Exploitation

Attaques sur le protocole SNMP

Brute force de la Community String par dictionnaire : les outils

- Tools
  - Metasploit
  - onesistyone (https://github.com/trailofbits/onesixtyone)
  - nmap : nmap -sU -p 161 —script snmp-brute.nse 40.0.0.4
  - medusa
  - hydra
  - patator…

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`