P1 Security

Priority One Security

2022

Training Description

TS-250 IMS Security & attacking telecom infrastructure

TS-250 IMS Security & attacking telecom infrastructure

Description of Training Class

Learn about modern telecom and mobile system and networks in the context of IMS and NGN core networks. The trainee will learn also about the core evolutions of the legacy telecom networks into IMS networks and the reuse of IETF-based protocols in the context of IMS along with its main benefits.

Duration

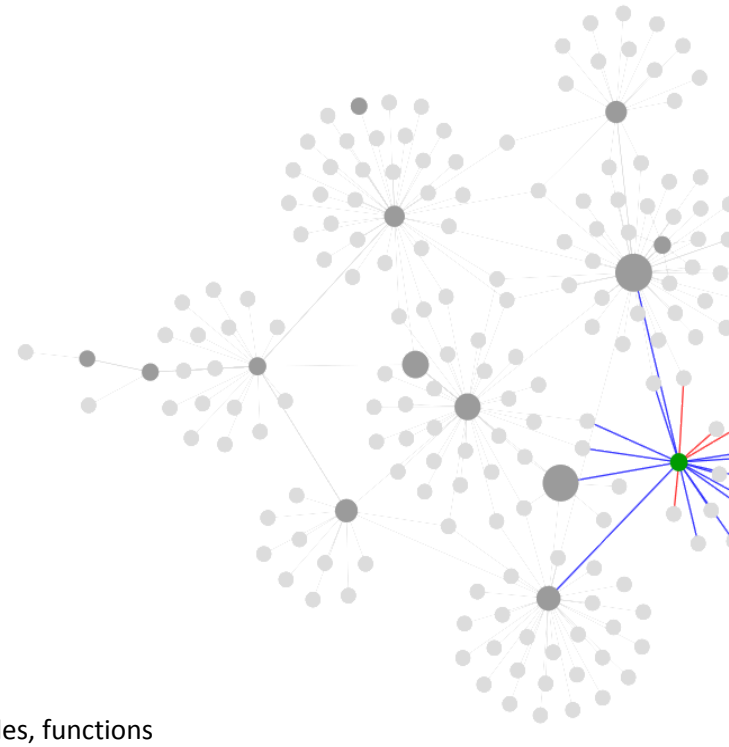
- Unique version: 3 days

Attendees will receive

- Training material: copy of the presenter's slides through Intralinks Web platform tool for a one Year duration after the training's delivery.

Pre-requisites of training class

- Basic knowledge of telecom & network principles:
  - What is 2G, 3G;
  - OSI network layers;
  - Basic knowledge of telecom technologies;
  - Basic knowledge of Linux.
- Laptop with Kali Linux installed either in VM or native;
- Good knowledge and usage of Wireshark;
- Good IT security background.



Covered in this training

- IMS Introduction
- IMS Benefits
- IMS Technologies
- Root of the technology of IMS
- IMS Security Architecture
- IMS-specific Protocols study
  - SIP IETF
  - SIP-I
  - SIP-T
  - Diameter
- Overview of other protocols still used in IMS
  - GTP-C
  - GTP-U
  - GTP v2
  - GTP'
- IMS Network Elements overview and security roles, functions
  - HSS
  - CSCFs: I-CSCF, P-CSCF, S-CSCF

    - BG / BGCF
    - MGCF
    - SGW
- Specific Network Elements in recent version of IMS core networks
    - SDP / SDR
    - PCRF
- Security of the different IMS planes
    - Access
    - Transport
    - Control
    - Application
- IMS Communication security
- Open Source IMS tools
- IMS network element fingerprinting
- Typical attacks on IMS infrastructure
- Role of legacy in IMS security
    - interconnection with SS7 signaling network element
    - H248
- Vulnerabilities of some Voice over IP protocols:
    - SIP-I
    - SIP-T
    - H323
- Analysis of Network Element and vulnerabilities
    - Generic IMS Network Element vulnerabilities
- Diameter security
- Scenario of attack of IMS network
    - Radio-based, subscriber role
    - Infrastructure-based, Transmission or RAN vector
    - Internal-based, attack

Next steps to become an IMS network auditor.