Nessus Essentials Diagnostic Report

Step 1: Install Nessus Essentials

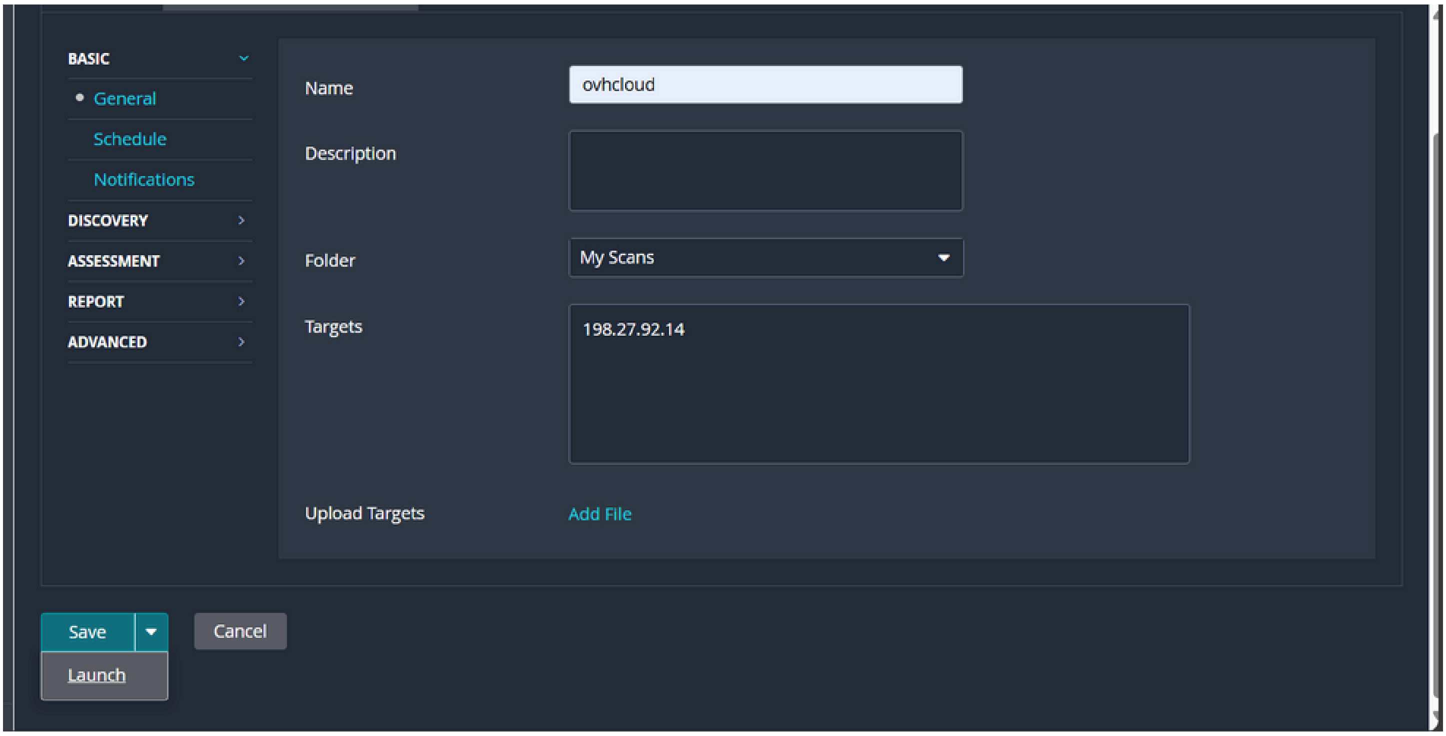
- Go to: https://www.tenable.com/products/nessus/nessus-essentials
- Register for a free activation code.
- Download the installer for your OS (Windows/Linux/Mac).
- Install Nessus and enter the activation code when prompted.

Step 2: Set up a Localhost Scan

- After installation, access Nessus via your browser at https://localhost:8834
- Login with the credentials you created.
- Create a **New Scan → Advanced Scan**.
  - **Name**: Localhost Vulnerability Scan
  - **Targets**: 198.27.92.14
- Save the scan.

Step 3: Run the Scan

- Click on your scan → Click **Launch**.
- Wait for it to complete (usually 30–60 minutes).



Name: ovhcloud

Description:

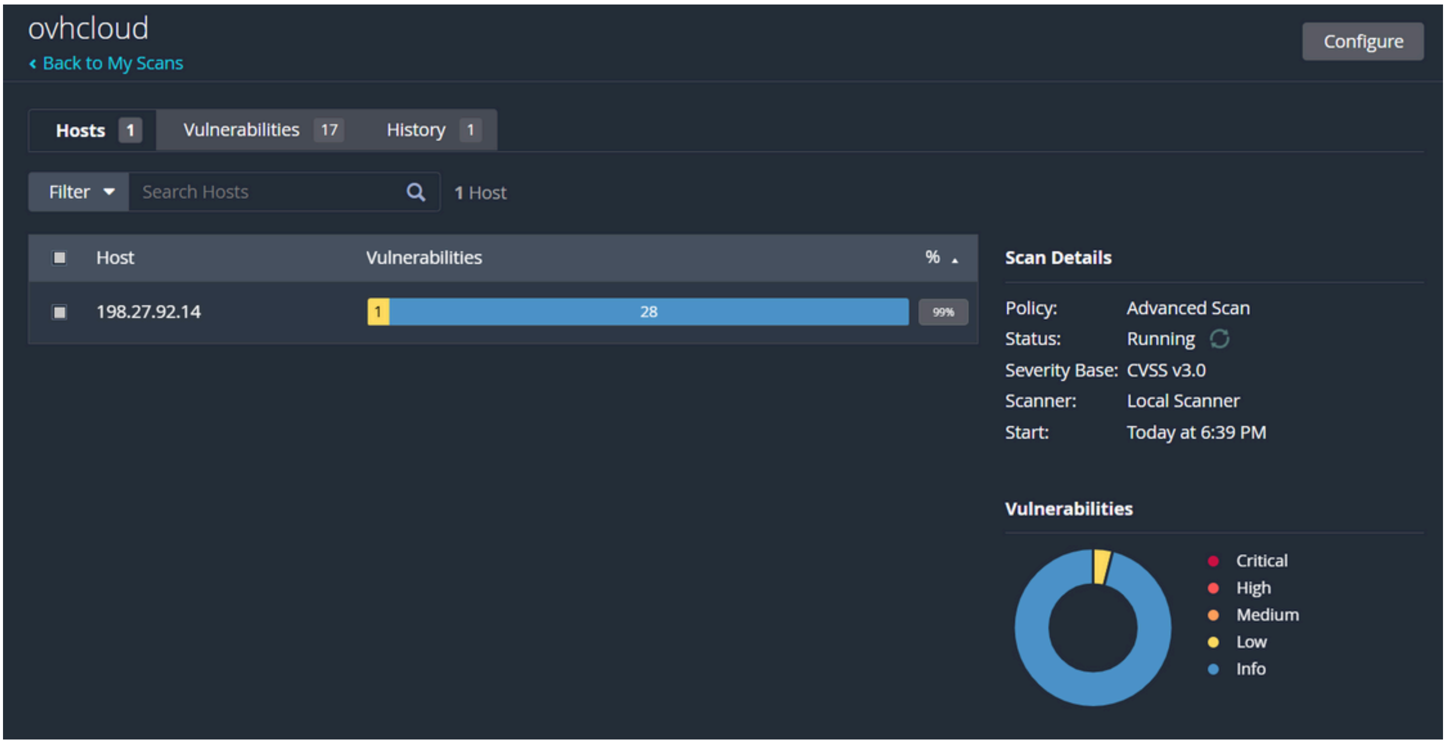
Folder: My Scans

Targets: 198.27.92.14

Upload Targets: Add File

Step 4: Review the Results

- After completion, open the scan report.
- Focus on:
  - **Critical** and **High** severity issues.
  - Plugin IDs, descriptions, CVE references.



Host	Vulnerabilities	%
198.27.92.14	1 28	99%

Scan Details

Policy:	Advanced Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:39 PM

Vulnerabilities

Step 5: Document Findings

Create a document or report including:

- A brief intro about the tool and target.
- A list of top 3–5 vulnerabilities (with:
  - Severity
  - Plugin Name
  - Description
  - Possible Fix or Mitigation)

How do scanners detect vulnerabilities?

Scanners like Nessus detect vulnerabilities by:

- **Fingerprinting the system** (OS, services, ports).
- **Comparing known vulnerabilities** (from databases like CVE, OVAL) with system configurations.
- **Sending probes or requests** to simulate attacks and check for weak or misconfigured services.
- **Matching plugins/scripts** to known vulnerabilities using version checks, file paths, and behavior.

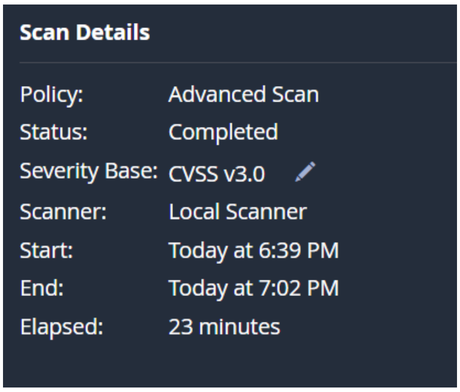
What is CVSS?

CVSS (Common Vulnerability Scoring System) is a standardized method to **evaluate the severity of a vulnerability**.

It provides a numeric score (from 0.0 to 10.0), often broken into:

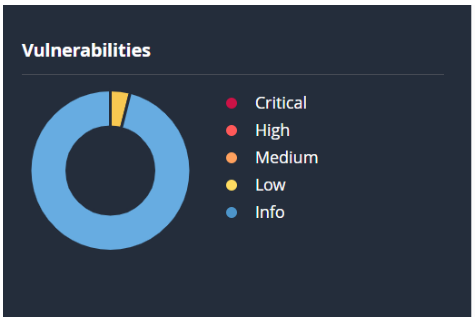
- **Base Score** (inherent risk)
- **Temporal Score** (changes over time)

- **Environmental Score** (risk in your environment)
  Example:
- **0.0–3.9** = Low
- **4.0–6.9** = Medium
- **7.0–8.9** = High
- **9.0–10.0** = Critical



Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:39 PM
End: Today at 7:02 PM
Elapsed: 23 minutes



How often should vulnerability scans be performed?

- **Monthly** at a minimum for most systems.
- **Weekly or daily** for critical or exposed systems.
- **After major changes** (e.g., new software, patching, network upgrades).
- **Before and after a security audit** or compliance assessment.

What is a false positive in vulnerability scanning?

A **false positive** occurs when the scanner **flags a vulnerability that doesn't actually exist**.
Reasons include:

- Misinterpreted system data
- Inaccurate plugin detection
- Non-standard configurations
  False positives waste time and reduce trust in scan results, so manual verification is important.

How do you prioritize vulnerabilities?

Vulnerabilities are prioritized based on:

- **CVSS score** (severity)
- **Asset importance** (e.g., critical servers, production systems)
- **Exploit availability** (is an attack tool publicly available?)
- **Exposure** (internal vs. internet-facing)

- **Business impact** (data loss, downtime, regulatory risk)
  Use a **risk-based approach**: patch high-severity vulnerabilities on high-value assets first.

Conclusion

Your Nessus Essentials installation is **successfully licensed and connected** to the plugin server, but it is currently **failing to download essential components and plugins** due to network-related issues. These failures are most likely caused by:

- Firewall or antivirus blocking connections
- Network proxy or DNS configuration issues
- Lack of administrative privileges

To resolve the issue, ensure Nessus has full internet access, temporarily disable security filters if needed, and run Nessus as Administrator. Once plugin downloads complete successfully, scanning functionality will be fully operational.

If problems persist, offline update methods or reviewing firewall/proxy settings is advised.