Analyse des rapports d’incidents - Répondre à un incident DDoS avec le cadre du NIST

Google Cybersecurity Certificate

Sommaire

L’entreprise a subi un événement de sécurité lorsque tous les services du réseau ont soudainement cessé de répondre pendant deux heures. L’équipe de cybersécurité a découvert que la perturbation avait été causée par une attaque de déni de service distribué (DDoS) via un afflux massif de paquets ICMP entrants. L’équipe a réagi en bloquant l’attaque et en arrêtant tous les services réseau non critiques afin de pouvoir restaurer les services réseau critiques.

Identifier

- **Type d’attaque** : Attaque DDoS par inondation ICMP.
- **Vulnérabilité exploitée** :Le pare-feu n’avait pas de règles en place pour limiter le nombre de paquets ICMP entrant provenant d’adresses IP inconnues, ce qui a permis un afflux massif de pings ICMP.
- **Systèmes concernés** : Les services Web, les bases de données, et l’accès aux ressources du réseau interne ont été touchés.
- **Impact** : Les services réseau de l’entreprise ont soudainement cessé de répondre en raison d’un afflux de paquets ICMP. Le trafic normal du réseau interne ne pouvait accéder à aucune ressource du réseau.

Protéger

L’équipe de cybersécurité a mis en place une nouvelle règle de pare-feu pour limiter le taux de paquets ICMP entrants et un système IDS/IPS pour filtrer une partie du trafic ICMP sur la base de caractéristiques suspectes.

- **Actions supplémentaires :**
    - Mise en place de règles de pare-feu avancées pour vérifier les adresses IP source afin de détecter les adresses IP suspectes.
    - Formation et sensibilisation des employés sur de meilleures pratiques de cybersécurité.
    - Utilisation de logiciels de surveillance du réseau pour détecter les schémas de trafic anormaux.
    - Configuration de la journalisation du pare-feu et des systèmes IDS/IPS pour enregistrer les événements et les utiliser pour l'analyse.

Détecter

L'équipe de cybersécurité a configuré la vérification de l'adresse IP source sur le pare-feu afin de détecter les adresses IP suspectes dans les paquets ICMP entrants et a mis en œuvre un logiciel de surveillance du réseau pour détecter les schémas de trafic anormaux.

- Implémentation d'un SIEM (Security Information and Event Management) pour centraliser et analyser les journaux de différents systèmes, facilitant ainsi la détection des anomalies.

Répondre

- **Plan de réponse** :
    - **Isolement des systèmes affectés** : Les systèmes affectés par l'attaque seront isolés du réseau pour empêcher la propagation de l'incident.
    - **Restauration des systèmes et services critiques** : Les services réseau critiques seront restaurés en priorité afin de rétablir les opérations essentielles.
    - **Analyse des logs** : Les journaux du réseau seront analysés pour identifier l'origine et l'ampleur de l'attaque, et pour identifier les éventuelles failles de sécurité.
    - **Communication et rapport** : Les incidents seront signalés à la direction générale et aux autorités juridiques compétentes, le cas échéant.

Récupérer

Pour se remettre d'une attaque DDoS par inondation ICMP, l'accès aux services du réseau doit être rétabli dans un état de fonctionnement normal.

Mesures de récupération :

- **Restauration des services critiques** : L'accès aux services réseau critiques sera rétabli dès que possible pour assurer la continuité des opérations.
- **Blocage des paquets ICMP suspects** : Des règles de pare-feu spécifiques seront mises en place pour bloquer les paquets ICMP provenant de sources malveillantes.
- **Mise en ligne des services non critiques** : Les services de réseau non critiques seront remis en ligne progressivement une fois que la situation est stabilisée.
- **Révision du processus de sécurité** : Les processus de sécurité seront révisés pour renforcer la résilience face à de futurs incidents similaires.

Réflexions/ Remarques

Dans cette analyse de rapport d'incident, nous avons appris quelques leçons :

- Importance de la configuration correcte des pare-feux.
- Nécessité de tester régulièrement les configurations de pare-feu pour s'assurer qu'elles sont efficaces.
- La surveillance continue du réseau est essentielle pour détecter les attaques et les anomalies.

Afin d'améliorer notre capacité à gérer de futurs incidents similaires, nous devrons mettre en place les améliorations suivantes :

- Renforcer les capacités de détection et de réponse aux incidents, notamment en investissant dans des outils de sécurité avancés.
- Mettre en place des formations régulières pour le personnel sur les meilleures pratiques de cybersécurité.
- Réaliser des audits réguliers des systèmes de sécurité pour identifier les vulnérabilités.