

L'évaluation technique de la sécurité des systèmes d'information par les tests d'intrusion s'inscrit dans une démarche projet et suit les standards du marché (ISO 27001 notamment). Elle aboutit à la rédaction de livrables clairs et didactiques.

Objectifs

- Mettre à l'épreuve la sécurité d'un système d'information
- Qualifier son niveau de résistance à une attaque informatique
- Révéler des points non visibles par un audit de sécurité
- Se conformer à une exigence réglementaire (type PCI-DSS de VISA & MasterCard)
- Sensibiliser le personnel au sein de l'entreprise

Evaluation du risque

- Le niveau de risque est calculé en fonction de l'impact et de la probabilité

		Risque			
		Elevé	Moyen	Elevé	Critique
Impact	Moyen	Faible	Moyen	Elevé	
	Faible	Nul	Faible	Moyen	
		Faible	Moyen	Elevé	
		Probabilité			

Livrable

- Un rapport comprenant :
 - ◆ L'ensembles des informations découvertes
 - ◆ L'ensemble des failles classées suivant une échelle de risques à 4 niveaux
 - ◆ Recommandations d'amélioration
- Des tableaux de bord :
 - ◆ Indicateurs métier
 - ◆ Indicateurs de sécurité
 - ◆ Tableaux de bord techniques
- Des graphiques de type « radar »

Périmètres possibles

- Phases techniques spécifiques aux périmètres testés :
- ◆ Test des infrastructures depuis Internet
 - ◆ Test du système d'information depuis le réseau local ou depuis un point du réseau étendu
 - ◆ Infrastructures téléphoniques,
 - ◆ Réseaux sans fil...

Charte de l'intrusion

- 5 principes fondateurs des règles déontologiques :
- ◆ La Moralité
 - ◆ La Transparence
 - ◆ La Confidentialité
 - ◆ La Probité
 - ◆ L'Adaptabilité