Lab 2: Perform SNMP Enumeration

Lab Scenario

As a professional ethical hacker or penetration tester, your next step is to carry out SNMP enumeration to extract information about network resources (such as hosts, routers, devices, and shares) and network information (such as ARP tables, routing tables, device-specific information, and traffic statistics).

Using this information, you can further scan the target for underlying vulnerabilities, build a hacking strategy, and launch attacks.

Lab Objectives

- Perform SNMP enumeration using SnmpWalk

Overview of SNMP Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP (User Datagram Protocol) and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on networking devices on Windows and UNIX networks.

SNMP enumeration uses SNMP to create a list of the user accounts and devices on a target computer. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

Task 1: Perform SNMP Enumeration using SnmpWalk

SnmpWalk is a command line tool that scans numerous SNMP nodes instantly and identifies a set of variables that are available for accessing the target network. It is issued to the root node so that the information from all the sub nodes such as routers and switches can be fetched.

Here, we will use SnmpWalk to perform SNMP enumeration on a target system.

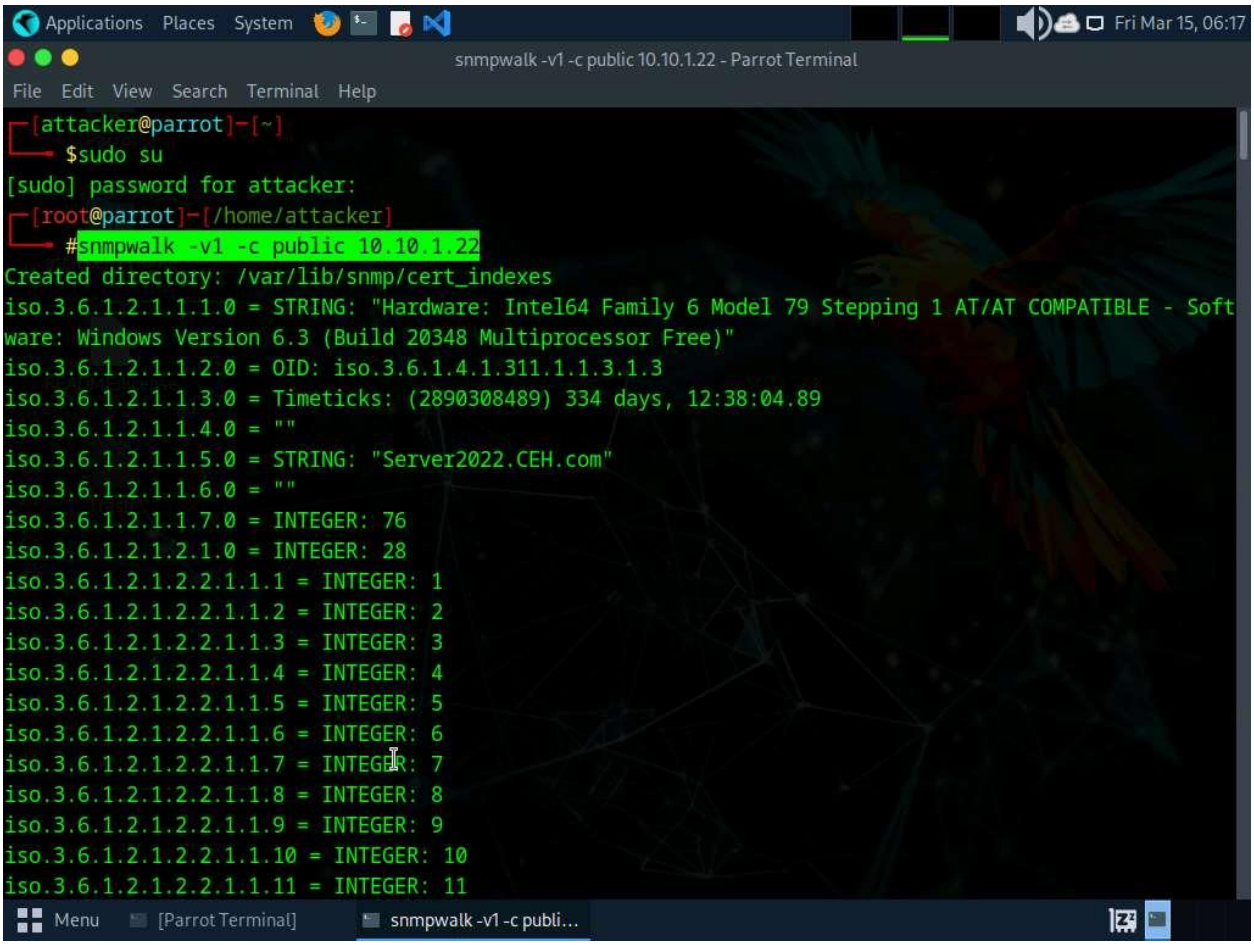
1. Click Parrot Security to switch to the **Parrot Security** machine. Login with **attacker**/**toor**, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

2. Run **snmpwalk -v1 -c public [target IP]** command (here, the target IP address is **10.10.1.22**).

–v: specifies the SNMP version number (1 or 2c or 3) and **–c**: sets a community string.

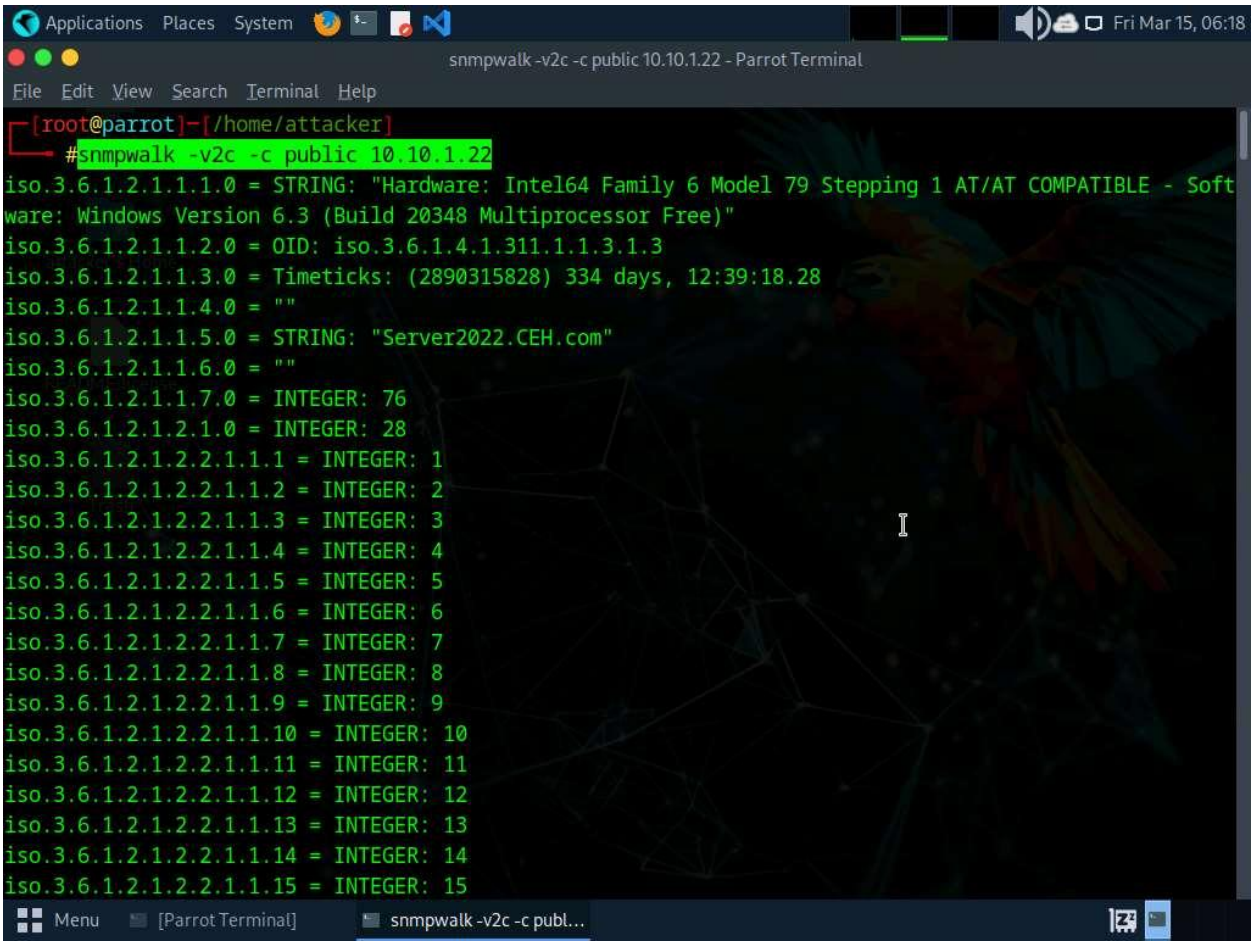
3. The result displays all the OIDs, variables and other associated information.



4. Run **snmpwalk -v2c -c public [Target IP Address]** command to perform SNMPv2 enumeration on the target machine (here, the target IP address is **10.10.1.22**).

–v: specifies the SNMP version (here, 2c is selected) and **–c**: sets a community string.

5. The result displays data transmitted from the SNMP agent to the SNMP server, including information on server, user credentials, and other parameters.



6. This concludes the demonstration of performing SNMP enumeration using the SnmpWalk.
7. Close all open windows and document all the acquired information.

Question 4.2.1.1

Use SnmpWalk to perform SNMP enumeration on the Windows Server 2022 machine. Enter the option that sets a community string.