
"the quieter you become,
the more you can hear"
KALI
BY OFFENSIVE SECURITY

What is KALI LINUX

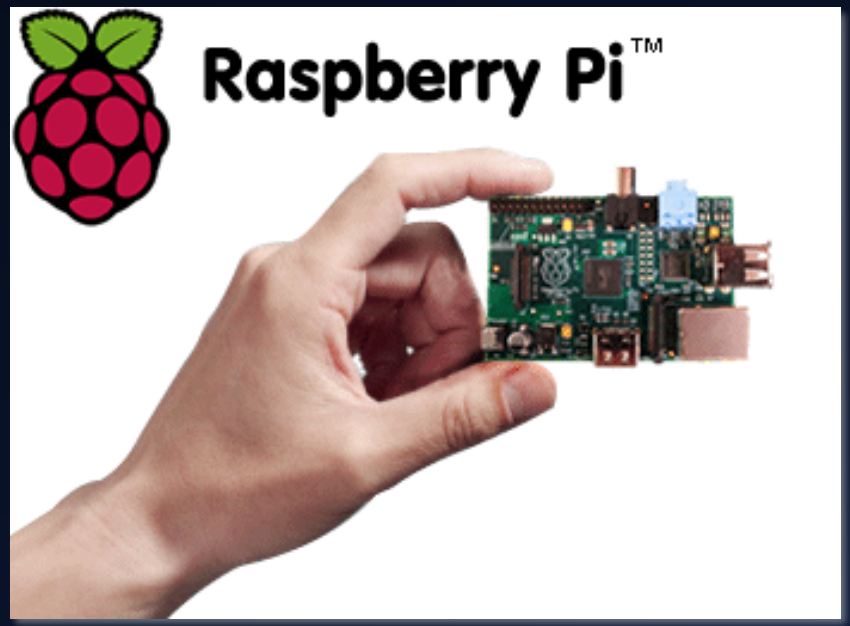
- Debian-derived Linux disto
- Member of UNIX OS family
- Maintained and funded by Offensive Security
- Primarily designed for Penetration Testing and Digital Forensics
- Completely customizable
- Free and always will be

Security Tools

- Metasploit – Develop and Execute Exploit Code
- John the Ripper – Password Cracker
- Nmap – Port scanning, services, and OS fingerprinting
- Aircrack-ng – Wireless Network “Auditing”
- Open-VAS – Vulnerability Scanner (add-on)
- Wireshark – Analyze Packets

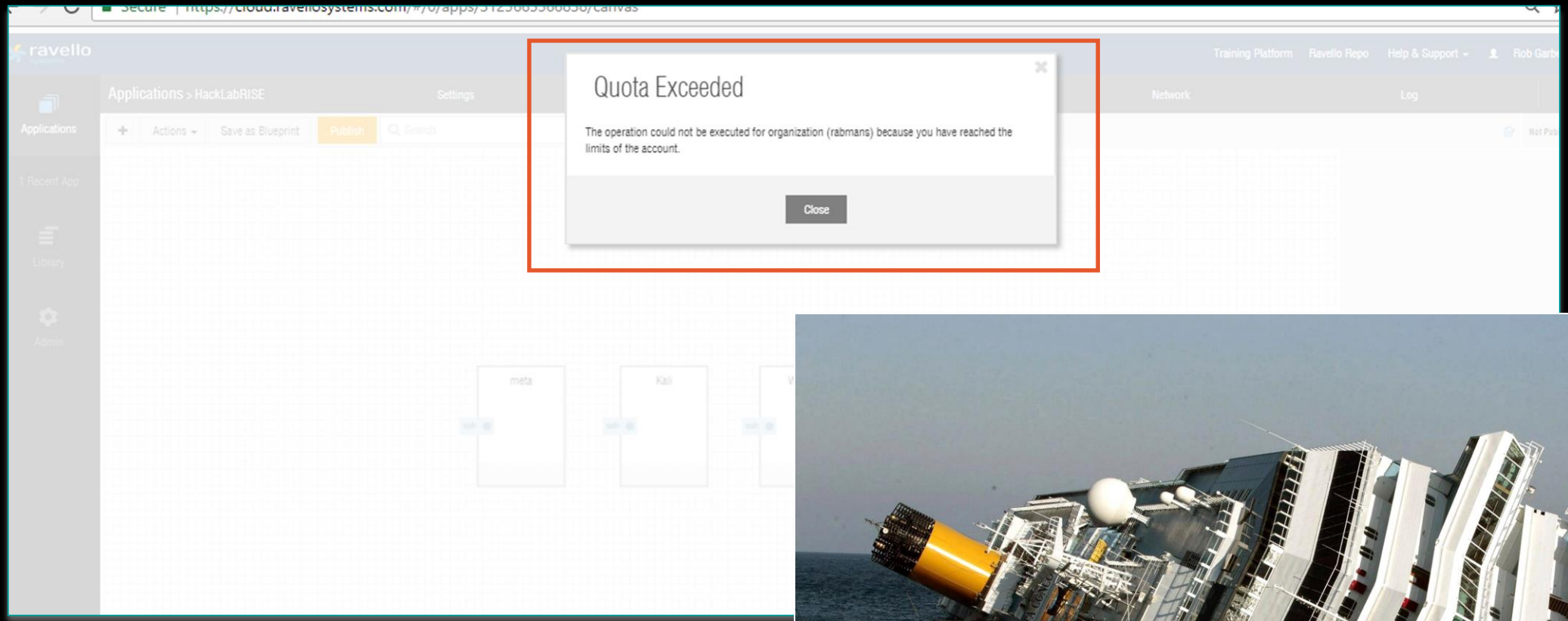
Flexibility of KALI LINUX

- Run on multiple platforms and methods
  - Installed locally to hard drive
  - Can be booted from live CD or USB
  - Virtual machine
  - Android
  - ARM devices



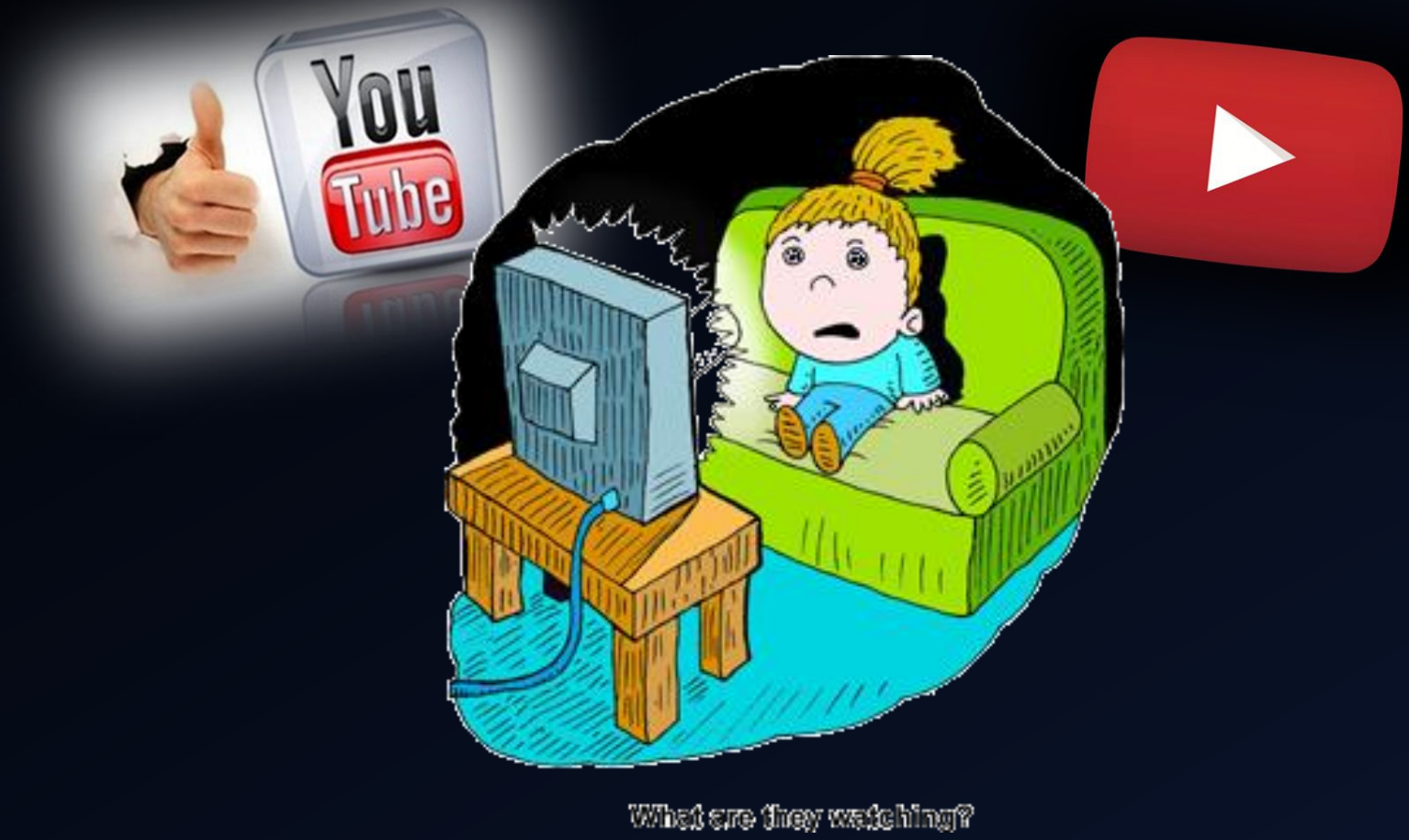
Demo time!

- My Hack Lab
  - Oracle Ravello
    - Thanks Grant
  - Flat network
  - Kali Linux
  - Windows 10
  - Metasploitable


ravello
Training Platform
Ravello Repo
Help & Support
Applications > HackLabRISE
Settings
Network
Log
Applications
Actions
Save as Blueprint
Publish
Library
Admin
meta
Kali
Quota Exceeded
The operation could not be executed for organization (rabmans) because you have reached the limits of the account.
Close


CARABINIERI
All aboard the failboat!!!

Thanks YouTube!



What follows has not been really reviewed for content. The presenter is not responsible for improper language use or just plain stupidity.

Thanks YouTube!

- MetaSploit – https://www.youtube.com/watch?v=Cs3LYS6pv6M
- John the Ripper – https://www.youtube.com/watch?v=eAn8dYdn1eY
- Aircrack-NG – https://www.youtube.com/watch?v=xGDkMutoz5Y
- NMAP –

Their all silent movies, so I'm gonna use my laptop

Offensive Security Certificates

- Offensive Security Certified Professional - OSCP
  - Penetration Testing with Kali Linux
- Offensive Security Wireless Professional – OSWP
  - Offensive Security Wireless Attacks (WiFu)
- Offensive Security Certified Expert – OSCE
  - Cracking the Perimeter (CTP)

Offensive Security Certificates

- Offensive Security Exploitation Expert – OSEE
  - Expertise in advanced windows exploit development
- Offensive Security Web Expert – OSWE
  - expertise in advanced web application exploitation

A warning!

Use of these tools against a live website, for which you do not have permission, is illegal and may land you in jail

Important Laws

18 USC Section 1029: The Access Device Statute

18 USC Section 1030 of The Computer Fraud and Abuse Act