SNMP Enumeration

The Simple Network Management Protocol (SNMP) is a widely used protocol for managing and monitoring network devices such as routers, switches, servers, and printers. While SNMP provides valuable information about the health and status of network devices, improper configuration or the use of default community strings can leave systems vulnerable to enumeration and exploitation.

Enumeration with nmap

Lets start with the SNMP Enumeration with nmap. The thing to note here is that SNMP works on UDP port 161. So, before throwing any script on it, lets first confirm it is running or not.

```
sudo nmap -Pn -sU -p 161 192.68.29.141
```

Now that we know that it is potentially running, lets perform nmap script scan to it.

```
sudo nmap -Pn -sU -p 161 -sC 192.68.29.141
```

Let see if we have other scripts related to SNMP. We does have a lot of them. Lets try all of them at once.

```
ls /usr/share/nmap/scripts | grep snmp

sudo nmap -Pn -sU -p 161 --script snmp-hh3c-logins,snmp-info,snmp-
interfaces,snmp-ios-config,snmp-netstat,snmp-processes,snmp-sysdescr,snmp-
win32-services,snmp-win32-shares,snmp-win32-software,snmp-win32-users
192.68.29.141
```

Enumeration with snmpwalk

Another tool that we can use for SNMP enumeration is snmpwalk.

So SNMP basically uses community strings which is like a password that allows devices on a network to communicate with each other.

There are two main types of community strings:

1. **Read-only**:
2. **Read-write**:

Most network devices come with default community strings, often "public" for read-only and "private" for read-write access.

Now lets enumerate snmp service using public community string,

```
snmpwalk -c public <IP>

snmpwalk -v2c -c public <ipAddr> - Enumerate SNMPv2 with a community
string of Public

snmpwalk -v2c -c public <ipAddr> hrSWInstalledName - To search for
installed software:

snmpwalk -v2c -c public <ipAddr> hrMemorySize - To search amount of RAM on
the host
```

Bruteforcing Community Strings with SNMP Brute

Sometimes, the read only community strings is not equal to public. In that case, we have to bruteforce it to get the actual one. We can use SNMP brute tool for that, this tool uses a wordlist containing common SNMP community strings and then tried to check it against the SNMP service, the successful hit gives us the information about the used community strings.

```
python3 ~/Tools/SNMP-Brute/snmpbrute.py -t 10.10.11.193 -f
~/Desktop/Wordlist/SecLists/Discovery/SNMP/common-snmp-community-
strings.txt
```

There are other tools like hydra and onesixtyone to perform community strings bruteforcing but for me SNMPbrute always works like a charm.

While performing SNMP enumeration, we are bombarded with a lot of data which can make us overwhelmed real quick. To avoid this, one advice would be to look for credentials only rather than processing the whole SNMP output. Look for the areas, where credentials are exposed and avoid unncessary information overload.
