

Audit de la sécurité de réseaux VoIP

Délivrable du projet VaDeSe¹

Author	J. Ehrensberger, X. Hahn, A. Doswald
Document creation	04 octobre 2006
Version	1.0
Latest modification	29 novembre 2006
Version control path	-

Résumé

Ce document est un livrable du projet VaDeSe. Il s'adresse aux auditeurs de sécurité de réseaux VoIP et décrit la méthodologie d'audit de réseaux VoIP développée dans le cadre du projet VaDeSe. Des checklists détaillées pour chaque étape de l'audit sont fournies. La méthodologie est complétée par des outils de tests, également développés dans le cadre du projet VaDeSe.

¹ Pour plus d'informations, consulter <http://www.vadese.org>.

1 Introduction

Un réseau VoIP est une cible potentielle de diverses menaces. Des attaques de Déni-de-Service peuvent empêcher les utilisateurs à communiquer et entraîner des pertes économiques considérables. L'écoute clandestine de communications, p.ex. par un employé depuis l'intérieure du réseau, est plus facilement réalisable que dans les services traditionnels (e-mail, Web), à cause de la durée d'une communication. Les attaques de vol de service permettent à un intrus d'acheminer du trafic VoIP sur l'infrastructure de l'entreprise. Des cas ont été reportés où le coût d'une attaque de vol de service a atteint plusieurs centaines de milliers de dollars.

Vu l'importance de la communication par téléphone pour la mission d'une entreprise, la gestion des risques de la VoIP doit être considéré comme une partie intégrante de la politique de sécurité de d'une entreprise. Pourtant, les compétences dans ce domaine sont encore rares.

Dans le cadre du projet VaDeSe, des recommandations pour la sécurisation de réseaux VoIP ainsi que l'audit de la VoIP ont été développées. Le document présent décrit une méthodologie d'audit pour les réseaux VoIP. Il décrit la procédure générale de l'audit et fournit des checklists détaillées, à utiliser lors de l'audit. Des outils de test (vulnérabilités, tests de pénétrations) sont également disponibles.

1.1 But, applicabilité et limitations

Le document présent permet à un auditeur de sécurité

- d'effectuer de tests techniques détaillées sous forme de checklists pour les différents aspects de la sécurité d'un réseau VoIP,
- d'analyser les résultats des tests et d'identifier des risques de sécurité,
- d'estimer le risque de différentes attaques,
- de développer des recommandations concrètes pour améliorer la sécurité du réseau VoIP (personnes, procédures et technique).

La méthodologie d'audit est applicable aux réseaux VoIP basés sur le protocole SIP. Tous les services de base (SIP, interconnexion VoIP-PSTN, localisation, proxy, routage, numérotation) ainsi que certains services supplémentaires (comptabilisation, redirection d'appels, NAT, ...) sont considérés.

La méthodologie d'audit traite la sécurité interne (menaces venant depuis l'intérieur du réseau) et la sécurité externe (menaces venant depuis l'extérieur, Internet).

Des technologies qui ne sont pas basées sur SIP, comme Skinny de Cisco ou H.323, ne sont pas considérées.

Les réseaux VoIP sont réalisés sur une infrastructure de réseaux LAN et IP classiques. Plusieurs méthodologies (p.ex. [2]) peuvent être utilisés pour l'audit de sécurité de ces réseaux classiques. Bien que la sécurité VoIP soit fortement influencée par la sécurité de l'infrastructure LAN/IP sous-jacente, nous nous limitons à l'analyse des mécanismes directement liés à la VoIP. Où nécessaire, des références aux méthodes d'audit de réseaux LAN/IP sont données.

1.2 Public cible

Ce document s'adresse aux personnes expérimentées dans la VoIP et les technologies de réseaux. Le public cible inclut :

- les auditeurs de sécurité de réseaux de télécommunications,
- les responsables de sécurité des systèmes d'information des entreprises,
- les administrateurs de réseaux des entreprises.

2 Références

Ce document a été élaboré après l'analyse des normes relevantes dans le domaine de la sécurité d'information. Il tient compte des normes et documents suivants :

- **NIST 800-30 : Risk Management Guide for Information Technology Systems.**
Décrit une méthodologie d'audit ayant comme approche la méthode d'évaluation de risques. Elle est spécifique pour la sécurité informatique et de réseaux.
- **OSSTMM Open Source Security Testing Methodology Manual.**
Recommandation pour les tests de sécurité, notamment des tests de pénétration.
- **CobiT Audit Guidelines, 3^{ème} édition.**
Décrit une méthodologie d'audit générique et haut niveau, pour l'évaluation de la sécurité d'information en générale (processus IT d'une entreprises).
- **CobiT framework, 4^{ème} édition.**
Décrit les processus IT d'une entreprise et les exigences à ces processus.
- **ISACA IS Standards, Guidelines and Procedures for Auditing and Control Professionals.** May 2006.
Décrit les normes et recommandations haut niveau pour l'audit, dans le cadre du Cobit Framework. Certaines procédures d'audit sont décrites de manière détaillée, p.ex. l'audit d'un firewall ou d'un VPN.

D'autres normes consultées sont ISO 17799, X.805 (Bell Labs), Standard of Good Practice (Information Security Society) et d'autres documents de NIST et SANS Institute.

Des informations complémentaires sur la sécurité de la VoIP sont données dans le document « Best Practice – Sécurité VoIP-SIP » [6], développé dans le cadre du projet VaDeSe. Il s'adresse aux responsables IT/administrateurs réseau désirant s'informer sur les risques de sécurité liés à la VoIP et qui ont besoin d'instructions pour sécuriser les différents éléments d'une infrastructure VoIP.

3 Terminologie

La terminologie suivante est basée sur les définitions de NIST et de CobiT.

Terme français	Terme anglais	Définition
Menace	Threat	Objectif d'une attaque ² . Exemples : déni de service, vol de service, spam, écoute clandestine, redirection d'appels.
Vulnérabilité	Vulnerability	Une faiblesse d'un composant qui peut conduire à une violation de la politique de sécurité du système. Elle peut être exploitée intentionnellement par un attaquant ou déclenchée accidentellement par un utilisateur normal. Exemples : mot de passe faible, buffer overflow d'un service, susceptibilité au déni de service
Contrôle de sécurité	Security control	Méthode de sécurisation au niveau de gestion, d'organisation et mesures technique afin de protéger la confidentialité, intégrité et la disponibilité du système et des informations. Exemples : firewall, méthode d'authentification, désactivation d'un service.
Attaque	Attack, Exploit	Une ou plusieurs actions coordonnées qui exploitent une vulnérabilité afin de réaliser une menace.
Risque	Risk	Paramètre qui quantifie le danger pour le bon fonctionnement d'une entreprise. Tient compte de la probabilité d'une attaque et de son impact.
Composant du système	System component	Élément du système VoIP, y compris : <ul style="list-style-type: none"> • le matériel (serveurs, dispositifs de réseau) • les logiciels • les services • les contrôles (méthodes de sécurisation, authentification, ...) • les données gérées.
Critères d'information	Information criteria	Dimensions de sécurité, définies par CobiT : <ul style="list-style-type: none"> • effectivité • efficacité • confidentialité • intégrité • disponibilité • compliance • « Reliability » (si les informations sont appropriées pour le but visé)

² Cette définition est basée sur la taxonomie de menaces de VOIPSA. Elle ne correspond pas à la définition de NIST.

Partie Audit technique

1 Introduction

L'audit technique permet d'effectuer une analyse de risques, qui inclut l'identification des menaces, l'estimation de la probabilité et l'impact des menaces et la recommandation de mesures pour la réduction des risques.

Un audit exhaustif doit analyser le risque sous trois points de vue :

- **Analyse des menaces** : cette analyse vise à prioriser les menaces en fonction des exigences de sécurité de l'entreprise. Elle permet de se concentrer sur les menaces qui ont le potentiel de compromettre la confidentialité, l'intégrité et la disponibilité des services.
- **L'analyse des contrôles** : cette analyse évalue les mécanismes et sécurité déjà en place et vérifie le bon fonctionnement. Elle permet de d'estimer la probabilité d'une attaque et permet ainsi de réduire le nombre de menaces et vulnérabilités à considérer dans la suite de l'audit technique.
- **L'analyse des vulnérabilités** : dans cette analyse, les composants du réseau sont évalués afin de détecter les vulnérabilités qui pourraient permettre une attaque.

La procédure d'audit est construite de manière à minimiser le temps et l'effort nécessaire pour l'audit technique. Comme une grande partie de l'effort est typiquement consacrée à l'analyse des vulnérabilités, cette étape est effectuée après les autres analyse et peut tenir compte de leurs résultats.

Les analyses techniques sont suivies par une analyse des risques, qui synthétise les résultats, estime le risque et établit des recommandations.

2 Procédure

La procédure de l'audit technique présentée dans ce document est similaire à celle développée par NIST [1]. Une procédure similaire est brièvement décrite dans « CobiT Audit Guidelines » [3], comme alternative à la procédure CobiT [4].

Elle vise à caractériser les risques auxquels un réseau VoIP est exposé à travers l'analyse des menaces, des contrôles en place et des vulnérabilités. Le résultat final de l'audit technique est un ensemble de recommandations techniques de sécurisation du réseau.

Séparation entre la collecte d'informations et l'analyse

La méthodologie présentée permet une séparation entre de la collecte d'information et l'analyse des résultats. Dans une première étape, l'auditeur effectue des tests et enregistre les résultats. Le type des données à enregistrer est clairement indiqué.

Dans une deuxième étape, l'auditeur analyse les résultats des tests et développe des recommandations. Dans la mesure du possible, des indications sont données qui permettent d'interpréter les résultats. L'interprétation étant dépendant de beaucoup de facteurs, à la fois techniques et organisationnels, les indications ne peuvent tenir compte que des situations les plus courantes. L'expérience de l'auditeur est requise afin de tenir compte des circonstances concrètes.

Procédure générale

La procédure générale de l'audit technique est illustrée à la Figure 1.

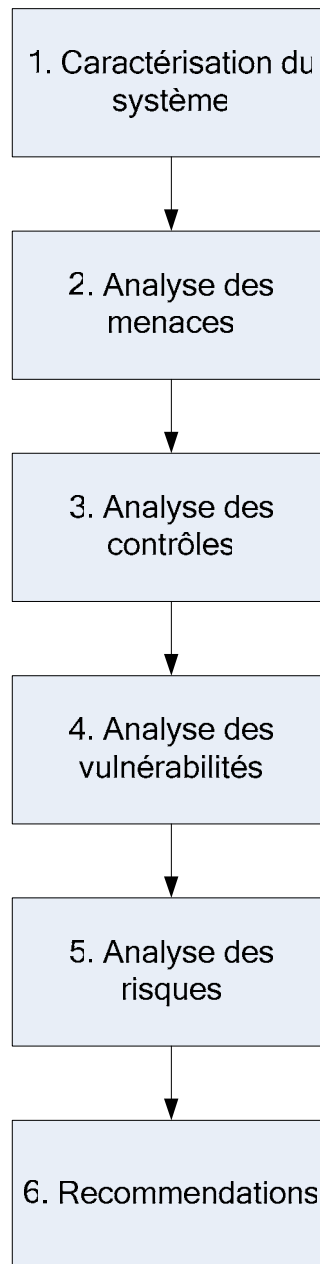


Figure 1: Procédure de l'audit technique

2.2 Caractérisation du système

La première étape de l'audit répertorie les composants du réseau, les services réalisés et les données gérées par les différents services. Elle documente aussi la politique de sécurité en place.

Résultats

Les résultats de cette étape sont :

1. des diagrammes du réseau,
2. une liste des serveurs et dispositifs du réseau,
3. une liste des contrôles techniques (méthodes de sécurisation) en place,
4. la classification des exigences en sécurité des services et informations gérées,
5. une description de la politique de sécurité du réseau.

Ces informations pourront être utilisées pour définir l'envergure de l'audit, donc des équipements, services et données à considérer.

Procédure

Cette étape utilise les sources d'informations suivantes :

- Diagrammes existants du réseau
- Documentation existante
- Interviews et inspection sur place
- Questionnaires
- Outils de scanning

Références

- NIST 800-30 et NIST 800-100

2.3 Analyse des menaces

Cette étape permet de déterminer les menaces à considérer dans les phases suivantes et d'identifier les sources de menaces.

Une menace est une violation potentielle de la politique de service à cause d'une attaque ou d'une action involontaire ou négligente qui compromet la sécurité. Des sources de menaces sont donc des personnes malintentionnées ou les utilisateurs normaux. Les sources de menaces peuvent être internes ou externes au réseau VoIP.

Résultats

Le résultat de cette étape est :

- Une liste des menaces à considérer. La liste indique les sources possibles d'une menace et l'importance d'une protection contre chaque menace.

Procédure

Cette étape part de la liste complète des menaces liées à la VoIP. En discussion avec les responsables de la société, les sources de menaces les plus probables sont identifiées. Ensuite, un niveau de protection requis est assigné à chaque menace ou à chaque source de menace.

Références :

1. NIST 800-30 et NIST 800-100
2. VOIPSA Threat Taxonomy
3. Vadese Best Practice « Sécurité VoIP-SIP »

2.4 Analyse des contrôles

Le but de cette étape est d'analyser les mécanismes de sécurité en place dans le système. Les contrôles en place ont été documenté dans la première phase de l'audit, la caractérisation du système.

Résultats

Le résultat de cette étape est :

- une liste des contrôles et leurs effets (menaces prévenues)
- un protocole des résultats des tests qui indique si le contrôle fonctionne correctement.

Dans la méthodologie NIST, cette étape est effectuée après l'identification des vulnérabilités. Or, le test des vulnérabilités est une procédure qui demande beaucoup de travail et qui peut interrompre le service normal du réseau. Elle doit donc être limitée à un minimum. Le fait d'analyser les contrôles d'abord permet de réduire le nombre de vulnérabilités à tester.

Procédure :

Cette étape se base sur la liste des contrôles en place, établie dans la première étape de l'audit.

- Pour chaque contrôle, son effet est défini, donc les menaces prévenues par ce contrôle.
- L'efficacité du contrôle doit être évaluée, par l'évaluation de la configuration et le test du contrôle.

Références :

1. NIST 800-30 et NIST 800-100 et NIST 800-53 et 53A
2. Vadese Best Practice « Sécurité VoIP »

2.5 Analyse des vulnérabilités

Le but de cette étape est d'identifier toutes les vulnérabilités à considérer qui :

- pourraient être présentes dans le système
- qui ne sont pas couvertes par les contrôles en place.

Procédure :

- Pour chaque composant (dispositif, logiciel, protocole, fonctionnalité) du système :
 - Partir d'une liste des vulnérabilités connues (utiliser NIST NVD, CVE)
 - Sélectionner les vulnérabilités à évaluer
 - Sur la base des composants du système.
 - Sur la base des contrôles en place.
 - Tester la présence des vulnérabilités
 - Interview, questionnaires
 - Scanning (nmap, Nessus, ...)
 - Tests de pénétration

Résultats

Les résultats de cette étape sont :

- Une liste qui indique, par composant du système, les vulnérabilités présentes et non couvertes par les contrôles.

Références :

1. NIST 800-30 et NIST 800-100
2. Bases de données de vulnérabilités (NIST NVD, CVE, ...)
3. Liste de catégories de vulnérabilités par composant.

2.6 Analyse des risques

Cette étape vise à prioriser les dangers constatés en déterminante la probabilité d'une attaque et son impact.

Procédure

Dans une première phase, elle met en relation :

- l'attractivité d'une menace pour un attaquant (étape 2)
- la possibilité d'une attaque, réalisée à travers une vulnérabilité.

Ceci détermine la probabilité d'une attaque (valeurs 0 – 1).

Dans une deuxième phase, l'impact d'une menace réalisée est évalué (valeurs 0 – 100).

Une méthode simple de prioriser les risques et la multiplication de la probabilité avec l'impact. Voir NIST 800-30 et 800-100 pour les détails.

Résultat

Le résultat de cette étape est :

- Une liste des menaces, priorisées par leur risque.

Références :

1. NIST 800-30 et NIST 800-100

2.7 Recommandations

Le but de cette étape est de proposer des contrôles supplémentaires, des procédures (pour augmenter l'efficacité des contrôles) qui permettent de réduire les risques pour l'entreprise.

Résultat

Le résultat de cette étape est :

- Une recommandation de modification du système pour éliminer des vulnérabilités.
- Une recommandation de procédures qui permettent d'augmenter l'efficacité des contrôles déjà en places
- Une recommandation de contrôles supplémentaires pour couvrir certaines vulnérabilités

Références :

1. NIST 800-30 et NIST 800-100

3 Références

- [1] Gary Stoneburner, Alice Goguen, and Alexis Feringa ; *"Risk Management Guide for Information Technology Systems"*; Recommendations of the National Institute of Standards and Technology; Special Publication 800-30; July 2002; <http://csrc.nist.gov/publications/nistpubs>.
- [2] Pete Herzog; *"Open-Source Security Testing Methodology Manual (OSSTMM)"*; Version 2.1.1; Institute for Security and Open Methodologies (ISECOM); August 2003; <http://www.isecom.org/osstmm>.
- [3] IT Governance Institute™; *"CobiT® Audit Guidelines"*; 3rd edition; July 2000; <http://www.isaca.org>.
- [4] IT Governance Institute™; *"CobiT® 4.0"*; 2005; <http://www.isaca.org>.
- [5] ISACA; *"IS Standards, Guidelines and Procedures for Auditing and Control Professionals"*; 2006; <http://www.isaca.org/standards>.
- [6] "Best Practice – Sécurité VoIP-SIP". Projet VaDeSe. Octobre 2006. <http://www.vadese.org>.