Incident analyse du rapport

Instructions

Au fur et à mesure que vous poursuivez ce cours, vous pouvez utiliser ce modèle pour enregistrer vos découvertes après avoir terminé une activité ou pour prendre des notes sur ce que vous avez appris sur un outil ou un concept spécifique. Vous pouvez également utiliser ce tableau pour vous entraîner à appliquer le cadre NIST aux différentes situations que vous rencontrez.

Résumé	Il a été informé au service informatique, par les utilisateurs, que les services du réseau interne étaient indisponibles. Le trafic normal du réseau interne ne pouvait accéder à aucune ressource du réseau. Les journaux ont montré un flux de paquets ICMP entrants. L'équipe de gestion des incidents a répondu en bloquant les paquets ICMP entrants, en mettant hors-ligne les services réseau non critiques et en rétablissant les services réseau critiques. Nous pensons qu'il peut s'agir d'une attaque DOS ou DDOS par inondation ICMP.
Identifier	L'équipe de sécurité a audité les appareils, systèmes et procédures impliqués dans cet incident. L'équipe a ensuite découvert qu'à travers un pare-feu mal configuré, un acteur malveillant a envoyé un flot de requêtes ping (ICMP) . Cette vulnérabilité a permis à l'attaquant de submerger le réseau de l'entreprise par le biais d'une attaque DDOS (Distributed Deny Of Service)
Protéger	Pour éviter la reproduction d'un pareil incident l'équipe a pris les mesures suivantes: une nouvelle règle de pare-feu les paquets ICMP entrants,des systèmes de détection/prévention d'intrusion (IDS/IPS)
Détecter	Pour détecter de nouvelles attaques de ce genre, l'équipe peut mettre en

	oeuvre une vérification de l'adresse IP source sur le pare-feu afin de détecter les adresses IP usurpées dans les paquet ICMP entrant pour filtrer une partie du trafic ICMP sur la base de caractéristiques suspectes et un logiciel de surveillance réseau pour détecter les trafics de schéma réseau.
Répondre	Une formation sera organisée pour les utilisateurs afin d'expliquer les meilleures pratiques en réponse ou préven.tion d'un incident de sécurité. Pour le futur, l'équipe tentera d'isoler le système perturber pour empêcher l'incident de se propager dans l'ensemble du réseau et analysera les journaux pour détecter toute activité malveillante. L'incident sera informé à la direction et aux utilisateurs pour mieux comprendre la raison de l'indisponibilité du réseau.
Récupérer	Pour récupérer d'une attaque DDOS, l'accès au service réseau doit retrouver son fonctionnement normal. A l'avenir les attaques par inondation ICMP seront prévenues au niveau du pare-feu, les services non critiques seront mis hors-service, pour alléger le trafic réseau interne et après l'attaque le réseau pourra retrouver son fonctionnement initial

---

Réflexions/Notes :