

Exploitation

Attaques sur le protocole SNMP

SNMP : Collecte d'informations

SNMP Pwnd :

Information data leakage attacks against SNMP enabled embedded devices



Deral Heiland and Matthew - HackinParis 2015

Enterprise Device Attacks

- **Kyocera printers (Various models)**
 - Independently discovered by both Artyon Breus and Chris Schatz

- SMB Path: 1.3.6.1.4.1.1347.42.23.2.4.1.1.2.x.1
- SMB Host: 1.3.6.1.4.1.1347.42.23.2.4.1.1.3.x.1
- SMB Port: 1.3.6.1.4.1.1347.42.23.2.4.1.1.4.x.1
- SMB Login: 1.3.6.1.4.1.1347.42.23.2.4.1.1.5.x.1
- SMB Password: 1.3.6.1.4.1.1347.42.23.2.4.1.1.6.x.1

X= user number



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`