Assignment Day 4 | 23rd August 2020

Question 1:

Find out the mail servers of the following domain:

a. Ibm.com

   responsible mail addr = hostmaster.akamai.com

b. Wipro.com

   responsible mail addr = awsdns-hostmaster.amazon.com

Question 2:

Find the locations, where these email servers are hosted.

a. ibm.com

b. Wipro.com

Question 3:

Scan and find out port numbers open 203.163.246.23

Question 4:

Install nessus in a VM and scan your laptop/desktop for CVE.

Scan Information

Start time: Wed Aug 26 10:35:50 2020

End time: Wed Aug 26 10:43:59 2020

Host Information

Netbios Name: DESKTOP-A90FB85

IP: 192.168.1.6

OS: Windows

Vulnerabilities

57608 - SMB Signing not required-

Synopsis

Signing is not required on the remote SMB server.

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.

See Also

https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

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.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Published: 2012/01/19, Modified: 2018/11/15

Plugin Output

tcp/445/cifs