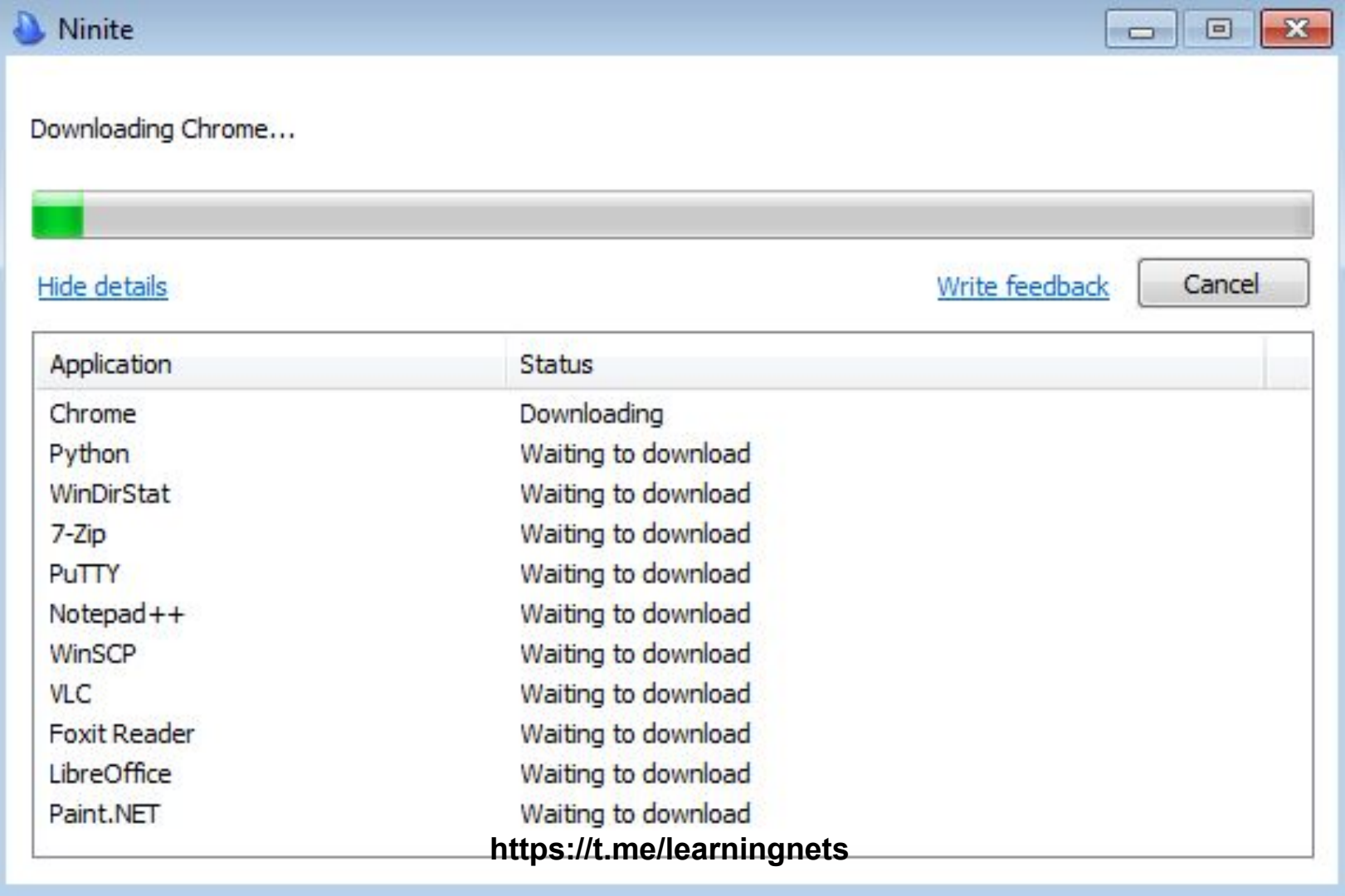
Windows software

- Ninite.com is **such** a relief here…
- Also consider Chocolatey, a package manager (like apt!) for Windows
  - https://chocolatey.org/
  - **choco install vscode** or **choco install visualstudio2019community** is *much* easier than the normal process
- Icecast 2.0.1 is a great and reliable service-side exploit (https://ftp.osuosl.org/pub/xiph/releases/icecast/icecast2_win32_2.0.1_setup.exe)
  - Metasploit: https://www.rapid7.com/db/modules/exploit/windows/http/icecast_header
  - Use this as a stand-in for any service-side exploit (i.e., instead of exploiting MS17-010)

Ninite







Stuff on the Internets

Care for your own domain?

Several Top-Level Domains are available for free:
http://www.freenom.com/en/index.html?lang=en

(including basic DNS records)

Yes! **jrmlabs.tk** is available!

1 domain in cart | Checkout

jrmlabs .tk	• FREE	USD 0.00 ✔ Selected

Get one of these domains. They are **free**!

jrmlabs .ml	• FREE	USD 0.00 Select
jrmlabs .ga	• FREE	USD 0.00 Select

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. Or Amazon EC2 for free, for a year, with some hassle (see slide notes)

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?!

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 7 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

Example Lab - Basic Enterprise Network, part 1

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 2012 R2 trial (one interface, internal network)
5. modern.ie Windows 10 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?

Example Lab - Forensic and Defense Notes

- This same lab can be used for forensics and defense, as well!
- Looking for memory artifacts? Pause the VM and copy away the .vmem file
  - It's a bit-for-bit consistent copy of memory, supported by Volatility and Rekal
- Set up centralized logging with Windows Event Forwarding
- I'd strongly recommend taking a look at @SwiftOnSecurity's sysmon configuration and sysmon itself
- Great example of defense / IR lab use from JP-CERT -
  - "Detecting Lateral Movement through Tracking Event Logs" - http://blog.jpcert.or.jp/.s/2017/06/1-ae0d.html

(More details in notes)

Individual VM Challenges

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

The SEED Project (https://seedsecuritylabs.org/) has both downloadable VM's with a specific challenge, and the complete corresponding walkthroughs.

Home | SEED Labs | Workshops | For Instructors | About | News

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)
   - For Ubuntu9.11 VM

What else can I do?

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

They 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!

2014 Holiday Hack Challenge

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 [illegible] boards, 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 ~$540 for 64 GB of RAM, 12 cores
- **Hypervisor?** VMware Workstation Pro 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?

Twitter: @jeffmcjunkin

Email: jeff@roguevalleyinfosec.com

Slides online at http://bit.ly/kickasslab

Recorded video on YouTube

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/

* 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/, find a domain to create a phishing campaign around and purchase it cheaply.

More defensive lab projects

- Please, please, PLEASE consider looking at Microsoft's LAPS:
  - https://gallery.technet.microsoft.com/Step-by-Step-Deploy-Local-7c9ef772
- 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
- Also by Neo23x0, Sigma for applying generic SIEM rules:
  - https://github.com/Neo23x0/sigma
- 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