25 to Try

Some Things to Know/Try for a Better 2018

by Aaron Grothe

Introduction

This talk is a collection of tips/things to try to hopefully help you have a better 2018. There are a wide of items here.

Links for the content are at the end of the slides.

The presentation and its links are available at the following URL: bit.ly/2DMeADh or you can drop me a line at ajgrothe <at> yahoo.com

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.

Free Scrum Certification

There isn't "one" Scrum certification body. There are several.

There are the Scrum Alliance, Scrum Study and some other ones as well.

Scrum Study - offers their Scrum Fundamentals Certified certification.

This a free certification. You do need to get 10 hours of study every 3 years to keep it current.

Free Scrum Certification (Cont'd)

Their site has free videos as well as their SBOK guide. Which is a very good guide to the total scrum process.

This provides a good entry to the Scrum certification process. They also have an entire hierarchy of certifications for developers, managers, coaches and so on.

I have been working through the certification but haven't completed it yet.

Six Sigma Yellow Belt

Six Sigma is a set of tools and techniques for process improvement. A lot of organizations have embraced this methodology.

The most popular levels of certifications for this are the green and black belts.

There are many groups that offer these certifications: Companies, Universities and others.

6sigmastudy.com is one of them as well

Six Sigma Yellow Belt (cont'd)

Also provided by VMedu.com the same company that runs Scrum Study.

Has online videos and other materials you need to study for the certification.

Yellow is free, simple unproctored online exam.

Read Only USB Drives

A Read Only USB Drive is a USB drive that has a physical switch that you can set that makes the usb drive read only.

Very useful when recovering a machine from an infection.

There are fewer companies making these nowadays. Kanguru, Buffalo, and a few others still make them.

Don't trust software write protect or the write-protect switches on sd cards either.

Other Browsers

Give a different browser a spin.

Mozilla's last couple of releases have been really good. Since 58 it is multi-core support has really sped things up.

Opera is chromium spin off with a lot of interesting features in it. Built-in VPN, improved privacy features and so on.

Vivaldi is another chromium spin off with a lot of interesting features as well.

Edge is also rather nice if you're on Microsoft Windows.

A few Firefox Extensions

There are a lot of extensions for firefox. Here are a few:

A lot of these extensions have equivalents for Google Chrome:

Multi-Account Firefox

Lets you create separate environments for banking/browsing/research/work, etc. Not perfect but just a part of defense in depth.

A Few Firefox Extensions (cont'd)

HTTPS Everywhere:

HTTPS everywhere will work with websites trying to automatically flip from using http to https.

Privacy Badger:

A plugin written by the Electronic Frontier Foundation (EFF) that gives you and allows you to block information what information you're sharing with a website.

Firefox Focus

Almost every app on your android phone or your iphone has a function that calls out to a web browser. These can do tracking cookies, load privacy tracking ads and so on. Firefox Focus is a simple single window private browser that uses temp files for info and blocks ads by default. Set your default browser to this and a lot less tracking will occur.

You might also find Firefox Focus to be a bit limiting so you probably won't want to make it your primary browser.

Burner Credit Cards

Privacy.com / virtual credit cards

Simple service for doing burner credit cards. Gives a small amount of increased confidence when you buy something online.

Most credit cards also offer a similar service as well.

NIST Guides

When I do a security talk one of the most common questions I get from people is "Where do I Start?"

NIST is part of the United States Department of Commerce.

NIST - National Institute of Standards and Technology puts out a lot of free information and guides that can help you with this.

These guides cover a wide range of topics.

NIST Guides (Con'td)

A quick example: NISTIR 7621 - Small Business Information Security: The Fundamentals, A 54 page guide that will help you get started.

Guide contains worksheets, information, checklists and so on. Great guide for a small business.

Just one guide. There are a lot more of them.

Automate The Boring Stuff

Automate the Boring Stuff with Python by Al Swiegart.

The book is freely available on line.

It is quite simply a cookbook for how to do things with python. No prior programming experience is necessary. A little wouldn't hurt though.

Also available as a Udemy course for $10.00 with the discount code FOR_LIKE_10_BUCKS (80% discount)

Automate The Boring Stuff (Cont'd)

Some of the topics covered

Working with Excel Spreadsheets
Working with PDF and Word Files
Web Scraping
Sending E-mail and Text Messages
GUI automation

There are also chapters covering the basics of python as well.

I've used this book a lot. E.g. SQL server access to remote database to create Excel spreadsheet for department

Development/Burner Chromebook

One of the most interesting features of Chromebooks is their powerwash feature. If you are traveling internationally this can be a very useful feature.

There is a link to a blog entry about that using YubiKey & Duo Mobile for 2 factor auth and making sure that you have as little data as possible on the system. In the worst case scenario you just let them have the laptop.

Being able to run android apps on Chromebook is also part of this as well.

OSALT

What is the Open Source equivalent to Microsoft Visio?

Lets hit OSALT.com and type in Visio

Some of the suggestions:

- StarUML
- Kivio
- ArgoUML
- LibreOffice Draw
- Dia

OSALT (cont'd)

OSALT has a lot of Open Source ALTernatives for various closed source programs.

Give it a spin and it might help you figure out an alternative to a program that is limiting your OS choices.

Beta Exams

Want to get Certified and hopefully save a lot of money. Various companies such as CompTIA, Oracle, Cisco, Microsoft and others use beta exams before they roll out a new exam.

Example

Next Monday I'll be sitting for the CompTIA Pentest+ Beta Exam. This exam normally costs $350.00, I'll be taking it for $50.00.

Beta Exams (Cont'd)

Couple of Caveats

- The exams are usually much longer than a regular exam. Sometimes 2 or 3 times longer than the regular exam.
- The questions are still being evaluated so some of them are probably going to be vague.
- The exams aren't available all the time. Usually when there is a new exam or it is refreshed
- You usually won't get the score until the whole beta exam is done and scored. It took me 9 months to find out I passed the CompTIA Cloud+ exam

Freezing a Hard Drive

This is one of those tricks that I've used a bunch of times and am still amazed every time it works. Note: only works with spinning hard drives.

You have a hard drive that has gone bad. You don't have a backup of it and you really need the data off of it.

One thing to consider is taking the hard drive out putting it in a plastic baggie and putting it in the freezer overnight.

Then take out the drive plug it into the system and try and get your data off of it.

DDRescue

Another tool to consider is DDRescue. This will attempt to pull data off of a device by reading a sector over and over again. It also allows you to run this tool. Then freeze the hard drive and pick up where you left off.

Combining the two I've had pretty good luck getting data off of bad hard drives.

One note: if either of these work don't continue to use the hard drive. It is going to fail soon again.

PortableApps.com

Portableapps.com allow you to put "portable" versions of apps onto a USB stick and take them with you from PC to PC.

The apps don't need admin privs or other rights on the machine so you can take the usb stick from machine to machine and use them like normal.

Example apps: firefox, libreoffice, gimp, etc. Also has a couple of anti-virus tools as well. Combined with a read-only USB can be a very nice portable toolkit.

Have I Been Pwned?

Very simply you put your e-mail address in their website and it tells you whether or not your e-mail address has been compromised.

E.g. ajgrothe@gmail - my gmail account which I don't use for much. Has NOT been compromised so far.

ajgrothe@yahoo.com - my yahoo account has been compromised 6 times. By companies such as LinkedIn, KickStarter, Dropbox and others

Give it a spin and you may be surprised

Have I Been Pwned? (Cont'd)

You can also do a domain search as well. If you control a domain. E.g. if you control company.com you can do a search for all the various @company.com e-mail addresses that have been compromised.

E.g. if ajgrothe@company.com has been compromised I may want to have the user change their passwords at various sites.

LetsEncrypt.com

If you have a website you should be defaulting to SSL by now. If not you'll be marked down in Google's search rankings and your users will start receiving warnings from browsers in the near future.

LetsEncrypt provides free SSL certificates that are pretty easy to setup and use.

NEbraskaCERT a website I admin uses LetEncrypt for our SSL certificates.

LetsEncrypt.com (cont'd)

Overall is pretty easy to do. One caveat LetEncrypt SSL certs are only valid for 90 days so you need to make sure you've got the renewal process figured out.

Many hosting sites like Dreamhost are now offering LetsEncrypt support with just a button click.

Ninite/GetMacApps.com

When you get a new PC or Mac one of the first thing you have to do is install all the apps you'll want.

Ninite and GetMacApps both provide the capability to install all the relevant apps in one install package. I use it quite often when I'm rolling out a new PC for myself or a friend.

Ninite also offers Ninite Pro which is the commercial version of it. I haven't used Ninite Pro.

GetMacApps.com is the Mac equivalent of this.

Kali Linux

If you've ever been interested in how hacking works Kali Linux is probably where you want to start. Kali Linux is a live CD/DVD that has a lot of the tools that hackers use.

The tools have notes for them. Network mapping tools, offline recon tools and exploit tools.

It is in Mr. Robot so you know it has to be good.

Tails

Tails is a Linux LiveDVD that can be used to browse the web more anonymously. Tails uses the Tor network and hardened versions of tools such as Mozilla Firefox to connect to the web.

Just burn the DVD and boot it and give it a spin. It'll teach you a lot about how paranoid people live.

Tails was supposed to be the OS choice of Richard Snowden.

Cybrary.IT

Cybrary offers free training about a lot of topics: CyberSecurity, ITIL, Programming and other things.

The training is all free. They offer micro-certifications that you do pay for.

I used them quite a bit when I was studying for the ITIL foundation course.

DD-WRT

For most routers you buy you have a choice of OSes for them. You can either run the stock firmware or choose one of the alternative OSes.

There are three major alternative OSes for routers

DD-WRT, OpenWRT and Tomato Firmware

DD-WRT

These open up a lot of possibilities for your router

Change power settings for radios, add new features. Share files from a USB drive. Run more services on a system. Capture all network traffic and run through an analyzer and so on.

Also will soon support additional 5ghz bands. Which will be awesome for people with 5ghz congestion.

Bug Bounty Programs

Setting up a bug bounty program can be a pain. There are now services available that make it a lot easier.

BugCrowd & HackerOne both offer programs. You pay a fee set up rules for engagement budget and so on.

Q & A

Questions???

Links

Tip - Free Scrum Certification

www.scrumstudy.com

Tip - Free Six Sigma Certification

www.6sigmastudy.com

Links

Tip - Read Only USB Drives

www.kanguru.com
www.buffalotech.com

Amazon search for USB + Write Protect

https://www.amazon.com/s/ref=nb_sb_noss_2?url=search-alias%3Daps&field-keywords=usb+drive+write+protect

Links

Tip - Other Browsers

Mozilla Firefox - www.firefox.com
Opera - www.opera.com
Vivaldi - www.vivaldi.com

Links

Tip - A Few Firefox Extensions

Multi-account firefox - https://addons.mozilla.org/en-US/firefox/addon/multi-account-containers/
HTTPS Everywhere - https://www.eff.org/https-everywhere
Privacy Badger - https://www.eff.org/privacybadger

Links

Tip - Firefox Focus

https://www.mozilla.org/en-US/firefox/mobile/

Links

Tip - NIST Guides

NIST Homepage

https://www.nist.gov

NISTIR 7621 - Small Business Information Security: The Fundamentals - https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

Links

Tip - Automate the Boring Stuff with Python

https://automatetheboringstuff.com

Links

Tip - Development/Burner Chromebook

https://blog.lessonslearned.org/building-a-more-secure-development-chromebook/

https://sites.google.com/a/chromium.org/dev/chromium-os/chrome-os-systems-supporting-android-apps

Links

Tip - OSALT

www.osalt.com

Links

Tip - Beta Exams

CompTIA - https:/www.pearsonvue.com/comptia
Oracle - https://education.oracle.com/pls/web_prod-plq-dad/db_pages.getpage?page_id=182
Cisco - https://learningnetwork.cisco.com/community/certifications/policies_reference_tools/exam_information
Others - www.gocertify.com

Links

Tip - DDRescue

https://www.gnu.org/software/ddrescue/

Tip - PortableAPPs.com

www.portableapps.com

Links

Tip - Have I Been Pwned?

https://haveibeenpwned.com/

Tip - Lets Encrypt

https://www.letsencrypt.com

Links

Tip - Ninite / Get Mac Apps.com

www.ninite.com
www.getmacapps.com

Tip - Kali Linux

www.kali.org

Tip - Tails

https://tails.boum.org

Links

Tip - Cybrary

www.cybrary.it

Tip - DDWRT/OpenWRT/Tomato Firmware

www.dd-wrt.com
www.openwrt.org
www.polarcloud.org/tomato

Links

Tip - Bug Bounty Programs

www.bugcrowd.com
www.hackerone.com