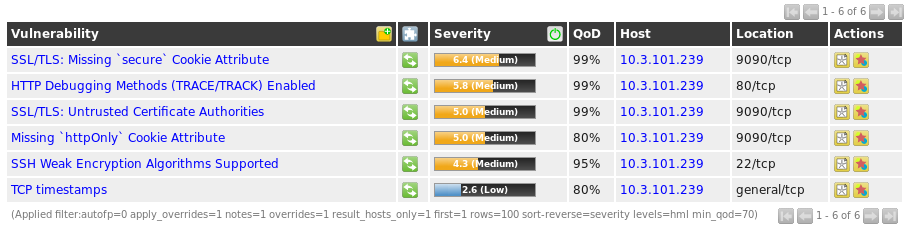
Results from OpenVAS:

Once you have run VA scans in OpenVAS, you need to interpret the data for your client. This involves:

* Specifying a CVSS cutoff value (i.e. ignore anything under 5)
* Organizing results by service/port
* Adding the “best” hyperlink to the action required (click on each result to see the available options)
* Specifying the priority (so the client knows which are more important)

For these two OpenVAS reports:

**System1:**



**System2:**



You could summarize (and provide hyperlinks) to the vulnerabilities with a CVSS > 5.0. You can find the hyperlinks you can copy and paste into your report by clicking on the Vulnerability name in the output above. There will be several hyperlinks listed - you only need to copy one hyperlink into your report. Select Microsoft KB articles where appropriate, or a link that describes the actual vulnerability and fix – if none of those apply, choose the link to the CVEs. Following is what a sample report would look like:

Vulnerability Assessment for XXXXX Organization:

**General Notes:**

* Only severity (CVSS) levels 5 and higher are included in our assessment
* Severity levels range from low (1) to high (10)

**System 1 (Fedora 29, 10.3.101.239) Vulnerable Services:**

Cockpit/zeus-admin (:9090)

* Missing secure cookie attribute (hyperlink to OWASP site identifying the vulnerability and actions to fix) - Severity=6.4
* Missing httpOnly cookie attribute (hyperlink to OWASP site identifying the vulnerability and actions to fix) - Severity=5
* Untrusted (self-signed) SSL/TLS certificate (replace with CA-signed certificate) - Severity=5

Apache (:80)

* HTTP Debugging enabled (hyperlink to OWASP site) - Severity=5

**System 2 (Windows Server 2012 R2, 10.3.101.204) Vulnerable Services:**

SMB (:445)

* Multiple core vulnerabilities (hyperlink to KB article from Microsoft listing update needed) - Severity=9.3

IIS (:80/443)

* Remote code vulnerabilities (hyperlink to KB article from Microsoft listing update needed) - Severity=10
* Vulnerable 3DES cipher used (hyperlink to the 2 CVEs) - Severity=5

MS RPC (:135)

* Enumeration enabled (prevent access to :135 on external firewalls) - Severity=5

Reference :google