< EXERCICE DDOS >

FICHE EXERCICE

< EXERCICE DDOS >

DEFINITION

Une attaque de Déni de Service Distribué (DDoS) consiste en une surcharge d'une application (site web, API, etc.) par une multitude de requêtes, conduisant à un éventuel arrêt de fonctionnement de l'application.

Les attaques DDoS peuvent être effectuées de différentes manières et à différents niveaux de couches réseaux, conduisant à une possible complexité dans la gestion de ce type d'attaque. Ce genre d'attaque est fréquemment utilisée pour masquer d'autres attaques (Exfiltration de données, Espionnage).

OBJECTIFS

- Comprendre le contexte spécifique de scénarios d'attaques DDoS, et la nature des indisponibilités et impacts possibles (court et long terme, compromission associée) ;
- Comprendre les aspects techniques et les capacités de l'organisation à résister à ce type d'attaque ;
- Tester la solution de contournement pour s'assurer de la disponibilité de service ;
- Tester le canal de communication alternative si le site officiel d'organisation n'est pas disponible ;
- Tester la stratégie de reprise d'activité en mode dégradé ;
- Identifier les points forts ainsi que les axes d'amélioration des plans et processus de gestion de crise couvrant ce scénario.

DURÉE

Exercice souvent assez court (1 à 3h), les attaques DDoS durant généralement quelques heures.

PUBLIC VISÉ

Cellule décisionnelle : Comité de direction, dont Juridique, DPO, Communication, et les métiers concernés.
Cellules opérationnelles : Equipes représentées dans la cellule stratégique.
Externes : Prestataires et partenaires si le DDOS simulé sur un système externalisé

PRÉPARATION, RESSOURCES ET LOGISTIQUES

- Il est important de faire ressentir une pression interne et externe (médiatique, client, écosystème) au travers du scénario (appels clients, des mails, des SMS, etc.) ;
- Selon la maturité de l'organisation, des simulations techniques de DDoS peuvent être réalisées sur des sites (à arbitrer selon les besoins de continuité d'activité). Si des systèmes de production sont mobilisés, ces derniers doivent l'être sur des plages horaires moins critiques ;
- Des outils de communication alternatifs peuvent être mobilisés en cas de perte du SI de communication.

< EXERCICE DDOS >

IMPACTS

Internes :

- Pertes financières importantes (e.g. : indisponibilité d'un site e-commerce) ;
- Stress extrême dans le cas d'attaques sur des applications/sites (notamment secteurs nécessitant une forte disponibilité ou à haute sensibilité) ;
- Impact sur le travail des collaborateurs en cas de DDoS sur des applications internes.

Externes :

- Image/réputation (e.g.: indisponibilité d'un réseau social, parfois partielle – un site peut fonctionner pour un client et pas pour un autre) ;
- Impact opérationnels et financières pour les tierces dépendantes.

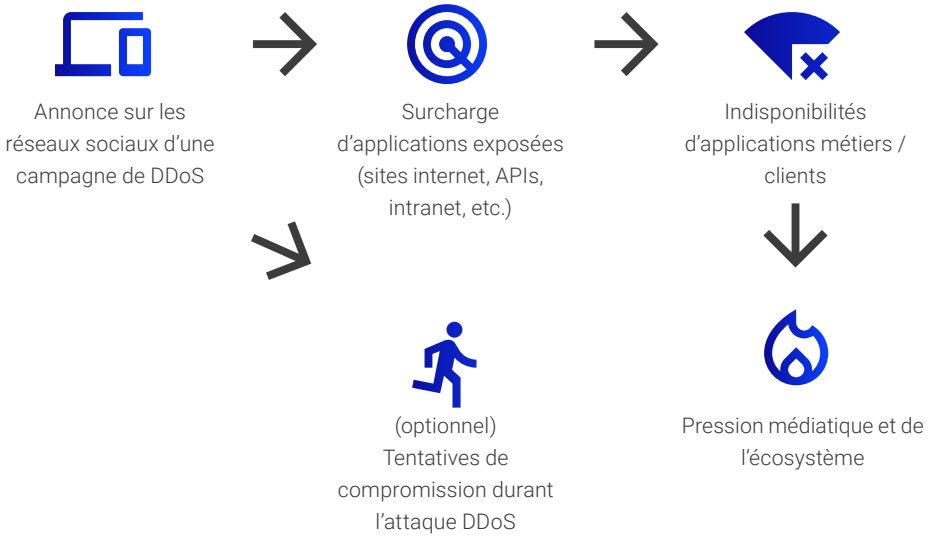
ÉLÉMENTS ÉVALUABLES

Evaluation :

- Temps de réponse à la crise ;
- Identification des solutions techniques pour résoudre une typologie d'attaque ;
- Identification des impacts financiers et réglementaires.
- Evaluation de la chaîne d'alerte, notamment dans le cas de l'implication d'un prestataire. ;
- Pression ressentie vis-à-vis de l'impact réel de l'attaque.
- Priorisation des applications métiers en cas d'attaques multiples ;
- Capacité de prise de recul sur d'autres attaques éventuelles, en identifiant des actions proactives à mettre en place pour réduire les impacts potentiels sur l'organisation.

EXEMPLE D'UNE ATTAQUE DDOS PAR UN ACTEUR HACKTIVISTE

Profil d'attaquants :
Etatique, hacktiviste, zone grise (ex: concurrence)



PHASES DE L'EXERCICE

1. Phase d'annonce d'une campagne de DDoS
2. Phase d'attaques, avec surcharge des applications visées :
   - Indisponibilité des sites
   - Pression des clients, des médias, des partenaires, etc.
3. Phase de défense face aux attaques
4. Ces phases d'attaque/défense sont susceptibles de se multiplier, les attaquants changeant de typologie d'attaques DDoS *(smurf, SYN flood, HTTP flood, etc.)* face aux actions de mitigation mises en place

< EXERCICE DDOS >

BÉNÉFICES ATTENDUS

- Evaluation de l'impact de ce type d'attaque sur le plan financier, réglementaire, notation client, etc ;
- Identification du seuil de service nécessaire permettant une reprise d'activité du site de l'organisation (approche préliminaire du Business Impact Analysis) ;
- Création d'un plan d'actions se reposant sur les résultats de cet exercice (notamment sur les services cibles du Business Impact Analysis) ;
- Evaluation du niveau de conformité vis-à-vis de certaines normes de continuité d'activités et gestion de crise (e.g. : ISO 22301, NIS2, DORA) ;
- Création de fiches réflexes (ou playbooks) traitant de ce scénario.

COMPÉTENCES DÉVELOPPÉES

- Capacité à se protéger des attaques, à la fois en termes de typologie (SYN flood, etc.) et en termes de volumétrie en relation avec la réalité des attaques actuelles ;
- Compétences pour réagir / mitiger l'attaque (notamment application des mesures techniques) ;
- Compétences de coordination et communication dans le contexte d'un scénario de «choc» (notamment pour les clients touchés par la perte de service, qui peut générer de la frustration / de la panique).

POSSIBLES DIFFICULTÉS ET BIAIS

- Il peut être difficile de mobiliser son prestataire de solutions de défense dans une approche de dépassement de sa solution de défense (le prestataire peut ne pas vouloir s'exposer) ;
- Des difficultés peuvent exister quant à l'évaluation exacte de la capacité précise à répondre à ce type d'attaque, sans réaliser une attaque sur la production en situation nominale ;
- Par ailleurs, il peut être difficile d'estimer la volumétrie précise d'une attaque DDoS sur un système de non-production. En effet, cela retire du jeu tout le trafic usuel d'un site fonctionnel et utilisé par les clients ;
- En cas de DDoS sur un SI assurant la communication de l'organisation, il peut être décidé (ou non) de simplifier en considérant que la communication fonctionne toujours ;
- Certaines campagnes de DDoS sur les organisations peuvent se matérialiser par des vagues d'attaques de quelques heures, réparties sur plusieurs jours. Ce type de campagne est difficilement reproductible dans un exercice.

VARIANTES

Débutant : Exercice sur table pour identifier des solutions techniques ainsi que les services alternatifs.
Intermédiaire : Simulation permettant de tester les alternatives évoquées dans les plans/processus de crise DDoS.
Confirmé : Simulation réelle sans préparation en amont. Cette variante testera principalement les flux de communication.

Contributeurs : Accenture, Airbus, ANSSI, BNP Paribas, Bouygues Telecom, Deloitte, ENEDIS, Française des Jeux, MACIF, Ministère de l'Intérieur et des Outre-Mer, Renault, SANOFI, Schneider Electric, SNCF, Technip Energies, Wavestone.

< Studio des Communs >

CAMPUS
CYBER

POUR EN SAVOIR PLUS : WIKI.CAMPUSCYBER.FR
MAIL : COMMUNAUTES@CAMPUSCYBER.FR / 5 - 7 RUE BELLINI 92800, PUTEAUX

FICHE EXERICE - DDOS