

[Énumération] LDAP

Introduction

LDAP pour Lightweight Directory Access Protocol, est un protocole d'annuaire utilisé par des outils libres tels que **OpenLDAP**, mais aussi des solutions propriétaires comme **Active Directory**.

Quand il est utilisé au sein d'une organisation, il est une source d'information gigantesque pour un pirate qui arriverait à énumérer l'annuaire.



Nmap

Un script est présent au sein de l'outil pour scanner les annuaires LDAP.

Pour cela, exécutez la commande suivante :

```
nmap -p 389 --script=ldap-search <IP>
```

