

[Reconnaissance] NBTscan

Introduction

L'outil **nbtscan** permet de scanner les hôtes windows présents sur un sous-réseau.

Ses utilisations sont variées et permettent de récupérer différentes informations utiles lors d'un pentest.



Codes NetBios

| Codes | Descriptions |
|-------|--|
| 00 | Workstation service |
| 03 | Messenger service |
| 20 | File Server service |
| 1B | Domain Master Brower (contrôleur de domaine) |
| 1C | Contrôleur de domaine |
| 2B | Services d'annuaire |

Manuel

Syntaxe globale

```
nbtscan <SUBNET_ID/CIDR_MASK>
```

Exemple :

```
nbtscan 192.168.1.0/24
```

Options

| Options | Descriptions |
|------------|---|
| -v | Mode verbeux. |
| -e | Affiche des informations d'extension (utilisateurs actifs etc). |
| -m | Affiche les informations MAC des machines. |
| -r <RANGE> | Scanner une plage d'IP spécifique. |
| -f <FILE> | Scanner les adresses IP du fichier spécifié. |
| -t <DELAY> | Définit un délai d'attente personnalisé. |
| -h | Affiche la page d'aide |