# Security Tapas
# A Series of Small Dishes to try for Security

by Aaron Grothe
www.grothe.us
May 26th, 2022

# Introduction

Tapas?

I can't spell Potpourri without a spell checker and I'm not sure if it is the right word to use either.  So I decided to go with Tapas.

Tapas is an appetizer or snack in Spanish cuisine.  A bunch of small dishes are served.  So this is a series of small security tips.

# Introduction (Continued)

If you have questions/comments please feel free to ask them anytime.  You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people please let the group know.

Hopefully this will be an interactive and productive session.

The slides for this are at my site https://www.grothe.us in the presentations section

# Our Meal has the Following Courses

- News & Information
- Training
- Utilities
- Miscellaneous

# News & Information

- College shuts down over ransomware
- Huawei Annual CyberSecurity Report
- NIST Small Business Cybersecurity Corner

# College shuts down over ransomware.

- This is a story of a college shutting down after a ransomware attack.
- CNET claims that 1 in 5 companies that are a victim of ransomware shut down.
- Lincoln College announced they were shutting down after 157 years
- Ransomware attack shut down their IT systems for approximately 3 months
- College paid ransomware of less than 100k, attack originate in Iran

# Huawei Annual Cyber Security Report

- Huawei has severe restrictions on doing business in the United States.
- They also have very strict requirements for doing business in the UK.
- The Huawei Cyber Security Evaluation Centre (HCSEC) issues annual reports on their current cybersecurity status
- These annual reports provide great insights into how a multi-national company deals with CyberSecurity

# NIST Small Business Cybersecurity Corner

- The NIST Small Business Cybersecurity Corner is a great resource for small businesses.
- A lot of this information applies to businesses of any size, but is really useful for smaller groups
- The information is written to be read by business people, not just Cybersecurity experts
- Is a great resource that helps a lot
- If you know of a small business/group/non-profit recommend you point them to this site

# NIST Small Business Cybersecurity Corner

Some of the items included at their site

Planning Guides
- Hiring a webhost
- FCC Cyber Planner
- Cyber Insurance

Responding to a Cyber Incident
- Data Breach Response
- Recovering from an incident
- Fraud Support

# Training

You should always be learning new things.  One good thing to come out of Covid was that a lot more places support remote testing and a lot of conferences are adding online options :-)

The following resources are all free and recommended.

# Training

- Microsoft Build Cloud Skills Challenge May 2022
- Microsoft Virtual Training Days
- Oracle Cloud Infrastructure Foundations
- Cybrary.it
- Cybermentor
- Toastmasters
- Six Sigma Yellow Belt
- Scrum Fundamentals Certified
- Other VMEdu certifications
- ISACA Engage

# Microsoft Build Cloud Skills Challenge May 2022

Between now and June 21 finish one of the 8 Microsoft Cloud Challenges

- Microsoft 365: Building Applications and Solutions Challenge
- Azure Developer Challenge
- IoT Developer Challenge
- Azure Cosmos DB Developer Challenge
- Power Platform: Functional Consultant Challenge
- Power Platform: App Maker Challenge
- Microsoft Security: Who Hacked? Challenge
- Data and AI: Who Hacked? Challenge

# Microsoft Build Cloud Skills Challenge May 2022

After that you'll get a Voucher for any of the 12 following certifications

- AI-102: Designing and Implementing a Microsoft Azure AI Solution
- AZ-204: Developing Solutions for Microsoft Azure
- AZ-220: Microsoft Azure IoT Developer
- AZ-400: Designing and Implementing Microsoft DevOps Solutions
- DP-420: Designing and Implementing Cloud - Native Applications Using Microsoft Azure Cosmos DB
- MS-600: Building Applications and Solutions
- PL-100: Microsoft Power Platform App Maker
- PL-200: Microsoft Power Platform Functional Consultant
- PL-300: Microsoft Power BI Data Analyst
- SC-200: Microsoft Security Operations Analyst
- SC-300: Microsoft Identity and Access Administrator

# Microsoft Build Cloud Skills Challenge May 2022

There are 3 that stick out here

- AZ-400: Designing and Implementing Microsoft DevOps Solutions
- SC-200: Microsoft Security Operations Analyst
- SC-300: Microsoft Identity and Access Administrator

SC-200 is a VERY popular certification that will you learn a lot for during the training.  Also recommend the other two as well.

DevOps leads to DevSecOps leads to money :-)

# Microsoft Build Cloud Skills Challenge May 2022

Microsoft has a couple of other programs to take a look at as well

- Microsoft 30 for 30 - an intensive program where you go through their self-paced training.  After completing it you get a 50% off voucher for a certification exam.  Most of them are $165.00 so $82.50 instead
- Microsoft in the fall will be having Microsoft Ignite - which usually has a similar challenge and you'll probably be able to get a free certification voucher from that as well.  That is how I got my AZ-104 Certification

# Microsoft Virtual Training Days

- Microsoft offers a bunch of online training for various topics.
- Some of them have optional certifications available
- If you see the word fundamentals in the description there is probably a certification available if you take the training.  Normally the fundamental exams cost $99

Here are 3 of them:

- Security, Compliance, and Identity Fundamentals - SC-900
- Azure Fundamentals - AZ-900
- AI Fundamentals - AI-900

# Microsoft Virtual Training Days

There are also some other security training available as well

- Zero Trust
- Modernize Security and Defend Against Threats
- Protect Data and Manage Risk

Nice thing about these training sessions is they are usually 2 half days and have a lot of good content.  Also getting a few certs as well doesn't hurt.

SC-900 and AZ-900 are both worthwhile certs to have and you'll learn a lot along the way

# Oracle Cloud Infrastructure Foundations

Oracle has a bunch of Oracle Cloud Infrastructure certifications.

At the end of 2021 they made 17 of them freely available. I got 12 of the 17 done before they were no longer available for free.

The Oracle Cloud Infrastructure Foundations exam is going to be being refreshed in June. It is still available for free.

If you combine their online training with their always free cloud tier you can get a bit of hands on training.

# Cybrary.it

Cybrary.it is an online training site.

- They have a lot of online content available for free
- They also have a paywall and you can get completion certificates for various courses from them
- Good resource to use

I used their materials years ago to study for the ITIL foundations exam as most of the alternative training materials were not great

# The Cyber Mentor

The Cyber Mentor is a youtube channel that has a lot of very good content on it.

3 Videos that I really enjoyed on it

- Hiring and Getting Hired in Cybersecurity
- How to be an Ethical Hacker in 2022
- Ethical Hacking in 12 Hours

The Cyber Mentor also has a company TCM Security and TCM Security Academy

# The Cyber Mentor

TCM Academy has an interesting certification they offer.

The PRACTICAL NETWORK PENETRATION TESTER (PNPT). It is $300.00 for the exam only.

It is one I'm considering taking in late 2022.

# Toastmasters

Quite simply one of the best investments you can make in yourself is working at being a better speaker.

Toastmasters is a group that works on helping people speak better.

I'm a member of the Tech Talker's Toastmaster group - we're a group that meets the 2nd and 4th Friday of the month over the lunch time hour over zoom.

We try to be a bit more technical in our talks.  Highly recommend them.

# Six Sigma Yellow Belt

Six Sigma is a set of processes for process improvement. Based on improving quality and reducing defects.

There are a whole lot of levels for Six Sigma.  You can get the Six Sigma Yellow Belt from vmedu for free.

I initially earned this years ago when a manager of mine, was very interested in this process and I figured it would help me impress him :-)

# Six Sigma Yellow Belt

Six Sigma is a set of processes for process improvement. Based on improving quality and reducing defects.

There are a whole lot of levels for Six Sigma.  You can get the Six Sigma Yellow Belt from vmedu for free.

I initially earned this years ago when a manager of mine, was very interested in this process and I figured it would help me impress him :-)

# Scrum Fundamentals Certified

There are several groups that offer Scrum Certifications. ScrumStudy is one of them.

ScrumStudy makes their ScrumStudy SBOK (Scrum Body Of Knowledge) guide freely available.

The Fundamentals class is nice as it has online training associated with it.

Covers a lot of stuff.

# Other VMEdu certifications

Six Sigma Yellow Belt and Scrum Fundamentals are both provided by VMedu

VMedu offers several other certifications as well

SMstudy Certifications
- Digital Marketing Fundamentals
- Marketing Research Fundamentals
- Marketing Strategy Fundamentals
- Corporate Sales Fundamentals

NGStudy Certifications
- Negotiation Associate

# Isaca Engage

Isaca Engage home page is a community that is used for doing a lot of things

- Whitepaper reviews
- Chapter Award Reviewers
- Training opportunities (bootcamps)
- Mentor program - sounds very interesting

# Utilties

- Ventoy
- Read Only USB Drives
- Kali Linux

# Ventoy

Ventoy is a simple utility that lets you put multiple .iso/.img/.vhd files onto a single USB drive and chose between them when you boot the drive

Highly recommend you give this a spin a lot easier that using etcher to keep rewriting your usb stick all the time

# Read Only USB Drive

Kanguru and a couple of other companies still manufacture usb drives with a physical switch that can be used to flip them to be read only

One of these can be a very useful tool to make sure you can safely move data around

BTW - DO NOT Try this with SD Cards - The "write protect" switch on an SD card is only a suggestion you can still write to the SD card. E.g. The Canon Hack Development kit requires you to flip the write project switch to start its software

# Kali Linux

Kali Linux is one of the best security tool distributions available.  They have a lot of tools installed and they are updated regularly.

A couple of other popular distros

- blackarch - Arch based distro - lot of good tools along with all the power/utilities of Arch Linux
- Parrot Linux - another tools distro
- Pentoo - Penetration Toolkit based on Gentoo

Throw them all in ventoys and pick whichever one is your favorite :-)

# Miscellaneous

Couple of other interesting things

- Fedora Silverblue
- Redox OS

# Fedora Silverblue

This is a radical reinvention of the Linux distribution

- Silverblue is a version of Fedora Workstation that is setup as an immutable system.
- The vast majority of the system is read-only.  If you try and upgrade the system and it goes poorly, you just roll back.
- This combined with containers gives you an idea of what the future of the desktop might look like.
- The amazing thing about this is how similar it is to regular Fedora.

# Redox OS

- Redox OS - is an operating system written in the Rust programming language.
- The Rust programming language is memory and type-safe. It is also being included in the Linux kernel as a supported language
  - This will make it the second language supported by Linux
  - It will be interesting to see if there will be any code sharing between these two projects

# Summary

This is just a small smattering of dishes

The links are at the end of the talk.  I'll be posting the slides to my website https://www.grothe.us tonight as well in my presentations section.

# Q & A

Any Questions?

Thanks for listening.

# Links

College Shuts down over Ransomware

https://www.governing.com/security/lincoln-college-closure-is-just-another-ransomware-milestone#:~:text=The%20predominantly%20Black%20college%20in,Who's%20next%3F&text=Lincoln%20College%20in%20Lincoln%2C%20Ill,a%20ransomware%20attack%20last%20semester.

# Links

Huawei Annual Cyber Security Report for HSEC (UK)

https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-hcsec-oversight-board-annual-report-2021

https://www.ft.com/content/269fd590-03bf-44bc-87cd-086897c14876

# Links

NIST Small Business Cybersecurity Corner

https://www.nist.gov/itl/smallbusinesscyber

https://www.grothe.us/presentations/isc2omaha-201909-nist.pdf

# Links

Microsoft Build Cloud Skills Challenge May 2022

https://www.microsoft.com/en-us/cloudskillschallenge/build/registration/2022?ranMID=24542&ranEAID=lw9MynSeamY&ranSiteID=lw9MynSeamY-mU6MAxfcW_7.YKmATa60hQ&epi=lw9MynSeamY-mU6MAxfcW_7.YKmATa60hQ&irgwc=1&OCID=AID2200057_aff_7593_1243925&tduid=%28ir_l2lq22vkcckf60lui16n1pmgr22xvwdgavqwoazl00%29%287593%29%281243925%29%28lw9MynSeamY-mU6MAxfcW_7.YKmATa60hQ%29%28%29&irclickid=_l2lq22vkcckf60lui16n1pmgr22xvwdgavqwoazl00

# Links

Microsoft Virtual Training Days

https://www.microsoft.com/en-us/trainingdays

Oracle Cloud Infrastructure Foundations 2021 Associate

https://education.oracle.com/oracle-cloud-infrastructure-foundations-2021-associate/pexam_1Z0-1085-21

Cybrary.it

https://www.cybrary.it

# Links

Cybermentor

https://www.youtube.com/c/TheCyberMentor

https://www.thecybermentor.com/

https://academy.tcm-sec.com/

Toastmasters

https://www.toastmasters.org/Find-a-Club/07252531-tech-talkers

# Links

Six Sigma Yellow Belt

https://www.6sigmastudy.com/

Scrum Fundamentals Certification

https://www.scrumstudy.com/certification/scrum-fundamentals-certified

# Links

Other VMedu certifications

https://www.vmedu.com

Isaca Engage

https://engage.isaca.org/home

# Links

VenToy

https://www.ventoy.net/en/index.html

Kali Linux & Others

https://www.kali.org/

https://www.parrotsec.org/

https://blackarch.org/

# Links

Fedora SilverBlue

https://silverblue.fedoraproject.org/

Redox OS

https://www.redox-os.org/