

Kali Linux – An overview

Michael Claudius, Associate Professor, Roskilde

10.04.2020

What is Kali Linux

- A toolkit for Penetration Testing and Security Auditing System
- Developed by Offensive Security <https://www.offensive-security.com/>
- 300+ various tools some say 600 tools
- A Github repository <https://gitlab.com/kalilinux>
- Free training and fee-based courses and penetration tests

Downloads

- Later in the exercise you will install Kali Linux
- 1. Install besides Windows 10, DON'T !
- Install it in VT-box YES, Using either
- 2. Download .iso file (3.3 Gb) and install like Ubuntu
- <https://www.kali.org/downloads/>
-
- 3. Download the .ova-file (premade 3.9 Gb VT-box image)
- <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>
- 4. Teachers' USB-stick !!
- 3 or 4 recommended. Notice the 2019 version is actually better and stronger than 2020 version !

Applications in Kali Linux

- Tools divided into 14 sections <https://tools.kali.org/>
- Information gathering
- Wireless attacks
- Vulnerability analysis
- Web applications
- Forensics
- Exploitation
- Stress tests
- Sniffing and spoofing
- Password attacks
- Etc etc

- Let us look at a simple tool nmap

Tutorials

- Thousands and thousands and also on YouTube
- Just two examples aircrack-ng and nmap
- Aircrack-ng hack your wireless router
- <https://www.kalitutorials.net/2013/08/kali-linux.html>
- Nmap scanning devices, services and ports on the network
- And action ! Demonstration of nmap.

Network Mapping (Nmap) package

- **The primary goals of the Nmap Project is**
- **To help make the Internet a little more secure**
- **Provide administrators/auditors/hackers with an advanced tool for exploring their networks**

- **Tools included:**
- **nmap**
- **ndiff**
- **nping**
- **ncat**

Assignments

- Time for a little discussion and hard practical work
- Download Kali Linux
- Investigations
 - Get an overview of tools
 - Decide to investigate nmap and 2 other tools
 - Run as fast as you can
 - *Just follow the "right" track and you find the gold mine*

All this is explained in [Kali Linux Tools Exercise](#)

