

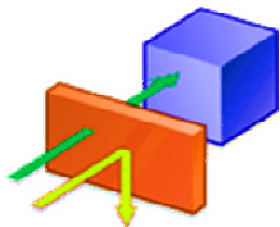
Audit intrusif

Audit des S.I

www.alliacom.com

ALLIACOM

Un Audit intrusif : Pourquoi ?



1. Vérifier la conformité par rapport à la politique de sécurité et par rapport aux différents standards internationaux,
2. Vérifier le bon fonctionnement des procédures de sécurité,
3. Vérifier le niveau de résistance d'un environnement à un certain type d'attaques ou à des agressions d'un niveau défini,
4. Sensibiliser les acteurs (management, équipe informatique sur site, les utilisateurs) par des rapports illustrant les failles décelées, les tests qui ont été effectués (scénarios et outils) ainsi que les recommandations permettant de pallier les insuffisances identifiées.

Audit de vulnérabilités face aux failles connues

Au cours de cette étape, le réseau, les équipements et les applications seront audités afin d'identifier les composants vulnérables du système d'information. Cette phase peut être abordée selon différentes techniques de test :

Tests automatiques : tests utilisant des scanners de vulnérabilités spécifiques pour chaque plateforme ou solution appartenant au périmètre audité. Un unique rapport sera dégagé où les scénarios d'attaques ainsi que la criticité des failles seront définis par l'auditeur Alliacom.

Tests semi-automatiques : opération de test avec des scripts développés par l'auditeur Alliacom ou des scripts d'exploitation issus de la communauté des professionnels de sécurité.

Tests manuels : opération d'audit des configurations par rapport à un ensemble de référentiels de bonnes pratiques (Check-list SANS, NIST). Au cours de cette étape, l'auditeur Alliacom devra accéder directement aux composants audités

Exemple de test : déni de service, forge d'URL, empoisonnement ARP, man in the middle, attaques de mots de passe, capture de trafic, attaque d'authentification, etc.

Audit de conformité

Il s'agit de vérifier l'application des règles de sécurité prescrites et imposées sur le système d'information, (politique de sécurité, standards, etc.). Cette phase d'audit couvrira :

- l'audit des postes de travail (configurations, mises à jours, périphériques, etc.),
- l'audit des serveurs en exploitation (configurations, droit d'accès, robustesse aux dénis de service, etc.),
- l'audit des applications (droits d'accès, résistance aux attaques de force brute, injections de codes, etc.),
- l'audit des bases de données (conformités, droits d'accès, déni de services, etc.),
- l'audit des équipements de réseaux (switches, routeurs, réseaux sans fils, téléphonie sur IP, etc.),
- l'audit des solutions de sécurité (firewalls, antivirus, IDS/IPS, infrastructure PKI, etc.).

Audit de l'opacité du système depuis l'extérieur

Au cours de cette phase, les possibilités offertes à un attaquant de récupérer depuis l'extérieur les caractéristiques du système d'information seront vérifiées. Une évaluation de l'herméticité des frontières du réseau, contre les tentatives d'exploitation par des attaquants externes sera également élaborée.

La démarche itérative comporte en général :

- Recueil d'informations sur la cible,
- Détection des systèmes et des services, cartographie,
- Recherche & exploitation de vulnérabilités réseau,
- Recherche et exploitation de vulnérabilités système,
- Recherche et exploitation des failles applicatives,
- Progression et escalade de privilèges,
- Maintenance.

Exemple de test : déni de service, ingénierie sociale, usurpation d'identité/ de droit, empoisonnement DNS, injection de codes malicieux dans le LAN, etc.

Audit intrusif Audit des S.I

www.alliacom.com

ALLIACOM

Démarche d'audit intrusif

Un audit intrusif sera réalisé selon une succession de phases respectant une approche méthodique allant de la découverte et la reconnaissance du réseau audité jusqu'à la réalisation des scénarios d'attaques expertes. Un audit complet englobera :



Une approche « boîte blanche » : l'auditeur dispose de toutes les informations et documentations nécessaires et essaiera de tester et de valider la conformité de l'existant par rapport au prévu.



Une approche « boîte grise » : l'auditeur dispose de quelques informations sur l'architecture interne et de privilèges minimaux sur le réseau cible (compte utilisateur quelconque). Il cherche à accroître ses privilèges depuis l'intérieur même du réseau.



Une approche « boîte noire » : l'auditeur ne connaît rien du réseau cible et ne dispose d'aucun accès à celui-ci : audit d'intrusion externe (en aveugle).

Savoir - faire :

Le savoir-faire Alliacom est fondé sur l'expertise de ses auditeurs ainsi que sur les normes et les standards du domaine : OSSTMM, OWASP, NIST SP-800, SANS.

Charges :

Mission	Réf.	Durée
Audit de conformité	ADECO	De 5 à 20 Jours
Audit de Vulnérabilités du système face aux failles connues	ADEV	De 5 à 10 Jours
Audit de l'opacité du système depuis l'extérieur	ADOS	De 5 à 15 Jours

Boite à outils :

La boîte à outils utilisée comprend plusieurs outils commerciaux, outils du monde libre, des scripts (Perl, Python) et des tests manuels: BackTrack, Metasploit, Nmap, Netcat, Nessus, Ettercap, Wireshark, TCPDUMP, Etherape, Ntop, Hping, Yersinia, Nemesis, Kismet, Aircrack, Aircrack-ng, MBSA, SAINT, ISS, PAROS, WebScarab, Burp, Hping, SqEEL, SQLInjector, Cain & Abel, John the Ripper, PWdump, Ophcrack, Hydra, Brutus, etc

Les Livrables :



Un rapport de tests d'audit



Une liste de recommandations avec plan d'actions



Une présentation de synthèse

Références :

Le service d'audit S.I et audit intrusif Alliacom jouit de la confiance de plusieurs clients de différents domaines, en particulier dans les secteurs suivants:

- Cosmétique,
- Paris et jeux en ligne,
- Juridique et réglementaire,
- Développement de progiciel,
- Conseil et intégration de services informatiques.



V2.1