PROJET TEST D'INTRUSION

Contenu

Informations pratiques

- Date de la soutenance : 07/12/2018
- Date limite de soumission des rapports et supports de présentation : 06/12/2018 à 23:59:59 (UTC+01:00). Retrait d'un point par heure de retard.
- Adresse mail de soumission :
  - Eric CARTER : eric.carter@c-s.fr
- Mail :
  - Objet du mail : PROJET ENSIIE – Groupe n°X
- Liste des livrables attendus :
  - Un rapport de test d'intrusion (DOC ou PDF) pour 3 des 4 VM ou un rapport par VM.
  - Un support de présentation (PPT ou PDF) présentant les travaux réalisés pour les tests d'intrusion.

Partie test d'intrusion

Détail du sujet

Réaliser un test d'intrusion sur trois des quatre machines virtuelles fournies dans le cadre du projet. L'objectif est de devenir admin/root. Il peut exister plusieurs façons d'y parvenir. Une fois root sur la machine vous pourrez récupérer le flag se trouvant généralement dans /root. Ce flag sera la preuve de preuve de votre réussite. Parfois le flag ne sera pas donné directement, et l'acquérir constituera la dernière étape de la machine virtuelle.

Il vous faudra ensuite retracer votre travail et vos résultats dans un rapport de test d'intrusion technique (DOC/PDF). Vous présenterez ensuite vos résultats oralement durant la soutenance (PPT/PDF).

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. Par exemple :

- Phrase technique : Il y a une XSS dans le champ login de la page d'accueil. On peut voler les cookies donc devenir administrateur. 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 petits changements au sein du code source de l'application sont à prévoir.

Critères d'évaluation

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

Annexe

Vulnérabilité et recommandation type

ID – Mineur/Majeur/Important/Critique	Titre de la vulnérabilité	Score CVSS 1-10
Description de la vulnérabilité et de son impact. Impact DICP : Elément concerné : **XXXXXX**		
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

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