15 For 15
15 Things to Know/Try for a Better 2015

by Aaron Grothe
Security+/CISSP/NSA
IAM/NSA IEM

Introduction

15 for 15?

I did a 12 for 12 talk in 2012, A 13 for 13 talk in 2013 and a 14 for 14 talk in 2014. So not being one to challenge tradition here is 15 for 15 in 2015.

Links are at the end of the talk
Slides will be posted at the NEbraskaCERT website http://www.nebraskacert.org/csf

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.

Try a Different Search Engine

How many of you still use google?/yahoo?/bing?

Try a different search engine. DuckDuckGo.com has a pretty good privacy policy and promises not to track you as much.

Not saying you have to stay with them just give them a try.

Get Rid of Windows XP

How many of you are still running Windows XP?
How many of you have been asked by a family member/friend if it is safe to still run Windows XP?
Windows XP is getting more and more dangerous with every patch Tuesday
You can still get by running Windows XP with good anti-virus and a browser still being updated, but it isn't recommended
If it comes down to a license issue consider trying out RoboLinux. RoboLinux is a Linux distro pre-configured to turn your C:\ drive into a vm inside Linux such as Linux Mint/Debian, etc

DOCSIS 3.0 Modem

- How many of you are using a cable modem to access the internet?
- How many of your are still using a DOCSIS 2.0 Modem?
- If you're not sure doublecheck. Your life will be so much better with a 3.0 modem

Install one Security Browser Plugin

- Try out one Security Browser Plugin
  - NoScript
  - Https Everywhere
  - Disconnect
  - Webtrust
  - AdBlock Plus

Try a New Browser

Try another browser. Consider possibly separating your tasks into different browsers.

E.g. I have my e-mail on my main machine in Chromium, do my browsing in Chrome and use Iceweasel for my research and use Lynx or wget when visiting "dangerous" sites

Comodo Dragon and Ice Dragon Internet Browsers have a good security rep
EPIC Browser is interesting and continuing to evolve

Fix your Router

How many of you have a router/wifi access point at home running the firmware that came with it?
How many of you have upgraded the software that came with the router if available?

If possible drop the stock firmware and go with a "real" firmware like dd-wrt/openwrt/tomato, etc

Adds a lot of features and updates are available

Was on last years list as well, but come on you should do this :-)

_nomap your wifi access points

If you don't want google to map your wifi access points, you have to put _nomap at the end of them. E.g. LilPrivacyPlease becomes LilPrivacyPlease_nomap

Microsoft has also agreed to support the _nomap option as well

Consider adding a virtual interface to your lan to let you migrate piecemeal. E.g. I've got both wiiplay and wiiplay_nomap sids on my network currently

Review your Wifi Settings

How many of you know what your current settings are on your router?

E.g. do you have a/b/g/n all available? Do you still have any 802.11b devices?

E.g. are you using TKIP+AES instead of just AES for your encryption standard. Heaven help you if you are still using wep.

Do you have the transmit power turned up all the way on your router and not need it for where you use it?

Consider changing your AES key :-(

Fixing Windows 8

Windows 7 just went into extended support. It is getting harder and harder to buy a new PC with Windows 7. Corporate PCs can still buy Windows 8 and "downgrade" to Windows 7.

Classic Shell makes Windows 8 act a lot more like Windows 7 or XP which is pretty much what you want.

Secunia PSI

Secunia PSI will go through your Windows PC and look for all the apps that need to updated.

It is free for personal/non-commercial use

Can help you when fixing a friend's/parent's machine and trying to make sure it is as secure as possible

OpenWireless.org

Cool project. Based around the concept of sharing. You put their firmware on your router and then freely share it.

Some of the benefits of it are deniability, increased access, and general hippieness

Only works on a couple of routers currently. Have not seen of the hotspots around town yet when driving

Know your Network

- If you've got an android device, install fing. If you've just got a regular desktop, use nmap
- map your network at least once and try and figure out every device on your network. This will tell you a lot about it you might not know

Get IPV6 Certified

Hurricane Electric has a free certification course for IPV6

Disclaimer: I'm still at the newb level

Easiest way to do it is to get a 2-month trial with Digital Ocean. Fire up an IPV6 droplet and go to town

IPV6 is coming might as well accept it :-)

Do One "Bad" Thing this Year

Buy a cheap android phone of craigslist. Root it and install CM or another distro on it
Hack your Nintendo Wii and install homebrew on it
Make a hackintosh
Strip the DRM off a PDF encrypted file
Download a torrent :-) Legal of course

Q & A

Questions???

Links

Tip #1 - Different Search Engine

Duck Duck Go

http://www.duckduckgo.com

Tip #2 - RoboLinux

http://www.robolinux.org

Links

Tip #4 - Browser Plugins

- NoScript - http://www.noscript.net
- Https Everywhere - https://www.eff.org/HTTPS-EVERYWHERE
- Disconnect - https://www.disconnect.me
- Webtrust - Mozilla Plugins
- AdBlock Plus - https://www.adblockplus.org

Links

Tip #5 - Try a New Browser

Chromium - http://www.chromium.org/Home
Comodo Dragon - https://www.comodo.com/home/browsers-toolbars/browser.php
Comodo Ice Dragon - https://www.comodo.com/home/browsers-toolbars/icedragon-browser.php
EPIC Browser - https://www.epicbrowser.com/

Links

Tip #6 - Fix Your Router

DD-WRT - http://www.dd-wrt.com/site/index
OpenWRT - https://openwrt.org/
Tomato - http://www.polarcloud.com/tomato

Links

Tip #8 - nomap

Not being mapped by google wifi

https://support.google.com/maps/answer/1725632?hl=en

Tip #10 - Fixing Windows 8

Classic Shell - http://www.classicshell.net/

Links

Tip #11 - Secunia PSI (Personal Software Inspector)

http://secunia.com/vulnerability_scanning/personal/

Tip #12 - OpenWireless.org

https://openwireless.org/

Links

Tip #13 - Know your Network

Fing - https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=en

Nmap - http://nmap.org

Tip #14 - Get IPV6 Certified

https://ipv6.he.net/certification/

Links

Tip #15 - Do One Bad Thing

Omaha Craigslist.org search for Android

http://omaha.craigslist.org/search/sss?query=android&sort=rel

Hacking your Wii

http://lifehacker.com/5830367/how-to-hack-your-wii-for-homebrew-in-five-minutes

Links (Last)

Tip #15 - Do One Bad Thing (cont)

Make a Hackintosh

http://www.hackintosh.com/