Title: Attacking 5G infrastructure and Defense

Short Course Abstract/ Session Description

This Training will help security professional, managers, security enthusiast, telecom security planning member and telecom professionals to get an understanding of the key concepts of 5G, security, different attacking technique. security threat modeling the implementation of such architectures and the impact in terms of related risks.

This project-based workshop style 5G cybersecurity training will identify several 5G use case (network slices) scenarios and demonstrate for each one how to strengthen the 5G architecture components to mitigate identified risks and meet cybersecurity compliance requirements.

Full Course Abstract

5G Penetration testing is a critical part of maintaining and fortifying your IP, network and physical security. This Training course prepares participants to conduct successful 5G penetration testing and ethical hacking. Participants will learn about tools and techniques to analyze 5G vulnerabilities, how to perform detailed 5G reconnaissance. ENISA's threat landscape for 5G Networks and NIST 5G cybersecurity/RMF prepares you with a secure evolution to 5G.

The goal of this practical course is to give the participant a strong and intuitive understanding of what cybersecurity in the 5G systems is and how the security functions are implemented in the 5G, 5G NR, Cloud RAN, MEC, 5GC, Service Based Architecture (SBA), HTTP2/JSON, REST API, and network slices.

Syllabus/outline

Day 1 Introduction

- 5G different architectures(SA/NSA) and impact on security
- Components of 5G deployments and danger areas
- 5G Domain Security Overview
- 5G RAN and virtualized RAN
- 5G UE, SIM & Handsets and SoCs
- 5G NR Radio access and security principles applied to 5G subscribers
- Anonymization of subscriber's fixed identity
- Authentication and Key Agreement (AKA)
- Encryption and integrity protection of control-plane and user-plane traffic
- Activation of the security and related signalling procedures
- Impact of new 5G protocols in term of security:
- X2 extensions for NSA deployment

F1AP

- E1AP
- PFCP
- 5G Core, Service Based Architecture (SBA), Roaming and Interconnect Security
- Infrastructure level deployment, security & risk of NFV (Network Functions Virtualization)
- Benefit and risk of 5G slicing in term of Security
- Understand the risks and attacks on isolation in a 5G multi-tenant environment (Slicing, NFV,

SDN)

Day 2
● 5G threat model and risk area
●5G Intrusion Detection
●Issues with Access Network Flash Network Traffic
●Radio interface key management
●User plane integrity
●DOS Attacks Against Network Infrastructure
● Overload of the signaling plane security issues
● CORE and MEC THreat
● Testbeds and network stacks securitypaperation
● 5G pen test procesand procedure

Day 3
Overview of 5G Testing Tools
● Penetration from Air interface and RAN
● Hands-on exercises for CORE and MEC networj testing
● Voice over LTE attack and tetsing
5G attack case study
5G Forensics Analysis

Auditing 5G Security Controls

Automating 5G Security
Top 3 take away

- This training will help to conduct successful 5G penetration testing and ethical hacking. Participants will learn about tools and techniques to analyse 5G vulnerabilities, reconnaissance

- Understanding and implementation of ENISA's threat landscape for 5G Networks and NIST 5G cybersecurity/RMF a secure evolution to 5G.

- Understand the 5G architecture and the challenges it poses to testing. Select and utilize the technology, tools, and applications available for 5G development and testing. Implement 5G testing practices to prevent failures at any of the different elements of a 5G network.

Who should take this course
This course is for students, , working professionals, or anyone interested to learn more about the exciting topic of 5G mobile network security challenges and solutions.This course assumes an engineering or IT background. An understanding of LTE security procedures would be an advantage as would a basic understanding of mobile network architecture.

Student requirement
Good knowledge of 4G architectures (LTE & EPC) Basic knowledge of telecom & network principles:
What is 2G, 3G; OSI network layers; Basic knowledge of telecom technologies; Good knowledge and usage of Wireshark;
Laptop with 4 Gb ram and 200 GB HDD with ubuntu OS , virtual machine and admin right
HW/KIT

Virtual machine contain all telecom testing tool

Training preference

- Interactive lecture and discussion.
- Lots of exercises and practice.
- Hands-on implementation in a live-lab environment.

% of training as practical and Theory

65% practical and 35% Theory and

What student should bring & provide with

This course assumes an engineering or IT background. An understanding of LTE security procedures would be an advantage as would a basic understanding of mobile network architecture.

How many hands-on labs you have

12

Keywords

#telecomsecurity #5Gsecurity #Mobilehacking #PenetrationTesting