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. Make sure you’re resolving [http.kali.org](http://http.kali.org) locally!

- **INSTALL THE CORE TOOLS WE’LL BE USING**
  Update your toolsets, specifically **git**, **curl**, **live-build**, and **cdebootstrap**, as shown on the image on the left.

apt-get update
apt-get dist-upgrade
apt-get install curl git
apt-get install live-build
apt-get install cdebootstrap
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

“the quieter you become, the more you are able to hear”
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 --variant xfce --verbose
MR. ROBOT DID NOT ATTEND THE KALI DOJO.
“THERE MUST BE A BETTER WAY...”
Try It **Yourself**

https://kali.training/exercises/ex-chapter-9-live-build/

1. **Minimal, Optimized Live Boot ISO**
   Minimal ISO, Live boot, non GUI, few tools *nmap*, *metasploit-framework* and *cryptsetup*.

2. **Custom Startup Script via Systemd**
   Automate the SSH connection Angela messed up - have it start up at boot time automatically. We can do this via live hooks.

3. **Self Installing ISO / OS backdoor**
   Self Installing ISO - just because we can, and it’s cool! We’ll add a preseed file which will allow for an unattended installation.

4. **Expected build time - 25 mins**
   Depending on the toolset you choose and your network speed, build times could be longer. You are welcome to try more complex setups at home!
Preseeding Unattended Installations

Adding Some Foo to Our Boot Menu

"the quieter you become, the more you are able to hear"

Boot menu

- Live (amd64)
- Live (amd64 failsafe)
- Live (forensic mode)
- Live USB Persistence (check kali.org/prst)
- Live USB Encrypted Persistence (check kali.org/prst)
- Install
- Graphical install
- Unattended Install
- Install with speech synthesis
- Advanced options
Kali Linux ISO Of Doom
Go ahead, try it!

https://kali.training/exercises/ex-chapter-9-live-build/