Diploma Programme
Programme du diplôme
Programa del Diploma

# Informatique
# Étude de cas : Le piratage éthique

A utiliser en mai et novembre 2026

---

**Instructions destinées aux élèves**

- Ce livret d'étude de cas est indispensable pour l'épreuve 3 du niveau supérieur.

5526 – 4411


8 pages

## Scénario

*CyberHealth Security* est une société se spécialisant dans l'analyse en cybersécurité. Une de ses équipes a récemment été chargée d'examiner les systèmes de cybersécurité de l'hôpital *MedTechPro* (*MTPH*), qui est fortement tributaire de la technologie, en particulier concernant les dossiers médicaux électroniques (en anglais EHR, acronyme de *electronic health record*), la communication interne et les dispositifs médicaux IdO (Internet des Objets).

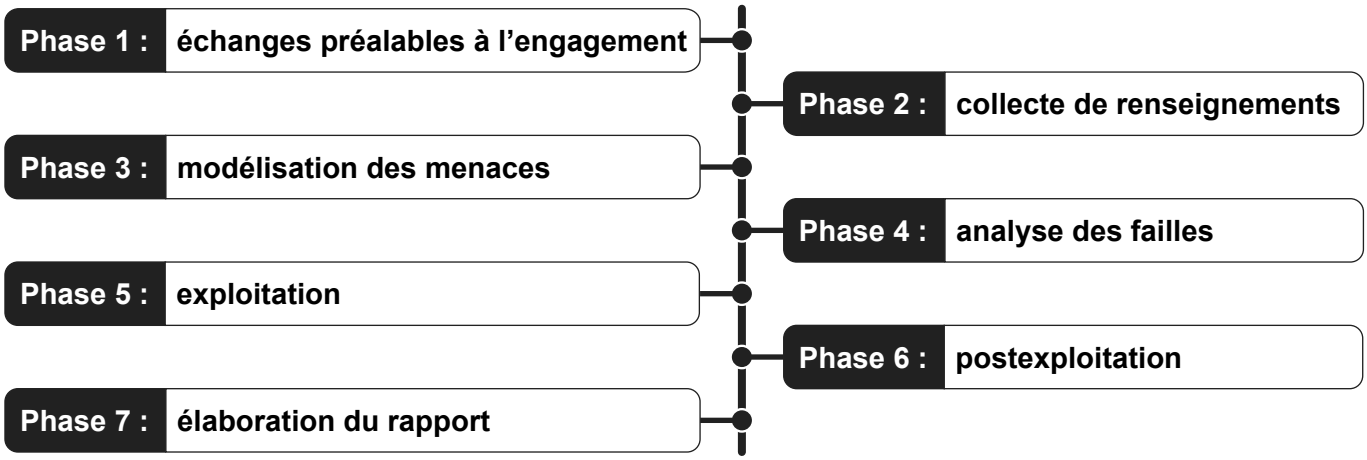
## Problèmes à résoudre

La mission de l'équipe de *CyberHealth Security* est d'effectuer des *tests d'intrusion* approfondis afin de découvrir toutes les failles du réseau de l'hôpital. L'équipe devra parcourir ce réseau en évaluant la sécurité du système ainsi que la confidentialité des données des patients dans tous les services du *MTPH*. Pour ce faire, elle adoptera le standard PTES (acronyme anglais de *penetration testing execution standard*).

## Le standard PTES

Le standard PTES fournit un cadre complet conçu pour apporter une méthode structurée de réalisation des tests d'intrusion et de communication des résultats. Le standard PTES est composé de sept phases (voir **figure 1**).

**Figure 1 : les sept phases de la méthode PTES**




1. **Échanges préalables à l'engagement**. Le processus commence par la préparation, l'obtention de l'approbation des documents et la mise en place des outils nécessaires.
2. **Collecte de renseignements**. Les données, provenant de sources externes, notamment les réseaux sociaux et les registres officiels, sont analysées. Ce procédé relève du *renseignement d'origine source ouverte* (en anglais *OSINT*, acronyme de *open-source intelligence*).
3. **Modélisation des menaces**. On identifie les menaces et les failles potentielles, et élabore les stratégies qui les atténuent.
4. **Analyse des failles.** On identifie et confirme les failles pouvant être exploitées par un·e *pirate informatique*.
5. **Exploitation**. On fait une tentative d'intrusion dans le système au moyen des failles préalablement identifiées et confirmées.
6. **Postexploitation**. Si l'accès au système a été obtenu, la priorité passe au maintien du contrôle du système et à l'extraction de ses données.
7. **Élaboration du rapport**. Le processus entier des tests est consigné et les résultats sont présentés dans un rapport au client.

## Phase 1 : échanges préalables à l'engagement

Dans cette phase, l'équipe de *CyberHealth Security* collabore avec le *MTPH* afin de définir les objectifs des tests d'intrusion, l'envergure du projet, les règles d'engagement, les outils de *test* et de logistique, et le calendrier global. Ce processus collaboratif est primordial pour assurer l'adéquation des tests avec les besoins opérationnels et les préoccupations en matière de sécurité de l'hôpital, tout en restant conformes aux normes éthiques professionnelles, au regard notamment de la nature sensible des données médicales.

### Établissement des objectifs et identification des cibles

- On établit des objectifs précis pour les tests, après avoir identifié les préoccupations principales du *MTPH*. Ces dernières peuvent comprendre l'intégrité des données des patients, la non-interruption des services et la conformité avec les réglementations du secteur de la santé.
- On identifie des cibles concrètes dans le réseau de l'hôpital. On détermine les éléments à haut risque qui demandent une attention particulière, comme les bases de données des dossiers des patients ou les dispositifs médicaux IdO.

### Définition du périmètre du test et des règles d'engagement

- Afin d'éviter une perturbation non intentionnelle des activités essentielles de l'hôpital, on confirme les limites des tests, ce qui inclut les systèmes faisant l'objet des tests et les limites des tests proprement dits.
- On met en place les règles d'engagement, afin que l'équipe de *CyberHealth Security* et les administrateurs du *MTPH* aient une bonne compréhension des méthodes utilisées et de l'ampleur des tests d'intrusion.

### Techniques de test

L'équipe de *CyberHealth Security* doit prendre en considération les implications des trois techniques de test suivantes : *boîte noire*, *boîte blanche* et *boîte grise*, et évaluer les risques et avantages potentiels de chacune dans un environnement de santé.

- **Tests boîte noire**. Avec cette technique, l'équipe simule une attaque par un·e pirate informatique externe et sans connaissance des systèmes de l'hôpital et étudie les failles immédiatement apparentes.
- **Tests boîte blanche**. Avec cette technique, l'équipe réalise une analyse approfondie grâce à une parfaite connaissance de l'infrastructure informatique de l'hôpital. Ceci implique l'accès aux diagrammes de réseau, aux configurations du système et aux failles connues.
- **Tests boîte grise**. Cette technique, étant un mélange de tests boîte blanche et boîte noire, utilise une connaissance partielle des systèmes de l'hôpital, comme dans le cas d'une menace interne ou d'un·e pirate informatique ayant obtenu des informations confidentielles.

**Tournez la page**

## Phase 2 : collecte de renseignements

Cette phase consiste à recueillir toutes les données publiques disponibles sur le *MTPH* afin d'identifier les failles potentielles. L'équipe de *CyberHealth Security* emploie plusieurs techniques OSINT à l'aide d'outils et de sources comme les moteurs de recherche, les réseaux sociaux, les forums et autres ressources accessibles par Internet pour recueillir des données exploitables concernant l'empreinte numérique de l'hôpital. Ces données vont permettre à l'équipe de créer une carte de la présence externe de l'hôpital qui sera utilisée pour découvrir les vulnérabilités susceptibles d'être exploitées.

Des exemples de données que l'équipe peut recueillir à l'aide de techniques OSINT comprennent :

- **Les informations sur les employés**. Obtenues au moyen d'une analyse de la présence du personnel dans les réseaux sociaux, en particulier les employés des services informatiques et administratifs.
- **L'utilisation de la technologie**. Connaissances des solutions matérielles et logicielles de l'hôpital publiquement accessibles.
- **Les politiques de sécurité**. Examen des politiques et des procédures de sécurité de l'établissement accessibles au public.

L'équipe de *CyberHealth Security* a également l'intention d'utiliser d'autres techniques de reconnaissance pour approfondir sa compréhension du réseau du *MTPH* :

- **Collecte de données ciblées**. L'équipe utilise des techniques avancées de recherche, comme le *dorking*, pour trouver les fichiers sensibles ou les portails de connexion vulnérables.
- ***Balayage réseau* et *cartographie réseau***. L'équipe utilise des outils avancés de cartographie réseau pour identifier les *topologies de réseau*, comme les serveurs internes et externes, les pare-feu et d'autres périphériques réseau. Les activités principales de balayage et de cartographie réseau comprennent notamment l'*analyse de ports*, la *détection des systèmes d'exploitation* et la cartographie des topologies réseau. Pendant le balayage et la cartographie réseau, les *adresses IP* de tous les périphériques du réseau de l'hôpital sont cataloguées afin de bien appréhender l'étendue du réseau.
- **Reconnaissance de l'ingénierie sociale**. L'équipe utilise l'*hameçonnage vocal* ou le *faux-semblant* pour obtenir des employés des informations qui pourraient faciliter les tests d'intrusion.

La phase de collecte de renseignements aide l'équipe à réaliser l'*évaluation de la posture de sécurité* de l'hôpital d'un point de vue externe, ce qui permet de cerner la manière d'aborder les tests d'intrusion.

## Phase 3 : modélisation des menaces

Dans cette phase, l'équipe de *CyberHealth Security* effectue une analyse détaillée des menaces en matière de cybersécurité du *MTPH*. Le processus comporte :

1. **L'identification des personnes antagonistes potentielles**. L'équipe détermine les personnes qui pourraient cibler l'hôpital, par exemple des cybercriminel·les à la recherche de données de patients pour en profiter financièrement, ou des personnes internes qui ont accès au réseau.
2. **L'évaluation des capacités et des intentions des pirates informatiques**. L'équipe analyse de quoi les personnes antagonistes potentielles sont capables et la manière dont elles ont l'intention d'utiliser les données ou les systèmes auxquels elles ont accédé.
3. **Les méthodes d'exploitation**. L'équipe recense les façons dont les failles peuvent être exploitées, par exemple le déploiement de *logiciels malveillants*, les *attaques d'ingénierie sociale* et les attaques de réseau.
4. **L'évaluation des actifs de valeur**. L'équipe détermine les actifs qui sont les plus essentiels à l'hôpital, par exemple les EHR, et évalue les conséquences potentielles de leur compromission.
5. **La hiérarchisation des efforts en matière de sécurité**. L'équipe utilise l'analyse susmentionnée pour orienter les tests d'intrusion afin que l'accent soit mis sur les éléments les plus importants et les plus vulnérables.

Cette approche structurée permet d'adapter efficacement les stratégies de tests d'intrusion afin qu'elles soient en adéquation avec le contexte de menaces particulier à l'hôpital.

## Phase 4 : analyse des failles

Dans cette phase, l'équipe de *CyberHealth Security* se sert d'outils automatisés ainsi que de techniques manuelles pour réaliser une analyse complète des failles du réseau du *MTPH*. Ce processus comporte :

1. **Le scannage des failles**. Afin d'identifier rapidement les failles connues sur tout le réseau comme les logiciels non corrigés et les configurations non sécurisées, l'équipe utilise des outils automatisés.
2. **L'examen manuel**. Pour détecter les défauts de sécurité plus subtils ou les failles complexes demandant une analyse spécialisée, l'équipe ajoute des contrôles manuels aux recherches automatisées.
3. **L'évaluation des faiblesses**. L'équipe évalue les failles identifiées pour en comprendre les conséquences potentielles ainsi que la manière dont les pirates informatiques pourraient les exploiter.
4. **La hiérarchisation**. L'équipe détermine les failles les plus dangereuses en fonction de facteurs comme la facilité d'exploitation ou le préjudice potentiel porté aux activités de l'hôpital et à la sécurité des patients.

Le résultat de cette analyse est crucial pour déterminer les étapes suivantes des tests d'intrusion en permettant à l'équipe de se concentrer sur les lacunes en matière de sécurité les plus importantes.

## Phase 5 : exploitation

Une fois que l'équipe de *CyberHealth Security* a identifié les failles du réseau du *MTPH*, elle commence la phase d'exploitation. Cette étape essentielle prend en considération les points suivants :

- **Les tentatives d'intrusion ciblées**. L'équipe utilise des techniques spécifiques pour exploiter les failles identifiées et tester les défenses de l'hôpital.
- **Le *développement de codes d'exploitation***. L'équipe développe des scripts ou des outils personnalisés adaptés spécifiquement aux failles identifiées dans le réseau de l'hôpital.
- **L'utilisation de diverses techniques**. En fonction des failles, l'équipe utilise certaines ou toutes les techniques possibles, notamment l'*injection SQL*, l'*injection de code indirecte* (en anglais *X-SS*, acronyme de *cross-site scripting*), les *attaques par dépassement de mémoire tampon*, et les *outils de craquage de mot de passe*.
- **L'évaluation des conséquences**. L'équipe cherche à comprendre le préjudice ou l'accès qui peut résulter d'une exploitation réussie, ce qui est essentiel pour évaluer la résilience de la sécurité de l'hôpital.

Cette phase est fondamentale pour démontrer comment les pirates informatiques peuvent exploiter les faiblesses et permettre à l'équipe d'élaborer des stratégies de défense.

## Phase 6 : postexploitation

Dans cette phase, l'équipe de *CyberHealth Security* évalue les conséquences des failles exploitées du réseau du *MTPH*. Les activités principales comprennent :

- **L'accès aux données et leur analyse**. Après l'intrusion, l'équipe étudie les types de données sensibles accessibles, par exemple les dossiers médicaux, les données administratives ou les informations confidentielles.
- **L'élévation des privilèges**. L'équipe examine dans quelle mesure on peut augmenter l'accès au sein du réseau en élevant les privilèges utilisateur.
- **L'établissement de la persistance**. L'équipe évalue les méthodes éventuellement employées par les pirates informatiques pour conserver un accès à long terme au réseau, ce qui est primordial pour comprendre la gravité d'une intrusion.
- **L'évaluation des répercussions opérationnelles**. L'équipe évalue les conséquences potentielles d'une intrusion sur les services hospitaliers et la sécurité des patients.
- **La *criminalistique informatique* et l'analyse des logiciels malveillants**. L'équipe analyse les traces laissées par l'exploitation en examinant les journaux système, en détectant les logiciels malveillants ou en identifiant les modifications apportées aux configurations du système.

Cette phase aide l'équipe à comprendre toute l'ampleur d'une cyberattaque et l'ensemble des conséquences pour l'hôpital.

## Phase 7 : élaboration du rapport

Dans la phase finale, l'équipe de *CyberHealth Security* compile un rapport complet sur les tests d'intrusion effectués au *MTPH*. Les éléments principaux de ce rapport comportent :

- **Un compte rendu détaillé sur les failles et les exploitations**. Ce compte rendu fait la synthèse des failles détectées, des méthodes utilisées pour les exploiter et des conséquences potentielles de chacune.
- **Des recommandations pragmatiques**. Le rapport dresse une liste de suggestions par ordre de priorité qui permettent de réduire les risques de sécurité identifiés et de renforcer les défenses de l'hôpital.
- **L'évaluation de la posture de sécurité**. Cette évaluation permet l'analyse globale des forces et des faiblesses de la cybersécurité de l'hôpital. Elle permet également de mettre en évidence les points à améliorer et ceux sur lesquels se concentrer à l'avenir.

Ce rapport permet à l'équipe informatique du *MTPH* d'élaborer un *plan d'intervention* qui comprend la détection des incidents, les stratégies d'intervention et les processus de reprise. Les efforts sont ainsi ciblés sur l'amélioration des mesures de cybersécurité, la réponse aux menaces et la protection de l'hôpital contre des menaces à venir.

## Considérations éthiques

Avant d'effectuer des tests d'intrusion sous quelque forme que ce soit, il est essentiel de réfléchir aux questions d'éthique, en particulier dans un environnement médical comme celui du *MTPH*. Cela comprend :

- l'obtention des autorisations nécessaires ;
- la confidentialité et l'intégrité des données ;
- la non-perturbation des services ;
- l'élaboration du rapport et la réactivité.

L'accent sur les considérations éthiques met en évidence la responsabilité qu'ont les professionnels de la cybersécurité de maintenir un juste équilibre entre la réalisation de tests méticuleux et la protection de l'institution et de ses parties prenantes.

## Défis rencontrés

Pour garantir la solidité du cadre de cybersécurité du *MTPH*, l'équipe de *CyberHealth Security* doit faire face aux défis suivants :

- évaluer les techniques de tests d'intrusion boîte noire, boîte blanche et boîte grise ;
- expliquer comment l'hôpital peut assurer la continuité des activités et protéger les données sensibles des patients tout en testant les failles ;
- étudier comment on peut utiliser le balayage et la cartographie réseau, ainsi que les outils OSINT pour découvrir les périphériques actifs et les informations concernant le réseau du *MTPH* ;
- établir un plan d'intervention qui englobe la détection des incidents, les stratégies d'intervention et les processus de reprise ;
- discuter des ramifications éthiques liées à la réalisation de tests d'intrusion au *MTPH*.

**Les candidat·es n'ont pas besoin de se documenter sur le fonctionnement des dispositifs médicaux, ni d'étudier la conformité juridique.**

**Tournez la page**

## Terminologie supplémentaire

Adresse IP (*IP address*)
Analyse de ports (*port scanning*)
Attaques d'ingénierie sociale (*social engineering attacks*)
Attaques par dépassement de mémoire tampon (*buffer overflow attacks*)
Balayage réseau (*network scanning*)
Cartographie réseau (*network mapping*)
Criminalistique informatique (s*ystem forensics*)
Détection des systèmes d'exploitation (*OS detection*)
Développement de codes d'exploitation (*exploit development*)
Dorking (*search engine dorking*)
Évaluation de la posture de sécurité (*security posture assessment*)
Faux-semblant (*pretexting*)
Hameçonnage vocal (*vishing [voice phishing]*)
Injection de code indirecte (*cross-site scripting [X-SS]*)
Injection SQL (*SQL injection*)
Logiciel malveillant (*malware*)
Outil de craquage de mot de passe (*password cracking tool*)
Pirate informatique (*hacker*)
Plan d'intervention (*response plan*)
Renseignement d'origine source ouverte (*open-source intelligence [OSINT]*)
Tests d'intrusion (*penetration testing*)
Tests (*testing*)
    Boîte blanche (*white box*)
    Boîte grise (*grey box*)
    Boîte noire (*black box*)
Topologie de réseau (*network topology*)

**Certains produits, sociétés et individus mentionnés dans cette étude de cas sont fictifs. Toute ressemblance avec des entités réelles ne saurait être que fortuite.**