1.A screenshot of a computer

Description automatically generated

The SRG I used was for Microsoft Windows Server 2016. It details what should be installed and in use to create a secure Microsoft Windows Server 2016. I choose this SRG as it Windows Server is a relatively common OS for running a server

2. There are 271 rules on this specific SRG. Two vendors that make products that fulfill goals for this SRG is McAfee. and Norton. McAfee and Norton sells a anti-virus software that meets the rule V-224829 stating The Windows Server 2016 system must use an anti-virus program.

3. I found that out of all the CAT I controls out of the 26 rules there were 13 findings. There were non that were N/A. I do not have confidence in the security of the system as there were numerous findings that can impact the confidentiality, integrity and availability of the system. For example the Anonymous enumeration of shares must be restricted rule is found to be not sat. This would allow anonymous users to list shared resources and account names, would potentially effects confidentiality of the system. Structured Exception Handling Overwrite Protection (SEHOP) must be enabled rule was found to be unsat which could potentially allow for a buffer overflow attack effecting the integrity of the system. The Data Execution Prevention (DEP) must be configured to at least OptOut rule was found to be unsat, potentially leading to attackers being able to commit remote code execution which can take down the system effecting the availability.

A screenshot of a computer

Description automatically generated5.