16 For 16
16 Things to Know/Try for a Better 2016

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

Introduction

16 for 16?

I did a 12 for 12 talk in 2012, a 13 for 13 talk in 2013 a 14 for 14 talk in 2014, and a 15 for 15 in 2015. So not being one to challenge tradition here is 16 for 16 in 2016.

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.

usbkill

usbkill is a simple program that monitors your USB settings and will shutdown or perform other tasks as needed

An example case is putting a usb drive on a lanyard and then pulling it out when you get tackled by the Po Po :-)

Beware "Secure" Browsers

A lot of companies have created their own "secure" browsers based on Chromimum

One example is Chromodo from Comodo which disabled the Same-origin policy

Another is the Avast SafeZone Browser - allowed the browser to access local files on the system from the browser

Beware "Secure" Browsers

Neither bug was present in Chromium/Chrome, both were security based enhancements.

Not to say other Chromiums aren't worthwhile, but be cautious

Feel kind of bad, because when I mentioned try a new browser in last year's 15 for 15 talk - one of the ones I listed was Chromodo :-(

Let's Encrypt

- Let's Encrypt is a joint project between EFF & Mozilla and other groups that has created a system for creating free SSL Certificates to help encrypt more of the web
- Let's is a Certificate Authority (CA)
- Will make it harder to eavesdrop on web traffic
- Also provides tools to convert sites from http to https
- Accepted by all major web browsers
  - SHA-256
  - All certs are only good for 90 days/easy renewal process
  - Hit beta in December 2015

Gophish

- Very nice Open Source/Free Phishing toolkit
- Has all the tools to create a basic phishing campaign for your company
- Pretty simple/easy to use

Malware Museum

Archive.org has put a classic museum of old Malware. For MS-DOS moslty right now

You can run them in a browser to see how they work

You can also download them to give them a spin locally

Be careful of course, but it is a very interesting snapshot of time. Also some of these have gotten very hard to find on the net

How to Stay on Windows 7 / 8 or 8.1

Microsoft is pushing Microsoft Windows 10 very hard.
They've moved it from optional to recommended updates.
So a lot of people have gotten it who don't want it.

Also if you have limited Disk Space it can run you right out of it. Did this for me on a netbook of mine with 16mb of flash storage.

Steps pretty much are turn off automatic updates
Unselect Windows 10 upgrade and hide that update
Turn automatic updates back on

Have until July 27, 2016 for free Windows 10 Upgrade

Parted Magic

Parted Magic is a commercial Linux distribution available as a LiveUSB or CD-Rom

It costs $4.95

Has one very nice feature that a lot of distros don't. It can wipe Solid State Drives (SSD) back to their factory state

Very nice addition to your toolbox

Alpine Linux

Alpine Linux is a very interesting little distribution

It is uses BusyBox/MUSL for the core of its system. It also uses some interesting security features such as Pax and grsec

What makes this one to watch is that the Docker group has recently hired the main developer of this and mentioned that they would be rebasing the Docker Images on an Alpine base instead of Ubuntu (since then corrected)

Privacy Badger

A web browser extension that provides you a lot information about tracking cookies and advertisements that don't comply with the Do Not Track settings

Can also block the cookies that contribute to your tracking

In a future release will work against web browser fingerprinting

Underhanded C Code Contest

The Underhanded C Contest (UCC) is an interesting contest held most years.

It is different than the Obfuscated C Code Contest in that the goal of it is to hide a bug in the system in plain sight.

Will show you a lot of the ways that people can try and hide malicious code into a program

Zerocoin/Zerocash

Zerocoin is an extension to Bitcoin that adds additional anonymity to the Bitcoin process

Right now it is in a trial state. They are proposing to reset the process in 6 months and go live

10% of all the coins mined are going to be sent to the creators

Interesting to see how this works out compared to DarkCoin and regular BitCoin

Reproducible Builds

- Debian and other Linux distributions are starting to provide this capability
- The goal here is to be able to verify the whole of a build environment and everything that comes out of it
- Anybody else will be able to reproduce this process
- This is still a work in progress
- When complete it will be possible to verify all of the packages in a system are the same for all builds

PirateBox

A very simple distribution based on OpenWRT that creates a small wifi hotspot that can be used to share files easily

Can be very useful for sharing information such as Wifi access information and files/information for a conference

When used with a TP-Link TL-M3040 can create a battery powered hotspot that is cheap enough ~$30.00 to be almost disposable

Talos SecWorkstation

Raptor Engineering
$3,100 Secure Workstation
8-core Power 8i CPU
Bios/Everything is Open Source
Still fighting for 3d Video acceleration to be Open Source
(Nvidia regression, Radeon still needs blobs)

Really Cheap Computers

Chip - small complete computer with wifi built in. Selling for $9.00 before shipping

Raspberry PI - small single board computers ranging in cost from $5.00 to $35.00. Have become very popular

Zsun Memory Card Reader - $11.00 on banggood small computer that can be battery powered and is able to run OpenWRT, a very interesting little tool for hacking

Android Tablets & Android Phones such as the LG G2 can be found at sites for as little as $10.00 / Wifi + 3/4g = Pentester's delight

Portable Apps

Portable Apps are a bunch of apps that have been modified to be able to be run from a USB stick

Has a good section of security apps

Spybot Search & Destroy Portable
Kapersky Rootkit remove
McAfee - Antivius toolkit

Windows 10 Update List

Until recently there was no real information about what is in an update from Microsoft

This is a decent first step, still not a complete. A lot of fixes are described as “performance improvements” and “application fixes”

Q & A

Questions???

Links

Tip #1 - usbkill

https://github.com/hephaest0s/usbkill

Tip #2 - Beware Secure Browsers

https://code.google.com/p/google-security-research/issues/detail?id=704

http://www.itworld.com/article/3030561/researcher-finds-serious-flaw-in-chromium-based-avast-safezone-browser.html

Links

Tip #3 - Let's Encrypt

https://letsencrypt.org/

Tip #4 - Open Source Phishing Toolkit

https://getgophish.com/
https://github.com/sptoolkit/sptoolkit
https://www.trustedsec.com/social-engineer-toolkit/

Links

Tip #5 - Virus Browser Museum

https://archive.org/details/malwaremuseum&tab=collection

Tip #6 - How to Stay on Windows 7 / 8 / 8.1

http://www.intowindows.com/remove-upgrade-to-windows-10-message-from-windows-78/

Links

Tip #7 - Parted Magic

http://partedmagic.com/

Tip #8 - Alpine Linux

https://alpinelinux.org/

Links

Tip #9 - Privacy Badger

https://www.eff.org/privacybadger

Tip #10 - Underhanded C-code Contest

http://www.underhanded-c.org/

Links

Tip #11 - Zerocoin

http://zerocoin.org/

Tip #12 - Reproducible Builds (Debian)

https://wiki.debian.org/ReproducibleBuilds

Links

Tip #13 - PirateBox

https://www.piratebox.cc/

Tip #14 - Talos Secure Workstation

https://raptorengineeringinc.com/TALOS/prerelease_info.php

Links

Tip #15 - Really Cheap Systems

Chip - http://nextthing.co/
Raspberry Pi - https://www.raspberrypi.org/

Tip #16 - Portable Apps

http://portableapps.com/

Links (Last)

Tip #17 - Windows 10 Update List

http://windows.microsoft.com/en-us/windows-10/update-history-windows-10