Exploitation

Attaques sur le protocole SNMP

- Prise d'empreinte de la version
  - `nmap -sU -p 161 -A 40.0.0.4`
- Attaque de la Community String
  - Sniffing : `ettercap, wireshark`…
  - Attaque par dictionnaire
- Collecte d'informations
- Modification de la configuration

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…