Groupe 5 :

Mame Awa GUEYE

Zeinab Abibatou DIALLO

Pape Ibra NDIAYE

Cheikh Ahmeth Tidiane NDAW

Boubacar Bakary CAMARA

A09 : Echec de journalisation et de défaillance de la sécurité

1. Matching

- Mauvais encodage des données des fichiers logs : on peut utiliser le chiffrement pour chiffrer les fichiers logs et ainsi éviter les injections ou les attaques sur les systèmes de journalisation .(cf Chapitre 4 et 5)
- Les traces d'audit ,telles que les accès réussis ou échoués et les transactions sensibles :absence de trace dans le système concept de non répudiation non pris en charge (cf Chapitre 1,les services de sécurité)

2.**Exploration de la catégorie**

Les éléments importants à noter dans la catégorie 09 sont :

- Implication d'entretien pour vérifier si des attaques ont été détectées
- Aide à la détection et aux violations
- Présence de journalisation et de surveillance actives

Présentons ci-dessous les différents CWE et quelques CVE liés à ceux-ci.

CWE	CVE lies
CWE-117 : Neutralisation incorrecte de la sortie pour les journaux : le logiciel ne neutralise pas ou neutralise de manière incorrecte la sortie écrite dans les journaux	**CVE-2006-4624 :** injecter de fausses entrées de journal avec de faux horodatages à l'aide de l'injection CRLF
CWE-223 : Omission d'informations relatives à la sécurité : L'application n'enregistre ni n'affiche d'informations qui seraient importantes pour identifier la source ou la nature d'une attaque, ou pour déterminer si une action est sûre	**CVE-1999-1029 :** Les tentatives de connexion ne sont pas enregistrées si l'utilisateur se déconnecte avant le nombre maximal d'essais. **CVE-2002-1839 :** L'adresse IP de l'expéditeur n'est pas enregistrée dans les e-mails sortants. **CVE-2000-0542 :** L'échec de la tentative d'authentification n'est pas enregistré si la tentative ultérieure réussit.

CWE-532 : Insertion d'informations sensibles dans le fichier journal : Les informations écrites dans les fichiers journaux peuvent être de nature sensible et donner des conseils précieux à un attaquant ou exposer des informations utilisateur sensibles.	**CVE-2017-9615 :** la journalisation détaillée stocke les informations d'identification de l'administrateur dans un fichier journal lisible par le monde **CVE-2018-1999036 :** Mot de passe SSH pour la clé privée stockée dans le journal de construction
CWE-778 : Journalisation insuffisante : **Lorsqu'un** événement critique pour la sécurité se produit, le logiciel n'enregistre pas l'événement ou omet des détails importants sur l'événement lors de sa journalisation.	**CVE-2008-4315 :** le serveur n'enregistre pas les tentatives d'authentification échouées, ce qui permet aux attaquants de deviner plus facilement le mot de passe par force brute sans être détectés **CVE-2008-1203 :** l'interface d'administration n'enregistre pas les tentatives d'authentification échouées, ce qui permet aux attaquants de deviner plus facilement le mot de passe par force brute sans être détectés **CVE-2007-3730 :**la configuration par défaut du serveur POP n'enregistre pas l'adresse IP source ou le nom d'utilisateur pour les tentatives de connexion
	CVE-2007-1225 : le proxy n'enregistre pas les requêtes sans "http://" dans l'URL, permettant aux internautes d'accéder au contenu Web restreint sans détection **CVE-2003-1566 :** le serveur Web n'enregistre pas les demandes pour un type de demande non standard

3.Creation du scénario

Un attaquant accède au réseau interne d'une université. Il exécute un outil d'analyse pour localiser les systèmes internes présentant des vulnérabilités connues et obtient des données sensibles. Etant donné que l'université ne suit pas les pratiques de journalisation et de surveillance régulières, elle est incapable de détecter les attaques actives. La violation de données continue sans être détectée pendant des mois. Des milliers de données des étudiants ont été volés, les comptes de l'école vidés.

- **Scénario pour le CWE-532 :**

Imaginez que vous développez une application de commerce en ligne pour une entreprise. Lorsque les utilisateurs effectuent des achats dans l'application, vous enregistrez des informations sur leurs transactions dans un fichier de journal pour suivre les performances de l'application. Cependant, lors de l'enregistrement des transactions, vous n'avez pas mis en place de contrôle pour vérifier si les données sensibles des utilisateurs, telles que leur nom, leur adresse et leur numéro de carte de crédit, ont été correctement chiffrées. En conséquence, ces informations sensibles sont enregistrées dans le fichier de journal en clair, ce qui peut être exploité par des attaquants pour voler les données des utilisateurs.

- **Scénario pour le CWE-778**

Imaginez que vous développez une application de commerce électronique pour une entreprise en ligne. Lorsque les utilisateurs ajoutent des produits à leur panier et passent une commande, l'application enregistre les détails de la transaction dans un fichier journal pour suivre les ventes et les paiements. Si l'application ne journalise pas suffisamment d'informations, un attaquant pourrait utiliser des techniques de falsification d'adresse IP ou de masquage de l'identité pour passer des commandes frauduleuses et échapper à la détection

- **Scénario pour le CWE-223**

Imaginez que vous développez une application de gestion de projet pour une entreprise. Lorsque les utilisateurs créent des comptes et se connectent à l'application, l'application leur demande de choisir un nom d'utilisateur et un mot de passe. Si l'application omet de fournir des informations sur les exigences de sécurité pour les mots de passe, comme la longueur minimale ou la nécessité d'inclure des lettres, des chiffres et des symboles, les utilisateurs pourraient choisir des mots de passe faibles et facilement devinables

4.Outils pour illustrer

Il existe plusieurs outils utiles que les entreprises peuvent utiliser pour mettre en place un système de journalisation.

- **OWASP : AppSensor** c'est un projet open source qui intègre les mécanismes de journalisation avec les meilleures pratiques de sécurité pour fournir une détection d'intrusion dans la couche d'application en temps réel.

- **NLog :** solution de journalisation flexible et open source pour le traitement des événements et des alertes principalement utilisées pour les plateformes .NET

- **EvenLog Analyzer :** outil complet d'analyse et de suivi des journaux d'application qui collecte, analyse et corrèle les données de journal de toute application et fournit des informations utiles avec des rapports prédéfinis.

- **LogDNA** : fournit une solution complète d'analyse et de surveillance des journaux pour contrôler toutes les données des journaux et en tirer davantage de valeurs.

- **Logentries** : offre le moyen le plus rapide et le plus simple d'analyser et de surveiller vos données de journal. Il fournit des réponses en quelques minutes de recherche au lieu de vous faire attendre des configurations complexes.

5. Mesures cryptographiques préventives

- Assurez-vous que les données du journal sont correctement cryptées pour empêcher l'injection ou les attaques sur les systèmes de journalisation ou de surveillance.
- Assurez-vous que les transactions de grande valeur disposent d'une piste d'audit avec des contrôles d'intégrité pour empêcher la falsification ou la suppression, comme l'ajout de tables de base de données uniquement ou de transactions similaires.

- Les équipes DevSecOps doivent mettre en œuvre une surveillance et des alertes efficaces pour détecter et agir rapidement en cas d'activité suspecte.
- Automatiser la surveillance et les alertes pour les évènements de journal
- Effectuer toujours des tests de pénétration pour identifier les lacunes