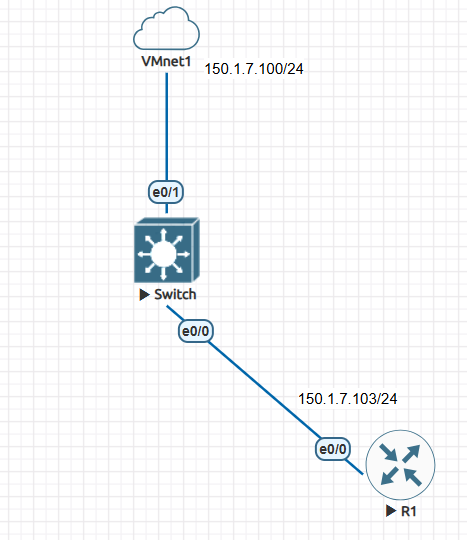
**Cyber Security – Assessment # 5**

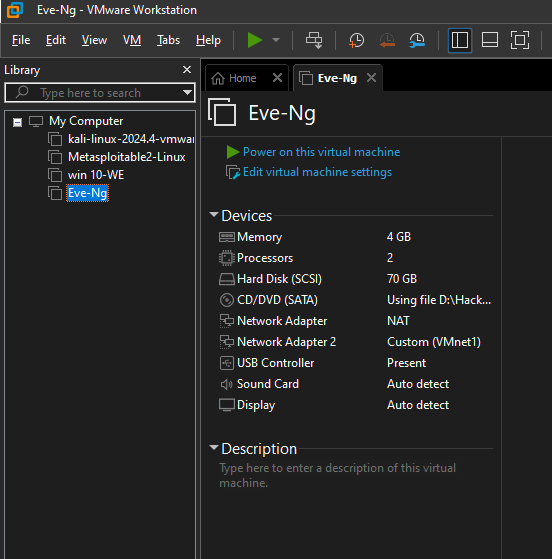
**Q1.** Build your topology in EVE-NG as per following diagram. Make your R1 is pingable from Kali Linux.



Q2. SNMP enumeration is the process of gathering detailed information about a network device using the Simple Network Management Protocol (SNMP). It typically involves querying a device for data such as system configurations, interfaces, routing tables, and more. To begin the enumeration, you would first need to determine the SNMP version and the community string, which acts like a password to access the device.

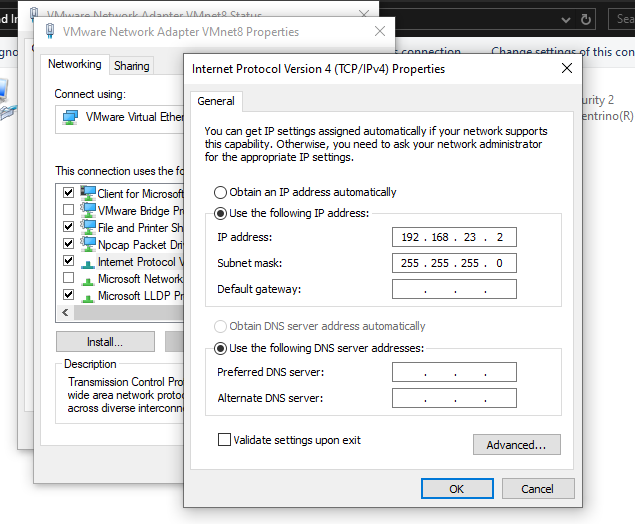
* Configure Cisco router as SNMP client with default community strings (read-only: **public** / read-write: **private**)
* Perform SNMP enumeration using Nmap. View port status of target.
* Confirm the nodes in the target network with default SNMP community strings. Use “**snmp-brute**” script (Nmap) to extract SNMP community string from target machine.

**Answer 1:**

**VMwere Setting to install Eve-Ng iso Image**

**Setting up EVE-NG on a Base Machine/Virtual Machine**

**Set IP to Vm8 network Adpater**



**Step-by-Step Instructions:**

**Base Machine/Virtual Machine Configuration**:

* Add a **VM Network Adapter** and assign these settings:
  + **IPv4 Address**: 192.168.23.1
  + **Subnet Mask**: 255.255.255.0
    - Proceed with the installation.

**Creating the Virtual Machine**:

* Select Linux as the operating system and choose Ubuntu 64-bit.
* Assign the following resources to the VM:
* **Memory (RAM)**: Minimum 12GB
* **Disk Space**: Minimum 50GB
* Add the required **network adapter(s)** to the VM.
* Enable **virtualization** in the processor settings.

**Initial Boot**:

* Power on the virtual machine.
* Choose the **default options** during setup and continue until prompted to reboot.
* After seeing the "Reboot" message, wait **10–20 seconds**, then **disconnect the virtual CD/DVD drive** before continuing.

**Assigning a Management IP to EVE-NG**:

* Once the system boots back up, you’ll configure the management network settings:
* Follow the prompts to select the default options.
* Use the **arrow key** and the **space bar** to select DHCP, then press Enter.
* If you’re assigning a static IP, input the following details:
  + **IP Address**: 192.168.23.60
  + **Subnet Mask**: 255.255.255.0
  + **Gateway**: 192.168.23.2
  + **Primary DNS**: 192.168.23.2
* Continue with the **default installation settings**.

**Installing Required Files**:

* Download and install **WinSCP** on your local machine.
* Use the default EVE-NG username/password to log in via WinSCP.
* Navigate to the following path: /opt/unetlab/addons/iol/bin
* Add and upload the necessary files to this directory:
  + iourc
  + L3-ADVENTERPRISEK9-M-15.4-2T
  + CiscoIOUKeygen
  + i86bi\_linux\_l2-advipservicesk9-ms.high\_iron\_20170202

**Install Additional Tools**:

* Install the **EVE-NG Windows Client Pack (Version 2.0)** for added functionality.

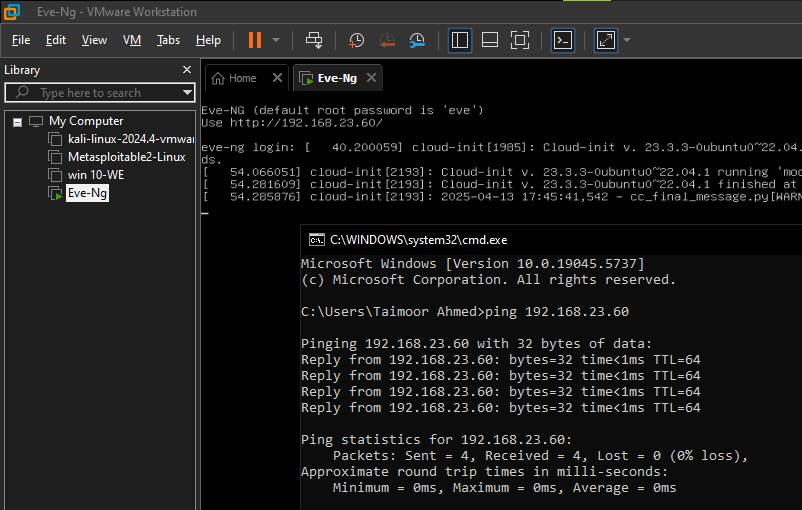
**Logging into EVE-NG**:

* Open a browser and connect to EVE-NG using the assigned management IP: http://192.168.23.60
* Log in to the EVE-NG web interface.

**Adding Cisco IOL Nodes**:

* Once logged in, add a new node in the web interface.
* Search for **Cisco IOL** and set up the desired network node.

After **installation** Eve-Ng open cmd and Ping from host machie “**ping 192.168.23.60**”

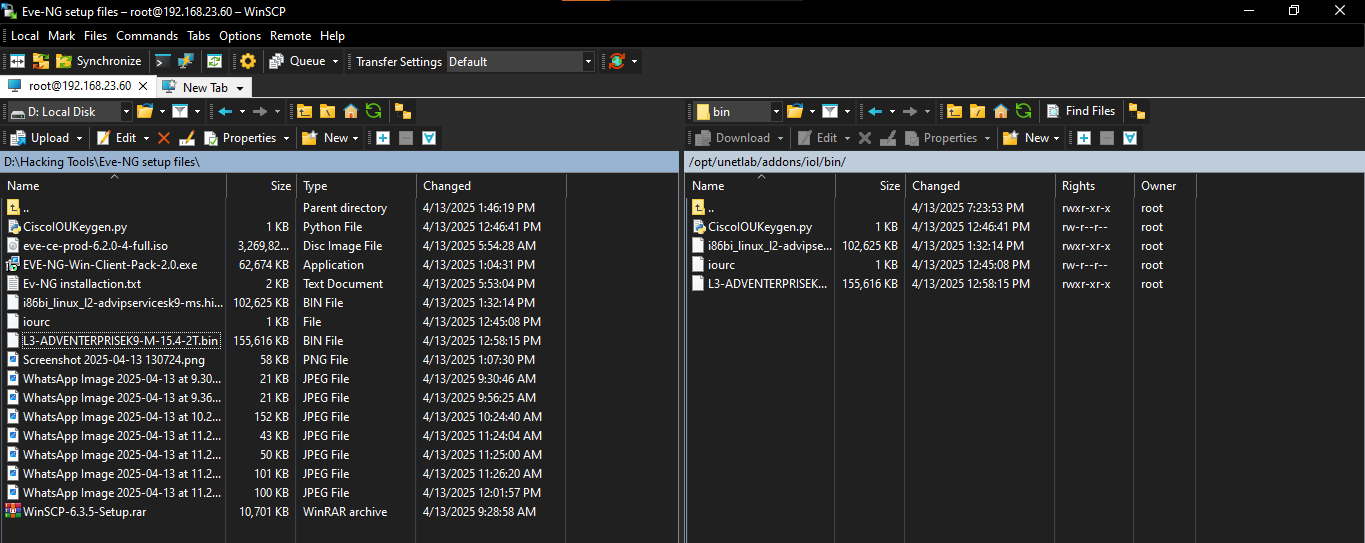


Now open any **browser & type 192.168.23.60**

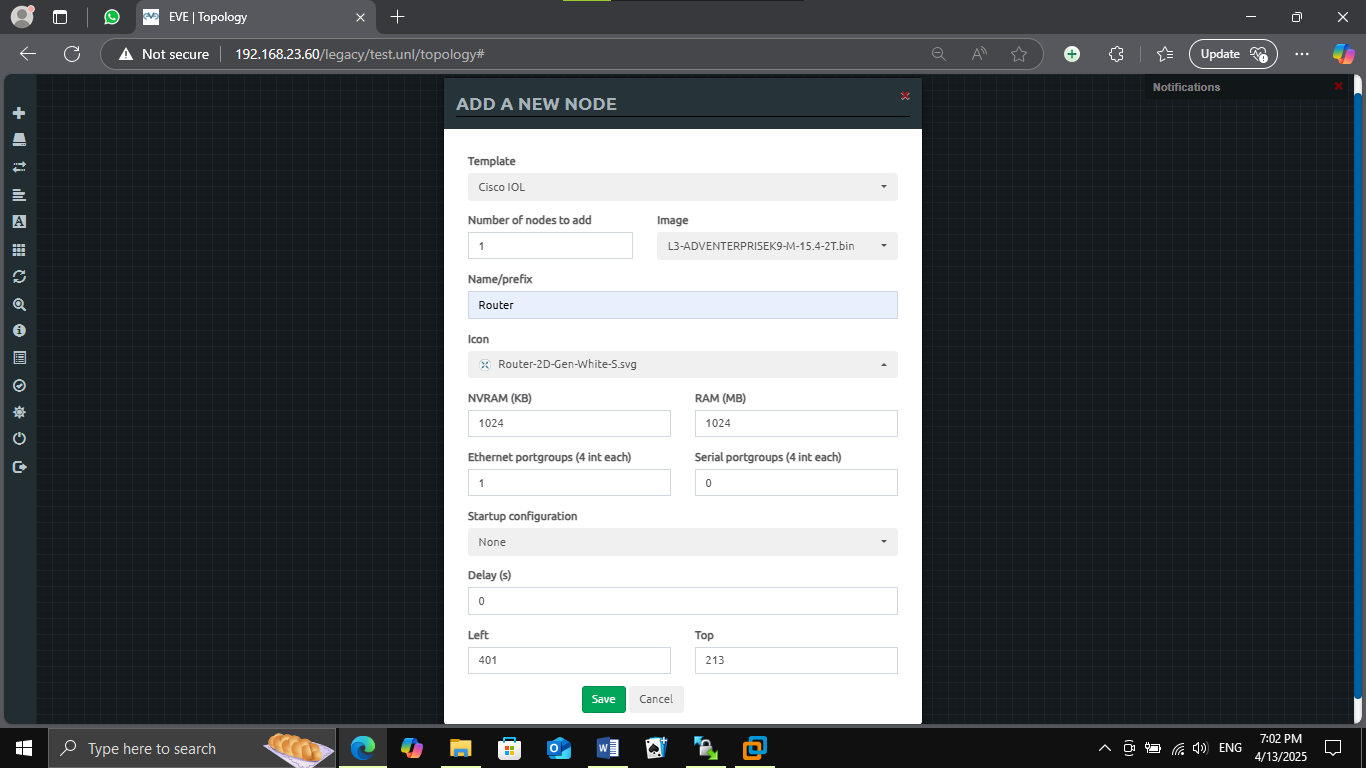
* **Username: admin**
* **Password: eve**



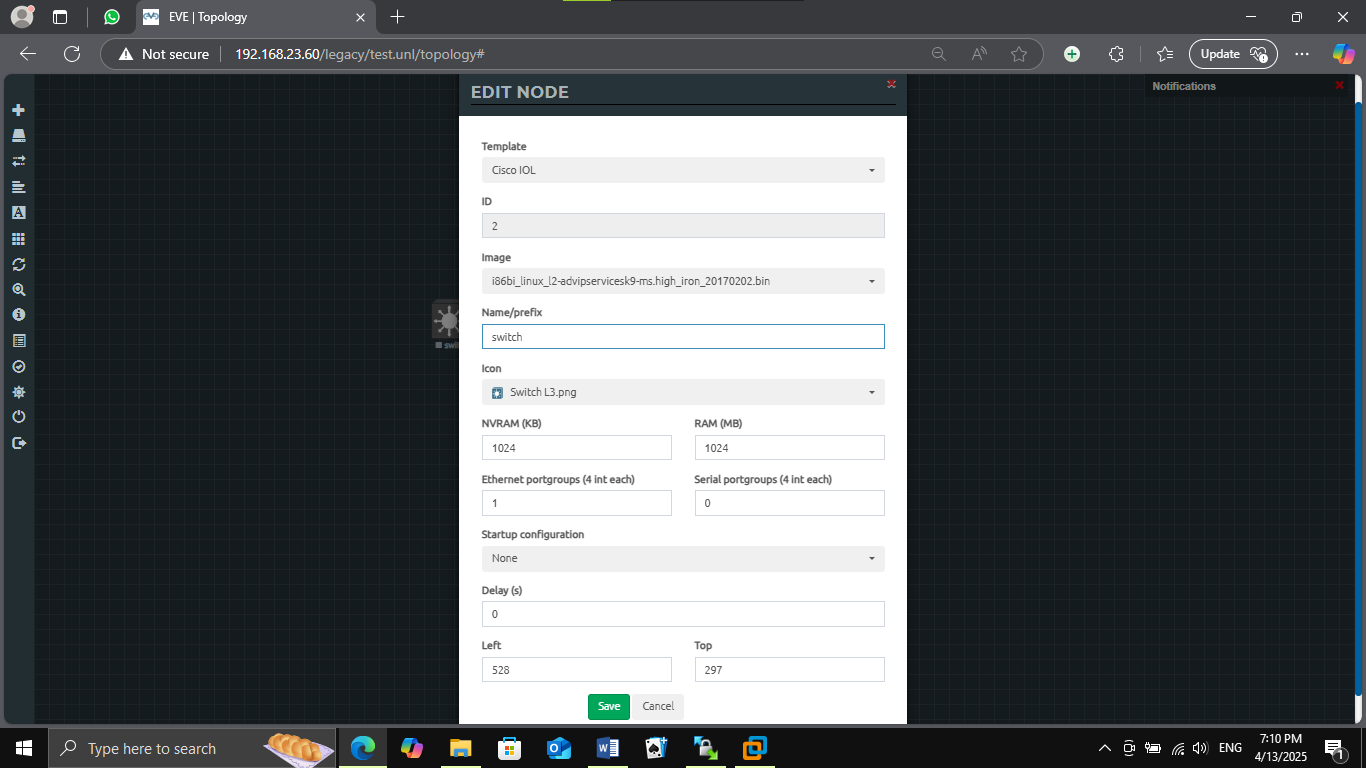
Adding host path or **“/opt/unetlab/addons/iol/bin/”**  to **Winscp**



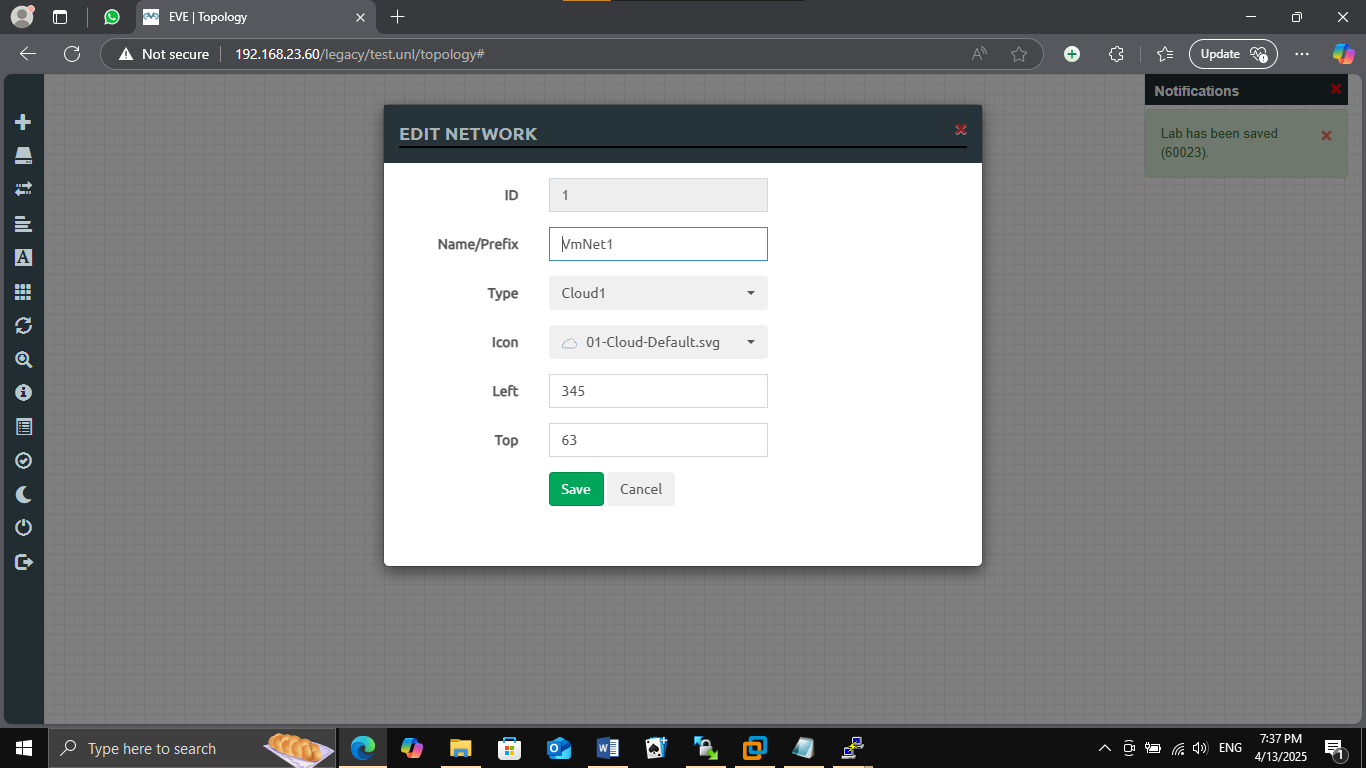
Adding **new node L3 Router** Image



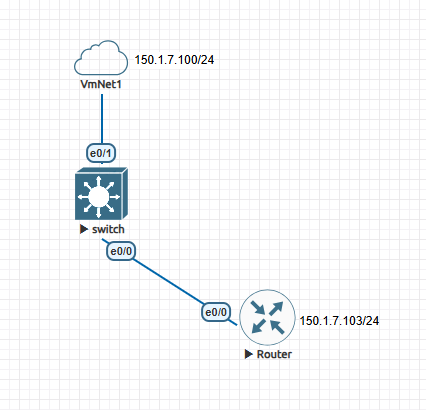
Adding **new Node L2 Switch** Image



Adding **Network Cloud 1 = Vmnet1**

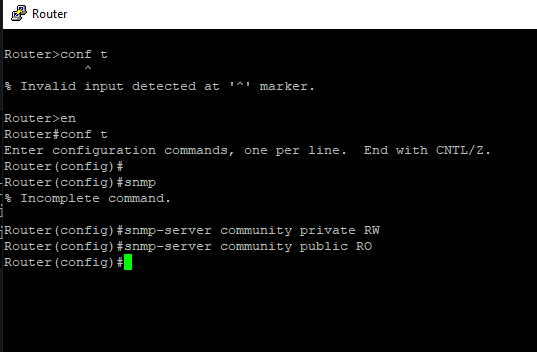


The **structure** will be something like this and you will need to start the **router** and **switch** and **configure their settings** now.

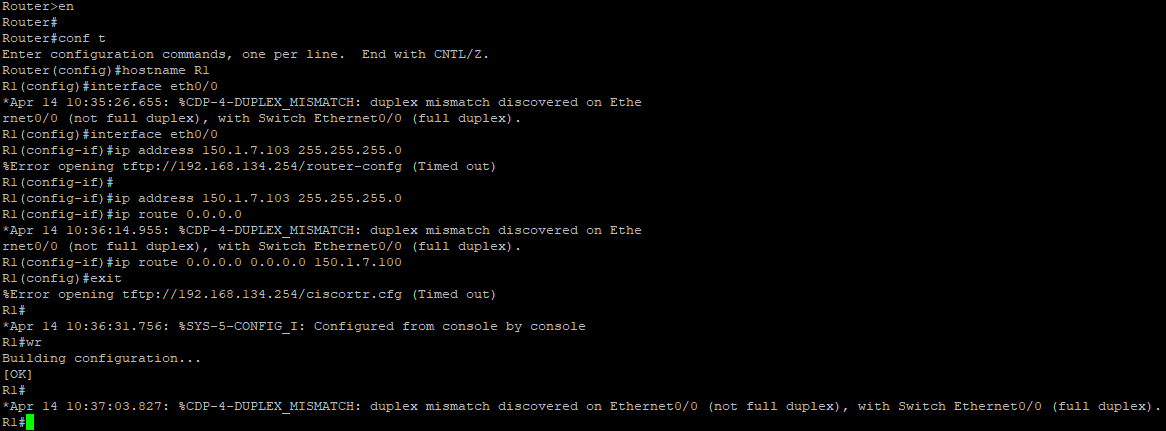
****

**Router:**

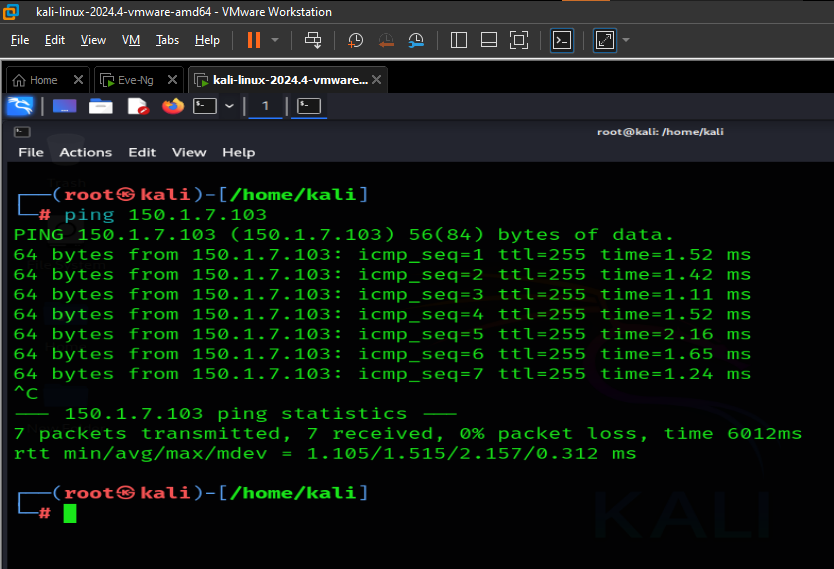
* **Gave permission SNMP**
  + **en**
  + **conf t**
  + **Snmp-server community private RW**
  + **Snmp-server community public RO**

****

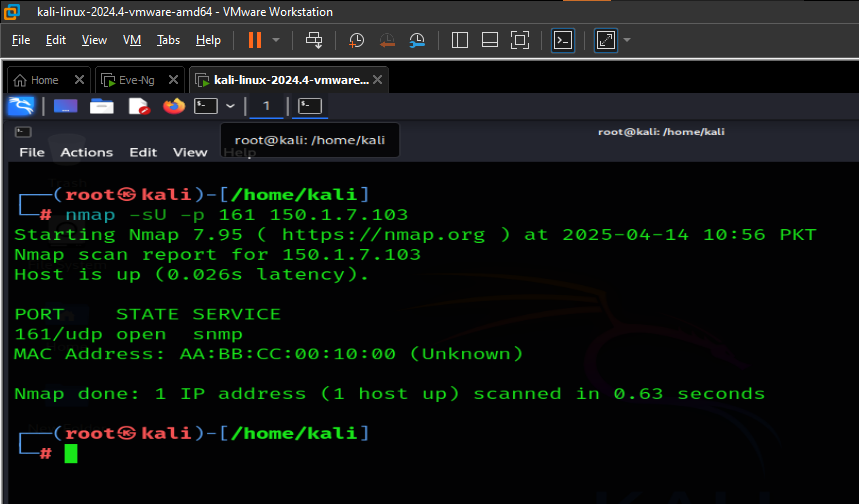
* **Than configure the router setting**
  + **Would you like to enter the initial configuration dialog? [yes/ no] : no**
  + **Router>en**
  + **Router#**
  + **Router#conf t**
  + **Router(config)#hostname R1**
  + **R1(config)#interface eth 0/0**
  + **R1(config-if)#ip address 150.1.7.103 255.255.255.0**
  + **R1(config-if)#no sh**
  + **R1(config-if)#exit**
  + **R1(config)#ip route 0.0.0.0 0.0.0.0 150.1.7.100**
  + **R1(config)#exit**
  + **R1#wr**

****

**In Kali ping 150.1.7.103**

****

**Now SCAN using Kali Linux with Nmap Tool 150.1.7.103 “nmap -sU -p 161 150.1.7.103”**

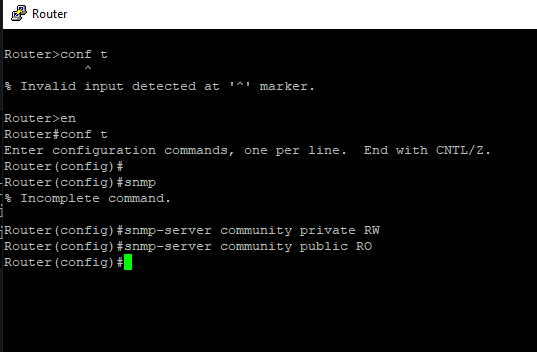
****

**Answer 2:**

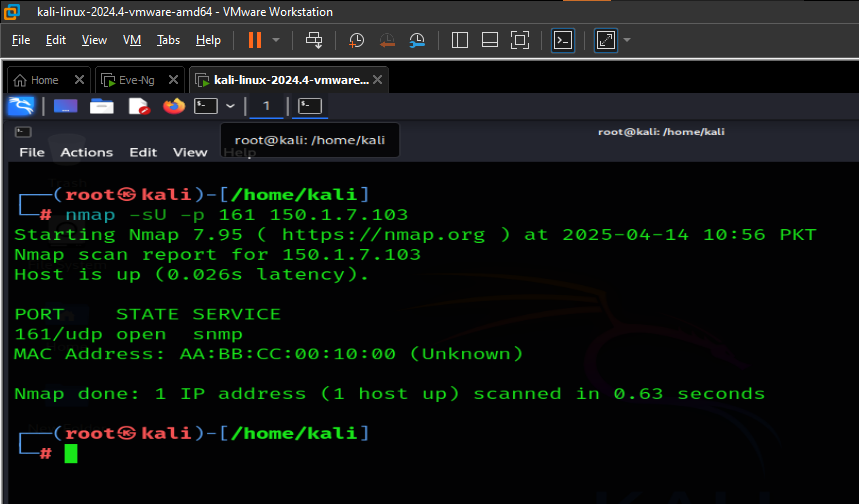
SNMP (Simple Network Management Protocol) allows extracting information from network devices — such as:

|  |  |
| --- | --- |
| Information Type | Example |
| System Info | Uptime, OS, hostname |
| Interface Info | IP addresses, MAC, status |
| Routing Table | Routes & gateways |
| User Accounts | Sometimes exposed |
| Running Services | Via SNMP OIDs |

Configure Cisco Router for SNMP (Lab Setup)



Discover SNMP Open Port Using Nmap “Nmap –sU –p 150.1.7.103”



Brute Force SNMP Community String (Nmap script) “Namp –sU –p –script=snmp-brute 150.1.7.103”

