

Le Scanning Réseau





Le **Scanning Réseau**

- ⦿ Se base sur les **informations** de l'étape précédente
- ⦿ Etape où l'on cherche **plus d'informations** (ports)
- ⦿ Que scanner et comment ?
- ⦿ Quels **services** écoutent ?
- ⦿ Quel **système d'exploitation** ?
- ⦿ Quelles **défenses** en place ?



L'énumération

- Suit le scan réseau
- Récupère plus d'informations **détaillées**
- Attention à ne pas TOUT scanner (128.X.X.X ou 129.X.X.X)



Différents types de scans

- ◉ **Ping Sweep** : identifier les machines qui répondent sur le réseau
- ◉ **Scan de port** : quels services ?
- ◉ **Network mapping** : carte du réseau
- ◉ **OS Fingerprinting** : quels systèmes d'exploitation sont utilisés ?



Aspects juridiques

- ◉ Scan non autorisé par défaut
- ◉ Peut faire réagir des **systèmes de détection d'intrusion**



Se protéger du Scanning Réseau

- Utiliser un pare-feu (ufw)
- Désactiver ou bloquer des ports
- Utiliser des IDS