[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@4c5f7de7100d4c5d80f34726cfa25da9?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

Port Scanning Using Netcat

**Use the nc command to scan for open ports.**

1. Run nc on device 2 to listen on port 1234:

nc -lkv 1234



The -k option ensures the connection stays open after a disconnect.

2. Run the following command on device 2 to check whether port 1234 is open:

nc -zv 10.0.2.4 1234



If the port is open, the output shows a successful connection message.

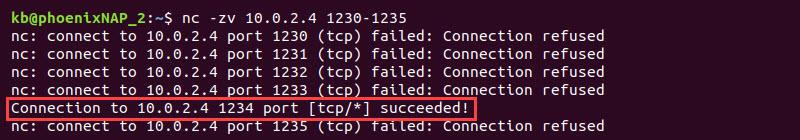
3. Alternatively, scan multiple ports on device 2 by adding a port range. For example:

nc -zv 10.0.2.4 1230-1235

If the port is open, the output shows a successful connection message.

3. Alternatively, scan multiple ports on device 2 by adding a port range. For example:

nc -zv 10.0.2.4 1230-1235



The output shows whether the connection is successful or not for each port.

4. When scanning for port ranges, filter the results using [grep](https://phoenixnap.com/kb/grep-command-linux-unix-examples):

nc -zv 10.0.2.4 1230-1235 2>&1 | grep 'succeeded'



For example, grepping for the word succeeded only shows open ports in the output.