Topics 2021

BTI7311p (23.02.2021)
Gerhard Hassenstein

FS 2021
1. ReconSpider

► «ReconSpider» is an advanced Open Source Intelligence (OSINT) Framework.
► What is OSINT?
► Use «ReconSpider» to gather information of different sources in a victim network and make yourself a picture of it.
► «ReconSpider» is used by Researchers, Penetration Testers as well as Defenders.
► Based on the gathered information try to establish an attack scenario.
► https://github.com/bhavsec/reconspider
2. SCRAM (Salted CRAM - RFC5802)

- Examine SCRAM according to RFC5802
- Explain the term «Channel Binding»
- Explain why and how «Channel Binding» is used in SCRAM
3. SIOP (Self-Issued OpenID Connect Provider)

- Explain Self-Issued OpenID Connect Provider DID Profile (SIOP) and the enhancements of SIOP v2
- https://identity.foundation/working-groups/authentication.html
4. AusweisApp2

- Explain the functionality of nPA and the new «AusweisApp2».
- Test the functionality of the AusweisAppv2 using a nPA (neuer deutscher Personal Ausweis).
- You don’t need to have a physical nPA, because you should be able to install a test environment (a kind of emulation) on your computer/smartphone or tablet.
- [https://www.ausweisapp.bund.de/ausweisapp2](https://www.ausweisapp.bund.de/ausweisapp2)
5. How-to detect hidden devices

- In the last years many institution bought digital surveillance equipment with the goal to survey their employees, guests, etc. – without the subject being aware of this.
- Such practices are illegal and a breach of a data protection legislation!
- Is it possible to detect hidden cameras, GPS trackers, Bluetooth trackers - in general any listening devices in home networks, at the office, hotel, and outside?
- What are the techniques used?
Other Question / Discussion