Audit-Friendly VoIP Deployment Hardening Checklist

Date: Thursday 12th June 2024

Prepared by: Group 8 Security Team [G8ST]

Purpose

This checklist is designed to assist audit teams and system administrators in verifying the secure configuration and deployment of Voice over IP (VoIP) systems. It ensures alignment with industry standards and internal VoIP security policies.

Instructions

- Use this checklist before system go-live, quarterly audits, and after significant configuration changes.
- Mark each item as **Compliant (✔)**, **Non-Compliant (✘)**, or **Not Applicable (N/A)**.
- Record additional notes or observations where relevant.

VoIP Deployment Hardening Checklist

#	Checklist Item	Compliance	Notes
1	SIP signaling is encrypted using TLS		
2	RTP media streams are encrypted using SRTP		
3	Strong, complex SIP passwords are enforced for all users		
4	Default VoIP account credentials have been changed		
5	Asterisk/VoIP server access is		

#	Checklist Item	Compliance	Notes
	restricted to authorized IP addresses		
6	Admin interfaces (AMI, web GUIs) are protected behind VPN or firewall		
7	All VoIP system software and firmware are up to date		
8	Unused SIP extensions, ports, and services are disabled		
9	IP phones are segmented via VLANs separate from data traffic		
10	QoS (Quality of Service) is configured to prioritize VoIP traffic		
11	Fail2Ban or equivalent is configured for brute-force SIP login attempts		
12	Snort/Suricata IDS rules for VoIP threats are enabled and tuned		
13	VoIP logs are centralized and stored for a minimum of 90 days		
14	Softphones are restricted to authorized apps (e.g., Zoiper, Linphone)		
15	VoIP system access via mobile devices requires VPN connection		
16	BYOD usage is governed by policy and devices are registered		
17	Rate limiting is enabled on SIP traffic to prevent DoS attacks		
18	Call Detail Records (CDRs) are retained for forensic review		
19	TLS certificates are valid and issued by trusted authorities		
20	SNMP and remote access services are disabled unless required		
21	Regular vulnerability scans are		

GROUP 8 SECURITY TEAM

#	Checklist Item	Compliance	Notes
	conducted on VoIP infrastructure		
22	Multi-factor authentication (MFA) is implemented for admin access		
23	Auto-provisioning of IP phones is secured and access-controlled		
24	Password policies enforce expiration, reuse prevention, and complexity		
25	VoIP system documentation and configurations are backed up securely		

Review & Sign-Off

This checklist must be reviewed and signed off by the designated VoIP Security Lead during each audit cycle.

Security Lead Name: G8ST
Title: ___Compliance Form_____
Signature: _____
Date: _____

Retention: Store a signed copy of each completed checklist for at least three years in the compliance audit archive.

G8ST
GROUP 8 SECURITY TEAM