

Nessus Vulnerability Scan

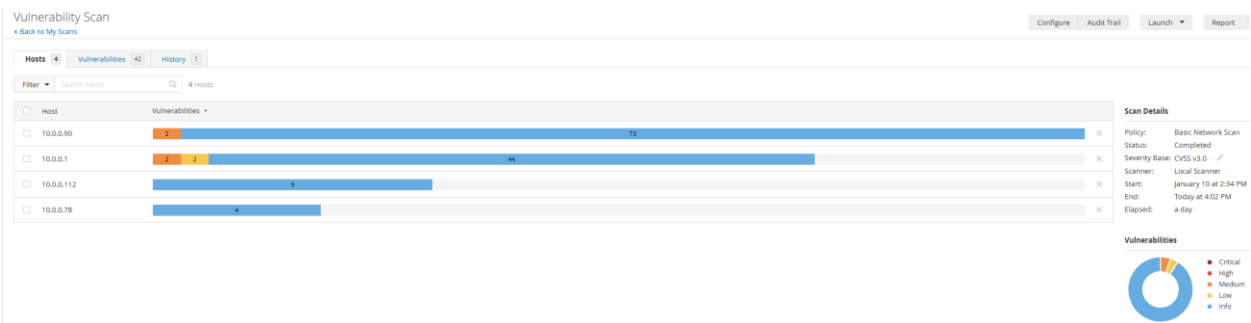
Project:

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

Vulnerability Scan / Plugin #57608

Configure Audit Trail Launch Report Export

Hosts 4 Vulnerabilities 42 History 2

Medium SMB Signing not required

Description
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also
<http://www.nessus.org/u/7f3988b3>
<http://technet.microsoft.com/en-us/library/cc731957.aspx>
<http://www.nessus.org/u/7f4b80723>
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
<http://www.nessus.org/u/3c3ac3ea>

Output
No output recorded.

To see debug logs, please visit individual host

Port	Hosts
445 / tcp / c6	10.0.0.90

Plugin Details

Severity: Medium
ID: 57608
Version: 1.20
Type: remote
Family: Misc.
Published: January 19, 2012
Modified: October 5, 2022

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/AU:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.7
CVSS v2.0 Vector: CVSS:2.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/AU:N
CVSS v2.0 Temporal Vector: CVSS:2.0/E:U/RL:O/RC:C

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters

Name	Type	Data
(Default)	REG_SZ	(value not set)
EnablePlainText...	REG_DWORD	0x00000000 (0)
EnableSecuritySi...	REG_DWORD	0x00000001 (1)
RequireSecurity...	REG_DWORD	0x00000000 (0)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\wkssvc.dll
ServiceDllUnloa...	REG_DWORD	0x00000001 (1)

Registry Editor

File Edit View Favorites Help

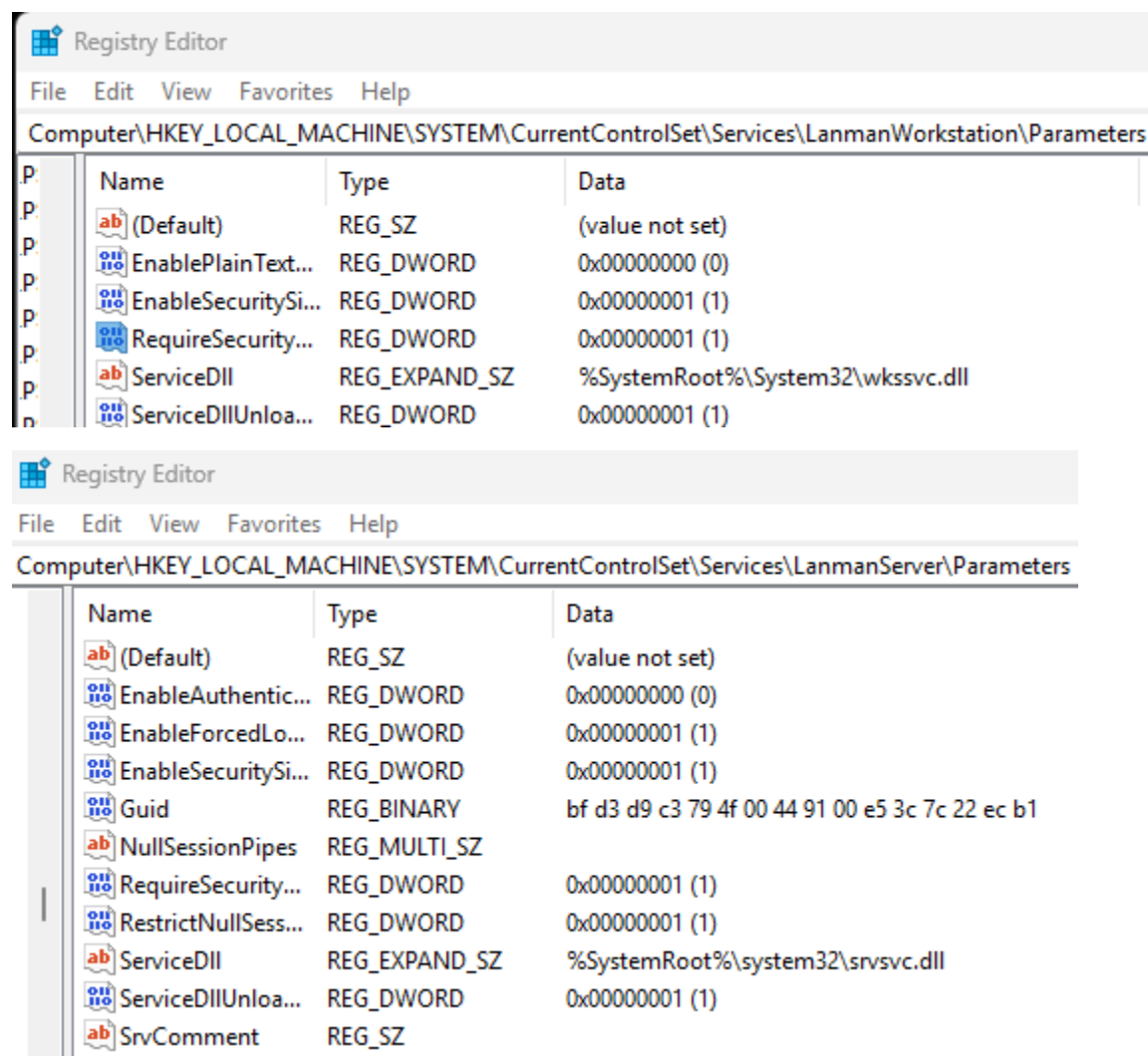
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Name	Type	Data
(Default)	REG_SZ	(value not set)
EnableAuthentic...	REG_DWORD	0x00000000 (0)
EnableForcedLo...	REG_DWORD	0x00000001 (1)
EnableSecuritySi...	REG_DWORD	0x00000000 (0)
Guid	REG_BINARY	bf d3 d9 c3 79 4f 00 44 91 00 e5 3c 7c 22 ec b1
NullSessionPipes	REG_MULTI_SZ	
RequireSecurity...	REG_DWORD	0x00000000 (0)
RestrictNullSess...	REG_DWORD	0x00000001 (1)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\svrsvc.dll
ServiceDllUnloa...	REG_DWORD	0x00000001 (1)
SrvComment	REG_SZ	

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



Vulnerability Scan / 10.0.0.90 / SMB (Multiple Issues)

[← Back to Vulnerabilities](#)

Vulnerabilities 24

Search Vulnerabilities



5 Vulnerabilities

<input type="checkbox"/>	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▲
<input type="checkbox"/>	INFO				Microsoft Windows SMB Service Detection
<input type="checkbox"/>	INFO				Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
<input type="checkbox"/>	INFO				Microsoft Windows SMB Versions Supported (remote check)
<input type="checkbox"/>	INFO				Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
<input type="checkbox"/>	INFO				Windows NetBIOS / SMB Remote Host Information Disclosure

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.