Investigations and Incident Response Using BackTrack

HTCIA New England Chapter General Meeting

September 22, 2009

Ming Chow

Tufts University

mchow@cs.tufts.edu

http://www.cs.tufts.edu/~mchow

Introduction

- Live CD – an entire operating system with applications on a bootable CD or USB drive; essential for your jump bag
- BackTrack is one of the highly regarded suites, with a wonderful suite of open source tools for law enforcement and investigators
- Originally published for security assessments and auditing
- 4th edition released at the ShmooCon convention in Washington D.C. back in March 2009. NOTE: still beta, not final

About Myself

- Day: Work at Harvard University
- Night: Instructor at Tufts University
- Taught the course *Security, Privacy, and Politics in the Computer Age* in Spring 2005 and 2007
- Taught *Cyber Security* at Middlesex Community College in Spring 2008 and Spring 2009
- Taught *Use of the Internet in Fraud Investigations* at NEAIFI Annual Trainings in 2007 and in 2008
- SANS / GIAC Certified Incident Handler (GCIH)

Basics

- Download distribution at **http://www.remote-exploit.org/backtrack_download.html**
- Make sure PC or virtual machine boots DVD or USB drive
  - To modify a VM's BIOS, add the line `bios.forceSetupOnce = "TRUE"` to the `.vmx` file
- Select one of the options on BT4 menu
- `root` password = `toor`
- On command prompt, enable networking by: `/etc/init.d/networking start`
- To start graphical user interface (KDE): `startx`

What is Included in BT4

- Many of the top 100 security tools listed on **http://sectools.org/**
- Categories of tools
  - Information Gathering
  - Network Mapping (e.g., nmap)
  - Vulnerability Identification
  - Penetration (e.g., Metasploit)
  - Privilege Escalation (e.g., password crackers including John the Ripper)
  - Maintaining Access
  - Radio Access Analysis
  - VoIP
  - Forensics
  - Reverse Engineering
  - Miscellaneous (e.g., a MAC address changer)

What is Not Included in BT4 and Changes

- Volatile memory forensics tools
- Nessus (licensing issues)
- No media player
- No Flash
- No Tor
- Changes:
  - Now based off of the Ubuntu Linux distribution, not Slackware
  - Networking no longer starts up by default
  - No CD ISO; either DVD, USB, or VMware VM

Forensics Capabilities

- New: on boot, option “Start BackTrack Forensics”
  - “Forensically clean”
  - Does not automount drives
  - Does not utilize swap
  - Does not alter data

Example 1: dcfldd

- Created by the Defense Cyber Forensics Lab (DCFL), part of the DoD DC3
- Resolves some of dd's shortcomings
- "Hash-on-the-fly" –calculates the MD5 checksum while data is being copied (requires hashwindow=0 flag)
- Has status bar
- Can be used to wipe disks
- Example: copy an entire NTFS drive (4096 block size) with SHA-1 hash of drive:

  -
    ```
    dcfldd if=driveimagename of=outputfilename bs=4096
    conv=sync,noerror hash=sha1 hashwindow=0
    hashlog=hashlogname
    ```

Example 2: `dd_rescue`

- Used to rescue a damaged disk
- Unlike `dd`, if `dd_rescue` tries to read but fails, it will go on with the next sectors
- Example:
  - `dd_rescue /dev/sda1 /dev/sda2/backup.img`

Example 3: `foremost`

- Also developed by the DC3
- File carving and recovery
- Reads header, footer, and internal data structures
- Creates an audit.txt file that lists the findings, and a folder of the outputs
- Examples:
  - Search for JPGs, skipping first 100 blocks:
    - `foremost -s 100 -t jpg -i image.dd`
  - Search and carve for all files in configuration file and output resultant carved files to output directory:
    - `foremost -o outputdir -c /etc/foremost.conf datafile.img`

Example 4: `Vinetto`

- Extracts information from `Thumbs.db` files
- Examples:
  - Displays metadata from Thumb.db file:
    - `vinetto /path/to/Thumbs.db`
  - Extract the related thumbnails to a directory and produce an HTML report to preview the thumbnails:
    - `vinetto -Ho /tmp/vinetto_output /path/to/Thumbs.db`

Example 5: Cracking WEP on a Wi-Fi Network

- Requires a compatible wireless adapter
- Get list of interfaces via `airmon-ng` (e.g, `eth1`)
- `airmon-ng stop <interface>`
- `ifconfig <interface> down`
- `macchanger --mac 00:11:22:33:44:55 <interface>`
- `airmon-ng start <interface>`
- `airodump-ng <interface>` # **pick network**
- `airodump-ng -c <channel> -w <file name> --bssid <bssid> <interface>` # **start to capture packets**
- On a new console window, `aireplay-ng -1 0 -a <bssid> -h 00:11:22:33:44:55 -e <essid> <interface>`
- `aireplay-ng -3 -b <bssid> -h 00:11:22:33:44:55 <interface>`
- `aircrack-ng -b <bssid> <file name>-01.cap`

Summary

- BackTrack was designed for penetration testers and incident response handlers
- Some minor shortcomings with version 4
- Still free ($) and open source unlike other distribution
- Typically, the differences between the beta and final releases of BT are very minor

References

- *The Best Damn Cybercrime and Digital Forensics Book Period* by Jack Wiles and Anthony Reyes (Syngress, 2007)
- *In My Jump Bag: BackTrack 4* by Ming Chow. HTCIA Firewall, Volume 2, Issue 1, 2009.
- **http://www.remote-exploit.org/backtrack.html**
- **https://wiki.remote-exploit.org/backtrack/**
- **http://www.offensive-security.com/blog/backtrack/backtrack-forensics/**
- **http://lifehacker.com/5305094/how-to-crack-a-wi+fi-networks-wep-password-with-backtrack**