Microsoft bsa

Technology, Information Technology

Question # 2 – Part a The Microsoft Baseline Security Analyzer (MBSA) tool provides multiple scan facilities to assess the weak local account passwords. The MBSA checks the passwords keeping in view the characteristics of the weak passwords include: the blank passwords, simple or easy to crack passwords and the password that is the same as the username (Green & Richard, 2011).

Question # 2 – Part b

One of the main reasons for emphasizing the strong passwords is that despite the development and implementation of latest technologies to protect secured information, the information can easily have unauthorized access if the user has not developed a strong password to secure its personal information. Moreover, most of the information leakage is due to the same reason, as a common hacker can attack to the vulnerability of weak password and break into your information (Green & Richard, 2011).

Question # 2 – Part c

The option of adopting the strong password policy set restricts the users to develop strong local account passwords. Therefore, after setting the strong password policy the user cannot develop simple, easy to crack, blank and / or the password that is the same as the username to avoid hacking and information leakage vulnerability (Green & Richard, 2011).

Question # 3 – Part a

The Malware attacks the digital information in multiple ways. The Malware gets downloaded with the product being downloaded and starts working slowly with the passage of time. Some of the Malware irritates by displaying diverse pop-ups, as the malicious pop-up program runs secretly in the

downloaded product (SpamLaws, n. d).

Question # 3 – Part b

There are many types of Malware that include but not limited to the Adware, Bot, Bug, Ransomware, Rootkit, Spyware, Trojan Horse, Virus and Worm (Lord, 2011). There are several software applications that could be utilized in the computers to prevent the Malware including anti-virus and anti-adware.

Question # 4 – Part a

The Conficker is a computer worm that has ability to infect a computer and widen itself automatically (without human interaction) to the other computer over the computer network. The Conficker worm attacks the computer network services through the internet on diverse Microsoft's operating systems including Windows 2000, XP and Windows Server 2008 etc. The Microsoft launches out-of-band patch in 2008 to avoid the Conficker attacks (Microsoft, 2013).

Question # 4 – Part b

The organizations could use the MBSA to detect the missing patches by utilizing the security information automatically received through the application of Conficker programs in the computer systems. Moreover, the Windows operating systems have ability to automatically check the updates; therefore, the missing patches can easily be recognized by the Microsoft.

Question # 5

After thorough analysis and assessment of the current version of the Microsoft Baseline Security Analyzer, it has been observed that there are several features could be added to the MBSA. In order to protect computer from the unauthorized users, the MBSA should have the ability to turn off

computer after three incorrect password attempts. Moreover, the verification key can be introduced for proper authentication of the computer password. This feature would reduce the frequency of changing the password frequently as per the policy of the MBSA.

References

Green, J. & Richard, A. (2011). Microsoft Baseline Security Analyzer Vulnerability Scanner. Retrieved from: http://www. famu. edu/cis/project3. pdf

SpamLaws. n. d. How Malware Works. Retrieved from: http://www. spamlaws. com/how-malware-works. html

Lord, N. (2011). Common Malware Types: Cyber-security 101. Retrieved from: http://www. veracode. com/blog/2012/10/common-malware-types-cybersecurity-101/

Microsoft. (2013). Protect your Computer from the Conficker Worm Virus. Retrieved from: http://www. microsoft. com/security/pc-security/conficker. aspx