Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	L'entreprise a subi une attaque DDoS par inondation ICMP pendant 2 heures. L'attaque a paralysé notre réseau en saturant la bande passante via des paquets ICMP entrants massifs provenant d'adresses IP usurpées. L'origine était un pare-feu non configuré. Les services critiques de conception web et de gestion des médias sociaux sont devenus inaccessibles, causant des pertes financières estimées à 20K€ et reportant 3 contrats clients. L'équipe a répondu en bloquant le trafic ICMP, en arrêtant les services non essentiels, et en restaurant les services prioritaires.
Identify	**Type d'attaque** : DDoS volumétrique (couche réseau) par flood ICMP ("Ping Flood") **Systèmes affectés** : Pare-feu principal (non configuré), routeurs centraux ,serveurs web (Apache), plateforme CRM client, outils de création graphique (Adobe Creative Cloud) **Source de l'attaque** : Botnet utilisant des IPs usurpées (trafic distribué

	depuis 15 000 sources) **Impact critique** : Indisponibilité complète du réseau pendant 2h, perte de productivité équipe créative (20h-homme), report de 3 projets clients et atteinte à la réputation
Protect	**Plan d'amélioration de la protection** : 1. **Hardening du pare-feu** : a. Implémenter le rate-limiting ICMP (max 100 paquets/sec par IP) b. Activer le filtrage BCP 38 contre l'usurpation IP 2. **Architecture réseau** : a. Segmenter le réseau : VLAN séparés pour services clients/interne b. Déployer Anycast DNS (Cloudflare/Amazon Route 53) 3. **Formations critiques** : a. Atelier "Configurations sécurisées" pour l'équipe réseau b. Simulations trimestrielles d'attaque DDoS 4. **Protection avancée** : a. Souscrire à un service de mitigation DDoS (ex: Cloudflare Pro) b. Micro-segmentation cloud via groupes de sécurité AWS
Detect	**Stratégie de détection proactive** : 1. **Monitoring réseau** : a. Déploiement de NetFlow/sFlow pour analyse du trafic en temps réel

	b. Alertes automatiques sur pics ICMP > 10 000 paquets/seconde 2. **Outils spécialisés** : a. Mise en place d'un IDS/IPS (Suricata) avec règles spécifiques : i. `alert icmp any any -> $HOME_NET any (msg:"ETPRO ICMP Flood"; threshold: type both, track by_src, count 500, seconds 1;)` b. Intégration de feeds de threat intelligence (AlienVault OTX) 3. **Surveillance comportementale** : a. Dashboard Kibana pour visualiser : [Trafic ICMP] - [Top Sources] - [Anomalies géographiques] b. Honeypots réseau (déploiement T-Pot) pour leurrer les attaquants
Respond	**Plan de réponse aux incidents DDoS** : 1. **Containement (0-5 min)** : a. Activer le mode "Under Attack" du CDN b. Bloquer les AS malveillants via BGP Flowspec 2. **Neutralisation (5-30 min)** : a. Contacter le fournisseur de mitigation (NTT/Scaleway) b. Documenter l'attaque pour plainte (OCLCTIC/ANSSI) 3. **Analyse post-incident** : a. Capturer les PCAP pour investigation b. Reverse-engineering des payloads ICMP 4. **Communication de crise** : a. Notifier les clients via StatusPage.io

	b. Briefing technique aux partenaires sous 24h
Recover	**Plan de rétablissement** : 1. **Priorités de restauration** : a. Services clients (CRM/Site web) : RTO ≤ 30 min i. Basculer vers CDN avec cache d'urgence ii. Vérifier l'intégrité des données (checksum) b. Outils créatifs : RTO ≤ 1h i. Redémarrage séquentiel via Ansible 2. **Sauvegardes critiques** : a. RPO : 15 min (snapshots EBS automatisés) b. Scénarios de test de restauration mensuels 3. **Améliorations** : a. Auditer toutes les règles de sécurité trimestriellement b. Tests de pénétration réseau mensuels

---
