Geinstalleerd:

* Ruby
* python pip
* snmp-check
* snmpwalk
* onesixtyone

SNMP

protocol versies v1,v2 en v3

3 key components van SNMP port 161,162:

* Managed devices
* Agent - software which runs on managed devices
* Network management (NMS) - software which runs on the manager

snmp brute force tools:

metasploit

snmpwalk

snmapstat

john the ripper

'community strings':

* GET – is the command to retrieve an OID from the MIB
* GET-Next – is the command to walk through the MIB tree going from one OID to the next, this is the command SNMP-walk is based on.
* SET – write a value in a parameter
* TRAP – send an error message or alert due to a configurable threshold being passed or a trigger activated

Gebruikte commando’s:

snmpwalk -v 3c -c sun 192.168.6.2

snmpwalk -v 2c -c <communitystring> 192.168.6.2

onesixtyone -c /usr/share/doc/onesixtyone/dict.txt 192.168.6.2

enumeration:

snmp-check

info over het achterhalen van informatie over SNMP(tools):

https://resources.infosecinstitute.com/snmp-pentesting/

#prerequisites:

sudo apt-get install python3-tk

sudo dnf install python3-tkinter

#python does not work for snmp-check -> install ruby

#Ruby '59' error solution: gem install text-table && gem install snmp

https://github.com/0xsauby/yasuo/issues/33

#info

#Server ip (DAVE IT NETWORK) = 172.16.40.67

#passwd = 02a843fe76d65a5a

frank@frank-GL553VW:~/Desktop$

Links:

<https://linuxhint.com/passowrd_brute_force_nmap/>

<https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol>

<https://tools.kali.org/information-gathering/snmp-check>

snmpcheck example:

<https://www.nothink.org/codes/snmpcheck/snmpcheck-1.8.pl>

file snmp-brute (nmap)

<https://nmap.org/nsedoc/scripts/snmp-brute.html>

Brute force tutorial (niet echt gebruikt, enkele keer als referentie)

<https://github.com/SECFORCE/SNMP-Brute>

snmpwalk:

<https://www.poftut.com/snmpwalk-command-line-examples/>

snmpcheck:

<https://tools.kali.org/information-gathering/snmp-check>

Algemene info SNMP op Linux (installatie)

<https://linoxide.com/how-tos/snmp-installation-linux-server/>

‘tk’ - error work around (python – probeersel)

[https://stackoverflow.com/questions/4783810/install-tkinter-for-python#4784123](https://stackoverflow.com/questions/4783810/install-tkinter-for-python" \l "4784123)

port 8686 details

<https://www.speedguide.net/port.php?port=8686>

netdiscover , uiteindelijk niet gebruikt → Nmap en ARP wel.

<https://kalilinuxtutorials.com/netdiscover-scan-live-hosts-network/>

‘Reduce risk of SNMP abuse:

https://www.us-cert.gov/ncas/alerts/TA17-156A