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, 5 mai 2015

N° 1814/ANSSI/SDE/PSS/CCN

Référence: ANSSI-CC-NOTE-18/1.0.EN

APPLICATION NOTE

ACKNOWLEDGEMENT OF TOOLS IN SOFTWARE EVALUATIONS

Application	:	From date of publication.
Distribution	:	Public.

COURTESY TRANSLATION

Version history

Version	Date	Modifications
1.0	05/05/2015	Creation

Pursuant to amended decree No. 2002-535 of 18th April 2002, this procedure has been submitted to the certification management committee, which gave a favourable opinion.

This procedure is available online on the ANSSI's institutional website (www.ssi.gouv.fr).

Table of contents

1. Subject of the note

1.1. Subject

This note specifies the acknowledgement of tools by the vulnerability analysis carried out during Common Criteria (CC) evaluations in the « software and network equipment » field within the French scheme.

1.2. References

[CEM] *Common Methodology for Information Technology Security Evaluation*, version 3.1 revision 4, Septembre 2012.

[CER] Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, référence : CER/P/01.1, version 1, 9 février 2004.

[CSPN] Certification de sécurité de premier niveau des produits des technologies de l'information, référence : ANSSI-CSPN-CER-P-01/1.1, version 1.1, 7 avril 2014.

[AGR] Agrément des centres d'évaluation, référence : AGR/P/01.2, version 2, 30 janvier 2008.

1.3. Scope

To determine the level of resistance (AVA_VAN level) reached by a product in the context of a CC evaluation, the [CEM] provides a scoring system which specifies the levels and points associated with several parameters involved in the success of an attack. One of these parameters corresponds to the tools available to the attacker (*Equipment* parameter).

The [CEM] is generic and applies to both hardware and software product evaluations. However, the unsuitability of the scoring proposed by [CEM] with the reality of software evaluations has been observed. In particular, the acknowledgement of the *Equipment* parameter in accordance with [CEM] lacks relevance for the « software and network equipment » field as the tools in question are often public and easily accessible to a motivated attacker.

2. Software tool scoring

Given the wide distribution of free or open source tools that enable attack paths to be identified or vulnerabilities to be exploited, no commercial software tools may be considered as corresponding to the *Bespoke* level (as well as'*a fortiori*, to the *Multiple bespoke* level) in [CEM]. However, the difficulty in using a tool will be taken into account and scored in the *Expertise* parameter in [CEM].

Only the generic tools are considered in this note. The tools specific to the ITSEF, which are developed by them and not made public, such as scripts, will be scored through the *Elapsed Tim*e and *Expertise* criteria in [CEM].

The following scoring grid must be taken into account for the software evaluations carried out under the French scheme.

Equipment factor		
Level	Value	Corresponding product categories
Standard	0	Free, open source or "mass market" commercial software. Examples: Gdb, OllyDbg, Wireshark, Nmap, Nessus, Metasploit, Scapy, etc.
Specialized	2	If there is no *Standard* level functional equivalent : - commercial software that does not have a trial version but may be used operationally by an attacker, - adaptation of open source software developed by the evaluator, Examples: IDA Pro, Cryptosense Analyzer, etc.