Wanna TEMPEST your computer?

Florian Barbarin, Maxime Gagliardini and Guillaume Squillaci

TLS-SEC

March 12, 2018

TLS-SEC

Toulouse Hacking Convention

Table of contents

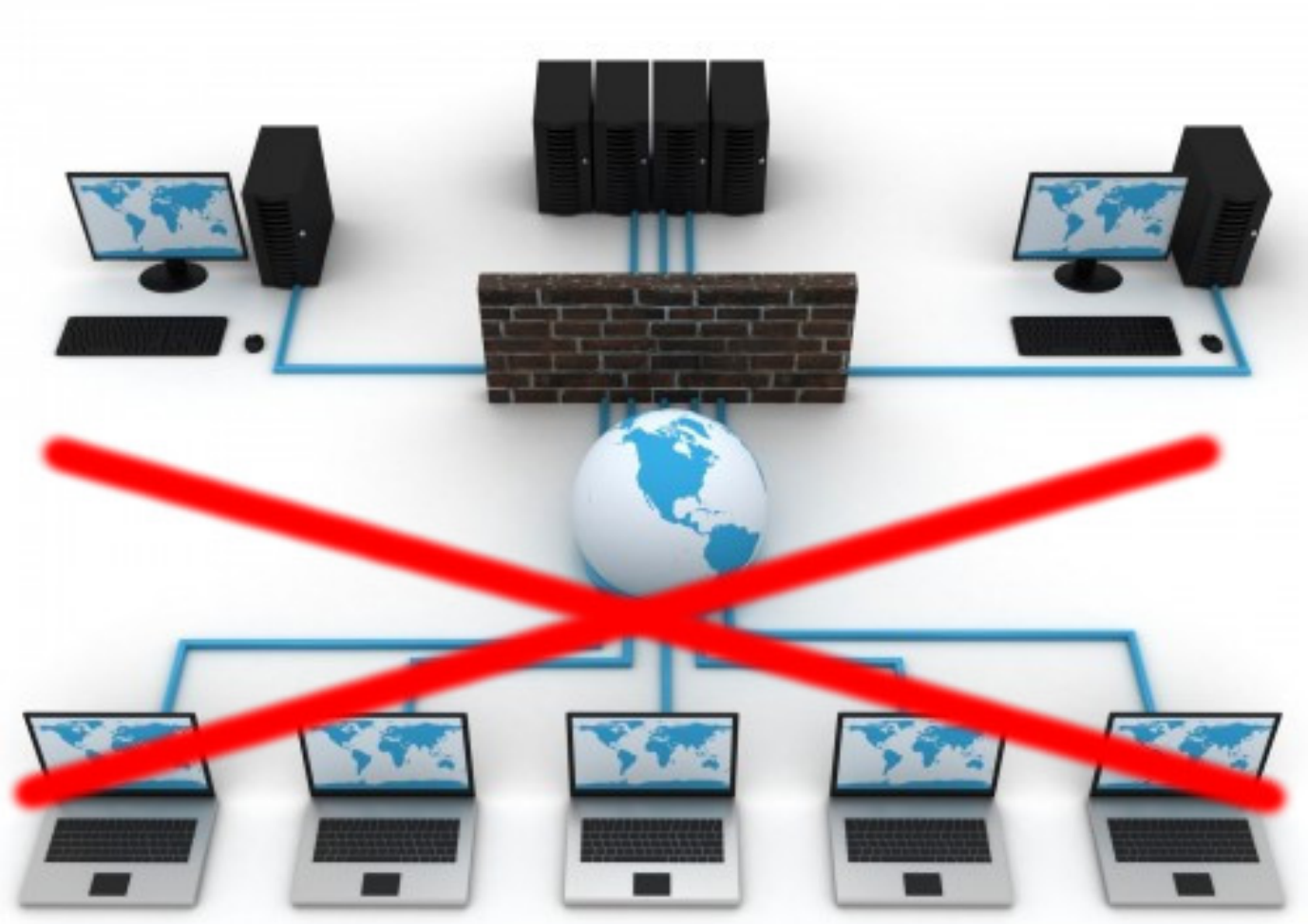
"Projet long" context

THC 2018 Challenge

- Prepare tutorial challenge
- Work based on *GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies* (24th USENIX Security Symposium)
- "Challenge" : data exfiltration form an air-gapped computer
- "Tutorial" : guide the challenger step-by-step
- Main idea : follow how we succeed to reproduce a part of the paper

Air-gapped networks

Air-gapped networks



Electromagnetic emanations

Emanations

- Each electronic device has emanations
- Could be electronical, acoustical, mecanical or electromagnetical
- Focus on electromagnetic emanations

TEMPEST

- Name given by NSA for standards protecting against electromagnetic emanations
- Context : EMSEC, surbpart of COMSEC

Challenge context

Goal

Get a password stored on the air-gapped computer

Problem

Air-gapped computer $\Longrightarrow$ no possibility to gain access and/or exfiltrate data via network

Solution

Use electromagnetic emanations to create a covert channel and exfiltrate data

Technical environment

Devices

- 1 air-gapped computer (attacked computer)
- 1 standard computer (attacker's computer)

Tools

- Spectrum analyzer
- Software-defined radio : USRP/RTL-SDR
- Antennas
- Softwares : URH/GNURadio

Table of contents

Test

test

- test

Table of contents

Test

test

- test

Table of contents

Test

test

- test

Table of contents

Test

test

- test