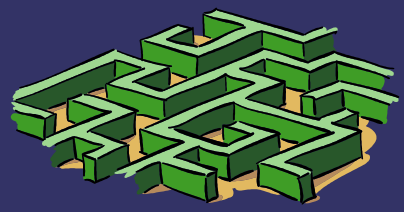
November 16, 2006
NEbraskaCERT CSF

35 or So Tools/Sites Every Computer Security Professional Should Know About

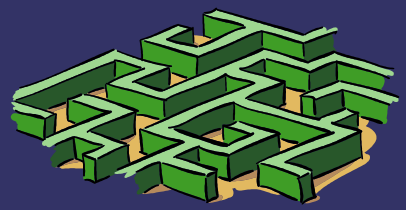
by

Aaron Grothe/CISSP



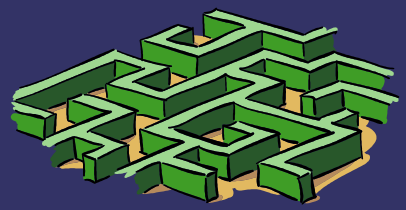
Disclaimers

- Your Mileage May Vary (YMMV)
- Questions Anytime
- Hoping for a bit of interactivity



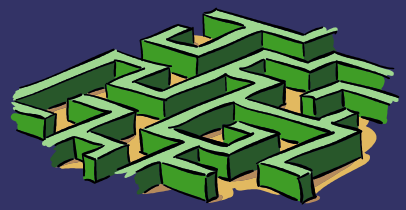
Broken down into 4 Sections

- For Users/Admin
- For Developers
- Most Misused Tools
- Websites



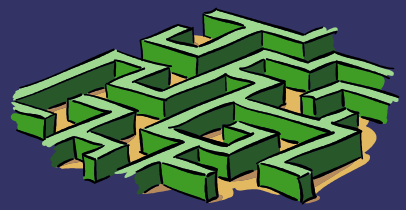
For Uses/Admins

- Automated Password Generator (APG)
- Cheops
- The Coroner's Toolkit
- Darik's Boot and Nuke
- John the Ripper
- LaBrea
- Linux Security LiveCDs
- LSOF
- Metasploit.



For Users/Admin (cont)

- Microsoft Audit Collection System
- Ndiff
- Netstat
- Password Safe
- Pstools
- Sentry Tools
- Smart Boot Manager
- Stunnel
- Swatch
- Windows LiveCDs

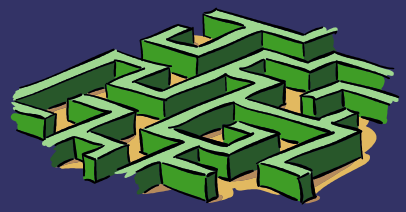


Automated Password Generator (APG)

URL: http://shrinkster.com/99t

Description: Random Password Generator

Use this when you reset someone's password.
Instead of just setting it to password.

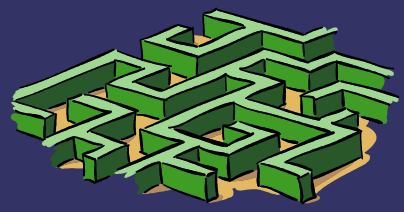


Cheops

URL http://shrinkster.com/997

Description: Network discovery tool

Cheops will explore your network and map what services/ports are available on your network

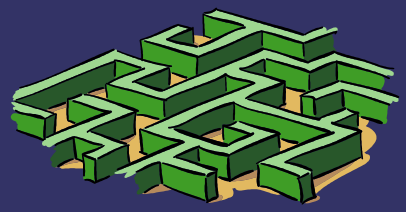


The Coroner's Toolkit

URL http://shrinkster.com/998

Description: Toolkit for doing forensics

TCT has some excellent documentation with it.
Can recover data by scavenging through inodes

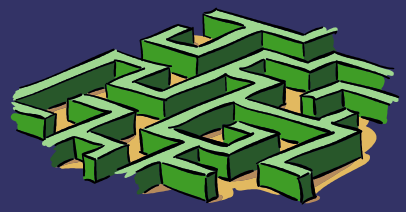


Darik's Boot and Nuke

URL http://shrinkster.com/999

Description: Tool to Wipe Hard Drives of a machine

Use DBN before you throw a machine out or when you get a new machine and want to clear the drive.



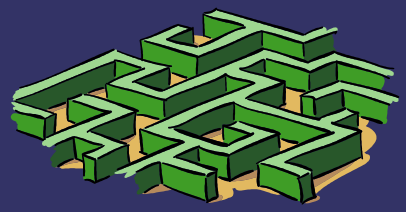
John the Ripper

URL http://shrinkster.com/99a

Description: Tool for cracking passwords

Tool that will attempt to crack passwords using word lists, brute force, etc. People have gone to jail for using this improperly.

Scarily effective

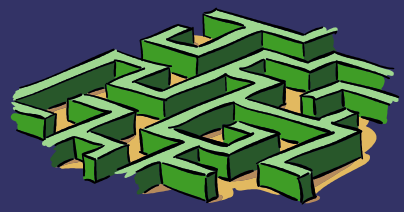


LaBrea

URL http://shrinkster.com/99b

Description: Stop Scans

Bringing up LaBrea on unused IPs will result in a tarpit that will slow scans of your network.

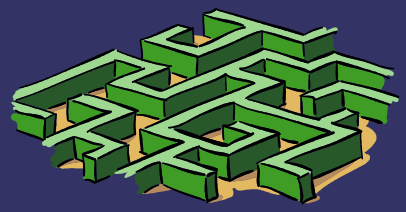


Linux Security LiveCDs

URL http://shrinkster.com/99e

Description: FrozenTech's Live CD list

A live Linux CD is a very cool tool to be able to experiment with. Auditor and Whax are both very popular.

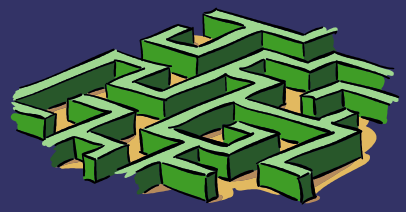


LSOF

URL http://shrinkster.com/99h

Description: List Open Files

LiSt the Open Files on your machine. What is using port 80 on your machine? What trojan is holding port 8323 on your machine open?

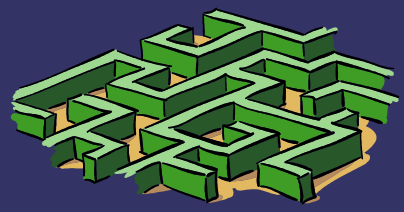


Metasploit

URL http://shrinkster.com/99i

Description: Point, Click, l33t

Simple tool to demonstrate vulnerabilites. A full framework for writing your own exploits. Very effective demonstration.

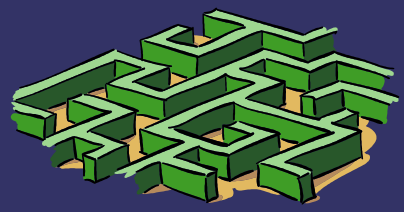


Microsoft Audit Collection System

URL ???
URL http://shrinkster.com/99j

Description: Event log management tool

A system for centralizing the event logs for all your Microsoft windows machines into one central searchable location. Hard to find info on Microsoft Windows site.

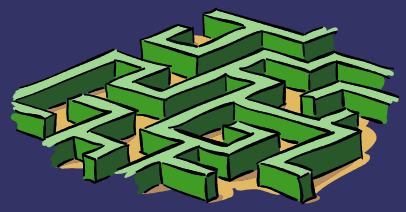


Ndiff

URL http://shrinkster.com/99k

Description: Network Diff

A program to compare the differences between 2 nmap scans. E.g. A new port opened up on a server in your DMZ. Why???

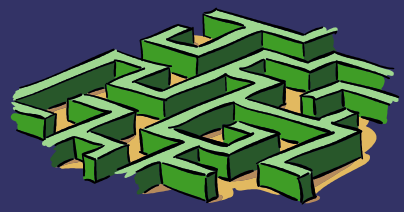


Password Safe

URL http://shrinkster.com/99l

Description: A place to store passwords

Simple tool to hold your passwords in an encrypted file.

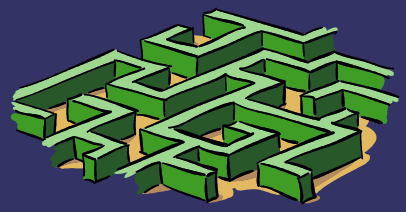


pstools

URL http://shrinkster.com/99m

Description: Command line powertool

Pstools can be used to start/stop/inspect the processes running on your Microsoft Windows machines. A rea swiss army knife for Microsoft Windows.

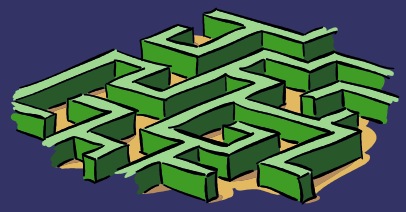


Sentry Tools

URL http://shrinkster.com/99o

Description: Tools for log monitoring and port map detection

Developed by psionic computing. Nice tools for monitoring log files on your system.

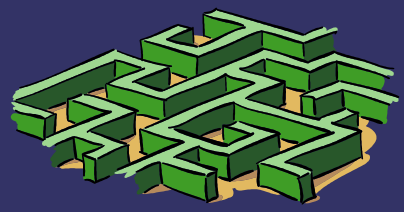


Smart Boot Manager

URL http://shrinkster.com/99p

Description: Floppy Boot anything

SBM can be used to boot a cd-rom or usb device on a system that has a bios that doesn't support it directly. Also useful for Linux installs instead of cutting a set of custom boot floppys.

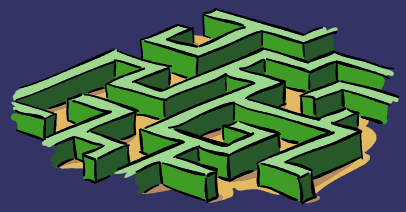


Stunnel

URL http://shrinkster.com/99q

Description: Create encrypted net tunnel

Stunnel can be used to secure protocols, programs that don't support SSL. E.g. Jdbc connections, vnc, pop-mail

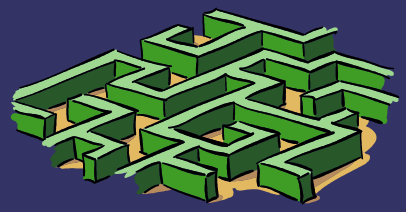


Swatch

URL http://shrinkster.com/99r

Description: Log monitoring tool

Tool for monitoring log files. Similar to logcheck but more generic.

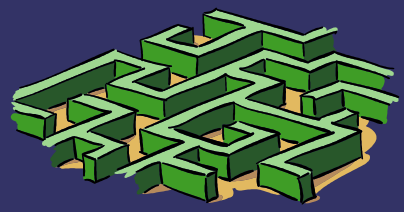


Windows LiveCDs

URL http://shrinkster.com/99s

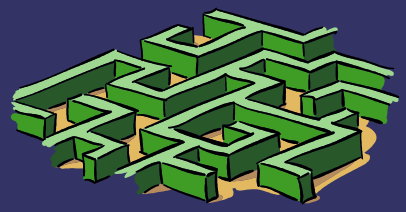
Description: Barts Preinstalled Environment

BartPE can be used to make your own Microsoft Windows LiveCD. Good base for spyware removal, Virus scanner, forensics tools. Needs a real Windows install CD to build!!!



For Developers

- Flawfinder
- RATS
- Splint
- PMD
- Hetergenous Compilers

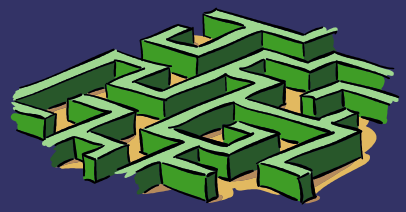


Flawfinder

URL http://shrinkster.com/99v

Description: Static analysis tool

Tool that looks for programming errors in your C/C++ code. Optimized for security checks. E.g. Fixed size buffers in sprintf, etc.

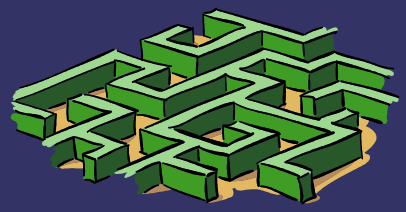


RATS

URL http://shrinksterr.com/99w

Description: Another Static Analysis Tool

Similar to flawfinder. Different rules design.
    Can be worthwhile to run in addition to flawfinder.

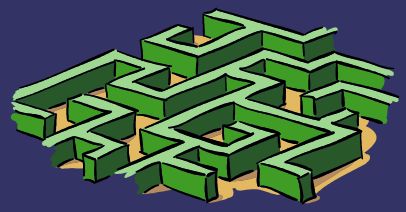


Splint

URL http://shrinkster.com/99u

Description: A better lint

If you annotate your code it can be used to make sure that you don't do invalid state changes. Checks for things like passing a float to a %d in a printf statement



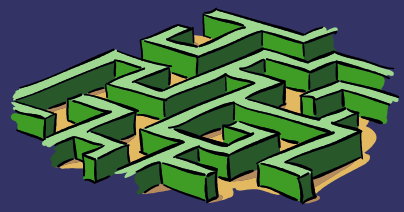
PMD

URL http://shrinkster.com/99x

Description: Tool for writing better C/C++/Java

Detects Cut & Paste, things like unused local variables, empty if/while statements

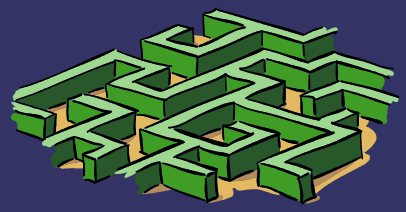
Extensible: be the first to enforce your coding standards on your company/group



Hetergenous Compilers

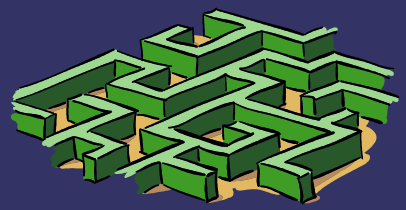
Description: Use more than one compiler

Tendra, Open Watcom, Digital mars, Intel's C Compiler, LCC each compiler generates different code and can result in different error/warnings being made visible!!!



Most Misused Tools

- Nessus
- Snort
- *bsd - * linux

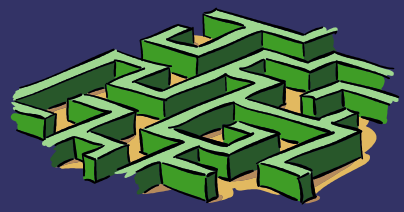


Nessus

URL http://shrinkster.com/99v

Description: Great tool. Often misused

The main problem is way too many people just take the ouptut report cross out the words should/could/possibl* and turn it into a man-date.

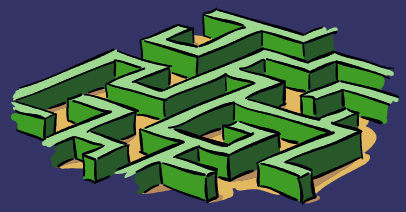


Snort

URL http://shrinkster.com/99z

Description: Intrusion Detection System

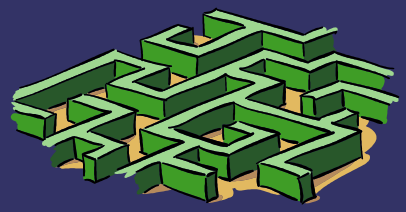
Buy a bundle of hardware run snort with all the rules turned on fill up logs, whine about snort, reset logs and repeat. Ideally with more expensive hardware :-(



**bsd/ *linux*

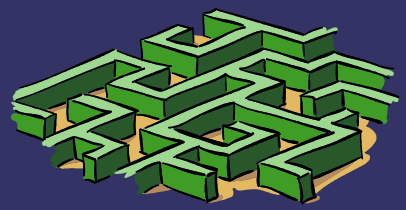
Description: A badly administered OpenBSD box is not more secure than a Microsoft Windows Box

Pet Peeve: Quit running Red Hat Linux 9 unpatched in your DMZ and talking about how secure you are.



Websites

- Sysinternals
- Security Focus
- CERT
- Insecure.org
- Bruce Scheiner's Blog
- Microsoft Security Site
- Linux Documentation Project

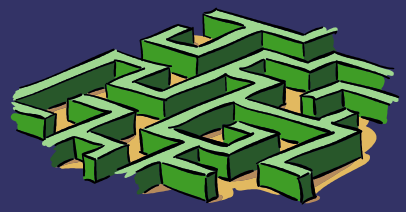


Sysinternals

URL http://shrinkster.com/9a0

Description: Pstools author's site

Authors wrote the Inside Microsoft WIndow series of books. Did a lot of work figuring out the Sony DRM software. Lot of good freeware tools there.

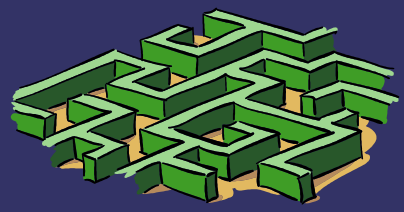


CERT

URL http://shrinkster.com/9a3

Description:Good Portal

Lot of good articles. Nice source for vulnerabilities

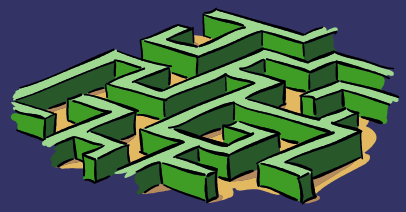


Insecure.org

URL http://shrinkster.com/9a4

Description: Homepage for nmap

Good mail lists. Fyodor also puts up a very good tutorial or editoral every now and then.

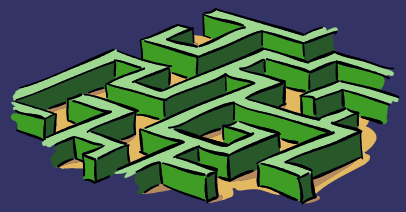


Bruce Scheiner's Blog

URL http://shrinkster.com/9a5

Description: Weblog of a security expert

This is a supplement to Bruce's cryptogram newsletter. Can get a bit technical sometimes but is also “manager friendly” most of the time.

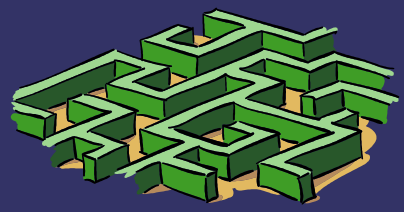


Microsoft Security Site

URL http://shrinkster.com/9a6

Description: Microsoft's Security Homepage

A lot of good information here. Even if you don't run the empire's software.

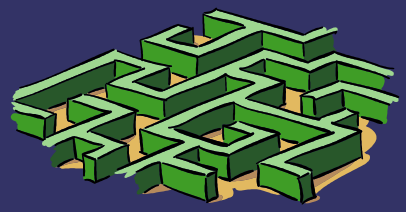


Linux Documentation Project

URL http://shrinkster.com/9a7

Description: Home of the HowTos

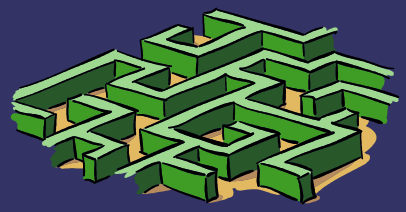
Good security texts available. Also covers a lot of topics like how to do a bridging firewall. How to do an SSL-VPN etc.



Summary

E-mail ajgrothe < at > yahoo.com

Thank you for listening



Microsoft Security Site

URL http://shrinkster.com/9a6

Description: Microsoft's Security Homepage

A lot of good information here. Even if you don't run the empire's software.