17 For 17
17 Things to Know/Try for a Better 2017

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

Introduction

17 for 17?

I did a 12 for 12 talk in 2012 and have just kept going from there. I might be in a bit of a rut.

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.

Have I Been Pwnd?

Have I Been Pwnd? Is a website that you can put your e-mail address in to see if your e-mail address has been compromised.

E.g. My yahoo e-mail was pwnd in both the LinkedIn & DropBox disclosures

Can also do this for a full domain as well E.g. testdomain.com, do this for your company if you're in the security group

Avast Ransomware Decryption Tools

This is a collection of Ransomware Decryption Tools

Currently up to about 11 ransomware strains, including Alcatraz Lockerware

Can save your bacon if your are “lucky” enough to have been infected by one of these variants.

No more Ransonware Alliance

Project devoted to stopping Ransomware

Have tools to unlock a variety of Ransomware programs

Sponsors include Intel Security, Kaspersky lab, Baracuda and others

Once again largely common sense stuff. Have backups, anti-virus, anti-malware, etc

Panopticlick

This is a project by the EFF to tell you how much data your browser is sharing with the sites you connect to. Also tells if your browser has a unique fingerprint.

It also provides some advice such as:

Install Privacy Badger
Enable Do Not Track

Etcher.io

Everybody does this at least once. Some more than once.

You put a usb stick into your PC to write a bootable image to it. Unfortunately you instead have selected from a hard drive on your system, and voila you've lost some data.

Etcher.io does checks to help prevent this from happening and provides a nice interface as well.

Multi-platform.

Register article on Red Teams

The Register has a really good article about how Red Teams work.

A very nice article about how red teams work. Short article, but this is part 1 of a two part series.

Red Teams are teams that attack a client with very few rules, can be allowed to use almost any techniques to get access.

MultiBootUSB

MultiBootUSB allows you to write multiple live linux images to a usb stick or external hard drive and provides you a menu so you can select which one you want.

E.g. You can put Kali, Parrot, Caine and other distros all on the same usb stick so you can have one USB stick with your tools on it.

Multi-platform: runs on Linux/Mac/Windows.

HackerOne

HackOne offers the ability to do a Bug Bounty Program as a Service (BBPaaS?)

If your company is releasing software this provides a way to setup a bug bounty program, with items like responsible disclosure and the rest included.

Uber, Slack, Square and others are all customers of HackerOne.

Interesting because it means you don't have to roll your own for this.

LinuxClone

Quite simply this creates a bootable image of your currently running linux onto a second (USB) stick.

This lets you customize a distro, put all of the tools settings you want into it and then create a portable copy of it.

If you customize a distro after installation extensively this can be a really useful tool.

Also has an UEFI bootloader which can be very useful.

Cybrary Free Training / Minicerts

Cybrary offers a bunch of free training courses. Also has a bunch of mini-certs which you can do to get some CEUs and/or some mastery of the stuff.

A good little site, recommend it. Goes from beginner to advanced. Their cloud terminology course is nice.

TeamViewer

Eventually you'll need to do tech support for a family member/friend etc.

TeamViewer is free (for non-commercial use), multi-platform, and pretty easy to use.

You can download and install it on your side. Ideally in a VM and then direct your parents to the TeamViewer QuickSupport and they won't have to download install anything just use the code/session id you generate on your side.

Good to do it before you need it.

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

Murphy's Laws for Computer Security

List of 10 Laws for Computer Security

A couple of examples

#10. Small system breeches don't need to be reported
#1. All Documents are out of date or simply missing

Very nice little article. Should have one or two make you guy "hmm" moments.

IoTseeker

Scanner will go through your network and look for IoT devices with default/simple passwords.

CCTVs, DVRs and some other devices

Source is out at github

Keep in mind this will generate some network traffic so make sure that your network team is ready for the onslaught :-)

MoFo Linux / Subgraph OS

Two Linux distributions designed to be resistant to state level surveillance/spying and censorship

Both use Tor/I2P and other techniques along with a hardened kernel

Part of what makes MoFo interesting is because of its anti-censorship tools and arabic support.

Supgraph OS is doing some work with containers which is interesting as well

Veracode - Software Report 2016

Veracode has been doing these "The State of Software Security XXXX - Reports" for quite a few years

They run the code against a large code base

Gives some interesting insights into things

Interesting stat: "97% of all java applications assessed had at least one component with a known vunerability"

You do have to give them your contact info :-(

NISTIR 8151

NIST report with the title “Dramatically Reducing Software Vulnerabilities”

Claims we could reduce the level of software errors from 25 per 1,000 lines by an order of magnitude in a 3 to 7 year timeframe

Combination of design changes - such as increased modularization, looser coupling, increased code analysis, etc.

Interesting read for just 64 pages

Have I Been Pwnd Dataset

Troy Hunt - who runs Have I Been Pwnd has anonymized the data set from his site and made it available

1.9 billion records in hibp - 1.4 billion unique, 500 million records have been Pwnd multiple times (including myself)

This will drive some serious analysis for this over the next few years.

SAMRi10

PowerShell script that works in Windows 10 and Windows Server 2016

Turns off the ability for querying the Windows Security Account Manager Remotely

Once a machine is compromised one of the goals is to get additional information. SAMRi10 makes it harder to get this information.

Tools like PowerSploit and Bloodhound are already automating this recon

Q & A

Questions???

Links

Tip - Have I Been Pwnd?

http://haveibeenpwned.com

Tip - Avast Ransomware Decryption Tools

https://www.avast.com/ransomware-decryption-tools

Tip - No More Ransom Project

https://www.nomoreransom.org

Links

Tip - Panopticlick

https://panopticlick.eff.org/

Tip - Etcher.io

https://etcher.io

Links

Tip - Register Article on Red Teams

https://www.theregister.co.uk/2016/12/08/inside_hacking_a_business_feature/

Tip - MultiBootUSB

http://multibootusb.org

Links

Tip - HackerOne

https://hackerone.com

Tip - LinuxClone

http://fex.belwue.de/linuxclone.html

Links

Tip - Cybrary free training / minicerts

https://www.cybrary.it

Tip - TeamViewer

https://www.teamviewer.com/en/

Links

Tip - Murphy's Laws for Computer Security

http://www.networkworld.com/article/3132566/security/murphys-law-the-security-version.html

Tip - IoTSeeker

https://github.com/rapid7/IoTSeeker

Links

Tip - MoFo Linux & Subgraph OS

MoFo Linux - http://mofolinux.com/
Subgraph OS - https://subgraph.com/index.en.html

Tip - VeraCode - State of Software Security Report

https://info.veracode.com/state-of-software-security-report.html

Links

Tip - NISTIR 8151

http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf

Tip - Have I Been Pwn'd Dataset

https://www.troyhunt.com/heres-1-4-billion-records-from-have-i-been-pwned-for-you-to-analyse/

Links

Tip #17 - SAMRi10

https://gallery.technet.microsoft.com/SAMRi10-Hardening-Remote-48d94b5b