

Audit de réseaux VoIP

3 – Contrôles

Project phase	WP6
Author	Juergen Ehrensberger, Alistair Doswald, Xavier Hahn, Sébastien Contreras
Document creation	24 octobre 2006
Version	1.0
Latest modification	24 octobre 2006
Version control path	

Résumé

Ce document fait partie de la méthodologie d'audit de réseaux VoIP du projet Vadese. Il fournit les check-lists pour la troisième étape de l'audit, l'analyse des contrôles. Cette analyse permet de déterminer les contrôles qui doivent être mis en place dans le réseau et comment tester leur présence.

© 2006 HES-SO

Relation avec les documents de l'audit VoIP

Ce document contient les check-lists pour la troisième étape de l'audit VoIP. La méthodologie d'audit générale est décrite dans le document « Audit sécurité VoIP » [1].

Structure du document

La première partie du document fournit les informations de base qui permettent de correctement effectuer l'audit. Ces informations sont relativement exhaustives et peuvent être consultées pour avoir de l'aide lors de l'audit.

La deuxième partie fournit les check-lists qui permettent d'analyser les menaces.

1 Liste des contrôles

Un contrôle de sécurité est une méthode de sécurisation au niveau de la gestion, de l'organisation et des mesures techniques afin de protéger la confidentialité, l'intégrité et la disponibilité du système et des informations.

Des exemples de contrôle sont la présence d'un firewall, d'une méthode d'authentification ou la désactivation d'un service.

Catégorie	Sous-catégorie	Explication
Sécurité de base		
		Les contrôles qui sont à la base de la sécurité de la VoIP.
Best Practices « sécurité réseau »		
		La sécurité VoIP est très liée à la sécurité du réseau en lui-même, la plupart des infrastructures étant des réseaux IP convergés. Il est important de s'assurer de la sécurité de son réseau. Un Best Practice tel que « <i>Network Infrastructure – Security Technical Implementation Guide</i> » [2] peut être utilisé comme référence.
Best Practices « Sécurité du poste client »		
		Bien que l'utilisation de softphones soit déconseillée pour des raisons de sécurité, toutes les machines installées sur les réseaux DATA et utilisant des softphones doivent être sécurisées afin d'empêcher toute attaque provenant d'elles. Le best practice « <i>Guide to securing Windows XP</i> » [3] peut être utilisé comme référence.
Sécurité Physique		
		La sécurité physique est la clé de voute de la sécurité du réseau. Un accès physique aux équipements réseau tels que switchs ou serveurs ne doivent pouvoir être fait que par les personnes autorisées (administrateurs ou techniciens). Il est aussi important que les employés ne puissent pas brancher ou débrancher des équipements sur le réseau de l'entreprise.
Mise à jour du software (IPBX, <i>hardphone</i> et <i>softphone</i>)		
		Les mises à jour pour les softwares des équipements sont fournies par le constructeur ou développeur de l'équipement et permettent de combler les failles de sécurité ou les bugs. La mise à jour, ainsi qu'une stratégie de déploiement, est impérative car les constructeurs publient en général les failles de sécurité qui ont été comblées par la dernière mise à jour.
Verrouillage de la configuration (<i>hardphone/softphone</i>)		

		Une fois la configuration faite, il est important de verrouiller la configuration afin qu'un utilisateur de l'équipement ne puisse pas modifier, ni même regarder la configuration de l'équipement. La divulgation des informations de configuration ainsi que la modification de la configuration peuvent faciliter grandement la mise en place d'attaques.
Sécurité administrative		
	Cette section regroupe tous les contrôles liés à la partie administrative de la sécurité.	
	Empêcher le masquage d'identité	
		Le masquage d'identité est un risque de sécurité car il peut faciliter le « Social Engineering », c'est-à-dire aider une personne mal intentionnée à se faire passer pour une autre personne. De plus, il peut permettre de faciliter le SPAM.
	Protection contre le SPAM	
		Il existe un grand nombre de type de SPAM sur les réseaux VoIP (Message SPAM, Voice SPAM, etc.) c'est pourquoi il est important de mettre en place des mesures afin de le limiter. Ces protections sont identiques à celles que l'on trouve déjà pour les messageries e-mails.
	Maintient d'une liste des équipements autorisés	
		Le maintien d'une liste des équipements autorisés sur le réseau VoIP permet de s'assurer qu'aucun équipement non autorisé se trouve sur le réseau en tout moment. De plus, il permet de créer des listes blanches interdisant tout accès non autorisé au réseau.
	Non utilisation des softphones	
		Les softphones sont un risque de sécurité important pour le réseau VoIP car ils sont par définition installés sur des ordinateurs qui ont accès au réseau DATA. C'est pourquoi il est conseillé de ne pas les utiliser.
Séparation des équipements DATA et VoIP		
	La manière la plus efficace de créer une sécurité accrue du réseau est de séparer le réseau en deux zones de sécurité, une zone étant réservée à la partie VoIP, l'autre à la partie DATA. Il est aussi recommandé de séparer la zone VoIP en différentes zones, par exemple une zone serveurs, une zone hardphones et une zone softphones.	
	Séparation au niveau IP (<i>layer 3</i>)	
		Cette séparation simple consiste à créer une plage

		d'adresse IP dédiée au réseau DATA et une plage d'adresse différente pour le réseau VoIP.
Séparation grâce aux VLAN (layer 2)		
		Après avoir créé les deux plages d'adresses pour les deux réseaux, l'étape suivante consiste à créer une séparation au niveau 2 en créant des VLAN. A nouveau, il peut être judicieux de créer plus d'un VLAN pour le réseau VoIP, afin de séparer, par exemple, les serveurs des softphones et des hardphones.
Filtrage Inter-VLAN		
		Les communications entre les VLAN doivent être filtrées de manière à empêcher toute communication inutile entre les différents VLAN. Le filtrage doit être du type liste blanche et peut être mis en place en utilisant les ACL des équipements interconnectant les VLAN ou en plaçant un firewall entre les VLAN.
Utilisation d'une carte réseau supportant 802.1Q		
		Le principal problème lié à l'utilisation de softphone vient du fait que l'ordinateur, banché sur le réseau DATA devient aussi un terminal VoIP. L'utilisation d'une carte réseau supportant 802.1Q permet d'éviter ce problème en séparant le trafic VoIP du trafic de données en mettant chaque type de trafic dans leur VLAN respectif.
Désactivation ou protection (802.1q) des ports réseaux supplémentaires		
		Certains hardphones disposent d'un port réseau supplémentaire permettant de connecter un ordinateur. Ils sont un risque de sécurité important car peuvent permettre de brancher un ordinateur sur le réseau VoIP. C'est pourquoi ils doivent être désactivés ou il faut s'assurer qu'ils ne permettent pas de se brancher sur le VLAN VoIP mais uniquement sur le VLAN DATA.
Sécuriser l'accès aux ports des switches (ACL,...)		
		Un accès aux ports non utilisé des switches peut permettre de déjouer la séparation des réseaux VoIP et DATA. Il est donc important de sécuriser l'accès aux ports de ces switches, par exemple en les désactivant ou en les plaçant dans des VLAN non utilisés. Il peut être aussi intéressant de créer une ACL au niveau du switch en autorisant uniquement des adresses MAC bien connue à se connecter au réseau.
Placer les services convergés dans une DMZ		
		Les services convergés, c'est-à-dire les services qui ont

		besoin d'être accessible à la fois pour le réseau DATA et le réseau VLAN doivent être mis dans une DMZ afin de ne pas compromettre la séparation des deux réseaux.
Authentification		
		L'authentification permet de s'assurer que seuls les utilisateurs légitimes peuvent se connecter au réseau et qu'il n'est pas possible de facilement se faire passer pour une personne légitime.
		Authentification HTTP Digest des messages SIP
		Le HTTP Digest Authentication permet au serveur d'authentifier les messages SIP INVITE ou REGISTER issus d'un IP Phone. Cela permet d'éviter les attaques se basant sur l'usurpation d'identité. L'authentification doit être mise en place à la fois sur les IP phones et sur le registrar.
		Authentification mutuelle
		L'authentification mutuelle permet au serveur d'authentifier le client et au client d'authentifier le serveur. Les attaques basées sur l'usurpation d'identité ne sont alors plus possibles. Il existe diverses méthodes d'authentification mutuelle, par exemple SIPS. Cette méthode doit être mise en place à la fois sur les serveurs et sur les IP Phones.
Chiffrement		
		Le chiffrement permet d'empêcher à un attaquant qui aurait récupéré un flux média d'une manière ou d'une autre de comprendre ce flux média. Il est possible de chiffrer le flux de signalisation (SIPS) et/ou les flux médias. Il est important de noter que le chiffrement est gourmand en performances et n'est pas facile à mettre en place. Il est donc nécessaire de mesurer l'utilité d'une telle mesure dans le réseau.
		Chiffrement du flux de signalisation : SIPS,...
		Le chiffrement du flux de signalisation permet de garantir la confidentialité et l'intégrité des données de signalisation. Les écoutes clandestines sur ce type de flux sont donc prévenues. Un exemple de mise en place d'un tel chiffrement est l'utilisation de SIPS.
		Chiffrement du flux média : SRTP,...
		Le chiffrement du flux média permet de garantir la confidentialité et l'intégrité des données des conversations téléphoniques. Les écoutes clandestines sur ce type de flux sont donc prévenues. Un exemple de mise en place d'un tel chiffrement est l'utilisation de SRTP.
		Chiffrement avec IPSec (ou autre technologie VPN)

		Le chiffrement des flux avec IPSec (ou une autre technologie VPN) permet de garantir la confidentialité et l'intégrité de tous les flux échangés. L'authentification mutuelle des protagonistes est également assurée.
Sécurité périmétrique		
	La sécurité périmétrique concerne les équipements placés en bordure du réseau VoIP et permet de se protéger contre les attaques externes.	
	Mise en place d'un SBC	
		Un SBC est un dispositif placé en bordure du réseau et étant capable de gérer les flux VoIP. Il offre des fonctionnalités différentes suivant les marques, mais les plus courantes sont les suivantes : contrôle d'appel entrant, conversion de codec media, réécriture du trafic de signalisation, ouverture des ports nécessaires sur le firewall, NAT traversal.
	SBC : Définitions de seuils / <i>Call Admission Control</i>	
		Les attaques DoS entraînent par définition un nombre anormalement élevé de transactions réseau. Grâce au SBC, l'administrateur réseau a la possibilité de définir des seuils, basés sur divers critères, permettant de limiter le trafic entrant et/ou sortant d'un réseau. De cette manière, le SBC évite de surcharger les <i>switchs</i> et de mettre hors-service certains équipements et/ou le réseau.
STUN/TURN		
	STUN est un protocole permettant aux applications l'utilisant de découvrir la présence et le type du NAT et des firewalls entre elles et Internet. Il permet aussi de déterminer quelle adresse IP publique a été allouée par le NAT. TURN (Traversal Using Relay NAT) est un protocole permettant à un élément derrière un NAT ou un firewall de recevoir des données entrantes.	
	Utilisation de serveurs dédiés pour STUN	
		Il est recommandé que les serveurs STUN tournent sur des serveurs dédiés, avec tous les ports TCP et UDP désactivés excepté ceux pour STUN. Ceci permettra d'éviter des virus ou chevaux de Troie d'infecter les serveurs STUN, et ainsi empêcher qu'ils soient compromis.
	Vérification de l'identité du serveur STUN	
		STUN possède un mécanisme de vérification de l'intégrité des messages, mais cette fonctionnalité est indiquée comme étant non obligatoire dans la RFC. Il est donc important de vérifier que l'implémentation de STUN

		utilisée fasse bien cette vérification.
	Client STUN : Continuation de l'écoute des réponses après la première	
		La réception d'une réponse de la part du serveur STUN (que ce soit une erreur ou une Binding Response) doit normalement terminer les transmissions de cette requête. Toutefois, les clients doivent continuer à écouter les réponses durant 10 secondes après la première réponse. Si durant ces dix secondes une réponse contenant d'autres informations est reçue, il est probable qu'une attaque est en cours.
	Relais STUN : Limitation de la bande passante allouée par personne	
		Puisque les serveurs STUN implémentant les fonctions de relais allouent des ressources, ils sont susceptibles d'être victimes d'attaques du type déni de service. Toutes les requêtes d'allocation sont authentifiées ce qui permet d'éviter à un attaquant inconnu de lancer une attaque. Toutefois, un attaquant authentifié pourrait générer de multiples requêtes d'allocation. Pour empêcher un simple utilisateur malicieux d'allouer toutes les ressources du serveur, il est recommandé qu'un serveur implémente une limite modeste de bande passante qui peut être allouée par personne.

2 Références

- [1] Projet VaDeSe : « Audit de la sécurité de réseaux VoIP » ; Version 1.0 ; Octobre 2006 ; HES-SO.
- [2] DISA ; "*Network Infrastructure – Security Technical Implementation Guide*" ; Version 6 release 4; 16 december 2005;
<http://iase.disa.mil/stigs/stig/network-stig-v6r4.pdf>
- [3] Murugiah Souppaya, Karen Kent and Paul M. Johnson; "Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist"; Recommendations of the National Institute of Standards and Technology; Special Publication 800-68; October 2005;
<http://csrc.nist.gov/itsec/SP800-68.zip>

3 - Contrôles

Description de l'audit :

Auditeurs :

Date début de l'audit :

Date fin de l'audit :

Sécurité de base

Vulnérabilité		Procédure suggérée	Résultats			
1	Sécurité Physique	a	Vérifier la présence de mesures de sécurité sur les portes d'accès aux serveurs et aux équipements réseau de la VoIP	OK	Pas OK	N/A
		b	Vérifier que seul les administrateurs et techniciens ont accès à ces équipements (par exemple, récupérer la liste des personnes autorisées).	OK	Pas OK	N/A
2	Mise à jour du software (IPBX, hardphone et softphone)	a	Récupérer la liste des versions de tous les logiciels et équipements qui peuvent être mis à jours.	Liste de versions logicielles et matérielles		
		b	Vérifier d'après cette liste que tous les logiciels et équipements soient à jour en regardant la dernière version sur le site Internet du fabriquant.			
3	Verrouillage de la configuration (hardphone/softphone)	a	Vérifier que tous les hardphones et équipements en contact avec des utilisateurs aient leur configuration bloquée	OK	Pas OK	N/A
		b	Vérifier qu'il ne soit pas possible pour un utilisateur de consulter la configuration et les informations liées au réseau (par exemple adresse IP) sur les hardphones et équipements auxquels il a accès.	OK	Pas OK	N/A

Sécurité administrative

Vulnérabilité		Procédure suggérée	Résultats			
1	Empêcher le masquage d'identité	a	Vérifier si une politique a été mise en place par l'entreprise pour ce détail.	OK	Pas OK	N/A
		b	Vérifier que l'option de masquage d'identité ne soit pas active sur les équipements de l'entreprise	OK	Pas OK	N/A
		c	Vérifier que cette configuration ne puisse être modifiée et qu'il n'existe pas de moyens détournés sur l'appareil	OK	Pas OK	N/A
2	Protection contre le SPAM	a	Vérifier qu'une politique de lutte contre le SPAM a été mise en place dans l'entreprise.	OK	Pas OK	N/A
		b	Vérifier que des équipements de lutte contre le SPAM ont été mise en place, qu'ils soient à jour et que leur configuration soit correcte.	OK	Pas OK	N/A
3	Maintient d'une liste des équipements autorisés	a	Vérifier l'existence et récupérer la liste des équipements autorisés.	Liste des équipements autorisés		
		b	Vérifier que cette liste soit tenue à jour en permanence.	OK	Pas OK	N/A
		c	Vérifier que la liste corresponde bien à la réalité des équipements connectés au réseau.	OK	Pas OK	N/A
		d	Vérifier qu'aucun équipement non autorisé ne soit enregistré sur le réseau, et qu'aucun ne puisse s'enregistrer.	OK	Pas OK	N/A
4	Non utilisation des softphones	e	Vérifier que des softphones ne sont pas utilisés dans l'entreprise ou qu'ils le sont uniquement après validation par l'administrateur.	OK	Pas OK	N/A

Séparation des équipements DATA et VoIP

Vulnérabilité		Procédure suggérée	Résultats	
1	Séparation au niveau IP (layer 3)	<p>a Récupérer la liste des adresses IP de tous les équipements liés à la VoIP ainsi que celles du réseau DATA.</p> <p>b Vérifier que toutes les adresses des équipements VoIP soient bien dans une plage d'adresse différentes des équipements DATA.</p>	<p>OK</p> <p>Pas OK</p>	<p>Liste des adresses IP</p> <p>N/A</p>
2	Séparation grâce aux VLAN (layer 2)	<p>a Vérifier qu'il existe bien des VLAN séparés pour la VoIP et les données. (Mieux s'il existe différents VLAN pour la partie VoIP)</p> <p>b Vérifier que tous les équipements sont bien configurés et branchés pour être sur leurs VLAN respectifs.</p>	<p>OK</p> <p>Pas OK</p>	<p>N/A</p> <p>N/A</p>
3	Filtrage Inter-VLAN	<p>a Vérifier que les équipements interconnectant les VLAN son bien configurés pour effectuer un filtrage.</p> <p>b Récupérer les tables de filtrage de tous ces équipements.</p>	<p>OK</p> <p>Pas OK</p>	<p>N/A</p> <p>N/A</p>
			Table de filtrage	
		<p>c Analyser les tables de filtrage et vérifier que les filtres en place soient utiles et que la liste soit complète</p> <p>d Vérifier s'il est possible d'envoyer des données depuis le VLAN DATA vers le VLAN VoIP et vice-versa depuis un équipement non autorisé à le faire.</p>	<p>OK</p> <p>OK</p>	<p>N/A</p> <p>N/A</p>
4	Utilisation d'une carte réseau supportant 802.1Q	<p>a Si l'entreprise utilise des softphones, vérifier que les cartes réseaux utilisées soient compatibles avec 802.1Q et qu'elles soient configurées correctement (les données VoIP et DATA vont sur leurs VLAN respectifs).</p>	<p>OK</p> <p>Pas OK</p>	<p>N/A</p> <p>N/A</p>
5	Désactivation ou protection (802.1q) des ports réseaux supplémentaires	<p>a Vérifier la présence de ports supplémentaires sur les hardphones de l'entreprise. S'ils sont présents, vérifier qu'ils soient soit désactivés, soit utilisent 802.1Q pour mettre les données informatiques sur le VLAN DATA.</p>	<p>OK</p> <p>Pas OK</p>	<p>N/A</p> <p>N/A</p>

				OK	Pas OK	N/A
6	Sécuriser l'accès aux ports des switches (ACL,...)	b	Essayer de brancher un ordinateur sur le port d'un hardphone et vérifier qu'il ne soit pas possible de pinger le hardphone.	OK	Pas OK	N/A
		a	Vérifier que les ports non utilisés des switches soient bien désactivés dans leur configuration ou qu'ils soient configurés pour utiliser un VLAN non affecté.	OK	Pas OK	N/A
		b	Vérifier que les switches utilisent une ACL afin de n'autoriser que les adresses MAC connues à se connecter au réseau.	OK	Pas OK	N/A
		c	Vérifier que la fonctionnalité « Port Security » soit bien configurée sur tous les ports utilisés des VLAN VoIP.	OK	Pas OK	N/A
		d	Vérifier s'il est possible d'insérer un ordinateur sur le(s) VLAN VoIP.	OK	Pas OK	N/A
		e	S'il est possible d'insérer un ordinateur, vérifier s'il est possible d'insérer des paquets sur le VLAN (par exemple en effectuant un ping sur un équipement du VLAN).	OK	Pas OK	N/A
	f	S'il est possible d'insérer un ordinateur, lancer un sniffer et vérifier s'il est possible de récupérer des données du VLAN.	OK	Pas OK	N/A	
7	Placer les services convergés dans une DMZ	a	Vérifier que les services qui doivent être accessibles à la fois par le(s) VLAN VoIP et le(s) VLAN DATA soient placés dans une DMZ.	OK	Pas OK	N/A

Authentification								
Vulnérabilité		Procédure suggérée			Résultats			
1	Authentification HTTP Digest des messages SIP	a	Vérifier que les serveurs et les IP Phones sont configurés pour utiliser le HTTP Digest Authentification.			OK	Pas OK	N/A
		b	Essayer de créer une fausse authentification sur les équipements et voir si cela fonctionne.			OK	Pas OK	N/A
2	Authentification mutuelle	a	Vérifier qu'à la fois les serveurs et les clients vérifient l'authentification de celui avec qui ils communiquent.			OK	Pas OK	N/A
		b	Tenter d'usurper l'authentification d'un client et de communiquer avec cette fausse identité avec un serveur. Faire de même en prenant l'identité d'un serveur pour communiquer avec un client.			OK	Pas OK	N/A
3	Verrouillage de la configuration (hardphone/softphone)	a	Vérifier que tous les hardphones et équipements en contact avec des utilisateurs aient leur configuration bloquée			OK	Pas OK	N/A
		b	Vérifier qu'il ne soit pas possible pour un utilisateur de consulter la configuration des hardphones et équipements en son contact.			OK	Pas OK	N/A

Chiffrement

Vulnérabilité		Procédure suggérée	Résultats			
1	Chiffrement du flux de signalisation : SIPS,...	a	Vérifier que les serveurs et les IP Phones sont configurés pour utiliser une méthode de chiffrement des flux de signalisation. (par exemple SIPS)	OK	Pas OK	N/A
		b	Vérifier que ce chiffrement utilise un ciphre récent et bien connu.	OK	Pas OK	N/A
		c	Récupérer un flux de signalisation issu d'une communication et voir s'il est possible de le décrypter facilement.	OK	Pas OK	N/A
2	Chiffrement du flux média : SRTP,...	a	Vérifier que les serveurs et les IP Phones sont configurés pour utiliser une méthode de chiffrement des flux média. (par exemple SRTP)	OK	Pas OK	N/A
		b	Vérifier que ce chiffrement utilise un ciphre récent et bien connu.	OK	Pas OK	N/A
		c	Récupérer un flux média issu d'une communication et voir s'il est possible de le décrypter facilement.	OK	Pas OK	N/A
3	Chiffrement avec IPsec (ou autre technologie VPN)	a	Si besoin est, vérifier qu'IPsec est configuré sur le réseau.	OK	Pas OK	N/A
		b	Si IPsec est configuré, vérifier que les Media Gateways, les contrôleurs de Media Gateway et de tout équipement compatible soit bien configuré pour utiliser IPsec.	OK	Pas OK	N/A
		c	Récupérer un flux média et un flux de signalisation issu d'une communication et voir s'il est possible de les décrypter facilement.	OK	Pas OK	N/A

Sécurité périmétrique

Vulnérabilité		Procédure suggérée		Résultats	
1	Mise en place d'un SBC	a	Vérifier la présence d'un SBC.	OK	N/A
		b	Récupérer la configuration du(des) SBC mis en place	Configuration des SBC	
		c	Se référer au document 4-Vulnérabilités, la partie sur les check-lists des équipements afin de vérifier la check-list concernant les SBC.	OK	Pas OK N/A

STUN/TURN

Vulnérabilité		Procédure suggérée	Résultats		
			OK	Pas OK	N/A
1	Utilisation de serveurs dédiés pour STUN	a	Vérifier que les serveurs STUN fonctionnent sur des serveurs dédiés.	OK	N/A
		b	Vérifier que les ports TCP et UDP de ces serveurs sont tous désactivés, exceptés les ports STUN.	OK	N/A
2	Vérification de l'identité du serveur STUN	a	Vérifier que l'implémentation de STUN utilisée effectue bien la vérification de l'intégrité des messages.	OK	N/A
3	Client STUN : Continuation de l'écoute des réponses après la première	a	Vérifier que l'implémentation de STUN sur les clients continue bien à écouter les réponses durant 10 secondes après la première réponse afin de vérifier qu'une attaque ne soit pas en cours.	OK	N/A
		b	Vérifier qu'une alerte est bien émise dans le cas où la situation se produit.	OK	N/A
4	Relais STUN : Limitation de la bande passante allouée par personne	a	Vérifier que la bande passante allouée par le relai STUN est bien limitée dans la configuration.	OK	N/A
		b	Expérimenter pour voir s'il est possible d'allouer plus de ressources que la limite configurée.	OK	N/A