SNMP Enumeration

SNMP Enumeration

Simple Network Management Protocol is an application layer protocol defined by the Internet Architecture Board in RFC 1157. SNMP is used to exchange management information between network devices. It is one of the most commonly used protocols for network management. SNMP is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite as defined by the Internet Engineering Task Force.Organizations use SNMP to monitor and manage devices in a local area network (LAN) or wide area network (WAN). Most network devices on the market come bundled with SNMP agents. If not, some devices allow network admins to install the agents.

SNMP Enumeration using nmap

`nmap -sU -p 161 --scipt=snmp-sysdescr [TARGET IP ADDRESS]`

`-p` - port

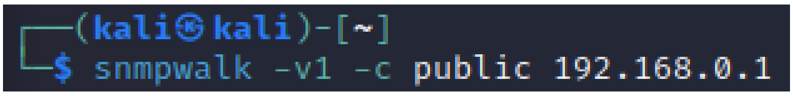
`-sU` - UDP

`nmap -sU -p 161 --script=snmp-processes [TARGET IP ADDRESS]`

`nmap -sU -p 161 --script=snmp-win32-software [TARGET IP ADDRESS]`

`nmap -sU -p 161 --script=snmp-interfaces [TARGET IP ADDRESS]`

SNMP Enumeration using snmpwalk



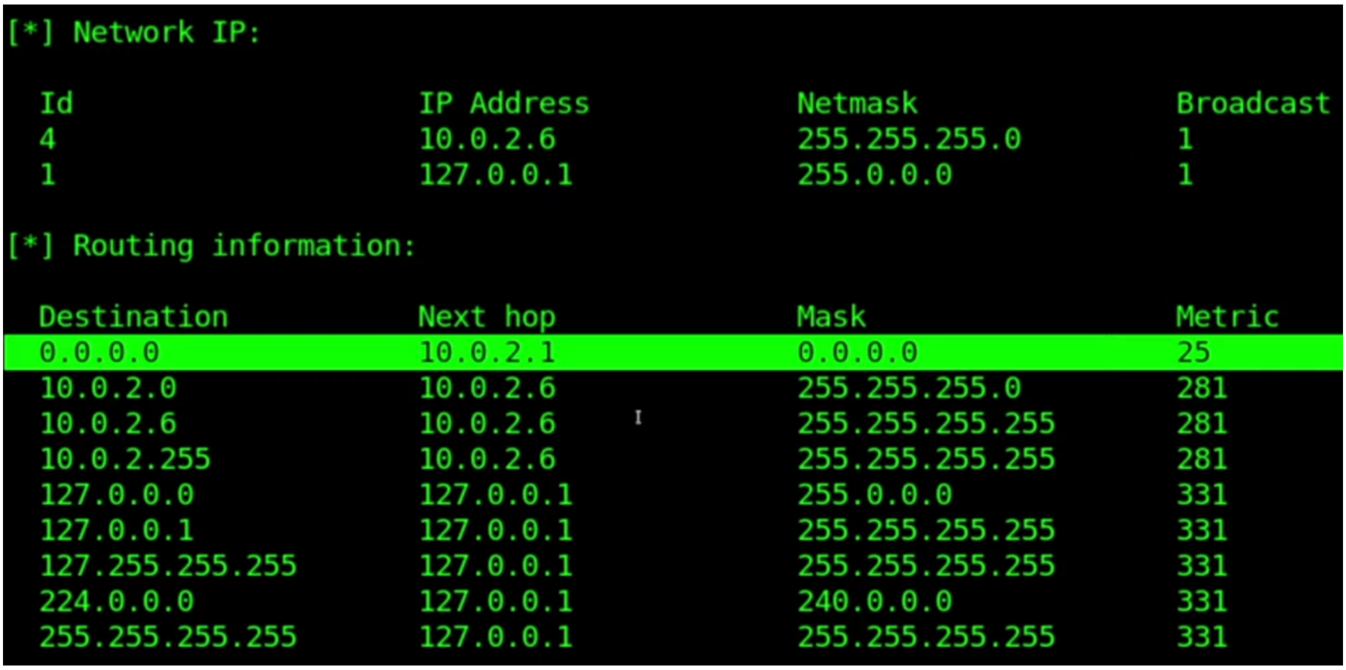
```
┌──(kali㉿kali)-[~]
└─$ snmpwalk -v1 -c public 192.168.0.1
```

`-v1` - version

`-c` - type

SNMP Enumeration using snmp-check

`snmp-check [IP ADDRESS]`



```
[*] Network IP:

  Id                     IP Address             Netmask                Broadcast
  4                      10.0.2.6               255.255.255.0          1
  1                      127.0.0.1              255.0.0.0              1

[*] Routing information:

  Destination            Next hop               Mask                   Metric
  0.0.0.0                10.0.2.1               0.0.0.0                25
  10.0.2.0               10.0.2.6               255.255.255.0          281
  10.0.2.6               10.0.2.6               255.255.255.255        281
  10.0.2.255             10.0.2.6               255.255.255.255        281
  127.0.0.0              127.0.0.1              255.0.0.0              331
  127.0.0.1              127.0.0.1              255.255.255.255        331
  127.255.255.255        127.0.0.1              255.255.255.255        331
  224.0.0.0              127.0.0.1              240.0.0.0              331
  255.255.255.255        127.0.0.1              255.255.255.255        331
```