

# [Énumération/Réseau] DNS

## Introduction

Il existe plusieurs outils qui permettent d'énumérer un serveur DNS car ce dernier est souvent le point d'entrée des attaquants et regorge d'informations utiles sur les sous-domaines, les serveurs de messageries ou les adresses IP utilisés par la cible.



## Dig

Certainement l'outil le plus connu pour énumérer les serveurs DNS, il est très puissant et possède de nombreuses options.

### Utilisation standard

```
dig <FQDN>
```

### Énumération des serveurs de messagerie

```
dig <FQDN> -t mx +short
```

## Host

Cette commande va énumérer tous les serveurs se trouvant derrière le nom de domaine indiqué :

```
host <FQDN>
```

# DNSenum

## Installation

```
sudo apt install -y dnsenum
```

## Manuel

```
dnsenum <FQDN>
```

Vous pouvez utiliser l'option **--noreverse** pour ne pas lancer la procédure de reverse lookup sur les IP trouvées.

---

Revision #2

Created 10 November 2023 13:32:17 by Elieroc

Updated 3 May 2024 14:37:24 by Elieroc