Bootable CD-Rom Linux Security Toolkits

NebraskaCERT

by

Aaron Grothe CISSP/Security+

Introduction

- Disclaimer
  - Tommy Chong example
  - Locksmiths
- From the Knoppix STD penetration section

“Remember:
You are the only person responsible for the actions you take. Your actions have a direct effect on other people.
Think First. Don't be a dick!”

Introduction

- Knoppix/Morphix easily modifiable distributions
  - Strong automatic hardware configuration
  - Knoppix is going through constant upgrades
- Others such as LNX-BBC also exist
  - Some such as runt are small enough to fit on a usb keychain fob

Introduction

- Two types of distro will be mentioned
  - General purpose security tool CD
    - Convert a PC into a temporary workstation to run some set of tests
    - Can also reuse PC into a specific purpose machine such as running dsniff
  - Forensics
    - has a lot of potential to grow once .pst files are worked out
    - Linux Forensics http://www.linux-forensics.com has a lot of great information about this area

Knoppix STD

- Knoppix Security Tools Distribution
- Homepage http://www.knoppix-std.org
- Probably the best one of these listed
  - Has quite a bit of documentation
  - Linking tools into some sub-shells works rather nicely

Local Area Security Linux

- Newer than STD
- Homepage http://www.localareasecurity.com
- Has several subdistros including secure server, mini-disc, firewall and so on

Fire

- Forensic Incident Response Environment (FIRE)
- Homepage http://fire.dmzs.com
- Can be operated over a serial cable, works well in console mode
- Virus scanner included

Penguin Sleuth

- Bootable CD containing most of the info from the Linux Forensics home page
- Homepage http://www.linux-forensics.com
- Uses Task and Autopsy for data examination and recovry

I.N.S.E.R.T Linux

- Inside Security Rescue Toolkit
- Homepage http://www.inside-security.de
- Credit card sized distribution
- Clam to fame is Clam Antivirus (pun bad!!)

WarLinux

- Project by wardriving.com to put together good wireless toolkit
- Homepage http://www.wardriving.com
- Includes all standard wireless tools (Airsnort, kismet, and so on)

Snarl

- FreeBSD based Coroner's system
- Hompage http://snarl.eecue.com
- Forensics toolkit similar to Fire and Penguin Sleuth
- Pretty green, might mature nicely though

Which One???

- Knoppix STD is currently the strongest for general purpose, best documentation and the greatest percentage of the tools work
- All are freely available downloads. At any given time LAS might be ahead of STD in version of nmap or the like
- For forensics, Penguin Sleuth is rather nice and more of it works on my hardware

A Few of the Tools

- Local
  - John the Ripper – one of the best password cracking tools
  - Wipe – tool to reformat hard drive several times in an attempt to make recovery harder
  - Secure_delete – tool to delete specific file by overwriting several times with different data
  - Anti-virus tools – tools to perform virus scans on mounted partitions
  - Chkrootkit – tool to look for rootkits

A Few of the Tools

- Network
  - Cheops – tool to try and map network
  - Nessus – great scanning tool
  - Nmap – tool to do port scans
  - Etherape – tool to display network activity
  - Honeyd – small tool to create simple honeynets
  - Labrea – tarpit to slow network scans and some attack types

A Few of the Tools

- Network
  - Snort – included with about everything nowadays
  - Iptraf – IP traffic visualization tool
  - Ethereal – traffic capture and replay tool
  - Ettercap – switched network sniffer++
  - Dsniff – looks for interesting traffic such as user-names and passwords
  - Whisker – web vulnerability analyzer
  - Spike Proxy – Man in the middle proxy

A Few of the Tools

- Forensics
  - Task and Autopsy - tools that allow you to check images into and out of evidence
  - Qparted – tool that allows you to make copies of partitions without mounting the data
  - Glimpse – indexing tool will index reams of data for info
  - Strings – always the classic

A Few of the Tools

- Wireless
  - Airsnort
  - Kismet
  - Macchanger

Other Resources

- Top 75 Security Tools
  - Found at http://www.insecure.org - the makers on nmap – lists some tools such as sara and ntop which aren't included in any of the distros yet
- Open Source Testing Methodology
  - Found at http://www.ideahamster.org - a good approach to doing scans with excellent resources to quite a few tools

Contact Info

- E-mail: grothe@earthlink.net
- Website: http://www.nebraskacert.org

Demo

- Quick overview of a couple of the toolkits
  - Knoppix STP
  - LAS