What's ahead for Google in 2020?
&
How to Build a Cyber Range

Presented by:

Kevin A. McGrail

kmcgrail@InfraShield.com

Google Cloud

Study Jams

CITY OF Thunder Bay
Superior by Nature

GDG

Lakehead UNIVERSITY

About the Speaker

Kevin A. McGrail
Director, Business Growth @ InfraShield.com

Member of the Apache Software Foundation
Release Manager for Apache SpamAssassin
Google G Suite TC, GDE & Ambassador.

Google Developers Experts 2019
G Suite Product GDE

https://www.linkedin.com/in/kmcgrail

GDG

Lakehead University

Some New Things for Google in 2020

CES Jan 2020

- No new new hardware at CES!

- Google Assistant & AI
  Hey Google, Read this Page

  Hey Google, turn on the lights at 6AM

  Hey Google, Leave a Note...

CES Jan 2020 (continued)

Google Assistant & AI

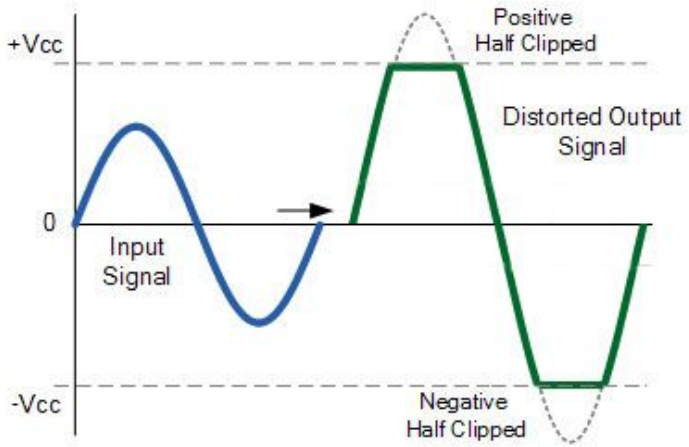
- Speed Dial
- Interpreter Mode (Transcript Mode)
- Hey Google, that wasn't for you

Live Transcripts

Hangouts Meet w/Captions

Recorder App w/Transcriptions

Live Transcribe



Coming Next...: https://mashable.com/article/google-translate-transcription-audio/

TIP: Whisper & Clipping

GDG

Lakehead
UNIVERSITY

Streaming Games?

- Google Stadia

GDG

Lakehead UNIVERSITY

Android Tablets

No more Android Tablets?

AI AI AI AI AI

Looker acquisition for 2.6B

https://www.cloudbakers.com/blog/why-cloudbakers-loves-looker-for-business-intelligence-bi

From Thomas Kurian, head of Google Cloud: “focusing on digital transformation solutions for retail, healthcare, financial services, media and entertainment, and industrial and manufacturing verticals.

He highlighted Google's strengths in AI for each vertical, such as behavioral analytics for retail, compliance for financial services, and the genomic data model for healthcare providers. ” written by Liam Tung.

What else?

Amazon will be the biggest threat

GDG

Lakehead UNIVERSITY

Google Graveyard

In Memoria

https://techcrunch.com/2020/01/07/heres-everything-google-announced-at-ces-2020/

Particularly sad about Google Cloudprint

Elephant in the Room

Google Cloud Layoffs?

Google Cloud (10b) vs Azure (50b) vs AWS (40b)

- Planet-scale

- Reselling internal products

https://www.zdnet.com/article/google-cloud-cuts-jobs-in-restructure-despite-growth/

What/Why/How to Build a Cyber Range?

Cyber Ranges: What's the Goal?

GDG

Lakehead UNIVERSITY

Quis Custodiet Ipsos Custodes?

USENIX / Systems Administrator’s Code of Ethics
https://www.usenix.org/system-administrators-code-ethics

Q/EH® Qualified/ Ethical Hacker
CEH Certified Ethical Hacker

GDG

Lakehead UNIVERSITY

Building a Cyber Range

“If you can’t build a network, you can’t secure a network…” - KAM

Materials needed:

Old Laptop/Chromebook, Raspberry Pi (full kit), Network Switch, Network Patch Cables, Commercial Off the Shelf (COTS) Router, Network Printer, USB Keyboard, Mouse, SD Card, SD Card Reader/Writer

Idea: Used Chromebook in Dev mode and install Ubuntu - See Appendix B

Basics of Networking

Basic Internet Protocol (IPv4)
  0.0.0.0 to 255.255.255.255
  Class A 1.X.X.X - Class B 1.1.X.X - Class C 1.1.1.X
  Ipconfig (Windows)/ifconfig or ip addr (*nix)
  IP Address, Netmask & your Gateway
  Dynamic Host Configuration Protocol (DHCP) & 169 Addresses
Routers - What is a COTS router? One device that does it all.
Request for Comments (RFC) 1918 & Network Address Translation (NAT)
Network Printers
Access Points & Invisible Wires
Loopback / 127.0.0.1 aka Localhost.localdomain

Shopping Tips

Selection of equipment for Cyber Range

Used vs New? You can buy everything on our list for ~$550 new w/tax & shipping

- Use expendable equipment in case you brick it
- “Replaced with known good”

Newegg/Fry’s/MicroCenter/Amazon/eBay/BestBuy

Cabling - What is a patch cable?

Network Switches

Switches vs Hubs

Can you even buy a Hub?

Span or Mirror Ports

Switches/Virtual LANs (VLANS)- Managed vs Unmanaged Switches

GDG

Lakehead UNIVERSITY

Story Time

The Nobel Prize in Mathematics aka the Fields Medal

GDG

Lakehead UNIVERSITY

Shopping List from Jan 2020

Patch Cables - Cat 5e Network:
https://www.amazon.com/Cable-Matters-8-Pack-Snagless-Ethernet/dp/B00HSSRWDU/

COTS Router:
https://www.amazon.com/NETGEAR-R6700-Nighthawk-Gigabit-Ethernet/dp/B00R2AZLD2/

Unmanaged Network Switch:
https://www.amazon.com/NETGEAR-16-Port-Gigabit-Ethernet-Unmanaged/dp/B01AX8XHRQ/

Network Printer (this one does NOT have WiFi):
https://www.amazon.com/Canon-imageCLASS-MF236n-Mobile-Printer/dp/B01K1KUQHK/

Shopping List (Continued)

Raspberry Pi:
https://www.amazon.com/CanaKit-Raspberry-Premium-Supply-Listed/dp/B01C6EQNNK/

Micro SD Card:
https://www.amazon.com/SanDisk-Ultra-microSDXC-Memory-Adapter/dp/B073JWXGNT/

SD Card Writer/Reader:
https://www.amazon.com/UGREEN-Reader-Adapter-5Gbps-Simultaneously/dp/B01ARAH6O0/

Raspberry Pi 4 model that costs $10 more:
https://www.amazon.com/CanaKit-Raspberry-1GB-Basic-Starter/dp/B07VWBHPMM/

Shopping List (Continued)

Monitor: https://www.amazon.com/gp/product/B07TS2ZHZX/

HDMI Cable: https://www.amazon.com/gp/product/B014I8SSD0/

USB keyboard/USB mouse - Included with monitor link above

Chromebook:https://www.amazon.com/Lenovo-ThinkPad-Chromebook-Dual-Core-1-5GHz/dp/B07B3LZD83/

~~https://www.amazon.com/Samsung-Chromebook-XE501C13-K02US-Dual-Core-Charcoal/dp/B07G576WS1/~~ - Example of a bad choice due to a lack of ethernet port & Crouton support

Shopping List Savings

Find a used HDMI Monitor or Use a Keyboard/Video/Mouse (KVM) Switcher

Use a spare keyboard & mouse instead of something new.

Skip the network printer

Skip the switch and/or try to find a used, managed switch on eBay

Ask around for an old Windows 7 laptop you can reload Linux on and repurpose

HINT: Win7 EOL on Jan 14

Basic Security Intro

Ports - Telnet Demonstration: Telnet to port 25 and do a manual SMTP injection

Port Scanning - nmap demo of a known safe system to scan

Honeypot & Sacrificial Lambs

Syn/Ack & SynFlood - Basic demonstration of how a DoS works

What's a DDoS?

How not to have the FBI visit you...

Follow an ethics guideline
https://www.usenix.org/system-administrators-code-ethics

Practice your offensive cyber with the range disconnected from the internet

Don’t run scripts or snippets of code from the internet that you don’t understand

Practice resetting your cyber range from scratch using new SD Cards for the Raspberry Pi and reloading your OS on the Chromebook, etc.

Don’t scan systems you don’t own! This includes systems in the cloud like AWS where you are likely breaking Terms and Conditions to scan things.

A Little about DNS on your Cyberrange

DNS is a Domain Name Server - Changes Names into Numbers

Record Types - A/CNAME/MX/PTR

Hosts files can be used to override DNS resolution

Images and Packages

Balena Etcher / Rufus / dd

What is a .ISO Image?

Minimal Images

Packages & Package Managers: apt-get / yum

.Spec files

Pop Quiz

What is the Most Secure Password from the list below and why?

1 - Password

2 - Password1234

3 - CaRoLiNe!

4 - MyWeddingAnniversary04-01-00

5 - P@SSw0rd!M0nd@y2020-8451234

GDG

Lakehead UNIVERSITY

PCCC Cyberrange Goals/Tests

Test 0: Install Raspbian on the Raspberry Pi

Test 1: Build a self-contained network with no internet access with Dynamic IP from the COTS router using cables

Test 1a: Add a wireless connection to the network

Test 2: Change the laptop and printer to static IPs

Test 2a: Discuss IPv4 Network Blocks

GDG

Lakehead UNIVERSITY

PCCC Cyberrange Goals/Tests (Continued)

Test 3: Be able to print from the laptop to the network printer

Test 4: Explain what is NAT

Test 5: Diagram your current network setup using LucidCharts

Test 6: Install the range with Double NAT to have internet access

GDG

Lakehead UNIVERSITY

PCCC Cyberrange Goals/Tests (Continued)

Test 7: Explain RFC 1918 Addresses

Test 8: Switch out your COTS router to a device running pfSense (protectli, old workstation/server with two Network Interface Cards (NICs), etc.)

Test 9: Explain the difference between a hub and a switch and how you might implement this on a modern cyberrange

Test 10: Explain the difference between a firewall, router, switch & access point

Now What?

Add a machine for the range to run insecure images and practice offensive techniques. IMPORTANT: Make sure to Disconnect it from the internet

Where to get images? VulnHub has a lot of images. Metasploitable & Mr. Robot are good images to start with!

Or use Hack the Box if you are looking for something simpler.

Replace the COTS Operating System on the COTS router such as DD-WRT (intermediate level task)

Replace the COTS router with an old PC with two NICs running pfSense (advanced level task)

GDG

Lakehead UNIVERSITY

Thanks!

Image Credits:

KAM photo taken by Ted King, used with permission.
https://imgs.xkcd.com/comics/devotion_to_duty.png CC BY-NC 2.5
Company logos used to represent the firms and do not imply any approval
Stadia advertisement used under fair use.
Clipping image from https://www.mtx.com/library-clipping

Thanks to:

Thad Bogner for his review and comments!

Also thanks to Collin Fields, Georgia Smith and Cameron Stanley for being guinea pigs with our cybercurriculum.

https://www.blog.google/products/assistant/ces-2020-google-assistant/
https://techcrunch.com/2020/01/07/heres-everything-google-announced-at-ces-2020/

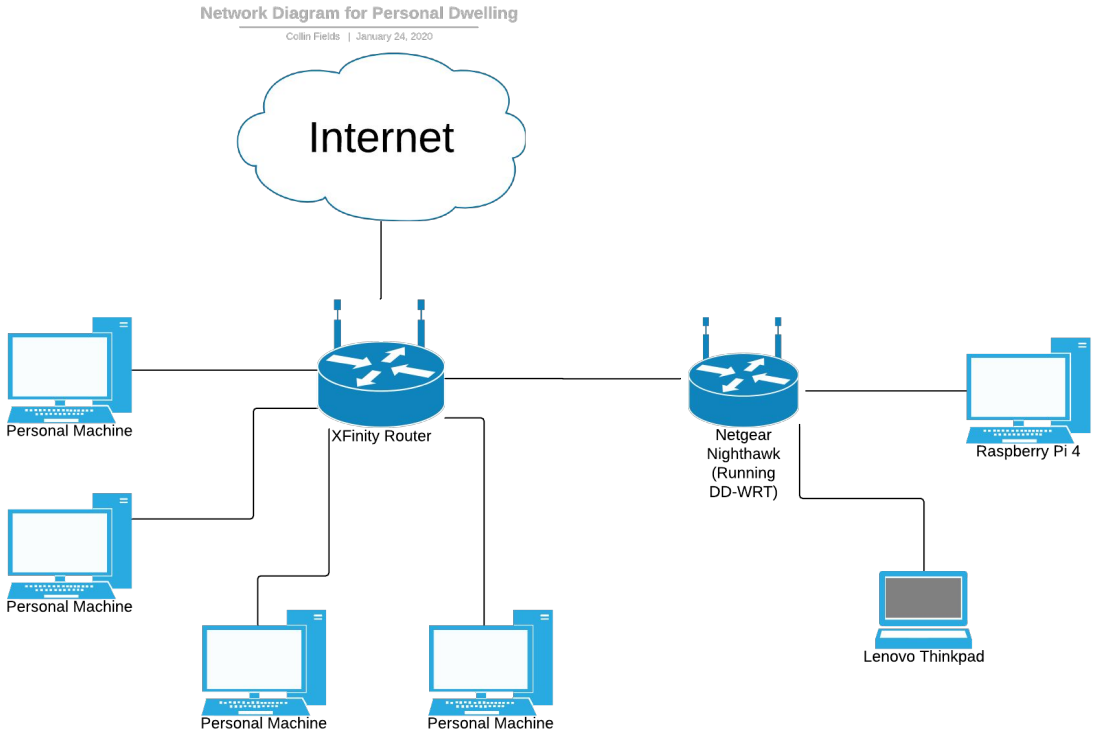
Kevin A. McGrail
www.linkedin.com/in/kmcgrail

GDG

Lakehead UNIVERSITY

Appendices

Appendix A: Sample Diagram



Appendix B: Getting Your Chromebook Ready for A Cyber Range

Thinkpad X131e Chromebook

Georgia Smith, PCCC

Notes about this Chromebook

- Amazon Link: https://www.amazon.com/Lenovo-ThinkPad-Chromebook-Dual-Core-1-5GHz/dp/B07B3LZD83/ref=sr_1_1?keywords=lenovo+thinkpad+renewed&qid=1578590523&sr=8-1
- No Longer Supported by Google - very cheap option
- Ports
  - 1x USB - 2.0
  - 2x USB - 3.0
  - 1x VGA
  - 1x HDMI
  - 1x Ethernet
  - 1x Aux

Part 1 - Developer Mode

“Chrome OS Developer mode is a special mode built into All Chromebooks which allowing users and developers to access the code behind the Chrome Operating System and load their own builds of ChromeOS. This mode also allows you to install dual-boot or another Linux system like Ubuntu that runs parallelly with Chrome OS.”

- Đinh Thành via https://medium.com/@dihuta/turn-on-developer-mode-on-chromebook-bd8a05c31bf9

Part 1 - Developer Mode

- Turn off, remove battery, unplug power
- Within 20 seconds of returning power press esc and the 'refresh' button (equivalent to f3) and POKE (do not hold) the power button
- Upon seeing recovery '!' press ctrl+d then press enter to turn off OS verification
- NOTE: On every boot a screen will ask confirming to keep OS verification off - just press Ctrl+D or wait 30 seconds
- For Specifics on this Model:
    - https://www.chromium.org/chromium-os/developer-information-for-chrome-os-devices/lenovo-thinkpad-x131e-chromebook

Part 2 - Chrome Shell “Crosh”

- On boot plug in ethernet
- Choose login mode (I used Guest Mode)
- Enter crosh shell with Ctrl+Alt+t and then typing ‘shell’ and pressing enter
    - This is the linux terminal, it can also be accessed with Ctrl+Alt+F2 (Forward Arrow) at boot with no login - recomended if going straight to Part 5 - Flashing Bios

Part 3 - Crouton

- “ChRomium Os Universal chrooT envirONment”
    - via https://github.com/dnschneid/crouton
- Allows user to switch between Chrome and Linux OS
- We used xfce desktop environment with Ubuntu 16.04

Part 3 - Crouton

- https://goo.gl/fd3zc
    - Crouton download link via https://github.com/dnschneid/crouton
- sudo sh -e ~/Downloads/crouton -t xfce
    - “~/Downloads/crouton” should be YOUR local download of crouton
- sudo startxfce4
    - Starts Crouton Process
- Ctrl+Alt+Shift+Back and Ctrl+Alt+Shift+Forward
- ^For ChromeOS ^For Ubuntu 16.4 xfce

Part 4 - Removing Crouton

- Enable OS Verification
- Reboot into Recovery Mode
- Re-enable Developer Mode

Part 5 - Flashing Chromebook BIOS

WARNING - THIS HAS THE POTENTIAL TO BRICK YOUR DEVICE AND INCLUDES HARDWARE MODIFICATION DO NOT CONTINUE UNLESS YOU FEEL COMFORTABLE WITH THE STEPS!!!!

Part 5 - Flashing Chromebook BIOS

- Changes Boot Protocol and Basic Firmware which can be brick laptop
- Create backup beforehand!
- Requires turning off the ‘write protect switch’
  - See: https://forums.lenovo.com/t5/ThinkPad-Chromebooks-11e-X-and/write-protection-switch-on-lenovo-x131E/td-p/4353761
  - Note: Crouton is an acceptable alternative! Don’t feel you need to do this!

Part 5 - Flashing Chromebook BIOS

Requires:

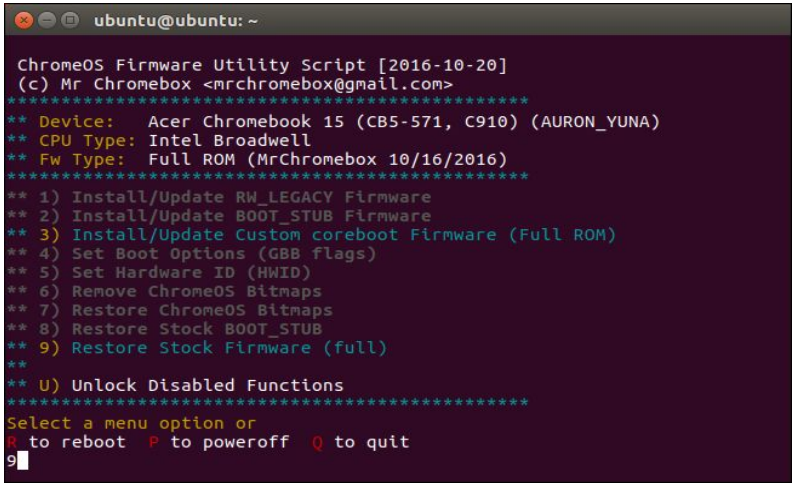
- Screwdriver for accessing motherboard (see link in previous slide)
- USB Flash Drive with Linux ISO
- USB Flash Drive for Chrome Stock Firmware Backup
- USB Flash Drive for Reinstall of Chrome OS (NOTE: can reuse Linux Bootable Drive)

Part 5 - Flashing Chromebook BIOS

- Download Linux Distribution
  - Ubuntu: https://ubuntu.com/download/desktop
- Make Bootable USB with Rufus/Balena Etcher/dd

Part 5 - Flashing Chromebook BIOS

- Enter Bash Terminal (See Slide 5)
- Run: cd; curl -LO https://mrchromebox.tech/firmware-util.sh && sudo bash firmware-util.sh
- Enter Option 3) Install/Update Custom coreboot Firmware (Full ROM)



Note: Also seen as 3) Install/Update Full ROM Firmware

Image via: https://www.howtogeek.com/279308/how-to-restore-your-chromebooks-original-bios-and-software/

GDG Lakehead University

Part 5 - Flashing Chromebook BIOS

- Follow Directions on the Screen
- Be sure to say yes to making a backup copy of your stock firmware and keep your usb in a safe place! This ensures you are able to get back chromeOS!
  - If you reuse an old flashdrive make sure you wipe it first
- When back to main menu press R for reboot

Part 6 - Ubuntu Install

- Upon Reboot Press ESC to enter Boot menu
  - Make sure to have your ubuntu flash drive plugged in! If not reboot, plug in USB, and re-enter Boot Menu
- Choose your drive on the boot menu to begin Ubuntu Install
- Follow Instructions to finish installation
  - Recommend Minimal Installation and Downloading updates during install

Part 7 - Recovery of Chrome OS

- Run: cd; curl -LO https://mrchromebox.tech/firmware-util.sh && sudo bash firmware-util.sh
- Option 9) Restore Stock Firmware (full)

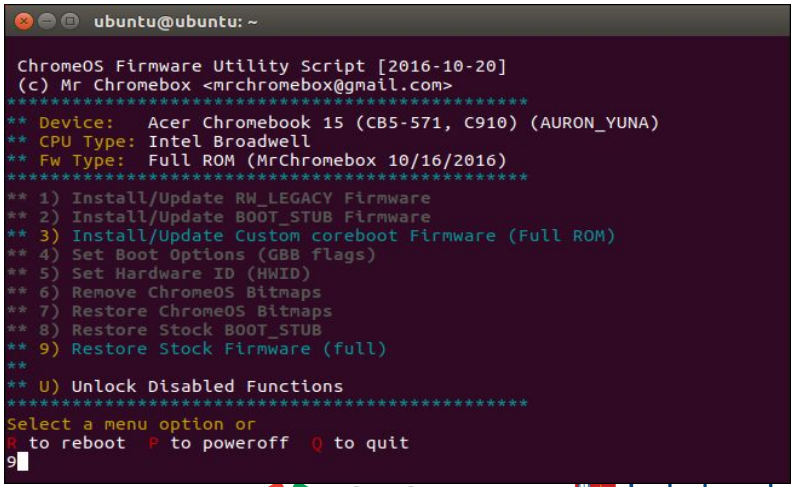


Image via: https://www.howtogeek.com/279308/how-to-restore-your-chromebooks-original-bios-and-software/

Part 7 - Recovery of Chrome OS

- https://chrome.google.com/webstore/detail/chromebook-recovery-utili/jndclpdbaamdhonoechobihbbiimdgai?hl=en
- Follow directions in chromebook utility app to make your recovery drive
- Reboot Chrome into Recovery mode and plug in recovery drive
- Follow directions and chrome stock firmware will be back on you computer

Appendix C: Cyber Ranges Pictures