Katana:
Portable Multi-Boot Security Suite

JP Dunning
DefCon 2010
JP Dunning

**Graduate Student:**
Computer Science, Virginia Tech

**Research Focus:**
Wireless and Portable Security

**Website:**
www.hackfromacave.com
To Many Tools!

- Finding Tools
- Cases of CDs
  - Keeping up with disks
- Tools on different devices
- Using different Operating Systems
- Indecent Response
  - Need It Now!
Katana

- Run from USB Flash Drive
  - No partitioning necessary
- Security Tools:
  - *Katana Tool Kit*: 100s of portable Windows applications
  - *Katana Live*: A dozen Live Distributions
  - Consolidation of tools onto one medium
- User configurable list of security related tools
  - Add, Remove, Update
## CD vs USB

<table>
<thead>
<tr>
<th>Attribute</th>
<th>CD/DVD</th>
<th>USB Flash Drive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write Speed</td>
<td>~ 5 MB/s (32x) / ~ 21 MB/s (16x)</td>
<td>~ 25 MB/s</td>
</tr>
<tr>
<td>Read Speed</td>
<td>~ 8 MB/s (52x) / ~ 26.5 MB/s (20x)</td>
<td>~ 35 MB/s</td>
</tr>
<tr>
<td>Transfer Rate</td>
<td>X * (150kb/s)</td>
<td>~ 60 MB/s</td>
</tr>
<tr>
<td>Environment</td>
<td>Static</td>
<td>Dynamic</td>
</tr>
<tr>
<td>BIOS Boot Support</td>
<td>Early 90's</td>
<td>Early 00's</td>
</tr>
<tr>
<td>Disk Space</td>
<td>700MB/4.7GB</td>
<td>128 MB–256 GB</td>
</tr>
<tr>
<td>Physical Space</td>
<td>~ 12x12x0.1 cm</td>
<td>~ 4x1.5x0.5 cm</td>
</tr>
<tr>
<td>Time To Failure</td>
<td>~ 1,000 writes OR 3 – 5 years</td>
<td>~ 10,000 to 100,000 writes OR 5 to 10 years</td>
</tr>
<tr>
<td>Bootable Tools</td>
<td>More</td>
<td>Less</td>
</tr>
</tbody>
</table>

© Shadow Cave LLC
Who Made The Cut?

- Security related
- Free (at least for personal use)
- Unique contribution
- Currently supported
Katana Live

KATANA 2.0
Backtrack
Ultimate Boot CD
UBCD4Win
Trinity Rescue Disk
Ophcrack
CAINE
Clonezilla
Puppy
Derik’s Boot and Muke
Ron-Boot

KATANA

More about currently selected:

BackTrack is a penetration testing arsenal that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking.
Katana Included Distros

- Backtrack
- Ultimate Boot CD
- UBCD4Win
- Ophcrack
- Puppy

- CAINE
- CloneZilla
- Trinity Rescue Kit
- Derik's Boot and Nuke
- Kon-Boot
Getting the Darn Thing to Work

- Boot loader **syslinux**
  - USB bootloader
- Binary Configuration file editing
  - Initd file
- Clean Up
  - Minimizing the mess of folders and files
Add Your Own Distros

- Each distro requires different modifications
  - Often change to init file
  - Modify \textit{cfg} menu file
  - Change file/directory names and structures
Example: Adding Samurai 0.8

1) Download Samurai from: samurai.inguardians.com

2) Extract/Burn Samurai ISO
   1) Extract using 7zip, isomaster, mount
   2) Burn Nero, k3b

3) Create “samurai” directory in root of Katana USB Flash drive
4) Go to “/casper” directory and edit init*.gz files

   1) Extract Gzip
   2) Edit “casper” file in “scripts” directory to point to the “samurai” directory
      1) Replace “$path/casper” with “$path/samurai/casper”
      2) Replace “$path/.disk/casper-uuid” with “$path/samurai/.disk/casper-uuid”
      3) Replace “$directory/casper” with “$directory/samurai/casper”

   - Rezip directory
Example: Adding Samurai 0.8

5) Add samurai boot menu
   - Open samurai.cfg in “boot” directory of samurai
   - Add “/samurai” in front of all strings with “/casper” and “/preseed” in them.
   - Move samurai.cfg to “/boot/menus” on Flash Drive.

6) Edit “/boot/menus/main.conf” to add samurai
   LABEL Samurai
   MENU LABEL Samurai
   KERNEL /boot/vesamenu.c32
   APPEND /boot/menus/samurai.cfg
NEW: Forge 0.1

- Install additional distributions to Katana
- Front end for installation scripts
  - Runs *bash* and *batch* scripts for Linux and Windows
- Users can post installation scripts on forum.hackfromacave.com

© Shadow Cave LLC
Operating Katana

- Configure host system to boot from USB
  - BIOS Configuration
  - Boot Options (F12)
- Navigation
  - Use up and down arrows to navigate
  - Use enter to make selections
  - Navigate backwards by selecting “..”
- Many tools are loaded form subfolders
Katana Toolkit
Katana Toolkit

- 100s of portable applications
- Portable Window Applications
  - Run natively from USB Drive on any Windows system
  - No resources installed on base system
- Run in other environments
  - Run in BartPE/UBCD4Win
  - Run under Wine on Linux
- Configurable / Updatable
Add Your Own Apps

• Install Windows apps into a subdirectory in /PortableApps
  – Example: /PortableApps/NetCat/netcat.exe

• Add Linux apps
  – Statically compiled binaries

• Add OSX apps ???
Getting Katana

- Free @ www.hackfromacave.com/katana.html
  - Released under GPL v2
  - Check specific tool licenses
- Size: ~ 4GB in size
- Download:
  - Torrent (preferred)
  - Direct Download
- Recommend install on 16GB+ Flash Drive, but fits on 8GB
Tips & Tricks

• Statically compile and link binaries
• Create/add Slax modules for some of the included distros
• For portable windows applications check out
  - http://portableapps.com/
  - http://www.pendriveapps.com/
• For portable OSX applications check out
  - http://www.freesmug.org/portableapps/
• Scripts are the bread and butter of portability
Installing Katana

1) Download **katana-v2.0.rar** to local disk.

2) Extract **katana-v2.0.rar** to the root of the USB flash drive.

3) Change directory to the freshly copied "boot" directory on the USB device.

4) Run the following with administrative privileges. For Linux/OSX run **./boostinst.sh**, for Windows run **./boostinst.bat**.

5) Boot from flash drive.

All Done!
NEW: Creating a Customized ISO

- Customize your own Katana
  - Add/Remove Distros & Apps
- Run the ISO creation script
  - `create_iso.bat` (Windows) or `create_iso.sh` (Linux)
    - located in `/boot` directory
    - Select a location for the iso
Help me Obi-Won Kanobie, Your my only Hope!

- Post installation directions for distros and portable applications on forum.hackfromacave.com.
- What have you done to configure these tools?
- What live distros and portable applications do you use or would like to see added to Katana?
- Can you use these tools in your work environment?