Veritas Vulnerability Report



# NetWork Status Report

## Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Total Hosts Scanned** | 1 | **Average # of Hosts Scanned** | 1 |
| **Scan Cycle Start Date** | Dec 1 | **Scan Cycle End Date** | Dec 17 |

## Vulnerabilities

|  |  |
| --- | --- |
| **Total Critical Vulnerabilities** | 0 |
| **Total High Vulnerabilities** | 2 |
| **Total Medium Vulnerabilities** | 5 |
| **Total Low Vulnerabilities** | 1 |
| **Total Vulnerabilities** | 8 |

## To Be Corrected

|  |  |  |
| --- | --- | --- |
| **Device** | **Vulnerability** | **Severity** |
| 192.168.10.145 | The SSL certificate for this service cannot be trusted. | 6.4 |
| 192.168.10.145 | The SSL certificate chain for this service ends in an unrecognized self-signed certificate. | 6.4 |
| 192.168.10.145 | The remote service encrypts traffic using an older version of TLS. | 6.1 |
| 192.168.10.145 | The remote service encrypts traffic using an older version of TLS. | 6.1 |
| 192.168.10.145 | An SSL certificate in the certificate chain has been signed using a weak hash algorithm. | 5.0 |
| 192.168.10.145 | The remote service supports the use of medium strength SSL ciphers. | 5.0 |
| 192.168.10.145 | Signing is not required on the remote SMB server. | 5.0 |