Exploitation

Attaques sur les protocoles Cisco :
Attaques d'empreinte des mots de passe

- Plusieurs formes d'authentification possibles. Les commandes associées en mode d'exécution privilégié
  - `enable password`
  - `enable secret`
- `enable password <password>`
  - mot de passe stocké en clair dans le fichier de configuration !
  - Possibilité de le chiffrer en « type 7 »
  - Commande `service password-encryption`
- `enable secret <password>`
  - Mot de passe chiffré en « type 5 » dans le fichier de configuration.

Exploitation

Attaques sur les protocoles Cisco :
Attaques d'empreinte des mots de passe

- Vulnérabilités
  - Pas de chiffrement du mot de passe
  - Ou faiblesse de l'algorithme de chiffrement
- Chiffrement type 7
  - Format reversible
  - Outils : `Cain & Abel, Ciscocrack, GetPass…`
- Chiffrement de type 5
  - Empreinte MD5 du mot de passe, unique et non réversible
  - Attaque possible par comparaison d'empreinte de mots de passe
  - Outils : `John The Ripper, Hachcat, RainbowTables…`