SNMP enumeration

This section will cover the tools that can be used to check for the **Simple Network Monitoring Protocol** (**SNMP**). Even though the information from a SNMP device may not look important, as pen-testers, we have seen misconfigured SNMP devices which allow us to read the configuration, get important information, and even have a privilege to modify the configuration.

We suggest you also check the SNMP devices when you encounter a penetration testing job; you may be surprised with what you find.

onesixtyone

The `onesixtyone` tool can be used as a SNMP scanner to find whether the SNMP string exists on a device. The difference with respect to other SNMP scanners is that this tool sends all the SNMP requests as fast as it can (10 milliseconds apart). Then it waits for the responses and logs them. If the device is available, it will send responses containing the SNMP string.

To access `onesixtyone` , go to the console and type `onesixtyone` .

Note

By default, Metasploitable 2 does not have the SNMP daemon installed. To install it, just type the following command after you are connected to the Internet:

```
apt-get install snmpd
```

Then, you need to change the configuration file, `/etc/default/snmpd` :

```
sudo vi /etc/default/snmpd
```

In the `SNMPDOPTIONS` line, remove the localhost address (`127.0.0.1`) and restart SNMPD:

```
sudo /etc/init.d/snmpd restart
```

Beware that you need to isolate the Metasploitable 2 machine from the network connected outside. If not, you will get attacked easily.

Let's try `onesixtyone` to find the SNMP strings used by a device located at `192.168.1.1` . The following is the appropriate command:

```
onesixtyone 192.168.56.103
```

The following is the scanning result:

```
Scanning 1 hosts, 2 communities
192.168.56.103 [public] Linux metasploitable 2.6.24-16-server #1 SMP Thu
Apr 10 13:58:00 UTC 2008 i686
192.168.56.103 [private] Linux metasploitable 2.6.24-16-server #1 SMP Thu
Apr 10 13:58:00 UTC 2008 i686
```

The SNMP strings found are `public` and `private` .

If we want the scanning to be more verbose, we can give the `-d` option:

```
onesixtyone -d 192.168.56.103
```

The result is as follows:

```
Debug level 1
Target ip read from command line: 192.168.56.103
2 communities: public private
Waiting for 10 milliseconds between packets
Scanning 1 hosts, 2 communities
```

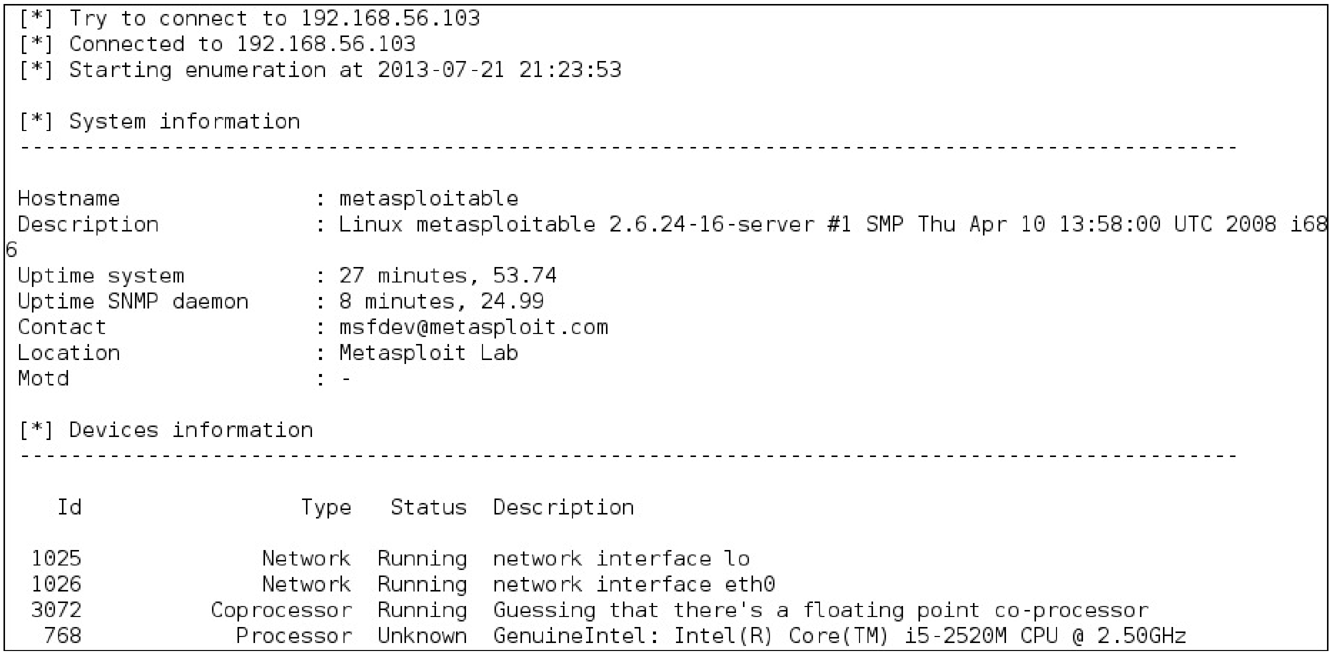
```
Trying community public
192.168.56.103 [public] Linux metasploitable 2.6.24-16-server #1 SMP Thu
Apr 10 13:58:00 UTC 2008 i686
Trying community private
192.168.56.103 [private] Linux metasploitable 2.6.24-16-server #1 SMP Thu
Apr 10 13:58:00 UTC 2008 i686
All packets sent, waiting for responses.
done.
```

snmpcheck

You can use `snmpcheck` to collect more information about the SNMP device using the following command:

```
snmpcheck -t 192.168.56.103
```

The following screenshot shows the information obtained from the preceding command:



```
 [*] Try to connect to 192.168.56.103
 [*] Connected to 192.168.56.103
 [*] Starting enumeration at 2013-07-21 21:23:53

 [*] System information
 -----------------------------------------------------------------------------------------------

 Hostname                : metasploitable
 Description             : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6
 Uptime system           : 27 minutes, 53.74
 Uptime SNMP daemon      : 8 minutes, 24.99
 Contact                 : msfdev@metasploit.com
 Location                : Metasploit Lab
 Motd                    : -

 [*] Devices information
 -----------------------------------------------------------------------------------------------

    Id                  Type   Status   Description

  1025               Network  Running   network interface lo
  1026               Network  Running   network interface eth0
  3072           Coprocessor  Running   Guessing that there's a floating point co-processor
   768             Processor  Unknown   GenuineIntel: Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz
```