The Kali Linux Dojo - Rolling Your Own ISOs
Before We Begin

Update Your Kali Linux OS

MAKE SURE YOU’RE CONNECTED

Verify you’re connected to the wired network and are getting an IP address. Also verify that http.kali.org resolves locally.

UPDATE THE CORE TOOLS WE’LL BE USING

Update your toolsets, specifically **git**, **live-build**, and **cdebootstrap**, as shown on the image on the left.
Kali Linux Dojo - Introduction
A Tale of Two Workshops

- Mati Aharoni, Kali Linux Developer
- Back to back workshops around the Kali Linux OS
  - Dojo 01 - Rolling Your Own
  - Dojo 02 - Ultimate Kali on USB
- Big thanks to Black Hat & DEF CON for hosting us!

WORKSHOP 01
Rolling Your Own ISOs
Customize all aspects of the Kali 2.0 ISO build using Live Build.

WORKSHOP 02
Ultimate Kali USB
Create Kali 2.0 Live USB images with persistence and encrypted storage.
What is Kali Linux?
More Than a Collection of Penetration Testing Tools.

- An Open-Source **Penetration Testing Distribution**
- Developed by **Offensive Security**
- Kali Linux is **more than a collection of security tools**
- **Kali LUKS Nuke** - Show of hands?
- Allows for the “**self destruction**” of your LUKS encrypted drive
- This Dojo is a **great opportunity** to demonstrate advanced features of Kali
More Than A Collection Of Tools
You Keep Using That Word…
Kali Linux 2.0 Teaser Video
Kali Linux 2.0 - What’s New?
Now a Rolling Distribution

- Kernel 4.0, Gnome 3.14
- Based on Debian Jessie
- Now a rolling distribution - big implications
- Upstream monitoring of tool updates
- Better workflow, new UI, reworked menus

"If Kali 1.0 was focused on building a solid infrastructure then Kali 2.0 is focused on overhauling the user experience and maintaining updated packages and tool repositories."
Building Kali Linux ISOs
Getting the Right Tool for the Job, Every Time.

**LIVE BUILD**

Live build is a set of wrapper scripts around `debootstrap` which contain the components to build a live system from a configuration directory. Allows you full customization of generated Kali Linux ISOs.

**THE FREEDOM TO CHOOSE**

Live build allows you to choose different Desktop Managers as well as customize your toolsets - down to adding custom files, scripts, and hooks to your custom Kali ISO.
Live build divides the ISO creation process into 3 distinct phases:

1. **BOOTSTRAP**
   - The initial phase of populating the chroot with packages to make a barebones Kali system.

2. **CHROOT**
   - Completes the construction of the chroot directory, populating it with listed packages.

3. **BINARY**
   - Builds a bootable image including installer using the parameters and configurations set.
git clone git://git.kali.org/live-build-config.git

- **kali-config** - templates for various Kali build flavours
- **kali-config/common/includes.installer** - preseeding
- **kali-config/config/package-lists** - list of packages
- **kali-config/config/hooks** - bash script hooks
- **kali-config/config/includes.chroot** - overlaying files
Building Kali Linux ISOs
Which Flavour Do You Like?

- ./build.sh --variant {gnome,kde,xfce,mate,e17,lxde,i3wm,light}
- ./build.sh --arch {i386,amd64,armel*,armhf*}
- ./build.sh --distribution {moto,sana,kali-rolling}
  *COUGH*
- ./build.sh --distribution sana
- ./build.sh --distribution sana --variant kde --arch amd64 --verbose
Hold On to Your **Horses**
Let’s Make a *Really* Cool Kali 2.0 ISO.

- Let’s get **even more granular**…and make deeper customizations to our build.
- For the sake of local bandwidth and build time, we’ll build “light”, **minimal versions of Kali**.
- Depending on your computer speed and network performance, it could take **a good 20 minutes**.
- You are welcome to **try this at home**!
Try It Yourself
http://archive.kali.org/workshop01.txt

1. Self-Installing ISO
   The ISO will self-install in an unattended way in a Virtual environment with a predictable set of answers.

2. Start SSHD at Boot Time
   As services are disabled by default in Kali, we need to explicitly allow the SSH service to start at boot time using `update-rc.d` commands. We can do this with `hooks`.

3. Custom Wallpaper
   Change the custom wallpaper with one of your own by simply overwriting the existing one. A well-styled Kali / Black Hat wallpaper will do!

4. Add Your Own SSH Public Key
   As SSH only allows root login with a key (by default) in Kali 2.0, let’s add our SSH key to the ISO ahead of time by overlaying the file in `~/.ssh/authorized_keys`
Preseeding Unattended Installations

Adding Some Foo to Our Boot Menu
Kali Linux ISO Of Doom

QUESTIONS and ANSWERS
muts@kali.org

Go ahead. Ask away.
THANK YOU FOR JOINING

KALI LINUX™

“the quieter you become, the more you are able to hear”