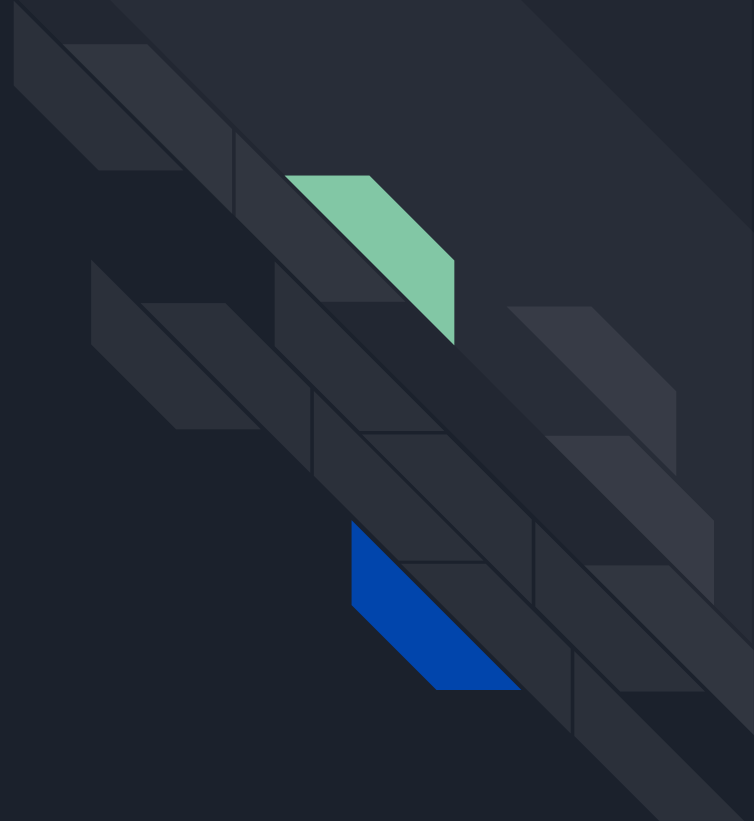


# Day 4: Kali Linux (basics)

Nemuel Wainaina

28th March 2024



# > whoami

Nemuel Wainaina

- Software Engineer
- Security Researcher
- Technical Instructor (1.7k+ students)



Github : <https://github.com/nemzyxt>

LinkedIn : <https://linkedin.com/in/nemuel-wainaina>

Twitter : <https://twitter.com/nemuelwainaina>

Medium : <https://medium.com/@nemzyxt>



## > a bit on Kali Linux ...

- It is a Debian-based distribution designed for use by cybersecurity practitioners on things like pentesting and digital forensics.
- Comes preinstalled with 600+ tools for this work.
- Some of the benefits of using it for cybersecurity are:
  - tools are preconfigured, so no need to install them separately
  - nice organization of tools by the purpose they serve eg. exploitation, information gathering, etc.
  - cross-platform compatibility, meaning it can be installed and used across a variety of hardware platforms and architectures.
- To download Kali Linux: <https://www.kali.org/get-kali/#kali-platforms>



## > demo: cracking a WPA key

- Challenge link: <https://cybertalents.com/challenges/machines/wpa-crack>
- Download the **cap** file (handshake capture): Remember the 'wget' command?
- Look through the 'Wireless Attack' tools and choose the right one (aircrack-ng)
- Go through its usage (manual pages or even help menu)
- Choose a wordlist to use (under 'Password Attacks' -> 'wordlists') eg. rockyou.txt
- Execute the command to start cracking ...
  - ***aircrack-ng -w /path/to/rockyou.txt /path/to/handshake.cap***



## > next steps

- Practise, practise, practise!
  - Learn Bash scripting
  - Learn version control with git
  - Practice using Kali Linux (ethically!)
  - Share your newly acquired knowledge & skills with others
- 
- You can also now consider building your own cool Linux distro in future 😊🎉



# Q&A