VoIP Checklist for Penetration Testers

pentestlab.blog/category/voip/page/2

September 18, 2016

Every VoIP assessment should follow a list of specific checks in order to give the client the necessary security assurance about his VoIP infrastructure. A checklist also disallows the pentester of forgetting to execute specific tests and therefore it prevents incomplete assessments.

After years of conducting this type of test I have compiled a list of attacks in a specific order of execution that I perform in every engagement.

- **VoIP-001** – VLAN hopping from data network to voice network
- **VoIP-002** – Extension Enumeration & Number Harvesting
- **VoIP-003** – Capturing SIP Authentication
- **VoIP-004** – Eavesdropping Calls
- **VoIP-005** – CallerID spoofing
- **VoIP-006** – RTP injection
- **VoIP-007** – Signaling Manipulation
- **VoIP-008** – Identification of insecure services
- **VoIP-009** – Testing for Default Credentials
- **VoIP-010** – Application level vulnerabilities
- **VoIP-011** – Voice Mail Attacks
- **VoIP-012** – Phone Firmware Analysis

You can find the list also on my GitHub account.

If you execute on your VoIP assessments more attacks please reply with a comment and I will update the list accordingly.