13 For 13
13 Things to Know/Try for a Better 2013

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

13 for 13?

Last year did a talk called 12 for 12 which went over reasonably well. This version has new tools and things to try for a better 2013.

Links are at the end of the talk
Slides are already 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.
HTTPS Everywhere

This is an extension for Mozilla Firefox and Google Chrome

Many websites offer https but do not default to it or switch between the two modes as you use the site. Google switched to default https largely as a result of this plugin. This flips everything to https as much as possible

It is a quick/easy extension that is very worthwhile if you are using your computer with a public access hotspot

Need to get from EFF for Firefox
Wget, Lynx/Links and grep

Sometime you are going to need to verify that a website has been compromised. How do you get a webpage that may have been infected safely onto your computer? And then how do you inspect it.

Wget is a command line tool with a lot of options (it can mirror a site), pull a specific webpage look for particular patterns and so on
**Wget, Lynx/Links and grep**

Lynx/Links are simple web browsers that do not support flash, pdf, etc. Can also use VIM as well.

*Grep can be used to look for strings in a web page you've retrieved.*

```bash
wget http://www.badsite.org -o localcopy.html
grep -i https localcopy.html | grep -i \.ru
lynx localcopy.html
```

*Available on Windows via Cygwin or as individual utilities.*
TrueCrypt

Truecrypt is disk encryption plain and simple :-)  

Can be used on hard drives, USB sticks, etc  

Works with Mac OS X, Windows, Linux  

Can do exotic stuff as well such as Rubber Hose filesystems and so on  

If you buy a USB stick that promises encryption odds are that it will be using TrueCrypt
Write-Protectable USB Drive List

Fencepost.com has a list of USB drive manufacturers that offer hardware write-protectable switches on them.

These are getting to be rarer and rarer nowadays.

The Write Protect Tab on a SD-card is only a request to the software not to write to the device and can be ignored. This is how CHDK works.

Some software does tricks likes filling the whole drive to simulate read-only access.
Blue Proximity

This is a simple program that allows you to use a bluetooth device paired with a computer to automatically lock the system or perform other actions when you are in/out of range of the computer.

There are similar programs for Mac OS X/Windows

Not foolproof but useful as part of defense in depth

I wrote about this for 2600 magazine
WIPFW

WIPFW is a port of the BSD IPFW firewall software to Microsoft Windows.

This gives a lot of interesting capabilities such as traffic shaping, port-knocking, port forwarding and so on that aren't available for most Windows Firewalls.

Note: not the easiest tool to use, command line by default with a couple of basic GUIs available.
Hushmail

Hushmail is a privacy enhanced webmail system. Encryption happens on the client side before the data is sent to the system.

There have been questions about the security of the system in the past and it has had a few issues.

It is a good way to semi-anomalousy send e-mail. It has been used by groups such as Anonymous and Wikileaks in the past.
Netwox/Netwag

Netwox/Netwag are truly the swiss-army knife of tools. They do over 200 tasks from things such as being a simple server (CIFS/HTTP/FTP) to Spoofing packets (IPV4 and IPV6), to sniffing traffic to a load of other options.

When it does packet capture it actually displays the packets in an ASCII representation of the IETF/Stevens Standard.

Won't get more functionality for less disk space.
Finished maintenance in 2007.
Microsoft now makes a version of Windows Defender Online that is capable of being burned as a LiveCD.

This is a very nice way to clean a machine that is just infested with spyware/viruses.

Other tools such as Kaspersky and Panda also make rescue disks as well. Good list of them is available at http://www.thefreecountry.com
Systrace

Systrace is a sandboxing environment that is built into OpenBSD and is available for Linux. There was a Mac OS X version but that has been left unmaintained for years.

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.
OSSEC

OSSEC is a host based intrusion detection system. It performs the following tasks:

- Log analysis
- Rootkit detection
- Windows registry monitoring
- Integration with various databases (PostgreSQL, MySQL) and so on
- Agent/Server design
- Can form the basis for a comprehensive IDS platform
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
SecTools.org

Sectools.org is a listing put together by Fyodor of nmap fame

It lists a lot of security tools with a very nice breakdown by cost, OSes support, and category (sniffers, sploits, fuzzers, etc.)

Well worth the time for a read. Our lists only share 2 entries truecrypt and ossec :-(
Links

HTTPS Everywhere - https://www.eff.org/https-everywhere

Wget/Lynx and Grep - http://www.cygwin.com

Truecrypt - http://www.truecrypt.org

Links

Blue Proximity - http://blueproximity.sourceforge.net/

BT Proximity (Bluetooth password program for Windows) http://www.daveamenta.com/products/btproximity/

Proximity (Similar program for Mac OS X) - http://code.google.com/p/reduxcomputing-proximity/

Bluemon (non-graphical program for Linux, can do multiple items as part of bluetooth access) - http://www.matthew.ath.cx/projects/bluemon/
Links

WIPFW - http://wipfw.sourceforge.net/

Hushmail - http://www.hushmail.com

Netwox/Netwag - http://ntwox.sourceforge.net/
Links


Free Country Page listing Windows Defender Offline and other tools

Links (Last)

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

OSSEC - http://www.ossec.net/

Google Chrome Remote Desktop - https://chrome.google.com/webstore/detail/chrome-remote-desktop/gbchcmhmhahfdphkhkmpfmihenigjmp

SecTools.org - http://www.sectools.org