Yuyang Zhang
zhang.yuya@husky.neu.edu

Lab report for vulnerability scan

1. Clarifications for vulnerability reports provided:

The report for windows machine found at 10.0.0.113 is named as 10.0.0.113.html

The report for LIN machine found at 10.0.0.124 is named as 10.0.0.124.html

For local Linux machine, the result for scanning eth1(10.0.100.1), eth0(192.168.254.15) and localhost(127.0.0.1) are the same. These three reports are aiming at the same local machine, so the outputs are the same.

2. Two high or medium vulnerabilities analysis:

(i) Vulnerability:

High (CVSS: 10.0)

NVT: SMBv1 Unspecified Remote Code Execution (Shadow Brokers) (OID: 1.3.6.1.4.1.25623.1.0.140151)

The vulnerabilities is found at port 445 TCP at 10.0.0.113(Windows).

Cause of this vulnerabilities:

SMBv1 server has a loophole that could enable the attackers to authenticate himself to SMBv1 server and have the authorization to execute code remotely.

(according to Microsoft Bulletin https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)

Steps to remediate this vulnerability:

1. To disable SMBv1 on the SMB server, run the following cmdlet:

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 –Force

2. Disable SMB v1 and/or block all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices. (according to the suggestion given by the scan report)

3. To remediate the whole loophole, update the latest patch concerning SMB servers.

(ii)Vulnerability:

Medium (CVSS: 4.3)

NVT: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611)

This vulnerability is found at port 22 at 10.0.0.124.

Cause of this vulnerability:
The remote SSH server is configured to allow weak encryption algorithms:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc

Steps to remediate this vulnerability:
1. Disable the weak encryption algorithms.

3. Are vulnerability scanners efficient in finding all the vulnerabilities of a system? Explain some situations where vulnerability scanners may not work efficiently.

Vulnerability tests are efficient when finding all the known vulnerabilities included in the database of OpenVAS. But it is not useful to find the new loopholes or vulnerabilities that are not updated in the database.