Free Modules! Building a Course with SANS CyberAces

3RD ANNUAL

VIRGINIA CYBERSECURITY EDUCATION CONFERENCE

July 27, 2020

About me

- Background is IT Networking and Security
- ~18 years at Blue Ridge Community College as Network Engineer and Information Security Officer, retired 2 years ago
- Developed(ing) course for Shenandoah Valley Governor's School in IT Security for seniors
- Adjunct instructor at BRCC
- Contact Info
  - @JohnYork_r2 on Twitter
  - yorkj@svgs.k12.va.us

Course Origins

The best online security courses. Free.

SANS Cyber Corps ~2012
- Assisted SVGS with an evening club

SANS Cyber Aces 2013 – 2019
- Asked to develop Cyber Security class at SVGS
- Primary goal: Hands-on experience in fundamentals
- Few textbooks were/are hands-on
- Used Cyber Aces as core
- Developed many labs and modules of my own

Links! Everyone wants Links!

- SANS Cyber Aces
  - https://www.cyberaces.org/ (Home page)
  - https://tutorials.cyberaces.org/tutorials.

Streaming Tutorials

1. Introduction to Operating Systems

- Linux
  - VMware Installation and Configuration
  - OS Background & Building the Linux VM
  - Core Commands
  - Users and Groups
  - Applications and Services
  - Files and Permissions
  - Installing Software

- Windows
  - Windows Virtual Machine Installation
  - Updating Windows
  - Command Line Basics
  - File System
  - Users and Groups
  - Policies and Credential Storage
  - Registry
  - Networking and Sharing
  - Services and Processes

2. Networking

- Introduction and Layer 1
- Layer 2 - Data Link
- Layer 3 - Network, Part 1: Addressing & Masking
- Layer 3 - Network, Part 2: Routing
- Layer 3 - Network, Part 3: Communication

Links! Everyone wants Links!

- My Modules

- https://github.com/john-r2/CyberSec-Modules
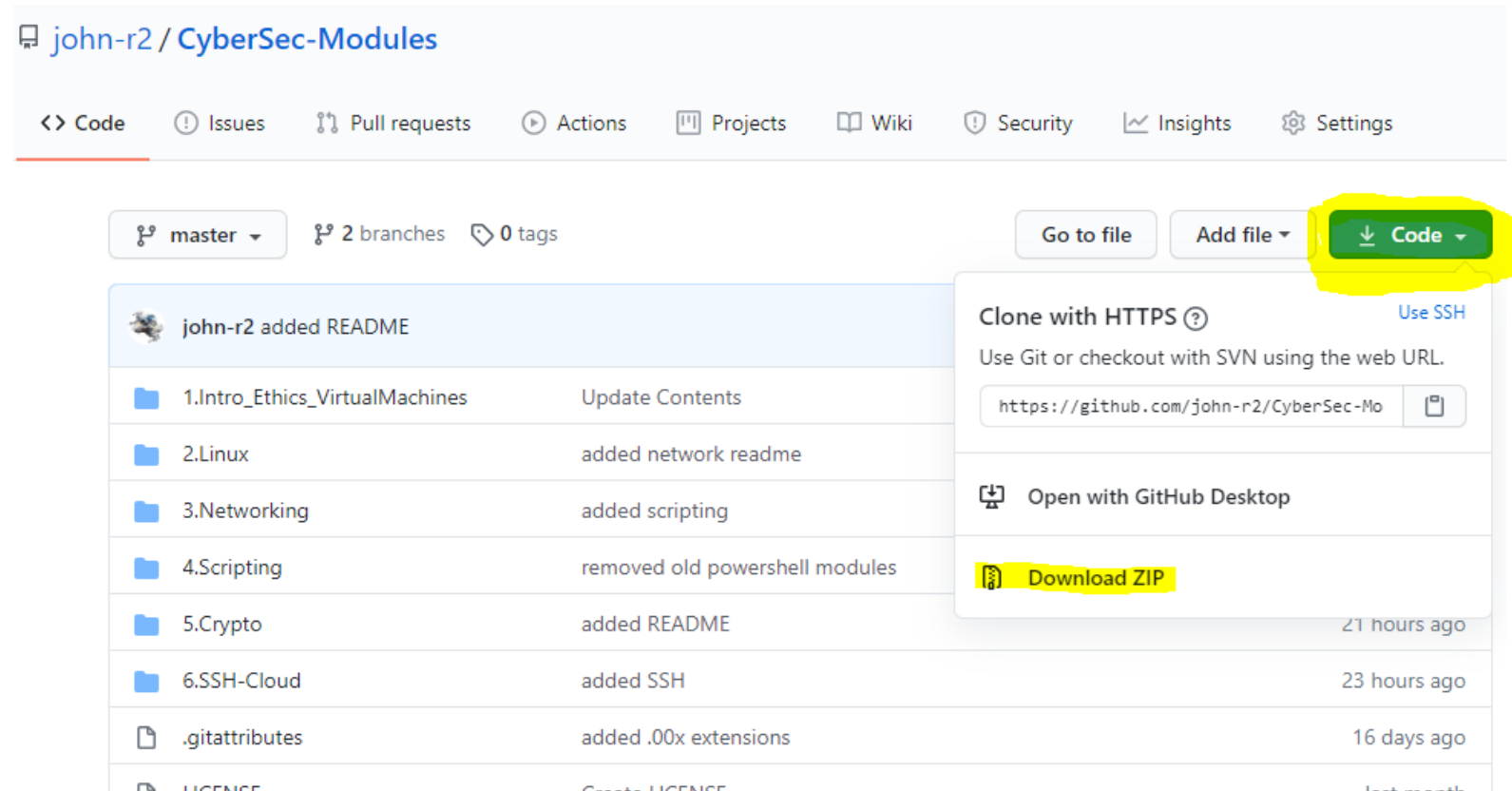
Teaching through hands-on labs

- Labs are essential for future IT workers
  - IT workers create, they don't memorize lists
  - Troubleshooting is a critical skill, difficult to teach

- Lab Goals
  - Students set up as much of their own equipment as possible
  - Labs proceed quickly and smoothly
  - There's an obvious conflict

https://krebsonsecurity.com/2020/07/thinking-of-a-cybersecurity-career-read-this/

Skill area	Percent of cybersecurity job candidates who were unable to perform even basic tasks	Percent of cybersecurity job candidates who demonstrated hands-on mastery
Common exploitation techniques	66%	4.5%
Computer architectures	47%	12.5%
Networking	46%	4%
Linux	40%	14%
Programming	32%	11.5%
Data and cryptography	30%	2%

Labs in the time of Covid-19

- Lab Types
  - Virginia Cyber Range
  - Student's personal computers
  - Cloud—AWS Educate
  - Classroom computer labs
- New problem—where will the students be?
  - Completely online
  - Half online, half in class
  - In class
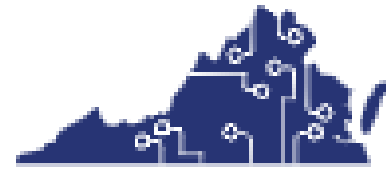
Virginia Cyber Range

- Available to all Virginia K-12/colleges (class must be cyber security)
- Pre-made VMs (Windows, CentOS, Kali, and Ubuntu)
- Pros
  - Only requires web browser and Internet connection
  - Students can work from home
  - Instructor can customize VM
- Cons
  - Students do not practice installing their own VM
- To use two VMs that communicate, find correct cyber range environment

Student personal computers

- Students install VMware Workstation Player (free) or other hypervisor
- Students create VMs as needed
  - Linux OSs are free, Windows eval downloads good for 180 days
- Pros
  - Teaches students to create their own labs
- Cons
  - Most difficult to teach
    - student errors and laptop capabilities
  - Some students do not have access to reasonable computers
    - Modern processor, >= 4 GB RAM, >= 250 GB hard disk

AWS Educate

- Teachers can sign up at https://aws.amazon.com/education/awseducate/
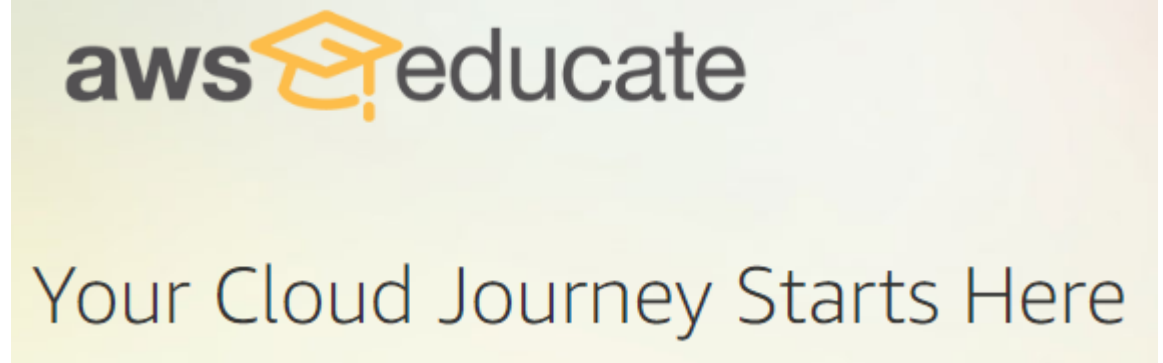
- Need to provide URL of your class on your school website

- Each student gets $50 of AWS credit by default

- Pros
  - Students create their own VM lab environments
  - Students learn cloud basics
  - Instructors can see student VMs

- Cons
  - Can be intimidating for instructors first time they use it

School Computer Labs

- A lab dedicated for your class is best
  - (hard to come by)
- Otherwise, lab software must include a hypervisor to build VMs
  - VMware Workstation Player is common
    - Required for US CyberPatriots, https://www.uscyberpatriot.org/
  - Microsoft HyperV
    - Included on Windows 10 Enterprise, Pro, or Education
    - Must be enabled
    - https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v
  - Oracle VirtualBox
    - https://www.virtualbox.org/
- Some networking labs require admin access—difficult unless lab is dedicated

Warning—Beta mode!

- I'm the only one that has taught the modules I've written
- Things change *really* fast. Labs that worked last month may blow up today
- I will be glad to assist anyone using my modules
- Twitter DM @JohnYork_r2
- Email yorkj@svgs.k12.va.us
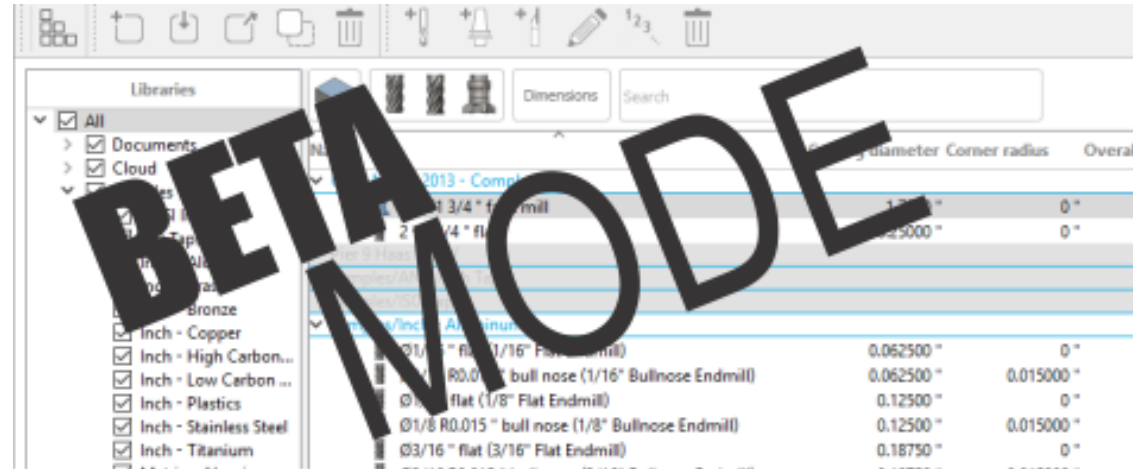
SVGS/BRCC modules

- Linux, Networking and Scripting modules expand on CyberAces modules

- No Windows module (yet) to go with CyberAces Windows module

- If you register for US Cyber Patriots, additional modules on cyber security, ethics, and Windows are available.

📁 1.Intro_Ethics_VirtualMachines

📁 2.Linux

📁 3.Networking

📁 4.Scripting

📁 5.Crypto

📁 6.SSH-Cloud

Linux Modules (1)

- CyberAces modules were not updated from 2015 until this year
  - During that time Linux moved from SysV to systemd for service control
  - I created new modules for systemd and SysV in response
- CyberAces uses CentOS, CyberPatriots competition uses Ubuntu
  - I adjusted modules for Ubuntu since my class competes in CyberPatriots
- The Linux Command Line book is very good and available for free
  - I adjusted modules to include it as well as CyberAces
  - http://www.linuxcommand.org/tlcl.php
  - https://svwh.dl.sourceforge.net/project/linuxcommand/TLCL/19.01/TLCL-19.01.pdf
- CyberAces modules have recently been updated
  - I am trying to make my modules compatible with both CentOS and Ubuntu

Linux Modules (2)

- CyberAces uses a CentOS VM
- CyberPatriots uses an Ubuntu VM
- Trying to make modules compatible with both
- Many modules follow CyberAces
- Module 4 is from The Linux Command Line
- Module 5 and 7 are new or expanded from CyberAces

📁	0.Install
📁	1.Basics
📁	10.Finding Stuff
📁	10a.CyberRangeQuiz
📁	11.Basic SSH
📁	12.Test
📁	2.Users and Groups
📁	3.Files and Permissions
📁	4.Commands Help and Path
📁	5.Apps and Services
📁	6.Process Commands
📁	7.Parsing Text
📁	8.Installing Software
📁	9.Unnecessary Services

Networking Modules

- Generally follow CyberAces, although VLAN module is new and under development
- Labs originally written for hardware switches and routers
- Expanded to use Cisco PacketTracer

0.Encapsulation
1.Physical and Hubs
2.Datalink and Switches
3.Network
4.DHCP
5.Routing Protocols
6.Transport Layer
7.Application and DNS
8.VLAN
9.Module Quiz
Allowing Ping through the Windows 10 Firewall.docx

Cisco PacketTracer

- Previously, only members of the Cisco Network Academy could get access

- My classes got access because it comes as part of Cyber Patriots

- A few months ago Cisco made it available for everyone

- https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer
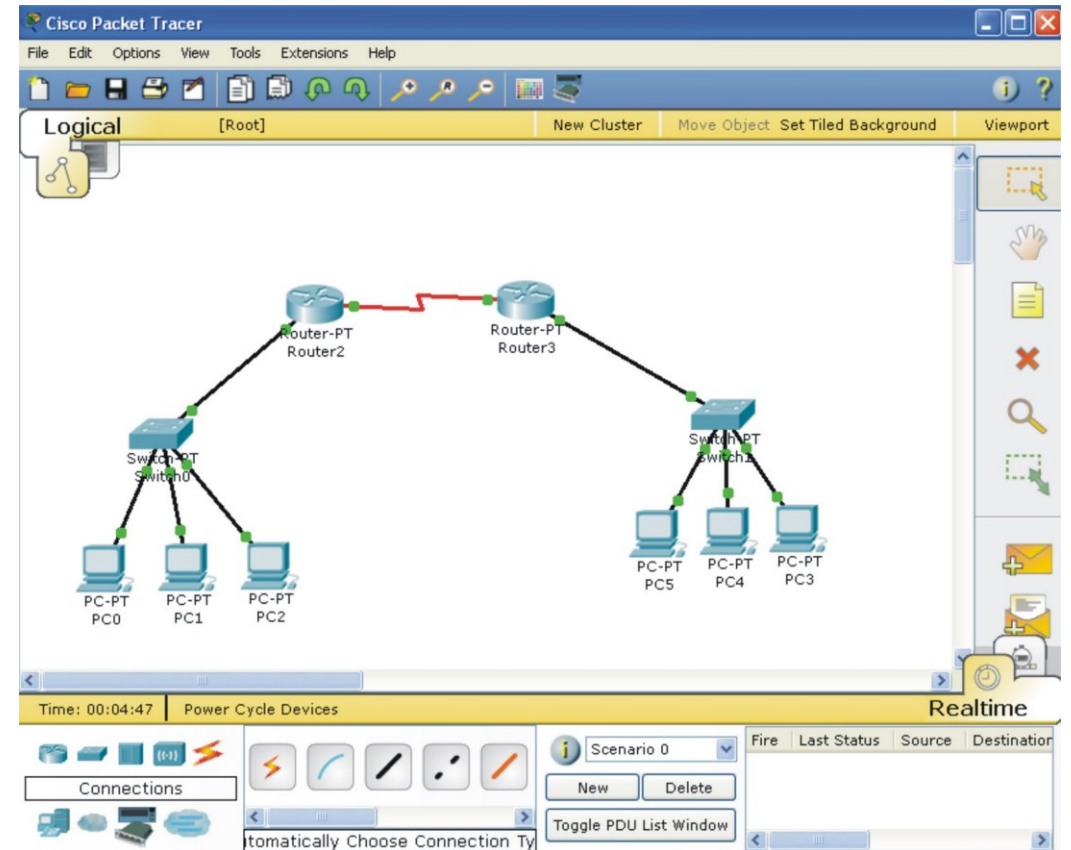
Network Labs with Hardware

- My preference. I learn better when I hold cables in my hands

- Requirements for a 12 – 15 person lab
  - 4 switches. The switches do not need to be enterprise switches with management. You can buy cheap switches at Amazon or a big box store for about $20 each.
  - ~30 Cat 5 or 6 network cables of varying length.
  - 3 routers. I prefer a Cisco 2911 router. At least 2 of the routers should have 3 Ethernet ports; one router may have 2 Ethernet ports. You can purchase these routers on Ebay for about $100 each.
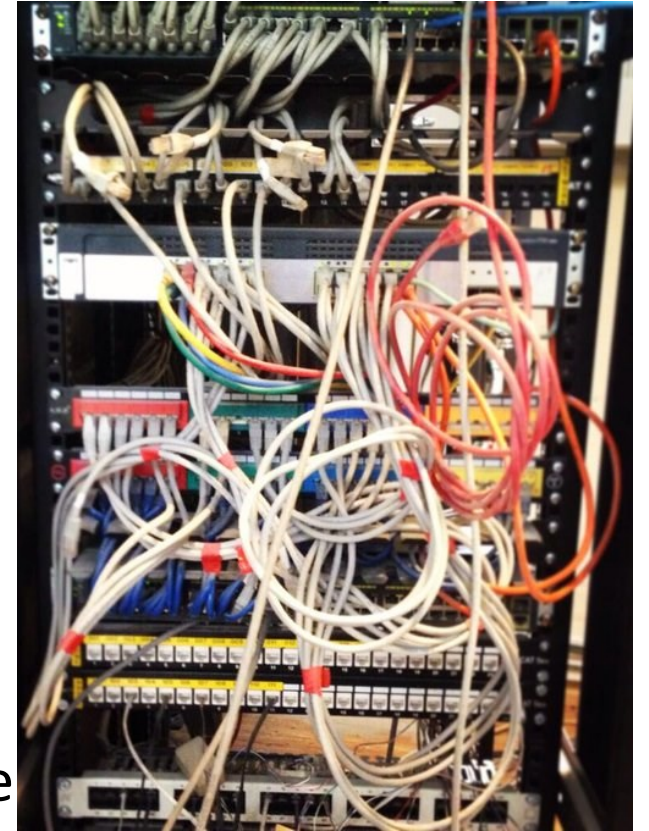
Scripting Modules (System Administration)

- BASH mostly follows Cyber Aces
  - Some additions for parsing text
- PHP was in the 2015 Cyber Aces, deleted in 2020
  - I kept the 2015 modules because I used them to demonstrate simple web vulnerabilities
  - My GitHub includes copies of old Cyber Aces PHP
  - Fun lab! Holiday Hack Trails lessons from the 2019 SANS Holiday Hack Challenge (HHC)
- PowerShell
  - Fun lab! Christmas Cheer Laser from 2019 HHC
- Python is on my to-do list
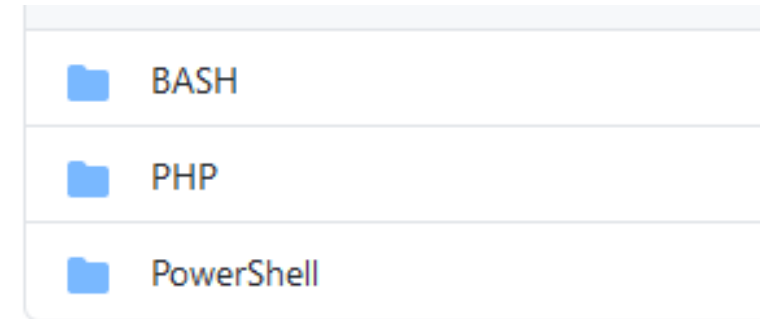
Cryptography Modules

- IMHO certification exams covering crypto are vocabulary tests
- Goals
  - Teach some of the math behind cryptography
  - Make the lessons accessible to non-math folks
  - Hands on as much as possible
  - Uses Python and PyCryptodome
- Inspired by "Understanding Cryptography" by
  Paar and Pelzl
- Terrific videos by Paar covering the book:
  - https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg/videos
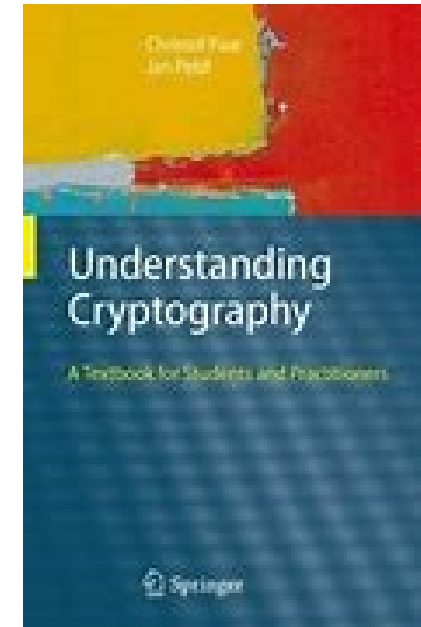
CRYPTOHACK

- Fun, always running

- Modern crypto challenges

- Not ciphers

- Range from easy/beginner to really hard

- Support available through cryptohack's Discord group

- https://cryptohack.org/

CRYPTOHACK

A fun platform for learning modern cryptography

SANS Holiday Hack Challenge by CounterHack

- Excellent real-world challenges from basic to advanced
- Range is always open
- https://www.holidayhackchallenge.com/
- "Lessonized" instructions in my GitHub
- https://github.com/john-r2/HolidayHackLessonized

Link Summary

- SANS Cyber Aces
  - https://www.cyberaces.org/
  - https://tutorials.cyberaces.org/tutorials
- My modules
  - https://github.com/john-r2/CyberSec-Modules
  - https://github.com/john-r2/HolidayHackLessonized
- KrebsOnSecurity article about need for hands-on
  - https://krebsonsecurity.com/2020/07/thinking-of-a-cybersecurity-career-read-this/
- AWS Educate
  - https://aws.amazon.com/education/awseducate/
- US Cyber Patriots
  - https://www.uscyberpatriot.org/

Link Summary (2)

- The Linux Command Line Book
  - http://www.linuxcommand.org/tlcl.php
  - https://svwh.dl.sourceforge.net/project/linuxcommand/TLCL/19.01/TLCL-19.01.pdf
- Cisco PacketTracer
  - https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer
- Understanding Cryptography by Paar and Pelzl
  - https://www.springer.com/gp/book/9783642041006
  - https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg/videos
- CryptoHack, a CTF on modern cryptography
  - https://cryptohack.org/
- SANS/CounterHack Holiday Hack Challenge
  - https://cryptohack.org/
  - https://github.com/john-r2/HolidayHackLessonized