Nessus Vulnerability Scan

Project:

I performed a vulnerability scan of a temporary LAN using Nessus. First, I identified all the hosts on the network, next I identified the most consequential vulnerability found. Lastly, I remediated the vulnerability.

Identify All Hosts on the LAN:

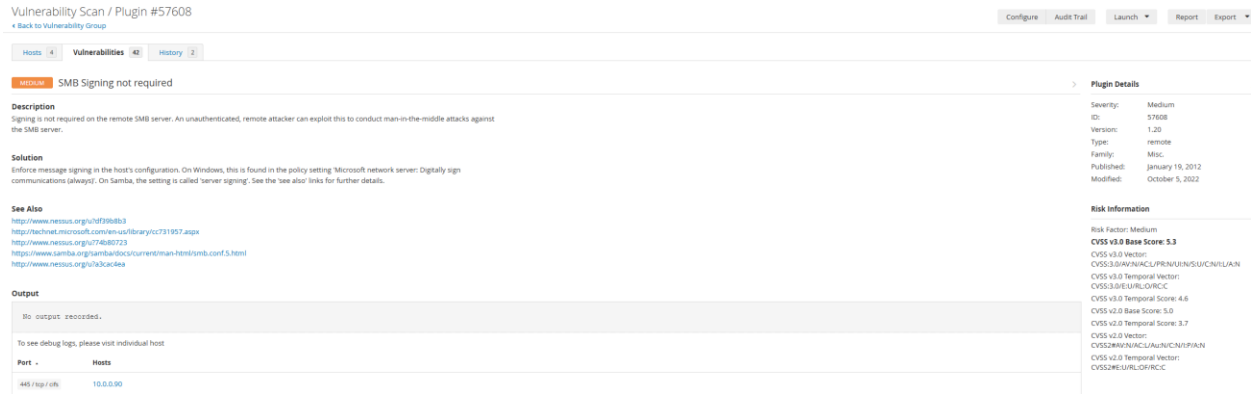
I identified 4 hosts on the LAN, with 42 vulnerabilities as detailed in Figure 1.

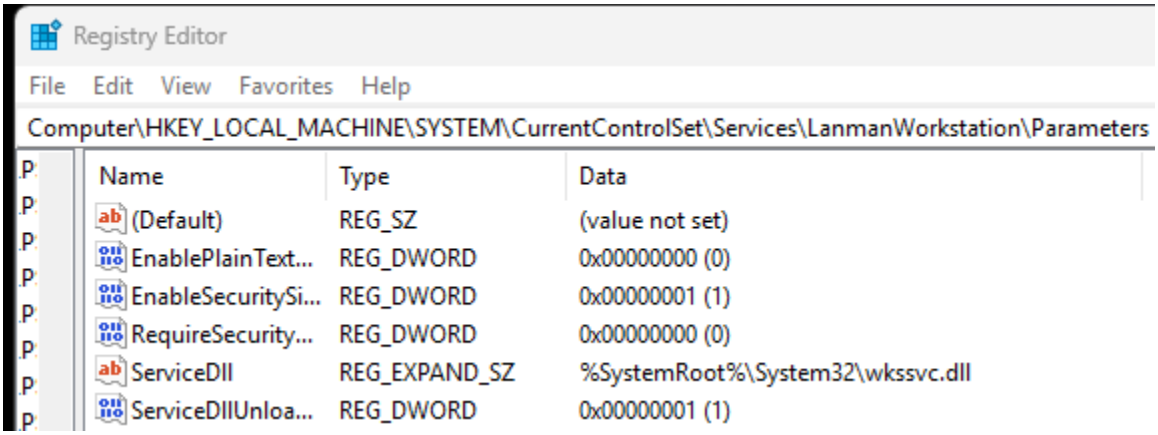
Figure 1: All Hosts Identified by Nessus

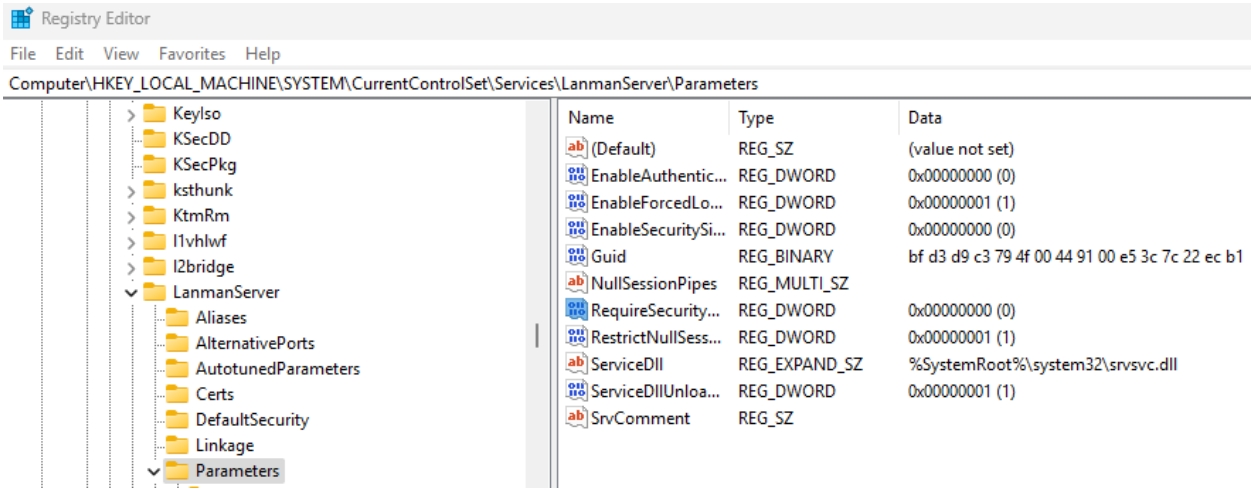
Investigate the Most Significant Vulnerability:

The most significant vulnerability found among network hosts is a server message block (SMB) related issue, with a CVSS score of 5.3, shown in Figure 3. The vulnerability occurs when digital signing is not required on the remote server message block (SMB) server; thereby creating a situation where an unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. I used the registry editor to locate the SMB signing registry parameters for both ‘LanmanWorkstation’ (client) and ‘LanmanServer’ (server), shown in Figures 4 and 5.

Figures 3, 4, 5: Nessus Scan Showing SMB Vulnerability, and Registry Editor SMB Parameters





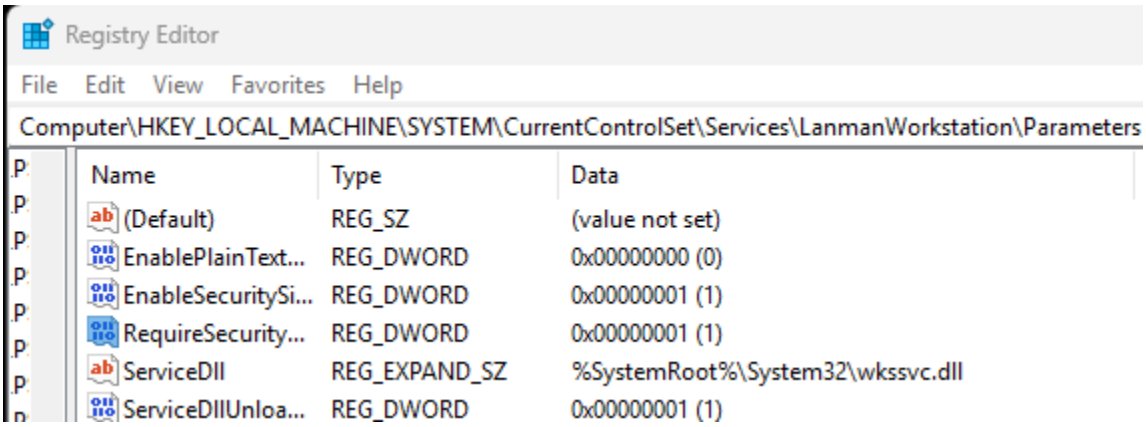


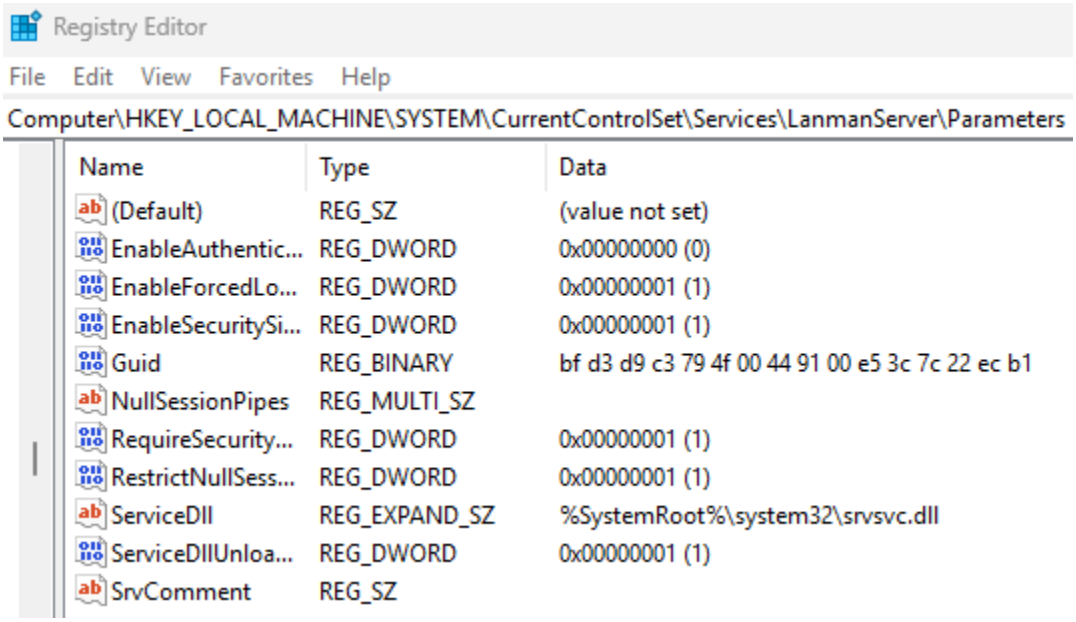
To remediate this vulnerability, I enabled the ‘RequireSecuritySignature’ function in the ‘LanmanWorkstation’ domain and, I enabled the ‘RequireSecuritySignature’ and ‘EnableSecuritySignature’ functions in the ‘LanmanServer’ domain by changing their values from ‘0’ to ‘1’; which are shown in Figures 5 and 6. These changes in policy mean all communication over the SMB protocol must now include a cryptographic signature to ensure the

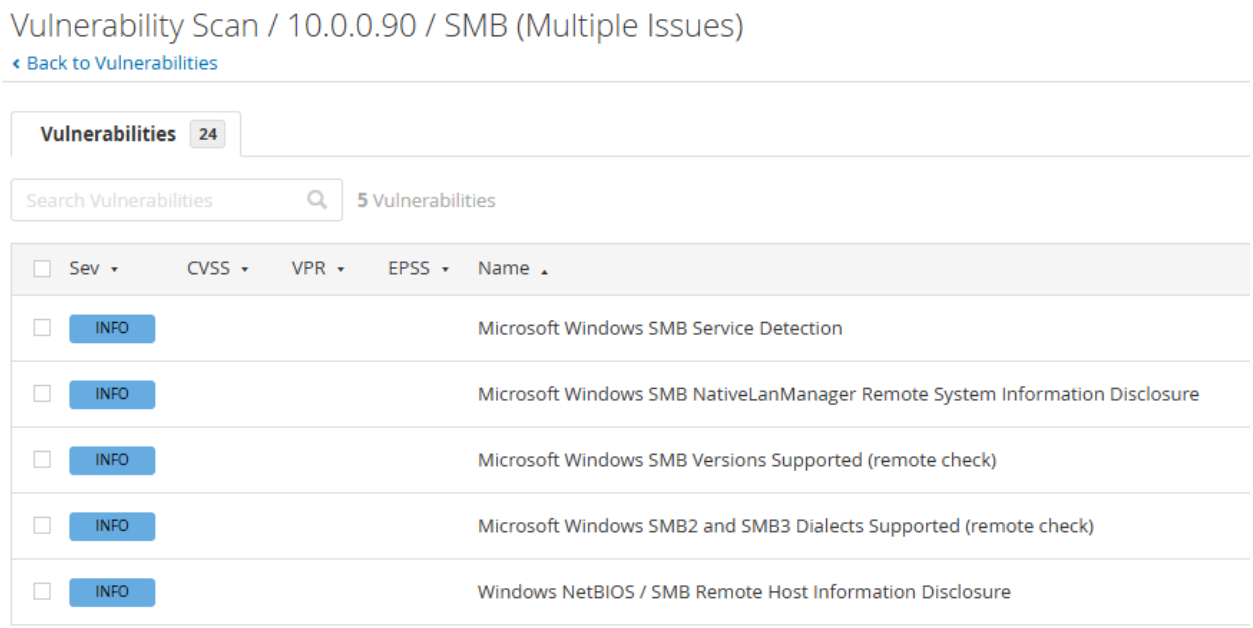
authenticity and integrity of the data being exchanged. I then ran the vulnerability scan again and the alert was no longer present, as shown in Figure 7.

Figures 5, 6, 7: Altered Registry Editor SMB Parameters and

Nessus Scan Showing Remediated SMB Vulnerability







Conclusion:

I performed a vulnerability scan of a LAN using Nessus. First, I identified all the network hosts, and then I analyzed the most significant vulnerability found, which was an SMB-related vulnerability. Lastly, I remediated the vulnerability by changing the SMB signing policies to require that the network clients and servers always digitally sign communications.