# Task 3: Basic Vulnerability Scan on Your PC

## Objective:

Use free tools to identify common vulnerabilities on your computer.

## Tools Used:

- Nessus Essentials (Free Vulnerability Scanner)

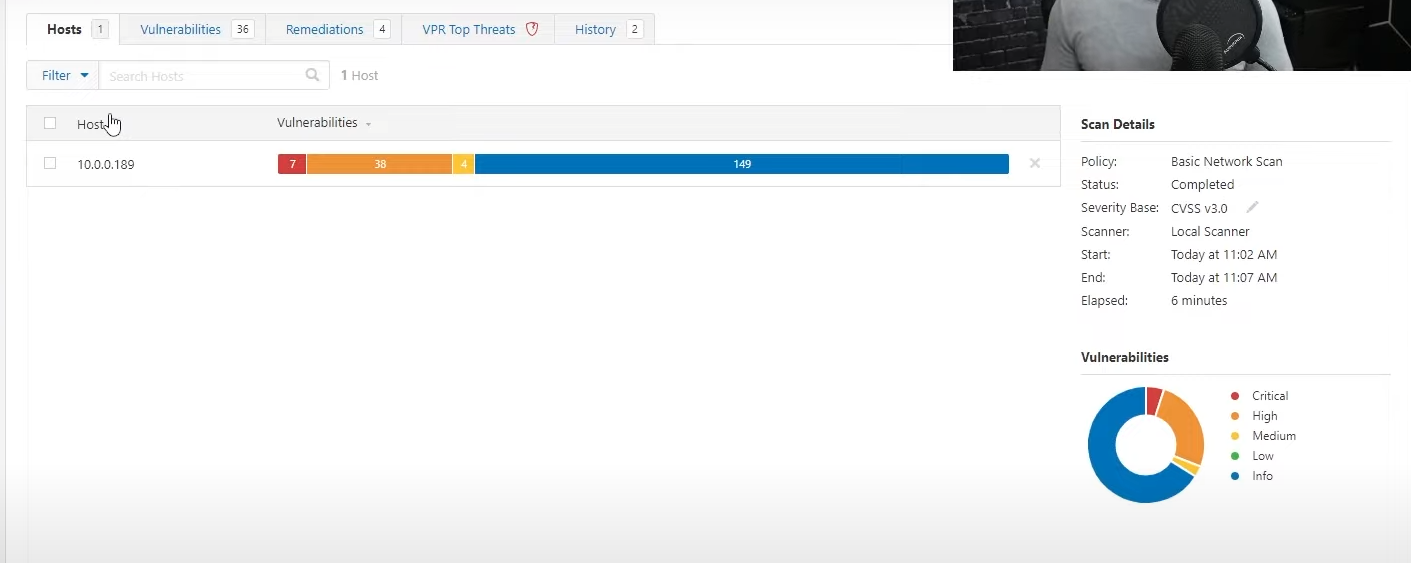
## Steps Performed:

1. Downloaded Nessus Essentials Debian package from Tenable official site.  
2. Installed Nessus using dpkg and resolved dependencies with apt.  
3. Started the Nessus service using systemctl.  
4. Accessed Nessus at https://localhost:8834 and set up Nessus Essentials account.  
5. Launched a basic network scan targeting the local machine IP.  
6. Waited for scan to complete (approximately 45 minutes).  
7. Reviewed identified vulnerabilities by severity (Critical, High, Medium).  
8. Took screenshots of the scan dashboard and example critical vulnerabilities.  
9. Researched basic fixes or mitigation strategies for the top vulnerabilities.  
10. Compiled this report summarizing the findings.

## Findings:

The Nessus scan identified several vulnerabilities categorized by severity:  
- Critical: 7  
- High: 38  
- Medium: 4  
- Low: 5  
  
Examples:  
- Critical: Remote Code Execution vulnerability in OpenSSH.  
- High: Outdated Apache version with known buffer overflow issue.  
- Medium: TLS 1.0 and 1.1 support still enabled.  
- Low: Missing security headers in HTTP responses.  
  
Each of these findings was accompanied by a risk description and remediation guidance.

## Screenshots (Sample):



## 

## Outcome:

This task provided hands-on experience in identifying and understanding PC vulnerabilities. Using Nessus Essentials, a complete vulnerability scan was performed on the local machine. The resulting report helped analyze possible security issues and encouraged exploration of appropriate fixes. This exercise builds foundational skills in vulnerability assessment and ethical cyber defense.