12 For 12
12 Things to Know/Try for a Better 2012

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

Introduction

12 for 12?

Goal is to provide a quick example of some tools/sites that you might not be aware of. Each one of them meets the following criteria: I found them cool/neat/useful
:-) Hopefully you will too

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.

Security LiveCDs/USB Sticks

Go back quite a ways - everybody seems to be doing a remaster of Ubuntu these days

Couple of the better ones

- CAINE - One I'm mostly using right now
- OpenDiag - Simple/Easy great for resetting NT passwords
- Katana - Bunch of Tools in one package
- Backtrack - one of the standards
- BartsPE - Windows XP live cd maker

Webgoat

Quite simply if you want to learn about web application security here is where to start

- Provides a simple Tomcat environment that is setup insecurely
- Provides a set of lessons to get you started
  - Learn about messing around with Input parameters
  - Learn about SQL injections
- Used together with WebScarab (a web proxy), you can learn a lot about how to test security for websites
- This is horribly insecure. Do not allow on the internet
- Part of the OWASP project

Mozilla Plugin Check

Mozilla Plugin Check is the site you should be mentioning to your parents/friends etc. It runs a basic check of the plugins in their browser and makes sure they are up to date

- Keep in mind this might result in more tech support headaches for you as well :-(
- The site works with Firefox/Chrome/Internet Explorer and so on

How To Forge

How To Forge is a collection of worked solutions. Quick plug I put one in there a while ago about how to make an almost Chromebook by using Google's Chromimum OS

A quick example of a couple of the topics there

- How to encrypt e-mails with SSL certificates
- How to create the perfect Centos 6 Server
- How to build an Almost Chromebook :-)

SANS Reading Room

Some parts of the SANS program require the applicants to write security papers that are put into their library. This is a very good resource on a lot of topics.

A couple of examples

Multiple papers available on hogwash
Some very nice little papers on selinux

Note: the quality of the individual papers can varies but it is a great resource

Virus Total

Virus Total allows you to upload a suspect file and they then run it against 40+ different anti-virus products. If you are concerned about a file this can be a lifesaver.

There are other similar services out there as well like jotti http://www.jotti.com sometimes Virus Total is swamped so having multiple options is helpful.

Qubes

Qubes is an heavily virtualized system where everything is run inside a VM. It gives an example of where a lot of people believe computer security is heading. Has the concept of Disposable VMs.

One of Qubes developers is Joanna Rutkowska who is well known for the Blue Pill exploit. Moving an operating system from hardware into a virtual environment without its awareness.

Current version is not production ready, but very interesting.

Dark Reading

Dark Reading is a news/info site for Security information. It is my current favorite now that SecurityFocus has been shutdown. Looks professional so you can forward links to it to your boss without being worried about him being 2 clicks away from bad stuff.

Shodan

Shodan is a computer search engine. It looks for embedded systems and devices.

Great searches to try

Voip
Scada
JetDirect
Your Company's name

Password Safe

Passwords are the first line of defense for most people.

Quick Questions

How many of you use unique passwords for each site?
No really how many of you do?

Password Safe is a tool you can use for this

There are a lot of other ones as well. Some people use pgp and a text file to hold their passwords as well. Some people also have a recipe file on top of their desks

Darik's Boot And Nuke (DBAN)

DBAN is a way to securely wipe hard drives and machines before you dispose of them

DBAN can be kind of slow as it can do a lot of passes depending on what you select

DBAN can also be a good way to get a machine that is being stubborn about boot sectors, etc to let you repartition a drive

Research being done into how this works with SSDs

Damn Vulnerable Linux (DVL)

Damn Vulnerable Linux (DVL) is a highly vulnerable version of Linux that can be used for learning and demonstration purposes.

Examples of a couple of its issues

- Old versions of PHP/Apache/MySQL/FTP and SSH are running on the system
- Most of them are also poorly configured as well

Threat Expert

You can upload a suspicious program to Threat Expert. It will then execute it in a sandbox on their site and send you a report on it.

Is not a signature based solution. Actually runs the program and looks for anomalous behaviour.

Service is currently free.

Q & A

Questions???

Links

LiveCD/USB Sticks

- Caine - http://www.caine-live.net/
- OpenDiagnostics Live CD - http://www.volatileminds.net/opendiagnostics/index.php/OpenDiagnostics_Live_CD
- BartsPE - http://www.nu2.nu/pebuilder/
- Katana - Multi-Boot Security Suite - http://sourceforge.net/projects/katana-usb/
- Backtrack - http://www.backtrack-linux.org/

Links

Webgoat

https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

Web Scarab

https://www.owasp.org/index.php/Webgoat

OWASP

https://www.owasp.org

Links

Mozilla Plugin Check

http://www.mozilla.org/en-US/plugincheck/

How To Forge

http://www.howtoforge.com

Sans Reading Room

http://www.sans.org/reading_room/

Links

Virus Total

http://www.virustotal.com

Qubes

http://qubes-os.org/Home.html

Dark Reading

http://www.darkreading.com/

Links

Password Safe

http://passwordsafe.sourceforge.net/

Darik's Boot And Nuke (DBAN)

http://www.dban.org

Links (Last)

Damn Vulnerable Linux (DVL)

http://www.damnvulnerablelinux.org/

Threat Expert

http://www.threatexpert.com