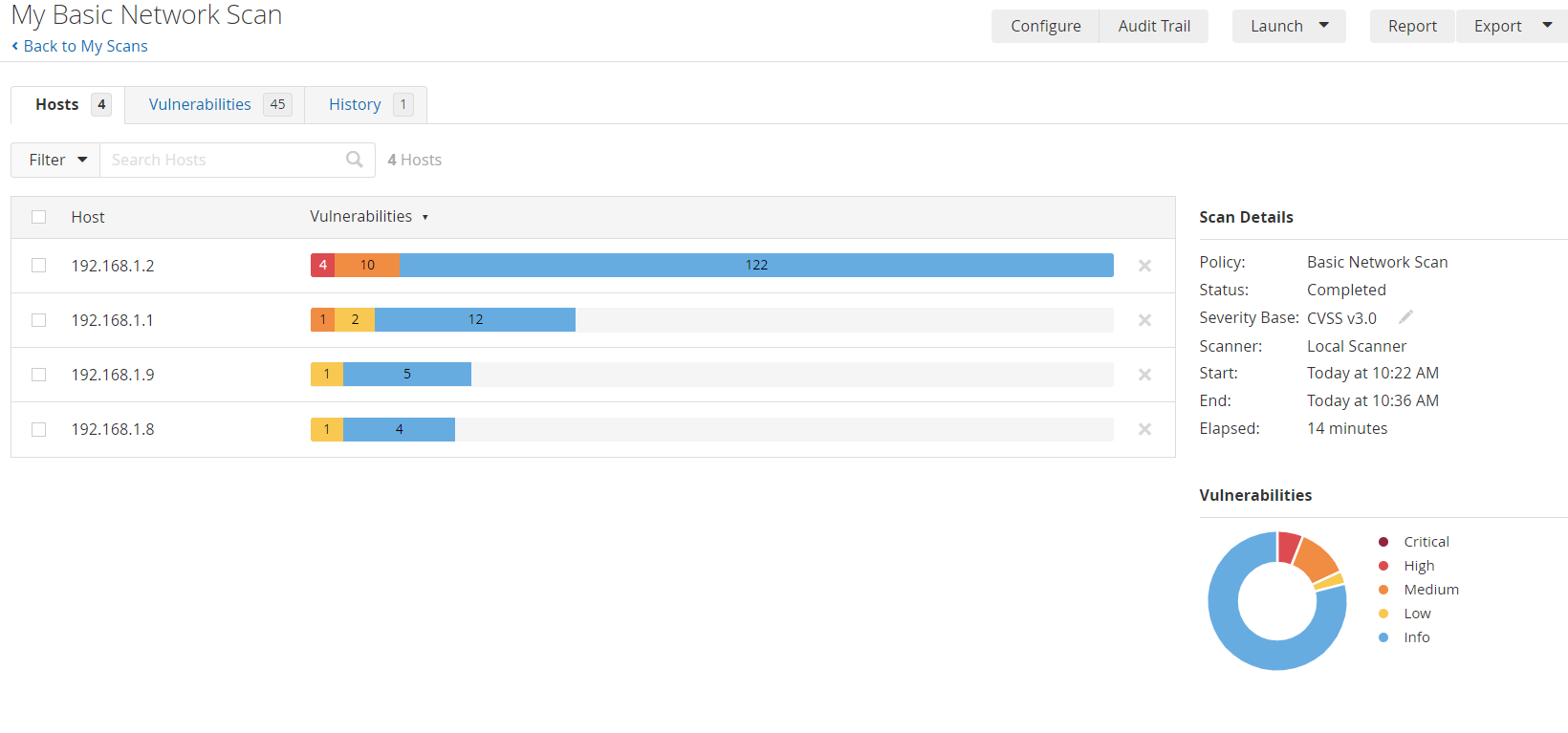
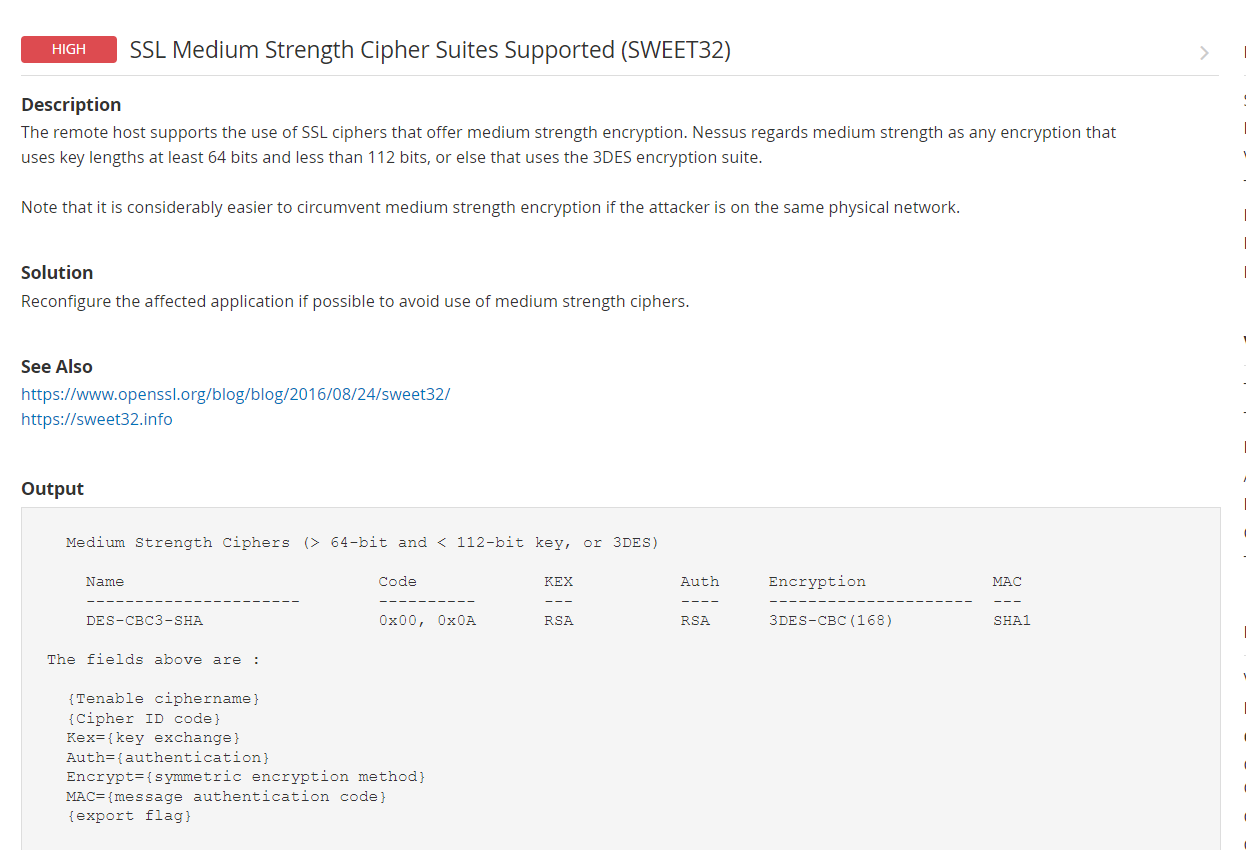
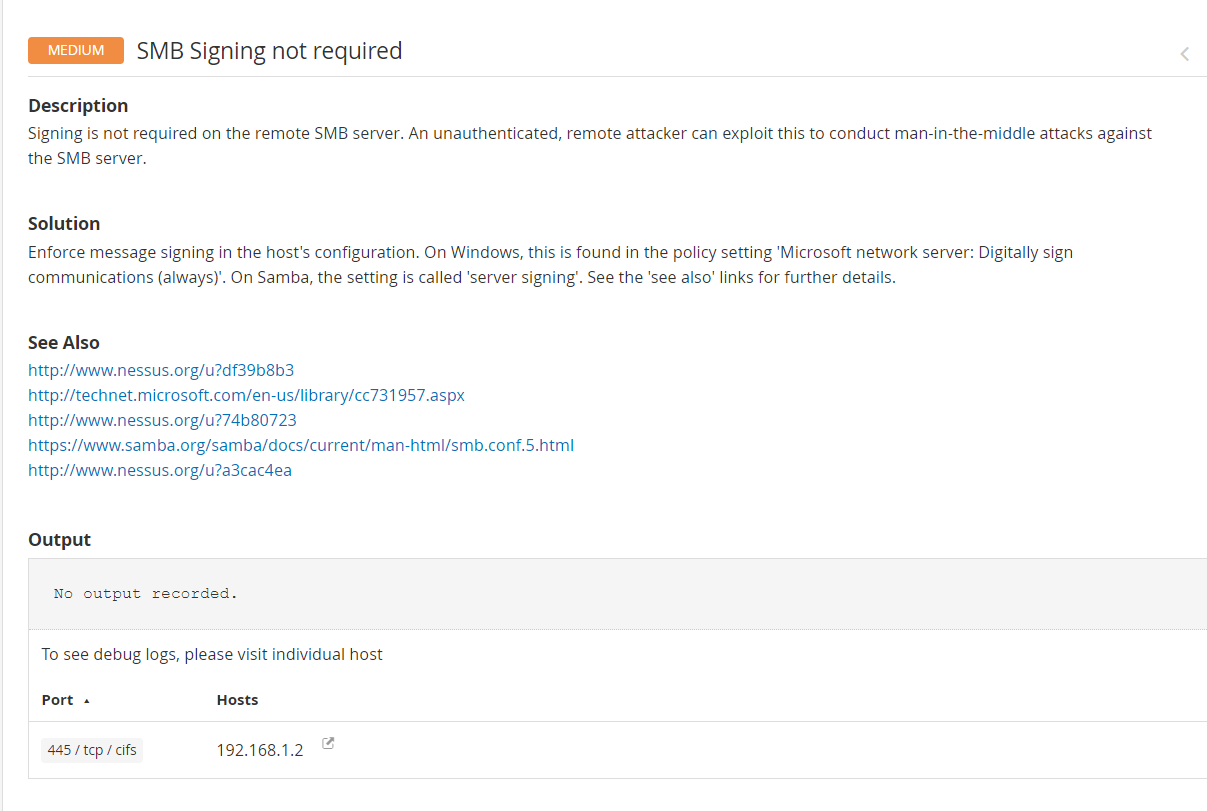
**Vulnerability assessment report**

**Using Nessus**

****

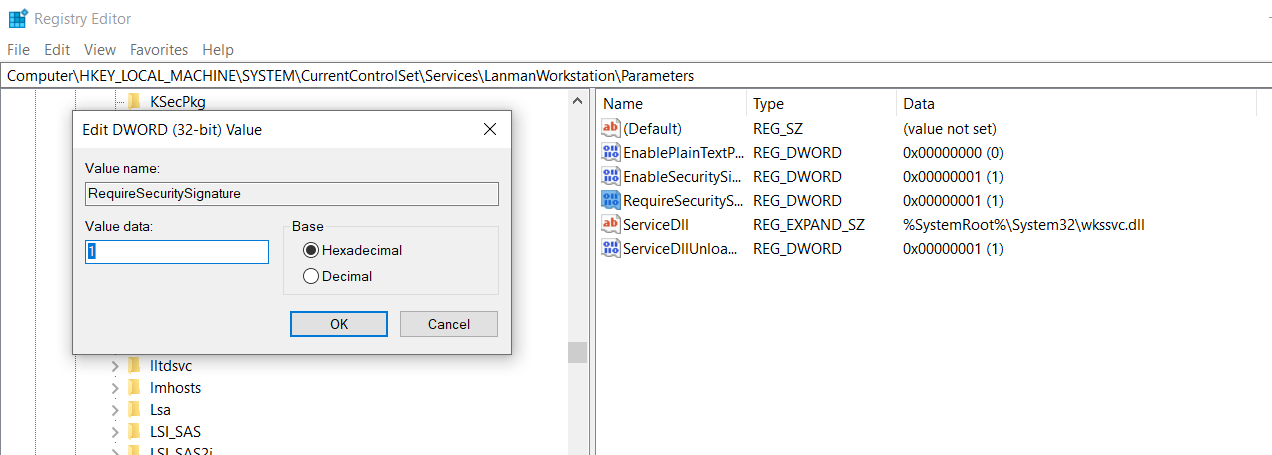
****

****

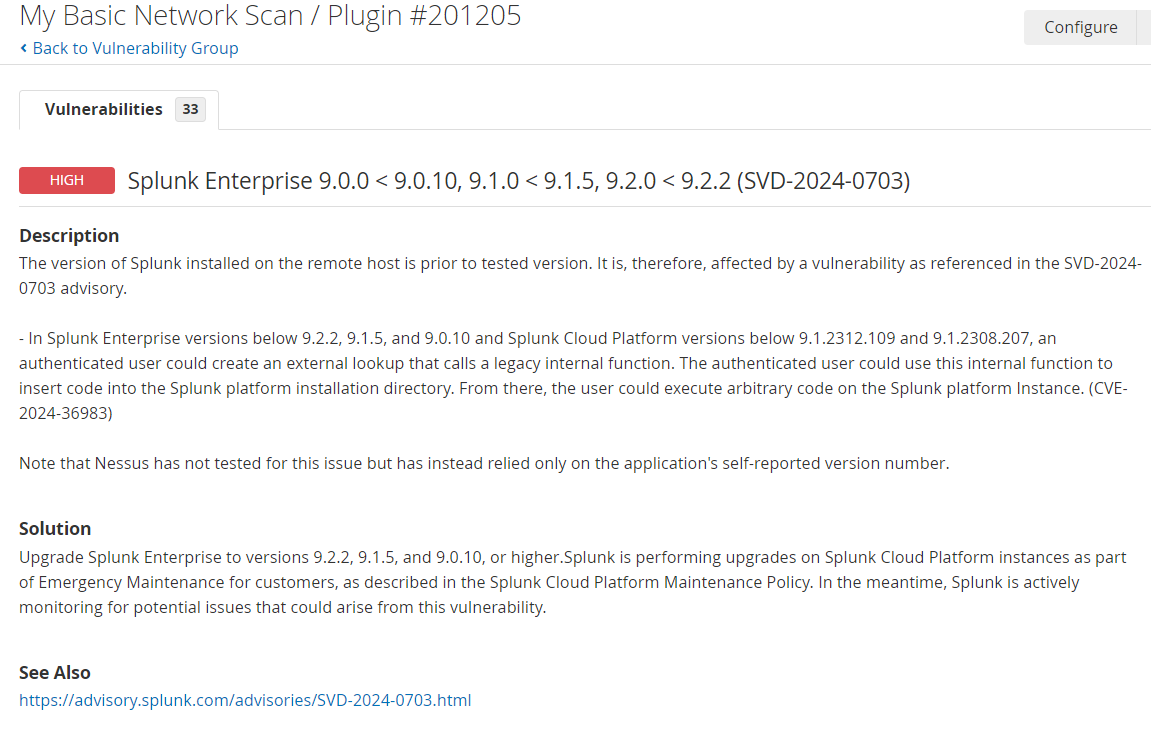
**Solution**

Registry key: HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Paramters

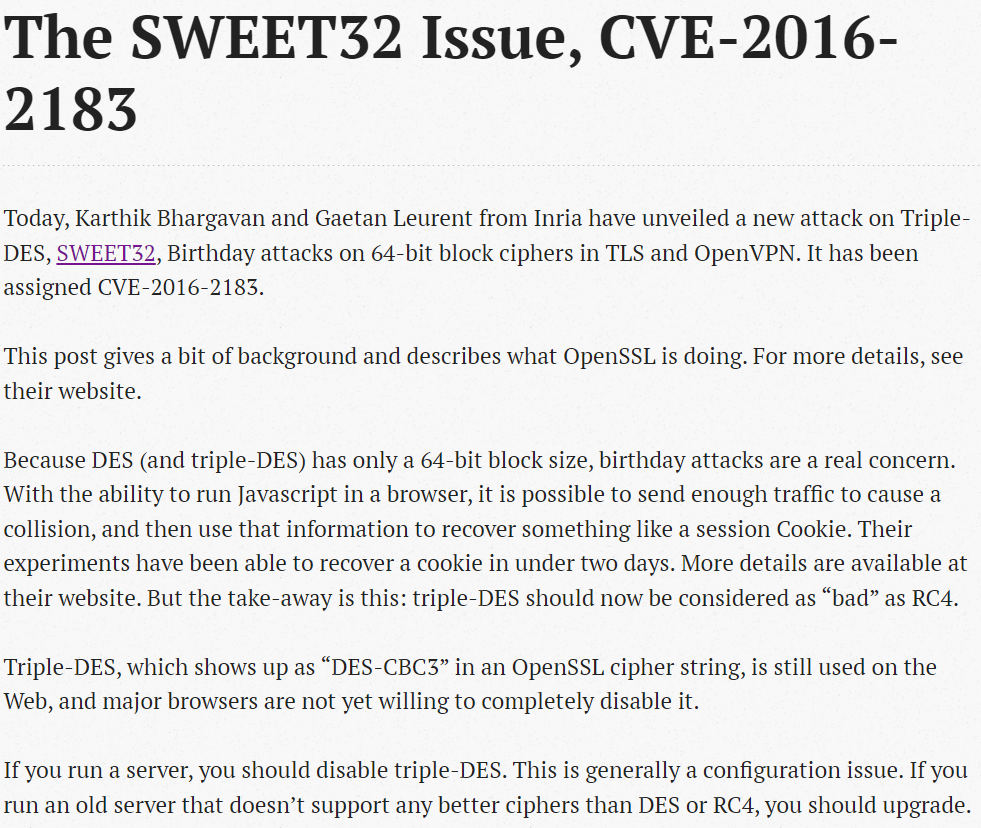
Make it 1 to be enable

****

**Always try to fix the high and critical vulnerabilities first**

****

**Upgrade to higher version of splunk cause this version indicates possible command injection**

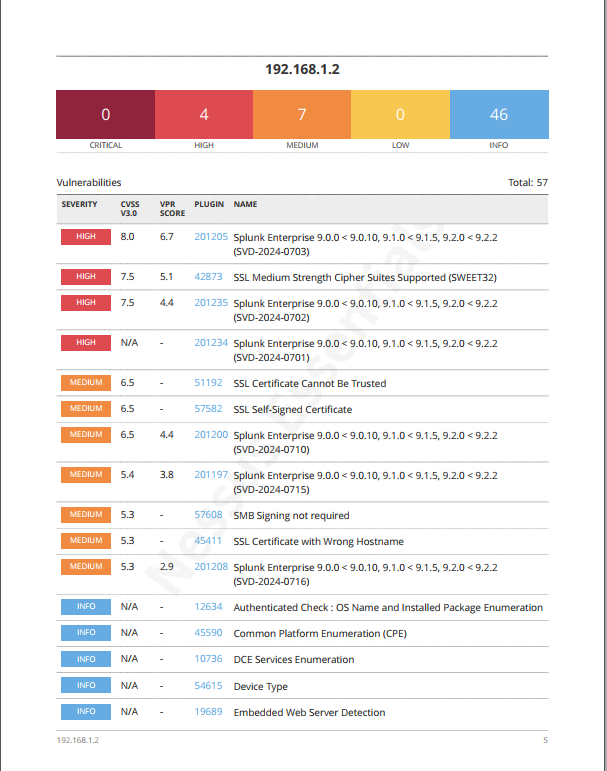
****

**Solution**

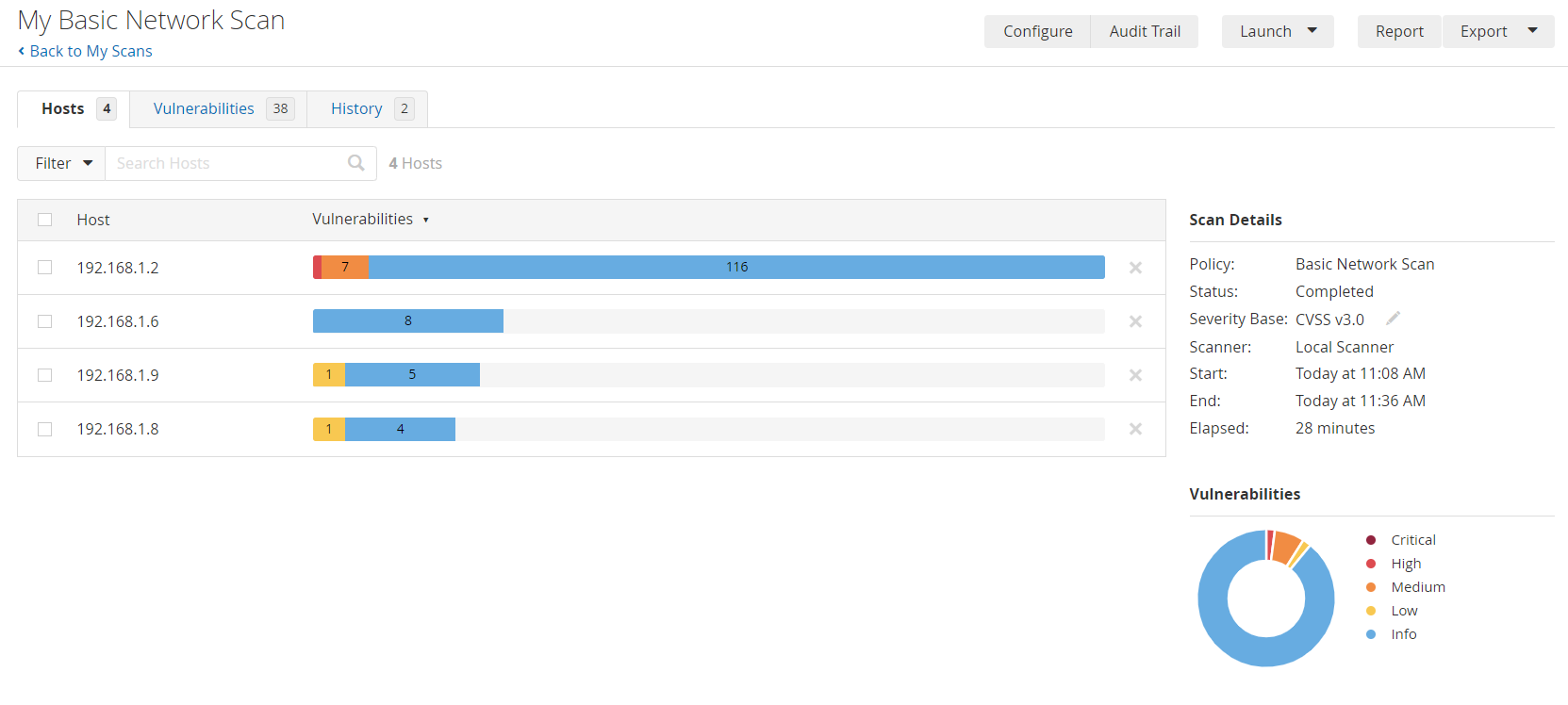
**IIS (Windows Server):**

* Open the Registry Editor (regedit).
* Navigate to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers.
* Disable weak ciphers by setting the Enabled DWORD value to 0 under the respective cipher suite.

**The generated report for the vulnerabilities before fixing the problems**

****

**After fixing some vulnerabilities**

****

**Mitigating vulnerabilities**

**Always keep system up to date**

**Access controls**

**Security Awareness and Training**

**Backup and Recovery**

**Patch Management Software:** Use tools like WSUS, SCCM, or third-party solutions to manage and automate patch deployment.

**Security Information and Event Management (SIEM):** Deploy a SIEM system to collect and analyze security event logs from across the network.