Mesures et incertitudes appliquée à la Cybersécurité — Act. Doc

Contexte

Vous êtes engagés dans un audit de sécurité pour une entreprise spécialisée dans la cybersécurité. Votre mission est d'évaluer la robustesse d'un pare-feu face à des attaques simulées ainsi que la fiabilité d'un système de cryptage. Pour ce faire, vous allez effectuer plusieurs mesures et calculer les incertitudes associées afin de garantir la précision de vos résultats.

Document 1 : Un audit de sécurité

Un audit de sécurité est un processus d'évaluation visant à vérifier la robustesse d'un système informatique face aux menaces potentielles, telles que les cyber-attaques, les intrusions ou les défaillances techniques. Il consiste à examiner les différents aspects de la sécurité d'un réseau, d'une application ou d'un système d'information, pour identifier les vulnérabilités, évaluer les risques et proposer des solutions d'amélioration.

Un audit de sécurité inclut des tests de performance, qui permettent de mesurer et d'analyser des paramètres clés. Parmi eux :

— Le temps de réponse : Il s'agit de mesurer la rapidité avec laquelle un système ou un dispositif (comme un pare-feu) réagit face à une attaque ou une requête. Un temps de réponse trop long peut laisser le système vulnérable, rendant ainsi l'audit crucial pour améliorer la réactivité.

— Le taux de détection : Ce test mesure la capacité d'un système de sécurité, tel qu'un logiciel de détection d'intrusion (IDS), à identifier les tentatives d'intrusion. Un taux de détection élevé indique que le système est efficace pour repérer les attaques, tandis qu'un taux faible met en lumière des faiblesses à combler.

— La vitesse de cryptage : Ce critère évalue la rapidité avec laquelle un système ou un algorithme chiffre les données. La vitesse de cryptage est cruciale pour maintenir un bon niveau de performance tout en assurant la sécurité des informations. Un algorithme de cryptage lent peut entraîner des délais importants dans le traitement des données, affectant ainsi l'efficacité globale du système. Il est donc important de trouver un équilibre entre la robustesse cryptographique et la performance pour garantir à la fois la sécurité et l'efficacité opérationnelle.

Ces tests sont essentiels pour garantir la fiabilité et la disponibilité des systèmes face aux menaces croissantes dans le domaine de la cybersécurité.

Document 2 : Résultat des différents tests

› Rapidité de réaction du dispositif pare-feu :

Essai	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Temps (ms)	50	52	51	53	49	50	51	52	50	53	49	52	50	51

Table 1 – Temps de réponse mesuré du pare-feu lors d'attaques simulées.

Objectif

☐ Calculer les incertitudes de type A et B sur des séries de mesures, et rédiger les résultats de mesurage.

Comprendre le contexte

Lecture sur la documentation

Q1 Expliquer pourquoi le temps de réponse d'un pare-feu est cruciale dans la cybersécurité.

Q2 Quelles pourraient être les sources de variabilité dans la mesure du temps de réponse lors d'une attaque simulée ?

Q3 Quel peut-être l'inconvénient d'un système de cryptage avec une robustesse cryptographique trop performante ?

Calcul d'incertitudes dans un audit de sécurité

Calcul de l'incertitude de type A

Q4 Calculer la moyenne arithmétique des temps de réponse (énoncés dans le document 2).

Q5 Calculer l'écart-type de ces mesures.

Q6 En déduire l'incertitude-type de type A.

Q7 Pourquoi devons nous utiliser les calculs de l'incertitude-type pour évaluer la robustesse d'un pare-feu ?

Méthode 1 : Écriture conventionnelle

On écrit un résultat de mesurage en suivant la méthode suivante :

- On utilise deux chiffres significatifs au maximum pour $u(x)$, en arrondissant par excès.
- Puis, on rédige la valeur expérimentale, sous la forme $x_{\text{exp}} = \ldots$ en précisant l'unité appropriée et l'incertitude-type associée à la valeur mesurée, sous la forme $u(x) = \ldots$, en utilisant la même puissance de 10 que celle de la valeur mesurée, et évidemment la même unité.

$$x_{\text{exp}} = \ldots ; \quad u(x) = \ldots$$

- Enfin, on adapte le nombre de chiffres significatifs de x_{exp} pour que la valeur ait le même nombre de décimales que $u(x)$.

Q8 Rédiger le résultat du mesurage du temps de réponse avec son incertitude-type élargie (au bon format) pour un intervalle de confiance de 95%.

Rappel

On note Δx, l'incertitude élargie liée au mesurage de la grandeur x.

- Pour un niveau de confiance de 68%, $\Delta x = \pm u(x)$: il y a 68% de chance pour que la valeur mesurée se trouve dans l'intervalle

$$[\bar{x} - u(x); \quad \bar{x} + u(x)].$$

- Pour un niveau de confiance de 95%, $\Delta x = \pm 2u(x)$: il y a 95% de chance pour que la valeur mesurée se trouve dans l'intervalle

$$[\bar{x} - 2u(x); \quad \bar{x} + 2u(x)].$$

Calcul de l'incertitude de type B

Document 3 : Système de cryptage

- Nom du Cryptosystème : CyberSecureX
- Type de Cryptage : Symétrique
- Algorithme Utilisé : AES (Advanced Encryption Standard)
- Clé : 256 bits
- Vitesse de Cryptage : 500 Mbits/s (précision ± 2%)
- Mode de Fonctionnement : CBC (Cipher Block Chaining)
- Niveau de Sécurité : Très Élevé
- Plateformes Supportées : Windows, Linux, macOS

Q9 Quelle est la vitesse de cryptage de CryptoSecureX ?

Q10 Calculer la valeur de la demie-étendue liée aux données du document 3.

Q11 Calculer l'incertitude de type B liée à la précision du constructeur.

Q12 Rédiger le résultat du mesurage de la vitesse de cryptage avec son incertitude-type élargie pour un intervalle de confiance de 95% (Voir méthode 1).

Q13 Faites de même pour une incertitude-type élargie pour un intervalle de confiance de 68%.

Après les tests

Justesse du mesurage

Document 4 : Résultats de l'audit sur la vitesse de cryptage

Les résultats d'un audit précédent son décrits dans le tableau ci-dessous.

Paramètre	Valeur Mesurée	Valeur de Référence	Incertitude-Type
Vitesse de Cryptage	500 Mb/s	495 Mb/s	5 Mb/s

Table 1 – Résultats de l'audit pour la vitesse de cryptage.

Q14 Rappeler la définition d'un mesurage juste.

Q15 Calculer le z-score pour vérifier la compatibilité de la mesure avec la valeur de référence.

Q16 Le résultat du mesurage est-il compatible avec la valeur de référence ? Justifiez.

Fidélité du mesurage

Q17 Rappeler la définition d'un mesurage fidèle.

Q18 Le résultat du mesurage présenté dans le document 4 est-il fidèle ?

Compatibilité entre deux systèmes

Document 5 : Deux systèmes IDS équivalents ?

Système	Temps de Réponse Mesuré	Incertitude-Type
Système A	52 ms	1.2 ms
Système B	55 ms	1.5 ms

Table 1 – Temps de réponse mesurés pour les systèmes de détection d'intrusion.

Q19 Calculer l'écart normalisé entre les temps de réponses des deux systèmes et conclure sur la comptabilité des deux systèmes.

Document 6 : Comparaison des deux systèmes IDS sur d'autres critères

Critère	Système A	Système B
Taux de Détection des Attaques	98%	85%
Nombre d'Incidents Non Détectés	2	15
Facilité de Mise à Jour	Moyenne	Élevée
Taux de Faux Positifs	5%	2%

Table 1 – Comparaison des performances entre les systèmes A et B en termes de cryptosécurité sur une simulation de 92 attaques

Q20 Calculer le pourcentage de d'incident non détectés pour chaque système.

Q21 Qu'est ce qu'un test "faux positif" ?

Q22 Pour conclure cet audit de sécurité, vous êtes en charge de sélectionner le système de cryptosécurité le plus performant. Lequel choisissez vous ? Justifier.

Formulaire

— Moyenne arithmétique :

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

— Écart-type :

$$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2}$$

— Incertitude-type A :

$$u(x) = \frac{\sigma}{\sqrt{N}}$$

— Incertitude de type B :

$$u(x) = \frac{a}{\sqrt{3}}$$

— Z-score :

$$z = \frac{|x_{\text{exp}} - x_{\text{ref}}|}{u(x)}$$

— Écart normalisé :

$$E_n = \frac{|x_A - x_B|}{\sqrt{u(x_A)^2 + u(x_B)^2}}$$

— Incertitude-type relative :

$$U_{r\%} = \frac{u(x)}{x} \times 100$$