CYBERSECURITY

SCANNING AND ENUMERATION: SNMP AND VYOS

EXERCISE

START THE SNMPHACK-VYOS MACHINE

Make sure your Virtualbox setup has a 192.168.62.0 network with a dhcp server handing out addresses from 192.168.62.200-254.
Import the SNMPHack-VyOs machine.
Before starting the machine:

- Make sure the network interface points to the 192.168.62.0 network.
- Set its MAC address to 08:00:27:3d:48:f5. (Note: during import you could also have check the option to import the MAC addresses. This would produce the same behaviour.)

GET THE TARGET IP ADDRESS

Try to obtain its IP address. (It should be in the 192.168.62.x range so make sure your testing machine can reach it. Setup networking in host-only mode.)
Hint: use “nmap” or “netdiscover” and check the MAC-address of your target-machine in VirtualBox.

Check which SNMP ports are open through a UDP scan. (Scan the specific ports if you want the scan to go faster.)

GET THE COMMUNITY STRING

We will show you 2 ways to “find” the community string, needed to connect to the SNMP service: brute force guessing the string and sniffing it from the network.

BRUTE FORCE

Use a dictionary file to bruteforce crack the community string.

Make a dictionary file with random possible community strings. The real community strings are ignite123 (read only) and ignite321 (read write). Make sure that these are in the dictionary file.

Use the snmp cracking tool “onesixtyone” with the option -c to crack the community string

Note1: there are other tools in KALI that can do the same.
Note2: the wordlists in kali are under /usr/share/wordlists

SNIFF

We have captured network traffic on the network between a machine (e.g. system management server) and our target. This SNMP traffic reveals the community name.

The capture can be found with the VMs and is named: SNMP-VyOsQuery.pcapng
You can use wireshark to see if you can find the community string.

Note: if the community string would be encrypted (SNMPv3+) this would require an extra de-encryption step.
Here the machine uses SNMPv1.

SNMP ENUMERATION

Perform an snmp enumeration on the target.
Use the “snmpwalk” tool with the options -v and -c
The community string to use (with rw options) is: ignite321
The snmp version is v1.

The machine should respond with a list of parameters that can be queried.
You can redirect the output of the command to a file for easier processing/reading.

Extra questions:

Can you see the type of OS? Give the MIB OID number.

GET READABLE INFO

Each number/parameter that snmpwalk retrieves is a MIB hierarchical number.
The format is not readable so we use another tool.
Use “snmp-check” with parameters -c and -p to get the information in readable form.

Check out the huge amount of information that is obtained.

By cross-referencing the output from “snmp-check” with “snmpwalk” you can get the MIB ID number.
Find the ID-number of the hostname. This should be a STRING type.

CHANGE INFO

We can change the snmp information.
This is possible because the community string “ignite321” has read/write permissions.

Try to do this by using the “snmpset” tool with the options -v and -c. Use the MIB ID you found previously.

You can use snmpwalk again to see if the snmp parameter has changed. (Not the actual hostname.)

EXTRA TOOL: BRAA

Braa is a very fast tool for snmp scanning.
Test it. It’s help function should give you enough information.
You know the community string and the IP address. The MIB IDs can be limited to a certain range.
