BAC PRO CIEL / TCIEL / DOCUMENT ÉLÈVE

S2 — Croiser les traces et vérifier une réduction

TC_CYB_03 · 3 h · Maquette isolée ou dossier fictif

Nom : _____ Binôme : _____ Date : _____

TA MISSION

Tu reprends la cartographie S1. Un service visible mérite d'être contrôlé. Tu dois distinguer faits et hypothèses, choisir une mesure proportionnée au besoin, puis vérifier son effet sans confondre changement, cause et identité.

Tu dois montrer une fiche de contrôle avec attendu écrit avant le test, résultat après et conclusion limitée aux preuves disponibles.

SUR TA TABLE / SÉCURITÉ

Périmètre S1 revalidé, scan avant/après préparé par le professeur, fiche et journaux fictifs. Aucun scan hors lab, aucune exploitation ni recherche de mot de passe.

Le professeur applique seul la mesure sur la cible partagée. Ne modifie jamais un service ou un filtrage de ta propre initiative. Si l'essai réel n'est pas prêt, utilise exclusivement le cas papier intégré.

Cible autorisée réelle : _____ Mode : ☐ réel ☐ traces fictives

COMMENCE ICI

Sur ta trace S1, choisis jusqu'à deux lignes utiles. Si une seule existe, conserve-la ; ne complète pas par invention.

Ligne et heure 1 : _____

Ligne et heure 2, si disponible : _____

Écris une conclusion que ces lignes ne permettent pas encore d'établir.

ÉTAPE 1 — LIRE LES JOURNAUX SANS INVENTER

Dossier entièrement fictif. APP-A, 18/05/2026, UTC. Les heures des deux extraits ont été alignées pour cet exercice ; dans une enquête réelle, cette synchronisation serait à vérifier. Les lignes sont simplifiées.

Journal d'authentification APP-A :

```
09:12:18 Failed password for admin from 203.0.113.40
09:14:03 Failed password for admin from 203.0.113.40
09:16:41 Failed password for admin from 203.0.113.40
09:18:55 Accepted password for admin from 203.0.113.40
```

Journal de service APP-A :

```
09:20:07 admin session opened
09:24:10 export status requested
```

1. Écris deux faits en citant l'heure et les mots utiles. Une authentification acceptée ne suffit pas à connaître la personne derrière un compte ou une adresse.

Fait 1 :

Fait 2 :

2. Propose une hypothèse plausible, puis une explication différente compatible avec ces mêmes lignes. Ni une attaque ni un vol de données ne sont établis par ces extraits seuls.

Hypothèse à contrôler :

Autre explication possible :

ÉTAPE 2 — RELIER LE CONTRÔLE À UN BESOIN

Besoin du dossier fictif : la page HTTP de suivi doit rester accessible depuis OBS-LAB. SSH est réservé au poste de maintenance. OBS-LAB est un poste utilisateur ; il ne doit pas pouvoir ouvrir SSH sur APP-A.

Scan fictif AVANT, depuis OBS-LAB, 10:05 UTC :

```
22/tcp open ssh OpenSSH 9.6
80/tcp open http nginx 1.24.0
```

Test applicatif AVANT, même poste, 10:06 UTC : page de suivi reçue, HTTP 200.

Le scan et les journaux n'ont pas le même point d'observation ni le même instant. Leur rapprochement guide une vérification ; il ne prouve pas l'auteur ou la cause d'un incident.

Mesures proposées dans ce scénario : A — couper tous les services ; B — limiter l'accès SSH au poste de maintenance tout en conservant HTTP ; C — ne rien changer parce que la page répond.

En réel, choisis uniquement parmi les mesures préparées et autorisées par le professeur ; les choix du dossier papier ne sont pas des commandes à exécuter.

Mesure retenue et besoin préservé — deux phrases :

Avant de lire l'après, écris ce que tu devrais observer depuis OBS-LAB pour SSH et pour la page HTTP.

Attendu SSH : _____

Attendu service témoin HTTP : _____

Un contrôle supplémentaire nécessaire côté poste de maintenance :

ÉTAPE 3 — COMPARER L'AVANT ET L'APRÈS

En réel : le professeur confirme l'application de la mesure ; relance uniquement la même commande nmap -sV sur la cible autorisée, depuis le même poste. Utilise le test applicatif préparé pour le service témoin. Aucun élargissement du scan.

En papier : après avoir écrit tes attendus, lis ces nouvelles preuves fictives. Filtrage préparé par le professeur dans le scénario ; aucune configuration réelle n'a été faite.

Scan APRÈS depuis OBS-LAB, 10:20 UTC :

```
22/tcp filtered ssh

80/tcp open http nginx 1.24.0
```

Test applicatif APRÈS, même poste, 10:21 UTC : page de suivi reçue, HTTP 200.

Test depuis MAINT-LAB, 10:22 UTC : connexion SSH au service autorisé réussie avec le compte de test du scénario. Aucun secret n'est fourni.

Résultat SSH réellement observé ou lu : _____

Résultat HTTP réellement observé ou lu : _____

Conclusion : la mesure respecte-t-elle les besoins testés ? Justifie en deux phrases et précise le mode réel ou papier.

Une limite de ce contrôle :

Rappel : filtered ne signifie pas que le service est arrêté. Une sortie Nmap ne garantit pas seule le bon fonctionnement applicatif. La réussite de ces tests ne démontre pas une sécurité absolue.

Avant le retour, vérifie les deux traces, puis sépare dans ta fiche attendu, résultat réellement lu et décision.

Coche ton premier choix avant l’appel. Après le retour et un nouvel essai, entoure ton choix actualisé sans effacer la première coche.

Repères de réussite

C04 — Interprétation

Ma comparaison décrit le changement entre les deux traces.

C04 — Fiche de test

Ma fiche relie attendu, résultat et conclusion du contrôle.

C04 — Interprétation

À construire : La comparaison manque ou contredit les deux traces.

Partiel : Un état est bien relevé, mais le passage de l’avant à l’après reste imprécis.

Conforme : La comparaison décrit exactement le changement, sans inventer sa cause.

Consolidé : Cette qualité se retrouve sur une autre comparaison effectivement examinée.

C04 — Fiche de test

À construire : Le lien attendu/résultat/conclusion manque ou contredit le contrôle.

Partiel : Le lien est amorcé, mais un élément manque ou reste imprécis.

Conforme : Le lien attendu/résultat/conclusion est cohérent et limité au contrôle.

Consolidé : Cette qualité se retrouve sur un autre contrôle effectivement examiné.

Le papier montre ton raisonnement, pas une manipulation réelle.

APPEL PROFESSEUR

Montre une comparaison et ta fiche attendu/résultat/conclusion. Explique ce qui reste une hypothèse. Chacun répond sans le partenaire ; garde ta première trace.

RETOUR ET NOUVEL ESSAI

Retour reçu — un point utile :

Ma correction sans effacer le premier essai ; si elle était juste, ce qui la confirme :

Nouveau cas fictif : le besoin exige de conserver la page HTTPS sur 443. Avant : 443/tcp open et page reçue. Après : 443/tcp filtered et page non accessible depuis le poste utilisateur autorisé. Le technicien dit : « Il y a moins de ports ouverts, donc la mesure est réussie. »

Es-tu d'accord ? Écris le fait déterminant, ta décision et le contrôle à refaire. Aucune modification à exécuter.

Fait déterminant :

Décision et contrôle suivant :

À RETENIR

Une mesure de sécurité doit répondre au besoin et préserver les services nécessaires. Une différence avant/après est une observation ; elle n'identifie pas à elle seule une personne ni la cause d'un incident.

Validation professeur — CYB03 S2 — croiser deux traces et réduire l'exposition

Critère observé / Ce que je montre	À construire	Partiel	Conforme	Consolidé
C04 — Les indicateurs de fonctionnement sont interprétés Ce que je montre : Je compare les deux traces datées et identifie exactement le changement observé.				
C04 — Les fiches de test ou d'intervention sont renseignées Ce que je montre : Ma fiche de test relie attendu, obtenu et décision suivante sans inventer un test joué.				

POUR TERMINER

Rends première trace, correction et nouvel essai. Le professeur gère la remise en état de la cible partagée ; note ce qui reste non exécuté. Au débrief : quel fait soutient ta décision ? Quelle hypothèse reste ouverte ?