Task 3: Perform a Basic Vulnerability Scan on Your PC

Objective: Use free tools to identify common vulnerabilities on your computer.

Tools Used: Nessus Essentials.

Vulnerability Report

1. **Vulnerability Title:** IP forwarding

   Severity: Medium

   Description: The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

   Unless the remote host is a router, it is recommended that you disable IP forwarding.

   Recommendation: On Linux, you can disable IP forwarding by doing:

   echo 0 > /proc/sys/net/ipv4/ip_forward

   On Windows, set the key 'IPEnableRouter' to 0 under

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

   On Mac OS X, you can disable IP forwarding by executing the command:

   sysctl -w net.inet.ip.forwarding=0

   For other systems, check with your vendor.

2. **Vulnerability Title:** Outdated OpenJDK Version

   Severity: Medium

   Description: The version of OpenJDK installed on the remote host is 8 prior to 8u432 / 11.0.0 prior to 11.0.25 / 17.0.0 prior to 17.0.13 / 21.0.0 prior to 21.0.5 / 23.0.0 prior to 23.0.1. It is, therefore, affected by a vulnerability as referenced in the 2025-01-21 advisory.

   Recommendation:
   1. The installed OpenJDK version is outdated and contains multiple security vulnerabilities.
   2. Upgrade to a supported version: 8u432 / 11.0.25 / 17.0.13 / 21.0.5 / 23.0.1 or later.
   3. Regularly check for security patches and keep Java up to date to prevent exploits.

3. **Vulnerability Title:** DHCP Information Disclosure

   Severity: Low

   Description: This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout. Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on. It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network

   Recommendation: Apply filtering to keep this information off the network and remove any options that are not in use.

Screenshot of Nessus output for findings: