Le service DNS – Attaques et surveillance

Objectifs :

Comprendre le fonctionnement d'une cyberattaque impactant le service DNS.
Utiliser des outils présents dans le système pour assurer la surveillance de ce dernier et/ou palier à la saturation ou l'absence de service.

Prérequis :

Pour la réalisation de ce TP, vous aurez besoin d'un service DNS fonctionnel, employant un serveur principal et un serveur secondaire, il convient d'utiliser les serveurs gérant la zone bts.sio. créés lors du TP01, vous vérifierez le bon fonctionnement du service DNS avant de commencer ce TP02.
Un ou plusieurs clients seront potentiellement nécessaires pour simuler une attaque sur le service DNS.
Un client pourrait être nécessaire pour réaliser des tests.

Précautions :

Tout téléchargement d'application tierce sera effectué via une machine virtuelle, en aucun cas vous ne devez utiliser votre poste physique pour la récupération d'un logiciel tiers.
La simulation d'attaque sera effectuée envers un serveur DNS virtuel, dans un réseau interne à VirtualBox ou à votre pool de ressources ESXi.

Etapes :

1. Choisissez un type d'attaque que vous estimez réalisable dans le cadre de ce TP, munissez vous des outils nécessaires à sa mise en place. Vous pouvez réaliser vous-même des solutions permettant de simuler un certain type d'attaque.
2. Lorsque votre attaque est active, vérifiez le comportement de votre serveur, à l'aide d'un client, et à l'aide des journaux d'activités ou d'outils disponibles sur votre serveur.
3. En fonction des informations remontées, listez les solutions pouvant être mises en place pour assurer la sécurité de votre service DNS et/ou de votre serveur.