
# Introduction to Qualys VMDR

**Notes:**

- VMDR - Vulnerability Management & Detection Response
- First, we need to discover the assets that we have and the information must be convenient / up-to-date
- The VMDR Cycle: Vulnerabilities >>> Remediation prioritization >>> Pushing info to the patching team >>> Actual Remediation
- It is essential to consider Time Take to Remediate vulnerabilities (TTR). This helps to reduce risks

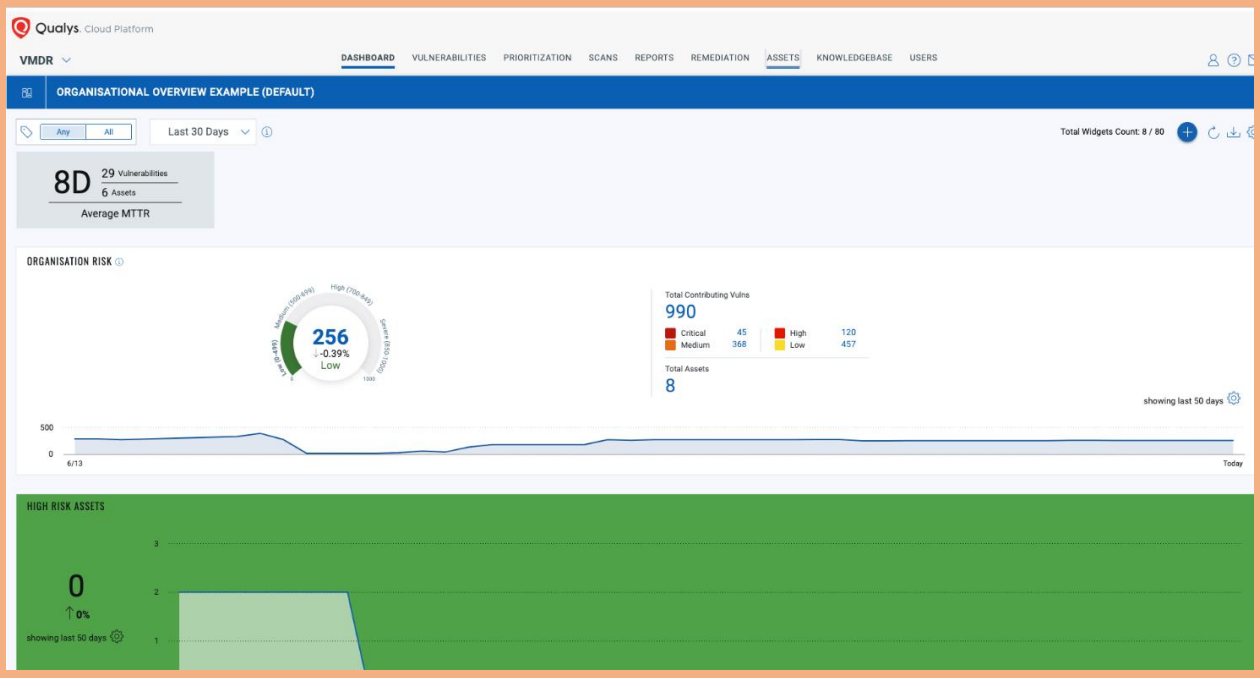
## Adding Scannable Host Lab (Step-by-step):

### Objectives:

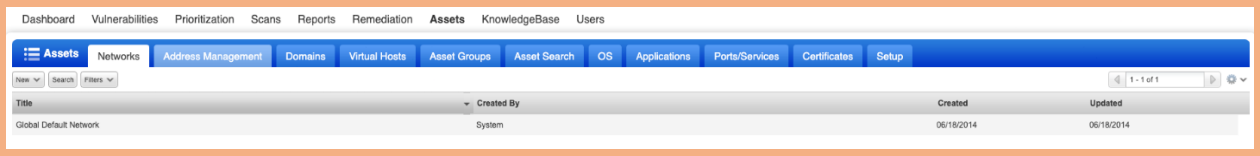
- This lab involves adding scannable host assets as IP - tracked assets
- The tracking methods impacts how the hosts will be listed in your scan

### Methodology:

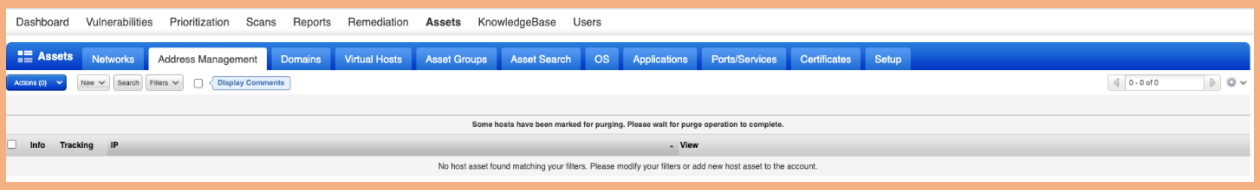
1. Click on the **'Asset'** section



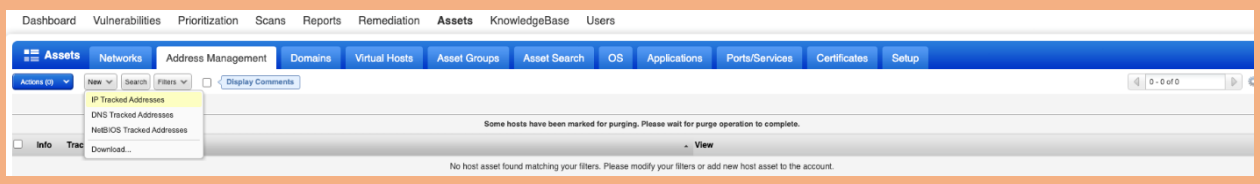
2. Click the **'Address Management'** Tab



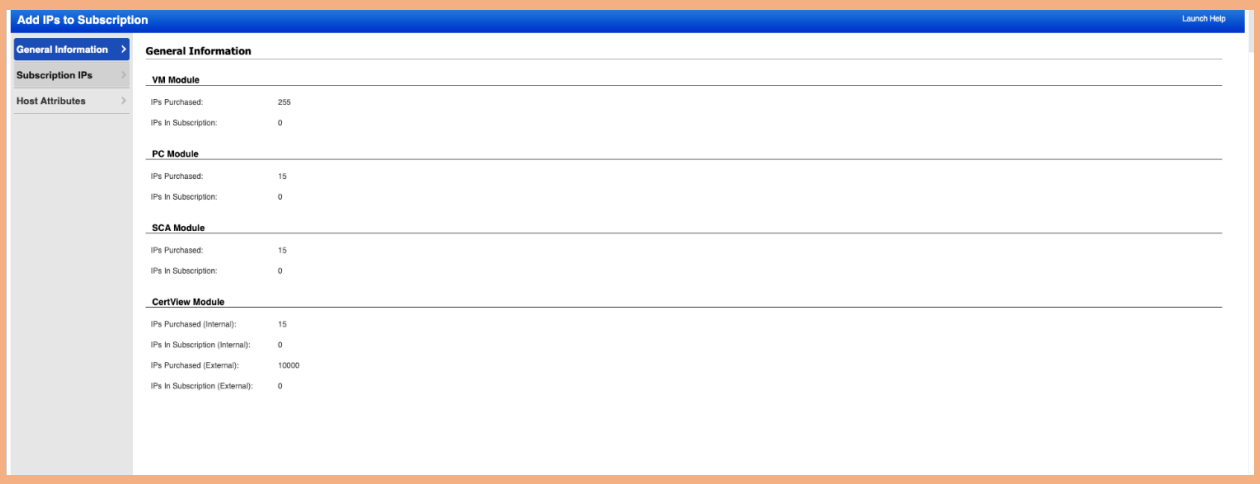

3. Click on the **'New'** button



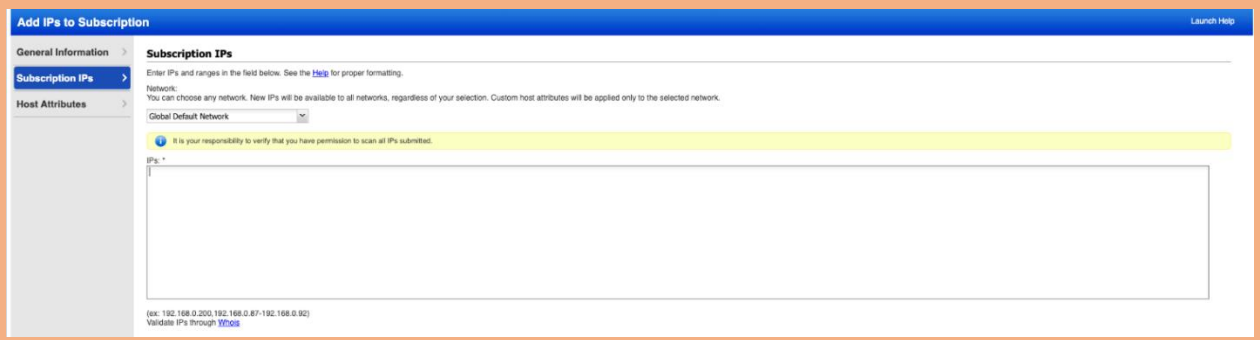

4. Click the drop-down button **'IP Tracked Address'**



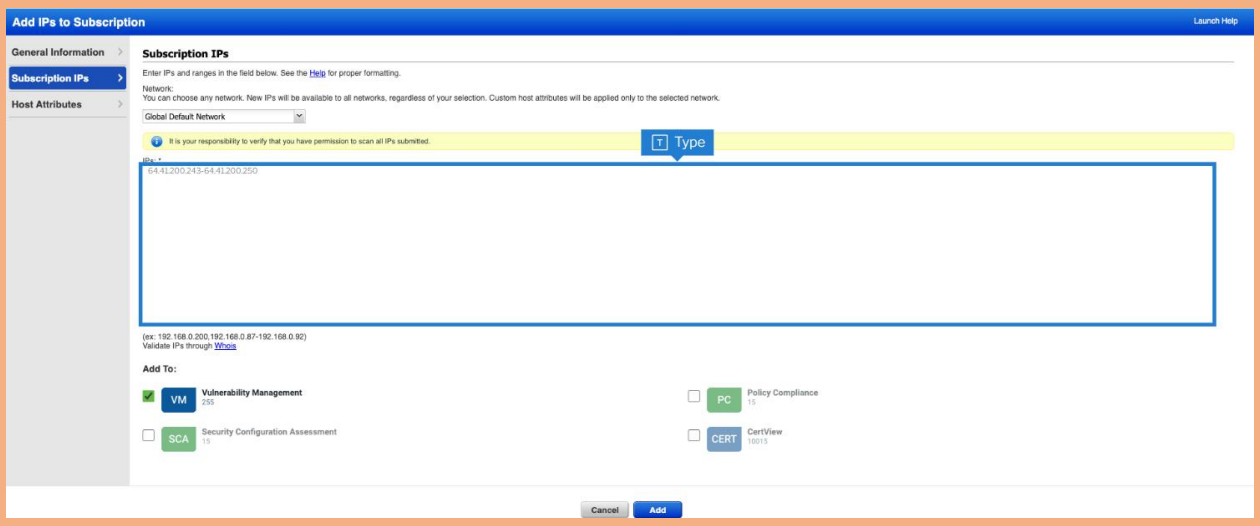

5. Click the **'subscription IPs'** tab



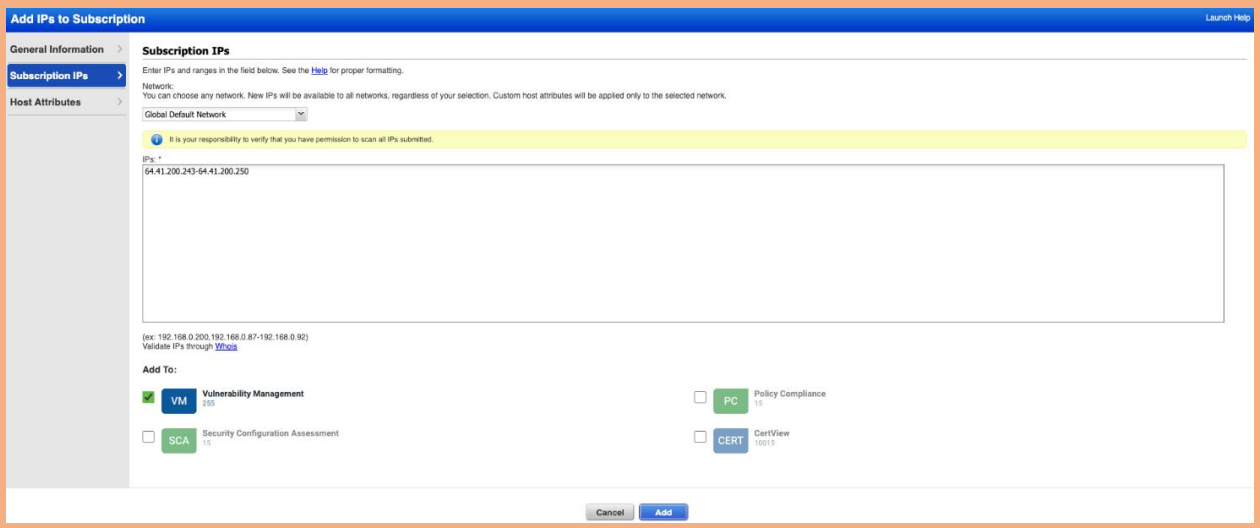

6. Click on the **'IP field'** and type **64.41.200.243.61.41.200.250**



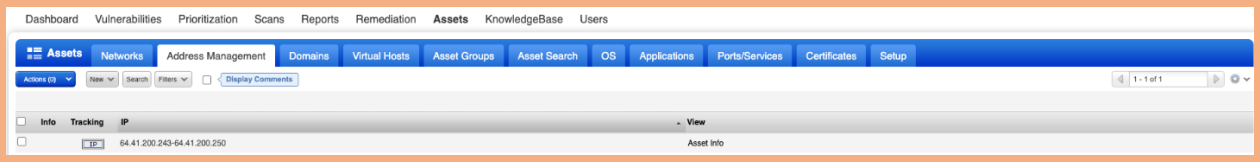
7. You can select any of the below tabs: (However in this case, select the **'VM'** tab and click the **'Add'** button):
    - **VM:** Vulnerability Management
    - **SCA:** Security Configuration Assessment
    - **PC:** Policy Compliance
    - **CERT:** View Certificate



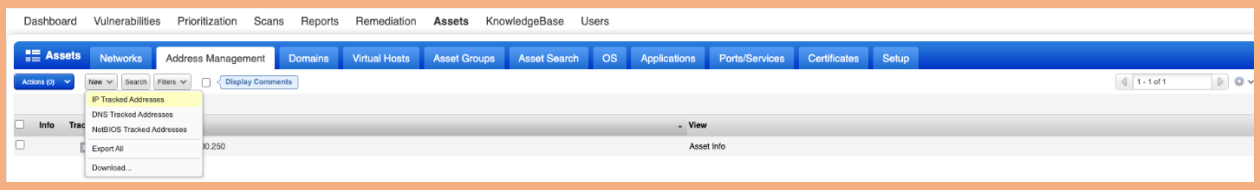

8. Confirm if a range of IP Addresses have been added. Hence you can click the **'New'** tab



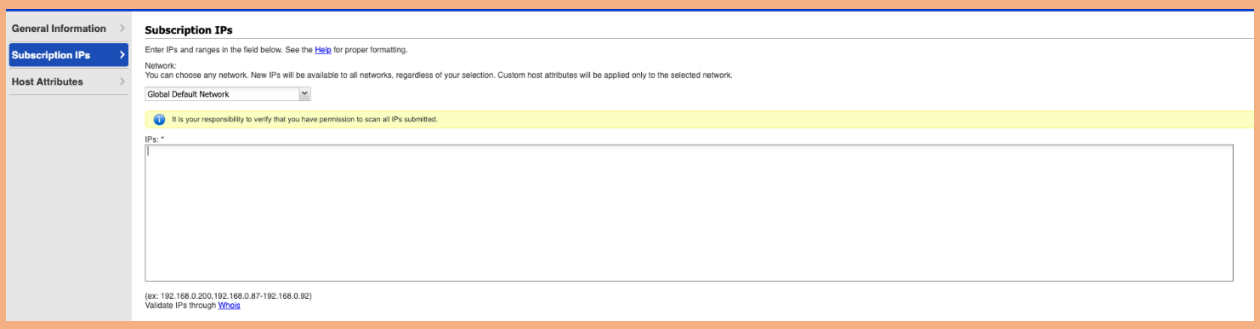
9. Click **the 'IP Tracked Addresses'** tab



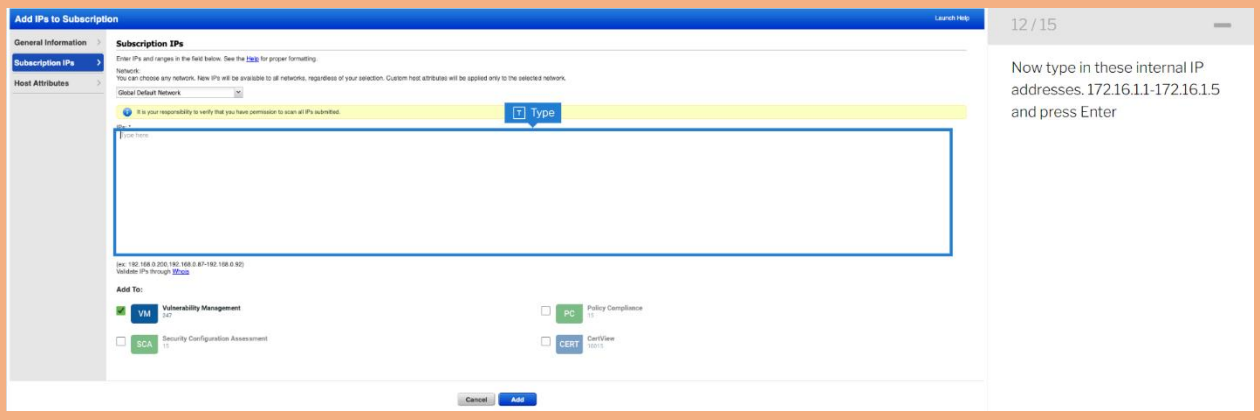

**10.** Click the **'IPs field'**



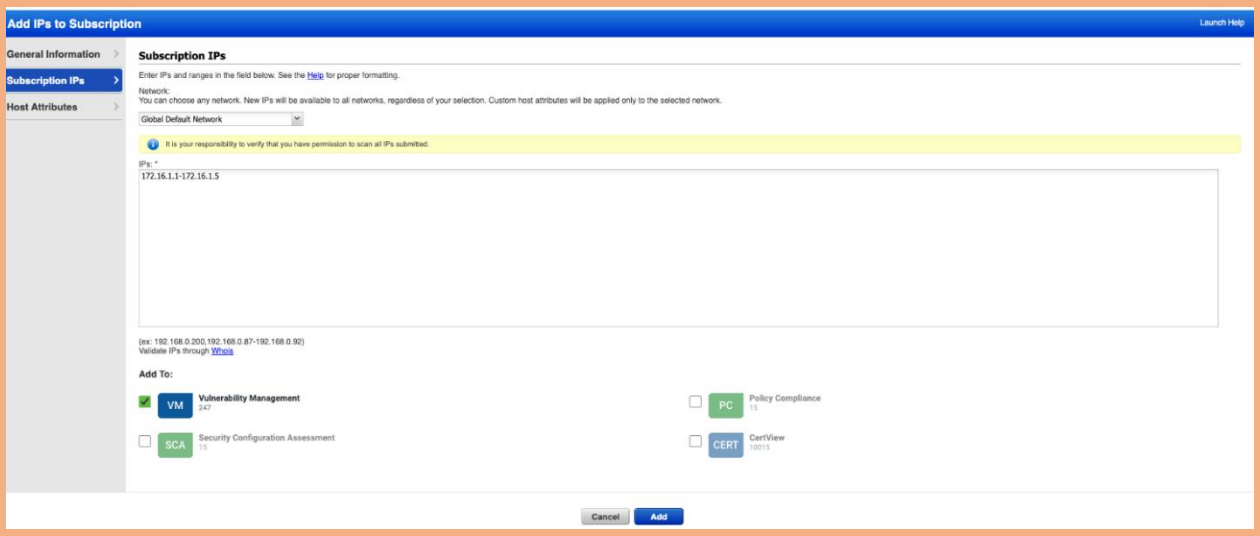

**11.** Type in this internal IP Addresses **172.16.1.1-172.16.1.5** and press **'Enter'**



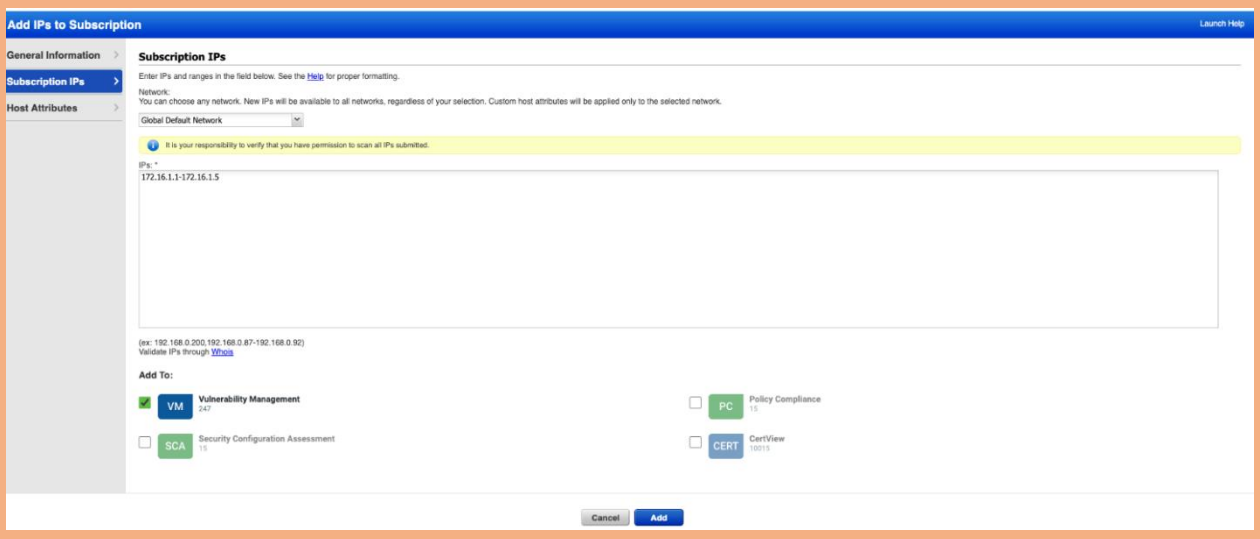

12. Click the **'Add'** button



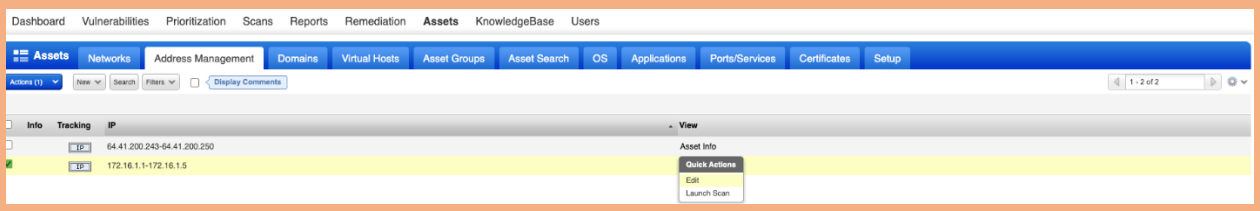
13. Confirm if a range of IP Addresses have been added




14. In the IP Asset **172.16.1.1-172.16.1.5**, click the drop-down button **'Asset Info'**




**15.** Confirm that you can see the button **'Launch scan'**



## Results:

1) A range of IP Addresses were added:

- 172.16.1.1-172.16.1.5
- 64.41.200.243.61.41.200.250

2) We could also run other activities apart from the **'VM'**- Vulnerability Management which include:

- **VM:** Vulnerability Management
- **SCA:** Security Configuration Assessment
- **PC:** Policy Compliance

3) CERT: View Certificate

## Conclusion:

Upon adding IP Addresses, we can:

- Perform Vulnerability Management
- perform Security Configuration Assessment
- Apply relevant Compliance policies
- view certificates