VoIP Security and Vulnerability

Who Should Attend?

This course is aimed at managers, engineers, and operation teams who need deep knowledge about Voice-over IP technologies, attacks, vulnerabilities, and auditing methods. Participants will learn about the current threat environment (in terms of VoIP abuse and fraud) and the trends in securing VoIP services.

Course Scope

1. VoIP Introduction.
2. VoIP Benefits.
3. VoIP Technologies.
4. Root of VoIP Technology.
5. VoIP Security Architecture.
6. VoIP Specific Protocols Study.
   - SIP IETF.
   - H323.
   - IAX.
   - RTP.
   - SDP.
7. View of Telecom Specific Evolution of SIP.
   - SIP-I.
   - SIP-T.
8. VoIP Network Elements Overview, Security Roles, and Functions.
   - SBC.
   - SIPAS.
   - PCRF.
9. Security of Different VoIP Planes.
   - Control.
   - Media.
10. VoIP Communication Security.
11. Open-source VoIP Tools.
    - Asterisk.
    - OpenSER, OpenSIPS, and Kamailio.
12. Open Source Audit Tools.
    - SIP Vicious.
    - ISME.
13. Network Taps for VoIP Attack.
14. Impact of Routers, Switches, VLAN and Routing in VoIP Security.
15. VoIP Network Element Fingerprinting.
16. Typical Attacks on VoIP Infrastructure.
17. Threat Environments.
    - Central American Gangs.
    - Romanian Fraud Rings.

18. Role of Legacy in VoIP Security.
    - Interconnection with SS7 Signalling Network Element.
    - H248.
19. Vulnerabilities of some Voice-over-IP Protocols:
    - SIP-I.
    - SIP-T.
    - H323.
20. Generic VoIP Network Element Vulnerabilities.
21. Practical Attack of a VoIP network in a Lab-based Environment.
    - InformationGathering Information.
    - Scanning.
    - Cracking.
    - Abuse.
    - Privacy attacks.
    - Eavesdropping.
22. Scenario of VoIP Network Attack.
23. Using Backtrack for VoIP auditing.
    - The Next steps to becoming a VoIP network auditor.

Prerequisites

- Basic knowledge of Telecom and network principles:
    - What is 2G, 3G, 4G.
    - OSI network layers.
    - Basic knowledge of Telecom technologies.
- Good knowledge and usage of Wireshark.
- Basic skills and usage of Linux for reverse engineering (strings, knowledge of tools in a Backtrack for reverse engineering).
- Laptop with Linux installed either in a VM or native, Backtrack or Ubuntu with reverse engineering and hacking tools recommended.
- Legal IDA Pro license recommended.

Training Structure

Two-day training divided into logical sessions.

Methodology

Instructor-led training.