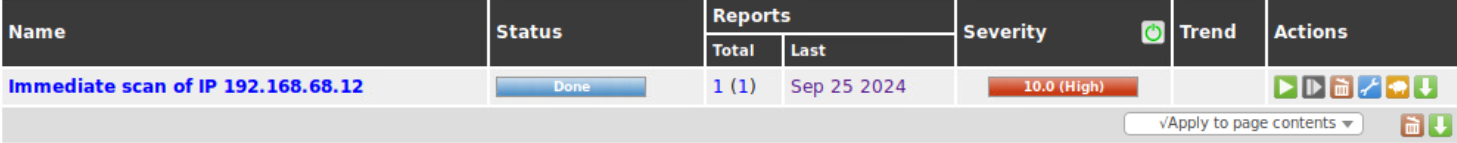
**Section 2, Step 6** – Take a Screenshot of the full report produced by the OpenVAS scan and paste it below:



**Questions**

1. What is the “worst” vulnerability found during this scan? How do you know it is the (or one of) the worst vulnerabilities discovered? (*Be specific as to how the severity of certain vulnerabilities can be measured and compared*) Report outdate /end of life for the GVM libraries was the worst vulnerability during this scan. The scan itself is not a security vulnerability, however it is an unstable release of the environment found. It also has a 97% quality of detection.
2. In Section 3 you were told to perform a “Full and very deep ultimate” scan of the target machine. Look over Chapter 10.9.1 of the documentation (<https://docs.greenbone.net/GSM-Manual/gos-21.04/en/scanning.html#default-scan-configurations>) for more information about this and other scan levels available.
   1. Should you run this scan against a server that your client has indicated is critical to their business functions? Why or why not? Running a full and very deep ultimate scan against a critical piece of the infrastructure is not recommended. The type of scan in question uses a lot of resources and could cause a slow down on the device being scanned or a reduction in speed of the network the scan is happening on. If the server is bottlenecked, critical services may go offline.