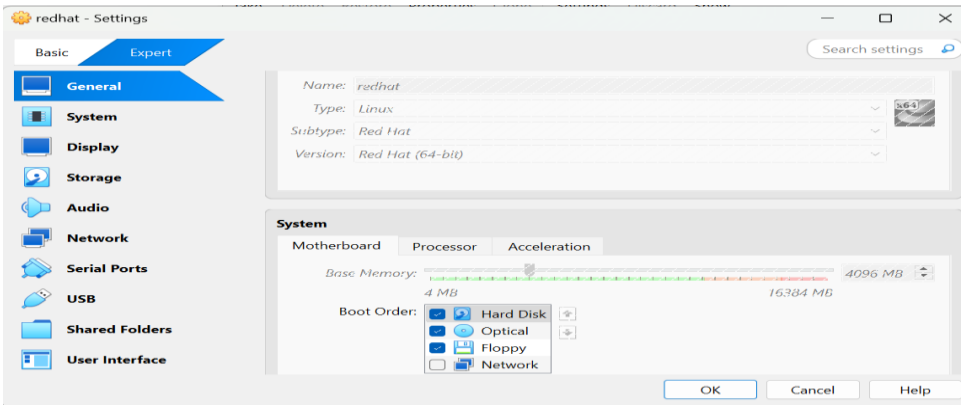
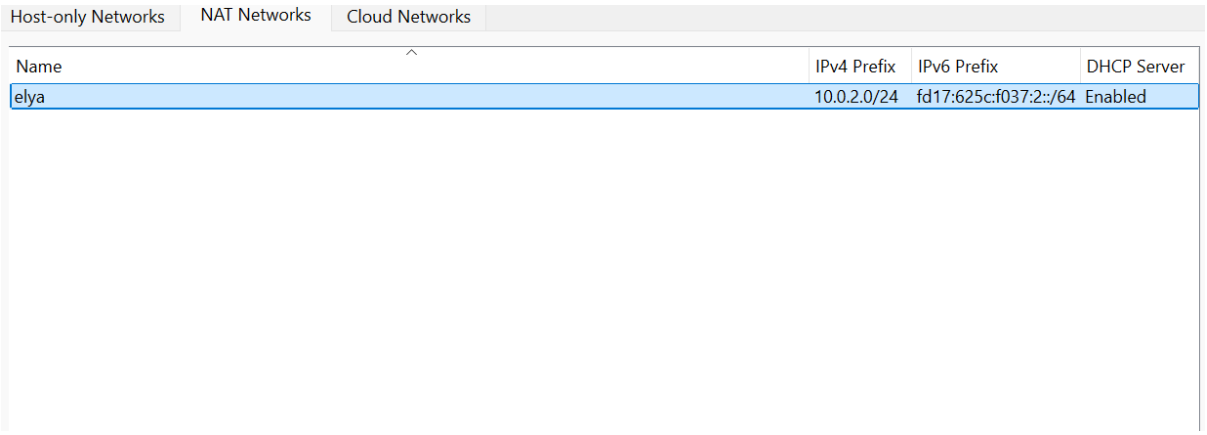
🛠️ Cybersecurity Lab: Day 1 — Red Hat Server Setup

✅ Objectives Completed:

1. **Red Hat Server Installation**
    - Installed Red Hat on VirtualBox.
    - Allocated proper storage, RAM, and network settings.



➢ Configured nat network for my server, kali machine and wazuh



2. Configured Apache Web Server

- Installed Apache using sudo yum install httpd.

  sudo systemctl enable httpd

  sudo systemctl start httpd

- Enabled and started Apache:
- Verified by visiting the server's IP via a browser (served Apache test page), using both the loopback address and another machine on the same nat network.

3. Enabled SSH Access
   sudo systemctl enable sshd
   sudo systemctl start sshd

➢ Verified remote access via: ssh username@<ip address of the server>

4. **Configured Firewall Rules**

   Opened Apache and SSH ports and allowed traffic through the firewall

   sudo firewall-cmd --permanent --add-service=http
   sudo firewall-cmd --permanent --add-service=ssh
   sudo firewall-cmd –reload

5. **Enumerated the web server using nikto on my kali machine**
   Reconnaissance and Vulnerability Scanning
   - Used nmap to identify open ports (22, 80, 443).
   - Ran **Nikto** to identify server misconfigurations and potential vulnerabilities.
     1. E.g., missing security headers, HTTP TRACE enabled, outdated modules, directory listing.

🔍 **Vulnerabilities Identified**

- Missing headers (X-Frame-Options, X-Content-Type-Options).
- HTTP TRACE enabled (can be abused via Cross-Site Tracing).
- Directory indexing exposed (/icons/, /manual/).
- Outdated mod_fcgid.

6. **Harden server**
   - Disable TRACE, directory indexing.
   - Add missing headers in Apache config.
   - Restrict access to sensitive directories/files.