Kali and ICS Lab Overview

Capacity Building for Control System Security Collaborative Project

Greg Randall

Program Chair Computer Information Systems

Snead State Community College

Outline

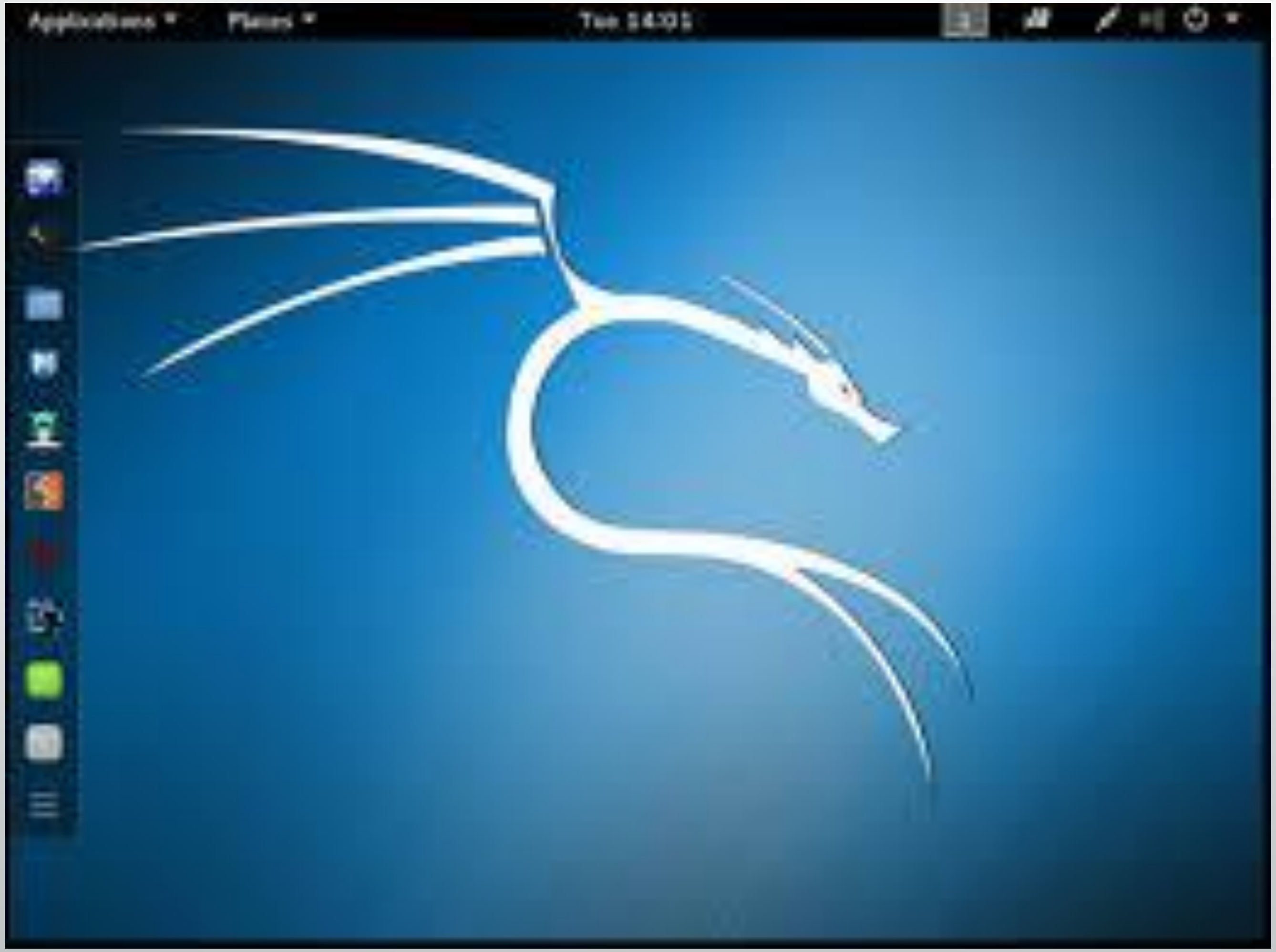
- Overview the Kali Linux OS
- ICS Labs
- Overview of Metasploit
- Overview of Armitage

Kali Linux

- Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.
- Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company. Kali replaced Backtrack as the penetration testing of choice.
- Kali Linux is specifically tailored to the needs of penetration testing professionals, and therefore prior knowledge of, and familiarity with, the Linux operating system is assumed.

Source: https://docs.kali.org/introduction/what-is-kali-linux

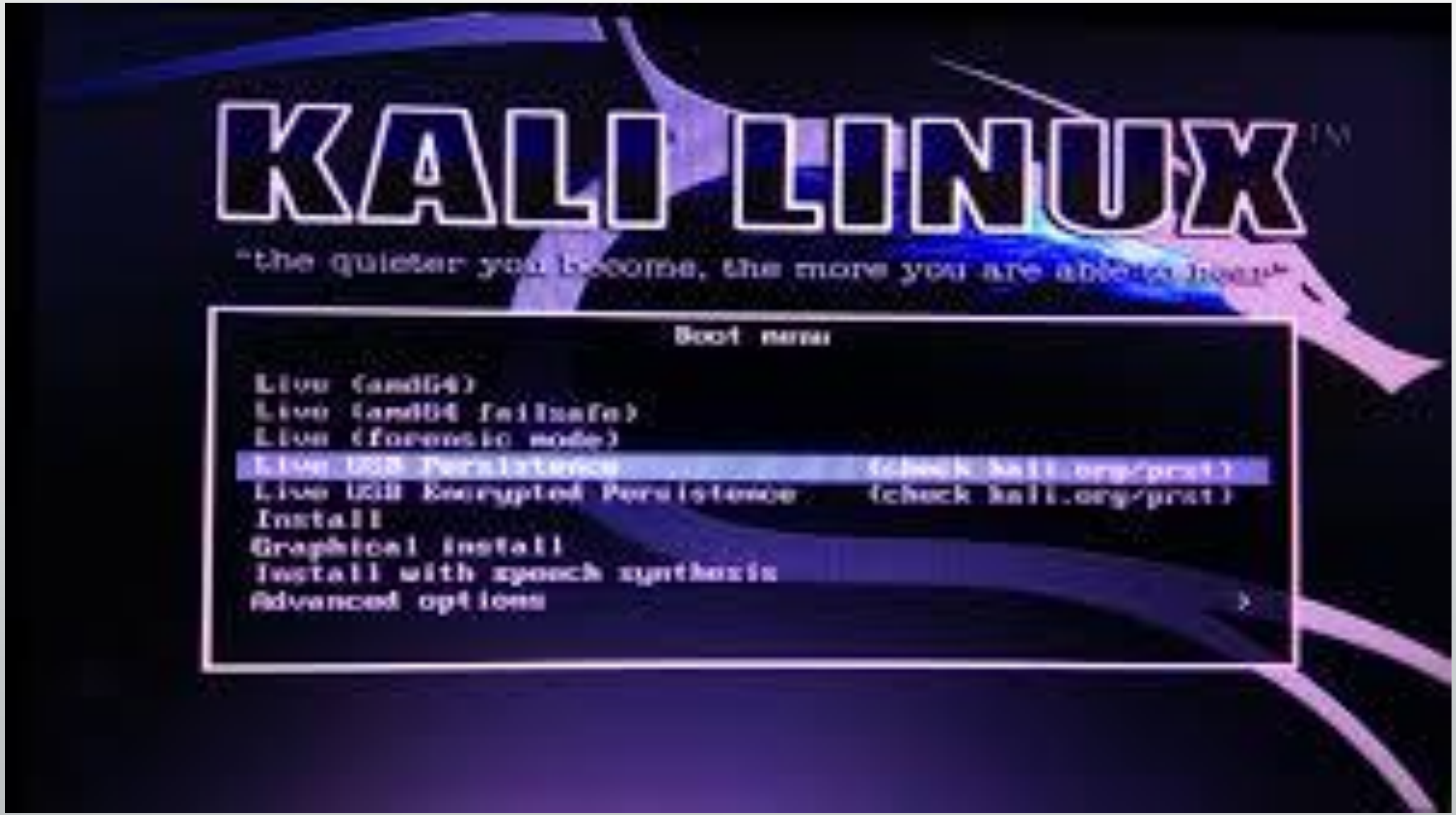
Kali Linux



ICS Labs

- The labs performed in the ICS portion of the workshop require Kali Linux (32bit) and a bootable USB drive
- Each lab will require booting to Kali Live Persistence in order to save files, payloads and scripts
- The BIOS of the device on which the Kali Live Persistence is booted must support USB booting options
- No downloaded applications can be saved between reboots of the USB OS
- Complete instructions for making a Live Kali USB bootable device can be found here: https://docs.kali.org/downloading/kali-linux-live-usb-install

Live USB Persistence Option at Boot



```
                    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
Install with speech synthesis
Advanced options                                            >
```

ICS Workshop Labs Overview

- Labs for the ICS workshop will consist of 8 labs containing the following topics:
- Day 1 Workshop (Thursday)

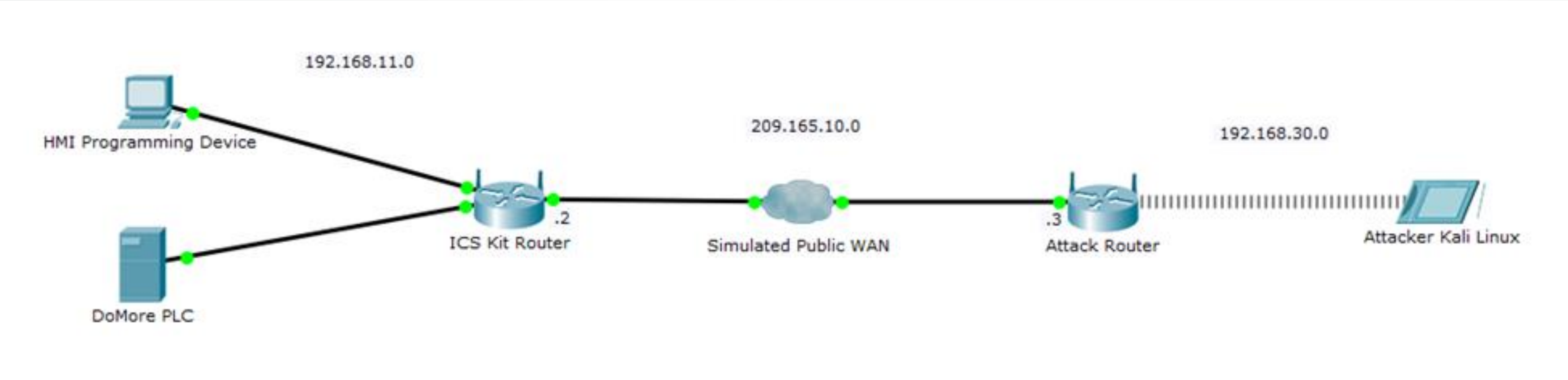
1. ICS Lab 1 Hacking a Wireless Network- Overview
2. ICS Lab 2 Scanning and Enumerating- Overview- How to boot into Kali Linux
3. ICS Lab 3 Packet Capture and Analysis- Overview- How to boot into Kali Linux
4. ICS Lab 4 Deep Packet Capture and Analysis

ICS Workshop Labs Overview

- Labs for the ICS workshop will consist of the following topics:
- Day 2 Workshop (Friday)

5. ICS Lab 5 Installing Veil-Evasion- Overview
6. ICS Lab 6 Using Python SimpleHTTPServer- Overview
7. ICS Lab 7 Exploiting a PLC Using Metasploit
8. ICS Lab 8 Exploiting an HMI Device Using Armitage

ICS Lab Topology



Metasploit

- The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
- The Project is contained in the Kali Linux OS and will be used in Day 2 of the Workshop

Source: https://en.wikipedia.org/wiki/Metasploit_Project

Armitage

- Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets (GUI-Based), recommends exploits, and exposes the advanced post-exploitation features in the framework.
- Armitage will be used in Day 2 of the Workshop

Source: https://tools.kali.org/exploitation-tools/armitage

Questions??