13 For 13
13 Security Resources you should know

by Aaron Grothe

Introduction

13 for 13?

Many people in the security business will refer to this source of data or that. This talk is a quick intro to 13 of them.

Most of these are issued yearly or quarterly so keep an eye out for updated versions of them

They are in no particular order

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.

Verizon Data Breach Report

Compiled by Verizon based on their Forensic investigations

An annual report the 2013 version should be out RSN

Doesn't appear to have a high level home

URL: http://www.verizonenterprise.com/us/about/events/2012dbir/

Verizon Data Breach Report

Pulls information from a variety of sources
Has some very good suggestions and guidelines
If you are running Point Of Sales Systems (POS), download read and implement now
High level, your manager can read it :-)

Let's take a look at the report

Administration Trade Secret Report

Report put together by the current Administration detailing Trade Secret theft and Intellectual Property Right infringement

Provides a national look at what the administration is committed to doing to protect IPR

http://s3.documentcloud.org/documents/605299/tade-secrets-022013.pdf

Administration Trade Secret Report

Not a lot of actionable data in the report

It does show a very interesting look at the role nation states play in this area

Has been accused of jingoism, but the case studies are interesting

Linux From Scratch

Linux From Scratch is a book on how to build your own Linux system. If you go through this you will have a much better idea what goes into making a Linux system.

There is also BLFS (Beyond Linux From Scratch), ALFS (Automated Linux From Scratch)

There are several distros that started from LFS

openSUSE build System

This is a service offered by Suse that allows you to automatically build your software into packages that are available for most OSes

I was using this for a couple of things I was building in the past

Autokey

Autokey is a program for doing desktop automation. E.g. Macro expansion, Keyboard shortcuts, etc.

It is similar to utilities available for Mac OS X and Windows. If you use Linux a lot it can save you some serious time

Expect/AutoExpect

Expect is a TCL application for automating typical command line tasks on your system.

E.g. you need to use sftp or ftp to send a file to a remote system. You need to run a variety of commands some of which require user interaction such as gpg you can use expect to do this.

Autoexpect is used to generate an expect script by turning your commands into an expect script

DDrescue/Safecopy

Sooner or later you're going to lose a drive that has information on it that you didn't back up. DD is an amazing command but when it runs into a disk error it stops. DDrescue can be run multiple times against a disk to try and get the information of it. Safecopy is a more user friendly version of this.

You haven't lived until you've put a hard drive in the freezer overnight wrapped in a towel in the hope that DDrescue will be able to get the data you need off of it

Turnkey Linux

Turnkey Linux is a company that makes a variety of easy to use VMs available. The VMs are available for a variety of VMs as well as in .iso format.

They provide ready to run VMs for things such as Ruby on Rails, Tracks, Mantis, Sencha and so on

If you just want to get up and running quickly this is a pretty good place to start

Debian GNU/Hurd, GNU/kFreeBSD

This is a pretty cool set of systems. This is the GNU Hurd Kernel or the FreeBSD Kernel with the Debian Userspace running on top of it.

This can make a very cool system if you want to do a firewall or just have a unique desktop

Keep in mind it also changes the way you refer to your devices it isn't eth0 anymore it is if0 and disk slices are weird

Systrace

Systrace is a sandboxing environment that is built into OpenBSD and is available for Linux. Not to be confused with Systrace for Android (a performance monitoring tool)

Allows you to create a policy that restricts the execution of a program. E.g. you can limit an FTP program or a server to being only able to access relevant files and devices

Systrace has also had some security vulnerabilities with it as well so buyer beware. It can be very useful for locking down programs you can't limit any other way

HoneyD

- HoneyD is a small program that can be used to deploy honeypots on your network. This can be very useful if you are doing it on un-used IP addresses and start seeing activity there
- If you use this with arpd you can create a pretty convincing honeypot with some old hardware pretty easily

Google Chrome Remote Desktop

This allows you to remotely control another computer

You can generate an access code to allow remote administration of another person's computer (E.g. my parents) or control your own desktops

Note: this is currently in beta but provides a nice way to help out someone remotely with their computer without having to install VNC/SSH, firewall settings, etc.

Note: also makes sure you give all info to Google :-P

Unetbootin

Unetbootin lets you create a Live USB drive for many Linux based OSes. It can do persistent live sections for some of them.

Fedora/Ubuntu and a lot of other distributions also have their own LiveUSB creation tools, but Unetbootin works for a lot of OSes

Q & A

Questions???

Links

Alien

http://joeyh.name/code/alien/

Qubes OS

http://qubes-os.org/trac

Linux From Scratch

http://www.linuxfromscratch.org

Links

openSUSE Build System

https://build.opensuse.org/

Autokey

http://code.google.com/p/autokey/

http://www.autohotkey.com/

Links

Expect/Autoexpect

http://www.nist.gov/el/msid/expect.cfm

DDrescue

http://www.gnu.org/software/ddrescue/ddrescue.html

Safecopy

http://safecopy.sourceforge.net/

Links

Turnkey Linux

http://www.turnkeylinux.org/

Links

Debian GNU Hurd

http://www.debian.org/ports/hurd/

Debian kFreeBSD

http://www.debian.org/ports/kfreebsd-gnu/

Links

Systrace

http://www.citi.umich.edu/u/provos/systrace/

HoneyD

http://www.honeyd.org/

Links (Final)

Google Chrome Remote Desktop

https://chrome.google.com/webstore/detail/chrome-remote-desktop/gbchcmhmhahfdphkhkmpfmihenigjmpp?hl=en

unetbootin

http://unetbootin.sourceforge.net/