Examen d'introduction à la Cybersécurité

Gaëtan Corin

La notation dépendra du détail apporté aux réponses. Le barème est indicatif. Les réponses devront être directement portées sur le présent document. Ce dernier est à déposer sur la boîte de livrable prévue à cet effet. Les réponses doivent être formulée en utilisant votre propre rédaction. Les documents sont autorisés. Toutes réponses recopiées pour tout ou partie d’une source extérieure ne seront pas prises en compte.

# Terminologie (4 points)

Donnez les définitions des termes suivants (~50 mots par définition) :

1. Bonnes pratiques

Les bonnes pratiques représentent l’ensemble des méthodes ou manière de faire permettant de minimiser le risque de failles ayant une forte vulnérabilité sur un système ou une application. Ces bonnes pratiques sont continuellement mises à jour, afin de toujours répondre aux besoins de la cybersécurité.

1. Sécurité

La sécurité représente la capacité d’une application ou un système à se montrer résilient aux différentes attaques. C’est en suivant une conception qui suit les bonnes pratiques de cybersécurité que le système peut se montrer sécurisé.

1. Risque

Le risque représente le calcul de l’ensemble des possibilités de failles ayant une vulnérabilité plus ou moins élevé qui peuvent avoir un impact sur la confidentialité, l’intégrité et/ou la disponibilité. C’est en calculant ce risque que l’on peut connaître le niveau de sécurité.

1. Contre-mesure

Les contre-mesures représente les actions correctives qui sont prisent à la suite de failles détectés qui sont considérés comme des vulnérabilités élevés. Il s’agit principalement de failles exploitables nécessitant une connaissance technique du système faible et/ou un besoin de domaine technique faible. La contre-mesure étant encore plus importante si cette faille a une vulnérabilité élevée sur les impacts de confidentialité, d’intégrité et/ou de disponibilité.

1. Vulnérabilité

La vulnérabilité représente la capacité d’un risque à être exploité. Plus les prérequis pour utiliser une faille sont faible, plus la vulnérabilité est considérée comme haute car à la portée de tous. La vulnérabilité est d’autant plus élevée si l’impact final est élevé.

1. Disponibilité

La disponibilité est un des impacts causés par des failles de système. Ce type d’impact représente la capacité d’un système ou une application à se montrer disponible et utilisable par les utilisateurs, à la suite d’une faille exploité.

1. Confidentialité

La confidentialité est un des impacts causés pour des failles de système. Ce type d’impact représente la capacité d’un système ou une application à divulguer des informations privées ou sensibles à des individus ne devant pas y avoir accès, à la suite d’une faille exploité.

1. Intégrité

L'intégrité est un des impacts causés pour des failles de système. Ce type d’impact représente la capacité d’un système ou une application à avoir des données qui sont modifiés ou corrompus, à la suite d’une faille exploité. Il peut aussi s’agir de pertes partiel ou intégral d’informations ne pouvant pas être récupérés par le système.

1. Faille

Une faille de sécurité représente l'ensemble des fonctionnalités d’un système pouvant devenir une potentielle vulnérabilité. Certaines failles de sécurité connus n’ont pas de contre-mesure, car la vulnérabilité n’est pas assez élevée.

1. Menace

La menace représente l’ensemble des impacts qui peuvent avoir lieu à la suite d’exploitation de failles. La menace est bien souvent proportionnelle à la vulnérabilité d’une faille.

# Hiérarchisation des critères de sécurité (2.5 points)

*Expliquer ce que sont les critères de sécurité et pourquoi il est nécessaire de les hiérarchiser en fonction du domaine d'application de la sécurité. (~100 mots)*

Les critères de sécurité représentent l’ensemble des méthodes qui doivent être appliqué pour que le système ou l’application soit considérés comme suffisamment sécurisé. Chaque système a un principe de hiérarchisation des critères de sécurité suivant le domaine dans lequel elle se trouve. Par exemple, une application bancaire aura des critères de sécurité bien plus élevé que le site internet du boulanger pâtissier.  
Il est donc nécessaire des hiérarchiser les critères de sécurité suivant la sensibilité des données recueillis par le système, ainsi que par l’impact qu’une faille exploité puisse avoir sur les utilisateurs ou le système.

# Menaces et risques (3 points)

1. *Quelles sont les difficultés rencontrées par les êtres humains qui peuvent amener à des menaces sur les systèmes d'information ? (~100 mots)*

Les difficultés rencontrées par les humains sont qu’ils ne sont pas toujours bien informés des risques. Chaque personne à son niveau de connaissance en termes de sécurité informatique, et un niveau de connaissance trop faible peu rendre la personne vulnérable a de nombreuses menaces sur les différents système et application qu’il utilise. Le meilleur moyen pour diminuer ce type de menaces est de réaliser de la prévention aux utilisateurs.

1. *Expliquer 2 méthodes d'attaque qui ciblent les humains pour exploiter leurs faiblesses et récupérer des informations. (~50 mots par méthode d'attaque)*

La première méthode d’attaque s’appelle le “phishing”. Il consiste à se faire passer pour l’entreprise ou le système par le biais d'email, sms ou fausse page internet, dans le but de récupérer des identifiants, mot de passe ou encore virement bancaire. Par la suite, l’accès utilisateur est corrompus et les hackers peuvent accéder aux informations privées ainsi qu’aux fonctionnalités destinés au propriétaire du compte.

La deuxième méthode d’attaque s’appelle le ”brute-force”. Les humains ont tendance à penser de la même manière. C’est pourquoi ils sont très mauvais pour inventer des mots de passe, car ils utilisent très souvent les mêmes sans le savoir.  
En récupérant une liste de mot de passe qui a déjà fuité, un hacker peut essayer de reliés des identifiant à des mots de passe sur un système, dans le but accéder et de corrompre des comptes utilisateurs.

# Dépassement de tampon, exécution et lecture arbitraire de code (8 points)

*Expliquer comment les entrées utilisateurs peuvent provoquer des erreurs d'exécution par dépassement de tampon et pourquoi ces erreurs sont nommées "erreurs de segmentation". (~150 mots)*

Lorsqu'un utilisateur insert de la donnée dans le système, à l’aide d’un input par exemple, cette donnée va être temporairement enregistrer dans ce que l’on appelle la “ mémoire tampon”.  
Il s’agit d’une zone de mémoire vive ou l’on va stocker temporairement des données, avant de transférer ces données vers un périphérique, ou de réécrire par-dessus.  
Cette mémoire tampon a une capacité de stockage limité. Lorsque le dépassement de capacité de stockage est atteint, les données supplémentaires se retrouvent stocké dans des zones mémoires adjacentes. On appelle cela un “buffer-overflow”.   
Cela est très problématique car le système réécrit du code arbitraire sur des fonctions système nécessaire à son bon fonctionnement.  
De plus, le système va essayer d’accéder à nouveau à cette zone mémoire, ce qui peut créer aux mieux des erreurs de segmentation, et aux pires des exécutions de code malveillants.  
  
Les erreurs de segmentation se produit lorsqu’un système essaye d’accéder à une zone de mémoire qui n’existe pas, auquel il n’a pas droit d’accès, ou bien qui est corrompus.

*Décrire le fonctionnement de l'attaque permettant de lire du code arbitrairement en exploitant une vulnérabilité de dépassement de tampon (~100 mots)*

En donnant intentionnellement une entrée utilisateur qui va dépasser la capacité de stockage du mémoire tampon, il est possible de réécrire du code arbitraire sur les zones mémoires adjacentes qui contiennent des fonctions systèmes.  
Si l'utilisateur écris dans cette entrée utilisateur des fonctions malveillantes consistant à lire des parties de code du système, et que ce code se retrouve dans une de ces zones mémoires adjacentes grâce aux buffer-overflow, alors le système devient corrompu.  
Il devient donc possible à l’utilisateur d’exécuter les fonctions qu’il a lui-même écris pour pouvoir lire les différentes parties de code du système. Cela représente une vulnérabilité très importante car un utilisateur malveillant qui a accès au code source augmente considérablement le risque de vulnérabilité causé par des exploitations de failles.

*Décrire le fonctionnement de l'attaque permettant d'exécuter du code arbitrairement en exploitant une vulnérabilité de dépassement de tampon (~100 mots)*

En utilisant le même principe d’attaque que lors de la réponse précédente, si l’utilisateur décide d’écrire des fonctions permettant de modifier des droits utilisateurs, de réaliser des exécutions dans la base de données, ou bien d’endommagé le système, et que ces fonctions se retrouve dans les zones mémoires adjacentes grâce aux buffer-overflow, alors le système devient corrompu, et peut exécuter ces fonctions durant son fonctionnement. En effet, le système n’a pas connaissance des modifications sur ces zones mémoires et va tenter d’exécuter le code précédemment effacé et réécris.

# Méthodes de cryptographie (2.5 points)

*Expliquer à l'aide d'un texte comment fonctionnent les chiffrements asymétrique et symétrique ainsi que les fonctions de hachage et les certificats (~50 mots pour chaque)*

Le chiffrement symétrique est un principe de chiffrement fonctionnant avec une clé unique.  
L’émetteur et le destinataire se partage la même clé, et c’est cette clé qui permet de chiffrer ainsi que déchiffrer le message ou l’information.

Le chiffrement asymétrique est un principe de chiffrement fonctionnant avec une deux types de clés.  
L’émetteur obtient la clé privée qu’il ne partage pas. C’est avec cette clé que le message sera chiffré.   
Il devra partager la clé publique avec le ou les destinataires du message. Ainsi, il est impossible pour un destinataire de se faire passer pour l’émetteur.

La fonction de hachage consiste à transformer une donnée d’entrée en un “hash”, qui consiste en une suite de caractère faisant constamment la même taille. Le principe du hash est qu’il est impossible à partir d’un hash de retrouvé la donnée d’entrée d’origine. En revanche, une donnée d’entrée identique donnera toujours le même hash. C’est donc un moyen privilégié pour conserver les mots de passe en base de données de manière sécurisé.

Le principe de certificat dans les méthodes de cryptographie fonctionne presque de la même manière que le chiffrement asymétrique.  
Nous retrouvons là aussi, une clé privé donné à l’émetteur et des clés publique données aux destinataires.  
La différence étant que la clé privée est soumise à un certificat prouvant l’authenticité de l’émetteur. Ainsi, le destinataire peut être sûr de la provenance du message.