IUT DE COLMAR

R316

Année 2022-23

Analyse de vulnérabilités

MARTIN BAUMGAERTNER

29 novembre 2022

Table des matières

Table des codes

1 TD 1 - 29 novembre 2022

1.1 Introduction aux commandes de bases

1.1.1 La commande HOST

Cette commande permet de récupérer les informations DNS d'un domaine. Elle permet de récupérer l'adresse IP d'un domaine, ainsi que les serveurs DNS associés. La différence entre **uha.fr** et **www.uha.fr** est que le premier est le domaine, alors que le second est un sous-domaine.

1.1.2 La commande DIG

La commande **dig** permet aussi d'intérroger un DNS. Elle donne des informations similaires à la commande **host** mais sous un autre format. En faisant **dig -h**, on peut voir les options disponibles. On peut par exemple faire **dig +trace** pour voir l'historique des requêtes DNS. On peut aussi faire **dig +short** pour n'afficher que les résultats.

1.1.3 La commande NSLOOKUP

La commande **nslookup** permet de faire des requêtes DNS. On peut par exemple faire **nslookup uha.fr** pour récupérer les informations DNS du domaine **uha.fr**. On peut aussi faire **nslookup -type=mx uha.fr** pour récupérer les serveurs mail du domaine **uha.fr**.

1.1.4 La commande WHOIS

La commande **whois** permet de récupérer les informations d'enregistrement d'un domaine. On peut par exemple faire **whois uha.fr** pour récupérer les informations d'enregistrement du domaine **uha.fr**. On peut aussi faire **whois -h whois.ripe.net uha.fr** pour récupérer les informations d'enregistrement du domaine **uha.fr** sur le serveur **whois.ripe.net**.

1.2 Le scan de réseaux

1.2.1 La commande NMAP

La commande **nmap** permet de scanner un réseau. Si on teste la commande : **nmap -sUV -F 192.168.2.23**, on peut voir que la commande **nmap** permet de scanner un réseau en utilisant les protocoles UDP, TCP et ICMP.