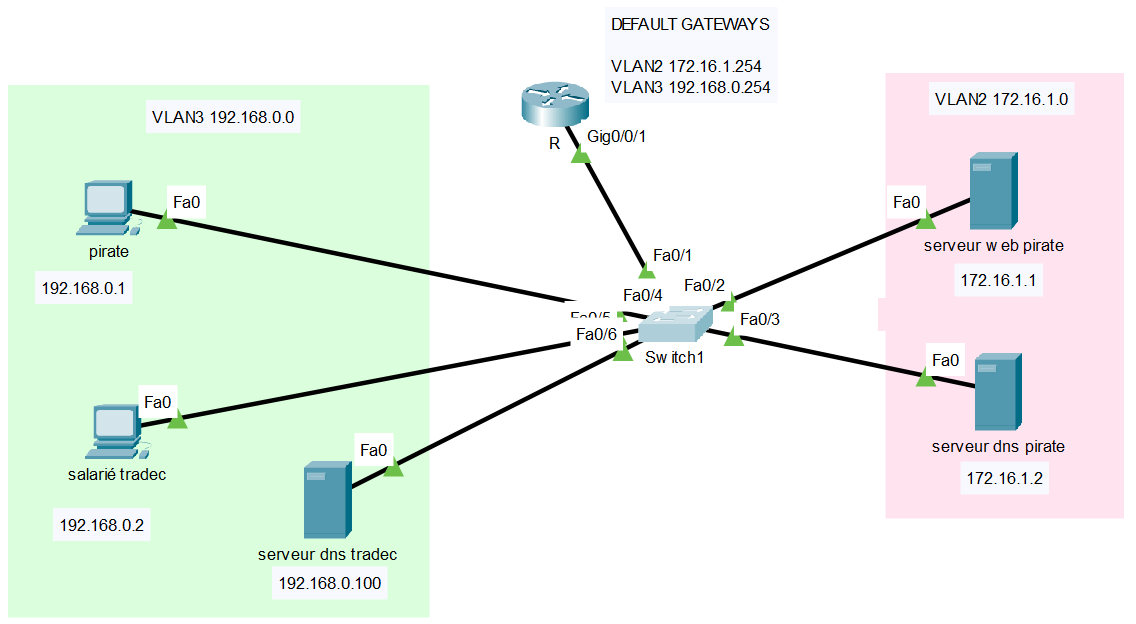
**Situation:**

L'entreprise Tradec a récemment été victime d'une attaque informatique, résultant dans la compromission de son serveur DNS. Les attaquants ont redirigé toutes les requêtes vers un site en Belgique, induisant en erreur sur la localisation géographique de Tradeco. Cette manipulation souligne l'importance cruciale de renforcer la sécurité des serveurs DNS pour prévenir de telles attaques. Tradeco doit désormais prendre des mesures urgentes pour restaurer la sécurité de son serveur DNS et évaluer les impacts potentiels sur ses opérations.

**La maquette à effectuer**

**Le script python**

# Simulated Python script to change DNS entry IP address on a router in Packet Tracer

# Sample DNS entry to change

domain\_to\_change = "example.com"

new\_ip\_address = "192.168.1.200"

# Simulate accessing the router's command-line interface

print("Router> enable")

print("Router# configure terminal")

# Simulate DNS configuration mode

print("Router(config)# ip dns server")

# Simulate changing the DNS entry

print(f"Router(config-dns)# no host {domain\_to\_change}") # Remove the existing entry

print(f"Router(config-dns)# host {domain\_to\_change} {new\_ip\_address}") # Add the new entry

# Simulate exiting configuration mode

print("Router(config-dns)# exit")

print("Router(config)# exit")

# Simulate saving the configuration

print("Router# copy running-config startup-config")

**Comment se protéger contre ce type d’infiltration**

Pour renforcer la sécurité, il est recommandé de maintenir le logiciel à jour, de configurer le serveur de manière minimale, d'utiliser **un pare-feu** pour contrôler le trafic, de privilégier des protocoles sécurisés tels que **DNS** sur **HTTPS** ou **DNS sur TLS**, et de limiter le nombre de requêtes par seconde.

De plus, la mise en place de listes de filtrage, la surveillance régulière du trafic DNS, une mise en cache efficace, et la sécurisation des mises à jour dynamiques avec des clés TSIG sont autant de pratiques importantes. La validation DNSSEC, garantissant l'intégrité des réponses DNS, ainsi que la séparation des rôles pour éviter d'héberger des services non essentiels sur le même serveur, contribuent également à renforcer la sécurité globale du serveur DNS. La surveillance des journaux et la prise de mesures en cas de détection d'activité suspecte complètent ces efforts pour assurer un environnement DNS robuste et résilient aux attaques.

(je n’ai pas réussi à exécuter le script afin de faire les modifications nécessaire sur le serveur dns à partir du post pirate)