Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 6 septembre 2018

N° 16400 /ANSSI/SDE/PSS/CCN

Référence : ANSSI-CC-NOTE-18/1.1

NOTE D'APPLICATION

PRISE EN COMPTE DES OUTILS DANS LES EVALUATIONS LOGICIELLES

Application : Dès son approbation.

Diffusion : Publique.

Le directeur général
de l'agence nationale de la sécurité
des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

Suivi des modifications

Edition	Date	Modifications
1.0	05/05/2015	Création.
1.1	6/9/2018	Mise à jour.

En application du décret n° 2002-535 du 18 avril 2002 modifié, la présente procédure a été soumise au comité directeur de la certification, qui a donné un avis favorable.

La présente procédure est disponible en ligne sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

Table des matières

1. Objet de la note

1.1. Objet

Cette note précise la prise en compte des outils par l'analyse de vulnérabilités réalisée lors d'évaluations du domaine « logiciel et équipements réseaux » au sein du schéma français. Elle concerne les évaluations Critères Communs (CC) et les évaluations selon la Certification de sécurité de premier niveau (CSPN).

1.2. Références

[CEM] *Common Methodology for Information Technology Security Evaluation,* version en vigueur.

[CER] Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, référence : ANSSI-CC-CER-P-01, version en vigueur.

[CSPN] Certification de sécurité de premier niveau des produits des technologies de l'information, référence : ANSSI-CSPN-CER-P-01, version en vigueur.

1.3. Périmètre

Pour déterminer le niveau de résistance (niveau AVA_VAN) atteint par un produit dans le cadre d'une évaluation CC, la [CEM] fournit un système de notation précisant les niveaux et les points associés à plusieurs paramètres impliqués dans la réussite d'une attaque. L'un de ces paramètres correspond aux outils à disposition de l'attaquant (paramètre *Equipment*).

La [CEM] est générique et est applicable aussi bien aux évaluations de produits matériels que logiciels. Cependant, il a été constaté l'inadéquation de la cotation proposée par [CEM] avec la réalité des évaluations logicielles. En particulier la prise en compte du paramètre *Equipment* conformément à [CEM] manque de pertinence pour le domaine « logiciel et équipements réseaux », les outils considérés étant souvent publics ou accessibles facilement par un attaquant motivé.

2. Cotation des outils logiciels

Etant donné la large diffusion d'outils gratuits ou libres permettant d'identifier des chemins d'attaque ou d'exploiter des vulnérabilités, aucun outil logiciel commercial ne peut être considéré comme correspondant au niveau *Bespoke* (ainsi qu'*a fortiori*, au niveau *Multiple bespoke*) de [CEM]. Cependant la difficulté d'utilisation d'un outil sera prise en compte et cotée dans le critère *Expertise* de [CEM].

Seuls les outils génériques sont considérés dans la présente note. Les outils propres au CESTI, développés par lui-même et non rendus publics, tels que des scripts, seront cotés au travers des critères *Elapsed Tim*e et *Expertise* de [CEM].

La grille de cotation suivante est à prendre en compte pour les évaluations logicielles réalisées dans le cadre du schéma français.

Facteur *Equipment*		
Niveau	Valeur	Catégories de produits correspondantes
Standard	0	Logiciel gratuit, libre, ou commercial « grand public ». Exemples : Gdb, OllyDbg, Wireshark, Nmap, Nessus, Metasploit, Scapy, etc.
Specialized	2	- Logiciel commercial ne disposant pas de version d'essai pouvant être utilisée de manière opérationnelle par un attaquant, - Adaptation de logiciel libre développée par l'évaluateur, pour autant qu'il n'existe pas d'équivalent fonctionnel de niveau *Standard*. Exemples : IDA Pro, Cryptosense Analyzer, etc.