18 For 18
18 Things to Know/Try for a Better 2018

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

Introduction

18 for 18?

I did a 12 for 12 talk in 2012 and have just kept going from there. Used to say I was in a rut not describe it as a groove.

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.

USBGuard

Part of Red Hat Linux 7.4 / also available for most other Linux distributions - currently only for Linux

System for whitelisting USB devices that are allowed to be seen by the system. Can be used to prevent things like badusb (usb/networking) from working on a system

You can create a rule file and it allows you to lock down by manufacturer etc. USB device IDs can be spoofed as well

DEO - Binding Disk to Network

Uses a service on the network to generate a highly-random key to encrypt a disk. This is then fed to the LUKS: Disk Encryption system

So if the disk is taken off the network it can't be accessed. There are manual processes so you can do access the data if the network is unavailable

Designed to let you have encrypted disks across the network with minimal setup

Redhat 7.5 has added Network-bound disk encryption

Linux Sandboxing

Firejail - simple linux sandboxing

Simple to use as

Firejail firefox

No access to private files in user's home directory
Downloads, browser config files are available
Everything else is temporary filesystem

Firecfg allows you to control settings, e.g. allow sound, etc

Microsoft Threat Modeling Tool

If you’re not doing threat modeling for your sensitive systems you probably should be. One of the problems is that there aren’t a lot of great tools out there.

Microsoft uses threat modeling extensively and have made their modeling tool freely available

It is a very nice tool for doing threat modeling. It works under Crossover’s Wine on Linux

CAPEC

CAPEC - Common Attack Pattern Enumeration and Classification

Mitre system to create a common language for attack patterns.

Provide common attack pattern information and helps classify attacks.

Can help you describe and classify your research

CAPEC (cont'd)

Some Well-Known Attack Patterns:

Cross Site Request Forgery (CAPEC-62)
SQL Injection (CAPEC-66)
Cross-Site Scripting (CAPEC-63)
Buffer Overflow (CAPEC-100)
Clickjacking (CAPEC-103)
Relative Path Traversal (CAPEC-139)
XML Attribute Blowup (CAPEC-229)

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 it might not be what you're looking for as well.

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.

Zero Trust Model

Forrester has put together a proposal for something called a “Zero Trust Model”. Idea is simply that you assume each individual machine is always under attack. You assume there is no “internal” network anymore.

E.g. Assumes there are two types of data in your org

1) Data that someone wants to steal
2) Everything else

Has good ideas for PCI/HIPPA and so on

Recon-NG / Offline Recon

Recon-NG is available as part of the Kali Linux distro
Recon-NG is also available independently

Written in Python
Based around getting data without directly hitting target
E.g. pull information from bing / mit pgp keyring, others
Interface similar to metasploit
Easily extendable

Privacy Paradox

5 Day plan to take back your digital privacy

Day 1: what your phone knows
Day 2: the search for identity
Day 3: something to hide - right to be forgotten
Day 4: fifteen minutes of anonymity
Day 5: personal terms of service - putting requirements around your personal information

IPv6 Certification

IPv6 is coming. It is in a race with Desktop Linux :-)

Hurricane Electric offers an online certification program for IPv6. Based around doing basic tasks (pinging, traceroute, sending e-mails, and other networking tasks).

Spent ten years as a “newb” in the program before finally getting to the “Sage” level.

Lot easier nowadays that Digital Ocean and Vultr both offer IPv6 as part of their vm creation

Also you can get a t-shirt if you finish :-)

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.

Linux Subsystem for Windows

This is quite simply a way to run a goodly amount of Linux executables (largely non-gui) on Windows. Can run OpenSuse, Ubuntu, Suse Linux Enterprise Server and in the future some others as well. The Arch guys are working around it.

Has some limitations but if you need/want to run one or two Linux only tools, this might be a way to do this

C9.io - Development system in Cloud

An ubuntu desktop in the cloud. Combined with a chromebook can make a relatively secure remote system.

Has a free tier to use as well

Portal Router

This isn't really a security thing and is a network thing

5 Ghz networking is broken into 2 types of usage, sections you can use without having to do anything special. There are also bands Dynamic Frequency Selection that you have to listen on periodically to make sure they aren't being used by radar systems. Not a lot of routers support this currently. Most end devices do support this. So if you're in a highly saturated 5ghz area DFS can get you back to normal wifi speeds.

Disclaimer: I have one of these. We're on a break right now.

AWS - Scanners

Almost everybody is using AWS nowadays and almost every day there is somebody who is putting data out there insecurely and it is being discovered.

The following are a list of tools that can help you monitor your AWS setup

Some of the tools Netflix/Security Monkey monitor your AWS/GCP accounts for policy changes
Bucketfinder uses a wordlist to look for buckets and see if they are set to public, private or a redirect
Several other tools are on the list as well

Tomoyo Linux

Tomoyo Linux can be used to harden Linux systems. It can be very useful in embedded systems such as SCADA and voting systems.

A lot easier to configure than SELinux and AppArmor, has a learning mode on this. One of my talks at OLUG last year was on Tomoyo.

Microsoft Edge

Quite simply Microsoft has created a decent browser.

They went back disabled a lot of legacy things such as ActiveX and Netscape plugins. Also has a smaller installed base than Google Chrome so fewer people are writing exploits against it.

Multi-Account Firefox

Firefox Multi-Account Containers extension allows you to create separate containers for different online duties.

E.g. banking can be kept separate, from research, shopping, e-mail, etc.

Labels and color-coded tabs help keep separate

Cookies, Saved Passwords and so on are specific to each account

Remember not a "perfect" solution one more part of defense in depth.

Q & A

Questions???

Links

Tip - USBGuard

https://bitbucket.org/LaNMaSteR53/recon-ng

Tip - DEO - Service binding data to network

https://github.com/npmccallum/deo
http://www.freeipa.org/page/Network_Bound_Disk_Encryption

Links

Tip - Linux Sandboxing

http://firejail.wordpress.com/2017/05/15/linux-mint-sandboxing-guide/
http://www.linuxandubuntu.com/home/firejail-a-namespace-separation-security-sandbox

Tip - Microsoft Threat Modeling Tool

https://blogs.microsoft.com/microsoftsecure/2015/10/07/whats-new-with-microsoft-threat-modeling-tool-2016/

Links

Tip - CAPEC - Common Attack Pattern Enumeration and Classification

https://capec.mitre.org/data/definitions/1000.html

Tip - Firefox Focus

https://en.wikipedia.org/wiki/Firefox_Focus
https://www.mozilla.org/en-US/firefox/focus/

Links

Tip - Burner Credit Cards (Privacy.com)

https://promotions.kinja.com/make-free-virtual-burner-cards-with-privacy-com-and-kee-1796339085

https://privacy.com/

Links

Tip - Zero Trust Networking

http://csrc.nist.gov/cyberframework/rfi_comments/040813_forrester_research.pdf

https://opensource.com/article/17/6/4-easy-ways-work-toward-zero-trust-security-model

Links

Tip - Recon-ng

https://bitbucket.org/LaNMaSteR53/recon-ng

Tip - Privacy Paradox

https://project.wnyc.org/privacy-paradox/

Links

Tip - IPv6 Certification

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

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 - Linux Subsystem for Windows

https://msdn.microsoft.com/en-us/commandline/wsl/install_guide

Tip - c9.io - Cloud Development Environment

http://c9.io

Links

Tip - Portal Router

https://portalwifi.com

Links

Tip - AWS Security Auditing Tools

https://www.peerlyst.com/posts/a-list-of-tools-you-can-use-to-security-test-your-amazon-aws-services-guurhart?utm_source=LinkedIn&utm_medium=Application_Share&utm_content=peerlyst_post&utm_campaign=peerlyst_shared_post&lipi=urn%3Ali%3Apage%3Ad_flagship3_feed%3BaW40dqG0R5eD8FFrnPVyig%3D%3D

Links

Tip - Tomoyo Linux

http://tomoyo.osdn.jp/

Tip - Microsoft Edge

https://www.microsoft.com/en-us/windows/microsoft-edge

Links

Tip - Multi-Account Firefox

https://addons.mozilla.org/en-US/firefox/addon/multi-account-containers/