June 18, 2008
NebraskaCERT CSF

45 Tools that Every Security Professional Should Know about
by
Aaron Grothe/CISSP

Disclaimers

- Your Mileage May Vary
- Questions Anytime
- Hoping for a bit of interactivity
- Some of these tools are dual purpose tools with an expected use and an alternative use

Intro

Did a talk similar to this about 2.5 years ago titled “35 or So Tools/Sites Every Computer Security Professional Should Know About”

Comparing the Two Talks

Added 10 for Inflation
8 Tools are on both lists

Broken Down Into 10 Sections

Net Tools
Vulnerability Scanners
Forensics Tools
Live CDs
Password Tools.

Broken Down Into 10 Sections

Making Windows Work
Webstuff
Virtual Machines
Misc
Websites

Net Tools

PBNJ
nmap
Netwox/Netwag
Wireshark
Kismet

PBNJ

URL: http://shrinkster.com/zcx

Description: PBNJ is a tool that tracks changes that occur on a network over time. E.g. a server opens a new port this will detect it.

Similar Tools: ndiff

NMAP

URL: http://nmap.org

Description: NMAP is the grandaddy of all network scan tools. It is also a valuable tools for doing DOS attacks against some versions of Netback

Similar Tools: zenmap – gui front end for nmap, doscan search for single port

Netwox

URL: http://shrinkster.com/zd0

Description: Netwox has over 200 different tools as part of its bag of tricks. It also displays packets in the Steven's Format

Similar Tools: Netwag a graphical front end to Netwox

Netcat

URL: http://shrinkster.com/zd1

Description: Netcat is simply cat that runs across the network. You can connect a port on this machine to a port on that machine

Similar Tools: bunch of variants, gnu's netcat, socat, etc...

Wireshark

URL: http://shrinkster.com/zd2

Description: Formerly Etherreal is pretty much the standard sniffer. It has the three pane display every body loves.

Similar Tools: tcpdump

Kismet

URL: http://shrinkster.com/zd3

Description: Kismet is a wireless network detector IDS and packet sniffer. Kismet runs in passive mode not sending any loggable packets

Similar Tools: Netstumbler

Vulnerability Scanners

Nikto
Nessus
Metasploit
Paros Proxy
MBSA

Nikto

URL: http://shrinkster.com/zcz

Description: Nikto is a webscanner that will look for a lot of items, such as misconfigured settings, public stuff that shouldn't be and the like

Note: can give a LOT of false positives

Nessus

URL: http://shrinkster.com/zd7

Description: Nessus is one of the classic vulnerability scanning tools. An example of an Open Source project going closed source.

Note: is a classic tool

Metasploit

URL: http://shrinkster.com/zd8

Description: Hacking like in the Movies. If you want to write exploits this framework is where to start.

Paros Proxy

URL: http://shrinkster.com/zd9

Description: Paros Proxy allows you to modify all the information that flows between a webserver and a browser. Forms, Cookies can all be modified.

MBSA

URL: http://shrinkster.com/zdb

Description: Microsoft Baseline Security Analyzer is a tool to help make sure you're in compliance with security patches.

Note: based on tech licensed from Shavlik technologies

Paros Proxy

URL: http://shrinkster.com/zd9

Description: Paros Proxy allows you to modify all the information that flows between a webserver and a browser. Forms, Cookies can all be modified.

Forensics Tools

ddrescue
Darik's Boot and Nuke
Apple's Time Machine
PhotoRec
Gparted

ddrescue

URL: http://shrinkster.com/zdd

Description: Gnu tool that is a super version of dd. Normal dd gives up one read errors ddrescue will keep trying to recover data.

Darik's Boot and Nuke

URL: http://shrinkster.com/zde

Description: BandN is a simple tool for overwriting drives before you throw them away. It has many modes available to it.

Apple's Time Machine

URL: http://shrinkster.com/zdf

Description: Apple's Time Machine monitors your system for changes so you can undo them. It will be a forensic guy's dream.

PhotoRec

URL: http://shrinkster.com/zdh

Description: PhotoRec is a tool to recover video, photos, documents and archives from cd-roms and harddisks. It goes around filesystem so it can get stuff off of reformatted drives.

Gparted – Gnome Partition Editor

URL: http://shrinkster.com/zdi

Description: gparted can copy, move, resize, backup and recover partitions. There is also a livecd version available as well.

LiveCDs

MandrakeFlash
Other Linux LiveCDs
Bart's PE
Ultimate Boot CD

MandrivaFlash

URL: http://shrinkster.com/zdj

Description: MandrivaFlash is a complete Linux distribution that runs off a USB key. So it can be updated and customized. It can also make CD images to boot off of older machines.

Info: there are sites to help you make your own usb distro.

Other Linux Live CDs

URL: http://shrinkster.com/zdk

Description: Backtrack is currently my favorite LiveCD for security purposes.

Others: Pentoo, Fedora Security Respin, nubuntu, etc...

Bart's PE

URL: http://shrinkster.com/zdl

Description: Bart's Preinstalled Environment bootable Windows CD/DVD is a LiveCD for windows.

Notes: Some people have been “remastering” windows vista boot cds to put their own software on them.

Ultimate Boot CD

URL: http://shrinkster.com/zdm

Description: A collection of utilities in the form of a LiveCD. Has boot disks from various systems, recovery tools and various mini-distros on it.

Password Tools

Password Safe
John the Ripper
Cain and Abel
Rainbow Crack

Password Safe

URL: http://shrinkster.com/zdn

Description: Password Safe is a program to hold passwords. Useful if you need to deal with the “if x gets run over by a bus” situtation, or if you're just getting old.

John the Ripper

URL: http://shrinkster.com/zdo

Description: Set this up running on a machine and see how many you can get by the end of a meeting. A very effective Demo.

Cain and Abel

URL: http://shrinkster.com/zdp

Description: C&A is a password sniffer, recovery tool for Microsoft Windows.

Project Rainbow Crack

URL: http://shrinkster.com/zdq

Description: Project Rainbow Crack creates tables in advance to really speed up cracking Microsoft Passwords.

Notes: Ophcrack is a liveCD with a modified version of this software on it.

Making Microsoft Windows Work

Cygwin
Sysinternals
Wipfw

Cygwin

URL: http://shrinkster.com/zdr

Description: Cygwin is an environment that allows you to largely treat your Microsoft Windows box like a Unix machine.

Other tools: uwin, mks toolkit, Microsoft Services for Unix

Sysinternals

URL: http://shrinkster.com/zds

Description: Site of some of the best tools for Microsoft Windows: pstools, process explorer, autorun, sdelete, and rootkit revealer

WIPFW

URL: http://shrinkster.com/zdt

Description: wipfw is a version of the BSD OS firewall IPFW that runs on Microsoft Windows. It is mostly compatible with IPFW.

Virtual Machines

UML
QEMU
Vmware Virtual Appliance
MarketPlace

UML

URL: http://shrinkster.com/zdu

Description: Allows you to run Linux as a process inside Linux. Very useful for trying out potentially dangerous software

QEMU

URL: http://shrinkster.com/zdv

Description: QEMU is a processor emulator. This means you can make up a virtual machine running DEC alpha and run it on your AMD x86-64 machine.

Vmware's Virtual Appliance Marketplace

URL: http://shrinkster.com/zdw

Description: A lot of images to use with Vmware player. Lot of security toolkits ready to try out.

Note: not always the most up to date.

Misc

LaBrea
Driftnet
Microsoft Security Screen Savers
TrueCrypt

LaBrea

URL: http://shrinkster.com/zdx

Description: LaBrea lets you put a tarpit on unused IP addresses and port numbers. This can make scanning your network much more difficult.

Note: Pointer is to freebsd package. Looking for real homepage

Driftnet

URL: http://shrinkster.com/zdy

Description: Driftnet grabs images off the wire and displays them on a computer. This can be a highly effective tool to give an idea of what is happening on your network.

Microsoft Security Screen Savers

URL: http://shrinkster.com/zdz

Description: Simple Screen Savers with 10 laws of security on each one. Great idea to make it the default on your machines.

E.g. if someone has physical access to your machine they can control your machine.

TrueCrypt

URL: http://shrinkster.com/ze0

Description: TrueCrypt is a simple tool to allow you to create encrypted files on your system. it works cross-platform and is very handy to carry sensitive information on.

Websites

Pete Finnigan's Oracle Site
TheFreeCountry.org
cve.mitre.org
Center for Internet Security
HowToForge
Sectools.org
Forensics Wiki

Pete Finnigan's Oracle Site

URL: http://shrinkster.com/ze3

Description: Pete has some of the best information about Oracle Database security at his website.

TheFreeCountry.org

URL: http://shrinkster.com/ze4

Description: TheFreeCountry.org's security section is a really nice place to find free security tools.

CVE.Mitre.org

URL: http://shrinkster.com/ze5

Description: Where to start reading about CVE's. Quite simply CVEs are the standard here is where to find out more about them.

Center For Internet Security

URL: http://shrinkster.com/ze6

Description: Has some really good guides and tools for helping to tie down the security of your infrastructure.

Notes: not always up to date. Some of the tools have restrictions on their use as well.

HowToForge

URL: http://shrinkster.com/ze7

Description: HowToForge has cookbooks of how to setup systems in reasonably secure fashion. Lots of good info there.

Sectools.org

URL: http://shrinkster.com/ze8

Description: Fyodor (nmap author's) list of security tools. Has a lot of interesting tools on it. I check it out periodically to see if there is anything I don't recognize.

Forensic's Wiki

URL: http://shrinkster.com/ze9

Description: A wiki devoted to Computer Forensics. Doing a random search for something like TimeStomp came back with a hit so while young it looks promising.

Future Tools

A couple I'm planning on evaluating.

Likewise Open – Tool to synchronize your Active Directory with Linux accounts
Hardened PHP/Sushoshin
Two factor authentication with Google's apps

Q & A

Questions and Hopefully Answers.

Summary

This is just a small example of some of the tools that I use or have used in the past and still consider useful.