PREMIER
MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 12 Juillet 2024

N° 1249 /**ANSSI/SDE/PSS/CCN**

Référence **: ANSSI-CSPN-NOTE-01_v4**

NOTE D'APPLICATION

CONTENU ET STRUCTURE DU RAPPORT TECHNIQUE D'ÉVALUATION CSPN

Application **:** le 1er Septembre 2024.

Diffusion **:** Publique.

Le sous-directeur « Expertise » adjoint de l'Agence nationale de la sécurité des systèmes d'information

Annaïg ANDRO

SUIVI DES MODIFICATIONS

Version	Date	Modifications
Phase expérimentale	30 janvier 2008	Première rédaction pour la phase expérimentale, abrogée par la présente procédure.
1	30 mai 2011	Fin de la phase expérimentale. Changement de dénomination de l'organisme de certification (ANSSI) et améliorations de forme.
2	23 avril 2014	Modification du domaine de classification du document : passage d'une instruction à une note d'application. Retrait des redondances vis-à-vis de [CER-P-02]. Mise en conformité vis-à-vis de la procédure ANSSI-CSPN-CER-P-01.
3	6 septembre 2018	Restructuration du contenu du RTE.
4	12 juillet 2024	Restructuration du contenu suite aux modifications introduites dans [CER-P-01] et [CER-P-02].

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

Cette note est également soumise pour avis lors de chaque modification majeure conformément au manuel qualité du centre de certification. Les évolutions mineures ne sont pas soumises au comité directeur de la certification.

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

TABLE DES MATIERES

1 Objet de la note d'application

La présente note d'application fixe le format et les informations attendues dans les rapports techniques d'évaluation (RTE) de certification de sécurité de premier niveau (CSPN). Elle constitue un complément à la description des critères d'évaluation CSPN décrit par [CER-P-02].

2 Exigences relatives au RTE

Le présent document impose des exigences de contenu et de présentation pour le rapport technique d'évaluation (RTE) rédigé par l'évaluateur dans le cadre d'une évaluation CSPN.

E_CSPN_RTE_1. Le RTE doit inclure au moins l'ensemble des chapitres imposés par l'annexe A.

E_CSPN_RTE_2. Les fiches de test annexées au RTE doivent inclure au moins les informations imposées par l'annexe C.

E_CSPN_RTE_3. La classification des vulnérabilités, dans le RTE, doit être conforme à l'annexe D.

Remarque : ces exigences ont pour but principal de faciliter l'analyse de conformité du RTE par rapport à [CER-P-02]. Elles permettent également de garantir un niveau minimum de qualité pour l'évaluateur, en tenant lieu de garde-fou contre des oublis éventuels. Elle vise enfin à faciliter la comparaison de RTE entre différents évaluateurs. Les évaluateurs sont invités à détailler et raffiner le modèle fourni par l'annexe A en fonction de leur propre retour d'expérience.

ANNEXE A. Contenu du rapport technique d'évaluation CSPN

1 Identification du rapport technique d'évaluation

E_CSPN_RTE_4. Le RTE doit fournir au moins les informations ci-dessous :

Nom du projet d'évaluation	Identifiant unique (référencé dans la lettre d'enregistrement)
Référence du RTE	Identifiant unique défini par le CESTI, et identification - De la date de création initiale du RTE ; - De sa version actuelle et de la date de révision correspondance.
Auteur(s)	Expert(s) intervenant dans la réalisation de l'analyse
Relecteur(s) et Approbateur(s)	Noms : - du ou des relecteurs techniques ; - du ou des approbateurs autorisant la libération du rapport.

Remarque : Il est important que les relecteurs techniques apparaissent distinctement, afin notamment que le CESTI puisse démontrer que les personnels compétents ont bien été consultés (présence de personnel-clé pour une compétence donnée, etc.).

2 Identification du produit évalué et de la cible

2.1 Identification de la cible d'évaluation et des fournitures documentaires

E_CSPN_RTE_5. Le RTE doit fournir au moins les informations ci-dessous :

Nom de l'éditeur	Nom de l'éditeur du produit
Nom du produit	Nom commercial
Identification de la cible d'évaluation	Identification de la cible si différente du nom commercial, incluant sa version exacte (version, *build, release,* correctifs éventuels…)
Identification des fournitures documentaires	Référence, version et date des documents exigés par les phases 1 et 3 de [CER-P-02]
Domaine technique CSPN	Sélectionner parmi les domaines de la procédure [AGR-P-01]

2.2 Procédure d'identification du produit évalué

E_CSPN_RTE_6. L'évaluateur doit décrire la procédure que doit suivre l'utilisateur final pour s'assurer qu'il dispose bien de la version évaluée du produit.

Remarque : Une capture d'écran ou photo de l'affichage de la version sera incluse. Dans le cas d'un boitier matériel, le numéro de série du boitier sera indiqué. Un avis pourra être émis dans le cas d'incohérences ou imprécisions sur l'identification du produit ou de ses composants.

3 Détail des travaux d'évaluation

3.1 Phase 1 - Analyse de la cible de sécurité et des spécifications cryptographiques

E_CSPN_RTE_7. Après avoir effectué les tâches de la Phase 1 de [CER-P-02], l'évaluateur doit, pour chacune des exigences, statuer sur la conformité à cette exigence et décrire toute non-conformité.

Remarques : Pour chaque exigence de [CER-P-02], le statut conforme ou non-conforme à cette exigence devra être justifié, et l'évaluateur devra préciser les éléments absents ou inexacts.

L'évaluateur pourra également fournir un avis sur le modèle de sécurité choisi dans la cible de sécurité et le reformuler, par exemple :

- cas d'un produit destiné au grand public mais nécessitant des connaissances avancées ;
- manière dont il est prévu d'utiliser le produit ;
- environnement prévu pour l'utilisation du produit et menaces supposées dans cet environnement.

E_CSPN_RTE_8. L'évaluateur devra émettre un avis sur les vulnérabilités potentielles identifiées lors de l'analyse de la phase 1.

Remarques : Ces vulnérabilités sont par exemple des problèmes de cohérence de la cible de sécurité et/ou de la spécification cryptographique, par exemple :

- une hypothèse abusive au regard de l'environnement d'utilisation prévue ;
- une menace non prévue par la cible, mais qui nécessite d'être ajoutée au regard des biens sensibles décrits ;
- une fonction de sécurité non pertinente pour couvrir une menace donnée ;
- l'absence de fonctions de sécurité pour couvrir une menace ;
- etc.

Il est recommandé de donner des identifiants[1] à ces vulnérabilités, qui seront à intégrer à la stratégie de tests de pénétration (phase 5).

3.2 Phase 2 - Installation et mise en œuvre du produit

E_CSPN_RTE_9. Après avoir effectué les tâches de la phase 2 de [CER-P-02], l'évaluateur devra, pour chacune des exigences, statuer sur la conformité à cette exigence et décrire toute non-conformité.

E_CSPN_RTE_10. Pour pouvoir statuer sur **l'installation de la plate-forme d'évaluation**, l'évaluateur devra décrire la plate-forme réellement utilisée pour réaliser les tests sur le produit. Cela inclut les versions précises des composants de l'environnement (par exemple le système d'exploitation si la TOE est une application).

E_CSPN_RTE_11. Pour pouvoir statuer sur **l'installation du produit**, l'évaluateur devra :

- lister la documentation d'installation et de configuration ;
- décrire les options d'installation retenues pour l'évaluation et les particularités de paramétrage de l'environnement.

E_CSPN_RTE_12. Pour pouvoir statuer sur la **mise en état sécurisé**, l'évaluateur devra :

[1] De préférence à un identifiant numérique, on privilégiera un nom plus parlant (par exemple « Absence de chiffrement local de la donnée sensible XXX »).

- décrire toutes les informations qui permettent de mener à bien l'installation et les non-conformités éventuelles de l'installation par rapport à la documentation existante, ainsi que la durée de l'installation ;
- décrire s'il est facile pour le produit de sortir de son état sécurisé, et si des avertissements sont donnés à l'utilisateur en cas de sortie de l'état sécurisé.

E_CSPN_RTE_13. L'évaluateur devra émettre un avis sur les vulnérabilités potentielles identifiées lors de l'analyse de la phase 2.

Remarques : L'évaluateur s'attachera aux fonctionnalités intrinsèquement non sûres, mais également au risque qu'un utilisateur finisse par placer le produit dans une configuration non sûre en raison de la complexité d'usage du produit. Ces vulnérabilités sont typiquement des réductions non intentionnelles du niveau de sécurité causées par la complexité du produit ou une documentation insuffisante concernant :

- son/ses processus d'installation ;
- ses modes d'utilisation ;
- les profils des utilisateur considérés ;
- etc.

Il est recommandé de donner des identifiants[2] à ces vulnérabilités, qui seront à intégrer à la stratégie de tests de pénétration (phase 5).

3.3 Phase 3 – Analyse de la documentation et des processus de développement

E_CSPN_RTE_14. Après avoir effectué les tâches de la phase 3 de [CER-P-02], l'évaluateur devra, *pour chacune des exigences*, statuer sur la conformité à cette exigence et décrire toute non-conformité.

Remarques : L'évaluateur doit faire une revue complète des fournitures. En particulier, si l'évaluation est tenue de suivre une méthode particulière pour un domaine donné, l'évaluateur doit systématiquement faire la revue des fournitures requises par la méthode. Les fournitures incluent typiquement les fournitures documentaires (par exemple les guides du produit). A ces fournitures de base peuvent s'ajouter d'autres documents (par exemple issues de la conception du produit). Il peut être également nécessaire, pour un produit donné, de fournir des fournitures non documentaires : environnements de développement ou de compilation, outils ou vecteurs de test, etc.

E_CSPN_RTE_15. Concernant l'évaluation (optionnelle) du **processus de développement,** si l'évaluateur a pu revoir la documentation et/ou s'entretenir sur le sujet avec les développeurs, alors l'évaluateur devra émettre un avis d'expert sur les risques pesant sur la sécurité du produit lors du cycle de vie de développement.

Remarques : L'évaluateur pourra s'inspirer de la liste qui suit pour étayer son avis :

- sécurité de l'environnement de développement : locaux, types de personnels, réseau de développement, etc. ;
- existence d'un système qualité ;
- existence d'une documentation de conception et de réalisation du produit ;

[2] De préférence à un identifiant numérique, on privilégiera un nom plus parlant (par exemple « Risque de mauvaise configuration des clés à l'installation »).

- existence d'une gestion de configuration ;
- existence d'un processus de livraison sécurisé ;
- capacité des développeurs à répondre aux questions posées.

Cette tâche est facultative. En revanche, si l'évaluateur a été amené à interagir avec le développeur dans le cadre de l'évaluation, il est tenu de décrire la nature des échanges avec le développeur, le résultat de ces échanges et, lorsqu'applicable, de donner un avis sur sa maîtrise du produit et ses processus de développement.

En outre, s'il s'avère impossible de conclure sur un sujet dans le cadre des tests de pénétration (voir 3.5), ces entretiens avec les développeurs peuvent être un moyen de confirmer ou d'infirmer la présence d'une vulnérabilité.

E_CSPN_RTE_16. L'évaluateur doit fournir un avis sur les vulnérabilités potentielles identifiées lors de l'analyse de la conception et des processus de développement.

Remarques : Ces vulnérabilités sont typiquement des failles de conception :

- erreur de conception sécuritaire, par exemple choix d'un protocole inadapté pour le problème considéré ;
- utilisation de mécanismes cryptographiques vulnérables ;
- failles organisationnelles lors du cycle de vie (pas de traçabilité des modifications du code, pas de sécurisation des livraisons, etc.)
- etc.

Il est recommandé de donner des identifiants[3] à ces vulnérabilités, qui seront à intégrer à la stratégie de tests de pénétration (phase 5).

3.4 Phase 4 - Analyse de la conformité des fonctions de sécurité et des mécanismes cryptographiques

E_CSPN_RTE_17. Après avoir effectué les tâches de la phase 4 de [CER-P-02], l'évaluateur devra, *pour chacune des exigences*, statuer sur la conformité à cette exigence et décrire toute non-conformité.

E_CSPN_RTE_18. L'évaluateur consacrera un chapitre à chaque fonction de sécurité ; l'analyse cryptographique peut être intégrée aux fonctions, ou bien rédigée à part (par exemple si les mécanismes cryptographiques sont utilisés dans plusieurs fonctions différentes).

E_CSPN_RTE_19. Pour pouvoir statuer sur la conformité des fonctions de sécurité et mécanismes cryptographiques, L'évaluateur devra fournir :

- un **plan de tests** : court paragraphe référençant des fiches de test conformes à l'ANNEXE C, et décrivant leur rôle respectif dans le plan général (séquencement, pertinence ou priorisation d'un test par rapport à un autre, etc.) ;
- les fiches de test renseignées, décrivant les résultats de la **campagne de tests**.

Remarques : Pour des raisons de lisibilité, les fiches de tests seront de préférence placées en annexe du RTE. L'évaluateur précisera clairement lorsque des fonctions n'ont pas pu être analysées ou ne l'ont été que partiellement, et comment a été réalisée cette analyse (analyse statique ou dynamique).

[3] De préférence à un identifiant numérique, on privilégiera un nom plus parlant (par exemple « Possible buffer overflow dans la classe XXX »).

Il est à noter que si des tests ne sont pas possibles, d'autres moyens de vérification peuvent être utilisés par l'évaluateur (par exemple revue de code source si disponible).

E_CSPN_RTE_20. L'évaluateur fournira une synthèse de la conformité des fonctions de sécurité en suivant le tableau ci-dessous :

Fonction	Fiches de test	Conformité de la fonction à la cible de sécurité	Conformité de la fonction à l'état de l'art
Fonction A	Référencer la ou les fiches de test correspondante(s).	Valeurs possibles : Oui / Non / Partielle / Impossible de conclure	Quand cela est pertinent[4], indiquer si les mécanismes mis en œuvre sont conformes[5] à des standards ou des recommandations de référentiels existants. Dans le cas d'une fonction s'appuyant sur des mécanismes cryptographiques, l'évaluateur indiquera ici la conformité à [ANSSI-PG-083].

E_CSPN_RTE_21. L'évaluateur doit fournir un avis sur les vulnérabilités potentielles identifiées lors de l'analyse de la phase 4.

Remarque : Ces vulnérabilités peuvent être liées :

- à une fonction de sécurité non conforme à sa spécification dans la cible ;
- à une faille résultant de l'écart à une bonne pratique ou un standard ;
- à des vulnérabilités permettant de contourner les fonctions de sécurité : canaux cachés, exploitation de données résiduelles ;
- etc.

Il est recommandé de donner des identifiants[6] à ces vulnérabilités, qui seront à intégrer à la stratégie de tests de pénétration (phase 5).

3.5 Phase 5 - Analyse de la résistance

E_CSPN_RTE_22. Après avoir effectué les tâches de la phase 5 de [CER-P-02], l'évaluateur devra, *pour chacune des exigences*, statuer sur la conformité à cette exigence et décrire toute non-conformité.

E_CSPN_RTE_23. Pour pouvoir statuer sur **l'identification de la surface d'attaque**, l'évaluateur devra décrire la surface d'attaque en termes d'interfaces du produit, d'attaquant potentiel, et les scénarios d'attaque pertinents.

E_CSPN_RTE_24. Pour pouvoir statuer sur les **tests de pénétration**, L'évaluateur devra fournir :

[4] Par exemple, des fonctions de contrôle d'accès ou de journalisation n'ont pas nécessairement d'état de l'art applicable.

[5] La non-conformité partielle concernera typiquement les cas « tangents », par exemple lorsqu'une fonction de protection des communications utilisant du TLS est conforme à la cible de sécurité, et permet d'utiliser à la fois des *cipher suites* conformes à [ANSSI-PG-083] et des *cipher suites* non conformes.

[6] De préférence à un identifiant numérique, on privilégiera un nom plus parlant (par exemple « Négociation d'une *cipher suite* interdite sur protocole XXX »).

- un plan de tests : court paragraphe décrivant la stratégie de tests (séquencement, pertinence ou priorisation d'un test par rapport à un autre, abandon d'un test au profit d'un autre en raison des données recueillies etc.).
  La description du plan de tests pourra également présenter un arbre d'attaque à des fins de lisibilité ou de synthèse des chemins explorés/non explorés ;
- la description des tests effectués et de leurs résultats.

Remarque : Concernant le plan de test de pénétration, ainsi que et la campagne de test associée, il est possible d'utiliser des fiches de test conformes à l'ANNEXE C, comme pour les tests de conformité. Il est cependant possible que ces fiches soient plus détaillées et de périmètre plus large (par exemple, au lieu de viser la conformité d'un canal TLS, une fiche de test pourra regrouper les tentatives d'élévation de privilèges UID sur le système évalué.

Remarque : Les tests incluent l'analyse du code source si celui-ci est disponible.

Remarque : En outre, si des outils ou des méthodologies spécifiques sont nécessaires pour l'exploitation de la vulnérabilité, ils seront décrits. Si l'évaluateur doit utiliser des outils fournis par le développeur ou un tiers, ils seront livrés avec le produit dans la mesure où ils sont libres de droits (logiciels libres ou développés sur mesure au titre du marché). L'évaluateur doit dans ce cas effectuer une phase de validation des outils, et préciser dans le RTE ce qui a été effectué lors de cette phase. Cette phase doit notamment être effectuée en conformité avec la [NOTE-18].

E_CSPN_RTE_25. L'évaluateur effectuera une synthèse des résultats de tests à travers la liste des biens qu'il est possible de compromettre ou des menaces qu'il est possible de réaliser. IL devra respecter le modèle ci-dessous :

Biens ou Menaces[7]	Vulnérabilité	Exploitation (non exploitable / exploitable / résiduelle)
Bien ou Menace XXX (tiré de la cible de sécurité)	#VULN	Indiquer si la vulnérabilité est exploitable, non exploitable ou résiduelle (voir ANNEXE D). Selon le cas, l'évaluateur sera amené à faire une cotation de la vulnérabilité : - Vulnérabilités **non exploitables** (ne peuvent pas être mises en œuvre dans le contexte d'usage prévu[8], notamment en raison des hypothèses sur le produit) : un argumentaire est requis de la part de l'évaluateur mais il n'est pas nécessaire de faire une cotation (voir Annexe C) ; - Dans les autres cas, l'évaluateur doit s'appuyer sur une cotation afin de distinguer entre vulnérabilités **exploitables** et **résiduelles**.

[7] L'évaluateur peut choisir de structurer le tableau selon les biens ou les menaces, et est invité à privilégier la clarté de l'explication.

[8] Le contexte d'usage est principalement défini par les hypothèses de la cible de sécurité. Conformément à [CER-P-02], il est possible de définir des *contre-mesures environnementales réalistes* permettant de remédier à certaines vulnérabilités. Dans ce cas, le développeur doit mettre à jour les guides du produit pour signaler ces contremesures à l'utilisateur. La vulnérabilité concernée sera alors déclarée comme *non exploitable*.

E_CSPN_RTE_26. Pour statuer sur la **recherche de vulnérabilités induites par le produit sur son système hôte**, l'évaluateur devra également effectuer la cotation des vulnérabilités induites sur la sécurité du système hôte.

Biens ou Menaces	Vulnérabilité	Exploitation (Exploitée / non exploitable / exploitable / résiduelle)
Sécurité du système hôte	#VULN	Même principe que dans le tableau précédent

E_CSPN_RTE_27. Dans le cas où des scénarios exploitables seraient identifiés, l'évaluateur recommandera une configuration, ou des conditions de mise en œuvre, permettant d'atteindre le meilleur niveau de sécurité afin de contrer les menaces identifiées. Une réduction du périmètre fonctionnel du produit (au sens de la sécurité) peut éventuellement être proposée.

Remarque : Lorsqu'une vulnérabilité n'entraîne qu'une attaque partielle, il n'est pas possible d'y associer un bien compromis ou une menace réalisée. Dans ce cas, il n'est donc pas nécessaire d'inclure la vulnérabilité dans le tableau de de synthèse.

4 Synthèse de l'évaluation

E_CSPN_RTE_28. Le rapport technique d'évaluation (RTE) élaboré par l'évaluateur, contenant et argumentant les résultats de l'évaluation, doit être présenté sous une forme acceptable pour être pris en considération par le centre de certification de l'ANSSI. Pour cela, le RTE doit comporter au minimum les informations suivantes :

- le rappel du contexte de l'analyse (en particulier la durée des travaux pour chaque phase) ;
- une synthèse des résultats des tests effectués sur le produit (phases 1 à 5) ;
- un avis d'expert sur l'aptitude ou non du produit à être certifié, constitué
  - du bilan des non conformités à la cible de sécurité ;
  - du bilan et de la cotation des vulnérabilités identifiées ;
  - du bilan des préconisations d'utilisation ou de paramétrage permettant, lorsque cela est possible, de limiter l'exploitabilité des vulnérabilités ;
  - du bilan des vulnérabilités induites par le produit sur son système hôte.

E_CSPN_RTE_29. L'évaluateur doit indiquer si selon lui, le produit est un bon ou mauvais candidat à la certification CSPN et motiver son choix en cohérence avec l'avis d'expert précédent.

Remarques :

Si le RTE fait apparaître que le produit ne répond pas ou ne répond que partiellement à sa cible de sécurité et qu'il n'est pas possible d'identifier des contre-mesures environnementales réalistes pour améliorer cette situation, le produit sera considéré comme ne répondant pas à sa cible de sécurité.

Il en est de même si les tests font apparaître des dysfonctionnements du produit, n'en permettant pas un usage normal ou l'usage prévu, l'affaiblissement du système hôte ou si certaines conclusions du RTE sont « non concluantes », par exemple faute d'information.

Le but de ce chapitre est de fournir une synthèse générale de la sécurité du produit. Cette synthèse condense l'ensemble des travaux décrits dans le chapitre 3 et les met en perspective par rapport au problème de sécurité défini dans la cible, afin de :

- mettre en lumière les vulnérabilités exploitables ou exploitées ;
- mettre en perspective ces vulnérabilités dans le contexte de la cible (clarifier quels biens peuvent être compromis, et par quel chemin d'attaque) ;
- conclure quant à l'aptitude ou non du produit à être certifié.

L'évaluateur peut utiliser ce chapitre pour donner un avis au format libre sur le produit. Par exemple, l'évaluateur peut décrire ici les réserves éventuelles qu'il a vis-à-vis du produit, indépendamment des vulnérabilités qu'il contient.

Par exemple, si l'analyse du code source a révélé de nombreux problèmes potentiels liés, par exemple, à des erreurs d'implémentation telles que l'utilisation de fonctions dépréciées et/ou de constructions jugées dangereuses, l'évaluateur n'aura pu dans le temps imparti en tester effectivement qu'un échantillon. Il est dans ce cas invité à appuyer son avis sur la probabilité que de telles vulnérabilités puissent, en dépit des résultats bruts de l'évaluation, être exploitées sur le terrain.

L'évaluateur est libre d'ajouter des sous-chapitres à la synthèse, tant qu'ils n'entrent pas en conflit avec les sous-chapitres imposés par le modèle. Par exemple, l'évaluateur peut ajouter :

- un sous-chapitre traitant des « points positifs » relevés sur le produit ;
- un sous-chapitre traitant de la gestion de projet ;
- etc.

ANNEXE B. Références

Référence	Document
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, version en vigueur.
[ANSSI-PG-083]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.
[CER-P-01]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version en vigueur.
[CER-P-02]	Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version en vigueur.
[AGR-P-01]	Agrément des centres d'évaluation en vue de la certification de sécurité de premier niveau, référence ANSSI-CSPN-AGR-P-01, version en vigueur.
[CRYPTO]	Fournitures nécessaires à l'analyse de mécanismes cryptographiques, version en vigueur (disponible sur le site institutionnel de l'ANSSI).
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations de générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P-01, version en vigueur.
[NOTE-18]	Prise en compte des outils dans les évaluations logicielles, référence ANSSI-CC-NOTE-18, version en vigueur.

La plupart de ces documents peuvent être consultés et téléchargés depuis le site de l'ANSSI (www.cyber.gouv.fr).

ANNEXE C. Modèle de fiche d'analyse de conformité des fonctions de sécurité

<table>
<tr><td colspan="2">Objectif de l'analyse</td><td colspan="2">Identification du produit évalué : Logiciel XXX version 3.5</td></tr>
<tr><td colspan="2" rowspan="2">Fonction de sécurité : filtrage IP</td><td>Réf. : Test-PPP-1</td><td>Auteur : XXXXX</td></tr>
<tr><td colspan="2">Objet du test : Un pare-feu devrait re jeter tout le trafic non explicitement autorisé. Ce test vérifie que le logiciel XXX est bien dans ce cas.</td></tr>
<tr><td colspan="4">Prérequis : machine tout juste installée</td></tr>
<tr><td>Opérations à effectuer</td><td>Résultats attendus</td><td colspan="2">Résultats observés</td></tr>
<tr><td>Désactiver la règle de rejet par défaut et faire un «scan» du réseau interne avec par exemple netwox 67 --ips 10.2.0.1-10.2.0.2 --ports 20-55 pour TCP et la même chose pour UDP avec la commande n° 69. Réactiver la règle.</td><td>Aucune connexion TCP ne réussit. Pour UDP, seul le port 53 doit être accessible.</td><td colspan="2">Le «scan» TCP déclare toutes les tentatives en «timeout», sauf pour le port autorisé correspondant à SMTP. Le «scan» UDP déclare «timeout» pour tous y compris le port 53 correspondant au DNS, ce qui est inattendu.</td></tr>
<tr><td colspan="4">Conclusion :</td></tr>
<tr><td colspan="4">Résultats corrects, le rejet du paquet UDP vers le port 53 étant dû, d'après le journal du firewall, au fait que celui-ci n'est pas un paquet DNS correct.</td></tr>
</table>

ANNEXE D. Classification des vulnérabilités

Les vulnérabilités doivent être classées en fonction des réponses aux questions suivantes :

Contexte d'usage :

La vulnérabilité est-elle applicable dans le contexte d'usage prévu par la cible ? (en particulier si l'on considère les mesures environnementales prévues)

- Si Oui : voir *Cotation* ci-dessous
- Si Non : l'évaluation a-t-elle démontré que les mesures environnementales sont abusives ou non réalistes ?
    - Si Oui : voir *Cotation* ci-dessous
    - SI Non : la vulnérabilité est considérée comme **non exploitable**

Cotation :

La vulnérabilité a-t-elle été cotée au-dessous de 13 points ?

- Si Oui, la vulnérabilité est considérée comme **exploitable** ;
- Si Non, elle est considérée comme **résiduelle.**