BAC PRO CIEL / TCIEL / DOCUMENT ÉLÈVE

S1 — Cartographier une exposition autorisée

TC_CYB_03 · 3 h · Maquette isolée ou dossier fictif

Nom : _____ Binôme : _____ Date : _____

TA MISSION

Un service peut être visible sans être vulnérable. Tu dois relever ce que le contrôle montre, puis choisir une vérification utile sans dépasser le périmètre autorisé.

Tu apprends à distinguer hôte repéré, port ouvert et service identifié. Ta preuve individuelle sera une commande conforme et une ligne de résultat correctement interprétée.

SUR TA TABLE / SÉCURITÉ

Fiche, dossier de laboratoire remis par le professeur, Nmap déjà préparé si l'essai réel est autorisé. Aucune installation ni élévation de droits pendant l'activité.

Le professeur remplit ces trois champs après contrôle de la maquette. S'ils restent vides, travaille uniquement sur les traces fictives de la fiche.

PLAGE_LAB : _____

CIBLE_A : _____

CIBLE_B : _____

Découverte : nmap -sn suivi de la plage validée. Services : nmap -sV suivi d'une seule cible validée. Remplace les noms de champs par les valeurs fournies ; ne saisis pas de chevrons.

Interdit : toute autre adresse, réseau du lycée, Internet, appareil personnel ; options -A, -sC, -p- ; exploitation, recherche de mots de passe ou déni de service. En cas de doute : STOP avant Entrée, puis appel professeur.

COMMENCE ICI

Sans lancer de commande : un hôte repéré et un port ouvert donnent-ils la même information ? Écris une phrase.

REPÈRE VISUEL — LE PÉRIMÈTRE

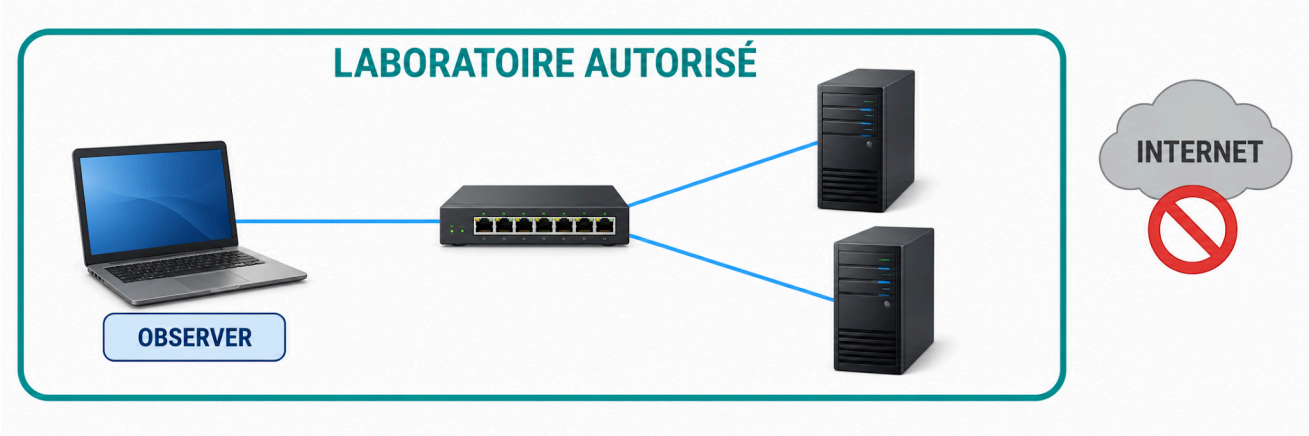


Illustration conceptuelle générée par IA : un poste observe deux cibles via un commutateur, dans un laboratoire isolé. Ce n'est ni le plan de B12 ni une preuve de connexion réelle. L'adresse d'un exemple papier ne devient jamais une cible autorisée.

ÉTAPE 1 — DÉCOUVRIR DANS LE BON PÉRIMÈTRE

Repère : -sn recherche les hôtes qui répondent aux sondes de découverte, sans poursuivre par un scan de ports. L'absence de réponse ne prouve pas qu'un appareil n'existe pas : le contrôle peut être bloqué ou inadapté.

1. Recopie la commande de découverte avec la plage fournie. Fais vérifier la cible par ton binôme puis par le professeur avant le premier lancement.

Commande prévue : _____

2. Si le lab est autorisé, exécute cette commande et conserve sa sortie avec l'heure. Si le lab est indisponible, lis le dossier fictif ci-dessous sans exécuter ses adresses.

Mode utilisé : ☐ essai réel autorisé ☐ analyse de traces fictives

Nombre d'hôtes signalés actifs : _____

Une adresse non prévue apparaît : ne la caractérise pas ; signale-la au professeur.

DOSSIER FICTIF — LECTURE SEULE, AUCUNE COMMANDE À EXÉCUTER

Extrait pédagogique simplifié de découverte, poste OBS-LAB, 10:00 UTC. Adresses réservées à la documentation ; aucune mesure de B12.

```
Nmap scan report for APP-A (192.0.2.20)
Host is up.
Nmap scan report for APP-B (192.0.2.30)
Host is up.
Nmap done: 8 IP addresses (2 hosts up) scanned.
```

Que peux-tu affirmer à propos des autres adresses ? Écris une limite en une phrase.

ÉTAPE 2 — LIRE PORT, ÉTAT, SERVICE ET VERSION

Un port TCP open indique qu'une application accepte des connexions sur ce port au moment et depuis le point du contrôle. Cela ne prouve ni l'usage complet du service, ni une vulnérabilité, ni une attaque.

Avec -sV, Nmap tente d'identifier le service et sa version par des sondes. Une étiquette SERVICE peut aussi venir d'une association habituelle au numéro de port ; ne la transforme pas en certitude si l'identification reste incertaine. Une case VERSION vide n'est pas une version « à jour ».

1. Choisis CIBLE_A ou CIBLE_B selon la consigne. Prévois la commande nmap -sV suivie de cette seule adresse. Si le lab est prêt, lance-la et conserve la sortie. Sinon utilise l'extrait fictif suivant.

Extrait fictif APP-A, même point de contrôle, 10:05 UTC :

```
PORT    STATE     SERVICE    VERSION
22/tcp  open      ssh        OpenSSH 9.6
80/tcp  open      http       nginx 1.24.0
443/tcp filtered  https
```

La dernière ligne ne prouve pas qu'un service HTTPS fonctionne : filtered signifie que Nmap ne peut pas déterminer si le port est ouvert à cause d'un filtrage ou d'un obstacle réseau.

2. Choisis deux lignes de ta sortie. Pour chacune, recopie port/état/service/version éventuelle puis formule ce que tu peux affirmer. Si la sortie réelle contient moins de deux lignes utiles, n'en invente pas : le professeur complète avec une trace fictive clairement marquée.

Ligne 1 — relevé exact : _____

Fait observable, en une phrase :

Ligne 2 — relevé exact : _____

Fait observable, en une phrase :

Une information que ces lignes ne prouvent pas :

ÉTAPE 3 — CHOISIR LA VÉRIFICATION SUIVANTE

Le dossier fictif indique que la page HTTP doit être accessible depuis OBS-LAB. L'administration SSH doit être réservée à un poste de maintenance distinct. Aucun besoin HTTPS n'est établi dans cet extrait.

En réel, utilise les besoins du dossier validé par le professeur. Choisis un service et propose une vérification liée à son utilité. N'exécute aucune commande supplémentaire sans consigne ; ne recherche pas d'exploitation.

Service choisi : _____

Besoin ou règle du dossier :

Question encore ouverte et contrôle proposé, en deux phrases :

SI TU BLOQUES

Aide 1 : retrouve le périmètre et l'en-tête des colonnes. Aide 2 : sépare ce qui est écrit de ce que tu supposes. Aide 3 : fais expliquer une autre ligne au professeur, puis reprends ta propre ligne sans modèle.

AVANT L'APPEL

Vérifie la cible et les options de la commande autorisée. Choisis une ligne de sortie et explique ce qu'elle montre, puis une conclusion qu'elle ne permet pas. Si tu as travaillé sur papier, dis-le : l'exécution n'a pas été réalisée.

APPEL PROFESSEUR

Montre ta commande et une ligne interprétée. Si tu travailles sur papier, précise-le. Chacun répond sans son binôme ; pendant l'attente, vérifie la limite de ta conclusion.

RETOUR ET NOUVEL ESSAI

Retour reçu — un point utile :

Ma correction sans effacer mon premier essai ; s'il était juste, ce qui le confirme :

Nouveau cas fictif : une sortie de détection indique « 8080/tcp open http nginx 1.24.0 ». Écris un fait, une conclusion que tu refuses d'affirmer et une vérification utile si le dossier exige une page de suivi accessible. Aucune commande à exécuter.

Fait :

Limite :

Vérification suivante :

À RETENIR

Périmètre vérifié → observation datée → interprétation bornée → prochaine vérification. Un port ouvert ne suffit pas à conclure à une faille. Une absence de ligne n'est pas un contrôle de tous les ports : la commande de base ne les examine pas tous.

POUR TERMINER

Conserve la première trace, le retour et le nouvel essai. Range le poste sans changer la maquette. Au débrief, explique une différence entre découvrir un hôte et identifier un service.

Sources : documentation officielle Nmap, découverte, états de ports et détection de versions, consultée le 10/10/2026. Les extraits de cette fiche sont fictifs et simplifiés.

Validation professeur — CYB03 S1 — cartographier une exposition

Critère observé / Ce que je montre	À construire	Partiel	Conforme	Consolidé
C04 — Les indicateurs de fonctionnement sont interprétés Ce que je montre : Je cite le port et le service observés, distingue visibilité et vulnérabilité, puis choisis une vérification ciblée.				