QUBES OS 4

A reasonably secure operating system

FIRST TC - 10 september 2018
Presented by Xavier BAHUON, CISSP at ACTION CYBER
Summary

- What is Qubes OS ?
- How does it works ?
- Use case :
  - Receipt of documents (HR, Marketing…)
  - Administrator IT
  - Pentesting Lab
- And more…
- Gaps and roadmap !
What is Qubes OS?

- License GNU GPL v2
- Hypervisor “bare metal” : Xen OS
- Virtualize : Linux, Windows
- Approach : Don’t trust the hardware
What is Qubes OS?

- Hardware Compatibility List
How does it works?

Architecture of QUBES OS
Use Case -> Receipt of documents (HR, Marketing...)

From: Pamela
To: Xavier
I send you my photo!
-> Kiss.jpeg

CV_Manager.pdf
Contract.doc
Use Case -> Administrator IT

Same machine but compartmentalization

- VM facebook
- VM shopping
- VM work
- VM critical

- firewall-internet
- IP tables
- sys-wifi

- firewall-intranet
- IP tables
- sys-net

- vpn-intra
  - OpenVPN
  - SSH

INTRANET -> DMZ
Use Case -> Pentesting Lab

VM Kali

Pentest-FW

IP tables

Pentest-NET

Network card
OR None

VM vuln

VM test
And more...

- The Salt Deployment architecture
- Anonymization with Tor

→ www.qubes-os.org
Gaps and roadmap!

- Air GAP
- Forensic lab
- GPU-passtru
Thank you for your attention

Questions ?