Exploitation

Attaques sur le protocole SNMP

Brute force de la Community String par dictionnaire : création d'un dictionnaire

- Objectif
  - Construire un dictionnaire de nom de communauté à partir de mots clés relatifs à une cible.

- Outils
  - `Cewl` à partir d'une URL
  - `Crunch`
  - `JTR`
    - `./john -wordlist=passw.lst –stdout -rules`
  - `rsmangler`
    - `./rsmangler.rb -f wordlist.txt -x 12 -m 7 -drlTulseiyac –pna –pnb –na –nb –space > output.txt`

Exploitation

Attaques sur le protocole SNMP

SNMP : Collecte d'informations

- Permet de fournir des informations sur :
  - Etat du réseau, activité CPU, charge mémoire…
  - Nom, type, statistiques des interfaces réseaux
  - Interfaces réseaux, table ARP
  - Etats ICMP, TCP et UDP
  - Ports en écoute, états des connexions établies
  - Ressources disque, partitions, processus
  - Liste du matériel : CPU, imprimantes, disques, cd-rom…