Cyber - Spécifications Techniques

Responsable : **Julien Pavoni**

Protocoles de Cybersécurité

L'infrastructure de ce projet doit être entièrement indépendante de toute autre infrastructure pour des raisons de ségrégation des données. Elle doit être resilient et exploiter au maximum l'automatisation pour garantir un service à haute disponibilité et une récupération efficace. Elle doit être adaptée à un haut niveau de sécurité, pour des raisons de confidentialité.

Chiffrement des données avec TLS

Le protocole TLS est utilisé pour établir une connexion sécurisée entre deux parties (par exemple, un client et un serveur) pour garantir la confidentialité et l'intégrité des données échangées. Voici une description détaillée de la manière dont cela pourrait être mis en œuvre :

1. **Négociation du protocole :** Lorsqu'une connexion est établie, le client et le serveur négocient le protocole de chiffrement à utiliser. Cela comprend le choix de la version de TLS, des algorithmes de chiffrement, des algorithmes de hachage, etc.
2. **Échange de clés :** Une fois le protocole de chiffrement choisi, le client et le serveur échangent des clés publiques. Ces clés publiques sont utilisées pour établir une clé

de session partagée qui sera utilisée pour le chiffrement des données. Cette étape utilise généralement le protocole d'échange de clés Diffie-Hellman ou RSA.

3. **Chiffrement des données :** Une fois la clé de session établie, toutes les données échangées entre le client et le serveur sont chiffrées avec cette clé. Cela garantit que même si les données sont interceptées, elles ne peuvent pas être lues sans la clé de session.
4. **Vérification de l'intégrité des données :** En plus du chiffrement, TLS utilise également un algorithme de hachage pour garantir l'intégrité des données. Cela signifie que si les données sont modifiées pendant le transport, cela sera détecté lorsque les données seront déchiffrées.
5. **Fermeture de la connexion :** Une fois que toutes les données ont été échangées, la connexion est fermée de manière sécurisée. Cela implique généralement l'envoi d'un message de "fin de transmission" qui indique à l'autre partie que la connexion est sur le point d'être fermée.

Audits de Cybersécurité

Les audits de cybersécurité seront mis en œuvre pour assurer la robustesse et la résilience de l'infrastructure. Ces audits comprendront des tests d'intrusion, des vérifications de configuration et des évaluations d'architecture.
Il est essentiel que ces capteurs soient robustes, résilients, sûrs et surveillés.
Toutes les données collectées doivent être stockées dans une base de données et analysées, synthétisées et surveillées en direct via un tableau de bord. Les données inhabituelles doivent faire l'objet d'une alerte.

Audit d’intrusion

L'audit d'intrusion est une évaluation proactive de la sécurité du système d'information en simulant une attaque par un adversaire malveillant. Voici une approche détaillée de la manière dont nous pourrions procéder :

1. **Phase de reconnaissance :** Cette phase consiste à collecter autant d'informations que possible sur l'infrastructure cible. Cela peut inclure des informations sur les domaines, les sous-réseaux, les adresses IP, les enregistrements DNS, les courriels des employés, etc. Des outils comme Nmap, Wireshark, et Maltego peuvent être utilisés à cette étape.
2. **Phase de balayage :** Dans cette phase, nous identifions les services actifs, les ports ouverts/fermés, les systèmes d'exploitation et les applications logicielles utilisées. Des outils comme Nessus, Nexpose et OpenVAS peuvent être utilisés pour le balayage de vulnérabilités.
3. **Phase d'exploitation :** Ici, nous tentons d'exploiter les vulnérabilités identifiées lors de la phase de balayage. Cela peut impliquer l'utilisation de diverses techniques d'ingénierie sociale, d'attaques par force brute, d'attaques par injection SQL, etc. Des outils comme Metasploit, Burp Suite et SQLmap peuvent être utilisés à cette étape.
4. **Phase de post-exploitation :** Dans cette phase, nous tentons de maintenir l'accès au système et de collecter autant d'informations que possible. Cela peut impliquer l'escalade des privilèges, le pillage de données, la création de backdoors, etc.
5. **Phase de rapport :** Enfin, nous documentons toutes nos découvertes, y compris les vulnérabilités identifiées, les méthodes d'exploitation utilisées, les données compromises, et nous fournissons des recommandations pour remédier aux vulnérabilités identifiées.

Audit d’architecture

L'audit d'architecture vise à évaluer la conception et la configuration de l'infrastructure du système d'information. Voici une approche détaillée :

1. **Examen de l'architecture réseau :** Nous commencerons par examiner l'architecture réseau globale, y compris les pare-feu, les routeurs, les commutateurs, les serveurs, les dispositifs de stockage, etc. Nous vérifierons si les principes de moindre privilège et de séparation des devoirs sont respectés.
2. **Examen des contrôles de sécurité :** Nous examinerons ensuite les contrôles de sécurité en place, tels que l'authentification à deux facteurs, le chiffrement des données en transit et au repos, les contrôles d'accès basés sur les rôles, etc.

3. **Examen des politiques et procédures :** Nous examinerons également les politiques et procédures liées à la sécurité de l'information, telles que les politiques de gestion des changements, les politiques de sauvegarde et de restauration, les politiques de gestion des incidents, etc.
4. **Rapport :** Enfin, nous documenterons toutes nos découvertes et fournirons des recommandations pour améliorer l'architecture de sécurité.

Audit de configuration

L'audit de configuration vise à évaluer la manière dont les systèmes et les applications sont configurés. Voici une approche détaillée :

1. **Examen des configurations du système d'exploitation :** Nous examinerons les configurations du système d'exploitation, y compris les paramètres de sécurité, les correctifs installés, les services en cours d'exécution, etc. Des outils comme Microsoft Baseline Security Analyzer (pour les systèmes Windows) ou Lynis (pour les systèmes Linux) peuvent être utilisés.
2. **Examen des configurations des applications :** Nous examinerons ensuite les configurations des applications, y compris les paramètres de sécurité, les correctifs installés, les comptes d'utilisateurs, etc. Des outils comme OWASP ZAP ou Nessus peuvent être utilisés pour auditer les applications web.
3. **Examen des configurations réseau :** Nous examinerons également les configurations réseau, y compris les règles de pare-feu, les configurations de routeur, les configurations de commutateur, etc.
4. **Rapport :** Enfin, nous documenterons toutes nos découvertes et fournirons des recommandations pour améliorer les configurations de sécurité.